POLSKA AKADEMIA NAUK

Instytut Podstawowych Problemów Techniki

ROZPRAWA DOKTORSKA

mgr Aneta Maria Wróblewska

Lingwistyczne układy dynamiczne oparte na grafach algebraicznych i ich zastosowanie w kryptografii

Promotor
prof. dr hab. Vasyl Ustimenko

Warszawa 2016

Pragnę złożyć serdeczne podziękowania wszystkim osobom, które swoimi cennymi uwagami przyczyniły się do realizacji rozprawy doktorskiej, w szczególności Profesorowi Vasylowi Ustimenko za okazaną życzliwość, opiekę, poświęcony czas oraz wskazówki udzielone mi w toku realizacji przewodu doktorskiego.

Spis treści

Wstęp

Tło badań

Szybki wzrost technologii informacyjnych prowadzi do znacznego rozwoju nowych systemów bezpieczeństwa. Dane przechowywane w komputerach, informacje przesyłane przez sieć muszą być bezpieczne. Dziedziną zajmującą się praktycznym zastosowaniem wiedzy matematycznej w celu ochrony danych jest kryptografia. Dzisiaj, żyjąc w społeczeństwie informacyjnym, wszelka postać informacji stała się jednym z najważniejszych towarów, już nie tylko dla sfer wojskowych, ale również dla wszystkich ludzi. Szyfrowanie zatem jest strażnikiem naszej prywatności i poufności. Używamy kryptografii do kontrolowania dostępu, elektronicznych płatności (zakupy przez Internet) czy w bezpiecznej wymiany korespondencji. Coraz więcej firm oraz osób prywatnych używa rozmaitych urządzeń i oprogramowania, których cechą wspólną jest wykorzystywanie silnych algorytmów kryptograficznych do ochrony prywatności oraz autentyczności przesyłanych informacji. Ważne jest to, aby zaszyfrowanej wiadomości nie można było odczytać w rozsądnym czasie. Wiadomo bowiem, że nie ma takiego algorytmu, którego nie dałoby się złamać w ogóle. Istnieją natomiast sposoby, by zadanie to skomplikować w stopniu znaczącym, tak iż setki a nawet tysiące komputerów nie mogłoby znaleźć odpowiedzi przez wiele lat.

Obecny stan wiedzy w dziedzinie bezpieczeństwa informacyjnego nie jest dostateczny dla zaspokojenia wymagań społeczeństwa. Niestety, dość często zdarzają sie udane ataki elektroniczne na chronione dane. Komputery są coraz szybsze, dostępne są prototypowe modele komputera kwantowego, możemy wiec spodziewać sie bardziej wzmożonych ataków. Z powyższych powodów, naturę interdyscyplinarną mają rozwijane w mojej rozprawie doktorskiej - sfera kryptografii oraz badania naukowe w tym kierunku. W celu udowodnienia poziomu bezpieczeństwa algorytmów wykorzystywane są różne dziedziny matematyki i informatyki.

Kryptografia wielu zmiennych, rozwijana w mojej pracy, daje możliwość użycia zarówno w konwencjonalnych, jak również kwantowych komputerach. Najbardziej popularne algorytmy w kryptografii wielu zmiennych oparte są o wielomiany drugiego stopnia. Rozwiązania takiego układu równań jest problemem NP-zupełnym. Zatem tego typu schematy są dobrymi kandydatami w kryptografii post-kwantowej, gdyż tradycyjne kryptosystemy oparte na trudnych problemach Teorii Liczb, mogą być z łatwością złamane dzięki komputerom kwantowym. Imai i Matsumoto w 1988r. zaproponowali pierwszy kryptosystem (MIC) oparty na odwzorowaniu grupy Cremona nad ciałem skończonym charakterystyki 2. Był to kryptosystem wydajny dla implementacji, niestety w 1995r. złamany przez Patarina. Nowy, rozważany w tej rozprawie, kierunek zastosowania kryptografii wielu zmiennych oparty jest z kolei na teorii układów dynamicznych, który jest rozważany w tej rozprawie.

Cel i zakres pracy

Rozprawa doktorska ma na celu skonstruowanie oraz badanie własności lingwistycznych układów dynamicznych opartych na grafach algebraicznych oraz ich potencjalne zastosowanie w algorytmach kryptograficznych. W tym celu wygenerowane zostały specjalne podgrupy grupy Cremona działające na modułach wolnych ogólnego wymiaru n nad pierścieniem przemiennym. Utworzone przez nas podgrupy zawierają grupy cykliczne dużego rzędu składające się z nieliniowych przekształceń wielomianowych o określonym stopniu. Poszukiwane są takie odwzorowania, których stopień jest ograniczony przez pewną niewielką stałą (co sprzyja szybkiej implementacji), zaś rząd tego odwzorowania dąży do nieskończoności (odpowiada za zwiększenie bezpieczeństwa). Obliczenia wykonywane w sposób symboliczny dodatkowo sprzyjają bezpieczeństwu i lepszej ochronie danych.

W pierwszej kolejności w rozprawie badane są problemy istnienia oraz własności układów dynamicznych utworzonych przez rodziny przekształceń o maksymalnym stopniu równym dwa, trzy i cztery, o dużym rzędzie, należących do grupy stabilnej. Stabilność grupy daje nam możliwość uzyskania lingwistycznego układu dynamicznego, w którym przekształcenia powstałe przez złożenie dowolnej ilości przekształceń z tej grupy mają ten sam stopień. Problem ten jest następnie rozszerzony na grafy skierowane nad pierścieniem przemiennym. Rodziny przekształceń niskiego stopnia mogą znaleźć zastosowanie jako podstawa logarytmu dyskretnego, na którym polega bezpieczeństwo nowych algorytmów symbolicznych, w tym protokołu uzgodnienia klucza Diffiego-Hellmana. Niestety,

otrzymany w tych przypadkach, niski stopień przekształceń odwrotnych nie sprzyja bezpieczeństwu algorytmów asymetrycznych na nich opartych.

Bardzo ważnym czynnikiem w kryptografii wielu zmiennych jest stopień odwracalnych i wielowymiarowych odwzorowań stabilnych. Łatwość złamania przekształceń niższego stopnia wynika z tego, że przekształcenie deszyfrujące da sie przedstawić jako przekształcenie tej samej postaci co przekształcenie szyfrujące, czyli przekształcenie wielomianowe niewielkiego stopnia. Umożliwia to obliczenie wszystkich współczynników wielomianów tego przekształcenia po wygenerowaniu odpowiedniej liczby szyfrogramów dla zadanych tekstów jawnych. Z powyższego powodu, w dalszej części pracy skupiamy się nad rodzinami przekształceń opartych na tych samych rodzinach grafów o dużej talii, ale pozbawionych przedstawionej wady. W tym celu dokonywane są modyfikacje przekształceń szyfrujących (np. technika kompresji grafu lub zaburzenie pierwszej współrzędnej), w taki sposób, aby możliwie zwiększyć stopień przekształcenia do niego odwrotnego. Zwiększenie stopnia odwzorowania szyfrującego powoduje lepszą odporność na ataki linearyzacji, przy czym ze względu na efektywność algorytmów, powinien być spełniony warunek wielomianowej gęstości. Znaleziona została rodzina przekształceń, dla której dzięki dowolnej regulacji stopniem odwzorowania i długością użytego hasła, można ustalać poziom bezpieczeństwa i efektywność obliczeń. W tym przypadku przekształcenia odwrotne mają stopień dostatecznie duży bądź trudny do określenia, co jest bardzo ważne w kryptografii wielu zmiennych. Bezpieczeństwo opisanych algorytmów kryptograficznych opiera się zatem na trudności znalezienia odwzorowania odwrotnego do nieliniowego bijektywnego odwzorowania wielomianowego wielu zmiennych oraz na problemie logarytmu dyskretnego w teorii grup.

W pracy doktorskiej użyta została teoria grafów algebraicznych, w celu skonstruowania lingwistycznego układu dynamicznego o zalecanych kryptograficznych właściwościach. Główne rezultaty opierają się na konstrukcji rodziny grafów $D(n, q)$ dużej talii i opisie jej spójnych składowych $CD(n, q)$. Istnienie nieskończonych rodzin grafów dużej talii zostało udowodnione przez Paula Erdösa ([5]). Razem z grafami Ramanujana wprowadzonymi przez G. Margulis [37] i badanymi w [36], grafy $CD(n, q)$ są jedną z pierwszych konstrukcji rodzin grafów nieograniczonego stopnia. Grafy $D(n, q)$ zostały również użyte w konstrukcji kodów LDPC oraz turbokodów (zastosowane w rzeczywistej komunikacji satelitarnej) ([10, 11, 44]) oraz dla rozwoju algorytmów klucza prywatnego ([54, 58, 69, 70]), jak również w kryptografii klucza publicznego w [17, 18, 19, 20, 56, 71, 72, 73, 70]. Istnienie lingwistycznych układów dynamicznych zostało udowodnione w [55], zaś kilka przykładów

konstrukcji możemy znaleźć w [29]. Pierwsza rodzina takich grafów nieliniowych była badana w projekcie National Science Foundation (USA).

Aktualnie prace nad zastosowaniem rodziny grafów $D(n, q)$ w kryptografii i teorii kodowania realizowane są przez grupę badawczą pod kierunkiem prof. dr hab. Vasyla Ustimenko. Kolejne wyniki prac wzajemnie się uzupełniają i są na bieżąco weryfikowane i modyfikowane przez członków grupy. Z tego powodu część wyników dotycząca implementacji rozpatrywanych algorytmów została zaczerpnięta z prac Klisowskiego i Ustimenko, jako że ich prace mają najbardziej zbliżony charakter do badań prezentowanych w rozprawie.

Na pierwszym etapie badań przeprowadziliśmy obliczenia symboliczne za pomocą dostępnych programów do obliczeń symbolicznych (np. Maple, Maxima), które posłużyły jako baza do sformułowania i udowodnienia większości twierdzeń z rozprawy. Niektóre z algorytmów zostały przetestowane przy pomocy oprogramowania stworzonego przez M. Klisowskiego, które zawiera odpowiednie biblioteki realizujące operacje symboliczne na wielomianach dla wybranych pierścieni przemiennych.

Struktura pracy

Układ niniejszej pracy przedstawia się następująco:

Rozdział 1 zawiera podstawowe zagadnienia matematyczne wykorzystywane w dalszej częsci pracy, m.in. elementy teorii grup, pierścieni skończonych, pierścieni wielomianów oraz modułów wolnych. W dalszej części przedstawiony jest problem logarytmu dyskretnego w teorii grup oraz zdefiniowane grupy stabilne i ich uogólnienia w przypadku pierścieni przemiennych. Rozdział ten zawiera również podstawowe definicje z teorii grafów.

Rozdział 2 opisuje podstawową terminologię z dziedziny kryptografii, kryptoanalizy, podział kryptosystemów na symetryczne i asymetryczne, uzgadnianie kluczy Diffiego-Hellmana oraz schemat szyfrowania ElGamal. Ważną częścią tego rozdziału jest opis kryptografii wielu zmiennych, do której w większości zaliczają się rozważane w pracy algorytmy kryptograficzne. Wspomniana jest także zagadnienie kryptografii opartej na teorii chaosu i układów dynamicznych.

Rozdział 3 wprowadza rodzinę grafów o dużej talii oraz grafów lingwistycznych, które posłużą głównie do konstrukcji specjalnych przekształceń wielomianowych, tworzących

lingwistyczne układy dynamiczne. Rozdział wprowadza następnie pojęcie linwistycznych układów dynamicznych oraz ich uogólnienie.

Rozdział 4 zawiera konstrukcję i analizę własności (w szczególności stopni) nieliniowych przekształceń wielomianowych, będących podstawą do tworzenia lingwistycznych układów dynamicznych. Rozważane w kolejnych podrozdziałach przekształcenia mają niski stopień: dwa, trzy oraz cztery. Konstrukcje oparte są na opisie grafów nieskierowanych, skierowanych oraz ich różnych modyfikacjach.

Rozdział 5 zawiera konstrukcję i analizę własności (w szczególności stopni) nieliniowych przekształceń wielomianowych określonego stopnia, większego od 4. Rezultat został osiągnięty na dwa sposoby. Pierwszy z nich opiera się na technice kompresjii grafu, poprzez zmniejszenie liczby spójnych składowych. Druga koncepcja umożliwia zwiększenie stopnia przekształceń, dzięki użyciu nieliniowego zaburzenia podczas zmiany koloru wierzchołka.

Rozdział 6 przedstawia możliwości zastosowania układów dynamicznych utworzonych przez przekształcenia wielomianowe, zdefiniowane w dwóch poprzednich rozdziałach, w algorytmach kryptograficznych: algorytmach symetrycznych, asymetrycznych oraz protokołach uzgadniania klucza Diffiego-Hellmana. Ze względu na czynniki, takie jak stopień, liczba jednomianów, rząd i gęstość, różne rodzaje przekształceń mogą mieć wielorakie zastosowania: przekształcenia niskich stopni w kryptografii symetrycznej oraz wymianie klucza, zaś wyższych stopni w algorytmach asymetrycznych. Przedstawione zostały również przykłady oraz wyniki symulacji komputerowych. Rozdział ten zawiera również powiązane wyniki prac z naszej grupy badawczej.

Rozdział 7 zawiera podsumowanie uzyskanych wyników rozprawy doktorskiej oraz elementy wkładu oryginalnego.

Rozdział 1

Podstawy matematyczne

W tym rozdziale przedstawione zostaną zagadnienia matematyczne wykorzystywane w dalszej części pracy. W początkowych podrozdziałach będą przypomniane podstawowe definicje i twierdzenia dotyczące teorii grup, pierścieni orach przestrzeni wektorowych. Wiadomości te zostały zaczerpnięte głównie z książek [1, 9, 26]. Następnie opisany zostanie problem logarytmu dyskretnego ([51]), teoria grup stabilnych z uogólnieniem w przypadku pierścieni przemiennych (wprowadzona w [67]) oraz wstępne definicje z teorii grafów (zaczerpnięte z [4] oraz [5]).

1.1 Grupy

Definicja 1.1. *Grupą* nazywamy zbiór G z działaniem dwuargumentowym $\cdot$ spełniających następujące warunki:

1. $\bigwedge\limits_{a,b,c\in G} (a \cdot b) \cdot c) = a \cdot (b \cdot c)$ (łączność)
2. $\bigvee\limits_{e\in G} \bigwedge\limits_{a\in G} e \cdot a = a \cdot e = a$, gdzie e nazywamy elementem neutralnym działania
3. $\bigwedge\limits_{a\in G} \bigvee\limits_{b\in G} a \cdot b = b \cdot a = e$, gdzie b nazywamy elementem odwrotnym do elementu a

Jeżeli operacja jest przemienna, tzn. $\bigwedge\limits_{a,b\in G} a \cdot b = b \cdot a$, to grupę G nazywamy przemienną lub abelową

Definicja 1.2. Jeżeli $(G, \cdot)$ jest grupą i H jest niepustym podzbiorem G, to $(H, \cdot)$ nazywamy *podgrupą* grupy $(G, \cdot)$, jeśli są spełnione następujące warunki:

1. $\bigwedge_{a,b \in H} a \cdot b \in H$ (domkniętość)

2. $\bigwedge_{a \in H} a^{-1} \in H$ (istnienie odwrotności)

Liczbę elementów grupy G oznaczamy symbolem $|G|$ i nazywamy *rzędem* grupy. Grupa G jest *skończona*, jeśli $|G|$ jest liczbą naturalną; w przeciwnym przypadku grupa G jest *nieskończona*.

Definicja 1.3. Grupę $(G, \cdot)$ nazywamy grupą cykliczną, jeśli istnieje element $g \in G$, taki, że $G = \{g^n | n \in \mathbb{Z}\}$ (każdy element można przedstawić jako potęgę pewnego ustalonego elementu). Element g nazywamy wtedy *generatorem* grupy cyklicznej. *Rzędem elementu* g w grupie $(G, \cdot)$ nazywamy najmniejszą liczę całkowitą dodatnią r, taką że $g^r = e$. Jeśli taka liczba nie istnieje, to mówimy, że element g ma rząd nieskończony.

Definicja 1.4. Niech będą dane dwie grupy $(G, \cdot)$ i $(H, \odot)$. Mówimy, że są one *izomorficzne*, jeżeli istnieje funkcja $\phi \colon G \to H$, taka, że

1. ϕ jest różnowartościowa;

2. ϕ jest "na";

3. ϕ zachowuje działanie, tzn.: dla każdego $x, y \in G$ zachodzi $\phi(x \cdot y) = \phi(x) \odot \phi(y)$.

Funkcję ϕ nazywamy *izomorfizmem* grupy G na grupę H. Jesli istnieje izomorfizm grup G i H, to mówimy, ze grupy G i H sa izomorficzne oraz piszemy $G \simeq H$. Izomorfizm grupy G na siebie nazywamy *automorfizmem* tej grupy. Odwzorowanie ϕ spełniające tylko trzeci z powyższych warunków nazywamy *homomorfizmem*. Homomorfizm grupy G w siebie nazywamy *endomorfizmem* grupy G.

1.2 Pierścienie i ciała

Definicja 1.5. Strukturę $(K, +, \cdot)$ nazywamy *pierścieniem*, jeżeli spełnione są następujące aksjomaty:

1. struktura $(K, +)$ jest grupą abelową.

2. $\bigwedge_{a,b,c \in K} (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (łączność działania $\cdot$)

3. $\bigwedge_{a,b,c \in K} a \cdot (b + c) = a \cdot b + a \cdot c$ oraz $(b + c) \cdot a = b \cdot a + c \cdot a$ (rozdzielność działania $\cdot$ względem działania $+$).

Jeśli istnieje element $1 \in K$, zwany jedynką, taki, że $1 \cdot a = a \cdot 1 = a$, to pierścień nosi nazwę *pierścienia z jedynką*. Jeśli działanie $\cdot$ jest przemienne, pierścień nazywa się *pierścieniem przemiennym*. Element $a \in K$ jest *dzielnikiem zera*, jeżeli istnieje niezerowy element $b \in K$ taki, że $ab = 0$. Element $a \in K$

Definicja 1.6. Niech K będzie pierścieniem przemiennym. Element a nazywamy odwracalnym w K, jeśli istnieje element $b \in K$, taki, że $ab = 1$. Elementami odwracalnymi w pierścieniu K są więc te elementy, które mają multiplikatywną odwrotność w R. Zbiór wszystkich odwracalnych elementów pierścienia K oznaczamy przez K^*.

Pierścień określony na zbiorze jednoelementowym nazywamy pierścieniem trywialnym. Nietrywialny pierścień przemienny bez dzielników zera nazywamy *dziedziną całkowitości*.

Definicja 1.7. *Charakterystykę* dla danego pierścienia z jedynką definiujemy jako najmniejszą liczbę $,,1''$, czyli elementów neutralnych mnożenia, którą należy dodać, aby otrzymać $,,0''$ (element neutralny dodawania) pierścienia. Mówimy, że pierścień ma charakterystykę zero, jeżeli taka liczba nie istnieje. Charakterystykę danego pierścienia K oznaczamy przez $\mathrm{char}(K)$

Definicja 1.8. Pierścień jest *ciałem*, jeśli jego niezerowe elementy stanowią grupę abelową względem mnożenia, tj. ciałem jest każdy nietrywialny pierścień przemienny K, w którym dla każdego niezerowego elementu $a \in K$ istnieje $a^{-1} \in K$ taki, że $a \cdot a^{-1} = 1$. Każde ciało jest dziedziną całkowitości, a więc nie ma dzielników zera. Pierścień $\mathbb{Z}_n$ jest ciałem wtedy i tylko wtedy, gdy n jest liczbą pierwszą. W danym ciele każdy element niezerowy jest odwracalny.

Twierdzenie 1.1. *[52] Niech q będzie liczbą pierwszą, zaś $\mathbb{F}_q^*$ zbiorem niezerowych elementów ciała $\mathbb{F}_q$. Wtedy istnieje element $g \in \mathbb{F}_q^*$, którego potęgi generują cały zbiór $\mathbb{F}_q^*$, czyli:*

$$\mathbb{F}_q^* = \{1, g, g^2, g^2, \cdots, g^{q-2}\} \tag{1.1}$$

Elementy o takiej własności nazywamy pierwiastkami pierwotnymi lub generatorami ciała $\mathbb{F}_q^*$.

Poniżej przedstawimy kilka przykładów grup, pierścieni i ciał, pośrednio lub bezpośrednio użytych w rozprawie (szczegóły można znaleźć w [2] oraz [3]):

1. *Multiplikatywna grupa klas reszt modulo m* - grupa, którą można traktować jako zbiór liczb naturalnych mniejszych od m i względnie pierwszych z m. $\mathbb{Z}_m^* = \{k \in \mathbb{N}: \quad 1 \leq k \leq, \quad NWD(k,m) = 1\}$, z działaniem $\odot$ zdefiniowanym w sposób następujący: dla $x, y \in \mathbb{Z}_m^*$, $x \odot y$ z definicji jest resztą z dzielenia iloczynu liczb x i y przez m.

2. *Ogólna grupa liniowa* $\mathrm{GL}_n(K)$ - zbiór wszystkich macierzy odwracalnych stopnia n nad ustalonym ciałem K. Wraz z operacją mnożenia macierzy zbiór ten tworzy grupę. Podzbiór $\mathrm{SL}_n(K) = \{x \in \mathrm{GL}_n(K): \quad \det(x) = 1\}$ wraz z ograniczoną do niego operacją mnożenia jest także grupą. Jest to podgrupa grupy $\mathrm{GL}_n(K)$.

3. *Grupa afiniczna* $\mathrm{AGL}_n(K)$. Grupa afiniczna (będąca rozszerzeniem $\mathrm{GL}_n(K)$) przestrzeni afinicznej nad ciałem K jest grupą wszystkich odwracalnych przekształceń afinicznych przestrzeni na siebie. Przekształcenie afiniczne można przedstawić jako złożenie dwóch funkcji - przesunięcia $(\vec{b})$ oraz odwzorowania liniowego (A), w postaci $\vec{y} = A\dot{\vec{x}} + \vec{b}$.

4. *Grupa permutacji (grupa symetryczna).* Niech n będzie ustaloną liczbą naturalną i $X = \{1, 2, 3, \ldots, n\}$. Permutacją zbioru X na siebie nazywamy dowolne, wzajemnie jednoznaczne odwzorowanie tego zbioru na siebie. Niech S_n będzie zbiorem wszystkich permutacji zbioru X. Permutację $F \in \mathrm{S}_n$, można zapisać w postaci:

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ f(1) & f(2) & f(3) & \ldots & f(n) \end{pmatrix}$$

W zbiorze S_n wprowadzamy operację złożenia odwzorowań: jeśli

$$g = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ g(1) & g(2) & g(3) & \ldots & g(n) \end{pmatrix},$$

to przyjmujemy

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ g(f(1)) & g(f(2)) & g(f(3)) & \ldots & g(f(n)) \end{pmatrix}.$$

Zbiór S_n wraz z tą operacją tworzy grupę. Istotnie, złożenie odwzorowań jest działaniem łącznym. Elementem neutralnym działania jest przekształcenie tożsamościowe:

$$e = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

Elementem odwrotnym do f jest funkcja do niej odwrotna:

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & f(3) & \dots & f(n) \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f^{-1}(1) & f^{-1}(2) & f^{-1}(3) & \dots & f^{-1}(n) \end{pmatrix}.$$

S_n nazywamy *grupą symetryczną* stopnia n. Wiadomo, że rząd tej grupy wynosi $|\,\mathrm{S}_n\,| = n!$ oraz jeśli G jest skończoną grupą rzędu n, to G jest izomorficzna z podgrupą grupy symetrycznej S_n (tw. Cayleya).

5. *Pierścień klas reszt modulo m* - pierścień, którego elementami są klasy reszt modulo m. Można go traktować jako zbiór $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ z działaniami $+$ i $\cdot$, zdefiniowanymi w następujący sposób: dla $x, y \in \mathbb{Z}_m$, $x + y$ z definicji jest resztą z dzielenia sumy liczb x i y przez m, zaś $x \cdot y$ - resztą z dzielenia iloczynu liczb x i y przez m.

6. *Ciało skończone $\mathbb{F}_q$* - ciało skończone mające q elementów.

7. *Rozszerzenie ciała $\mathbb{F}_p$ stopnia n* Niech $\mathbb{F}_p$ będzie ciałem prostym, a $m \in \mathbb{F}_p[u]$ nierozkładalnym wielomianem zmiennej u nad ciałem $\mathbb{F}_p$ stopnia n. Przez $\mathbb{F}_p[u]/(m)$ oznaczamy zbiór klas reszt wielomianów z $\mathbb{F}_p[u]$ modulo m. Zbiór ten wraz z operacją zwykłego dodawania wielomianów w $\mathbb{F}_p[u]$ oraz operacją mnożenia wielomianów modulo m tworzy ciało o rozmiarze p^n.

8. *Pierścień Bool'a $\mathbb{B}_n$* - pierścień, w którym dla każdego elementu pierścienia $x \in \mathbb{B}_n$ mamy $x^2 = x$. Pierścieniem Bool'a jest zbiór 2^A z operacjami różnicy symetrycznej i części wspólnej zbiorów, gdzie 2^A oznacza zbiór wszystkich podzbiorów zbioru skończonego o mocy n.

1.2.1 Zbiory i generatory multiplikatywne

Niech $\mathbb{K}$ oznacza pierścień przemienny.

Definicja 1.9. Zbiór Q pierścienia K jest *zbiorem multiplikatywnym* pierścienia K, jeśli jest domknięty ze względu na operację mnożenia ($x, y \in Q \Rightarrow x \cdot y \in Q$) i nie zawiera 0.

Przykłady zbiorów multiplikatywnych:

1. grupa multiplikatywna $\mathbb{F}_q^*$ ciała skończonego $\mathbb{F}_q$, $q = p^n$, gdzie p jest liczbą pierwszą,
2. $Q_a = \{b \in \mathbb{Z}_m : \ NWD(a, b) = 1\}$, gdzie $\mathbb{Z}_m$ jest pierścieniem reszt modulo n,$a \in \mathbb{Z}_m$,
3. $Q_i = \{y \in \mathbb{B}_m : y_i = 1\}$, gdzie $\mathbb{B}_m = \{f : \{1, 2, \ldots, m\} \to \mathbb{F}_2\}$,
4. $\mathrm{Reg}(K)$ - zbiór elementów regularnych pierścienia K (tzn. nie bedących dzielnikami zera w K).

Elementy $t_1, t_2, \ldots, t_s$, $s \geq 1$ z K nazywamy *multiplikatywnymi generatorami*, jeśli istnieje zbiór multiplikatywny Q zawierający wszystkie t_i, $i = 1, 2, \ldots, s$.

Symbol $< t_1, t_2, \ldots, t_s >$ oznacza minimalny podzbiór multiplikatywny K zawierający wszystkie multiplikatywne generatory t_i.

1.3 Pierścienie wielomianów

Definicja 1.10. Jeśli K jest pierścieniem przemiennym, to *pierścieniem wielomianów* jednej zmiennej x nad pierścieniem K nazywamy zbiór wszystkich wyrażeń $p(x)$ postaci:

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

gdzie $a_a, a_2, \ldots, a_n \in K$ i $n \in \mathbb{N}$. Element a_i nazywamy *współczynnikiem* przy x^i w $p(x)$. Jeśli n jest największą liczbą całkowitą, dla której $a_n \neq 0$, mówimy, że wielomian $p(x)$ ma *stopień* n i piszemy $\deg p(x) = n$.

Definicja 1.11. Pierścieniem wielomianów n zmiennych nad pierścieniem K (oznaczanym przez $K[x_1, x_2, \ldots, x_n]$) nazywamy zbiór wszystkich wielomianów f, zmiennych $x_1, x_2, \ldots, x_n$ o współczynnikach z K następującej postaci:

$$f = \sum_{i_1,i_2,\ldots,i_n \leq s} t_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

gdzie $s \in \mathbb{N}$, $i_1, i_2, \ldots, i_n \in \mathbb{N}$ oraz $t_{i_1,i_2,\ldots,i_n} \in K$. Wyrażania $t x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$, gdzie $t \in K$ oraz $i_1, i_2, \ldots, i_n \in \mathbb{N}$ nazywamy *jednomianami*.

Stopniem wielomianu (oznaczanym przez $\deg(f)$) nazywamy dodatnią liczbę całkowitą d, dla której istnieje różny od zera współczynnik $t_{i_1,i_2,\ldots,i_n}$, taki, że $i_1 + i_2 + \cdots + i_n = d$ oraz $t_{j_1,j_2,\ldots,j_n} = 0$ gdy $j_1 + j_2 + \cdots + j_n > d$

Niech dane będzie odwzorowanie wielomianowe n zmiennych oraz stopnia d następującej postaci:

$$f = \sum_{i_1,i_2,\ldots,i_n \leq d} t_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

gdzie $d \in \mathbb{N}$, $i_1, i_2, \ldots, i_n \in \mathbb{N}$ oraz $t_{i_1,i_2,\ldots,i_n} \in K$.

Liczba jednomianów powyższego wielomianu jest liczbą d-elementowych kombinacji z powtórzeniami zbioru n-elementowego, czyli $\binom{n+d-1}{d}$.

Wynika stąd, że liczbę jednomianów (ozn. $L_{n,d}(f)$) wielomianu n zmiennych stopnia nie większego od d można wyrazić następującym wzorem:

$$L_{n,d}(f) = \sum_{k=0}^{d} \binom{n+k-1}{k} = \binom{n+d}{d}. \tag{1.2}$$

Liczba jednomianów w tym przypadku może być zatem oszacowana jako $\mathcal{O}(n^d)$ (dowód indukcyjny tego faktu można znaleźć w pracy [16]).

1.4 Przestrzenie wektorowe, moduły i moduły wolne

Definicja 1.12. Przestrzenią liniową (wektorową) nad ciałem F nazywamy strukturę matematyczną $(V, F, +, \cdot)$, w której:

- $(V, +)$ jest grupą abelową,
- dla wszystkich $x, y \in V$, $a, b \in F$ zachodzą równania:
  - $a \cdot (x + y) = a \cdot x + a \cdot y$
  - $(a + b) \cdot x = a \cdot x + b \cdot x$

- $a \cdot (b) \cdot x = (a \cdot b) \cdot x$
- $1 \cdot x = x$

Elementy zbioru V nazywamy wektorami, zaś elementy zbioru F skalarami. Dowolny uporządkowany zbiór n wektorów liniowo niezależnych n - wymiarowej przestrzeni V nazywamy bazą przestrzeni.

Uogólnieniem przestrzeni wektorowej nad ogólny pierścień przemienny K jest pojęcie *modułu* nad pierścieniem K (innymi słowy: moduły nad ciałami nazywamy przestrzeniami wektorowymi). Moduł posiadający bazę nazywamy *modułem wolnym*.

Przykłady:

1. pierścień wielomianów $K[x]$ o współczynnikach z K jest modułem nad pierścieniem K z mnożeniem:

$$a \sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} (a a_i) x^i$$

2. modułem jest zbiór $K^n = K \times \cdot \times K$ z działaniami:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

oraz

$$a \cdot (x_1, \ldots, x_n) = (a \cdot x_1, \ldots, a \cdot x_n)$$

Elementy zbioru K^n nazywamy wektorami o współczynnikach należących do K.

1.5 Problem logarytmu dyskretnego

Pierwsza opublikowana konstrukcja klucza publicznego, według Diffiego i Hellmana ([7]), opierała się na problemie logarytmu dyskretnego w ciele skończonym $\mathbb{F}_p$. Niech p będzie dużą liczbą pierwszą. Każdy niezerowy element $\mathbb{F}_p^*$ jest równy pewnej potędze generatora g ((1.1)), co oznacza, że lista elementów

$$\{1, g, g^2, g^2, \ldots, g^{p-2}\} \in \mathbb{F}_p^*$$

wyczerpuje listę wszystkich elementów $\mathbb{F}_p^*$ w pewnej kolejności.

Definicja 1.13. Niech g będzie generatorem ciała $\mathbb{F}_p$ oraz h będzie niezerowym elementem $\mathbb{F}_p$. Problem logarytmu dyskretnego jest problemem znalezienia liczby całkowitej x, takiej że:

$$g^x \equiv h \quad (\mod p).$$

Wykładnik x nazywamy logarytmem dyskretnym h przy podstawie g modulo p i oznaczamy $\log_g(h)$

Logarytm dyskretny nie zawsze istnieje, a nawet jeżeli istnieje może nie być określony w sposób jednoznaczny. Najszybszy algorytm (sito ciała liczbowego w ciałach $\mathbb{F}_p$) ma złożoność czasową $\exp c \log_2^{\frac{1}{3}}(p) \log_2^{\frac{2}{3}}(\log_2(p))$, gdzie c jest pewną stałą. Jedną z metod, dla ogólnej grupy cyklicznej, jest redukcja Pohliga-Hellmana.

Definicja 1.14. Problem logarytmu dyskretnego może być sformułowany dla ogólnej grupy skończonej G: "znalezienie liczby całkowitej dodatniej x spełniającej warunek $g^x = b$ gdzie $g \in G$ oraz $b \in G$".

Problem ten jest powszechnie uważany za trudny do rozwiązania. Nawet w przypadku grupy cyklicznej C istnieje wiele problemów otwartych. Jeśli $C = \mathbb{Z}^*_{p-1}$ lub $C = \mathbb{Z}^*_{pq}$ gdzie p oraz q są „dostatecznie dużymi" liczbami pierwszymi, wtedy złożoność problemu logarytmu dyskretnego uzasadnia klasyczny protokół uzgodnienia klucza Diffiego-Hellmana oraz algorytm generowania klucza publicznego RSA. W większości pozostałych przypadków złożoność problemu logarytmu dyskretnego nie jest zbadana dokładnie. Problem jest bardzo zależny od wyboru podstawy g oraz sposobu reprezentacji danych w grupie. Grupa może być zdefiniowana poprzez generatory i relacje, jako grupa automorfizmów rozmaitości algebraicznej, jako grupa macierzy, jako grupa permutacji, itd.

Przyjmujemy tutaj, że G jest podgrupą grupy S_{p^n}, która jest grupą wielomianowych bijektywnych transformacji przestrzeni wektorowej ${\mathbb{F}_p}^n$ na siebie. Oczywiście $|S_{p^n}| = (p^n)!$, każda permutacja π może być zapisana w formie $x_1 \to f_1(x_1, x_2, \ldots x_n), x_2 \to f_2(x_1, x_2, \ldots x_n), \ldots, x_n \to f_n(x_1, x_2, \ldots x_n)$, gdzie f_i są wielomianami wielu zmiennych z $\mathbb{F}_p[x_1, x_2, \ldots, x_n]$. Jako reprezentacje G wybieramy podgrupę S_{p^n} ze względu na zastosowanie obliczeń symbolicznych w protokole uzgodnienia klucza Diffiego-Hellmana. Innym powodem jest uniwersalność: z klasycznego rezultatu Cayleya wynika, że każda grupa skończona G może być wybrana jako podgrupa S_{p^n} dla odpowiednich p i n na różne sposoby.

1.6 Grupy stabilne

Definicja 1.15. Ciąg elementów $g_n \in G_n$ taki, że wszystkie jego nieidentyczne potęgi są stopnia c, nazywamy *elementami stabilnego stopnia*. Jest to równoznaczne ze stabilnością rodziny grup cyklicznych generowanych przez g_n, co zostało wykorzystane jako bardzo istotny element w protokołach Diffiego-Hellmana.

Grupa afiniczna $AGL_n(\mathbb{F}_p)$, $n \to \infty$ tworzy rodzinę podgrup stabilnego stopnia dla $c = 1$ oraz wszystkie transformacje afiniczne są stabilnego stopnia. Zauważmy, że jeśli g jest liniowym diagonalizowalnym elementem $AGL_n(\mathbb{F}_p)$, wtedy problem logarytmu dyskretnego dla podstawy g jest równoważny klasycznemu problemowi w teorii liczb. Oczywiście w tym przypadku tracimy korzyści płynące z obliczeń symbolicznych.

Weźmy podgrupę H grupy $AGL_n(\mathbb{F}_p)$ i rozważmy jej sprzężenie z nieliniowym bijektywnym odwzorowaniem wielomianowym f. Wtedy grupa $H' = f^{-1}Hf$ będzie również grupą stabilną, ale dla większości par f i H grupa H' będzie miała stopień $\deg f \times \deg f^{-1} \geq 4$, co wynika z nieliniowości f i f^{-1}. Wynika stąd, że problem konstrukcji nieskończonej rodziny podgrup G_n w grupie S_{p^n} stopnia 2 i 3 jest bardzo interesujący.

Ogólny problem konstrukcji nieskończonej rodziny podgrup stabilnych G_n grupy S_{p^n} stopnia c, spełniających pewne dodatkowe warunki (np. nieograniczony wzrost minimalnego rzędu nieidentycznych elementów w grupie, istnienie dobrze zdefiniowanej granicy rzutowej) może być również interesujące z powodu możliwych zastosowań w kryptografii.

Zauważmy, że jeśli nawet sprzężymy nieliniowe odwzorowanie g z odwracalnymi transformacjami liniowymi $\tau \in AGL_n(\mathbb{F}_p)$, pewne znaczące parametry kryptograficzne g i $g' = \tau^{-1}g\tau$ mogą być różne. Oczywiście sprzężone generatory g i g' mają taką samą liczbę punktów stałych, taką samą strukturę cykliczną jak permutacje, ale zliczenie tych samych par współrzędnych $(x,\ g(x))$ i $(x\ ,\ g'(x))$ może przynieść różne rezultaty. Wynika stąd, że dwie sprzężone rodziny stabilnego stopnia nie są zupełnie równoznaczne, ponieważ odpowiednie kryptanalityczne problemy mogą mieć różną złożoność.

1.6.1 Uogólnienie problemu w przypadku pierścieni przemiennych

Uogólnimy powyższy problem dla przypadku grupy Cremona nad modułem wolnym K^n, gdzie K jest dowolnym pierścieniem przemiennym. Ze względu na zastosowania w kryptografii przypadek pierścieni skończonych jest bardziej istotny. Ciała skończone

$\mathbb{F}_{p^n}$, $n \geq 1$ i pierścienie cykliczne $\mathbb{Z}_m$ (zwłaszcza $m = 2^7$ (kody ASCII), $m = 2^8$ (kody binarne), $m = 2^{16}$ (arytmetyka z pojedynczą precyzją), $m = 2^{32}$ (arytmetyka z podwójną precyzją)) są najbardziej popularne.

Definicja 1.16. Niech K będzie pierścieniem przemiennym. Grupą Cremona $C(K^n)$ nazywamy ogół wszystkich odwracalnych przekształceń wielomianowych f modułu wolnego K^n na siebie, takich, że przekształcenie odwrotne f^{-1} jest również wielomianem. Innymi słowy, grupą Cremona jest zbiór wszystkich wielomianowych bijekcji przestrzeni K^n.

Wtedy naturalna jest zmiana przestrzeni wektorowej ${\mathbb{F}_p}^n$ na moduł wolny K^n oraz rodziny grup symetrycznych S_{p^n} na grupę Cremona $C(K^n)$ wszystkich wielomianowych automorfizmów K^n.

Powtórzymy teraz definicje dla bardziej ogólnego przypadku pierścieni przemiennych.

Definicja 1.17. Niech G_n, $n \geq 3$, $n \to \infty$ będzie ciągiem podgrup z $C(K^n)$. Mówimy, że G_n jest rodziną grup stabilnego stopnia (lub podgrup stopnia c), jeśli maksymalny stopień reprezentanta $g \in G_n$ jest równy pewnej niezależnej stałej c.

Pierwsza rodzina podgrup stabilnych z $C(\mathbb{F}_q^n)$, $K = \mathbb{F}_q$ ze stopniem $c = 3$ była skonstruowana i badana w [75], gdzie zostały policzone stopnie wielomianów klucza publicznego opartego na przejściu po grafie (ale nie został tam użyty język teorii grup oraz nie był rozważony problem wymiany klucza).

Symulacje komputerowe pokazują, że podgrupa stabilna odpowiadająca grafowi $D(n, q)$ zawiera elementy bardzo dużego rzędu, ale nasze teoretyczne liniowe ograniczenie rzędu jest stosunkowo słabe - mamy nadzieję uzupełnić tę lukę w przyszłości.

W rozdziale 4 użyjemy grafów dla konstrukcji rodziny podgrup stabilnych stopnia 3 w grupie Cremona $C(K^n)$ nad ogólnym pierścieniem K zawierającym elementy dużego rzędu (rząd wzrasta wraz ze wzrostem n). Pierwsza rodzina podgrup stabilnych została otrzymana dzięki rozważeniu prostego grafu algebraicznego nad ciałem skończonym $\mathbb{F}_q$. W ogólnej konstrukcji grup stabilnych na pierścieniem przemiennym K używamy grafów skierowanych ze specjalnym kolorowaniem. Głównym rezultatem publikacji [67] jest następujące twierdzenie:

Twierdzenie 1.2. *Dla każdego pierścienia przemiennego K posiadającego przynajmniej 3 elementy regularne, istnieją rodziny Q_n z grupy Cremony $C(K^n)$ stopnia 3, takie, że granica rzutowa Q z Q_n , $n \to \infty$ jest dobrze zdefiniowana, grupa Q mająca nieskończony rząd, zawiera elementy g nieskończonego rzędu, takie, że istnieje ciąg $g_n \in Q_n$ $n \to \infty$ elementów stabilnych spełniających warunek* $\lim g_n = g$.

1.7 Podstawowe pojęcia teorii grafów

Definicja 1.18. *Grafem nieskierowanym, skończonym* G nazywamy parę (V, E), gdzie $V = \mathrm{V}(G)$ jest zbiorem skończonym, niepustym, natomiast $E = \mathrm{E}(G)$ jest rodziną (mogących się powtarzać) dwuelementowych podzbiorów (niekoniecznie różnych) elementów ze zbioru V.

Niech $\mathrm{V}(G)$ i $\mathrm{E}(G)$ oznaczają zbiór wierzchołków i zbiór krawędzi grafu G, odpowiednio. Wtedy $|\mathrm{V}(G)|$ nazywamy *rzędem* grafu G, oraz $|\mathrm{E}(G)|$ nazywamy *rozmiarem* grafu G.

Jeżeli w grafie G istnieją co najmniej dwie krawędzie $\{u, v\}$, to krawędź tę nazywamy *krawędzią wielokrotną*. Krawędź $\{v, v\}$ w grafie G nazywamy *pętlą*. Graf, który nie ma krawędzi wielokrotnych i pętli nazywamy grafem prostym.

Definicja 1.19. Dwa wierzchołki u, v w grafie G są *sąsiednie*, jeżeli $\{u, v\} \in \mathrm{E}(G)$. Mówimy wtedy, że wierzchołki u, v sa *incydentne* z krawędzią $\{u, v\}$. Dwie różne krawędzie są *sąsiednie*, jeżeli mają przynajmniej jeden wspólny wierzchołek.

Definicja 1.20. *Stopień wierzchołka* v *grafu* G jest liczbą krawędzi incydentych z wierzchołkiem v i jest oznaczany symbolem $\deg_G v$

Definicja 1.21. *Podgraf* danego grafu G to graf powstały przez usunięcie z grafu G pewnej liczby wierzchołków lub krawędzi, z zastrzeżeniem, że usuwając pewien wierzchołek usuwamy wszystkie do niego incydentne krawędzie. *Podgrafem indukowanym wierzchołkowo* danego grafu G jest graf, którego zbiór wierzchołków jest podzbiorem zbioru wierzchołków grafu G, a zbiór krawędzi składa się ze wszystkich krawędzi grafu G, których końce należą do zbioru wierzchołków nowo powstałego grafu. *Podgrafem indukowanym krawędziowo* danego grafu G nazywamy graf powstały z grafu G, którego zbiór krawędzi jest podzbiorem zbioru krawędzi grafu G, a zbiór wierzchołków stanowią końce krawędzi.

Definicja 1.22. *Drogą* z wierzchołka v_1 do wierzchołka v_m w grafie G nazywamy skończony ciąg wierzchołków $v_1, v_2, \ldots, v_m$, $m \geq 2$ i krawędzi $\{v_i, v_{i+1}\}$, $i = 1, 2, \ldots, m-1$. Drogę, w której $v_m = v_1$ nazywamy cyklem. Jeżeli droga (cykl) nie zawiera dwóch tych samych wierzchołków (z wyjątkiem $v_1 = v_m$) to drogę (cykl) nazywamy drogą elementarną (cyklem elementarnym). Jeżeli droga (cykl) nie zawiera dwóch tych samych krawędzi, to drogę (cykl) nazywamy drogą prostą lub *ścieżką* (cyklem prostym). Graf spełniający warunek, że dla każdej pary wierzchołków istnieje ścieżka, która je łączy, nazywamy *grafem*

spójnym. Graf nie posiadający powyższej własności to graf niespójny. *Graf acykliczny* – graf nie zawierający cykli. Graf, który jest acykliczny i spójny nazywamy *drzewem*, zaś *las* to graf, którego każdy spójny podgraf jest drzewem.

Definicja 1.23. Graf G nazywamy grafem *dwudzielnym*, jeśli zbiór wierzchołków $V(G)$ można podzielić na dwa rozłączne zbiory V_1 i V_2 tak, by nie było krawędzi łączących wierzchołki tego samego zbioru.

W pewnych przypadkach, jeśli będzie to wygodne, będziemy identyfikować G z odpowiadającą antyzwrotną relacją na zbiorze wierzchołków $\mathrm{V}(G)$, tzn. $\mathrm{E}(G)$ jest podzbiorem $\mathrm{V}(G) \times \mathrm{V}(G)$ i piszemy wtedy vGu dla wierzchołków sąsiadujących (przyległych) u i v.

Definicja 1.24. *Ścieżką w grafie* nazywamy ciąg różnych wierzchołków $v_1, \ldots, v_t$, takich, że $v_i G v_{i+1}$ dla $i = 1, \ldots, t-1$.

Definicja 1.25. Długością ścieżki nazywamy liczbę jej krawędzi. Odległość $\mathrm{dist}(u, v)$ między dwoma wierzchołkami jest długością najkrótszej ścieżki pomiędzy nimi.

Definicja 1.26. *Średnica grafu* oznaczana przez $\mathrm{diam}G$ to maksymalna odległość między dowolnymi wierzchołkami u i v w grafie.

Niech C_m oznacza cykl długości m, tzn. ciąg różnych wierzchołków $v_1, \ldots, v_m$, takich że $v_i G v_{i+1}$, $i = 1, \ldots, m-1$ i $v_m G v_1$.

Definicja 1.27. *Talia grafu* G, oznaczona przez $g = \mathrm{g}(G)$, jest długością najkrótszego cyklu w grafie G. Stopniem wierzchołka v nazywamy liczbę jego sąsiadów.

Definicja 1.28. Graf nazywamy *krawędziowo tranzytywnym*, jeśli dla każdych dwóch krawędzi e_1 i e_2 należących do $E(G)$, istnieje automorfizm δ zbioru krawędzi $E(G)$, dla którego $\delta(e_1) = e_2$. Analogicznie, graf nazywamy *wierzchołkowo tranzytywnym*, jeśli dla każdych dwóch wierzchołków v_1 i v_2 należących do $V(G)$, istnieje automorfizm λ zbioru wierzchołków $V(G)$, dla którego $\lambda(v_1) = v_2$.

Rozdział 2

Elementy kryptografii

W poniższym rozdziale opisana jest podstawowa terminologia i wstępna wiedza dotycząca zagadnień kryptologii, podział algorytmów szyfrujących oraz pewne zagadnienia kryptoanalizy. W kolejnych podrozdziałach opisana zostanie kryptografia wielu zmiennych, do której można użyć odwzorowań wielomianowych omawianych w rozprawie. Z racji tego, że badane odwzorowania tworzą rodzinę lingwistycznych układów dynamicznych (zdefiniowanych w rozdziale 3.4) w tym rozdziale poruszone zostanie zagadnienie użycia teorii chaosu i układów dynamicznych w kryptografii wielu zmiennych. Podstawowa wiedza została zaczerpnięta m.in. z [14, 21, 22, 39].

2.1 Podstawowa terminologia i klasyfikacja algorytmów kryptograficznych

Kryptografia jest nauką obejmującą techniki matematycznych związane z aspektami bezpieczeństwa informacji, takimi jak:

- poufność (ang. *confidentiality*) – Zapewnienie dostępu do informacji wyłącznie osobom upoważnionym,
- integralność (spójność) danych (ang. *integrity*) – Zapewnienie, że dane nie zostaną podmienione ani zmodyfikowane przez osoby nieupoważnione,
- uwierzytelnianie (ang. *entity authentication*) – Potwierdzenie tożsamości podmiotu oraz źródła pochodzenia informacji,

- niezaprzeczalność (ang. *non-repudiation*) – Zapewnienia, że strony komunikacji nie mogą zaprzeczyć autentyczności podpisu lub wysłania wiadomości.

Praktyczna kryptografia jest badaniem metod szyfrowania informacji, tworzeniem podpisów cyfrowych, kontrolą kluczy i certyfikatów. Kryptoanaliza jest przeciwieństwem kryptografii. Zajmuje się ona badaniem metod ataków na systemy kryptograficzne (bez znajomości klucza) oraz ich analizą i monitorowaniem, celem znalezienia i wykorzystania ich słabych stron. Kryptologia jest dziedziną obejmującą kryptografię i kryptoanalizę.

W następnych dwóch podrozdziałach przedstawiona zostanie podstawowa klasyfikacja algorytmów - algorytmy symetryczne oraz asymetryczne.

2.1.1 Algorytmy z kluczem symetrycznym

Algorytm z kluczem symetrycznym (algorytm z kluczem prywatnym) jest algorytmem kryptograficznym korzystającym z tych samych kluczy kryptograficznych zarówno do szyfrowania i deszyfrowania tekstu jawnego w szyfrogram. Klucze służące do szyfrowania i deszyfrowania mogą być takie same lub mogą istnieć proste przekształcenie między nimi. Klucze w praktyce stanowią wspólne hasło dwóch lub więcej stron, które mogą być stosowane do utrzymywania prywatnego łącza informacyjnego. Ten wymóg, że obie strony mają dostęp do tajnego klucza, jest jednym z głównych wad symetrycznego szyfrowania klucza w stosunku do szyfrowania z kluczem publicznym.

Zadaniem szyfrowania z kluczem symetrycznym jest zapewnienie tajności komunikacji pomiędzy dwiema stronami (powiedzmy, między Alicją i Bobem). Przeciwnik, który przechwytuje wiadomość nie powinien uzyskać żadnych istotnych jej treści. Aby ustanowić bezpieczny kanał komunikacyjny, Alicja i Bob uzgadniają wspólny klucz k, który zachowują w tajemnicy. Przed wysłaniem wiadomości m do Boba, Alicja szyfruje m przy użyciu algorytmu szyfrującego E i klucza k, uzyskując szyfrogram $c = E(k, m)$, który wysyła do Boba. Przy użyciu algorytmu deszyfrowania D i tego samego klucza k, Bob deszyfruje c w celu uzyskania tekstu jawnego $m = D(k, c)$. Mówimy o szyfrowaniu symetrycznym, ponieważ obie strony używają tego samego klucza k do szyfrowania i deszyfrowania. Algorytm szyfrujący E i deszyfrujący D są powszechnie znane. Każdy może odszyfrować szyfrogram, jeśli zna odpowiedni klucz. Podstawowym problemem w kryptografii symetrycznej jest to, w jaki sposób Alicja i Bob mogą ustalić klucz k w sposób bezpieczny i efektywny. Do tej wymiany kluczy niezbędne są metody kryptografii z kluczem publicznym (algorytmy asymetryczne), które zostaną omówione w dalszej części rozprawy.

Wymagane jest, aby tekst jawny m mógł być w sposób jednoznaczny odzyskany z szyfrogramu c. Oznacza to, że dla ustalonego klucza k, odwzorowanie szyfrujące musi być funkcją wzajemnie jednoznaczną (bijektywną).

Niech K będzie zbiorem możliwych kluczy, M - zbiorem tekstów jawnych oraz C - zbiorem szyfrogramów. Z matematycznego punktu widzenia algorytm szyfrowania symetrycznego można zdefiniować w następujący sposób:

Definicja 2.1. Algorytm z kluczem symetrycznym składa się z odwzorowania:

$$E\colon K \times M \to C,$$

takiego że dla każdego $k \in K$ odwzorowanie

$$E_k\colon M \to C,\ m \longmapsto E(k, m)$$

jest odwracalne. Element $m \in M$ nazywamy tekstem jawnym (wiadomością), C jest zbiorem szyfrogramów, element $k \in K$ kluczem. E_k nazywamy funkcją szyfrującą względem klucza k. Funkcję odwrotną $D_k := E_k^{-1}$ nazywamy funckją deszyfrującą.

Podstawowym wymogiem bezpieczeństwa dla odwzorowania szyfrującego E jest to, aby bez znajomości klucza k nie było możliwe pomyślne odnalezienie funkcji deszyfrującej D_k. Ważnymi przykładami systemów szyfrujących z kluczem symetrycznym są: DES, AES czy Blowfish. Spośród wszystkich algorytmów szyfrujących, algorytmy symetryczne mają najszybsze implementacje pod względem sprzętowym i w oprogramowaniu. W związku z tym bardzo dobrze nadają się do szyfrowania dużych ilości danych. Jeśli Alicja i Bob chcą użyć systemu szyfrowania z kluczem symetrycznym, muszą wymienić się między sobą tajnym kluczem za pomocą bezpiecznego kanału komunikacyjnego. Najczęściej w tym celu stosowana jest kryptografia z kluczem publicznym (algorytmy asymetryczne). Systemy szyfrujące z kluczem publicznym są mniej efektywne, w związku z tym nie nadają się do dużych ilości danych. W ten sposób systemy symetryczne i asymetryczne uzupełniają się wzajemnie, współtworząc kryptosystemy.

Rozróżniamy szyfry blokowe i szyfry strumieniowe. Funkcja szyfrująca pierwszego typu przetwarza bloki tekstu jawnego na bloki szyfrogramu tej samej długości. Szyfry strumieniowe działając na strumieniach tekstu jawnego znak po znaku, szyfrują ciągi tekstów

o dowolnej długości. Jeśli długość tekstu jawnego przekracza długość bloku w szyfrowaniu blokowym, stosuje się różne tryby działania wykorzystujące szyfry strumieniowe. Tak więc, szyfry blokowe mogą być także traktowane jako budulec dla szyfrów strumieniowych.

2.1.2 Algorytmy z kluczem publicznym

Do końca lat siedemdziesiątych obowiązywała kryptografia symetryczna, jako jedyna koncepcja konstrukcji algorytmów szyfrujących. Przełomowym momentem było opracowanie teorii kryptografii asymetrycznej (kryptografii z kluczem publicznym). W kryptografii z kluczem publicznym klucz składa się z dwóch różnych części, klucza publicznego i klucza prywatnego. Klucz publiczny jest dostępny dla wszystkich i jest używany do szyfrowania wiadomości lub do weryfikacji autentyczności podpisu elektronicznego. Klucz prywatny jest używany do deszyfrowania zaszyfrowanej wiadomości lub do tworzenia podpisu elektronicznego. Ta asymetryczna konstrukcja pozwala na bezpieczną komunikację kanałem publicznym bez wcześniejszej wymiany klucza prywatnego. W kryptografii symetrycznej dwaj użytkownicy, oczekujący bezpiecznej komunikacji między sobą muszą posiadać ten sam klucz (który muszą uzgodnić między sobą wcześniej) lub mogą użyć publicznego protokołu wymiany klucza.

W systemie szyfrowania z kluczem publicznym, partnerzy komunikacji nie dzielą tajnego klucza. Każdy użytkownik ma parę kluczy: klucz tajny k_s, znany tylko przez niego i klucz publiczny k_p znany każdemu. Załóżmy, że Bob posiada taką parę kluczy $(k_p; k_s)$, zaś Alicja chce zaszyfrować wiadomość m dla Boba. Jak wszyscy inni, Alicja zna klucz publiczny Boba k_p. Alicja oblicza szyfrogram $c = E(k_p, m)$, stosując funkcję szyfrującą E oraz klucz publiczny Boba. Szyfrowanie z ustalonym kluczem k_p oznaczamy przez E_{k_p}, czyli $E_{k_p}(m) : E = (k_p; m)$. Oczywiście, system szyfrowania może być bezpieczny, jeśli to jest praktycznie niemożliwe, aby obliczyć m z $C = E_{k_p}(m)$.

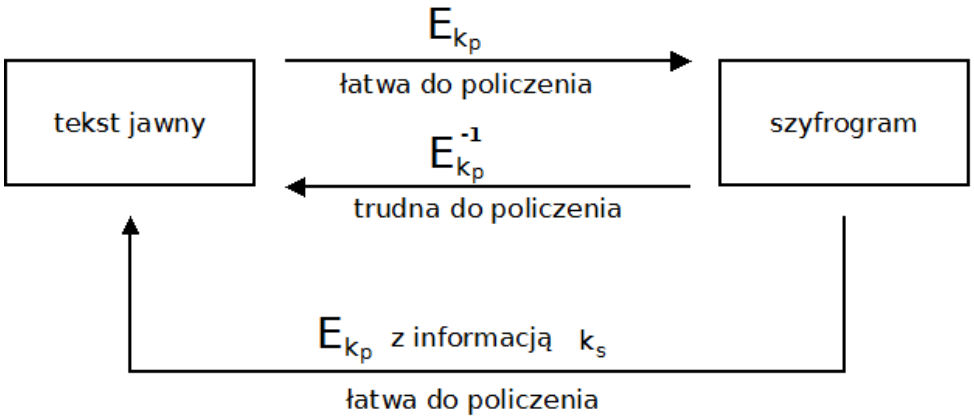
Następnie, w celu odzyskania wiadomości m z szyfrogramu c, Bob używa swojego tajnego klucza. Funkcja szyfrowania E_{k_p} musi mieć własność, że przeciwobraz m szyfrogramu $c = E_{k_p}(m)$ jest łatwy do obliczenia przy użyciu tajnego klucza Boba k_s. Ponieważ tylko Bob zna tajny klucz, on jest jedynym, który może odszyfrować wiadomość. Nawet Alicja, która zaszyfrowała wiadomość m, nie byłby w stanie uzyskać m od $E_{k_p}(m)$, jeśli wcześniej straciłaby m.

Podsumowując, szukamy rodziny funkcji $(E_{k_p})_{k_p \in K_p}$ spełniającej następujące warunki:

1. każda funkcja E_{k_p} jest obliczalna za pomocą efektywnego algorytmu (o złożoności wielomianowej)

2. przeciwobraz E_{k_p} powinien być praktycznie niemożliwy do obliczenia

Takie rodziny $(E_{k_p})_{k_p \in K_p}$ nazywane są rodzinami funkcji jednokierunkowych. K_p oznacza zbiór dostępnych kluczy. Dla każdej funkcji E_{k_p} z tej rodziny powinna istnieć informacja k_s, utrzymywana w tajemnicy, która umożliwia sprawne obliczenie odwrotności E_{k_p}. Funkcje spełniające powyższe własności nazywane są funkcjami jednokierunkowymi z zapadką. Opisany wyżej schemat działania tej funkcji zobrazowany jest na rysunku 2.1



Rysunek 2.1: Schemat działania funkcji jednokierunkowej z zapadką

Rewolucyjna idea kryptosystemu klucza publicznego została zainicjowana w 1976r. przez Diffiego i Hellmana [7] poprzez dostarczenie protokołu uzgodnienia klucza publicznego. Pierwszą praktyczną realizacją kryptografii asymetrycznej jest kryptosystem RSA, zaprojektowany przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana ([48]). Kryptosystem RSA zapewnia szyfrowanie oraz podpisy cyfrowe i jest najbardziej popularnym oraz szeroko stosowanym kluczem algorytmem z kluczem publicznym. Opiera się na trudności faktoryzacji dużych liczb, co umożliwia budowę jednokierunkowych funkcji z zapadką. Kolejną podstawą powstania funkcji jednokierunkowych używanych w RSA jest trudność rozwiązania logarytmu dyskretnego.

Algorytmy z kluczem publicznym są również wykorzystywane do różnych form uwierzytelniania i niezaprzeczalności, takich jak podpisy cyfrowe. Podpis cyfrowy powinien być odpowiednikiem cyfrowym podpisu odręcznego. Podpis powinien zależeć od podpisywanej wiadomości i wiadomy jedynie dla osoby podpisującej. Bezstronna osoba trzecia powinna być w stanie zweryfikować podpis bez dostępu do tajemnicy podpisującego. Załóżmy,

że mamy rodzinę $(E_{k_p})_{k_p \in K_p}$ funkcji jednokierunkowych z zapadką oraz każda funkcja E_{k_p} jest bijekcją. Niech k_p będzie kluczem publicznym Alicji. Alicja jest jedyną osobą posiadającą klucz prywatny k_s, dzięki któremu może obliczyć funkcję odwrotną $E_{k_p}^{-1}$ dla funkcji E_{k_p}. Następnie Alicja chcąc podpisać wiadomość m, wylicza wartość $s = E_{k_p}^{-1}(m)$, która staje się podpisem dla wiadomości m. W tej sytacji każdy może zweryfikować podpis Alicji, używając klucza publicznego p_k do obliczenia $E_{k_p}(s)$. Jeśli $E_{k_p}(s) = m$, użytkownik publiczny (Bob) jest przekonany, że Alicja rzeczywiście podpisała wiadomość m, ponieważ tylko ona była w stanie policzyć $E_{k_p}^{-1}(m)$. Podpisy cyfrowe stosowane są w celu zagwarantowania autentyczności kluczy publicznych przez władze certyfikujące. Urząd certyfikacji zatwierdza zgodność klucza publicznego każdego użytkownika z jego kluczem prywatnym.

Jednym z najważniejszych algorytmów kryptografii asymetrycznej (obok RSA), umożliwiający szyfrowanie i obsługę podpisów cyfrowych, jest algorytm ElGamal. System jest oparty na trudności problemu logarytmu dyskretnego w ciele liczb całkowitych modulo duża liczba pierwsza.

Ważnym bezpośrednim zastosowaniem kryptosystemów z kluczem publicznym jest dystrybucja kluczy sesji. Klucz sesji jest tajnym kluczem używanym w klasycznych symetrycznych schematach szyfrowania do szyfrowania wiadomości pojedynczej sesji komunikacyjnej. Jeśli Alicja zna klucz publiczny Boba, to może wygenerować klucz sesji, szyfruje wiadomość kluczem publicznym Boba i wysłać go do niego. Jednym z głównych przykładów może być protokół uzgodnienia klucza Diffiego-Helmanna, dokładniej opisana i użyta w dalszej części rozprawy.

2.1.3 Protokół uzgodnienia klucza Diffiego-Hellmana

Protokół uzgodnienia klucza Diffiego-Hellmana po raz pierwszy opublikowany przez W. Diffiego i M. Hellmana w roku 1976 w publikacji [7]. Protokół pozwala na uzgodnienie jednego klucza dla obu stron (Alicji i Boba) bez przesyłania żadnych poufnych informacji. Obie strony używają w tym celu niebezpiecznego kanału publicznego, w którym każda informacja może być obserwowana przez przeciwnika. W ten sposób utworzony klucz można później wykorzystać w symetrycznych algorytmach szyfrujących. Siła algorytmu oparta jest na trudnym problemie logarytmu dyskretnego opisanego w 1.5.

Protokół uzgodnienia klucza Diffiego-Hellmana można przedstawić w następujących krokach:

1. Alicja i Bob uzgadniają dużą liczbę pierwszą p oraz niezerową liczbą całkowitą g, $2 \leq g \leq p-2$, której rząd modulo p jest dostatecznie duży. Liczba g może być na przykład pierwiastkiem pierwotnym (generatorem) z p (potęgi g dają wszystkie możliwe reszty modulo p, które są względnie pierwsze z p.) Liczby p i g są znane publicznie (jawne).

2. Alicja wybiera losowo, tajną liczbę całkowitą a, taką, że $2 \leq a \leq p-2$, oblicza: $A = g^a \mod p$ i przesyła ją do Boba.

3. Bob wybiera losowo, tajną liczbę całkowitą b, taką, że $2 \leq b \leq p-2$, oblicza: $B = g^b \mod p$ i przesyła ją do Alicji.

4. Alicja oblicza $K = B^a \mod p = (g^b)^a \mod p = g^{ab} \mod p$.

5. Bob oblicza $K = A^b \mod p = (g^a)^b \mod p = g^{ab} \mod p$, uzyskując razem z Alicją wspólny tajny klucz K.

Problemem Diffiego-Hellmana nazywamy problem obliczenia klucza $K = g^{ab} \mod p$ mając dane: liczbę pierwszą p, podstawę g oraz g^a i g^b.

2.1.4 Schemat szyfrowania ElGamal

Schemat szyfrowania ElGamal należy do asymetrycznych algorytmów kryptograficznych, opartych na protokole uzgodnienia klucza Diffiego-Hellmana. Schemat został opisany przez T. Elgamal w 1985r. w pracy [8]. Szyfrowanie w schemacie ElGamal może być zdefiniowane nad dowolną grupą cykliczną, a jego bezpieczeństwo oparte jest na problemie logarytmu dyskretnego.

Przedstawmy schemat działania kryptosystemu ElGamal.

W pierwszym etapie Alicja generuje klucze (prywatny i publiczny) w następujących etapach:

1. wybiera dowolną liczbę pierwszą p,

2. wybiera grupę cykliczną G rzędu p wraz z jej generatorem g (pierwiastkiem pierwotnym modulo p),

3. wybiera dowolne a takie, że $1 < a < p$,

4. liczy $\alpha = g^a \mod p$.

Ostatecznie Alicja publikuje (p, g, α) jako klucz publiczny i zachowuje (p, g, a, α) jako klucz prywatny

Bob, będąc w posiadaniu powyższego klucza publicznego (p, g, α), dokonuje szyfrowania tekstu jawnego x należącego do zbioru $\{0, 1, 2, \cdots, p-1\}$ w następujący sposób:

1. wybiera losowo b ze zbioru $\{0, 1, \ldots, p-1\}$,
2. oblicza $y = \alpha^b x \mod p$,
3. oblicza $\beta = g^b \mod p$.

W rezultacie Bob otrzymuje szyfrogram postaci: $(y, \beta) = (\alpha^b x \mod p, g^b \mod p$.

Deszyfrowanie w systemie ElGamal – Alicja, mając swój klucz prywatny (p, g, a, α) oraz szyfrogram (y, β), oblicza $x = \beta^{-a} y \mod p$ otrzymując tekst jawny x.

2.2 Złożoność obliczeniowa, kryptoanaliza i ataki kryptograficzne

2.2.1 Złożoność obliczeniowa

Od lat 70-tych, kiedy urodziła się nowoczesna kryptografia, o bezpieczeństwie algorytmów zaczęto dyskutować w terminach złożoności obliczeniowej. Z perspektywy czasu to połączenie wydaje się naturalne, ponieważ podsłuchujący ma ograniczone zasoby obliczeniowe. Zatem, w celu zapewnienia bezpieczeństwa należy starać się zapewnić złamanie algorytmu problemem jak najbardziej trudnym obliczeniowo. Podstawowe definicje i terminologia została zaczerpnięta z [41].

Algorytm komputerowy, zajmując się określonym problemem obliczeniowym, ma do dyspozycji dwa zasoby: czas i pamięć. Dlatego w zależności od rozważanego zasobu rozróżniamy złożoność czasową i pamięciową.

Definicja 2.2. Złożoność czasowa - liczba operacji podstawowych niezbędna do rozwiązania problemu, przedstawiona jako funkcja zależna od rozmiaru danych wejściowych.

Definicja 2.3. Złożoność pamięciowa - liczba komórek pamięci, zajęta przez dane i wyniki w trakcie działania algorytmu.

Oceniając koszt działania algorytmów najczęściej korzystamy z tzw. notacji "dużego O" (pozostałe notacje można znaleźć w [41]).

Definicja 2.4. Niech $f, g : \mathbb{N} \to \mathbb{N}$. Mówimy, że funkcja $f(n)$ jest co najwyżej rzędu g (zapisujemy $f(n) = \mathcal{O}(g(n))$) jeśli istnieje nieujemna licza całkowita n_0 i $c > 0$, takie, że dla wszystkich $n \geq n_0$ mamy $f(n) \leq cg(n)$. Nieformalnie, $f(n) = \mathcal{O}(g(n))$ oznacza, że f rośnie najwyżej tak szybko jak g.

2.2.2 Kryptoanaliza i ataki kryptograficzne

Podstawowym celem kryptografii jest utrzymanie tekstu jawnego w tajemnicy przed podsłuchującym. Przeciwnicy są również aktywni i mogą próbować modyfikować wiadomość. Oczekuje się więć, że kryptografia zagwarantuje integralność wiadomości. Przeciwnicy z założenia posiadają pełny dostęp do kanału komunikacyjnego. Kryptoanaliza jest nauką dotyczącą ataków na schematy kryptograficzne. Udane ataki mogą, na przykład, odzyskać tekst jawny (lub jego część) z szyfrogramu, zastąpić część oryginalnej wiadomości lub podrobić podpisy cyfrowe. Podstawowe założenie kryptoanalizy po raz pierwszy sformułowane przez A. Kerkhoffa w XIX wieku, jest zwykle określane jako zasada Kerckhoffa. Zgodnie z tą zasadą, przeciwnik zna wszystkie szczegóły kryptosystemu, w tym algorytm i jego implementację. Stąd bezpieczeństwo kryptosystemu musi w całości opierać się na tajnym kluczu.

Ataki mają głównie na celu odzyskać tekst jawny z szyfrogramu, albo jeszcze bardziej radykalnie, odzyskać tajny klucz. Przeciwnik, zwykle zwany Ewą, nie próbuje modyfikować wiadomości. Monitoruje kanał komunikacyjny i punkty końcowe kanału. Może ona więc nie tylko przechwytywać szyfrogram, ale (co najmniej od czasu do czasu) może być w stanie obserwować szyfrowanie i deszyfrowanie wiadomości. Nie ma ona żadnej informacji o kluczu. Możliwe ataki zależą głównie od aktualnych możliwości przeciwnika. Zazwyczaj klasyfikowane są w następujący sposób:

1. Atak ze znanym szyfrogramem. Przeciwnik ma możliwość uzyskania zaszyfrowanego tekstu i odzyskanie tekstu jawnego dla danych szyfrogramów. Metoda stosowana zazwyczaj do łamania szyfrów asymetrycznych.

2. Atak ze znanym tekstem jawnym. Przeciwnik ma możliwość otrzymania pary tekst jawny - szyfrogram. Wykorzystując informacje dotyczące tych par, ma ona możliwość uzyskania klucza szyfrującego.

3. Atak z wybranym tekstem jawnym. Przeciwnik ma możliwość uzyskania zaszyfrowanego tekstu dla wybranego tekstu jawnego. Na tej podstawie próbuje odszyfrować zaszyfrowany tekst, dla którego nie posiada tekstu jawnego.

4. Adaptacyjny (dopasowany) atak z wybranym tekstem jawnym. Jest to odmiana ataku z wybranym tekstem jawnym, lecz teraz atakujące może dokonać analizy pary tekst jawny-szyfrogram i na tej podstawie dobrać kolejne dane do zaszyfrowania i uzyskać więcej par.

2.3 Kryptografia wielu zmiennych

Algorytmy kryptografii asymetrycznej wykorzystują głównie operacje jednokierunkowe, czyli takie, które można z łatwością przeprowadzić w jedną stronę zaś bardzo trudno w drugą, np. RSA: mnożenie i faktoryzacja, w ElGamal, DSA i ECC: potęgowanie modulo i logarytmowanie dyskretne.

Peter Shor w pracy [51] pokazał, że problemy faktoryzacji i logarytmu dyskretnego, będące generalnie problemami trudnymi w klasycznych komputerach, mogą być rozwiązane w czasie wielomianowym (względem wielkości danych wejściowych) na hipotetycznym komputerze kwantowym. Pomimo tego, że nie istnieje jeszcze odpowiedni kwantowy komputer do wykonania tego zadania, jest ogromna motywacja do poszukiwania algorytmów kryptograficznych bardziej wydajnych i bezpiecznych.

Poszukiwania kryptosystemów klucza publicznego rozchodzą w wielu różnych kierunkach, np. oparte na krzywych eliptycznych lub kratach. Kryptografia wielu zmiennych, oparta na geometrii algebraicznej, jest również jednym z takich kierunków.

Kryptografia wielu zmiennych jest terminem ogólnym dla asymetrycznych operacji kryptograficznych bazujących na wielomianach wielu zmiennych nad ciałami skończonymi. W pewnych przypadkach wielomiany te mogą być zdefiniowane również nad rozszerzeniem ciała. Jeśli wielomiany te mają stopień dwa, mówimy o problemie $\mathcal{MQ}$ (ang. *multivariate quadratics*). Metody te oparte są na twierdzeniu mówiącym, że rozwiązanie układu równań wielomianowych wielu zmiennych nad ciałem skończonym jest w ogólności problemem NP-trudnym. Dzięki temu algorytmy te mogą być dobrymi kandydatami kryptografii post-kwantowej.

Chcąc opisać w ogólności użycie kryptografii wielu zmiennych w szyfrowaniu i podpisie elektronicznym, wprowadzimy pewne oznaczenia. Przez $\mathrm{x} = (x_1, x_2, \ldots, x_n)$ i $\mathrm{y} = (y_1, y_2, \cdots, y_m)$ oznaczmy standardowe wektory w układzie współrzędnych w K^n i K^m, odpowiednio, gdzie K będzie tutaj odpowiednim ciałem skończonym. W szyfrowaniu przez $\mathrm{x}' = (x'_1, x'_2, \ldots, x'_n)$ oznaczamy element w K^n, który będziemy traktowali jako tekst jawny, zaś $\mathrm{y}' = (y'_1, y'_2, \ldots, y'_m)$ w $K^n = m$ jako szyfrogram. W przypadku podpisu

elektronicznego y′ będzie wiadomością do podpisania, zaś x′ elektronicznym podpisem wiadomości y′.

W publicznym kryptosystemie wielu zmiennych używamy odwzorowania F z K^n do K^m następującej postaci:

$$F(x_1, x_2, \ldots, x_n) = (F_1(x_1, x_2, \ldots, x_n), \ldots, F_m(x_1, x_2, \ldots, x_n)) = (y_1, y_2, \ldots, y_m) = \mathrm{y},$$

gdzie $F_i(x_1, x_2, \ldots, x_n)$ są wielomianami zmiennych $x_1, x_2, \ldots, x_n$.

Konstrukcja tego klucza wymaga uprzedniego zbudowania odwzorowania f z K^n do K^m postaci

$$f(x_1, x_2, \ldots, x_n) = (f_1(x_1, x_2, \ldots, x_n), \ldots, f_m(x_1, x_2, \ldots, x_n)),$$

gdzie $f_i(x_1, x_2, \ldots, x_n)$ są wielomianami zmiennych $x_1, x_2, \ldots, x_n$ zaś równanie

$$(f_1(x_1, x_2, \ldots, x_n), \ldots, f_m(x_1, x_2, \ldots, x_n)) = (a_1, a_2, \ldots, a_m)$$

może być z łatwością rozwiązane (zauważmy, że tutaj f^{-1} oznacza znalezienie przeciwobrazu, co nie musi oznaczać funkcji odwrotnej, która pokrywa się z pojęciem przeciwobrazu wtedy i tylko wtedy, gdy funkcja jest bijekcją). Wtedy F jest skonstruowane w następujący sposób:

$$F = T_1 \circ f \circ T_2, \tag{2.1}$$

gdzie T_1 jest losowo wybranym afinicznym odwzorowaniem liniowym z K^m do K^m, $T_1(x_1, x_2, \ldots, x_m) = \mathrm{x} \times A_1 + C_1$, A_1 jest odwracalną macierzą wymiaru $m \times m$ oraz $C_1 \in K^m$; oraz T_2 jest (afinicznym) odwzorowaniem liniowym z K^n do K^n, $T_2(x_1, x_2, \ldots, x_n) = \mathrm{x} \times A_2 + C_2$, A_2 jest odwracalną macierzą wymiaru $n \times n$ oraz $C_2 \in K^n$. W takiej sytuacji, klucz publiczny składa się z m wielomianowych składowych odwzorowania F oraz struktury ciała K. Klucz prywatny składa się głównie z odwzorowań afinicznych T_1 i T_2, mających na celu ukrycie odwzorowania f, które w przeciwnym razie mogłoby być łatwo rozwiązane.

W celu zaszyfrowania wiadomości X', użytkownik oblicza wartość $F(X')$, zaś chcąc odszyfrować wiadomość Y' należy rozwiązać równanie

$$F(x_1, x_2, \ldots, x_n) = \mathrm{y}' \tag{2.2}$$

W przypadku podpisu elektronicznego, aby podpisać wiadomość y′ należy rozwiązać równanie 2.2, którego rozwiązanie oznaczmy przez x′. Aby sprawdzić poprawność podpisu, należy sprawdzić, czy rzeczywiście jest spełnione poniższe równanie:

$$F(x'_1, x'_2, \ldots, x'_n) = \mathrm{y}'$$

2.4 Kryptografia wielu zmiennych oparta na teorii chaosu i układach dynamicznych

Jednym z nowych kierunków w kryptografii wielu zmiennych jest użycie narzędzi spoza algebry przemiennej takich jak układy dynamiczne lub teorię algebraicznych automatów dla stworzenia nieliniowych odwzorowań o naturze pseudolosowej.

Celem rozprawy jest rozwój nowych kryptosystemów w dziedzinie kryptografii wielu zmiennych, które mają pewien potencjał do użycia w kryptografii postkwantowej. Komputer kwantowy jest specjalną, losową maszyną obliczeniową. Algorytmy kryptograficzne muszą tworzyć szyfrogram przypominający chaos. Wynika stąd, że teoria ciągłych układów dynamicznych i ich dyskretnych aproksymacji może być użyta w kryptografii wielu zmiennych.

Najwcześniejsze zastosowanie chaosu w kryptografii było zaproponowane przez Pecora i Caroll w 1990r. w pracy [43] i rozwijane przez Kocareva w [23] oraz Parlitza w [42], używając sygnałów analogowych i binarnego modelu informacyjnego, odpowiednio. Rozważane są dyskretne i ciągłe chaotyczne układy dynamiczne.

Zastosowanie dyskretnych układów dynamicznych było po raz pierwszy zaproponowane przez Habutsu w [12], następnie rozwijane przez Kotulskiego i Szczepańskiego w [24]. Idea zaproponowana przez Habutsu zakłada pewien wewnętrzny parametr odwzorowania, grający rolę klucza prywatnego. Następnie wiadomość (warunek początkowy) jest przekształcana przez wiele iteracji odwzorowania odwrotnego. Kotulski i Szczepański w [24] podali uogólnienie powyższej idei, gdzie klucz prywatny jest powiązany z warunkiem początkowym zamiast parametrem układu. Zaletą użycia dyskretnych układów dynamicznych w szyfrach blokowych jest precyzyjny matematyczny opis własności (chaos, ergodyczność, mieszanie) oraz możliwość konstrukcji nowych szyfrów o z góry zadanej lub możliwej do ocenienia sile szyfrowania. Takie układy mogą być również użyte w generatorach liczb pseudolosowych.

W przypadku ciągłym wiadomość jest szyfrowana dzięki użyciu ciągłego, chaotycznego układu dynamicznego. Układ ten opisany jest przez nieliniowy układ równań różniczkowych zwyczajnych i jego charakterystykę, np. chaos, ergodyczność. Własność chaosu zapewnia wrażliwość na małe zmiany warunków początkowych. W tym przypadku takie parametry jak czas i przestrzeń stanów (bloki bitów) są parametrami ciągłymi. Znane są dwie metody bezpiecznej komunikacji z użyciem ciągłych układów dynamicznych - są nimi sterowanie i synchronizacja chaosu.

Badania pod kątem zastosowania układów dynamicznych w kryptografii prowadzoną są np. w USA, Rosji, Szwajcarii, Polsce, Ukrainie ([13, 25, 15, 45, 46, 53]).

Rozdział 3

Rodzina grafów $D(n, K)$, grafów lingwistycznych oraz odpowiadające im lingwistyczne układy dynamiczne

W tym rozdziale przedstawiona zostanie rodzina grafów $D(n, K)$ i grafów lingwistycznych, użytych do konstrukcji lingwistycznych układów dynamicznych oraz ich uogólnień. Definicje rodziny grafów $D(n, K)$ w przypadku ciał skończonych zostały zaczerpnięte z [27, 28, 29, 30]. Różne typy przedstawionych układów dynamicznych oraz ich uogólnień posłużą w kolejnych rozdziałach (4 oraz 5) do konstrukcji i badania specjalnych nieliniowych odwzorowań wielomianowych.

3.1 Graf prosty $D(n, K)$

3.1.1 Algebraiczna definicja grafu $D(n, K)$

Podane w tym rozdziale definicje grafów $D(K)$ oraz $D(n, K)$ dla pierścieni przemiennych K są naturalnymi uogólnieniami grafów $D(q)$ oraz $D(n, q)$, dla ciał skończonych F_q.

Definicja 3.1. Strukturą incydencji nazywamy zbiór V ze zbiorami podziału P i L wraz z symetryczną relacją binarną I, taką że incydencja dwóch elementów implikuje, że jeden z nich jest *punktem* zaś drugi *prostą*. I identyfikujemy jak graf prosty dla tej relacji incydencji.

Jeśli liczba sąsiadów każdego elementu jest skończona i zależy tylko i wyłącznie od jego typu (*punkt* lub *prosta*), wtedy struktura incydencji jest *taktyczną konfiguracją* w sensie Moore'a ([40]).

Graf jest *q-regularny*, jeśli każdy jego wierzchołek ma stopień q, gdzie q jest stałą. W publikacjach [27, 29] q-regularne drzewa zostały opisane w terminach równań nad ciałem skończonym F_q.

Niech P i L będą dwoma policzalnymi nieskończenie wymiarowymi przestrzeniami wektorowymi nad K. Elementy P nazywać będziemy *punktami* zaś L *prostymi*. W celu odróżnienia punktów od prostych, użyjemy różnych rodzajów nawiasów. Jeśli $x \in V$, wtedy $(x) \in P$ oraz $[x] \in L$. Korzystne będzie zaadoptowanie notacji dla współrzędnych punktów i prostych wprowadzonych w [37]:

$$(p) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots),$$

$$[l] = [l_1, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, l_{23}, \ldots, l_{ii}, l'_{ii}, l_{i,i+1}, l_{i+1,i}, \ldots].$$

Definicja 3.2. Zdefiniujmy teraz strukturę incydencji (P, L, I) następująco. Mówimy, że punkt (p) jest incydentny z prostą $[l]$ ($(p)I[l]$), jeżeli pomiędzy odpowiednimi współrzędnymi zachodzą następujące relacje:

$$\begin{aligned}
l_{1,1} - p_{1,1} &= l_{1,0}p_{0,1} \\
l_{1,2} - p_{1,2} &= l_{1,1}p_{0,1} \\
l_{2,1} - p_{2,1} &= l_{1,0}p_{1,1} \\
l_{i,i} - p_{i,i} &= l_{1,0}p_{i-1,i} \\
l'_{i,i} - p'_{i,i} &= l_{i,i-1}p_{0,1} \\
l_{i,i+1} - p_{i,i+1} &= l_{i,i}p_{0,1} \\
l_{i+1,i} - p_{i+1,i} &= l_{1,0}p'_{i,i}
\end{aligned} \tag{3.1}$$

Ostatnie cztery relacje zdefiniowane są dla $i \geq 2$. Tę strukturę incydencji (P, L, I) oznaczamy przez $D(K)$. Mówimy wtedy o *grafie incydencji* dla (P, L, I), którego zbiorem wierzchołków jest zbiór $P \cup L$, a zbior krawędzi składa się ze wszystkich par $\{(p), [l]\}$, dla których $(p)I[l]$.

W celu uproszczenia notacji, przyjmiemy następujące oznaczenia $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = 1$, $p_{0,1} = p_1$, $l_{1,0} = l_1$, $l'_{1,1} = l_{1,1}$, $p'_{1,1} = p_{1,1}$ i zapiszemy układ równań (3.1) w formie :

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0}p_{i-1,i} \\ l'_{i,i} - p'_{i,i} &= l_{i,i-1}p_1 \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i}p_1 \\ l_{i+1,i} - p_{i+1,i} &= l_1 p'_{i,i} \end{aligned} \tag{3.2}$$

dla $i = 0, 1, 2, \ldots$

Zauważmy, że dla $i = 0$, cztery ostatnie warunki z (3.1) są spełnione przez wszystkie punkty i proste oraz dla $i = 1$, pierwsze dwa równania pokrywają się i dają w rezultacie $l_{1,1} - p_{1,1} = l_1 p_1$.

Dla każdej liczby naturalnej $n \geq 2$ otrzymujemy strukturę incydencji (P_n, L_n, I_n) w następujący sposób. Początkowo, P_n i L_n otrzymujemy z P i L, odpowiednio, poprzez rzutowanie (obcięcie) każdego wektora na jego n początkowych współrzędnych. W przypadku notacji zaproponowanej przez [37], dla podkreślenia liczby n współrzędnych wierzchołka u (punktu bądź prostej) będziemy używać oznaczenia $\big|_n$ na końcu wektora:

$u = (u_1, u_{11}, u_{12}, u_{21}, u_{22}, u'_{22}, u_{23}, \ldots, u_{ii}, u'_{ii}, u_{i,i+1}, u_{i+1,i}, \ldots)\big|_n$.

Relacja incydencji I_n jest wtedy zdefiniowana przez uwzględnienie pierwszych $n-1$ relacji incydencji i zignorowanie pozostałych. Dla ustalonego pierścienia K, graf incydencji odpowiadający strukturze (P_n, L_n, I_n) jest oznaczony przez $D(n, K)$.

Graf $D(n, K)$ w przypadku ciał skończonych $K = F_q$, (q - potęga liczby pierwszej) oznaczamy przez $D(n, q)$.

Pewne własności rozważanego grafu $D(n, q)$ opisane są w poniższym twierdzeniu.

Twierdzenie 3.1. *([29]) Niech q będzie potęgą liczby pierwszej, oraz $n \geq 2$. Wtedy*

(i) $D(n, q)$ jest q-regularnym, krawędziowo-tranzytywnym grafem dwudzielnym rzędu $2q^n$;

(ii) dla nieparzystego n, $\mathrm{g}(D(n, q)) \geq n + 5$, dla parzystego n, $\mathrm{g}(D(n, q)) \geq n + 4$.

Rodzina grafów $D(n, q)$ została wprowadzona w pracach [28, 30] przez Ustimenko, Lazebnika i Woldara. Jest to jedna z rodzin grafów o dużej talii.

Definicja 3.3. Niech $\{G_{i,i\in\mathbb{N}}\}$ będzie rodziną grafów q-regularnych o rosnącym rzędzie o_i. Mówimy, że $\{G_i\}$ jest rodziną grafów o dużej talii jeżeli

$$g(G_i) \geq c \log_{n-1}(o_i),$$

dla pewnej niezależnej od i stałej c.

Równania (3.1) i (3.2) opisujące graf $D(n, K)$ zawierają podwójne indeksowanie, którego będziemy używać przy teoretycznych rozważaniach. Natomiast w obliczeniach i opisach algorytmów wygodniej będzie używać pojedynczego indeksowania, przedstawiając punkty i proste jako: $[l] = [l_1, l_2, \ldots, l_n]$ oraz $(p) = (p_1, p_2, \ldots, p_n)$, zaś równania (3.2) możemy przekształcić do następującej postaci:

$$\begin{aligned} l_2 - p_2 &= l_2 p_2 \\ l_2 - p_2 &= l_2 p_2 \\ \text{oraz dla } i > 3&\text{:} \\ l_i - p_i &= l_1 p_{i-2}, \quad \text{dla } i \equiv 0 \vee i \equiv 1 \pmod 4 \\ l_i - p_i &= l_{i-2} p_1, \quad \text{dla } i \equiv 2 \vee i \equiv 3 \pmod 4. \end{aligned} \tag{3.3}$$

Rysunek 3.1 przedstawia przykładowe wykresy grafów dla ciał $D(2, F_2)$ oraz $D(2, F_4)$, zaś rysunek 3.2 – wykresy grafów dla pierścieni $D(2, \mathbb{Z}_4)$ oraz $D(2, \mathbb{Z}_6)$.

3.1.2 $CD(n, K)$ – spójne składowe grafu $D(n, K)$

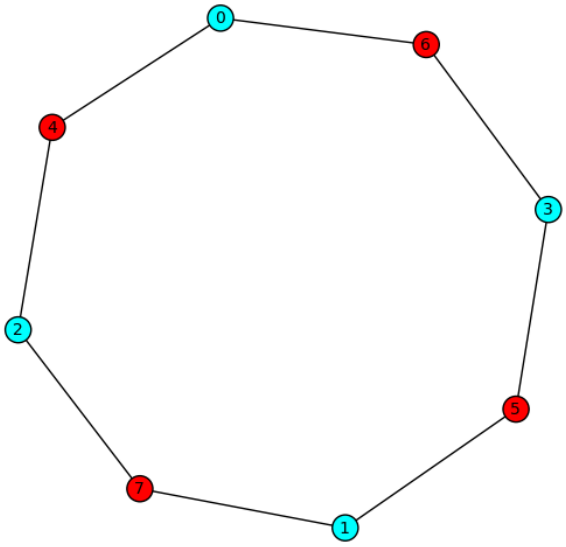
Rozważmy teraz opis spójnych składowych grafu $D(n, K)$.

Niech $n \geq 6$, $1 \leq t \leq \lfloor \frac{n+2}{4} \rfloor$, oraz niech $u = (u_1, u_{11}, \ldots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \ldots)\big|_n$ będzie wierzchołkiem grafu $D(n, K)$. (W tym momencie nie jest istotne, czy u jest punktem, czy prostą). Dla każdego r, $2 \leq r \leq t$, definiujemy formę kwadratową a_r postaci:

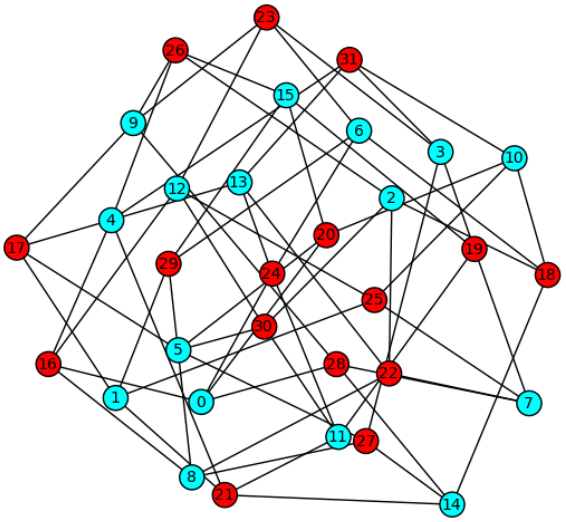
$$a_r = a_r(u) = \sum_{i=0}^{m} (u_{ii} u'_{r-i,r-i} - u_{i,i+1} u_{r-i,r-i-1}), \tag{3.4}$$

oraz $a = a(u) = (a_2, a_3, \ldots, a_t)$.

Definiujemy tutaj

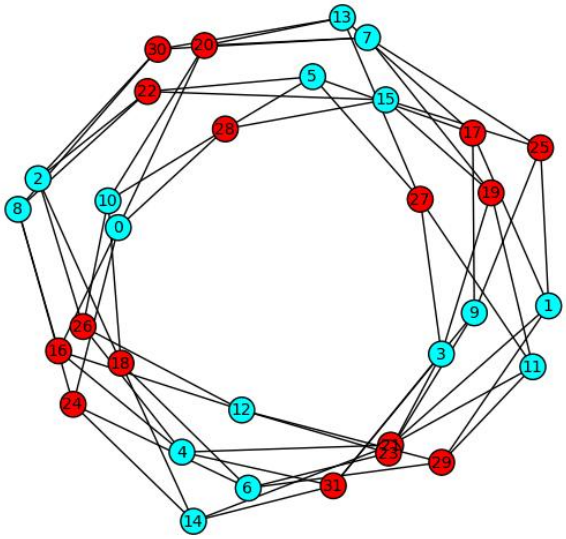


(a) Graf $D(2, \mathbb{F}_2)$

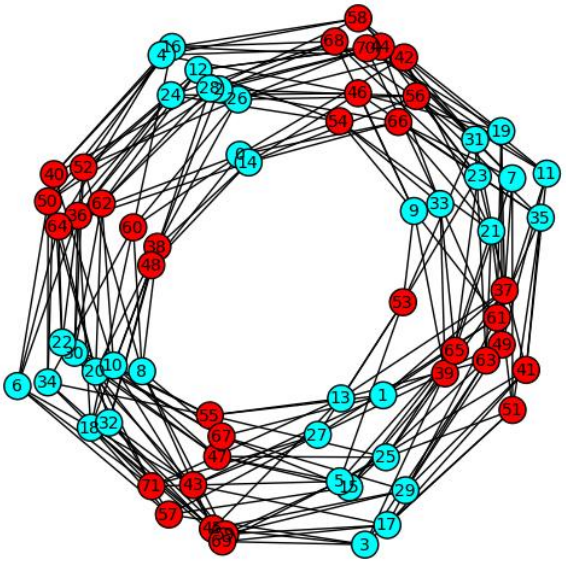


(b) Graf $D(2, \mathbb{F}_4)$

Rysunek 3.1: Wykresy grafów $D(n, K)$ dla $n = 2$ oraz ciał $\mathbb{F}_2$ oraz $\mathbb{F}_4$



(a) Graf $D(2, \mathbb{Z}_4)$



(b) Graf $D(2, D(2, \mathbb{Z}_6)$

Rysunek 3.2: Wykresy grafów $D(n, K)$ dla $n = 2$ oraz pierścieni $\mathbb{Z}_4$ oraz $\mathbb{Z}_6$

$p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{00} = l_{00} = -1$, $p_{0,1} = p_1$, $l_{1,0} = l_1$, $p'_{00} = l'_{00} = 1$ $l'_{11} = l_{11}$, $p'_{1,1} = p_{1,1}$.

W publikacji [27] dla przypadku ciała skończonego $K = \mathbb{F}_q$, (q - potęga liczby pierwszej) zostało udowodnione następujące twierdzenie.

Twierdzenie 3.2. *Jeżeli u i v są wierzchołkami w tej samej spójnej składowej grafu $D(n,q)$, wtedy $a(u) = a(v)$. Mówimy wtedy, że wierzchołki u i v należą do jednej spójnej składowej $CD(n,q)$. Co więcej, dla wszystkich $t-1$ elementów ciała $x_i \in \mathbb{F}_q$, $2 \leq t \leq \lfloor \frac{n+2}{4} \rfloor$, istnieje wierzchołek v grafu $D(n,q)$, dla którego*

$a(v) = (x_2, \ldots, x_t) = (x)$.

Rozważmy następującą relację równoważności τ : $u\tau v$ wtedy i tylko wtedy, gdy $a(u) = a(v)$ na zbiorze $P \cup L$ wierzchołków z $D(n,q)$ ($D(q)$). Klasa równoważności τ zawierająca wierzchołek v spełniająca zależność $a(v) = a(x)$ może być rozważana jako zbiór wierzchołków podgrafu indukowanego $EQ_x(n,q)$ ($EQ_{(x)}(q)$) grafu $D(n,q)$ ($D(q)$ odpowiednio). Dla $x = (0, \ldots, 0)$, pomijamy indeks dolny x i piszemy $EQ(n,q)$.

Niech $CD(q)$ będzie spójną składową grafu $D(q)$ zawierającą $(0,0,\ldots)$. Niech τ' relacją równoważności na zbiorze wierzchołków $V(D(n,q))$ ($V(D(q))$), w ten sposób, że klasą równoważności jest suma spójnych składowych tego grafu.

Oczywiście $u\tau v$ implikuje $u\tau' v$. Jeśli charakterystyka ciała $\mathbb{F}_q$ jest liczbą nieparzystą, odwrotność ostatniego twierdzenia również jest prawdziwa, czyli:

Twierdzenie 3.3. *[73] Niech q będzie liczbą nieparzystą. Wierzchołki u i v grafu $D(q)$ ($D(n,q)$) należą do tej samej spójnej składowej wtedy i tylko wtedy, gdy $a(u) = a(v)$, tzn., $\tau = \tau'$ oraz $EQ(q) = CD(q)$ ($EQ(n,q) = CD(n,q)$).*

Warunek $\mathrm{char}(\mathbb{F}_q) \neq 2$ jest kluczowy. Na przykład, graf $EQ(n, \mathbb{F}_4))$, $n > 3$, zawiera dwie izomorficzne spójne składowe. Wyraźnie $EQ(n,2)$ jest sumą cykli $CD(n, \mathbb{F}_2)$. Dlatego ani $EQ(n, \mathbb{F}_2)$, ani $CD(n, \mathbb{F}_2)$ nie jest interesującą rodziną grafów dużej talii w algorytmach kryptograficznych. Mimo to, rodzina grafów $EQ(n,q)$, gdzie q jest potęgą 2, $q > 2$ jest bardzo istotna w teorii kodowania.

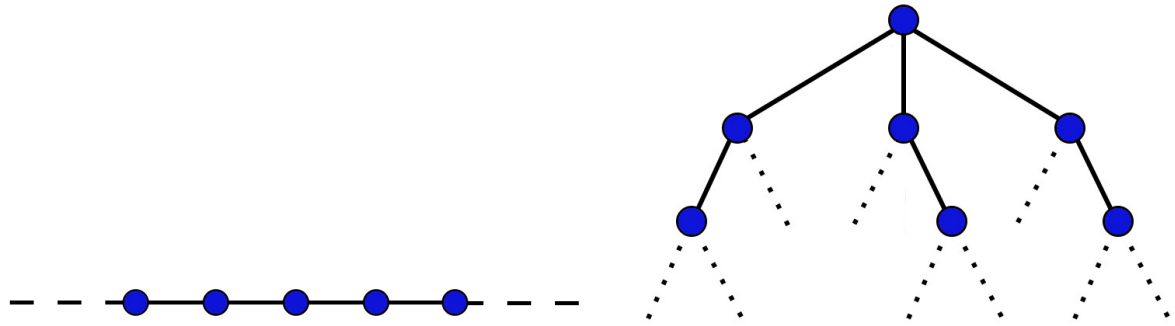
Lemat 3.4. *Rozważmy ogólny wierzchołek*

$$x = (x_1, x_{1,1}, x_{2,1}, x_{1,2} \ldots, x_{i,i}, x'_{i,i}, x_{i+1,i}, x_{i,i+1}, \ldots)\big|_n,$$

$i = 2, 3, \ldots$ należący do spójnej składowej $CD(n,q)$, zawierającej wybrany wierzchołek v. Wtedy współrzędne $x_{i,i}$, $x_{i,i+1}$, $x_{i+1,i}$ mogą być wybrane niezależnie jako "wolne parametry"

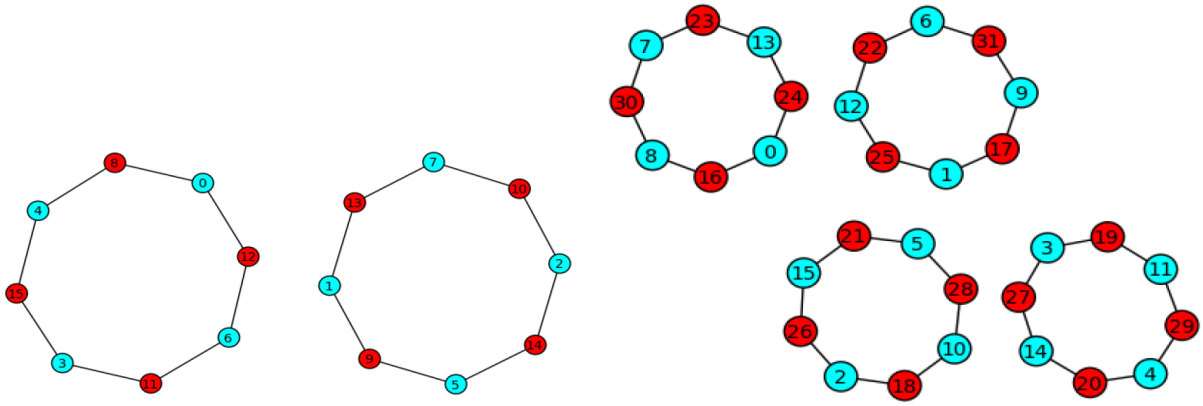
z $\mathbb{F}_q$, *zaś* $x'_{i,i}$ *mogą być obliczane sukcesywnie jako jednoznaczne rozwiązania równań* $a_i(x) = a_i(v)$, $i = 1, \ldots$.

Rysunek 3.3 przedstawia wykresy spójnych składowych nieskończonych grafów $CD(\mathbb{F}_2)$ oraz $CD(\mathbb{F}_3)$, zaś rysunek 3.4 – wykresy niespójnych grafów skończonych $D(3, \mathbb{F}_2)$ oraz $D(4, \mathbb{F}_2)$.



(a) Graf $CD(\mathbb{F}_2)$ (b) Graf $CD(\mathbb{F}_3)$

Rysunek 3.3: Wykresy grafów $CD(K)$ dla ciał $\mathbb{F}_2$ oraz $\mathbb{F}_3$



(a) Graf $D(3, \mathbb{F}_2)$ (b) Graf $D(4, \mathbb{F}_2)$

Rysunek 3.4: Wykresy grafów $D(n, K)$ dla $n = 3$ oraz $n = 4$ ciała $\mathbb{F}_2$

3.1.3 Kolorowanie wierzchołków grafu $D(n, K)$

Załóżmy, że mamy dwa wierzchołki (punkt $(p) \in P$ i prosta $[l] \in L$, odpowiednio) należące do zbioru wierzchołków grafu $V(\Gamma) = V(D(n, K))$, zadane jako n-elementowe wektory nad pierścieniem K (przez $v|_n$ oznaczamy wektor v obcięty do n współrzędnych):

$$(p) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots)\big|_n,$$

$$[l] = [l_1, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, l_{23}, \ldots, l_{ii}, l'_{ii}, l_{i,i+1}, l_{i+1,i}, \ldots]\big|_n.$$

Funkcję $\rho : \mathrm{V}(\Gamma) \to K$ określającą kolorowanie wierzchołków grafu $D(n, K)$ definiujemy następująco:

$$\rho((p)) = p_1,$$

$$\rho([l]) = l_1,$$

odpowiednio dla $(p) \in P$ oraz $[l] \in L$. Zatem kolor wierzchołka jest jednoznacznie określony przez jego pierwszą współrzędną.

Z definicji grafu $D(n, K)$ wynikają następujące fakty:

- wierzchołki sąsiadujące z wybranym wierzchołkiem mają różne kolory,
- w sąsiedztwie każdego wierzchołka istnieje reprezentant każdego koloru.

3.1.4 Polaryzacją grafu $D(n, K)$

Definicja 3.4. Strukturę incydencji (P, L, I) definiujemy jako graf dwudzielny ze zbiorem wierzchołków $P \cup L$ i zbiorem krawędzi $\{\{p, l\}|p \in P, l \in L, (p, l) \in L\}$. Niech $\pi : P \cup L \to P \cup L$ będzie bijekcją spełniającą poniższe warunki:

- $P^\pi = L$ and $L^\pi = P$,
- dla wszystkich $p \in P$ i $l \in L$ $(l^\pi,\ p^\pi) \in I$ wtedy i tylko wtedy, gdy $(p, l) \in I$,
- $\pi^2 = 1$

Odwzorowanie π nazywamy *polaryzacją struktury incydencji* (P, L, I). *Graf polaryzacji* Γ^π dla struktury (P, L, I) względem polaryzacji π nazywamy graf ze zbiorem wierzchołków $V(\Gamma^\pi) = P$ oraz zbiorem krawędzi $E(\Gamma^\pi) = \{\{p_1, p_2\}\}|p_1, p_2 \in P, p_1 \neq p_2, (p_1, {p_2}^\pi) \in I\}$. Punkt $p \in P$ nazywamy *punktem absolutnym* polaryzacji π jeżeli $(p, p^\pi) \in I$.

Twierdzenie 3.5. *([31])*

Niech N_π oznacza liczbę punktów absolutnych dla odwzorowania π oraz niech Γ i Γ^π będą odpowiednio grafem incydencji i grafem polaryzacji. Prawdziwe są następujące stwierdzenia:

- $\deg_{\Gamma^\pi} = \deg_{\Gamma^\pi} - 1$ *jeśli* p *jest punktem absolutnym dla* π*, oraz* $\deg_{\Gamma_\pi} = \deg_\Gamma$ *w przeciwnym przypadku.*

- $|V(\Gamma)^\pi| = 1/2|V(\Gamma)|$, $|E(\Gamma^\pi)| = |E(\Gamma)| - N_\pi$.

- *Jeżeli* Γ^π *zawiera* $(2k+1)$*-cykl wtedy* Γ *zawiera* $(4k+2)$*-cykl.*

- *Jeżeli* Γ^π *zawiera* $2k$*-cykl wtedy* Γ *zawiera dwa wierzchołkowo rozłączne* $2k$*-cykle* C *oraz* C' *takie, że* $C^\pi = C'$*. W rezultacie, jeżeli* Γ *nie zawiera* $2k$*-cykli to jest równy*Γ^π.

- *Talia obu grafów jest związana nierównością* $g(\Gamma^\pi) \geq 1/2g(\Gamma)$.

Następujące twierdzenie podane w [31] dla $K = \mathbb{F}_q$ (lub [55] dla przypadku ogólnego pierścienia przemiennego)

Twierdzenie 3.6. *Odwzorowanie* π *dane w następującej postaci:*

$$\mathrm{p}^\pi = [p_{10}, -p_{11}, p_{21}, p_{12}, -p'_{22}, -p_{22}, \ldots, -p'_{ii}, -p_{ii}, p_{i+1,i}, p_{i,i+1}, \ldots],$$

$$\mathrm{l}^\pi = (l_{01}, -l_{11}, l_{21}, l_{12}, -l'_{22}, -l_{22}, \ldots, -l'_{ii}, -l_{ii}, l_{i+1,i}, l_{i,i+1}, \ldots)$$

jest polaryzacją grafu $D(2n, K)$ *(ozn. przez* $D^\pi(2n, K)$*).*

3.2 Operatory sąsiedztwa N_α oraz G_α

Niech $\rho(v)$ będzie funkcją definiującą kolorowanie wierzchołka v (3.1.3), gdzie wierzchołek v grafu Γ przedstawiamy w postaci n-wymiarowego wektora z przestrzeni K^n: $v = (x_1, x_2, \ldots, x_n)$.

Operator $N_\alpha(v)\colon V(\Gamma) \to \mathrm{V}(\Gamma)$ określamy jako operator wybrania sąsiada wierzchołka v o kolorze α.

Rozpatrywany graf $D(n, K)$ składa się z dwóch rodzajów wierzchołków: punktów i prostych. Jeśli zatem operator N_α zastosujemy do punktu (p), otrzymujemy prostą $[l]$, gdzie pierwszą współrzędną jest $l_1 = \alpha$, zaś pozostałe współrzędne $l_2, l_3, \ldots, l_n$ z równań (3.3). Analogicznie, jeżeli operator N_α zastosujemy do prostej $[l]$, otrzymujemy punkt (p), gdzie pierwszą współrzędną jest $p_1 = \alpha$, zaś pozostałe współrzędne $p_2, p_3, \ldots, p_n$ z równań (3.3).

Dla ciągu kolorów $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s)$, gdzie $\alpha_i + \alpha_{i+1} \neq 0$, określamy złożenie odwzorowań $N_\alpha = N_{\alpha_1} N_{\alpha_2} \ldots N_{\alpha_{s-1}} N_{\alpha_s} := N_{\alpha_s}(N_{\alpha_{s-1}} \cdots (N_{\alpha_2}(N_{\alpha_1})))$, $N_{\alpha_i} : V(\Gamma) \to \mathrm{V}(\Gamma)$.

Niech $v_i = (x_1^i, x_2^i, \ldots, x_n^i)$ oznacza i-ty wierzchołek na ścieżce w grafie, gdzie $i = 0, 1, 2, \ldots, s$

Dla danego wierzchołka początkowego v_0 powyższe złożenie operatorów N_α definiuje następującą ścieżkę w grafie:

$$v_0 \longrightarrow v_1 = N_{\alpha_1}(v_0) \longrightarrow v_2 = N_{\alpha_2}(v_1) \longrightarrow \cdots \cdots \longrightarrow v_s = N_{\alpha_s}(v_{s-1}).$$

Wierzchołkom powyższej ścieżki odpowiadają następujące kolory (wartości pierwszych współrzędnych poszczególnych wektorów:

$$\rho(v_0) = x_1^0 \longrightarrow x_1^1 = \alpha_1 \longrightarrow x_1^2 = \alpha_2 \longrightarrow \cdots \longrightarrow x_1^s = \alpha_s = \rho(v_s).$$

Niestety, odwzorowanie N_α nie jest odwzorowaniem wzajemnie jednoznacznym. Rozpatrzymy zatem modyfikację operatora N_α, definiując nowy operator $G_\alpha(v) := N_{x_1+\alpha}$, dla którego zmiana koloru kolejnego wierzchołka polega na dodaniu koloru α do pierwszej współrzędnej wierzchołka v. Odwzorowanie G_α jest odwzorowaniem wzajemnie jednoznacznym.

Jeśli zatem operator G_α zastosujemy do punktu (p), otrzymujemy prostą $[l]$, gdzie pierwszą współrzędną obliczamy ze wzoru $l_1 = p_1 + \alpha$, zaś pozostałe współrzędne $l_2, l_3, \ldots, l_n$ z równań (3.3). Analogicznie, jeżeli operator G_α zastosujemy do prostej $[l]$, otrzymujemy punkt (p), gdzie pierwszą współrzędną obliczamy ze wzoru $p_1 = l_1 + \alpha$, zaś pozostałe współrzędne $p_2, p_3, \ldots, p_n$ z równań (3.3).

Złożenie operatorów

$$G_\alpha = G_{\alpha_1} G_{\alpha_2} \ldots G_{\alpha_{s-1}} G_{\alpha_s} := G_{\alpha_s}(G_{\alpha_{s-1}} \cdots (G_{\alpha_2}(G_{\alpha_1}))),$$

gdzie $G_{\alpha_i} : V(\Gamma) \to \mathrm{V}(\Gamma)$, definiuje ścieżkę w grafie Γ o następujących kolorach kolejnych wierzchołków:

$$\rho(v_0) = x_1^0 \longrightarrow x_1^1 = x_1^0 + \alpha_1 \longrightarrow x_1^2 = x_1^1 + \alpha_2 = x_1^0 + \alpha_1 + \alpha_2, \longrightarrow$$
$$\cdots \longrightarrow x_1^s = x_1^{s-1} + x_1^0 + \alpha_1 + \alpha_2 + \cdots + \alpha_s = \rho(v_s).$$

3.3 Graf lingwistyczny

W tym podrozdziale zdefiniujemy graf lingwistyczny, będący uogólnieniem grafu $D(n, K)$.

Niech M będzie zbiorem skończonym, przedstawionym jako rozłączna suma zbiorów M_1 i M_2, o liczebnościach odpowiednio $|M_1| = r$ oraz $|M_2| = s$. Graf Γ niech będzie grafem dwudzielnym, z podziałem wierzchołków na zbiory P_1 oraz P_2, o liczebnościach $|P_1| = j$ oraz $|P_2| = k$.

Definicja 3.5. [71] Graf (Γ, j, k, r, s) nazywamy *grafem równoległym*, jeżeli istnieje funkcja (surjekcja) $\rho\colon V(\Gamma) \to M$ taka, że jeżeli $v \in P_i$ $(i = 1, 2)$, to $\rho(v) \in M_i$ oraz dla każdej pary (v, m) ($v \in P_i$ oraz $m \in M_i$) istnieje dokładnie jeden sąsiad u, dla którego $\rho(u) = m$. Oznacza to, że dla danego wierzchołka v istnieje dokładnie jeden sąsiad u koloru m.

Z definicji grafu wynika, że $js = kr$. Liczba ta jest rozmiarem grafu równoległego o podanych wyżej parametrach.

Definicja 3.6. Graf $(\Gamma, t_1, t_2, s_1, s_2, K)$ nazywamy *grafem równoległym nad pierścieniem* K, jeżeli $P_1 \simeq K^{t_1}$, $P_2 \simeq K^{t_2}$, $M_1 \simeq K^{s_1}$ oraz $M_2 \simeq K^{s_2}$. W tym przypadku mamy $t_1 + s_2 = t_2 + s_1$, co wynika z rozmiaru grafu $|E(\Gamma)| = |K|^{t_1} \cdot |K|^{s_2} = |K|^{t_2} \cdot |K|^{s_1}$. Jeżeli $|K| < \infty$, wtedy graf równoległy nad pierścieniem K jest grafem równoległym (Γ, j, k, r, s), gdzie $j = |K|^{t_1}$, $k = |K|^{t_2}$, $r = |K|^{s_1}$ oraz $s = |K|^{s_2}$.

Definicja 3.7. Graf równoległy nad K jest *grafem lingwistycznym*, jeżeli $t_1 = s_1 + m$ oraz $t_2 = s_2 + m$.

Pojęcie grafu lingwistycznego pojawiło się po raz pierwszy w pracy [71], zaś w pracy [50] zostały zaprezentowane zastosowania grafów lingwistycznych w protokołach uzgodnienia klucza.

Niech $P = K^{s_1+m}$ (zbiór punktów) i $L = K^{s_2+m}$ (zbiór prostych) będą dwiema przestrzeniami wektorowymi nad K. Jeśli $x \in V$, wtedy $(x) \in P$ oraz $[x] \in L$.

Niech

$$(p) = (p_1, p_2, \ldots, p_{s_1}, p_{s_1+1}, \ldots, p_{s_1+m})$$

oraz

$$[l] = [l_1, l_2, \ldots, l_{s_2}, l_{s_2+1}, \ldots, l_{s_2+m}].$$

Definicja 3.8. Zdefiniujmy teraz lingwistyczną strukturę incydencji (P, L, I_L) pomiędzy wierzchołkami grafu. Mówimy, że punkt (p) jest w relacji incydencji I_L z prostą $[l]$

$((p)I_L[l])$, jeżeli pomiędzy poszczególnymi współrzędnymi punktów i prostych zachodzą następujące równości:

$$\begin{aligned}
a_1 l_{s_1+1} - b_1 p_{s_2+1} &= f_1(p_1, p_2, \ldots, p_{s_1}, l_1, l_2, \ldots, l_{s_2}) \\
a_2 l_{s_1+2} - b_2 p_{s_2+2} &= f_2(p_1, p_2, \ldots, p_{s_1}, p_{s_1+1}, l_1, l_2, \ldots, l_{s_2}, l_{s_2+1}) \\
&\ldots \\
a_m l_{s_1+m} - b_m p_{s_2+m} &= f_m(p_1, p_2, \ldots, p_{s_1}, p_{s_1+1}, \ldots, p_{s_1+m-1}, l_1, l_2, \ldots, l_{s_2}, l_{s_2+1}, \ldots, l_{s_2+m-1})
\end{aligned} \tag{3.5}$$

gdzie, dla $i = 1, 2, \ldots, m$, mamy $a_{s_1+i}, b_{s_2+i} \in \mathrm{Reg}(K)$, zaś f_i są przekształceniami wielomianowymi o współczynnikach z K.

Funkcję kolorującą wierzchołki grafu definiujemy następująco:

$$\begin{aligned}
\rho((p)) &= (p_1, p_2, \ldots, p_{s_1}) \\
\rho([l]) &= [l_1, l_2, \ldots, l_{s_2}]
\end{aligned} \tag{3.6}$$

Zdefiniowaną w ten sposób rodzinę grafów, zależną od wyboru funkcji f_i, $i = 1, \ldots, m$, oznaczamy jako $L(s_1, s_2, m, K)$. W przypadku $s_1 = s_2 = 1$ graf $T(m, K) := L(1, 1, m, K)$ nazywamy *grafem trójkątnym*. Jednym z jego przykładów jest rodzina grafów $D(n, K)$.

3.4 Lingwistyczny układ dynamiczny

Znane przykłady lingwistycznych układów dynamicznych zależnych od czasu zostały skonstruowane dla przypadków ciał skończonych ([55]). Odpowiadają one znanym rodzinom grafów algebraicznych o dużej talii w klasycznej teorii grafów ekstremalnych ([4, 5]). Dla zbudowania ogólnych konstrukcji nad pierścieniem przemiennym K użyjemy głównych rezultatów z ekstremalnej teorii grafów nad K.

Niech $T(n, K)$ będzie grafem trójkątnym, zdefiniowanym w poprzednim rozdziale, z dwoma rodzajami wierzchołków: $(x) = (x_1, x_2, \ldots, x_n)$ (punkty) oraz $[y] = [y_1, y_2, \ldots, y_n]$ (proste). Rozważamy dwie rodziny odwzorowań przestrzeni K^n na siebie: P_α oraz L_α, $\alpha \in K$, takie że:

$$P_\alpha((x_1, x_2, \ldots, x_n)) = [y_1, y_2, \ldots, y_n],$$

gdzie $[y_1, y_2, \ldots, y_n]$ jest sąsiadem wierzchołka $(x_1, x_2, \ldots, x_n)$ o kolorze $\rho([y]) = x_1 + \alpha$.

Podobnie:

$$L_\alpha([y_1, y_2, \ldots, y_n]) = (x_1, x_2, \ldots, x_n),$$

gdzie $(x_1, x_2, \ldots, x_n)$ jest sąsiadem wierzchołka $[y_1, y_2, \ldots, y_n]$ o kolorze $\rho((x)) = y_1 + \alpha$.

Z definicji wynika, że złożenie $P_\alpha L_\alpha$ jest odwzorowaniem tożsamościowym. Możemy również zapisać, że $P_\alpha^{-1} = L_{-\alpha}$ oraz $L_\alpha^{-1} = P_{-\alpha}$. Rodziny odwzorowań P_α oraz L_α, dla $\alpha \in K$ dają pełną informację o grafie $T(n, K)$.

Rozważmy ścieżkę w grafie $v_0, v_1, v_2, \ldots, v_k$ długości k startującej z wierzchołka $v_0 = (x_1, x_2, \ldots, x_n)$ i daną porzez ciąg kolorów $\beta_1, \beta_2, \ldots, \beta_k \in K$ kolejnych wierzchołków, gdzie $\beta_i = \rho(v_i) + \alpha_i$ dla $i = 1, 2 \ldots, k$ (k-nieparzyste):

$$\begin{aligned} v_1 &= P_{\alpha_1}(v_0) = x_1 + \alpha_1 \\ v_2 &= L_{\alpha_2}(v_1) = x_1 + \alpha_1 + \alpha_2 \\ &\vdots \\ v_k &= P_{\alpha_k}(v_{k-1}) = x_1 + \alpha_1 + \alpha_2 + \ldots \alpha_k. \end{aligned}$$

przy czym, ostatni wierzchołek v_k może być równy $v_k = L_{\alpha_k}(v_{k-1})$, w przypadku parzystego k.

Zauważmy, że wierzchołki v_i oraz v_{i+2} są różne, jeżeli $\alpha_{i+1} + \alpha_{i+2} \neq 0$.

Przyjmijmy, że $K = \mathbb{F}_q$ jest ciałem. Rodzina $T(n, K)$ jest rodziną grafów dużej talii. Talia grafu $T(n, K)$ jest wyrażeniem w postaci $cn + b$. Grafy te nie mają cykli C_k dla $k < cn + b$. Dlatego, odwzorowania $P_{\beta_1} L_{\beta_2} P_{\beta_3} \cdots P_{\beta_k}$ (jeśli k jest parzyste) oraz $P_{\beta_1} L_{\beta_2} P_{\beta_3} \cdots L_{\beta_k}$ (jeśli k - nieparzyste) nie mają punktów stałych. Istnienie grafów $T(n, K)$ o dużej talii zostało udowodnione. Okazało się, że tali grafu $D(n, q)$, jako przykładu grafu trójkątnego, jest większa bądź równa $n + 5$ (w większości przypadków jest równa $n + 5$).

Niech P_α i L_α będą odwzorowaniami zdefiniowanymi nad grafem $D(n, K)$, dla ogólnego pierścienia K. W [55] zostało pokazane, że złożenia odwzorowań $P_{\beta_1} L_{\beta_2} P_{\beta_3} \cdots P_{\beta_k}$ (jeśli k jest parzyste) oraz $P_{\beta_1} L_{\beta_2} P_{\beta_3} \cdots L_{\beta_k}$ (jeśli k - nieparzyste) nie mają punktów stałych, jeśli wartości $\alpha_i + \alpha_{i+1}$ $(i = 1, 2, \ldots, k-1)$ są elementami regularnymi pierścienia K. Rozważania te stały się motywacją do zdefiniowania i udowodnienia istnienia lingwistycznych układów dynamicznych ([55]).

Definicja 3.9. *Lingwistycznym układem dynamicznym wymiaru n nad dowolnym pierścieniem przemiennym K* nazywamy rodzinę F nieliniowych odwzorowań wielomianowych $f_\alpha \colon K^n \to K^n$, $\alpha \in \{K - 0\}$, takich że

- $f_\alpha^{-1} = f_{-\alpha}$,
- $f_{\alpha_1}(x) = f_{\alpha_2}(x)$ dla pewnego $x \in K^n$, implikuje $\alpha_1 = \alpha_2$,
- każde odwzorowanie f_α nie ma punktów stałych.

Sąsiedztwo $\{f_\alpha | \alpha \in \{K - 0\}\}$ elementu v definiuje graf $\Gamma(F)$ lingwistycznego układu dynamicznego na zbiorze wierzchołków K^n.

Niech $f_\alpha = f_{\alpha_1} f_{\alpha 2} \cdots f_{\alpha_k} = f_{\alpha_k}(f_{\alpha_{k-1}}(\cdots f_{\alpha_2}(f_{\alpha_1})))$ będzie złożeniem odwzorowań $f_{\alpha_1}, f_{\alpha_2}, \ldots, f_{\alpha_k}$.

Definicja 3.10. Mówimy, że lingwistyczny układ dynamiczny $F = \{f_a \mid K^n \to K^n,\ \alpha \in \{K - 0\}\}$ ma poziom $d = d(n)$, jeżeli dla każdego ciągu $a = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, $k \leq d$, gdzie wyrażenie $\alpha_i + \alpha_{i+1}$ nie jest dzielnikiem zera dla $i = 1, 2, \ldots, d - 1$, wierzchołki v i $v_a = f_a(v)$ są ze sobą połączone jednoznacznie wyznaczoną ścieżką. Oznacza to, że odwzorowanie f_a nie ma punktów stałych.

Zauważmy, że w grafie $D(n, K)$ operator G_α możemy zdefiniować następująco:

$$G_\alpha(x) = \begin{cases} P_\alpha(x), & x \text{ jest punktem}, \\ L_\alpha(x), & x \text{ jest prostą}. \end{cases}$$

Niech H_α operatorem sąsiedztwa dla grafu polaryzacji $D^\pi(2n, K)$ (3.1.4) koloru $x_1 + \alpha$, można go interpretować jako złożenie $G_\alpha \cdot \pi$ obcięte do zbioru punktów grafu $D(2n, K)$. W [55] zostało udowodnione, że odwzorowanie H_α tworzy lingwistyczny układ dynamiczny poziomu $d(n) \geq \frac{1}{3}n$, którego grafem jest $D^\pi(2n, K)$. Złożenie operatorów $H_\alpha = H_{\alpha_1} H_{\alpha 2} \cdots H_{\alpha_k} = H_{\alpha_k}(H_{\alpha_{k-1}}(\cdots H_{\alpha_2}(H_{\alpha_1})))$ nie ma punktów stałych, jeśli wyrażenia $\alpha_i + \alpha_{i+1} \in \mathrm{Reg}(K)$ dla $i = 1, 2, \ldots, k - 1$, $k < d(n)$. W artykule [60] zostało udowodnione, że warunkiem dostatecznym braku punktów stałych jest, aby $\alpha_1(\alpha_1 + \alpha_2)(\alpha_2 + \alpha_3) \ldots (\alpha_{k-1} + \alpha_k) \neq 0$. Jest to warunek bardziej ogólny, pozwala w łatwiejszy sposób dobrać odpowiednie parametry $\alpha_1, \alpha_2, \ldots, \alpha_k$.

Niech $P = K^n$ oraz $L = K^n$ będą dwiema kopiami modułu wolnego nad pierścieniem K.

Definicja 3.11. *Arytmetycznym układem dynamicznym nad pierścieniem przemiennym* K nazywamy rodzinę F nieliniowych odwzorowań wielomianowych $f_\alpha \colon P \cup L \to P \cup L$, $\alpha \in K$, takich że:

- $f_\alpha^{-1} = f_{-\alpha}$,
- $f_{\alpha_1}(x) = f_{\alpha_2}(x)$ dla pewnego $x \in P \cup L$, implikuje $\alpha_1 = \alpha_2$,
- $f_\alpha(P) = L$ oraz $f_\alpha(L) = P$.

Przykładem arytmetycznego układu dynamicznego nad pierścieniem K może być operator G_α obliczenia sąsiada koloru $\rho(v) + \alpha$ dla wierzchołka v w grafie lingwistycznym $L(1, 1, n, K)$.

Definicja 3.12. Mówimy, że arytmetyczny układ dynamiczny $F = \{f_a \mid P \cup L \to P \cup L,\ \alpha \in K\}$ ma poziom $d = d(n)$, jeżeli dla każdego ciągu $a = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, $k \leq d$, gdzie wyrażenie $\alpha_i + \alpha_{i+1}$ nie jest dzielnikiem zera dla $i = 1, 2, \ldots, d-1$, wierzchołki v i $v_a = f_a(v)$ są ze sobą połączone jednoznacznie wyznaczoną ścieżką.

Przykładem arytmetycznego układu dynamicznego poziomu $d(n)$ może być operator G_α obliczenia sąsiada koloru $\rho(v) + \alpha$ dla wierzchołka v w grafie lingwistycznym $D(n, K)$ (rozdział 3.2). Inny przykład otrzymujemy zamieniając graf $D(n, K)$ na $CD(n, K)$ nad pierścieniem K. Rodzina operatorów G_α wybrania sąsiada koloru $\rho(v) + \alpha$ dla $v \in CD(n, K)$ (rozdział 5.1) tworzy arytmetyczny układ dynamiczny poziomu $d(n) > \frac{1}{3}$.

Rozważmy graf skierowany $\Gamma = DD(n, K)$ (konstrukcja zostanie przedstawiona w rozdziale 4.2), którego zbiór wierzchołków składa się z rozłącznej sumy F_1 oraz F_2, zdefiniowanych następująco:

$$F_1 = \{\langle (p), [l] \rangle \mid (p) I [l]\} \quad \cong K^{n+1},$$
$$F_2 = \{\{[l], (p)\} \mid [l] I (p)\} \quad \cong K^{n+1}.$$

Operator sąsiedztwa $G_\alpha \colon K^{n+1} \cup K^{n+1} \to K^{n+1} \cup K^{n+1}$, działa na wierzchołkach grafu w poniższy sposób:

$$G_\alpha(\langle (p), [l] \rangle) = \big\{\{[l], (p')\} \big|\ [l] I (p'),\ \rho(p') = p_1 + \alpha\big\},$$
$$G_\alpha(\{[l], (p)\}) = \big\{\langle (p), [l'] \rangle \big|\ (p) I [l'],\ \rho(l') = l_1 + \alpha\big\}.$$

W [60] zostało pokazane, że operator G_α dla grafu $DD(n, K)$ (rozdział 4.2) tworzy dwudzielny lingwistyczny układ dynamiczny o dużej talii, zdefiniowany poniżej.

Niech $P = K^n$ oraz $L = K^n$ będą dwiema kopiami modułu wolnego nad pierścieniem K.

Definicja 3.13. Rodzinę F bijektywnych, nieliniowych odwzorowań wielomianowych $f_{\alpha,n}$, $n = 3, 4, \ldots$, $t \in K$ zbioru $P \cup L$ w siebie nazywamy *dwudzielnym lingwistycznym układem dynamicznym dużej talii*, jeżeli odwzorowania odwrotne do $f_{\alpha,n}$ są odwzorowaniami wielomianowymi $f'_{\alpha,n}$ oraz istnieje niezależna stała $c > 0$, taka że dla każdego zbioru multiplikatywnych generatorów Q z K są spełnione następujące warunki:

- dla ciągu elementów α_1, α_2, $\ldots$, α_s, $1 \leq k \leq 2cn$ z Q złożenie $f_{\alpha_1,\alpha_2,\ldots,\alpha_s,n}$ odwzorowań $f_{\alpha_1,n}$, $f_{\alpha_2,n}$, $\ldots$, $f_{\alpha_s,n}$ nie ma punktów stałych,
- dla każdej pary różnych ciągów $(\alpha_1, \alpha_2, \ldots, \alpha_s) \in Q^k$ i $(\beta_1, \beta_2, \ldots, \beta_s) \in Q^s$ długości $k < cn$ i $s < cn$ i dla każdego punktu x z $P \cup L$ wartości $f_{\alpha_1,\alpha_2,\ldots,\alpha_s,n}(x)$ i $f_{\beta_1,\beta_2,\ldots,\beta_s,n}(x)$ są różne,
- dla każdego zbioru multiplikatywnych generatorów $\{\alpha_1, \alpha_2, \ldots, \alpha_s\}$ rząd odwzorowania $f_{\alpha_1,\alpha_2,\ldots,\alpha_s,n}$ dąży do nieskończoności, gdy parametr n dąży do nieskończoności.

Użycie zbiorów multiplikatywnych zamiast elementów regularnych pierścienia w lingwistycznych układach dynamicznych, pozwala na rozszerzenie zbioru kolorów M. Dobrym przykładem jest tutaj pierścienia Boole'a $\mathbb{B}_n$ (np. 2^A zdefiniowany w rozdziale 1.2), który nie ma elementów regularnych, ale posiada duże zbiory multiplikatywne, np podzbiór zbioru A, wszystkich elementów pierścienia zawierających jedynkę - taki zbiór ma 2^{n-1} elementów.

3.5 Uogólnienie lingwistycznych układów dynamicznych i odpowiadające im obliczenia symboliczne

Niech $N_{\alpha,\phi} := N_{a_1(p_1),a_2(p_1),\ldots,a_s(p_1),\phi}$ będzie uogólnieniem operatora sąsiedztwa nad pierścieniem przemiennym K. Operator ten definiuje przejście ścieżki w grafie lingwistycznym z wierzchołkiem startowym $(p_1, p_2, \ldots, p_n) \in K^n$ i ciągiem kolorów kolejnych wierzchołków $a = a_1(p_1), a_2(p_1), \ldots, a_s(p_1)$, podanych w sposób rekurencyjny:

$$\begin{aligned} a_0(p_1) &= p_1 \\ a_1(p_1) &= \phi_1(p_1) \\ a_i(p_1) &= \phi_i(a_{i-1}(p_1)),\ i = 2, 3, \ldots, s, \end{aligned} \tag{3.7}$$

gdzie ϕ_i, dla $i = 1, 2, \ldots, s$ są odwzorowaniami wielomianowymi zmiennej p_1.

W tym przypadku funkcje a_i, dla $i = 1, 2, \ldots, s$ są odwzorowaniami wielomianowymi zmiennej p_1, zaś dodatkowo $a_s(p_1)$ jest funkcją wzajemnie jednoznaczną.

Operator $N_{\alpha,\phi}$ definiuje lingwistyczny układ dynamiczny, który możemy przedstawić w postaci:

$$\begin{cases} g_1(p_1) = c_1 \\ g_2(p_1, p_2) = c_2 \\ \vdots \\ g_n(p_1, \ldots, p_n) = c_n. \end{cases} \tag{3.8}$$

W powyższym układzie $g_1(p_1) = a_s(p_1)$, zaś $g_i(p_1, \ldots, p_i)$ są odwzorowaniami wielomianowym zmiennych $p_1, \ldots, p_i$, dla $i = 2, 3 \ldots, n$.

Lemat 3.7. *Niech $a_s(p) \in K[p]$ będzie bijekcją nad pierścieniem K. Wtedy przekształcenie $F_{a,n}$, zdefiniowane powyżej, jest bijekcją w postaci wielomianowej.*

Przykład 3.1. Niech $\phi_i(p_1) = p_1 + \alpha_i$ dla $i = 1, 2, \ldots, s$. Obliczmy zatem kolejne kolory wierzchołków:

$$\begin{aligned} a_0(p_1^0) &= p_1 \\ a_1(p_1^1) &= \phi_1(p_1) = p_1 + \alpha_1 \\ a_2(p_1^2) &= \phi_2(a_1(p_1)) = p_1 + \alpha_1 + \alpha_2 \\ &\ldots \\ a_k(p_1^k) &= \phi_s(a_{k-1}(p)) = p_1 + \alpha_1 + \alpha_2 + \cdots + \alpha_s \end{aligned} \tag{3.9}$$

Operator sąsiedztwa $N_{a,\phi} = N_{a_1(p_1),a_2(p_1),\ldots,a_s(p_1),\phi}$ jest równoznaczny operatorowi $G_{\alpha_1,\alpha_2,\ldots,\alpha_s}$, zdefiniowanemu wcześniej w rozdziale 3.2. Otrzymany operator $N_{a,\phi}$ generuje lingwistyczny układ dynamiczny odpowiadający stabilnym przekształceniom kubicznym, których konstrukcja będzie przedstawiona w rozdziale 4.1.

3.6 Lingwistyczny układ dynamiczny z pojedynczym zaburzeniem

Korzystając z oznaczeń z poprzedniego podrozdziału, rozpatrzmy operator sąsiedztwa $N_{a,\phi,h} := N_{a_1(p_1),a_2(p_1),\ldots,a_s(p_1),\phi,h}$ nad pierścieniem przemiennym K. Operator ten definiuje przejście ścieżki w grafie lingwistycznym z wierzchołkiem startowym $(p_1, p_2, \ldots, p_n) \in K^n$ i ciągiem kolorów kolejnych wierzchołków $a = a_1(p_1), a_2(p_1), \ldots, a_s(p_1)$, podanych w sposób rekurencyjny:

$$\begin{aligned} a_0(p_1) &= p_1 \\ a_1(p_1) &= h(p_1) \\ a_i(p_1) &= \phi_i(a_{i-2}(p_1)),\ i = 2, 3, \ldots, s, \end{aligned} \tag{3.10}$$

gdzie ϕ_i, dla $i = 1, 2, \ldots, s$ są wielomianami zmiennej p, zaś h jest wzajemnie jednoznacznym odwzorowaniem wielomianowym, zwanym "zaburzeniem".

Przykład 3.2. Niech

$$\begin{aligned} a_0(p_1) &= p_1 \\ a_1(p_1) &= h(p_1) + \alpha_1 \end{aligned}$$

Niech $\phi_i(p_1) = p_1 + \alpha_i$ dla $i = 2, 3, \ldots, s$ Obliczmy zatem kolejne kolory wierzchołków:

$$\begin{aligned} a_0(p_1) &= p_1 \\ a_1(p_1) &= h(p_1) + \alpha_1 \\ a_2(p_1) &= \phi_2(a_0(p_1)) = p_1 + \alpha_2 \\ a_3(p_1) &= \phi_3(a_1(p_1)) = h(p_1) + \alpha_1 + \alpha_3 \\ &\ldots \\ a_{2k}(p_1) &= \phi_{2k}(a_{2i-2}(p_1)) = p_1 + \alpha_2 + \alpha_4 + \cdots + \alpha_{2k} \\ a_{2k+1}(p_1) &= \phi_{2k+1}(a_{2i-1}(p_1)) = h(p_1) + \alpha_1 + \alpha_3 + \cdots + \alpha_{2k+1} \end{aligned} \tag{3.11}$$

Otrzymany operator $N_{a,\phi,f}$ generuje lingwistyczny układ dynamiczny z pojedynczym zaburzeniem h, którego konstrukcja będzie przedstawiona w rozdziale 5.2.

Rozdział 4

Rodziny stabilnych odwzorowań wielomianowych niskich stopni

W poniższym rozdziale zajmiemy się konstrukcją i badaniem własności (w szczególności stopni) odwzorowań wielomianowych powstałych przez użycie operatorów sąsiedztwa, tworzących lingwistyczne układy dynamiczne opisane w poprzednim rozdziale. Rozważane w tym rozdziale odwzorowania mają niski stopień: dwa, trzy oraz cztery. Cechą charakterystyczną jest stabilność tych odwzorowań, co oznacza zachowanie stopnia niezależnie od wielokrotności złożenia ze sobą. Opisane przekształcenia mogą być wykorzystane w kryptografii z kluczem prywatnym i publicznym, stanowiąc podstawę wielu algorytmów szyfrujących.

4.1 Kubiczne odwzorowania wielomianowe - konstrukcja podstawowa

Przedstawiona w tym rozdziale, podstawowa konstrukcja odwzorowań kubicznych, oparta na grafach prostych $D(n, K)$, stanowi podstawę wielu algorytmów kryptograficznych rozpatrywanych przez członków naszego zespołu badawczego.

Udowodniony został fakt, że przekształcenie wielomianowe, powstałe przez złożenie specjalnych operatorów sąsiedztwa, zdefiniowanych dla rodziny grafów $D(n, K)$, ma trzeci stopień, niezależnie od wielokrotności złożenia. Dowód poniższego twierdzenia został przedstawiony w pracy [75].

Twierdzenie 4.1. *Przekształcenie F_α, gdzie $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s)$, powstałe przez złożenie operatorów G_{α_i} zdefiniowanych dla rodziny grafów $D(n, K)$, $1 \leq i \ \leq s$, czyli*

$$F_\alpha = G_{\alpha_1} G_{\alpha_2} \ldots G_{\alpha_{s-1}} G_{\alpha_s} = G_{\alpha_s}(G_{\alpha_{s-1}} \ldots (G_{\alpha_2}(G_{\alpha_1})) \ldots)$$

jest przekształceniem wielomianowym stopnia trzeciego, niezależnie od wyboru $s \in N$ (niezależnie od długości ścieżki w grafie s).

Dowód. Dowód tego twierdzenia (będący również konstrukcją) otrzymujemy używając zasady indukcji matematycznej ze względu na długość ścieżki s.

Jako pierwszy wierzchołek w grafie bierzemy punkt postaci $p = (p_1, p_2, \ldots, p_n) \in K^n$. Z racji tego, że ta konstrukcja oparta jest na grafach algebraicznych, podczas obliczeń będzie używana notacja zaczerpnięta z definicji grafu $D(n, K)$, czyli:

$$p = (p_1, p_2, p_3 \ldots, p_i, \ldots, p_n) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots)\big|_n,$$

$$l = (l_1, l_2, l_3 \ldots, l_i, \ldots, l_n) = [l_1, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, l_{23}, \ldots, l_{ii}, l'_{ii}, l_{i,i+1}, l_{i+1,i}, \ldots]\big|_n.$$

Ciąg $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s)$, zostanie wykorzystany do zmiany koloru kolejnych wierzchołków przez dodanie elementu α_j, $1 \leq j \leq s$ do pierwszej współrzędnej kolejnego wierzchołka w każdym kroku o numerze j. Pozostałe współrzedne obliczane są według instrukcji podanej w definicji operatora G_α (3.2). Dostajemy w ten sposób odwzorowanie będące złożeniem odwzorowań $G_{\alpha_1} G_{\alpha_2} \cdots G_{\alpha_s}$. Jeśli potraktujemy współrzędne pierwszego wierzchołka jako zmienne, wszystkie ten sposób powstałe odwzorowania G_{α_1}, $G_{\alpha_1} G_{\alpha_2}$, $G_{\alpha_1} G_{\alpha_2} \cdots G_{\alpha_s}$ są wielomianami tych zmiennych. W poniższych podpunktach będziemy poszukiwać stopni tak powstałych odwzorowań wielomianowych.

Odwzorowanie G_{α_1} Nasze obliczenia rozpoczniemy od zbadania stopni wielomianów odwzorowania G_{α_1}. Zatem kolejne współrzędne wierzchołka $[l]^{(1)}$ są wielomianami następującej postaci:

$$l_1^{(1)} = p_1 + \alpha_1,$$

$$l_{1,1}^{(1)} = p_{1,1} + l_1 p_1 = p_{1,1} + \alpha_1 p_1 + p_1^2$$

$$l_{1,2}^{(1)} = p_{1,2} + p_1 l_{1,1} = p_{1,2} + p_1 p_{1,1} + \alpha_1 p_1^2 + p_1^3$$

$$l_{i,i}^{(1)} = p_{i,i} + l_1 p_{i-1,i} = p_{i,i} + \alpha_1 p_{i-1,i} + p_1 p_{i-1,i}$$

$$l_{i,i+1}^{(1)} = p_{i,i+1} + p_1 l_{i,i} = p_{i,i+1} + \alpha_1 p_1 p_{i-1,i} + p_1 p_{i,i} + p_1^2 p_{i-1,i}$$

Podobnie otrzymujemy:

$$l_{i+1,i} = p_{i+1,i} + l_1 p'_{i,i} = p_{i+1,i} + \alpha_1 p'_{i,i} + p_1 p'_{i,i}$$

$$l'_{i,i} = p'_{i,i} + p_1 l_{i,i-1} = p'_{i,i} + \alpha_1 p_1 p'_{i-1,i-1} + p_1 p_{i,i-1} + p_1^2 p_{i-1,i-1}$$

dla wszystkich $i = 2, 3, \ldots, \lfloor \frac{n+2}{4} \rfloor$. Jeżeli weźmiemy wierzchołek (p) jako punkt $(p_1, p_2, \ldots, p_n)$, po użyciu powyżej sformułowanego odwzorowania, otrzymujemy wierzchołek będący prostą następującej postaci: $(f_1(p_1), f_2(p_1, p_2), \ldots, f_n(p_1, p_2, \ldots, p_n))$, której składowe są wielomianami o następujących stopniach:

$$\deg f_n(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 2, & n = 2, \\ 2, & n = 4m, 4m+1, \\ 3, & n = 4m+2, 4m-1 \quad \text{gdzie} \quad m = 1, 2, \ldots, (n-2)/4. \end{cases}$$

Odwzorowanie $G_{\alpha_1} G_{\alpha_2}$ Korzystając z powyższych obliczeń możemy policzyć stopnie odwzorowania $G_{\alpha_1} G_{\alpha_2}$, tworzącego współrzędne kolejnego wierzchołka.

$$p_1^{(2)} = p_1 + \alpha_1 + \alpha_2$$

$$p_{1,1} = l_{1,1} - l_1 p_1^{(2)} = -(\alpha_1 + \alpha_2)(\alpha_1 + p_1)$$

$$p_{1,2}^{(2)} = l_{1,2} - p_1^{(2)} l_{1,1} = p_{1,2} - (\alpha_1 + \alpha_2) p_{1,1} - \alpha_1(\alpha_1 + \alpha_2) p_1 - (\alpha_1 + \alpha_2) p_1^2$$

$$p_{i,i+1}^{(2)} = l_{i,i+1} - p_1^{(2)} l_{i,i} = p_{i,i+1} - (\alpha_1 + \alpha_2)(p_{i,i} + \alpha_1 p_{i-1,i} + p_1 p_{i-1,i})$$

$$p_{i,i}^{(2)} = l_{i,i} - l_1 p_{i-1,i}^{(2)} = p_{i,i} + (\alpha_1 + p_1)(\alpha_1 + \alpha_2)(p_{i-1,i-1} + \alpha_1 p_{i-2,i-1} + p_1 p_{i-2,i-1})$$

Podobnie otrzymujemy:

$$p_{i,i}^{\prime(2)} = l'_{i,i} - p_1^{(2)} l_{i,i-1} = p'_{i,i} - (\alpha_1 + \alpha_2)(p_{i,i-1} + \alpha_1 p_{i-1,i-1} + p_1 p'_{i-1,i-1})$$

$$p_{i+1,i}^{(2)} = l_{i+1,i} - l_1 p_{i,i}^{\prime(2)} = p_{i+1,i} + (\alpha_1 + p_1)(\alpha_1 + \alpha_2)(p_{i-1,i-1} + \alpha_1 p'_{i-1,i-1} + p_1 p'_{i-1,i-1})$$

dla wszystkich $i = 2, 3, \ldots, \lfloor \frac{n+2}{4} \rfloor$.

W ten sposób otrzymaliśmy punkt: $(p)^{(2)} = (g_1(p_1), g_2(p_1, p_2), \ldots, g_n(p_1, p_2, \ldots, p_n))$, którego składowe są wielomianami o następujących stopniach:

$$\deg g_n(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 1, & n = 2, \\ 2, & n = 4m-1, 4m+2, \\ 3, & n = 4m, 4m+1 \quad \text{gdzie} \quad m = 1, 2, \ldots, (n-2)/4. \end{cases}$$

Odwzorowanie $G_\alpha := G_{\alpha_1} G_{\alpha_2} \ldots G_{\alpha_s}$ Stopnie poszczególnych wierzchołków będących kolejno punktami bądź prostymi, po zastosowaniu odwzorowań $G_{\alpha_1} G_{\alpha_2} \cdots G_{\alpha_{s-1}}$ i $G_{\alpha_1} G_{\alpha_2} \cdots G_{\alpha_s}$ odpowiednio, będą wyznaczone z użyciem indukcji matematycznej (dla parzystej liczby s).

Załóżmy, że przy pomocy złożenia odwzorowań $G_{\alpha_1} G_{\alpha_2} \cdots G_{\alpha_{s-3}}$ otrzymamy punkt:

$$(p)^{(s-3)} = (g_1^{(s-3)}(p_1), g_2^{(s-3)}(p_1, p_2), \ldots, g_n^{(s-3)}(p_1, p_2, \ldots, p_n)),$$

którego składowe są wielomianami o następujących stopniach:

$$\deg g_n^{(s-3)}(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 1, & n = 2, \\ 2, & n = 4m-1, 4m+2, \\ 3, & n = 4m, 4m+1 \quad \text{gdzie} \quad m = 1, 2, \ldots, (n-2)/4. \end{cases}$$

Zakładamy również, że przy użyciu odwzorowania $G_{\alpha_1} G_{\alpha_2} \cdots G_{\alpha_{s-2}}$ otrzymujemy prostą:

$$[l]^{(s-2)} = (f_1^{(s-2)}(p_1), f_2^{(s-2)}(p_1, p_2), \ldots, f_n^{(s-2)}(p_1, p_2, \ldots, p_n))$$

której współrzędne są wielomianami o następujących stopniach:

$$\deg f_n^{(s-2)}(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 2, & n = 2, \\ 2, & n = 4m, 4m+1, \\ 3, & n = 4m+2, 4m-1 \quad \text{where} \quad m = 1, 2, \ldots, (n-2)/4. \end{cases}$$

Następnym krokiem będzie zbadanie stopnia wielomianu $g_n^{(s-1)}$.

$$p_1^{(s-1)} = p_1 + \alpha_1 + \alpha_2 + \ldots + \alpha_{s-3} + \alpha_{s-2} + \alpha_{s-1} = p_1^{(s-3)} + \alpha_{s-2} + \alpha_{s-1}$$

$$p_{i,i+1}^{(s-1)} = l_{i,i+1}^{(s-2)} - p_1^{(s-1)} l_{i,i}^{(s-2)} = p_{i,i+1}^{(s-3)} + p_1^{(s-3)} l_{i,i}^{(s-2)} - p_1^{(s-3)} l_{i,i}^{(s-2)} - (\alpha_{s-2} + \alpha_{s-1}) l_{i,i}^{(s-2)} =$$
$$= p_{i,i+1}^{(s-3)} - (\alpha_{s-2} + \alpha_{s-1}) l_{i,i}^{(s-2)}$$

Widać, że $p_{i,i+1}^{(s-3)}$ jest niezależny od α_{s-2} i α_{s-1} oraz zarówno $p_{i,i+1}^{(s-3)}$ jak i $l_{i,i}^{(s-2)}$ mają stopnie równe 2, otrzymujemy, że $p_{i,i+1}^{(s-1)}$ posiada stopień równy 2.

Przy analogicznym rozumowaniu otrzymujemy, że $p_{i,i}^{(s-1)}$ ma stopnień 3, $p_{i,i}^{'(s-1)}$ stopień 2, oraz $p_{i+1,i}^{(s-1)}$ stopień 3.

Stąd używając odwzorowania wielomianowego $G_{\alpha_1} G_{\alpha_2} \cdots G_{\alpha_{n-1}}$ z wektora początkowego $(p_1, p_2, \ldots, p_n)$ otrzymujemy wektor końcowy postaci:
$(p)^{(s-1)} = (g_1^{(s-1)}(p_1), g_2^{(s-1)}(p_1, p_2), \ldots, g_n^{(s-1)}(p_1, p_2, ..., p_n))$,

którego składowe są wielomianami o następujących stopniach:

$$\deg g_n^{(m-1)}(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 1, & n = 2, \\ 2, & n = 4m-1, 4m+2, \\ 3, & n = 4m, 4m+1 \quad \text{gdzie} \quad m = 1, 2, \ldots, (n-2)/4. \end{cases}$$

W podobny sposób, używając drugiej części założenia indukcyjnego (po zastosowaniu odwzorowania $G_{\alpha_1} G_{\alpha_2} \cdots G_{\alpha_s}$) otrzymujemy prostą postaci: $[l]^{(s)} = (f_1^{(s)}(p_1), f_2^{(s)}(p_1, p_2), \ldots, f_n^{(s)}(p_1, p_2, \ldots, p_n))$ o następujących stopniach:

$$\deg f_n^{(s)}(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 2, & n = 2, \\ 2, & n = 4m, 4m+1, \\ 3, & n = 4m+2, 4m-1 \quad \text{gdzie} \quad m = 1, 2, \ldots, (n-2)/4. \end{cases}$$

Otrzymujemy ostatecznie wierzchołek, którego współrzędne są wielomianami stopnia co najwyżej trzeciego. Zatem odwzorowanie G_α przekształcające wierzchołek początkowy w końcowy, jest wzajemnie jednoznacznym odwzorowaniem kubicznym. □

Twierdzenie 4.2. *[66, 67, 75] Rodzina odwzorowań* $G_\alpha\colon K^n \to K^n$, *tworzy rodzinę podgrup stabilnych grupy Cremona* $C(K^n)$ *stopnia* 3.

Następujące twierdzenie jest wnioskiem z rezultatów uzyskanych w [55]:

Twierdzenie 4.3. *Niech* $a = \alpha_1, \alpha_2, \ldots, \alpha_{2s}$, *gdzie* $\alpha_1+\alpha_2,\ \alpha_2+\alpha_3, \ldots, \alpha_{2s-1}+\alpha_{2s},\ \alpha_{2s}+\alpha_1 \in \mathrm{Reg}(K)$. *Wtedy rząd odwzorowania* $G_a\colon K^n \to K^n$ *dąży do nieskończoności, gdy* n *dąży do nieskończoności.*

4.2 Odwzorowania kubiczne oparte na grafach skierowanych

4.2.1 Idea

W tym rozdziale skupimy się nad stopniami wielomianów, które powstają w wyniku łączenia wierzchołków w grupy po 2 wierzchołki. Analiza tego przypadku, wraz z dowodem została przedstawiona w [67]. Okazało się, że jeśli łączymy wierzchołki po 2 lub 3 (przypadek rozpatrzony w 4.4) otrzymujemy wielomiany o stopniach odpowiednio 3 i 4. Sytuacja zmienia się w przypadku połączenia 4 wierzchołków i więcej. Wtedy stopnie powstałych wielomianów powstałych przez zastosowanie operatora sąsiedztwa rosną liniowo wraz ze wzrostem długości ścieżki w grafie.

4.2.2 Wprowadzenie

Graf skierowany definiujemy jako przeciwzwrotną relacją binarną $\phi \subset V \times V$, gdzie V jest zbiorem wierzchołków grafu.

Wprowadźmy dwa zbiory

$$id(v) = \{x \in V | (a, x) \in \phi\},$$

$$od(v) = \{x \in V | (x, a) \in \phi\}$$

jako zbiory „wejść" i „wyjść" z wierzchołka v. Pojęcie regularność oznacza tutaj, że liczba elementów obu tych zbiorów jest taka sama dla każdego wierzchołka v.

Niech Γ będzie regularnym grafem skierowanym, $E(\Gamma)$ będzie zbiorem krawędzi grafu Γ. Dodatkowo przyjmujemy, że mamy funkcję kolorującą tzn. odwzorowanie $\rho : E \to M$

zbioru krawędzi na zbiór kolorów M, takie, że dla każdego wierzchołka $v \in V$ i $\alpha \in M$ istnieje dokładnie jeden wierzchołek sąsiadujący $u \in V$, z własnością $\rho((v,u)) = \alpha$ oraz operator $G_\alpha(v) := G(\alpha, v)$ wybrania sąsiada u dla wierzchołka v o krawędzi $v \to u$ koloru α jest bijekcją. W tym przypadku graf Γ nazywamy *grafem tęczowym.*

Dla każdego ciągu kolorów $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s)$, $\alpha_i \in M$ możemy wygenerować permutację G_α, która jest złożeniem $G_{\alpha_1} G_{\alpha_2} \cdots G_{\alpha_s}$ bijektywnych odwzorowań $G_{\alpha_i} : V(\Gamma) \to V(\Gamma)$ dla $i = 1, 2 \ldots, s$. Przyjmijmy, że odwzorowanie $u \to G_\alpha(u)$ jest bijekcją. Dla danego wierzchołka $v \in V(\Gamma)$ obliczenie G_α odpowiada łańcuchowi w grafie:

$$v \to v_1 = G(\alpha_1, v) \to v_2 = G(\alpha_2, v_1) \to \cdots \to v_s = G(\alpha_s, v_{s-1}) = v'.$$

Moore [40] użył terminu *taktyczna konfiguracja* rzędu (r_1, r_2) dla biregularnego dwudzielnego grafu prostego o stopniach $r_1 + 1$ i $r_2 + 1$. Odpowiada to strukturze incydencji o zbiorze punktów P, zbiorze prostych L oraz symetrycznej relacji incydencji I. Ich rozmiary są odpowiednio równe $|P|(r_1 + 1)$ oraz $|L|(r_2 + 1)$.

Niech $F = \{(p, l) | p \in P, l \in L, pIl\}$ będzie zbiorem flag dla taktycznej konfiguracji o zbiorach podziału P (zbiór punktów) oraz L (zbiór prostych) i relacji incydencji I. Definiujemy następującą przeciwzwrotną relację binarną ϕ na zbiorze F: Niech (P, L, I) będzie strukturą incydencji odpowiadającą regularnej taktycznej konfiguracji rzędu t.

Niech $F_1 = \{\langle (p), [l] \rangle \mid (p)I[l]\}$, oraz $F_2 = \{\{[l], (p)\} \mid [l]I(p)\}$ będą dwiema kopiami ogółu flag dla (P, L, I). Różne nawiasy pozwolą nam odróżnić elementy zbiorów z F_1 i F_2. Niech $DD(K)$ będzie podwójnym grafem skierowanym na rozłącznej sumie F_1 i F_2 zdefiniowanym poprzez następujące relacje:

$\{[l]^1, (p)^1\} \to \langle (p)^2, [l]^2 \rangle \quad \Leftrightarrow \quad (p)^1 = (p)^2$ oraz $[l]^1 \neq [l]^2$,
$\langle (p)^1, [l]^1 \rangle \to \{[l]^2, (p)^2\} \quad \Leftrightarrow \quad [l]^1 = [l]^2$ oraz $(p)^2 \neq (p)^1$.

4.2.3 Konstrukcja wraz z obliczeniem stopni podwójnego grafu skierowanego odpowiadającemu grafowi tęczowemu

Rozważmy podwójny graf skierowany $DD(n, K)$ dla dwudzielnego grafu $D(n, K)$ oraz nieskończony podwójny graf skierowany $DD(K)$ dla grafu $D(K)$, zdefiniowane nad pierścieniem przemiennym K. Niech G_α będzie operatorem sąsiedztwa wzdłuż krawędzi wychodzących o kolorze $\alpha \in \mathrm{Reg}(K)$ według następującej reguły: jeśli $v^0 = \{[l]^1, (p)^1\} \in F_1$ wtedy $v^1 = \langle (p)^2, [l]^2 \rangle \in F_2$, gdzie kolor v^1 jest równy $\alpha = l_1^2 - l_1^1$, oraz jeśli $v^0 = \langle (p)^1, [l]^1 \rangle \in F_2$ wtedy $v^1 = \{[l]^2, (p)^2\} \in F_1$, gdzie kolorem v^1 jest równy $\alpha = p_1^2 - p_1^1$.

Rozważmy grupę $GF(n+1,K)$ ($GF(K)$, odpowiednio) wygenerowaną przez wszystkie odwzorowania G_α dla niezerowych $\alpha \in \mathrm{Reg}(K)$ działających na $F_1 = K^{n+1}$ (K^∞).

Twierdzenie 4.4. *Ciąg podgrup $GF(n,K)$ grupy Cremona $C(K^n)$ tworzy rodzinę stabilnych podgrup trzeciego stopnia.*

Dowód. W pierwszym kroku połączymy punkty z prostymi, w celu uzyskania dwóch zbiorów wierzchołków nowego grafu:

$$F_1 = \{\langle (p),[l]\rangle \mid (p)I[l]\} \quad \cong K^{n+1},$$

$$F_2 = \{\{[l],(p)\} \mid [l]I(p)\} \quad \cong K^{n+1}.$$

Następnie zdefiniujemy następującą relację pomiędzy wierzchołkami nowego grafu:

$$\langle (p),[l]\rangle R\{[l^{'}],(p^{'})\} \quad \Leftrightarrow \quad [l]=[l^{'}] \ \ \& \ \ p_1 - p_1^{'} \in K$$

$$\{[l^{'}],(p^{'})\}R\langle (p),[l]\rangle \quad \Leftrightarrow \quad (p^{'})=(p) \ \ \& \ \ l_1^{'} - l_1 \in K.$$

Rozważamy następujący ciąg kolorów $\alpha_1, \alpha_2, \ldots, \alpha_s$, taki, że $\alpha_i \in \mathrm{Reg}(K)$ dla $i = 1, \ldots, s$.

Jako pierwszy wierzchołek weźmiemy:

$$\{[l],(p)\} = (l_1, l_{1,1}, l_{1,2}, \ldots, l_{i,j}, p_1)\big|_{n+1}.$$

Współrzędne tego wierzchołka traktujemy jako zmienne. Używając powyższych relacji obliczamy współrzędne kolejnego wierzchołka:

$$\langle (p)^{(1)},[l]^{(2)}\rangle = (p_1, p_{1,1}^{(1)}, \ldots, p_{i,j}^{(1)}, l_1+\alpha_1)\big|_{n+1}$$

o stopniach 2 lub 3, gdzie:

$$\begin{aligned}
&p_{1,1}^{(1)} = l_{1,1} - l_1 p_1, \quad deg = 2\\
&p_{1,2}^{(1)} = l_{1,2} - l_{1,1} p_1 \quad deg = 2\\
&p_{2,1}^{(1)} = l_{2,1} - l_1(l_{1,1} - l_1 p_1) \quad deg = 3\\
&p_{i,i}^{'(1)} = l_{i,i}^{'} - p_1 l_{i,i-1} \quad deg = 2\\
&p_{i,i+1}^{(1)} = l_{i,i+1} - p_1 l_{i,i} \quad deg = 2\\
&p_{i,i}^{(1)} = l_{i,i} - l_1(l_{i-1,i} - p_1 l_{i-1,i-1}) \quad deg = 3\\
&p_{i+1,i}^{(1)} = l_{i+1,i} - l_1(l_{i,i}^{'} - p_1 l_{i,i-1}) \quad deg = 3
\end{aligned}$$

W podobny sposób dostajemy trzeci wierzchołek:

$$\{[l]^{(2)}, (p)^{(3)}\} = (l_1 + \alpha_1, l_{1,1}, \ldots, l_{i,j}, p_1 + \alpha_2)\big|_{n+1},$$

którego współrzędne również mają stopnie 2 lub 3:

$$\begin{aligned}
&l^{(2)}_{1,1} = l_{1,1} + l_1 p_1, \quad deg = 2\\
&l^{(2)}_{1,2} = l_{1,2} + \alpha_1 p_1^2 \quad deg = 2\\
&l^{(2)}_{2,1} = l_{2,1} + \alpha_1 p^{(1)}_{1,1} \quad deg = 2\\
&l^{(2)}_{i,i} = l_{i,i} + \alpha_1 p^{(1)}_{i-1,i} \quad deg = 2\\
&l^{(2)}_{i+1,i} = l_{i+1,i} + \alpha_1 p^{'(1)}_{i,i} \quad deg = 2\\
&l^{'(2)}_{i,i} = l^{'}_{i,i} + \alpha_1 p_1 p^{'(1)}_{i-1,i-1} \quad deg = 3\\
&l^{(2)}_{i,i+1} = l_{i,i+1} + \alpha_1 p_1 p^{(1)}_{i-1,i} \quad deg = 3
\end{aligned}$$

Przyjmijmy poniższe oznaczenia, odpowiednio dla kroków o numerach $(s = 2k-1)$ i $(s = 2k)$ mamy:

$$p_1^{(2k-1)} = p_1 + \alpha_2 + \alpha_4 + \ldots + \alpha_{(2k-2)} = p_1^{(2k-3)} + \alpha_{(2k-2)}$$

$$l_1^{(2k)} = l_1 + \alpha_1 + \alpha_3 + \ldots + \alpha_{(2k-1)} = l_1^{(2k-2)} + \alpha_{(2k-1)}$$

Załóżmy, że współrzędne wierzchołka:

$$\langle (p)^{(2k-1)}, [l]^{(2k)} \rangle = (p_1^{(2k-1)}, p_{1,1}^{(2k-1)}, \ldots, p_{i,j}^{(2k-1)}, l_1^{(2k)})\big|_{n+1}$$

$$\{[l]^{(2k)}, (p)^{(2k+1)}\} = (l_1^{(2k)}, l_{1,1}^{(2k)}, \ldots, l_{i,j}^{(2k)}, p_1^{(2k+1)})\big|_{n+1}$$

mają stopnie:

$$\deg p^{(2k-1)}_{i,j}(l_1, l_2, \ldots, l_k, p_1) = \begin{cases} 2, & (i,j) = (i,i)^{'} \ \text{ lub } \ (i,j) = (i, i+1),\\ 3, & (i,j) = (i,i) \ \text{ lub } \ (i,j) = (i+1, i) \end{cases}$$

$$\deg l^{(2k)}_{i,j}(l_1, l_2, \ldots, l_k, p_1) = \begin{cases} 3, & (i,j) = (i,i)^{'} \ \text{ lub } \ (i,j) = (i, i+1),\\ 2, & (i,j) = (i,i) \ \text{ lub } \ (i,j) = (i+1, i) \end{cases}$$

Teraz, zgodnie z zasadą indukcji matematycznej, chcielibyśmy znaleźć stopnie wielomianowych współrzędnych wierzchołków: $\langle (p)^{(2k+1)}, [l]^{(2k+2)} \rangle$ oraz $\{[l]^{(2k+2)}, (p)^{(2k+3)}\}$. Korzystając z założenia otrzymujemy następujące współrzędne kolejnych wierzchołków

(dla kroków o numerach ($s = 2k + 1$) i ($s = 2k + 2$)) wraz z odpowiadającymi im stopniami:

$$
\begin{aligned}
p_{i,i}^{'(2k+1)} &= p_{i,i}^{'(2k-1)} - \alpha_{2k} l_{i,i-1}^{(2k)} \quad deg = 2 \\
p_{i,i+1}^{(2k+1)} &= p_{i,i+1}^{(2k-1)} - \alpha_{2k} l_{i,i}^{(2k)} \quad deg = 2 \\
p_{i,i}^{(2k+1)} &= p_{i,i}^{(2k-1)} + \alpha_{2k} l_1^{(2k)} l_{i-1,i-1})^{(2k)} \quad deg = 3 \\
p_{i+1,i}^{(2k+1)} &= p_{i+1,i}^{(2k-1)} + \alpha_{2k} l_1^{(2k)} l_{i,i-1}^{(2k)} \quad deg = 3
\end{aligned}
$$

oraz

$$
\begin{aligned}
l_{i,i}^{(2k+2)} &= l_{i,i}^{(2k)} + \alpha_{2k+1} p_{i-1,i}^{(2k+1)} \quad deg = 2 \\
l_{i+1,i}^{(2k+2)} &= l_{i+1,i}^{(2k)} + \alpha_{2k+1} p_{i,i}^{'(2k+1)} \quad deg = 2 \\
l_{i,i}^{'(2k+2)} &= l_{i,i}^{'(2k)} + \alpha_{2k+1} p_1^{(2k+1)} p_{i-1,i-1}^{'(2k+1)} \quad deg = 3 \\
l_{i,i+1}^{(2k+2)} &= l_{i,i+1}^{(2k)} + \alpha_{2k+1} p_1^{(2k+1)} p_{i-1,i}^{(2k+1)} \quad deg = 3
\end{aligned}
$$

Otrzymujemy w ten sposób następujące wyniki:

$$
\deg p_{i,j}^{(2k+1)}(l_1, l_2, \ldots, l_k, p_1) = \begin{cases} 2, & (i,j) = (i,i)^{'} \ \text{ lub } \ (i,j) = (i,i+1), \\ 3, & (i,j) = (i,i) \ \text{ lub } \ (i,j) = (i+1,i) \end{cases}
$$

$$
\deg l_{i,j}^{(2k+2)}(l_1, l_2, \ldots, l_k, p_1) = \begin{cases} 3, & (i,j) = (i,i)^{'} \ \text{ lub } \ (i,j) = (i,i+1), \\ 2, & (i,j) = (i,i) \ \text{ lub } \ (i,j) = (i+1,i) \end{cases}
$$

Ostatecznie, niezależnie od długości ścieżki w grafie s, dzięki użyciu odwzorowania G_α otrzymujemy wierzchołek, którego współrzędne są wielomianami trzeciego stopnia.

□

W pracach [59, 60] przedstawione zostało następujące twierdzenie:

Twierdzenie 4.5. *Niech $a = \alpha_1, \alpha_2, \ldots, \alpha_s$, gdzie α_i dla $i = 1, 2, \ldots, s$ są elementami zbioru multiplikatywnego. Wtedy rząd odwzorowania $G_a \in GF(n, K)$ dąży do nieskończoności, gdy n dąży do nieskończoności.*

4.3 Uogólnienie algorytmu bazującego na grafach skierowanych z użyciem specjalnej grupy automorfizmów

W celu rozszerzenia przestrzeni klucza, w tym rozdziale wprowadzimy uogólnienie wcześniej wprowadzonego algorytmu na grafach skierowanych, używając do tego zmodyfikowanej grupy automorfizmów nieskończonego grafu $D(K)$, zdefiniowanej po raz pierwszy w [29].

W [29] przedstawione zostały dwie grupy automorfizmów

$$G = \langle t_{1,0}(\beta), t_{0,1}(\gamma),\ \beta, \gamma \in K \rangle,$$

$$G' = \langle t_{m,m}(\beta), t'_{m,m}(\gamma),\ \beta, \gamma \in K \rangle.$$

przekształcających $P \to P$ oraz $L \to L$ reguł przedstawionych w tabelach 4.1 oraz 4.2. Na przykład, odwzorowanie $t_{0,1}(\gamma)$ przekształca współrzędną typu $l'_{i,i}$ na współrzędną postaci $l'_{i,i} + l_{i,i-1}\gamma$.

Tabela 4.1: Automorfizmy $t_{1,0}(\beta)$ oraz $t_{0,1}(\gamma)$

x_{ij}	$t_{1,0}(\beta)$	$t_{0,1}(\gamma)$
$l_{i,i}$	$l_{i,i}$	$l_{i,i} + l_{i,i-1}\gamma$
$l_{i,i+1}$	$l_{i,i+1}$	$l_{i,i+1} + (l_{i,i} + l'_{i,i})\gamma + l_{i,i-1}\gamma^2$
$l_{i+1,i}$	$l_{i+1,i} + l_{i,i}\beta$	$l_{i+1,i}$
$l'_{i,i}$	$l'_{i,i} + l_{i-1,i}\beta$	$l'_{i,i} + l_{i,i-1}\gamma$
$p_{i,i}$	$p_{i,i} + p_{i-1,i}\beta$	$p_{i,i} + p_{i,i-1}\gamma$
$p_{i,i+1}$	$p_{i,i+1}$	$p_{i,i+1} + p'_{i,i}\gamma$
$p_{i+1,i}$	$p_{i+1,i} + (p_{i,i} + p'_{i,i})\beta + p_{i-1,i}\beta^2$	$p_{i+1,i}$
$p'_{i,i}$	$p'_{i,i} + p_{i-1,i}\beta$	$p'_{i,i}$

Powyższy grupa automorfizmów nieskończonego grafu prostego $D(K)$ może być użyta jako grupa automorfizmów grafu skierowanego $DD(K)$, przedstawionego w poprzednim rozdziale.

Rozważmy zatem dwie grupy automorfizmów $\widetilde{G}$ oraz $\widetilde{G'}$ grafu skierowanego $DD(K)$ zdefiniowane w następujący sposób:

$$\widetilde{G} = \langle \widetilde{t_{1,0}(\beta)}, \widetilde{t_{0,1}(\gamma)},\ \beta, \gamma \in K \rangle,$$

Tabela 4.2: Automorfizmy $t_{m,m}(\beta)$ oraz $t'_{m,m}(\gamma)$

x_{ij}	$t_{1,0}(\beta)$
$l_{i,i}$	$l_{i,i} - l_{r,r}\beta,\ r = i - m \geq 0$
$l_{i,i+1}$	$l_{i,i+1} - l_{r,r+1}\beta,\ r = i - m \geq 0$
$l_{i+1,i}$	$l_{i+1,i}$
$l'_{i,i}$	$l'_{i,i}$
$p_{i,i}$	$p_{i,i} - p_{r,r}\beta,\ r = i - m \geq 0$
$p_{i,i+1}$	$p_{i,i+1} - p_{r,r+1}\beta,\ r = i - m \geq 0$
$p_{i+1,i}$	$p_{i+1,i}$
$p'_{i,i}$	$p'_{i,i}$.

x_{ij}	$t_{1,0}(\beta)$
$l_{i,i}$	$l_{i,i}$
$l_{i,i+1}$	$l_{i,i+1}$
$l_{i+1,i}$	$l_{i+1,i} + l_{r+1,r}\gamma,\ r = i - m \geq 0$
$l'_{i,i}$	$l'_{i,i} + l'_{r,r}\gamma,\ r = i - m \geq 0$
$p_{i,i}$	$p_{i,i}$
$p_{i,i+1}$	$p_{i,i+1}$
$p_{i+1,i}$	$p_{i+1,i} + p_{r+1,r}\gamma,\ r = i - m \geq 0$
$p'_{i,i}$	$p'_{i,i} + p'_{r,r}\gamma,\ r = i - m \geq 0.$

$$\widetilde{G'} = \langle \widetilde{t_{m,m}(\beta)}, \widetilde{t'_{m,m}(\gamma)},\ \beta, \gamma \in K \},$$

gdzie:

$$\langle (p), [l] \rangle^{\widetilde{t_\lambda(x)}} = \langle (p^{t_\lambda(x)}), [l^{t_\lambda(x)}] \rangle,$$

$$\{ [l], (p) \}^{\widetilde{t_\lambda(x)}} = \{ [l^{t_\lambda(x)}], (p^{t_\lambda(x)}) \},$$

dla $\lambda \in \{(1,0), (0,1), (m,m), (m,m)'\}$ i $x = \beta, \gamma$.

Następnie, poprzez złożenie powyższych odwzorowań, definiujemy dwa przekształcenia T_s oraz T'_r postaci:

$$T_s = \widetilde{t_{1,0}(\beta_1)} \widetilde{t_{0,1}(\gamma_1)} \widetilde{t_{1,0}(\beta_2)} \widetilde{t_{0,1}(\gamma_2)} \ldots \widetilde{t_{1,0}(\beta_s)} \widetilde{t_{0,1}(\gamma_s)},$$

$$T'_r = \widetilde{t_{2,2}(\beta_2)} \widetilde{t'_{2,2}(\gamma_2)} \widetilde{t_{3,3}(\beta_3)} \widetilde{t'_{3,3}(\gamma_3)} \cdots \widetilde{t_{r,r}(\beta_r)} \widetilde{t'_{r,r}(\gamma_r)}.$$

Możemy teraz złożyć powyższe odwzorowanie z odwzorowaniem, danym poprzez ścieżkę w grafie długości k (k jest parzystą liczbą naturalną) $G_k = G_{\alpha_1} G_{\alpha_2} \dots G_{\alpha_k}$ z warunkiem $\alpha_i + \alpha_{i+1} \in \mathrm{Reg}(K)$, dla $i = 1, 2 \dots, k-1$ oraz $\alpha_1 + \alpha_k \in \mathrm{Reg}(K)$.

Na podstawie powyższych założeń w pracy [63] zostały udowodnione następujące twierdzenia:

Twierdzenie 4.6. *Dla dowolnych parametrów s, r i k otrzymujemy zależność $T_s T'_r G_k = G_k T_s T'_r$.*

Twierdzenie 4.7. *Dla grafu nieskończonego $D(K)$, rząd odwzorowania $G_k = G_{\alpha_1} G_{\alpha_2} \dots G_{\alpha_k}$, gdzie k jest parzystą liczbą naturalną oraz $\alpha_i + \alpha_{i+1} \in \mathrm{Reg}(K)$, dla $i = 1, 2 \dots, k-1$ oraz $\alpha_1 + \alpha_k \in \mathrm{Reg}(K)$, jest równy nieskończoność.*

Twierdzenie 4.8. *Jeżeli K ma przynajmniej 3 elementy regularne (nie będące dzielnikami zera), wtedy rząd odwzorowanie T_s, działającego na wierzchołkach grafu nieskończonego, jest nieskończoność.*

Dla celów praktycznych rzutujemy G_k, T_s oraz T'_r na n początkowych współrzędnych, w celu ostatecznego otrzymania odwzorowań G_k^n, T_s^n oraz $T_r'^n$, odpowiednio.

Z poprzednich twierdzeń wynika, że

- rzędy odwzorowań G_k^n oraz T_s^n rosną wraz ze wzrostem n,
- rząd $g = T_s^n T_r'^n G_k^n$ jest najmniejszą wspólną wielokrotnością $T_s T_r'^n$ i G_k.

rzędy odwzorowań G_k^n oraz T_s^n rosną wraz ze wzrostem n.

Grupa $\widetilde{G'} = \langle \widetilde{t_{m,m}(\beta)}, \widetilde{t'_{m,m}(\gamma)},\ \beta, \gamma \in K \}$ działa wierzchołkowo i krawędziowo tranzytywnie na spójnych składowych grafu $DD(n, K)$. Oznacza to możliwość przejścia z dowolnego wierzchołka do każdego innego, nawet jeśli leżą w różnych spójnych składowych. Ważną zaletą jest również zwiększenie rzędu przez użycie podanych grup automorfizmów.

4.4 Odwzorowania wielomianowe stopnia czwartego

W tym rozdziale rozważymy kolejną modyfikację odwzorowań wielomianowych opartych na of $D(n, K)$ (or $D(K)$). Wyniki tego podrozdziału zostały opublikowane w [62] Podobnie jak w rozdziale 4.2.3 łączyliśmy wierzchołki w pary, tak teraz będziemy łączyć wierzchołki grafu w trójki. Konstrukcja powstała w sposób analogiczny, mimo to powoduje zwiększenie stopnia odwzorowania z 3 na 4. Zauważyliśmy również, że w przypadku

połączenia ze sobą czterech wierzchołków lub więcej, sytuacja zmienia się diametralnie - stopnie rosną liniowo, w zależności od długości klucza oraz wymiaru przestrzeni.

Niech F_1 będzie ogółem ścieżek długości 3 w $D(n, K)$ postaci $u = (p_1)I[l]I(p_2)$, zaś F_2 ogółem ścieżek postaci $[l_1](p)[l_2]$

Zdefiniujmy teraz relacje incydencji pomiędzy dwiema rodzajami wierzchołkami nowego grafu:

$$\langle (p^1), [l], (p^2)\rangle R\{[l'^1], (p'), [l'^2]\} \quad \Leftrightarrow$$
$$\Leftrightarrow \quad [l] = [l'^1] \ \ \& \ \ (p^2) = (p') \ \ \& \ \ {l'^2}_{0,1} - {p^2}_{1,0} \in \operatorname{Reg} K$$

$$\{[l^1], (p), [l^2]\} R\langle (p'^1), [l'], (p'^2)\rangle \quad \Leftrightarrow$$
$$\Leftrightarrow \quad (p) = (p'^1) \ \ \& \ \ [l^2] = [l'] \ \ \& \ \ {p'^2}_{1,0} - l^2_{0,1} \in \operatorname{Reg}(K)$$

Rozważmy zatem następujące kolorowanie: kolorem krawędzi pomiędzy $u = (p^1)I[l]I(p^2)$ i $u' = [l]I(p^2)I[l']$ jest wartość $\alpha = l'_{0,1} - {p^2}_{1,0}$, zaś pomiędzy $u' = [l]I(p)I[l']$ oraz $u = (p)I[l'](p')$ kolorem jest $\beta = p'_{1,0} - l'_{0,1}$. Ścieżkę w grafie wyznacza następujący ciąg kolorów parzystej długości: $\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_k, \beta_k$.

Utworzona zostaje w ten sposób grupa permutacji $TF_n(K)$ $(TF(K))$ działająca na $F_1 = K^{n+2}$ (K^∞), odpowiadająca powyższemu kolorowaniu. Generatorami tej grupy są odwzorowania wielomianowe $G_{\alpha,\beta}$ nad K^{n+2} powstałe w wyniku przejścia w grafie ścieżki długości 2, gdzie zmiennymi tych odwzorowań są współrzędne pierwszego wierzchołka w nowym grafie.

Twierdzenie 4.9. *Ciąg podgrup $TF_n(K)$ grupy Cremona $C_n(K)$ tworzy rodzinę podgrup stabilnych stopnia* 4.

Dowód. Aby udowodnić powyższą tezę rozważmy wyżej zdefiniowane dwa rodzaje wierzchołków:

$$F_1 = \big\{\langle (p^1), [l], (p^2)\rangle \ \ | \ \ (p^1)I[l]I(p^2)\big\},$$
$$F_2 = \big\{\{[l^1], (p), [l^2]\} \ \ | \ \ [l^1]I(p)I[l^2]\big\},$$

ciąg kolorów $\alpha_1, \alpha_2, \ldots, \alpha_{2k}$ oraz zdefiniowane powyżej relacje pomiędzy wierzchołkami nowego grafu.

Według tego schematu ostatnie dwa wierzchołki (krok $(2k)$ i $(2k+1)$) mają postać odwzorowań wielomianowych nad K^{n+2}:

$$\langle (p^{2k-2}), [l^{2k-1}], (p^{2k}) \rangle =$$

$$= (p_{1,0}+\alpha_1+\beta_1+\ldots+\alpha_{k-1}, p_{1,1}, \ldots, p_{i,j}, l^2_{0,1}+\beta_1+\alpha_2+\ldots+\beta_{k-2}, p_{1,0}+\alpha_1+\ldots+\alpha_k)\big|_{n+2},$$

$$\{[l^{2k-1}], (p^{2k}), [l^{2k+1}]\} =$$

$$= (l^2_{0,1}+\beta_1++\alpha_2+\ldots+\beta_{k-1}, l_{1,1}, \ldots, l_{i,j}, p_{1,0}+\alpha_1+\ldots+\alpha_k, l^2_{0,1}+\beta_1+\ldots+\beta_k)\big|_{n+2},$$

gdzie stopnie są równe:

$$\deg p^{(2k)}_{i,j}(l_1, l_2, \ldots, l_k, p_1, l_1)\big|_{n+2} = \begin{cases} 3, & (i,j) = (i,i)' \text{ or } (i,j) = (i,i+1), \\ 4, & (i,j) = (i,i) \text{ or } (i,j) = (i+1,i), \end{cases}$$

oraz

$$\deg l^{(2k+1)}_{i,j}(l_1, l_2, \ldots, l_k, p_1, l_1)\big|_{n+2} = \begin{cases} 4, & (i,j) = (i,i)' \text{ or } (i,j) = (i,i+1), \\ 3, & (i,j) = (i,i) \text{ or } (i,j) = (i+1,i), \end{cases}$$

Widzimy więc, że niezależnie od długości ciągu kolorów odwzorowanie tworzy ciąg podgrup stabilnych stopnia 4. □

Homomorfizm grafu $D(n,K)$ na graf $D(n-1,K)$ może być rozszerzony do homomorfizmu grup $TF_{n+2}(K)$ na grupę $TF_{n+1}(K)$. Oznacza to, że grupa $TF(K)$ jest granicą rzutową grupy $TF_n(K)$ dla $n \to \infty$. Niech δ_n będzie homomorfizmem $TF(K)$ na $TF_n(K)$. W pracy [62] udowodniliśmy dodatkowo poniższe twierdzenie:

Twierdzenie 4.10. *Rząd elementu g_n grupy $TF_n(K)$, powstałego przez n-krotne złożenie generatorów $G_{\alpha,\beta}$, takich, że α i β są elementami* $\mathrm{Reg}(K)$*, jest ograniczony przez $[n+5]/2k$, gdzie $[n+5]/2 \geq k$.*

4.5 Odwzorowania wielomianowe stopnia drugiego

W tym rozdziale rozważymy przekształcenia wielomianowe stopnia drugiego, przedstawione przez nas w pracy [64]. Przekształcenia te powstają przez złożenie ze sobą na przemian dwóch operatorów sąsiedztwa oraz użycie równań kwadratowych charakteryzujących spójne składowe grafu $D(n,K)$.

Niech $P_{D,\alpha,n}$ będzie operatorem sąsiedztwa dla punktu

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i})\big|_n,$$

następującej postaci:

$$[l] = [p_{0,1} + \alpha, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}]\big|_n,$$

gdzie parametry $l_{1,1}, l_{1,2}, l_{1,2}, l_{2,2}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots$ są policzone kolejno z równań definiujących graf $D(n, K)$. Podobnie, $L_{D,\alpha,n}$ będzie operatorem sąsiedzwa dla prostej

$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, \ldots, l_{i,i}, l_{i,i+1}, l'_{i,i}, l_{i+1,i}]\big|_n$$

postaci

$$(p) = (l_{1,0} + \alpha, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i})\big|_n,$$

gdzie parametry $p_{1,1}$, $p_{1,2}$, $p_{2,1}$, $p_{2,2}$,..., $p_{i,i}$, $p'_{i,i}$, $p_{i,i+1}$, $p_{i+1,i}$, ... są policzone kolejno z równań podanych powyżej.

Zauważmy, że $P_n = L_n = K^n$. Możemy więc przyjąć, że $P_{D,\alpha,n}$ oraz $L_{D,\alpha,n}$ są bijektywnymi operatorami modułu wolnego K^n.

Jako pierwszy wierzchołek weźmy punkt zdefiniowany jak powyżej, ale z ustaloną pierwszą współrzędną:

$(p) = (c_1, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i})\big|_n,$

wtedy dla kolejnych elementów $\alpha_1, \alpha_2, \ldots, \alpha_s$ ($\alpha_i \in K$, dla $i = 1, 2, \ldots, s$), (tzn. w każdym kolejnym kroku i, $i = 1, 2, \ldots, s$) wykonujemy następujące czynności:

1. Współrzędne kolejnych wierzchołków o indeksach $1, (1,1), (1,2), (2,1), (2,2), (2,2)', (2,3), \ldots, (i,i)$ wyznaczamy, używając operatorów $P_{D,\alpha,n}$ lub $L_{D,\alpha,n}$, według następującej zasady:

   $(p)^{(0)} \longrightarrow [l]^{(1)} = P_{D,\alpha_1,n}((p)^{(0)}) \longrightarrow (p)^{(2)} = L_{D,\alpha_2,n}([l]^{(1)}) \longrightarrow \ldots \longrightarrow [l]^{(s)} = P_{D,\alpha_s,n}((p)^{(s-1)}) \longrightarrow (p)^{(s+1)} = L_{D,\alpha_{s+1},n}([l]^{(s)})$.

2. Ostatnią współrzędna z indeksem $\lfloor n + 2/4 \rfloor$ (współrzędną z indeksem $(i,i)'$), obliczamy korzystając z równania kwadratowego opisującego spójne składowego grafu $D(n, K)$ $a_r = a_r(u) = \sum_{i=0}^{r}(u_{ii}u'_{r-i,r-i} - u_{i,i+1}u_{r-i,r-i-1}) = 0$. Otrzymujemy w ten sposób:

   $l'_{ss} = \sum_{i=0}^{s-2}(l_{ii}l'_{s-i,s-i} - l_{i,i+1}l_{s-i,s-i-1}) + l_{s-1,s-1}l_{11} - l_{s-1,s}l_1 + l_{ss}$, lub

   $p'_{ss} = \sum_{i=0}^{s-2}(p_{ii}p'_{s-i,s-i} - p_{i,i+1}p_{s-i,s-i-1}) + p_{s-1,s-1}p_{11} - p_{s,s-1}p_1 + p_{ss}$,

   odpowiednio.

3. Ostatnie dwie współrzędne $p_{i,i+1}, p_{i+1,i}$, w każdym kroku, są policzone z udziałem operatorów $P_{D,\alpha,n}$ oraz $L_{D,\alpha,n}$.

Z racji tego, że pierwsza współrzędna pierwszego wierzchołka została ustalona, operotory $P_{D,\alpha,n}$ i $L_{D,\alpha,n}$ grafu K^n sprawiają, że współrzędne ostatniego wierzchołka $c_1, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}$ są odwzorowaniami liniowymi (w dowodzie twierdzenia 4.1 jednomiany stopnia trzeciego mają postać $p_1^2 p_i$). Ostatnia współrzędna $p'_{i,i}$, będąca odwzorowaniem kwadratowym, zostaje usunięta. Powstałe w ten sposób dwie ostatnie współrzędne $p_{i,i+1}$ i $p_{i+1,i}$ są również odwzorowaniami kwadratowymi.

Otrzymujemy zatem złożenie operatorów $P_{D,\alpha_1,n} L_{D,\alpha_2,n} D_{D,\alpha_3,n} L_{D,\alpha_4,n} \cdots D_{D,\alpha_l,n} L_{D,\alpha_{l+1},n}$ wraz z powyższymi modyfikacjami na ostatnich współrzędnych. W ten sposób powstaje przekształcenie f, które przekształca wierzchołek początkowy na końcowy. Wymiar przestrzeni jest równy $n-2$, gdyż pierwsza współrzędna jest ustalona zaś ostatnia zmienna o indeksie $(i,i)'$ - usunięta.

Niech f^k oznacza k-krotne złożenie ze sobą funkcji f w grupie wszystkich wielomianowych automorfizmów modułu wolnego K^{n-2}. Otrzymujemy zatem następujące twierdzenie:

Twierdzenie 4.11. *[64] Zbiór przekształceń typu $f^k \colon K^{n-2} \to K^{n-2}$, niezależnie od wartości k tworzy grupę stabilnych przekształceń wielomianowych drugiego stopnia oraz rosnącego rzędu.*

Rozdział 5

Rodziny stabilnych odwzorowań wielomianowych wyższych stopni

W celu zwiększenia poziomu bezpieczeństwa algorytmów kryptograficznych, bazujących na przekształceniach wielomianowych, skonstruowane zostały nowe rodziny odwzorowań bazujących na dwudzielnych grafach algebraicznych. Konstrukcja ta może mieć zastosowanie w szyfrach strumieniowych, algorytmie klucza publicznego oraz protokołach wymiany klucza ([65, 66, 68]). Nieobecność krawędziowo tranzytywnej grupy elementów stabilnych z odwracalnym rozkładem znacząco komplikuje kryptanalizę. Przedstawimy poniżej konstrukcje odwzorowań stabilnych określonego stopnia c dla każdego pierścienia przemiennego K zawierającego co najmniej 3 elementy. Pierwsza z nich opiera się na technice kompresji rozpatrywanego grafu $D(n, K)$, która pozwala wyeliminować niektóre zmienne (poprzez zmniejszenie liczby spójnych składowych grafu) oraz znacząco zwiększyć stopień odwzorowania wielomianowego. Utworzona rodzina stabilnych odwzorowań wielomianowych, spełniając niezbędne kryteria, tworzy lingwistyczny układ dynamiczny. Druga konstrukcja również umożliwia otrzymanie odwzorowań o określonym zwiększonym stopniu, przy jednoczesnym zachowaniu odpowiedniej gęstości powstałych odwzorowań wielomianowych.

Konstrukcja rodziny odwzorowań stabilnych o stałym stopniu większym od czterech jest bardzo interesującym zadaniem, biorąc pod uwagę istnienie odwzorowań o odwracalnym rozkładzie. Większy stopień stabilnych przekształceń szyfrujących odpowiada za lepszą odporność na ataki linearyzacji. W przypadku rodzin stabilnych o odpowiednio dużym

stopniu ataki linearyzacji są praktycznie niewykonalne. Jednak w celu tworzenia efektywnych reguł publicznych potrzebujemy warunku wielomianowej gęstości. Przedstawmy zatem definicje pojęcia odwracalnego rozkładu oraz wielomianowej gęstości.

Niech $f = f_n$ będzie zapisana w formie $x_i \to f_i(x_1, x_2, \ldots, x_n)$, gdzie $i = 1, 2, \ldots, n$.

Definicja 5.1. Mówimy, że ciąg $f_n \in C(K^n)$ tworzy rodzinę odwzorowań o wielomianowej gęstości d, jeżeli ogólna ilość wszystkich wyrażeń jednomianowych we wszystkich f_i, $i = 1, 2, \ldots, n$, może być dana jako $\mathcal{O}(n^d)$ dla pewnej niezależnej stałej d. Jeżeli f_n jest rodziną odwzorowań wielomianowych stopnia s z wielomianową gęstością d, wtedy wartość f_n w punkcie $x \in K^n$ może być policzona w ilości $\mathcal{O}(n^{s+d})$ elementarnych kroków.

Definicja 5.2. Mówimy, że ciąg $f_n \in C(K^n)$ ma odwracalny rozkład o prędkości d, jeżeli f_n może być zapisane jako złożenia elementów $f^1(n), f^2(n), \ldots, f^{k(n)}(n)$ oraz ten rozkład pozwala na policzenie wartości $y = f(x)$ oraz przeciwobrazu dla danego y w czasie $k(n)\mathcal{O}(n^d)$.

5.1 Rodzina odwzorowań stabilnych powstałych przez kompresję grafu $D(n, K)$

W tym rozdziale przedstawimy rodzinę odwzorowań stabilnych utworzoną poprzez zabieg kompresji grafu $D(n, K)$. Procedura ta znacznie zwiększa stopień odwzorowania, powodując lepszą odporność na ataki linearyzacji kryptosystemów na nich opartych.

5.1.1 Wprowadzenie

Niech $J = j_1, j_2, \ldots, j_s$, gdzie $2 \le j_1 \le j_2, \ldots, j_s \le [(n+2)/4]$. Niech $T = T_n(K, J, b_1, b_2, \ldots, b_s)$ będzie podzbiorem wszystkich wierzchołków v grafu $D(n, K)$ spełniającego warunki $a_{j_1}(v) = b_i$, $i = 1, 2, \ldots, s$. Jest on rozłączną sumą kilku spójnych składowych grafu. Niech $CD_J(n, K)$ będzie grafem ograniczonym do relacji incydencji na podzbiorze T.

Definiujemy graf skompresowany $CD'_J(n, K)$ grafu $CD_J(n, K)$ ze zbiorem punktów

$$(p) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p_{23}, \ldots, p_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots)\big|_n,$$

oraz prostych

$$[l] = [l_1, l_{11}, l_{12}, l_{21}, l_{22}, l_{23}, \ldots, l_{ii}, l_{i,i+1}, l_{i+1,i}, \ldots]\big|_n,$$

z pominięciem współrzędnych p'_{ii} oraz l'_{ii}, $i \in J$. Relacja incydencji I' jest zdefiniowana przez relacje (3.1) bez równań $l'_{ii} - p'_{ii} = l_{i,i-1}p_1$, $i \in J$.

Wyrażenia l'_{ii} (p'_{ii}), $i \in J$ w pozostałych równaniach zastąpione są przez równania kwadratowe opisujące spójne składowe grafu $D(n, K)$:

$$a'_i(\mathrm{l}) = b_i - (-1)^e l'_{ii} \ (a'_i(\mathrm{p}) = b_i - (-1)^e p'_{ii}),$$

gdzie $e = 0$ jeżeli parametry l_{ii} (p'_{ii}) pojawiają się jako składniki sumy $a_i(\mathrm{l})$ ($a_i(\mathrm{p})$), odpowiednio) ze współczynnikami $+1$ i $e = 1$ w przeciwnym przypadku (współczynnik jest równy -1).

Bezpośrednio z definicji wynika, że graf $CD_J(n, K)$ jest strukturą incydencji (P', L', I'), gdzie rozmaitości P' i L' są izomorficzne z $K^{n-|J|}$. Procedura kompresji Δ_J jest izomorfizmem grafu $CD_J(n, K)$ na $CD'_J(n, K) = \Delta_j(CD_J(n, K))$. W maksymalnym możliwym przypadku $J = \{2, 3, \ldots, t(n)\}$ piszemy $CD(n, K)$ i $CD'(n, K)$ oraz używamy notacji Δ zamiast Δ_J.

Niech $\mathrm{p} = (p_{1,0}, p_{11}, \ldots)\big|_n$ i $\mathrm{l} = [l_{0,1}, l_{1,1}, \ldots]\big|_n$ będą punktem i prostą jednego z grafów $D(K), CD(K), CD_J(n, K), D(n, K), CD(n, K)$. Pierwsze współrzędne $\rho(\mathrm{p}) = p_{1,0}$ i $\rho(\mathrm{l}) = l_{0,1}$ odpowiadają kolorom punktu i linii, odpowiednio. Kolorowanie ρ, dane powyżej, spełnia własność *równoległości* (patrz [69] lub [70]), tzn. dla każdego wierzchołka grafu istnieje jeden sąsiad wybranego koloru. Można zauważyć również, że Δ_J zachowuje kolor homomorfizmu grafu, tzn. $\rho(v) = \rho(\Delta_J(v))$.

5.1.2 Konstrukcja rodziny odwzorowań wielomianowych wyższych stopni

Jednym z głównych wyników tego rozdziału jest znalezienie rodziny odwzorowań wielomianowych, których stopnie rosną liniowo wraz ze wzrostem n. Wprowadzona modyfikacja, poprzez zabieg kompresji, pozwala na zmniejszenie liczby zmiennych.

Rozważmy na początek pełną kompresję Δ maksymalnym możliwym przypadku $J = \{2, 3, \ldots, t(n)\}$. Zdefiniujmy zatem operatory sąsiedztwa dla punktów i prostych w spójnej składowej $CD(n, K)$. Niech L_{β_k}, $\beta_k \in K$ będzie operatorem wybrania sąsiada dla punktu:

$$(p)^{2k-2} = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots)\big|_n,$$

postaci

$$[l]^{2k-1} = [\beta_k, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots]\big|_n,$$

gdzie parametry $l_{1,1}, l_{1,2}, l_{1,2}, l_{2,2}, \ldots, l_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots$ są wyznaczone kolejno z równań definiujących graf $D(n,K)$, zaś wszystkie $l'_{i,i}$ dla $i = 2,3,\ldots$ wyznaczone są z użyciem równań opisujących spójne składowe tego grafu (3.4) .

Podobnie, niech P_{α_k}, $\alpha_k \in K$ będzie operatorem wybrania sąsiada dla prostej

$$[l]^{2k-1} = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, \ldots, l_{i,i}, l_{i,i+1}, l'_{i,i}, l_{i+1,i}, \ldots]\big|_n,$$

postaci

$$(p)^{2k} = (p_{0,1}^{2k-2} + \alpha_k, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots)\big|_n,$$

gdzie parametry $p_{1,1}$, $p_{1,2}$, $p_{2,1}$, $p_{2,2}$,..., $p_{i,i}$, $p_{i,i+1}$, $p_{i+1,i}$, ... są wyznaczone kolejno z równań definiujących graf $D(n,K)$, zaś wszystkie $p'_{i,i}$ dla $i = 2,3,\ldots$ wyznaczone są z użyciem równań opisujących spójne składowe tego grafu (3.4) .

Mając dany wektor

$$(p)^0 = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots)\big|_n,$$

(długości n) oraz elementy $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ i $\beta = (\beta_1, \beta_2, \ldots, \beta_k)$ z K^k definiujemy złożenie odwzorowań:

$$F_{\alpha,\beta} = L_{\beta_1} P_{\alpha_1} L_{\beta_2} P_{\alpha_2} \ldots L_{\beta_k} P_{\alpha_k}.$$

Dla większej przejrzystości konstrukcji przejdziemy teraz na pojedyncze indeksowanie punktów i prostych należących do grafu $D(n,K)$. Niech wektor początkowy (punkt) $(p)^0$ będzie postaci $(p)^0 = (p_1, p_2, p_3, \ldots, p_n)$. Korzystając z operatorów sąsiedztwa zdefiniowanych powyżej, możemy wypisać kilka kolejnych punktów i prostych (obciętych do żądanej długości n):

$$\begin{aligned}
[l]^1 &= L_{\beta_1}((p)^0) = [\beta_1, l_2^1, \ldots, l_{4t+1}^1, l_{4t+2}^1, l_{4t+3}^1, l_{4t+4}^1, \ldots]\big|_n,\\
(p)^2 &= P_{\alpha_1}([l]^1) = (p_1 + \alpha_1, p_2^2, \ldots, p_{4t+1}^2, p_{4t+2}^2, p_{4t+3}^2, p_{4t+4}^2, \ldots)\big|_n,\\
[l]^3 &= L_{\beta_2}((p)^2) = [\beta_2, l_2^3, \ldots, l_{4t+1}^3, l_{4t+2}^3, l_{4t+3}^3, l_{4t+4}^3, \ldots]\big|_n,\\
(p)^4 &= P_{\alpha_2}([l]^3) = (p_1 + \alpha_1 + \alpha_2, p_2^4, \ldots, p_{4t+1}^4, p_{4t+2}^4, p_{4t+3}^4, p_{4t+4}^4, \ldots)\big|_n,\\
&\vdots\\
[l]^{2k-1} &= L_{\beta_k}((p)^{2k-2}) = [\beta_k, l_2^{2k-1}, \ldots, l_{4t+1}^{2k-1}, l_{4t+2}^{2k-1}, l_{4t+3}^{2k-1}, l_{4t+4}^{2k-1}, \ldots]\big|_n,
\end{aligned}$$

$$(p)^{2k} = P_{\alpha_k}([l]^{2k-1}) = (p_1 + \alpha_1 + \cdots + \alpha_k, p_2^{2k}, \ldots, p_{4t+1}^{2k}, p_{4t+2}^{2k}, p_{4t+3}^{2k}, p_{4t+4}^{2k}, \ldots)\big|_n.$$

Niech $1 \leq t \leq \lfloor \frac{n+2}{4} \rfloor$ oraz $1 \leq i \leq 2k$. Wszystkie współczynniki $p_2^i, \ldots, p_{4t+1}^i, p_{4t+3}^i, p_{4t+4}^i$ oraz $l_2^i, \ldots, l_{4t+1}^i, l_{4t+3}^i, l_{4t+4}^i$ wyznaczone są z równań definiujących graf $D(n, K)$ (3.1). Współczynniki p_{4t+2}^i oraz l_{4t+2}^i (odpowiadające $p'_{i,i}$ oraz $l'_{i,i}$) obliczamy z równań kwadratowych $a_i(u) = b_i$ (dla uproszczenia bierzemy $b_i = 0$) opisujących spójne składowe grafu $D(n, K)$ (3.4) zapisanych w postaci (u oznacza dowolny wierzchołek p lub l):

$$u_{4t+2} = u_2 u_{4t-2} - u_3 u_{4t-4} + \sum_{i=1}^{t-2} (u_{4i+1} u_{4(t-i)-2} - u_{4i+3} u_{4(t-i)-4}) + u_{4t-3} u_2 - u_{4t-1} u_1 + u_{4t+1}.$$

Otrzymujemy w ten sposób w kolejnych krokach $1 \leq i \leq 2k$ odwzorowania wielomianowe l_n^i oraz p_n^i w zależności od n zmiennych $(p_1, p_2, p_3, \ldots, p_n)$ o następujących stopniach:

$$\deg l_n^i = \begin{cases} 1 & \text{dla } n = 1 \mod 4 \\ \frac{n+2}{4} & \text{dla } n = 2 \mod 4 \\ 2 & \text{dla } n = 3 \mod 4 \\ \frac{n}{4} & \text{dla } n = 0 \mod 4 \end{cases}$$

$$\deg p_n^i = \begin{cases} 1 & \text{dla } n = 1 \mod 4 \\ \frac{n+2}{4} & \text{dla } n = 2 \mod 4 \\ 1 & \text{dla } n = 3 \mod 4 \\ \frac{n+2}{4} & \text{dla } n = 0 \mod 4 \end{cases}$$

Procedura kompresji Δ w maksymalnym możliwym przypadku polega na wyeliminowaniu współczynników p_{4t+2}^i oraz l_{4t+2}^i (tzw. „z primem"), zmniejszając wymiar przestrzeni do $K^{n-\lfloor \frac{n+2}{4} \rfloor}$ Otrzymujemy zatem ograniczenie F' odwzorowania $F_{\alpha,\beta}$ na graf $CD'(n, K)$ zawierający wszystkie wierzchołki v, takie, że $a_2(v) = b_1, a_3(v) = b_2, \ldots$.

Otrzymujemy zatem następujące twierdzenie:

Twierdzenie 5.1. *([65, 66]) Niech $F' = F'_{\alpha,\beta}$ będzie zdefiniowanym powyżej odwzorowaniem modułu wolnego $K^{n-\lfloor \frac{n+2}{4} \rfloor}$ grafu $CD'(n, K)$. Niezależnie od wyboru $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in (\mathrm{Reg}(K))^k$ i $\beta = (\beta_1, \beta_2, \ldots, \beta_k) \in (\mathrm{Reg}(K))^k$ takich, że $\beta_{i+1} - \beta_i \in \mathrm{Reg}(K)$:*

1. *odwzorowanie F' jest bijekcją o stopniu $\left\lfloor \frac{n+2}{4} \right\rfloor$.*

2. *rząd odwzorowania F' wzrasta do nieskończoności wraz ze wzrostem n.*

Rozważmy teraz kompresję Δ_J, czyli ograniczenie F'_J odwzorowania F na graf $CD_J(n,K)$, $J = \{j_1, j_2, \ldots, j_s\}$, $2 \leq j_1 \leq j_2 \leq \ldots j_s \leq t(n)$. $F'_{J\alpha,\beta}$ przekształca zbior punktów K^{n-J} w K^{n-J} w grafie $CD'_J(n,K)$. Ta metoda kompresji pozwala nam na wyeliminowanie tylko wybranych zmiennych p^i_{4t+2} oraz l^i_{4t+2}, zmniejszając stopień odwzorowania. Oznacza to, że w zależności od wyboru zbioru J, możemy otrzymać odpowiedni stopień odwzorowania.

Przypomnijmy, że zbiór Q jest zbiorem multiplikatywnym pierścienia przemiennego K, jeżeli jest domknięty względem operacji mnożenia ($x, y \in Q \Rightarrow x \cdot y \in Q$) i nie zawiera 0.

Następujące twierdzenie wynika bezpośrednio z rezultatów uzyskanych w [57], [59].

Twierdzenie 5.2. *Niech Q będzie zbiorem multiplikatywnym pierścienia K. Dla każdego $\alpha_i \in Q$, $i \in Q$ i $\beta_i - \beta_{i+1} \in Q$, $i = 1, 2, \ldots, k-1$ oraz $\beta_1 - \beta_k \in Q$. Wtedy rząd odwzorowania $F'_{J_{n,\alpha,\beta}}$ dąży do ∞, gdy $n \to \infty$ dla dowolnego J.*

Następujące twierdzenia zostało przedstawione w [65] (oraz udowodnione w [66]).

Twierdzenie 5.3. *Niech $F'_J(n,K)$ odpowiada ciągom α_1,α_2,...,α_k i β_1,β_2,...,β_k, gdzie k jest niezależną stałą. Załóżmy, że to odwzorowanie jest zapisane w standardowej formie $x_i \to F_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$. Wtedy gęstość każdego odwzorowania wielomianowego F_i wynosi $O(n^3)$. Wynika stąd, że odwzorowanie $F'_J(n,K)$ dla $|J| \geq cn$, gdzie c jest niezależną stałą, tworzy rodzinę odwzorowań stabilnych o rosnącym stopniu, nieograniczonym rzędzie, posiadającą własność odwracalnego rozkładu oraz wielomianowej gęstości.*

5.2 Rodzina odwzorowań wielomianowych z nieliniowym zaburzeniem

W tym rozdziale przedstawimy rodzinę odwzorowań wielomianowych powstałych poprzez ścieżkę w grafie $D(n,K)$ z użyciem nieliniowej, wzajemnie jednoznacznej funkcji podczas zmiany koloru wierzchołka. Tak powstała rodzina odwzorowań tworzy lingwistyczny układ dynamiczny z nieliniowym zaburzeniem, zdefiniowany w rozdziale 3.6.

Podobnie jak w poprzednim rozdziale zastosujemy pojedyncze indeksowanie punktów i prostych należących do grafu $D(n,K)$. Niech wektor początkowy (punkt) $(p)^0$ będzie

postaci $(p)^0 = (p_1, p_2, p_3, \ldots, p_n)$. Niech $h(x)$ będzie wielomianem nieliniowym, zależnym od pierwszej współrzędnej. Wypiszmy zatem ścieżkę w grafie $D(n, K)$ składającą się z kolejnych punktów i prostych (obciętych do żądanej długości n) z zastosowaniem nieliniowego zaburzenia na pierwszej współrzędnej. Zaburzenie h jest wzajemnie jednoznacznym odwzorowaniem wielomianowym zmiennej p_1.

$$
\begin{aligned}
[l]^1 &= [h(p_1) + \alpha_1, l_2^1, \ldots, l_{4t+1}^1, l_{4t+2}^1, l_{4t+3}^1, l_{4t+4}^1, \ldots]\big|_n \\
(p)^2 &= (p_1 + \alpha_2, p_2^2, \ldots, p_{4t+1}^2, p_{4t+2}^2, p_{4t+3}^2, p_{4t+4}^2, \ldots)\big|_n \\
[l]^3 &= [h(p_1) + \alpha_1 + \alpha_3, l_2^3, \ldots, l_{4t+1}^3, l_{4t+2}^3, l_{4t+3}^3, l_{4t+4}^3, \ldots]\big|_n \\
(p)^4 &= (p_1 + \alpha_2 + \alpha_4, p_2^4, \ldots, p_{4t+1}^4, p_{4t+2}^4, p_{4t+3}^4, p_{4t+4}^4, \ldots)\big|_n \\
&\ldots \\
[l]^{2k-1} &= [h(p_1) + \alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1}, l_2^{2k-1}, \ldots, l_{4t+1}^{2k-1}, l_{4t+2}^{2k-1}, l_{4t+3}^{2k-1}, l_{4t+4}^{2k-1}, \ldots]\big|_n \\
(p)^{2k} &= (p_1 + \alpha_2 + \alpha_4 + \cdots + \alpha_{2k}, p_2^{2k}, \ldots, p_{4t+1}^{2k}, p_{4t+2}^{2k}, p_{4t+3}^{2k}, p_{4t+4}^{2k}, \ldots)\big|_n
\end{aligned}
$$

Dla $1 \leq i \leq 2k$, wszystkie współczynniki $p_2^i, \ldots, p_{4t+1}^i, p_{4t+2}^i, p_{4t+3}^i, p_{4t+4}^i$ oraz $l_2^i, \ldots, l_{4t+1}^i, l_{4t+2}^i, l_{4t+3}^i, l_{4t+4}^i$ wyznaczone są z równań definiujących graf $D(n, K)$ (3.1).

Niech $\alpha = (\alpha_1, \alpha_2, \ldots \alpha_s)$ oraz $H = H(n, \alpha, h(x), K)$ będzie odwzorowaniem, które przekształca punkt startowy na punkt końcowy, korzystając ze ścieżki w grafie z zastosowaniem nieliniowego zaburzenia $h(x)$. Możemy rozpatrzyć dwa przypadki ostatniego wierzchołka, który może być punktem lub prostą. W przypadku ścieżki nieparzystej długości $s = 2k - 1$ otrzymujemy prostą, zaś w przypadku parzystej długości $s = 2k$ - punkt.

Twierdzenie 5.4. *Otrzymane w powyższy sposób odwzorowanie $H = H(n, \alpha, f, K)$ jest odwzorowaniem wielomianowym, zależnym od zmiennych tworzących pierwszy wierzchołek, o następujących stopniach:*

$$
\deg H = \begin{cases} \deg h + 2 & dla\ s = 2k - 1 \\ 2 \deg h + 1 & dla\ s = 2k \end{cases}
$$

Dowód. W celu udowodnienia powyższego twierdzenia, zastosujemy zasadę indukcji matematycznej w zależności od długości ścieżki w grafie s. Na początku zbadamy stopnie wielomianów powstałych w dwóch początkowych krokach algorytmu z zaburzeniem pierwszej współrzędnej (zdefiniowanego na początku tego rozdziału). Załóżmy, że wierzchołek początkowy będzie punktem postaci $(p)^0 = (p_1, p_2, p_3, \ldots, p_n)$. Kolejnym wierzchołkiem

będzie prosta $[l]^1$, gdzie $l_1^1 = h(p_1) + \alpha_1$:

$$[l]^1 = [h(p_1) + \alpha_1, l_2^1, \dots, l_{4t+1}^1, l_{4t+2}^1, l_{4t+3}^1, l_{4t+4}^1, \dots]$$

Wyznaczmy zatem współczynniki tej prostej w zależności od zmiennych $p_1, p_2, p_3, \dots, p_n$:

$$\begin{aligned}
l_2^1 &= p_2 + l_1^1 p_1 = p_2 + (h(p_1) + \alpha_1)p_1 \\
l_3^1 &= p_3 + l_2^1 p_1 = p_3 + [p_2 + (h(p_1) + \alpha_1)p_1]p_1 \\
l_4^1 &= p_4 + l_1^1 p_2 = p_4 + (h(p_1) + \alpha_1)p_2 \\
l_5^1 &= p_5 + l_1^1 p_3 = p_5 + (h(p_1) + \alpha_1)p_3 \\
l_6^1 &= p_6 + l_4^1 p_1 = p_6 + [p_4 + (h(p_1) + \alpha_1)p_2]p_1 \\
l_7^1 &= p_7 + l_5^1 p_1 = p_7 + [p_5 + (h(p_1) + \alpha_1)p_3]p_1 \\
&\dots \\
l_{4t}^1 &= p_{4t} + l_1^1 p_{4t-2} = p_{4t} + (h(p_1) + \alpha_1)p_{4t-2} \\
l_{4t+1}^1 &= p_{4t+1} + l_1^1 p_{4t-1} = p_{4t+1} + (h(p_1) + \alpha_1)p_{4t-1} \\
l_{4t+2}^1 &= p_{4t+2} + l_{4t}^1 p_1 = p_{4t+2} + [p_{4t} + (h(p_1) + \alpha_1)p_{4t-2}]p_1 \\
l_{4t+3}^1 &= p_{4t+3} + l_{4t+1}^1 p_1 = p_{4t+3} + [p_{4t+1} + (h(p_1) + \alpha_1)p_{4t-1}]p_1
\end{aligned}$$

Otrzymujemy zatem następujące stopnie współczynników:

$$\deg l_n^1 = \begin{cases} \deg h + 1 & \text{dla } n = 1 \mod 4 \\ \deg h + 2 & \text{dla } n = 2 \mod 4 \\ \deg h + 2 & \text{dla } n = 3 \mod 4 \\ \deg h + 1 & \text{dla } n = 0 \mod 4 \end{cases}$$

Kolejnym wierzchołkiem będzie punkt $(p)^2$, gdzie $p_1^2 = p_1 + \alpha_2$:

$$(p)^2 = (p_1 + \alpha_2, p_2^2, \dots, p_{4t+1}^2, p_{4t+2}^2, p_{4t+3}^2, p_{4t+4}^2, \dots)$$

o współczynnikach postaci:

$$p_2^2 = l_2^1 - l_1^1 p_1^2 = p_2 - \alpha_2(h(p_1) + \alpha_1)$$

$$
\begin{aligned}
p_3^2 &= l_3^1 - l_2^1 p_1^2 = p_3 - \alpha_2(p_2 + (h(p_1) + \alpha_1)p_1) \\
p_4^2 &= l_4^1 - l_1^1 p_2^2 = p_4 + \alpha_2(h(p_1) + \alpha_1)^2 \\
p_5^2 &= l_5^1 - l_1^1 p_3^2 = p_5 + \alpha_2(h(p_1) + \alpha_1)[p_2 + (h(p_1) + \alpha_1)p_1] \\
p_6^2 &= l_6^1 - l_4^1 p_1^2 = p_6 - \alpha_2[p_4 + (h(p_1) + \alpha_1)p_2] \\
p_7^2 &= l_7^1 - l_5^1 p_1^2 = p_7 - \alpha_2[p_5 + (h(p_1) + \alpha_1)p_3] \\
&\dots \\
p_{4t}^2 &= l_{4t}^1 - l_1^1 p_{4t-2}^2 = p_{4t} + \alpha_2(h(p_1) + \alpha_1)p_{4t-4} + \alpha_2(h(p_1) + \alpha_1)^2 p_{4t-6} \\
p_{4t+1}^2 &= l_{4t+1}^1 - l_1^1 p_{4t-1}^2 = p_{4t+1} + \alpha_2(h(p_1) + \alpha_1)p_{4t-3} + \alpha_2(h(p_1) + \alpha_1)^2 p_{4t-5} \\
p_{4t+2}^2 &= l_{4t+2}^1 - l_{4t}^1 p_1^2 = p_{4t+2} - \alpha_2[p_{4t} + (h(p_1) + \alpha_1)p_{4t-2}] \\
p_{4t+3}^2 &= l_{4t+3}^1 - l_{4t+1}^1 p_1^2 = p_{4t+3} - \alpha_2[p_{4t+1} + (h(p_1) + \alpha_1)p_{4t-1}]
\end{aligned}
$$

Otrzymaliśmy zatem współrzędne wierzchołka p^2 o następujących stopniach:

$$
\deg p_n^2 = \begin{cases}
2\deg h + 1 & \text{dla } n = 1 \mod 4 \\
\deg h + 1 & \text{dla } n = 2 \mod 4 \\
\deg h + 1 & \text{dla } n = 3 \mod 4 \\
2\deg h + 1 & \text{dla } n = 0 \mod 4
\end{cases}
$$

Na podstawie dwóch powyższych kroków, możemy założyć, że w dla $1 \leq i \leq 2k-2$ współrzędne kolejnych punktach i prostych, czyli odwzorowania wielomianowe l_n^i oraz p_n^i w zależności od n zmiennych $(p_1, p_2, p_3, \dots, p_n)$ mają następujące stopnie:

$$
\deg l_n^i = \begin{cases}
\deg h + 1 & \text{dla } n = 1 \mod 4 \\
\deg h + 2 & \text{dla } n = 2 \mod 4 \\
\deg h + 2 & \text{dla } n = 3 \mod 4 \\
\deg h + 1 & \text{dla } n = 0 \mod 4
\end{cases}
$$

$$
\deg p_n^i = \begin{cases}
2\deg h + 1 & \text{dla } n = 1 \mod 4 \\
\deg h + 1 & \text{dla } n = 2 \mod 4 \\
\deg h + 1 & \text{dla } n = 3 \mod 4 \\
2\deg h + 1 & \text{dla } n = 0 \mod 4
\end{cases}
$$

Aby udowodnić tezę rozważanego twierdzenia zbadamy stopnie wierzchołków l^{2k-1} oraz p^{2k} (dla długości ścieżki odpowiednio $s = 2k-1$ oraz $s = 2k$). Pominięte zostaną obliczenia stopni kilku początkowych współrzędnych oraz szczegóły pośrednich obliczeń w poszczególnych współrzędnych.

Wierzchołek l^{2k-1} o pierwszej współrzędnej $l_1^{2k-1} = h(p_1)+\alpha_1+\alpha_3+\cdots+\alpha_{2k-1}$ posiada współrzędne następującej postaci:

$$\begin{aligned}
l_{4t}^{2k-1} &= p_{4t}^{2k-2} + l_1^{2k-1}p_{4t-2}^{2k-2} = l_{4t}^{2k-3} + \alpha_{2k-1}p_{4t-2}^{2k-2}\\
l_{4t+1}^{2k-1} &= p_{4t+1}^{2k-2} + l_1^{2k-1}p_{4t-1}^{2k-2} = l_{4t+1}^{2k-3} + \alpha_{2k-1}p_{4t-1}^{2k-2}\\
l_{4t+2}^{2k-1} &= p_{4t+2}^{2k-2} + l_{4t}^{2k-1}p_1^{2k-2} = l_{4t+2}^{2k-3} + \alpha_{2k-1}p_{4t-2}^{2k-2}p_1^{2k-2}\\
l_{4t+3}^{2k-1} &= p_{4t+3}^{2k-2} + l_{4t+1}^{2k-1}p_1^{2k-2} = l_{4t+3}^{2k-3} + \alpha_{2k-1}p_{4t-1}^{2k-2}p_1^{2k-2}
\end{aligned}$$

Wierzchołek p^{2k} o pierwszej współrzędnej $p_1^{2k} = p_1 + \alpha_2 + \alpha_4 + \cdots + \alpha_{2k}$ posiada współrzędne następującej postaci:

$$\begin{aligned}
p_{4t}^{2k} &= l_{4t}^{2k-1} - l_1^{2k-1}p_{4t-2}^{2k} = l_{4t}^{2k-3} - l_1^{2k-3}p_{4t-2}^{2k-2} + \alpha_{2k}l_1^{2k-3}l_{4t-4}^{2k-1} + \alpha_{2k-1}\alpha_{2k}l_{4t-4}^{2k-1}\\
p_{4t+1}^{2k} &= l_{4t+1}^{2k-1} - l_1^{2k-1}p_{4t-1}^{2k} = l_{4t+1}^{2k-3} - l_1^{2k-3}p_{4t-1}^{2k-2} + \alpha_{2k}l_1^{2k-3}l_{4t-3}^{2k-1} + \alpha_{2k-1}\alpha_{2k}l_{4t-3}^{2k-1}\\
p_{4t+2}^{2k} &= l_{4t+2}^{2k-1} - l_{4t}^{2k-1}p_1^{2k} = p_{4t+2}^{2k-2} - \alpha_{2k}l_{4t}^{2k-1}\\
p_{4t+3}^{2k} &= l_{4t+3}^{2k-1} - l_{4t+1}^{2k-1}p_1^{2k} = p_{4t+3}^{2k-2} - \alpha_{2k}l_{4t+1}^{2k-1}
\end{aligned}$$

Udowodniliśmy zatem tezę twierdzenia, że dla każdego $1 \leq i \leq 2k$:

$$\deg l_n^i \leq \deg h + 2$$

oraz

$$\deg p_n^i \leq 2\deg h + 1.$$

□

Utworzona rodzina odwzorowań wielomianowych $H = H(n, \alpha, h(x), K)$ tworzy lingwistyczny układ dynamiczny z nieliniowym zaburzeniem, zdefiniowany w 3.6. Rodzina tych odwzorowań nie może być nazwana lingwistycznym układem dynamicznym (zdefiniowanym w 3.4), z racji braku operacji złożenia funkcji. W przypadku odwzorowań

rozpatrywanych w 4 oraz 5.1 operacja złożenia operatorów sąsiedztwa była jednoznaczna z przejściem odpowiedniej ścieżki w grafie. W tym rozdziale definiujemy ścieżkę w grafie, bez użycia operatorów sąsiedztwa. Mimo to powstałe odwzorowanie $H = H(n, \alpha, h(x), K)$, dla $\alpha = (\alpha_1, \alpha_2, \ldots \alpha_s)$ posiada bardzo dobre właściwości analogiczne do kryteriów lingwistycznego układu dynamicznego, takie jak:

- brak punktów stałych odwzorowania H,
- $H(n, \alpha, h(x), K) \neq H(n, \alpha', h(x), K)$ dla dwóch różnych ciągów α i α'.

Powyższe właściwości wynikają z własności grafu $D(n, K)$, w szczególności jego talii.

Rozdział 6

Zastosowanie odwzorowań wielomianowych w algorytmach kryptograficznych

W tym rozdziale przedstawimy możliwości zastosowania przekształceń wielomianowych, wygenerowanych dzięki użyciu lingwistycznych układów dynamicznych, w algorytmach kryptograficznych: algorytmach symetrycznych, asymetrycznych oraz protokole uzgodnienia klucza Diffiego-Hellmana. Rozpatrując algorytmy kryptograficzne oparte na zdefiniowanych wyżej lingwistycznych układach dynamicznych, zwrócimy szczególną uwagę na czynniki wpływające na ich bezpieczeństwo i efektywność. Takimi czynnikami są stopień odwzorowania, liczba jego jednomianów, rząd i gęstość odwzorowań wielomianowych powstałych w wyniku przejścia po ścieżce w grafie złożonych z odwzorowaniami afinicznymi. Różne rodzaje przekształceń mogą mieć wielorakie zastosowania: przekształcenia niskich stopni w kryptografii symetrycznej oraz wymianie klucza, zaś wyższych stopni w algorytmach asymetrycznych. Przedstawimy również przykłady oraz wyniki symulacji komputerowych.

6.1 Odwzorowania afiniczne w kryptografii

Podobnie jak w algorytmach kryptografii wielu zmiennych (rozdział 2.3), w celu ukrycia przekształcenia szyfrującego F użyjemy odwzorowań afinicznych (odpowiednio do równania (2.1)).

Według [2] przekształcenie T nazywa się afinicznym, jeśli można go przedstawić w postaci:

$$T\colon x \mapsto f(x) + b,$$

gdzie f jest pewnym przekształceniem liniowym, zaś b wektorem przesunięcia. Jeśli przestrzeń ma wymiar skończony, wtedy przekształcenie afiniczne (w naszym przypadku nad pierścieniem przemiennym K) $T\colon K^n \to K^n$ korzystnie jest przedstawić wzorem:

$$T\colon x \mapsto Ax + b,$$

gdzie A jest odwracalną macierzą wymiaru $n \times n$ nad K, zaś b n-elementowym wektorem nad K.

Po raz pierwszy pomysł ten został przedstawiony w pracy [71] w przypadku ciał:

Definicja 6.1. Niech F_p, gdzie p jest liczbą pierwszą, będzie ciałem skończonym. Afiniczne transformacje $\mathrm{x} \to A\mathrm{x} + b$, gdzie A jest macierzą nieodwracalną oraz $b \in F_p^n$ tworzą *grupę afiniczną* $AGL_n(F_p)$ działającą na ${F_p}^n$.

Afiniczne transformacje tworzą grupę afiniczną $AGL_n(F_p)$ rzędu $p^n(p^n - 1)(p^n - p)\dots(p^n - p^{n-1})$ w grupie symetrycznej S_{p^n} rzędu $p^n!$. W [40] została udowodniona maksymalność grupy $AGL_n(F_p)$ w S_{p^n}. Możemy więc reprezentować każdą permutację π jako złożenie kilku odwzorowań typu $T_1 g T_2$, gdzie $T_1, T_2 \in AGL_n(F_p)$ i g jest ustalonym odwzorowaniem stopnia ≥ 2.

6.2 Kryptografia symetryczna

W rozprawie rozpatrujemy w większości algorytmy kryptografii z kluczem publicznym, jednakże dla kompletności wywodu przedstawimy zastosowanie rodziny grafów o dużej talii $D(n, K)$ i operatora przejścia G_α w kryptografii symetrycznej. Po raz pierwszy rodzina grafów $D(n, K)$ została użyta w kryptografii z kluczem prywatnym przez Ustimenko w pracy [69], zaś implementacje zostały opisane w pracach [54, 58, 61, 74].

Rozważmy zatem dwudzielny graf $D(n, K)$, gdzie każdy wierzchołek grafu będzie reprezentował n-wymiarowy wektor o współrzędnych z pierścienia przemiennego K. Proces szyfrowania polega na wyznaczeniu ścieżki w grafie takiej długości jak długość hasła, gdzie kolejne odwiedzane wierzchołki przetwarzane są za pomocą operatora sąsiedztwa G_α opisanego w 3.2. Wierzchołek początkowy v_0 niech będzie tekstem jawnym, ostatni odwiedzony wierzchołek - szyfrogramem, zaś ciąg $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_s)$ – hasłem.

W celu poprawienia właściwości statystycznych można użyć dwóch odwracalnych przekształceń afinicznych T_1 i T_2, co w skrócie przedstawia schemat:

$$m \text{ (tekst jawny)} \longrightarrow v_0 = T_1(m) \longrightarrow v_1 = G_{\alpha_1}(v_0) \longrightarrow v_2 = G_{\alpha_2}(v_1) \longrightarrow \cdots$$

$$\cdots \longrightarrow v_s = G_{\alpha_s}(v_{s-1}) \longrightarrow T_2(v_s) = c \text{ (szyfrogram)}.$$

W tej sytuacji kluczem szyfrującym będzie trójka:

$$(T_1,\, (\alpha_1, \alpha_2 \ldots, \alpha_s),\, T_2).$$

Proces deszyfrowania polega na przejściu w grafie z użyciem operatów G_α w odwrotnym kierunku, czyli z hasłem $(-\alpha_s, \ldots, -\alpha_2, -\alpha_1)$. Razem z przekształceniami afinicznymi, klucz deszyfrujący jest następującej postaci:

$$(T_2^{-1},\, (-\alpha_s, \ldots, -\alpha_2, -\alpha_1),\, T_1^{-1}).$$

W pracy [55] zostało pokazane, że jeśli długość hasła $s < \frac{g(D(n,K))}{2} = \frac{n+5}{2}$ (długość drogi jest krótsza niż połowa talii grafu) oraz $\alpha_i + \alpha_{i+1} \in \mathrm{Reg}(K)$ dla $i = 1, 2, \ldots, s-1$ (nie ma możliwości cofania się podczas kolejno odwiedzanych wierzchołków), mamy spełnione dwa warunki poprawnego szyfrogramu:

1. tekst jawny jest zawsze różny od szyfrogramu,

2. dwa różne hasła użyte do jednego tekstu jawnego dają różne szyfrogramy.

W celu zwiększenia przestrzeni haseł zbiór $\mathrm{Reg}(K)$ może być wymieniony na dowolny zbiór multiplikatywny ([59]).

Przeanalizujmy złożoność czasową wykonania algorytmu symetrycznego (bez użycia transformacji afinicznych) dla tekstu jawnego długości n oraz hasła długości s. Stosując operator G_α w każdym kroku szyfrowania wykonujemy n dodawań i $n-1$ mnożeń. Zatem złożoność czasowa procesu szyfrowania, w przypadku hasła długości s, wynosi $\mathcal{O}(sn)$. Użycie przekształceń afinicznych zwiększa nam złożoność algorytmu do $\mathcal{O}(n^2)$, ze względu na mnożenie macierzy i dodanie wektora. Z uwagi na powyższy fakt przekształcenia afiniczne nie powinny być w zbyt ogólnej postaci. Kotorowicz w pracy [58] oraz Klisowski w [16] zastosowali w kryptosystemach symetrycznych transformacje afiniczne $T(x) = Ax + b$ oparte na macierzach tzw. „rzadkich" (takich, których większość elementów jest zerowa), np.:

typ 1 A - macierz kwadratowa nad pierścieniem K, która w każdym wierszu i w każdej kolumnie ma dokładnie jeden element odwracalny pierścienia K, b - wektor zerowy.

typ 2 A - macierz z jedynkami na przekątnej, elementami odwracalnymi w pierwszym wierszu i pozostałymi elementami zerowymi, b - wektor zerowy.

Takie przekształcenia (jak również przekształcenia do nich odwrotne) zmniejszają nam złożoność czasową i pamięciową do $\mathcal{O}(n)$.

W pracy [16] Klisowski przedstawił przykładowe czasy szyfrowania dla wybranych pierścieni, które potwierdzają liniową zależność od długości tekstu jawnego i długości hasła. Autor porównuje czasy szyfrowania dla różnych pierścieni, pokazując m.in. znaczne większą szybkość wykonania algorytmu symetrycznego w pierścieniu $\mathbb{Z}_{2^8}$ w porónaniu z ciałem $\mathbb{F}_{2^8}$. Kotorowicz w pracy [58] wykazał większą szybkość podstawowego algorytmu szyfrowania opartego na grafach $D(n, K)$ z algorytmami DES i RC4.

Przykład 6.1. Rozważmy przykład szyfrowania i deszyfrowania w algorytmie symetrycznym dla grafu $D(n, K) = D(6, Z_{2^7})$, gdzie tekst jawny, szyfrogram oraz kolejne wierzchołki pomiędzy nimi zostaną przedstawione jako wektory. Operacje arytmetyczne dokonywane są w pierścieniu $\mathbb{Z}_{2^7}$ (wyniki są resztami modulo 2^7). Niech przykładowym tekstem jawnym będzie $m = v_0 = (p^{(0)}) = (88, 92, 7, 17, 49, 65)$ (pierwszy wierzchołek), zaś hasłem $\alpha = (5, 43, 12, 23, 8)$. Szukany szyfrogram (ostatni wierzchołek) oznaczmy przez c.

Równania definiujące graf $D(6, K)$ mają postać:

$$\begin{aligned} l_2 - p_2 &= l_1 \cdot p_1 \\ l_3 - p_3 &= l_2 \cdot p_1 \\ l_4 - p_4 &= l_1 \cdot p_2 \\ l_5 - p_5 &= l_1 \cdot p_3 \\ l_6 - p_6 &= l_4 \cdot p_1. \end{aligned} \tag{6.1}$$

Kolejne kroki szyfrowania można zatem przedstawić w następującej postaci:

$$m = \begin{bmatrix} 88 \\ 92 \\ 7 \\ 17 \\ 49 \\ 65 \end{bmatrix} \longrightarrow \begin{bmatrix} 88+5 = 93 \\ 92+88\cdot 93 = 84 \\ 7+84\cdot 88 = 103 \\ 17+93\cdot 92 = 125 \\ 49+93\cdot 7 = 60 \\ 92+88\cdot 93 = 57 \end{bmatrix} \longrightarrow \begin{bmatrix} 93+43 = 8 \\ 84-8\cdot 93 = 108 \\ 103-84\cdot 8 = 71 \\ 125-93\cdot 108 = 65 \\ 60-93\cdot 71 = 113 \\ 57-125\cdot 8 = 81 \end{bmatrix} \longrightarrow$$

$$\longrightarrow \begin{bmatrix} 8+12 = 20 \\ 108+8\cdot 20 = 12 \\ 71+12\cdot 8 = 39 \\ 65+20\cdot 108 = 49 \\ 113+20\cdot 71 = 125 \\ 81+49\cdot 8 = 89 \end{bmatrix} \longrightarrow \begin{bmatrix} 20+23 = 43 \\ 12-20\cdot 43 = 48 \\ 39-12\cdot 43 = 35 \\ 49-20\cdot 48 = 113 \\ 125-20\cdot 35 = 65 \\ 89-49\cdot 43 = 30 \end{bmatrix} \longrightarrow \begin{bmatrix} 43+8 = 51 \\ 48+43\cdot 51 = 65 \\ 35+65\cdot 43 = 14 \\ 113+51\cdot 48 = 1 \\ 65+51\cdot 35 = 58 \\ 30+1\cdot 43 = 73 \end{bmatrix} = c$$

Otrzymaliśmy zatem szyfrogram postaci $c = (51, 65, 14, 1, 58, 73)$.

Przedstawmy teraz proces deszyfrowania dla hasła $-\alpha = (120, 105, 116, 85, 123)$:

$$c = \begin{bmatrix} 51 \\ 65 \\ 14 \\ 1 \\ 58 \\ 73 \end{bmatrix} \longrightarrow \begin{bmatrix} 51+120 = 43 \\ 65-51\cdot 43 = 48 \\ 14-65\cdot 43 = 35 \\ 1-51\cdot 48 = 113 \\ 58-51\cdot 35 = 65 \\ 73-1\cdot 43 = 30 \end{bmatrix} \longrightarrow \begin{bmatrix} 43+105 = 20 \\ 48+43\cdot 20 = 12 \\ 35+12\cdot 43 = 39 \\ 113+20\cdot 48 = 49 \\ 65+20\cdot 35 = 125 \\ 30+49\cdot 43 = 89 \end{bmatrix} \longrightarrow$$

$$\longrightarrow \begin{bmatrix} 20+116 &= 8 \\ 12-20\cdot 8 &= 108 \\ 39-12\cdot 8 &= 71 \\ 49-20\cdot 108 &= 65 \\ 125-20\cdot 71 &= 113 \\ 89-49\cdot 8 &= 81 \end{bmatrix} \longrightarrow \begin{bmatrix} 8+85 &= 93 \\ 108+8\cdot 93 &= 84 \\ 71+84\cdot 8 &= 103 \\ 65+93\cdot 108 &= 125 \\ 113+93\cdot 71 &= 60 \\ 81+125\cdot 8 &= 57 \end{bmatrix} \longrightarrow \begin{bmatrix} 93+123 &= 88 \\ 84-93\cdot 88 &= 92 \\ 103-84\cdot 88 &= 7 \\ 125-93\cdot 92 &= 17 \\ 60-93\cdot 7 &= 49 \\ 57-125\cdot 88 &= 65 \end{bmatrix} = m$$

6.3 Kryptografia asymetryczna

Główną ideą rozprawy jest zastosowanie lingwistycznych układów dynamicznych w konstrukcji algorytmów klucza publicznego, przedstawionych w postaci przekształceń wielomianowych $F(p) = (f_1(x), f_2(x), \ldots, f_n(x))$:

$$\begin{cases} f_1(x_1, \ldots, x_n) = y_1 \\ f_2(x_1, \ldots, x_n) = y_2 \\ \vdots \\ f_n(x_1, \ldots, x_n) = y_n \end{cases} \tag{6.2}$$

W celu wygenerowania powyższego układu, używamy złożenia odwzorowania G_s powstałego przez przejście po grafie (wraz z jego modyfikacjami, przedstawionymi w dwóch poprzednich rozdziałach 4 oraz 5) z dwoma afinicznymi odwzorowaniami T_1 i T_2, otrzymując klucz publiczny $T_1 G_s T_2$ w postaci przekształcenia wielomianowego.

Ważnymi czynnikami wpływającymi na efektywność oraz bezpieczeństwo algorytmów kryptografii wielu zmiennych są takie czynniki jak stopień oraz gęstość użytych przekształceń wielomianowych.

Stopień jest jednym z głównych kryteriów oceny właściwości przekształceń wielomianowych omawianych w tej rozprawie. Najlepsza możliwa sytuacja jest wtedy, gdy stopień przekształcenia szyfrującego jest niski (mamy wtedy wysoką efektywność algorytmu), przy jednoczesnym wysokim stopniu przekształcenia deszyfrującego (odpowiednie bezpieczeństwo).

Gęstość przekształcenia wielomianowego (stopnia d) definiujemy jako stosunek liczby niezerowych jednomianów do liczby wszystkich jednomianów stopnia $\leq d$. Mniejsza gęstość przekształcenia szyfrującego zwiększa jego efektywność, zaś bezpieczeństwu sprzyja

zwiększenie gęstości przekształcenia deszyfrującego (odwrotnego). Na gęstość ma wpływ wiele czynników, takich jak wybór przekształceń afinicznych, wybór grafu (w tym pierścienia - aspekt ten został szczegółowo omówiony w [16]) oraz sposobu przejścia po nim. Cecha ta nie jest jeszcze dokładnie zbadana pod kątem teoretycznym, przeanalizowane zostały wyniki doświadczalne uzyskane poprzez symulacje komputerowe.

Rząd grupy przekształceń wielomianowych. Istotnym zagadnieniem dla algorytmów kryptograficznych, szczególnie opartych na problemie logarytmu dyskretnego, jest rząd grupy i rząd elementu danej grupy, opisanych ogólnie w 1.1. W algorytmach kryptografii wielu zmiennych opisywanych w tej rozprawie bierzemy pod uwagę przekształcenia wielomianowe postaci $F = T_1 G_\alpha T_2$ (analogicznie do przekształcenia 2.1), gdzie T_1 i T_2 są przekształceniami afinicznymi (6.1) zaś G_α nieliniowym odwzorowaniem wielomianowym danych poprzez ścieżkę w grafie $D(n, K)$ (szczegółowa konstrukcja tych odwzorowań została pokazana w rozdziałach 4 oraz 5). Przekształcenia te tworzą cykliczną grupę przekształceń wielomianowych z operacją złożenia funkcji. Rząd takiej grupy przekształceń jest głównie uzależniony od rzędu odwzorowania G_α, który z kolei jest ściśle związany z talią grafu $D(n, K)$. Z własności (3.1) wynika, że talia grafu $g(D(n, K)) \geq n + 5$, czyli rząd grupy przekształceń wielomianowych (w pracy piszemy w skrócie rząd przekształcenia) rośnie do nieskończoności wraz ze wzrostem n. Romańczuk i Ustimenko w [49] wykazali, że dla pierścienia F_{p^n} (p - liczba pierwsza, n - liczba naturalna) rząd odwzorowania F jest potęgą p, wzrasta więc wraz ze wzrostem p. Dodatkowo, w tej samej pracy, została postawiona hipoteza (poparta wieloma testami komputerowymi), że w przypadku $K = Z_m$, gdzie $m = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$, rząd odwzorowania F jest postaci $p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, gdzie $k_1, k_2, \cdots, k_s \in \{0, 1, 2, \cdots\}$. Powyższe fakty, mogą zostać wykorzystane przy wyborze odpowiednich pierścieni w algorytmach opartych na problemie logarytmu dyskretnego.

6.3.1 Użycie odwzorowań wielomianowych niskich stopni

Rozważmy przypadek przekształceń wielomianowych niskich stopni omówionych w rozdziale 4. Pierwszą i bazową grupą przekształceń opartych na rodzinie grafów $D(n, K)$ były otrzymane i zbadane w [75] odwzorowania wielomianowe stopnia 3. W przypadku odwzorowań kubicznych (rozdziały 4.1, 4.2 oraz 4.3), otrzymane przekształcenia $f_i(x_1, \ldots, x_n)$ są wielomianami n zmiennych zapisanych jako sumy jednomianów typu $x_{i_1}^{m_1} x_{i_2}^{m_2} x_{i_3}^{m_3}$ (w przypadku odwzorowań trzeciego stopnia) ze współczynnikami z K, gdzie $i_1, i_2, i_3 \in 1, 2, \ldots, n$ i m_1, m_2, m_3 są liczbami naturalnymi takimi, że $m_1 + m_2 + m_3 \leq 3$. Jak wspomniano wcześniej, równania wielomianowe $y_i = f_i(x_1, x_2, \ldots, x_n),\ i = 1, 2 \ldots n$, będące kluczem

publicznym, mają stopień 3 (ewentualnie 2 lub 4, jeżeli użyjemy odwzorowań wielomianowych z rozdziałów 4.4 oraz 4.5). Stąd proces szyfrowania może być wykonany w czasie wielomianowym $O(n^4)$ (w pojedynczym $y_i,\ i = 1, 2 \ldots, n$ mamy $2(n^3 - 1)$ dodawań i mnożeń).

Przykład 6.2. Poniżej przedstawimy przykład konstrukcji i użycia przekształcenia wielomianowego w algorytmie symetrycznym bez użycia przekształceń afinicznych. Tak jak w przykładzie 6.1 użyjemy grafu $D(n, K) = D(6, Z_{2^7})$, zdefiniowanego równaniami (6.1) oraz hasła $\alpha = (5, 43, 12, 23, 8)$. Tekst jawny przedstawiamy w postaci ogólnej jako wektor $m = (x_1, x_2, x_3, x_4, x_5, x_6)$, zaś szyfrogram $c = (y_1, y_2, y_3, y_4, y_5, y_6)$. Poszukujemy zatem zależności między tekstem jawnym a szyfrogramem w postaci odwzorowania wielomianowego. Kolejne kroki (wierzchołki $m = v_0 \to v_1 \to \cdots \to v_5 = c$) przejścia w grafie można przedstawić w następujący sposób:

$$
\begin{aligned}
v_0 = p^{(0)} &= (x_1, x_2, x_3, x_4, x_5, x_6) \\
v_1 = l^{(1)} &= (x_1 + 5, x_2 + {x_1}^2 + 5x_1, x_3 + x_1x_2 + {x_1}^3 + 5{x_1}^2, x_4 + x_2x_1 + 5x_2, x_5 + x_3x_1 \\
&\quad + 5x_3, x_6 + x_1x_4 + x_2{x_1}^2 + 5x_2x_1) \\
v_2 = p^{(2)} &= (x_1 + 48, x_2 + 80x_1 + 16, x_3 + 80x_2 + 80{x_1}^2 + 16x_1, x_4 + 48{x_1}^2 + 96x_1 + 48, \\
&\quad x_5 + 48x_2x_1 + 112x_2 + 48{x_1}^3 + 96{x_1}^2 + 48x_1, x_6 + 80x_4 + 80x_2x_1 + 16x_2) \\
v_3 = l^{(3)} &= (x_1 + 60, x_2 + {x_1}^2 + 60x_1 + 80, x_3 + x_2x_1 + {x_1}^3 + 60{x_1}^2 + 32x_1, x_4 + x_2x_1 \\
&\quad + 60x_2 + 48x_1 + 112, x_5 + x_3x_1 + 60x_3 + 48x_2 + 48{x_1}^2 + 112x_1, x_6 + x_1x_4 + x_2{x_1}^2 \\
&\quad + 60x_2x_1 + 80x_2 + 48{x_1}^2 + 112x_1) \\
v_4 = p^{(4)} &= (x_1 + 83, x_2 + 45x_1 + 92, x_3 + 45x_2 + 45{x_1}^2 + 92x_1 + 16, x_4 + 83{x_1}^2 + 72x_1 + 96, \\
&\quad x_5 + 83x_2x_1 + 36x_2 + 83{x_1}^3 + 72{x_1}^2 + 80x_1 + 64, x_6 + 45x_4 + 45x_2x_1 + 92x_2 \\
&\quad + 112x_1 + 48) \\
v_5 = l^{(5)} &= (x_1 + 91, x_2 + {x_1}^2 + 91x_1 + 93, x_3 + x_2x_1 + {x_1}^3 + 91{x_1}^2 + 58x_1 + 55, \\
&\quad x_4 + x_2x_1 + 91x_2 + 35x_1 + 20, x_5 + x_3x_1 + 91x_3 + 35x_2 + 35{x_1}^2 + 20x_1 + 112, \\
&\quad x_6 + x_1x_4 + x_2{x_1}^2 + 91x_2x_1 + 93x_2 + 35{x_1}^2 + 93x_1 + 44)
\end{aligned}
$$

Ostatecznie otrzymujemy następujący układ:

$$
\begin{aligned}
y_1 &= x_1 + 91 \\
y_2 &= x_2 + x_1^2 + 91x_1 + 93 \\
y_3 &= x_3 + x_2x_1 + x_1^3 + 91x_1^2 + 58x_1 + 55 \\
y_4 &= x_4 + x_2x_1 + 91x_2 + 35x_1 + 20 \\
y_5 &= x_5 + x_3x_1 + 91x_3 + 35x_2 + 35x_1^2 + 20x_1 + 112 \\
y_6 &= x_6 + x_1x_4 + x_2x_1^2 + 91x_2x_1 + 93x_2 + 35x_1^2 + 93x_1 + 44
\end{aligned}
$$

Aby zaszyfrować wiadomość $m = v_0 = (88, 92, 7, 17, 49, 65) = (x_1, x_2, x_3, x_4, x_5, x_6)$, podstawiamy wszystkie wartości x_i dla $i = 1, 2, \ldots, 6$ do powyższego układu otrzymując szyfrogram $c = (y_1, y_2, y_3, y_4, y_5, y_6) = (51, 65, 14, 1, 58, 73)$.

Deszyfrowanie odbywa się tak samo jak w przypadku szyfrowania symetrycznego 6.1.

Przykład 6.3. Niech graf oraz hasło pozostaną takie same jak w poprzednim przykładzie 6.2. Poniższy przykład obrazuje to, jak zmienia się przekształcenie wielomianowe po zastosowaniu przekształceń afinicznych. Użyjmy zatem przekształceń afinicznych typu II (zdefiniowanych w rozdziale 6.2):

$$
T_1 = \begin{bmatrix}
1 & 4 & 39 & 17 & 2 & 64 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}, \quad
T_2 = \begin{bmatrix}
1 & 51 & 16 & 9 & 72 & 3 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix},
$$

Po zastosowaniu powyższych przekształceń (T_1 przejście w grafie, T_2) otrzymujemy przekształcenie wielomianowe następującej postaci:

$$
\begin{aligned}
y_1 = {} & 10 + 36x_1^2 + 104x_2^2 + 92x_3^2 + 87x_4^2 + 16x_5^2 + 64x_6x_4 + 22x_5x_4 + 20x_5x_2 \\
& + 16x_5x_1 + 53x_4x_3 + 118x_4x_2 + 75x_4x_1 + 102x_3x_2 + 64x_3x_1 + 74x_2x_1 \\
& + 52x_1 + 37x_2 + 20x_3 + 125x_4 + 48x_5 + 3x_6 + 16x_1^3 + 32x_4x_3x_1 + 64x_5x_3x_1 \\
& + 64x_5x_4x_1 + 64x_5x_4x_3 + 12x_5^2x_2 + 48x_5x_2^2 + 35x_4^2x_2 + 24x_4x_2^2 \\
& + 19x_3^2x_2 + 40x_3x_2^2 + 24x_2^2x_1 + 67x_2x_1^2 + 48x_2^3 + 76x_5x_4x_2 \\
& + 84x_5x_3x_2 + 12x_5x_2x_1 + 10x_4x_3x_2 + 102x_4x_2x_1 + 106x_3x_2x_1 \\
& + 64x_5^2x_4 + 64x_5^2x_3 + 64x_5^2x_1 + 96x_5x_4^2 + 96x_5x_3^2 + 96x_5x_1^2 \\
& + 80x_4^2x_3 + 48x_4^2x_1 + 48x_4x_3^2 + 48x_4x_1^2 + 48x_3^2x_1 + 80x_3x_1^2 + 16x_4^3 \\
& + 112x_3^3 \\
y_2 = {} & 93 + x_1^2 + 16x_2^2 + 113x_3^2 + 33x_4^2 + 4x_5^2 + 68x_5x_4 + 28x_5x_3 + 16x_5x_2 \\
& + 4x_5x_1 + 46x_4x_3 + 8x_4x_2 + 34x_4x_1 + 56x_3x_2 + 78x_3x_1 + 8x_2x_1 \\
& + 91x_1 + 109x_2 + 93x_3 + 11x_4 + 54x_5 + 64x_6 \\
y_3 = {} & 55 + 91x_1^2 + 52x_2^2 + 43x_3^2 + 59x_4^2 + 108x_5^2 + 64x_6x_2 + 44x_5x_4 + 116x_5x_3 \\
& + 50x_5x_2 + 108x_5x_1 + 90x_4x_3 + 105x_4x_2 + 22x_4x_1 + 15x_3x_2 + 58x_3x_1 \\
& + 89x_2x_1 + 58x_1 + 104x_2 + 87x_3 + 90x_4 + 116x_5 + x_1^3 + 10x_4x_3x_1 + 84x_5x_3x_1 \\
& + 76x_5x_4x_1 + 20x_5x_4x_3 + 48x_5^2x_2 + 96x_5x_2^2 + 12x_4^2x_2 + 48x_4x_2^2 \\
& + 76x_3^2x_2 + 80x_3x_2^2 + 48x_2^2x_1 + 12x_2x_1^2 + 64x_2^3 + 48x_5x_4x_2 \\
& + 80x_5x_3x_2 + 48x_5x_2x_1 + 40x_4x_3x_2 + 24x_4x_2x_1 + 40x_3x_2x_1 \\
& + 64x_6x_4^2 + 64x_6x_3^2 + 64x_6x_1^2 + 76x_5^2x_4 + 84x_5^2x_3 + 12x_5^2x_1 \\
& + 70x_5x_4^2 + 38x_5x_3^2 + 6x_5x_1^2 + 21x_4^2x_3 + 99x_4^2x_1 + 3x_4x_3^2 \\
& + 51x_4x_1^2 + 83x_3^2x_1 + 117x_3x_1^2 + 49x_4^3 + 8x_5^3 + 55x_3^3 \\
y_4 = {} & 64x_6x_2 + 64x_6 + 2x_5x_2 + 70x_5 + 17x_4x_2 + 84x_4 + 39x_3x_2 + 85x_3 + 4x_2^2 \\
& + x_2x_1 + 103x_2 + 35x_1 + 20 \\
y_5 = {} & 112 + 35x_1^2 + 48x_2^2 + 26x_3^2 + 3x_4^2 + 12x_5^2 + 64x_6x_3 + 76x_5x_4 + 86x_5x_3 \\
& + 48x_5x_2 + 12x_5x_1 + 91x_4x_3 + 24x_4x_2 + 38x_4x_1 + 44x_3x_2 + 43x_3x_1 \\
& + 24x_2x_1 + 20x_1 + 115x_2 + 103x_3 + 84x_4 + 41x_5
\end{aligned}
$$

$$
\begin{aligned}
y_6 = {} & 44 + 35x_1^2 + 28x_2^2 + 115x_3^2 + 20x_4^2 + 12x_5^2 + 64x_6x_4 + 64x_6x_2 + 78x_5x_4 \\
& + 84x_5x_3 + 102x_5x_2 + 12x_5x_1 + 113x_4x_3 + 39x_4x_2 + 39x_4x_1 + 5x_3x_2 \\
& + 42x_3x_1 + 115x_2x_1 + 93x_1 + 81x_2 + 43x_3 + 45x_4 + 58x_5 + 65x_6 + 4x_5^2x_2 \\
& + 16x_5x_2^2 + 33x_4^2x_2 + 8x_4x_2^2 + 113x_3^2x_2 + 56x_3x_2^2 + 8x_2^2x_1 + x_2x_1^2 \\
& + 16x_2^3 + 68x_5x_4x_2 + 28x_5x_3x_2 + 4x_5x_2x_1 + 46x_4x_3x_2 + 34x_4x_2x_1 \\
& + 78x_3x_2x_1
\end{aligned}
$$

Klisowski w [18] oraz [16] zaimplementował część rozpatrywanych przez nas przekształceń wielomianowych (w szczególności kubicznych) w celu wygenerowania klucza publicznego, szyfrowania tekstu, używając niektórych - badanych przez nas ((4.1)) - przekształceń wielomianowych. Uzasadnił fakt, że wraz z zastosowaniem przekształceń afinicznych złożoność wygenerowania takiego klucza wynosi $\mathcal{O}(n^5)$ oraz podał wzory na rozmiary przestrzeni klucza w tym przypadku. Uzasadnił również (pod kątem teoretycznym i praktycznym) efektywność generowania kluczy, pokazując, że liczba możliwych kluczy jest zbyt duża, aby zastosować przeszukiwanie wyczerpujące. Użyte tam zostały: macierz A, która na przekątnej ma same 1, zaś elementy w pierwszym wierszu są niezerowa, macierz identycznościowa B oraz zerowy wektor c i d. W takim przypadku koszt użycia odwzorowania afinicznego jest liniowy.

Tabela 6.1 prezentuje czas (w milisekundach) generowania klucza publicznego w zależności od liczby zmiennych (n) oraz długości hasła (p), zaś tabela 6.2 przedstawia czas w milisekundach procesu szyfrowania, zależnie od liczby bajtów teksu jawnego (n) oraz liczby bajtów wyrażenia (w).

Z tabeli 6.3 możemy odczytać liczbę jednomianów i gęstość w procentach, w zależności od użytych przekształceń afinicznych dla różnych pierścieni. Przedstawione są trzy przypadki:

I przypadek brak przekształceń afinicznych (tzn. T_1 i T_2 - przekształcenia tożsamościowe)

II przypadek T_1 i T_2 - przekształcenia afiniczne *typu 2* (zdefiniowane w rozdziale 6.2)

III przypadek T_1 i T_2 - przekształcenia afiniczne ogólnego typu

W pracy [16] oprócz powyższych zostały rozpatrzone przypadki gdzie T_1 jest toższamościowe, a T_2 ogólnego typu, oraz T_1 - typu 2, T_2 - ogólnego typu.

Tabela 6.1: Czas wygenerowania klucza publicznego, źródło [18]

	$p = 10$	$p = 20$	$p = 30$	$p = 40$	$p = 50$	$p = 60$
$n = 10$	15	15	16	32	31	32
$n = 20$	109	250	391	531	687	843
$n = 30$	609	1484	2468	3406	4469	5610
$n = 40$	2219	7391	12828	18219	24484	29625
$n = 50$	5500	17874	34078	49952	66749	82328
$n = 60$	12203	42625	87922	138906	192843	242734
$n = 70$	22734	81453	169250	286188	405500	536641
$n = 80$	46015	165875	350641	619921	911781	1202375
$n = 90$	92125	332641	708859	1262938	1894657	2525360
$n = 100$	159250	587282	1282610	2220610	3505532	4899657

Tabela 6.2: Czas szyfrowania, źródło [18]

	$\mathbb{Z}_{2^8}$	$\mathbb{Z}_{2^{16}}$	$\mathbb{Z}_{2^{32}}$
$n = 20$	16	0	0
$n = 40$	265	47	15
$n = 60$	1375	188	15
$n = 80$	3985	578	47
$n = 100$	10078	1360	125

Tabela 6.3: Liczba jednomianów i gęstość przekształceń wielomianowych dla rożnych pierścieni i przekształceń afinicznych, źródło [16]

graf $D(64, K)$		
I przypadek	II przypadek	III przypadek
$K = \mathbb{Z}_{2^{16}}$		
2143 (0,07%)	1043714 (34,04%)	3065372 (99,98%)
$K = \mathbb{Z}_{3^{10}}$		
2143 (0,07%)	1058343 (34,52%)	3065747 (99,99%)
$K = \mathbb{Z}_{7^6}$		
2143 (0,07%)	1057414 (34,49%)	3065881 (100,00%)
$K = \mathbb{Z}_{2^{16}}$		
2112 (0,07%)	119854 (3,91%)	399420 (13,03%)
$K = \mathbb{F}_{3^{10}}$		
2143 (0,07%)	556224 (18,14%)	3065851 (100,00%)
$K = \mathbb{F}_{7^6}$		
2143 (0,07%)	1058859 (34,54%)	3065896 (100,00%)

Z tabeli 6.3 można wywnioskować, że użycie przekształceń tożsamościowych pozwala uzyskać najmniejszą gęstość, zaś dla przekształceń afinicznych ogólnego typu osiągamy praktycznie maksymalną gęstość dla kubicznych odwzorowań wielomianowych. Zwiększenie gęstości powoduje mniejszą efektywność szyfrowania, ale przy tym zwiększa bezpieczeństwo algorytmów opartych na tego typu przekształceniach.

Rozważmy bezpieczeństwo algorytmu szyfrującego w kryptograffi z kluczem publicznym używając odwzorowań wielomianowych opisanych w powyższych rozdziałach. Cechą charakterystyczną odwzorowań trzeciego stopnia rozpatrywanych w 4.1 jest fakt, że odwzorowanie odwrotne jest również odwzorowaniem trzeciego stopnia (co wynika stąd, że może być otrzymane poprzez symetryczne przejście w grafie w przeciwnym kierunku).

Niech klucz publiczny F będzie następującej postaci:

$$\begin{aligned} y_1 &= f_1(x_1, x_2, \cdots, x_n) \\ y_2 &= f_2(x_1, x_2, \cdots, x_n) \\ &\vdots \\ y_n &= f_n(x_1, x_2, \cdots, x_n), \end{aligned}$$

gdzie $f_i(x_1, x_2, \cdots, x_n)$, (dla $1 \leq i \leq n$) będą wielomianami trzeciego stopnia).

Na tym etapie badań, z powyższego układu równań nie jesteśmy w stanie znaleźć hasła $\alpha = (\alpha_1, \alpha_2 \ldots, \alpha_s)$ ani odwzorowań afinicznych T_1 i T_2. Niestety, przekształcenie odwrotne F^{-1} jest również przekształceniem wielomianowym stopnia trzeciego, który możemy przedstawić w postaci:

$$\begin{aligned} x_1 &= g_1(y_1, y_2, \cdots, y_n) \\ x_2 &= g_2(y_1, y_2, \cdots, y_n) \\ &\vdots \\ x_n &= g_n(y_1, y_2, \cdots, y_n) \end{aligned}$$

Umożliwia to obliczenie wszystkich współczynników wielomianów tego przekształcenia po wygenerowaniu odpowiedniej liczby szyfrogramów dla zadanych tekstów jawnych. Z [16] dowiadujemy się, że złożoność uzyskania klucza deszyfrowania, czyli trójki T_1, α, T_2, można

oszacować od góry przez $\mathcal{O}(n^{10})$. Pokazuje to, że algorytmy szyfrujące oparte na transformacjach wielomianowych o niskich stopniach (rozdział 4), dla których odwzorowania odwrotne również mają niski stopień, nie zapewniają bezpieczeństwa w algorytmach kryptograficznych z kluczem publicznym.

6.3.2 Użycie stabilnych odwzorowań wielomianowych rosnących stopni powstałych w wyniku procedury kompresji

Użycie odwzorowań wielomianowych niskich stopni, dla których stopień odwzorowania szyfrującego jest równy stopniowi odwzorowania deszyfrującego, wiąże się ze zmniejszoną odpornością na ataki linearyzacji. Z powyższego powodu w dalszej kolejności skupimy się nad schematach szyfrowania opartych na tych samych rodzinach grafów o dużej talii, ale pozbawionych przedstawionej wady (omówionych w rozdziale 5.1). W tym celu dokonywane zostały modyfikacje przekształceń szyfrujących, w taki sposób, aby możliwie zwiększyć stopień przekształcenia do niego odwrotnego. Niestety, w przypadku 5.1 zwiększamy przy tym również stopień przekształcenia szyfrującego, co powoduje spadek efektywności oraz zwiększenie rozmiaru klucza. Dokonując jednak starannego wyboru przekształceń afinicznych (6.1 - poprzez wybór macierzy „rzadkich"), możemy kontrolować gęstość odwzorowań wielomianowych, tym samym zwiększając efektywność, przy zachowaniu odpowiedniego bezpieczeństwa.

Rozważmy kryptosystem oparty na rodzinie odwzorowań stabilnych rosnących stopni i rosnącego rzędu opartych na spójnych składowych grafu $D(n, K)$, po przeprowadzeniu procedury kompresji (konstrukcja opisana w rozdziale 5.1).

Właściciel klucza (Alicja) wybiera podzbiór multiplikatywny Q pierścienia K oraz ciągi $\alpha_1, \alpha_2, \ldots, \alpha_k$, $\alpha_i \in Q$ i $\beta_1, \beta_2, \ldots, \beta_k$, $\beta_i \in Q$, takie, że $\beta_i - \beta_{i+1} \in Q$ dla $i = 1, 2, \ldots, k-1$, gdzie k jest stałą niezależną od n. Alicja wybiera również dla wierzcholków v parametry $d_2, d_3, \ldots, d_{[(n+1)/2]+1}$ spełniające równania: $a_2(\mathrm{v}) = d_2, a_3(\mathrm{v}) = d_3, \ldots, a_{[(n+1)/2]+1}(\mathrm{v}) = d_{[(n+1)/2]+1}$ w celu kompresji tych bloków dla relacji równoważności τ.

Następnie Alicja generuje odwzorowanie H' na $K^{n-[(n+1)/2]}$ opisane w rozdziale 5.1, w standardowej formie

$x_1 \to f_1(x_1, x_2, \ldots, x_d)$

$x_2 \to f_2(x_1, x_2, \ldots, x_d)$

$\ldots$

$x_d \to f_d(x_1, x_2, \ldots, x_d)$

gdzie $d = 2n - [(n+1)/2]$

Czas generowania H' jest porównywalny z czasem generowania odwzorowania stabilnego odpowiadającego $D(n, K)$ (szacunkowe czasy można znaleźć [20]). Alicja używa transformacji jednomianowej T_1 typu $x_i \to l_i x_i$, gdzie l_i są elementami regularnymi pierścienia dla $i = 1, 2, \ldots, d$ oraz przekształcenia afinicznego T_2: x $\to$ xA + b, gdzie A jest macierzą odwracalnego afinicznego przekształcenia dla K^d, zaś b jest wybranym wektorem.

Następnie Alicja oblicza złożenie $G = T_1 H' T_2$ w standardowej postaci

$x_1 \to g_1(x_1, x_2, \ldots, x_d)$

$x_2 \to g_2(x_1, x_2, \ldots, x_d)$

$\ldots$

$x_d \to g_d(x_1, x_2, \ldots, x_d)$.

Zauważmy, że ogólna liczba jednomianowych wyrażeń w f_i, $i = 1, 2, \ldots, d$ jest równa $O(n^4)$. Liniowe odwzorowanie T_1 nie zmienia liczby jednomianów. Złożenie z afinicznym odwzorowaniem T_2 z prawej strony może zwiększać liczbę odwzorowań n razy. Stąd, ogólna liczba jednomianów ze wszystkich g_i może być oszacowana przez $O(n^5)$. Oznacza to, że policzenie wartości G w danym punkcie x może być wykonane w czasie wielomianowym. Teraz Alicja może zaprezentować odwzorowanie G użytkownikowi publicznemu (Bob). Każdy jednomian wymaga wykonania $O(n)$ elementarnych operacji. Dlatego, Bob może obliczyć wartość reguły publicznej w czasie $O(n^6)$.

Proces deszyfrowania może odbyć się w czasie $O(n)$, używając operatorów przejścia po grafie bez korzystania z jawnej postaci przekształcenia odwrotnego. Stopień jawnej postaci odwzorowania odwrotnego jest równy $n - [(n+1)/2]$, co skutecznie utrudnia ataki linearyzacji. Na tym etapie badań, oprócz wyników teoretycznych, nie posiadamy niestety jeszcze szczegółowej analizy symulacji komputerowych algorytmów kryptograficznych, bazujących na tym schemacie.

6.3.3 Użycie odwzorowań wielomianowych z nieliniowym zaburzeniem

Z punktu widzenia kryptografii wielu zmiennych, najlepsze odwzorowania wielomianowe to takie, które mają niski stopień odwzorowania szyfrującego (dla lepszej efektywności) oraz wysoki stopień odwzorowania deszyfrującego (dla zwiększenia odporności na ataki linearyzacji). W tym podrozdziale przedstawimy algorytm asymetryczny oparty

na odwzorowaniach wielomianowych z nieliniowym zaburzeniem, opisanych w 5.2. Niech h będzie wzajemnie jednoznaczną funkcją wielomianowa jednej zmiennej. Otrzymana w ten sposób rodzina odwzorowań $H = H(n, \alpha, h, K)$, $(\alpha = (\alpha_1, \alpha_2, \dots \alpha_s))$, wraz z zastosowaniem odwzorowań afinicznych (T_1 oraz T_2), przed przejściem ścieżki długości s w grafie i po jej przejściu, tworzy rodzinę odwzorowań $F = T_1 H T_2$, gdzie

$$\deg F = \begin{cases} \deg h + 2 & \text{dla } s = 2k - 1 \\ 2 \deg h + 1 & \text{dla } s = 2k \end{cases}$$

Mamy zatem dwa przypadki, które bardzo się od siebie różnią, pod względem zastosowania w algorytmach asymetrycznych.

Dla uproszczenia wywodu, rozpatrzymy przypadek tożsamościowych przekształceń afinicznych. W pierwszej kolejności weźmy pod uwagę przypadek drugi, gdzie jako przekształcenie szyfrujące będzie użyte odwzorowanie F, którego stopień $\deg F = 2 \deg h + 1$.

Ostatnim wierzchołkiem – szyfrogramem c – jest wtedy punkt (obcięty do n współrzędnych) postaci

$$c = (c_1, c_2, \dots, c_n) = (p_1 + \alpha_2 + \alpha_4 + \dots + \alpha_{2k}, p_2^{2k}, \dots, p_{4t+1}^{2k}, p_{4t+2}^{2k}, p_{4t+3}^{2k}, p_{4t+4}^{2k}, \dots),$$

wtedy

$$p_1 = c_1 - (\alpha_2 + \alpha_4 + \dots + \alpha_{2k}).$$

Zatem poprzedni wierzchołek (na ścieżce w odwrotnym kierunku) ma postać:

$$[h(c_1 - (\alpha_2 + \alpha_4 + \dots + \alpha_{2k})) + \alpha_1 + \alpha_3 + \dots + \alpha_{2k-1}, l_2^{2k-1}, \dots, l_{4t+1}^{2k-1}, l_{4t+2}^{2k-1}, l_{4t+3}^{2k-1}, l_{4t+4}^{2k-1}, \dots],$$

gdzie wszystkie współczynniki $l_2^{2k-1}, \dots, l_{4t+1}^{2k-1}, l_{4t+2}^{2k-1}, l_{4t+3}^{2k-1}, l_{4t+4}^{2k-1}$ wyznaczone są z równań definiujących graf $D(n, K)$ (3.1).

Kolejne wierzchołki możemy otrzymać w analogiczny sposób, dochodząc do pierwszego wierzchołka, będącego tekstem jawnym. Można zatem otrzymać odwzorowanie deszyfrujące $\deg F^{-1}$ zaczynając od ostatniego wierzchołka i przechodząc tą samą ścieżkę w grafie, tylko w odwrotnym kierunku. Wynika stąd, że stopień odwzorowania odwrotnego nie zmienia się, czyli $\deg F = \deg F^{-1} = 2 \deg h + 1$. Widzimy zatem, że ten przypadek, ze względu na równy stopień przekształcenia szyfrującego i deszyfrującego, nie stanowi najlepszego rozwiązania w algorytmach asymetrycznych.

Zupełnie inna sytuacja jest w przypadku ścieżki nieparzystej długości ($s = 2k - 1$), gdzie mamy $\deg F = \deg h + 2$. Ostatnim wierzchołkiem – szyfrogramem c– jest wtedy prosta (obcięta do n współrzędnych) postaci:

$$c = (c_1, c_2, \ldots, c_n) = (h(p_1) + \alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1}, l_2^{2k-1}, \ldots, l_{4t+1}^{2k-1}, l_{4t+2}^{2k-1}, l_{4t+3}^{2k-1}, l_{4t+4}^{2k-1}, \ldots).$$

Z równania

$$c_1 = h(p_1) + \alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1}$$

otrzymujemy

$$p_1 = h^{-1}(c_1 - (\alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1})).$$

Analiza stopnia przekształcenia deszyfrującego

Widzimy zatem, że obliczenie kolejnych wierzchołków na ścieżce w odwrotnym kierunku, wiąże sie z poziomem trudności obliczenia funkcji odwrotnej do h. Dzięki symbolicznemu przejściu ścieżki długości $s = 2k - 1$ w grafie w przeciwnym kierunku, możemy ocenić stopień przekształcenia szyfrującego w zależności od stopnia h^{-1}. Oznaczmy kolory wierzchołków (pierwsze współrzędne wektorów) przez $x_1^0, x_1^1, \ldots, x_1^{2k-1}$, gdzie $x_1^0 = p_1$, zaś $x_1^{2k-1} = c_1$. Przedstawmy zatem ciąg kolorów wierzchołków w odwrotnym kierunku, korzystając z tego, że $p_1 = h^{-1}(c_1 - (\alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1}))$.

$x_1^{2k-1} = c_1$
$x_1^{2k-2} = h^{-1}(c_1 - (\alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1})) + \alpha_2 + \alpha_4 + \cdots + \alpha_{2k-2}$
$x_1^{2k-3} = h(h^{-1}(c_1 - (\alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1}))) + \alpha_1 + \alpha_3 + \cdots + \alpha_{2k-3}$
$\cdots$
$x_1^3 = h(h^{-1}(c_1 - (\alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1}))) + \alpha_1 + \alpha_3$
$x_1^2 = h^{-1}(c_1 - (\alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1})) + \alpha_2$
$x_1^1 = h(h^{-1}(c_1 - (\alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1}))) + \alpha_1$
$x_1^0 = h^{-1}(c_1 - (\alpha_1 + \alpha_3 + \cdots + \alpha_{2k-1}))$

Po przejściu ścieżki nieparzystej długości, ostatnim kroku kolor wierzchołka stanowi funkcja odwrotna o stopniu $\deg h^{-1}$. Korzystając z twierdzenia 5.4 wnioskujemy, że stopień przekształcenia deszyfrującego wynosi $\deg h^{-1} + 2$. Odpowiednio dobierając funkcję h oraz pierścień K możemy wygenerować przekształcenia o niewielkim stopniu przekształcenia szyfrującego i znacząco zwiększonym stopniu odwzorowania deszyfrującego.

Zastosowanie wielomianów permutacji jako nieliniowego zaburzenia

Rozważmy użycie przekształceń wielomianowych z nieliniowym zaburzeniem w kryptografii z kluczem publicznym, używając wielomianów permutacji, jako zaburzenia h. Niech h będzie wzajemnie jednoznaczną funkcją wielomianową jednej zmiennej, nazywaną w literaturze ([6, 33, 34, 47]) *wielomianem permutacji*, w większości dotyczącym ciał skończonych. Wielomiany permutacji stosowane były w kryptografii w kryptosystemach takich jak RSA ([32, 33]) czy schemat Imai-Matsumoto ([38]). Weźmy pod uwagę jedne z prostszych nieliniowych wielomianów permutacji postaci $f(x) = x^a$ nad ciałem skończonym F_q, gdzie a (*wykładnik szyfrujący*) jest liczbą całkowitą większą od 1.

Dla ciał skończonych F_{p^s} (p - liczba pierwsza, s - pewna liczba całkowita dodatnia), wielomian $h(x) = x^a$ jest wielomianem permutacji, jeśli:

$$nwd(a, p^s - 1) = 1 \quad ([35]). \tag{6.3}$$

Funkcją odwrotną jest wtedy $h^{-1} = x^b$ (*wykładnik deszyfrujący*), jeśli:

$$ab \equiv 1 \ (\mod p^s - 1). \tag{6.4}$$

Jednym z rozwiązań równania (6.3) jest $a = p$, dla którego $b = p^{s-1}$. Korzystając, z tego, że dla ciał skończonych o charakterystyce p zachodzi równanie $(x + y)^{p^i} = x^{p^i} + y^{p^i}$ dla całkowitej liczby dodatniej i, można zauważyć, że nawet większy wykładnik b nie zawsze zwiększa liczby jednomianów przekształcenia deszyfrującego. Z tego powodu rozpatrujemy również wykładniki postaci $a \neq p^i$, których nie zachodzi powyższe równanie.

Na podstawie tabel 6.6 oraz 6.8 możemy porównać liczby jednomianów w przekształceniach odwrotnych dla $a = p = 2$ oraz $a = 3 \neq p^i = 2^i$. W przypadku wykładnika $a \neq p^i$, można zaobserwować znacznie większą liczbę jednomianów przekształcenia deszyfrującego.

Tak jak było wspominane wcześniej, szczególnie interesują nas te przypadki funkcji h, dla których a jest najmniejsze (ze względu na efektywność), zaś b - możliwie największe (ze względu na bezpieczeństwo algorytmu).

Klisowski w [16] udowodnił następujące twierdzenie:

Twierdzenie 6.1. *Najmniejszy możliwy wykładnik szyfrujący a taki, że*

$$a \neq p^i, \qquad i \in \mathbb{Z}_+, \tag{6.5}$$

wynosi 3 i można go użyć w przypadku ciał $\mathbb{F}_{p^s}$ spełniających następujące warunki:

$$p \equiv 2 \pmod 3, \tag{6.6}$$

$$s \equiv 1 \pmod 2. \tag{6.7}$$

Klisowski w [16] zbadał również pary wykładników szyfrujących i deszyfrujących przy najmniejszym możliwym różnym od p^i wykładniku szyfrującym dla różnych ciał skończonych. Część z tych wyników możemy zaobserwować w tabelach 6.4 i 6.5.

Na podstawie (6.4), dla ciała o charakterystyce p i wykładnika szyfrującego a, wykładnik deszyfrujący b spełnia nierówność:

$$b > \frac{p^s - 1}{a} \tag{6.8}$$

Powyższa nierówność oznacza, że wykładnik b może być wybrany odpowiednio duży, tzn. w zależności od wyboru wykładnika a, charakterystyki p możemy dobrać ciało skończone (parametr s), aby wartość b była większa od zadanej liczby.

Tabela 6.6 przedstawia obliczenia dotyczące stopni i liczby jednomianów przekształceń szyfrujących i deszyfrujących z użyciem zaburzenia $h(x) + \alpha$ w grafie $D(n, \mathbb{F}_{2^3})$ dla wielomianów $h_1(x) = x^2$ oraz $h_2(x) = x^3$ i hasła długości 7. W algorytmie zastosowano przekształcenie afiniczne w ogólnej postaci, jednokrotnie, po użyciu przekształceń wielomianowych (po przejściu ścieżki w grafie). Przekształceniami odwrotnymi do h_1 i h_2 w przypadku ciała $\mathbb{F}_{2^3}$ są odpowiednio $h_1^{-1}(x) = x^4$ oraz $h_2^{-1}(x) = x^5$. Doświadczenia komputerowe potwierdzają wyniki teoretyczne uzyskane w rozdziale 5.2 mówiące, że dla hasła nieparzystej długości i wykładników a i b, stopień przekształcenia szyfrującego wynosi $a + 2$ zaś deszyfrującego $b + 2$. Porównajmy uzyskane wyniki dla tego algorytmu i algorytmu wcześniej opracowanego przez Klisowskiego (będzie on omówiony na koniec rozdziału w 6.5.1). W obu przypadkach badane były te same wielomiany permutacji dla tego samego grafu. Klisowski w [16] zaproponował zastosowanie kubicznych odwzorowań (4.1) z zaburzeniem, ale tylko w ostatnim kroku. Wyniki uzyskane w rozprawie wskazują na poprawę efektywności, poprzez zmniejszenie liczby jednomianów przekształcenia szyfrującego oraz zwiększenie poziomu bezpieczeństwa dzięki zwiększeniu liczby jednomianów przekształcenia deszyfrującego.

Powyższy fakt oraz wyniki doświadczalne dotyczące liczby jednomianów wskazują na dobre rokowania dla zastosowań w kryptosystemach klucza publicznego.

Tabela 6.4: Pary wykładników szyfrowania i deszyfrowania dla ciał $\mathbb{F}_{p^n}$, $p = 2, 3, 5,$, źródło [16]

$p = 2$					
n	1	2	3	4	5
	—	—	$(3, 5)$	$(7, 13)$	$(3, 21)$
n	6	7	8	9	10
	$(5, 38)$	$(3, 85)$	$(7, 73)$	$(3, 341)$	$(5, 614)$
n	11	12	13	14	15
	$(3, 1365)$	$(11, 2606)$	$(3, 5461)$	$(5, 9830)$	$(3, 21845)$
n	16	17	18	19	20
	$(7, 56173)$	$(3, 87381)$	$(5, 157286)$	$(3, 349525)$	$(7, 299593)$
n	21	22	23	24	25
	$(3, 1398101)$	$(5, 2516582)$	$(3, 5592405)$	$(11, 12201611)$	$(3, 22369621)$
$p = 3$					
n	1	2	3	4	5
	—	$(5, 5)$	$(5, 21)$	$(7, 23)$	$(5, 97)$
n	6	7	8	9	10
	$(5, 437)$	$(5, 1749)$	$(7, 5623)$	$(5, 7873)$	$(5, 35429)$
n	11	12	13	14	15
	$(5, 141717)$	$(11, 193251)$	$(5, 637729)$	$(5, 2869781)$	$(5, 11479125)$
$p = 5$					
n	1	2	3	4	5
	$(3, 3)$	$(7, 7)$	$(3, 83)$	$(7, 535)$	$(3, 2083)$
n	6	7	8	9	10
	$(11, 11363)$	$(3, 52083)$	$(7, 111607)$	$(3, 1302083)$	$(7, 8370535)$
n	11	12	13		
	$(3, 32552083)$	$(11, 110973011)$	$(3, 813802083)$		

Tabela 6.5: Pary wykładników szyfrowania i deszyfrowania dla ciał $\mathbb{F}_{p^n}$, $p = 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$, źródło [16]

n	1	2	3	4	5	6
$p = 7$	$(5, 5)$	$(5, 29)$	$(5, 17)$	$(11, 1091)$	$(5, 13445)$	$(5, 70589)$
$p = 11$	$(3, 7)$	$(7, 103)$	$(3, 887)$	$(7, 4183)$	$(3, 107367)$	$(13, 953917)$
$p = 13$	$(5, 5)$	$(5, 101)$	$(5, 1757)$	$(11, 20771)$	$(5, 148517)$	$(5, 2896085)$
$p = 17$	$(3, 11)$	$(5, 173)$	$(3, 3275)$	$(7, 23863)$	$(3, 946571)$	$(5, 14482541)$
$p = 19$	$(5, 11)$	$(7, 103)$	$(5, 4115)$	$(7, 111703)$	$(5, 1485659)$	$(11, 21384491)$
$p = 23$	$(3, 15)$	$(5, 317)$	$(3, 8111)$	$(7, 239863)$	$(3, 4290895)$	$(5, 88821533)$
$p = 29$	$(3, 19)$	$(11, 611)$	$(3, 16259)$	$(11, 321491)$	$(3, 13674099)$	$(11, 378523931)$
$p = 31$	$(7, 13)$	$(7, 823)$	$(7, 17023)$	$(7, 263863)$	$(7, 20449393)$	$(11, 322728611)$
$p = 37$	$(5, 29)$	$(5, 821)$	$(5, 20261)$	$(7, 1606423)$	$(5, 55475165)$	$(5, 691696355)$
$p = 41$	$(3, 27)$	$(11, 611)$	$(3, 45947)$	$(11, 1798211)$	$(3, 77237467)$	$(11, 2159138291)$
$p = 43$	$(5, 17)$	$(5, 1109)$	$(5, 63605)$	$(13, 2103877)$	$(5, 58803377)$	$(5, 3792817829)$

Tabela 6.6: Stopnie i liczba jednomianów przekształceń szyfrujących i deszyfrujących z użyciem zaburzenia $h(x) + \alpha$ w grafie $D(n, \mathbb{F}_{2^3})$ dla różnych wielomianów h i hasła długości 7

$h(x) = x^2$, $h^{-1}(x) = x^4$								
n	4	6	8	10	12	14	20	26
stopień	4	4	4	4	4	4	4	4
l. jednomianów	36	74	140	235	355	462	991	1713
stopień prz. odwr.	6	6	6	6	6	6	6	25
l. jedn. prz. odwr.	88	434	1994	7084	17538	23037	196580	794196
$h(x) = x^3$, $h^{-1}(x) = x^5$								
n	4	6	8	10				
stopień	5	5	5	5				
l. jednomianów	28	73	152	253				
stopień prz. odwr.	7	7	7	7				
l. jedn. prz. odwr.	47	3373	16522	58176				

6.4 Symboliczny protokół uzgodnienia klucza Diffiego-Hellmana

W tym podrozdziale przedstawione zostanie zastosowanie grupy stabilnych odwzorowań wielomianowych niskich stopni w protokole uzgodnienia klucza Diffiego-Hellmana. Niski stopień odwzorowania odwrotnego nie stanowi przeszkody w tego rodzaju algorytmach wymiany klucza, więc lingwistyczny układ dynamiczny bazujący na odwzorowaniach niskich stopni może być tu zastosowany z powodzeniem. Poszczególne kroki podstawowego algorytmu zostały wypisane w 2.1.3. Różnica polega na użyciu jako generatora grup cyklicznych odwzorowania wielomianowego, wybranego z pośród odwzorowań stabilnych niskich stopni. Wersję algorytmu przedstawioną w rozprawie nazywamy symboliczną, z racji obliczeń symbolicznych wykonywanych w kolejnych krokach algorytmu.

Rozważmy protokół Diffie-Hellman w grupie symetrycznej S_{p^n} dla uzgodnienia klucza w przypadku użycia teorii grup. Generator będzie następującej postaci:

$$g = TG_\alpha T^{-1},$$

gdzie

T - odwracalne przekształcenie afiniczne,

$G_\alpha = G_{\alpha_1} G_{\alpha_2} \dots G_{\alpha_{s-1}} G_{\alpha_s}$ - odwzorowanie wielomianowe powstałe przez złożenie operatorów przejścia po grafie (opisane w różnych wersjach w tym rozdziale).

Wtedy, dla całkowitego a, g^a interpretujemy jako a - krotne złożenie odwzorowania g ze sobą, zaś wspólny klucz k podany jest jako przekształcenie wielomianowe, np dla $a = 4$ otrzymujemy:

$$\begin{aligned} g^4 = g \circ g \circ g \circ g &= T \circ G_\alpha \circ T^{-1} \circ T \circ G_\alpha \circ T^{-1} \circ T \circ G_\alpha \circ T^{-1} \circ T \circ G_\alpha \circ T^{-1} \\ &= T \circ G_{\alpha'} \circ T^{-1}, \end{aligned}$$

gdzie $\alpha' = (\alpha_1, \cdots, \alpha_s, \alpha_1, \cdots, \alpha_s, \alpha_1, \cdots, \alpha_s, \alpha_1, \cdots, \alpha_s)$.

Przedstawmy zatem symboliczny protokół uzgodnienia klucza Diffiego-Hellmana w następującej postaci:

1. Korespondenci Alicja i Bob ustalają grupę symetryczną S_{p^n} oraz generator grupy $g \in S_{p^n}$ - jako odwzorowanie wielomianowe przedstawione wyżej. Grupa S_{p^n} i g są znane publicznie (jawne).

2. Alicja wybiera losowo tajną liczbę całkowitą a i oblicza: $A = g^a \mod p$ (a - krotne złożenie odwzorowania g) i przesyła ją do Boba.

3. Bob wybiera losowo tajną liczbę całkowitą b i oblicza: $B = g^b \mod p$ (b - krotne złożenie odwzorowania g) i przesyła ją do Alicji.

4. Alicja oblicza $k = B^a = (g^b)^a = g^{ab}$, zaś Bob oblicza $k = A^b \mod p = (g^a)^b \mod p = g^{ab} \mod p$, uzyskując razem z Alicją wspólny tajny klucz K, podany w postaci odwzorowania wielomianowego.

Bezpieczeństwo przedstawionego systemu wymiany klucza jest zależne od efektywności obliczania logarytmów dyskretnych w rozważanych grupach przekształceń (1.5). Biorąc pod uwagę użyte odwzorowanie wielomianowe g, protokół Diffie-Hallman może być bezpieczny, jeśli rząd odwzorowania g jest "odpowiednio duży" i przeciwnik nie jest w stanie odnaleźć liczb a ani b jako funkcji zależnej od stopnia g oraz A. Oczywistym złym przykładem jest odwzorowanie g przekształcające x_i w ${x_i}^t$ dla każdego i. W tym przypadku a może być wyznaczone jako stosunek $\deg A$ oraz $\deg g$. Aby uniknąć takiego problemu, można wziąć pod uwagę rodzinę podgrup stabilnych G_n grupy S_{p^n}, $n \to \infty$, taką, że maksymalny stopień jego elementów jest równy c, gdzie c jest niewielką niezależną stałą (grupy stabilne zostały omówione w podrozdziale 1.6). Grupy stabilne g_n, utworzone przez przekształcenia zdefiniowane w rozdziale 4, tworzą grupę przekształceń, której rząd dąży do nieskończoności wraz ze wzrostem n. Jest to związane z rosnącą talią grafu $D(n, K)$. Problem rzędu przekształceń wielomianowych został szerzej omówiony w rozdziale 6.3 tej pracy.

Efektywność tego algorytmu jest zależna od sposobu zaimplementowania działań w wybranej grupie przekształceń (w szczególności złożenia) oraz sposobu potęgowania. Klisowski w [16] oszacował czas wykonania złożenia n wielomianów składających się na przekształcenie g^n przez $\mathcal{O}(n^{10})$ oraz przedstawił przykładowe czasy wykonania złożenia przekształceń dla różnych pierścieni i różnych typów przekształceń afinicznych (tabela 6.7). Przypadek I zawiera przekształcenia afiniczne $Ax + b$, gdzie S jest macierzą z jedynkami na przekątnej, odwracalnymi elementami w pierwszym wierszu i zerami poza. Przypadek II oznacza przekształcenia afiniczne ogólnego typu.

Tabela 6.7: Czas w ms złożenia ze sobą dwóch przekształceń wielomianowych — pierścienie $\mathbb{F}_{2^{16}}$, $\mathbb{Z}_{2^{16}}$, źródło [16]

n	przypadek I	przypadek II
	$D(n, \mathbb{F}_{2^{16}})$	
16	130	450
24	1120	3870
32	5400	19010
40	18370	72680
	$D(n, \mathbb{Z}_{2^{16}})$	
16	60	120
24	610	1320
32	3350	7690
40	12820	31240

6.5 Inne zastosowania i modyfikacje odwzorowań stabilnych w algorytmach z kluczem publicznym

Znaczny wkład w badanie zastosowań rodziny grafów $D(n, K)$ w algorytmach kryptograficznych mieli Klisowski i Romańczuk-Polubiec (algorytmy asymetryczne) oraz Kotorowicz (algorytmy symetryczne). Wykorzystując przedstawione w pracy (a wcześniej opublikowane) odwzorowania wielomianowe i ich stopnie, badali własności opartych na nich algorytmów, modyfikując niektóre z nich. W tym podrozdziale opiszemy w skrócie wyniki przez nich otrzymane wraz z własnymi pomysłami dotyczącymi rozszerzenia tych idei.

6.5.1 Zastosowanie odwzorowań stabilnych w kluczu publicznym

M. Klisowski w [16] zaproponował następującą zmianę podstawowego schematu szyfrowania z kluczem publicznym.

W podstawowym algorytmie opisanym poprzez ścieżkę w grafie (3.2) kolory kolejnych odwiedzanych wierzchołków możemy zapisać za pomocą następującego schematu:

$$x = x_1^0 \longrightarrow x_1^1 = x_1^0 + \alpha_1 \longrightarrow x_1^2 = x_1^1 + \alpha_2 + \cdots + x_1^s = x_1^{s-1} + \alpha_s = y,$$

gdzie dowolny wierzchołek może być postaci $v_i = (x_1^i, x_2^i, \cdots, x_n^i)$, α_i są elementami hasła (dla $i = 0, 1, 2, \cdots, s$), x - kolor pierwszego wierzchołka, y - kolor ostatniego wierzchołka.

Wprowadzona zmiana dotyczy sposobu obliczania kolejnych odwiedzanych wierzchołków. Powyższy ciąg kolorów zostaje zapisany w bardziej ogólny sposób:

$$x = x_0 \longrightarrow f_1(x) = x_1 \longrightarrow f_2(x) = x_2 \longrightarrow \ldots \longrightarrow f_{s-1}(x) = x_{s-1} \longrightarrow f_s(x) = y.$$

W celu poprawienia właściwości kryptograficznych, M. Klisowski używa funkcji f_i $1 \leq i \leq s$ następujących postaci:

1. $f_i(x) = a_i x + b_i$, $a_i, b_i \in K$
2. $f_i(x) = x^a + \alpha$, $\alpha \in K$, $a > 1$ – funkcja użyta tylko do wyznaczenia ostniego koloru.

Powyższe przypadki zostały zaimplementowane dla ciał skończonych w [16]. Parametry klucza zostały tak dobrane, aby przy znacznym zwiększeniu bezpieczeństwa nie pogorszyć efektywności algorytmów.

W tabeli 6.8 prezentujemy użycie wielomianu $f(x) + \alpha$ do uzyskania koloru ostatniego wierzchołka w grafie $D(n, \mathbb{F}_{2^3})$ w przypadku $f(x) = x^2$ oraz $f(x) = x^3$. W algorytmie zastosowano przekształcenie afiniczne w ogólnej postaci, jednokrotnie, po przejściu ścieżki w grafie. Porównajmy zatem liczbę jednomianów w przekształceniach odwrotnych dla wykładnika szyfrującego 2 i dla wykładnika 3. Można zauważyć w drugim przypadku, liczba jednomianów w wielomianowym przekształceniu deszyfrującym jest znacznie większa, przy nieznacznym wzroście liczby jednomianów przekształcenia szyfrującego. Fakt ten wpływa korzystnie na bezpieczeństwo algorytmów opartych na przekształceniach wielomianowych tego typu.

Naturalnym rozszerzeniem powyższej idei jest zastosowanie zaburzenia $f_\alpha(x)$, $\alpha, \in K$, $a > 1$ na pierwszej współrzędnej każdego kroku (nie tylko ostatniego), gdzie funkcja $f(x)$ jest funkcją nieliniową zależną od pierwszej współrzędnej pierwszego wierzchołka i odpowiedniego elementu hasła. Ciąg kolorów kolejno odwiedzanych wierzchołków można zapisać następująco:

$$x = x_0 \longrightarrow f_{\alpha_1}(x) = x_1 \longrightarrow f_{\alpha_2}(x) = x_2 \longrightarrow \ldots \longrightarrow f_{\alpha_3}(x) = x_{s-1} \longrightarrow f_{\alpha_s}(x) = x_s = y$$

Tabela 6.8: Użycie wielomianu $f(x)+\alpha$ do uzyskania koloru ostatniego wierzchołka w grafie $\mathbb{D}(n, \mathbb{F}_{2^3})$ dla różnych wielomianów f oraz długości klucza 7, źródło [16]

$f(x) = x^2$, $f^{-1}(x) = x^4$								
n	4	6	8	10	12	14	20	26
stopień	4	4	5	5	5	5	5	5
l. jednomianów	38	81	161	283	375	603	1335	2376
stopień prz. odwr.	6	6	6	6	6	6	6	6
l. jedn. prz. odwr.	86	352	1476	3880	5461	15282	72053	195382
$f(x) = x^3$, $f^{-1}(x) = x^5$								
n	4	6	8	10	12	14		
stopień	5	5	5	6	6	6		
l. jednomianów	44	78	162	312	377	706		
stopień prz. odwr.	7	7	7	7	7	7		
l. jedn. prz. odwr.	154	808	3802	34167	27836	461699		

Aby móc odszyfrować wiadomość w sposób jednoznaczny funkcja $f_\alpha(x)$ musi być funkcją wzajemnie jednoznaczną (bijekcją).

Przykład 6.4. Niech $K = F_p$, p - liczba pierwsza. Rozważmy przypadek zaburzenia na pierwszej współrzędnej postaci $f_{a,b}(x)$, gdzie $f(x) = ax^r + b$ dla $a \in F_p*$ i $b \in F$ takich, że $NWD(r, p-1) = 1$. w algortymie asymetrycznym (bez użycia przekształceń afinicznych) ostatni kolor $ax^r + b + \alpha_s$ stanowi pierwszą współrzędną szyfrogramu, czyli

$$ax^r + b = y_1.$$

Zatem odwzorowaniem odwrotnym w ciele skończonym F_p jest odwzorowanie postaci:

$$x = (\frac{y_1 - b}{a})^{r'},$$

gdzie $r' = r^{-1}$ w F_p.

Modyfikacja ta wprowadza korzystne dla algorytmów klucza publicznego zwiększenie stopni przekształceń wielomianowych do $3r$, co wynika ze złożenia przekształcenia opartego na ścieżce w grafie $D(n, K)$ (stopień 3) z funkcją f (stopień r). Niestety, następuje również zwiększenie liczby jednomianów. Problem ten można zminimalizować, używając odpowiednich przekształceń afinicznych w konstrukcji klucza publicznego. Zwiększenie

stopnia odwzorowania nie stanowi problemu w procesie deszyfrowania, które można dokonać stosując przejście w grafie, zamiast korzystania z jawnej postaci funkcji odwrotnej do przekształcenia szyfrującego.

6.5.2 Zastosowanie odwzorowań stabilnych w symbolicznym schemacie ElGamala

M. Klisowski w pracy [16] przedstawił i zbadał własności symbolicznej wersji systemu ElGamal, którą w skrócie możemy przedstawić następująco w trzech krokach:

1. Generowanie symbolicznego klucza
   - Alicja generuje parę przekształceń wielomianowych (g, g^{-1}), gdzie g jest generatorem grupy.
   - Alicja wybiera tajny wykładnik a i oblicza $\alpha := g^a$
   - Alicja generuje dwa klucze (g^{-1}, α) — publiczny, (a, α) — prywatny
2. Szyfrowanie (p — tekst jawny)
   - Bob wybiera tajny wykładnik szyfrujący b a następnie oblicza $c := \alpha^b(p)$ oraz $\beta := (g^{-1})^b$,
   - Bob otrzymuje szyfrogram postaci (c, β)
3. Deszyfrowanie
   - Alicja oblicza $p := \beta^a(c)$

Ustimenko na konferencji *The 16th Central European Conference on Cryptology* w 2016r. na Słowacji przedstawił kolejną modyfikację kryptosystemu ElGamala:

1. Generowanie symbolicznego klucza
   - Alicja generuje parę przekształceń wielomianowych (g, g^{-1}) (g jest generatorem grupy) oraz wybiera dwie pary nieliniowych (np. kwadratowych) wielomianów: Q_1 , Q_1^{-1} , Q_2 , Q_2^{-1}.
   - Alicja wybiera tajny wykładnik a i oblicza $G := Q_1^{-1} g^a Q_1$ oraz $H := Q_2^{-1} g^{-1} Q_2$
   - Alicja generuje dwa klucze (H, G) — publiczny, $(a, Q_1, Q_1^{-1}, Q_2, Q_2^{-1})$ — prywatny

2. Szyfrowanie (p — tekst jawny)

   - Bob wybiera tajny wykładnik szyfrujący b a następnie oblicza $c := G^b(p)$ oraz $y = H^b$,
   - Bob otrzymuje szyfrogram postaci (c, y)

3. Deszyfrowanie - w celu odzyskania tektu jawnego Alicja wykonuje następujące kroki:

   - $W_1 = Q_2 y Q_2^{-1}$
   - $W_2 = Q_1 W_1 Q_1^{-1}$
   - $W_2^a(c) = p$

Rozdział 7

Podsumowanie

Sedno rozprawy stanowią zebrane w całość wyniki pracy badawczej powstałe pod kierownictwem promotora prof. dr hab. Vasyla Ustimenko, opisujące użycie lingwistycznych układów dynamicznych opartych na grafach algebraicznych w kryptografii wielu zmiennych. Uzasadniony został poziom bezpieczeństwa zaproponowanych algorytmów poprzez analizę złożoności problemu znalezienia odwzorowania odwrotnego do nieliniowego, bijektywnego odwzorowania wielomianowego wielu zmiennych oraz problemu logarytmu dyskretnego. Przedstawione kolejno wersje odwzorowań były badane pod kątem różnych własności, w szczególności odporności na ataki i czasu wykonywanych obliczeń. Podczas realizacji rozprawy niektóre uprzednio uzyskane wyniki wymagały modyfikacji i dostosowania ich do aktualnych wymagań bezpieczeństwa, stosując m.in. technikę kompresji grafu. Opisane szczegółowo wielowymiarowe odwzorowania stabilne, w zależności od uzyskanych własności, zostały użyte w algorytmach symetrycznych, asymetrycznych oraz protokołach uzgadniania klucza Diffiego-Hellmana. Wprowadzone również zostały modyfikacje służące tworzeniu wielu kryptosystemów klucza publicznego, polegające na uzależnieniu ścieżek w grafie od specjalnych parametrów danych jako wielomiany wielu zmiennych zależnych od przestrzeni wektorowej.

Tematyka rozprawy stanowi część dużego projektu naukowego realizowanego przez grupę badawczą (M. Klisowski, J. Kotorowicz, M. Polak, U. Romańczuk-Polubiec, A. Wróblewska) pod kierunkiem prof. dr hab. Vasyla Ustimenko. Wyniki osiągane przez nasz zespół są na bieżąco weryfikowane i modyfikowane, co umożliwia dalszy rozwój badań w tym kierunku. Zaproponowane w pracy rodziny przekształceń wielomianowych nie

stanowią, na tym etapie badań, kompletnych narzędzi gotowych do zastosowania w wydajnych i bezpiecznych algorytmach kryptograficznych. Mimo to, przedstawione rezultaty mogą zapoczątkować podjęcie dalszych prac konstrukcyjnych, w celu poszukiwania nowych funkcji kryptograficznych o pożądanych własnościach. Potrzebna jest dokładniejsza analiza pod kątem implementacji, np. zastosowanie odpowiednich technik przyspieszających działanie algorytmów poprzez wykorzystanie komputerów równoległych bądź wielordzeniowych. W przyszłości można jeszcze kontynuować badania nad parametrami algorytmu, takimi jak użyte przekształcenia afiniczne, pierścień czy wymiar przestrzeni.

7.1 Elementy wkładu oryginalnego

W poniższych punktach przedstawione zostały oryginalne elementy pracy:

1. Wprowadzenie pojęcia grup stabilnych, w szczególności rodziny podgrup stabilnych grupy Cremona w przypadku pierścieni przemiennych (1.6). Istnienie tego typu grup umożliwiło użycie przekształceń wielomianowych w konstrukcji lingwistycznych układów dynamicznych.

2. Uogólnienie lingwistycznych układów dynamicznych, poprzez zapisanie ciągu kolorów w sposób rekurencyjny (3.5). Zdefiniowanie lingwistycznych układów dynamicznych z zaburzeniem (3.6).

3. Konstrukcja i analiza własności (w szczególności stopni) lingwistycznych układów dynamicznych, powstałych przez użycie własności następujących przekształceń wielomianowych:

    - konstrukcja podstawowa - kubiczne przekształcenia wielomianowe (4.1),
    - przekształcenia wielomianowe stopnia 3 i 4, oparte na grafach skierowanych (konstrukcja polegająca na łączeniu wierzchołków grafu w grupy - rozdział 4.2 oraz 4.4),
    - uogólnienie powyższych konstrukcji z użyciem liniowych symetrii - grupy automorfizmów grafu skierowanego (4.3),
    - kwadratowe przekształcenia wielomianowe, otrzymane przez zastosowanie równań opisujących spójne składowe grafu (4.5).

4. Konstrukcja i analiza własności lingwistycznych układów dynamicznych opartych na rodzinach przekształceń stopnia większego niż 4, powstałych przez procedurę kompresji grafu (5.1).

5. Opis oraz analiza własności rodziny przekształceń wielomianowych z nieliniowym zaburzeniem na pierwszej współrzędnej - podczas zmiany koloru wierzchołka (5.2). Poprzez dobór odpowiedniego zaburzenia możemy regulować stopniem przekształcenia i przekształcenia do niego odwrotnego.

6. Analiza możliwości zastosowania wraz z przykładami poszczególnych rodzin przekształceń wielomianowych dużego rzędu w zagadnieniach kryptograficznych, takich jak algorytmy z kluczem prywatnym i publicznym, czy protokół uzgadniania klucza Diffiego-Hellmana (6). Wskazanie zalet i wad poszczególnych rodzin w praktycznych zastosowaniach:

    - rodziny przekształceń mniejszych stopni – zastosowanie w kryptografii symetrycznej oraz wymianie klucza (ze względu na bezpieczeństwo i efektywność); w kryptografii asymetrycznej – możliwe ataki linearyzacji,
    - rodziny przekształceń większych stopni – zastosowanie w kryptografii asymetrycznej (niemożliwe ataki linearyzacji), mniejsza efektywność algorytmów.
    - rodziny przekształceń z ustalonym stopniem – odpowiednie użycie funkcji zaburzającej daje możliwość regulowania stopniem przekształcenia odwrotnego.

Spis rysunków

Spis tabel

Oznaczenia

$\mathrm{AGL}_n(K)$	Grupa afiniczna
$\mathbb{B}_n$	Pierścień Boole'a mający 2^n elementów
$\mathrm{char}(K)$	Charakterystyka pierścienia K
$\mathrm{E}(G)$	Zbiór krawędzi grafu G
$\mathbb{F}_q$	Ciało skończone q-elementowe
$\mathrm{g}(G)$	Talia (obwód) grafu G
$\mathrm{GL}_n(K)$	Ogólna grupa liniowa - zbiór wszystkich macierzy odwracalnych stopnia n nad ustalonym ciałem K
$\mathbb{N}$	Zbiór liczb naturalnych: $\{0, 1, 2, \dots\}$
$\mathrm{Reg}(K)$	Zbiór elementów regularnych pierścienia K, tzn. nie bedących dzielnikami zera w K
$\S_n$	Grupa permutacji (grupa symetryczna)
$\mathrm{S}(A)$	Grupa symetryczna zbioru A
$\mathrm{V}(G)$	Zbiór wierzchołków grafu G
$\mathbb{Z}$	Zbiór liczb całkowitych
$\mathbb{Z}_m$	Pierścień klas reszt modulo m
$\mathbb{Z}_m^*$	Multiplikatywna grupa klas reszt modulo m
$\mathbb{Z}_+$	Zbiór liczb całkowitych dodatnich
$C(K^n)$	Grupa Cremona
$K[x]$	Pierścień wielomianów jednej zmiennej x nad pierścieniem K
$K[x_1, x_2, \dots, x_n]$	Pierścień wielomianów n zmiennych nad pierścieniem K

Bibliografia

[1] C. Bagiński. *Wstęp do teorii grup*. SCRIPT, Warszawa, 2002.

[2] J. Bednarczuk. *Urok przekształceń afinicznych*. Wydawn. szkolne i pedagogiczne, Warszawa, 1978.

[3] M. Berger. *Geometry I*. Springer-Verlag Berlin Heidelberg, 1987.

[4] N. Biggs. *Graphs with large girth*, wolumen C. Ars Combinatoria, 1987.

[5] B. Bollobás. *Extremal Graph Theory*. Academic Press, London, 1978.

[6] L. E. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Annals of Mathematics*, 11(1/6):65–120, 1896.

[7] W. Diffie, M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, 1976.

[8] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[9] W. J. Gilbert, K. W. Nicholson. *Algebra współczesna z zastosowaniami*. Wydawnictwa Naukowo-Techniczne, Warszawa, 2008.

[10] P. Guinand, J. Lodge. Graph theoretic construction of generalized product codes. *Proceedings of the 1997 IEEE International Symposium on Information Theory ISIT '97, Ulm, Germany*, strony 111–112, 1997.

[11] P. Guinand, J. Lodge. Tanner type codes arising from large girth graphs. *Proceedings of the 1997 Canadian Workshop on Information Theory CWIT '97, Toronto, Ontario, Canada*, strony 5–7, 1997.

[12] T. Habutsu, Y. Nishio, I. Sasase, S. Mori. A secret key cryptosystem by iterating a chaotic map. *EUROCRYPT '91*, wolumen 547 serii *Lecture Notes in Computer Science*, strony 127–140. Springer, 1991.

[13] M. Hasler, Y. Maistrenko. An introduction to the synchronization of chaotic systems: coupled skew tent maps. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions*, 44(10):856–866, 1997.

[14] J. Hoffstein, J. Pipher, J. Silverman. *An Introduction to Mathematical Cryptography*. Springer Publishing Company, Incorporated, wydanie 1, 2008.

[15] T. Kapitaniak. *Chaos for engineers, theory and applications*. Springer, 2000.

[16] M. Klisowski. *Zwiększenie bezpieczeństwa kryptograficznych algorytmów wielu zmiennych bazujących na algebraicznej teorii grafów*. Rozprawa doktorska, Politechnika Częstochowska, Częstochowa, 2014.

[17] M. Klisowski, U. Romańczuk, V. Ustimenko. The implementation of cubic public keys based on a new family of algebraic graphs. *Annales UMCS, Informatica*, 11(2):127–141, 2011.

[18] M. Klisowski, V. Ustimenko. On the implementation of public keys algorithms based on algebraic graphs over finite commutative rings. *IMCSIT*, strony 303–308, 2010.

[19] M. Klisowski, V. Ustimenko. On the implementation of cubic public keys based on algebraic graphs over the finite commutative rings and their symmetries. *Albanian Journal of Mathematics*, 5(3), 2011.

[20] M. Klisowski, V. Ustimenko. On the comparison of cryptographical properties of two different families of graphs with large cycle indicator. *Mathematics in Computer Science*, 6(2):181–198, 2012.

[21] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer, wydanie drugie, 1994.

[22] N. Koblitz. *Algebraic aspects of cryptography, Algorithms and Computation in Mathematics*. Springer, 1998.

[23] L. J. Kocarev, K. Halle, K. Eckert, L. Chua, U. Parlitz. Experimental demonstration of secure communications via chaos synchronization. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, 2(3):709–716, 1992.

[24] Z. Kotulski, J. Szczepański. Discrete chaotic cryptography. *Annalen der Physik*, 6:381–394, 1997.

[25] K. Kymakya, W. Halang, H. Unger. *Recent Advances in Nonlinear Dynamics and Synchronization Theory*. Springer, 2009.

[26] S. Lang. *Algebra*. Addison-Wesley, Menlo Park Cal, 1993.

[27] F. Lazebnik, V. Ustimenko, A. Woldar. A characterization of the components of the graphs $d(k, q)$. *Discrete Mathematics*, 157(1-3):271 – 283, 1996.

[28] F. Lazebnik, V. A. Ustimenko. Some algebraic constructions of dense graphs of large girth and of large size. *DIMACS Series Discrete Math. Theoret. Comput. Sci.*, 10:75–93, 1993.

[29] F. Lazebnik, V. A. Ustimenko. Explicit construction of graphs with an arbitrary large girth and of large size. *Discrete Applied Mathematics*, 60(1-3):275–284, 1995.

[30] F. Lazebnik, V. A. Ustimenko, A. J. Woldar. A new series of dense graphs of high girth. *Bull. Amer. Math. SIC.*, 32:73–79, 1995.

[31] F. Lazebnik, V. A. Ustimenko, A. J. Woldar. Polarities and 2k-cycle-free graphs. *Discrete Mathematics*, 197/198:503–513, 1999.

[32] R. Lidl. On cryptosystems based on polynomials and finite fields. T. Beth, N. Cot, I. Ingemarsson, redaktorzy, *Advances in Cryptology*, wolumen 209 serii *Lecture Notes in Computer Science*, strony 10–15. Springer Berlin Heidelberg, 1985.

[33] R. Lidl, W. Möller. Permutation polynomials in RSA-cryptosystems. D. Chaum, redaktor, *Advances in Cryptology*, strony 293–301. Springer US, 1984.

[34] R. Lidl, G. L. Mullen. When does a polynomial over a finite field permute the elements of the fields? *Am. Math. Monthly*, 95(3):243–246, Mar. 1988.

[35] R. Lidl, H. Niederreiter. *Finite Fields*. Number 20 serii Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[36] A. Lubotsky, R. Philips, P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[37] G. A. Margulis. Explicit construction of graphs without short cycles and low density codes. *Combinatorica*, 2:71–78, 1982.

[38] T. Matsumoto, H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. *Advances in Cryptology - EUROCRYPT 1988*, wolumen 330 serii *Lecture Notes in Computer Science*, strony 419–453. Springer Berlin Heidelberg, 1988.

[39] A. J. Menezes, S. A. Vanstone, P. C. V. Oorschot. *Handbook of Applied Cryptography.* CRC Press, Inc., Boca Raton, FL, USA, wydanie 1st, 1996.

[40] E. H. Moore. Tactical memoranda i-iii. *American Journal of Mathematics*, 18:264–303, 1896.

[41] C. H. Papadimitriou. *Computational complexity.* Academic Internet Publ., 2007.

[42] U. Parlitz, L. Chua, L. Kocarev, K. Halle, A. Shang. Transmission of digital signals by chaotic synchronization. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, 2:973–977, 1992.

[43] L. Pecora, T. L. Caroll. Synchronization in chaotic systems. *Physical Review Letters*, 64(8):821–824, 1990.

[44] U. N. Peled, I. Perepelitsa, V. Pless, S. Friedland, J.-L. Kim. Explicit construction of families of ldpc codes with no 4-cycles. *Information Theory, IEEE Transactions*, 50(10):2378 –2388, 2004.

[45] A. Pikovsky. *Synchronization Theory and application*, wolumen 109 serii *Nato Science Series II.* Springer Netherlands, 2003.

[46] A. Pikovsky, Y. M. Editors. Synchronization: Theory and application. *Proceedings of Advanced Studies NATO Institute*, strony 419–453. Kluwer Academic Publishers, 2003.

[47] R. L. Rivest. Permutation polynomials modulo 2^w. *Finite Fields and Their Applications*, 7(2):287 –292, 2001.

[48] R. L. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[49] U. Romańczuk, V. Ustimenko. On the key exchange with new cubical maps based on graphs. *Ann. UMCS, Inf.*, 11(4):11–19, 2011.

[50] U. Romańczuk-Polubiec, V. Ustimenko. On two windows multivariate cryptosystem depending on random parameters. *Algebra Discrete Math.*, 19:101–129, 2015.

[51] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[52] J. H. Silverman. *A friendly introduction to number theory; 3rd ed.* Prentice-Hall, Upper Saddle River, NJ, 2006.

[53] A. Stefański. *Determining Thresholds of Complete Synchronization and Application*, wolumen 67 serii *Nonlinear Science Series A*. World Scientific, 2009.

[54] V. Ustimenko. Cryptim: Graphs as tools for symmetric encryption. S. Boztaş, I. E. Shparlinski, redaktorzy, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, wolumen 2227 serii *Lecture Notes in Computer Science*, strony 278–286. Springer Berlin Heidelberg, 2001.

[55] V. Ustimenko. On linguistic dynamical systems, families of graphs of large girth, and cryptography. *Journal of Mathematical Sciences*, 140(3):461–471, 2007.

[56] V. Ustimenko. On the graph based cryptography and symbolic computations. *Proceedings of International Conference on Application of Computer Algebra, ACA-2006*, wolumen 1, strony 131–156. Serdica Journal of Computing, 2007.

[57] V. Ustimenko. On the k - theory of graph based dynamical systems and its applications. *Dopovidi National Academy of Sci of Ukraine*, (8):44–51, 2013.

[58] V. Ustimenko, S. Kotorowicz. On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings. *Condesed Matter Physics*, 11(2(54)):347–360, 2008.

[59] V. Ustimenko, U. Romańczuk. On dynamical systems of large girth or cycle indicator and their applications to multivariate cryptography. X. Yang, redaktor, *Artificial*

Intelligence, Evolutionary Computing and Metaheuristics - In the Footsteps of Alan Turing, wolumen 427 serii *Studies in Computational Intelligence*, strony 231–256. Springer, 2013.

[60] V. Ustimenko, U. Romańczuk. On extremal graph theory, explicit algebraic constructions of extremal graphs and corresponding turing encryption machines. X. Yang, redaktor, *Artificial Intelligence, Evolutionary Computing and Metaheuristics - In the Footsteps of Alan Turing*, wolumen 427 serii *Studies in Computational Intelligence*, strony 257–285. Springer, 2013.

[61] V. Ustimenko, A. Touzene. Cryptall: System to encrypt all types of data. *Notices of Kiev Mohyla Academy*, 2004.

[62] V. Ustimenko, A. Wróblewska. On the key exchange with nonlinear polynomial maps of degree 4. *Proceedings of Applications of Computer Algebra 2010, Vlora*, wolumen 4, strony 161–170. Albanian Journal of Mathematics, 2010.

[63] V. Ustimenko, A. Wróblewska. On the key expansion of d(n;k)-based cryptographical algorithm. *Annales UMCS, Informatica*, 11(2):95–111, 2011.

[64] V. Ustimenko, A. Wróblewska. Dynamical systems as the main instrument for the constructions of new quadratic families and their usage in cryptography. *Annales UMCS, Informatica*, 12(3):65–74, 2012.

[65] V. Ustimenko, A. Wróblewska. On some algebraic aspects of data security in cloud computing. *Proceedings of Applications of Computer Algebra (ACA 2013), Malaga*, strony 144–147, 2013.

[66] V. Ustimenko, A. Wróblewska. On the key exchange and multivariate encryption with nonlinear polynomial maps of stable degree. *Annales UMCS, Informatica*, 13(1):63–80, 2013.

[67] V. Ustimenko, A. Wróblewska. On the key exchange with nonlinear polynomial maps of stable degree. *CoRR*, abs/1304.2920, 2013.

[68] V. Ustimenko, A. Wróblewska. On new examples of families of multivariate stable maps and their cryptographical applications. *Annales UMCS, Informatica*, 14(1):19–35, 2014.

[69] V. A. Ustimenko. Coordinatisation of regular tree and its quotients. wolumen 2 serii *Voronoi's Impact on Modern Science*, strony 125–152. National Academy of Sciences of Ukraine, Institute of Mathematics, 1998.

[70] V. A. Ustimenko. Graphs with special arcs and cryptography. *Acta Applicandae Mathematicae*, 74:117–153, 2002.

[71] V. A. Ustimenko. Maximality of affine group, and hidden graph cryptosystems. *Algebra and Discrete Mathematics*, 2005(1):133–150, 2005.

[72] V. A. Ustimenko. On the extremal graph theory for directed graphs and its cryptographical applications. T. Shaska, W. C. Huffman, D. Joyner, V. Ustimenko, redaktorzy, *Advances in Coding Theory and Cryptography*, wolumen 3 serii *Series on Coding Theory and Cryptology*, strony 181–199. World Scientific, 2007.

[73] V. A. Ustimenko. On the cryptographical properties of extremal algebraic graphs. *Algebraic Aspects of Digital Communications, NATO Science for Peace and Security*, wolumen 24 serii *Series - D: Information and Communication Security,*. 2009.

[74] V. A. Ustimenko, Y. M. Khmelevsky. Walks on graphs as symmetric or asymmetric tools to encrypt data. *The South Pacific Journal of Natural and Applied Sciences*, 2002.

[75] A. Wróblewska. On some properties of graph based public keys. *Albanian Journal of Mathematics*, 2(3):229–234, 2008.

Streszczenie

Rozprawa doktorska ma na celu analizę algorytmów kryptograficznych powstałych dzięki użyciu lingwistycznych układów dynamicznych opartych na grafach algebraicznych. Użycie specjalnych układów dynamicznych jest motywowane wygenerowaniem specjalnych podgrup grupy Cremona działających na modułach wolnych ogólnego wymiaru n nad pierścieniem przemiennym. Takie podgrupy zawierają grupy cykliczne dużego rzędu, składające się z nieliniowych wielomianowych przekształceń ustalonego stopnia. Skonstruowane zostały różne rodzaje przekształceń stabilnych i badane były ich własności pod kątem zastosowania w kryptografii, takie, jak stopień, rząd czy liczba jednomianów. Przekształcenia niskich stopni mogą mieć zastosowanie w kryptografii symetrycznej. Rosnący rząd oraz stabilny stopień przekształceń sprawiają, że mogą one zostać użyte w algorytmach wymiany kluczy Diffiego-Hellmana. Pod kątem zastosowania w algorytmach asymetrycznch, dokonaliśmy pewnych modyfikacji przekształceń wielomianowych, aby uzyskać zwiększenie odporności na ataki linearyzacji, przy jednoczesnej poprawie efektywności badanych algorytmów.

Abstract

The aim of this thesis is to analyze cryptographic algorithms created by the use of linguistic dynamic systems based on algebraic graphs. The use of special dynamical systems is motivated by generating specific subgroups of the Cremona acting on free modules dimension n over the commutative ring. These subgroups include the high order cyclic groups consisting of a nonlinear polynomial transformations of a prescribed degree. We have constructed various types of stable transformations and tested their properties for use in cryptography, such as the degree, order or number of monomials. Transformation of low degree can be used in symmetric cryptography. Growing order and a stability of transformation, makes that it may be used in the algorithms Diffie-Hellman for key exchange . For use in asymmetric algorithms, we made some modifications of polynomial transformations to obtain increased resistance to attacks linearisation, while improving the efficiency of the tested algorithms.