Parametry systemów klucza publicznego

Andrzej Chmielowiec

Instytut Podstawowych Problemów Techniki
Polskiej Akademii Nauk

24 marca 2010

Idea klucza publicznego

1. Wysyłanie klucza publicznego

2. Wysyłanie wiadomości zaszyfrowanej kluczem publicznym

3. Odszyfrowanie wiadomości przy użyciu klucza prywatnego

Podpis cyfrowy

- Uwierzytelnienie serwera WWW przed użytkownikiem (bankowość elektroniczna, sklepy internetowe).
- Logowanie do systemu informatycznego.
- Oprogramowanie i sterowniki urządzeń.

Szyfrowanie danych

- Wymiana symetrycznych kluczy sesyjnych (bankowość elektroniczna, sklepy internetowe).
- Szyfrowanie wiadomości elektronicznych bez konieczności wcześniejszego uzgadniania klucza.
- Nawiązywanie bezpiecznych połączeń typu SSH.

Opis algorytmu

Losowo wybieramy liczby pierwsze p, q i wyznaczamy $N = pq$.
Znajdujemy taką liczbę e, że $NWD(e, (p-1)(q-1)) = 1$
i wyznaczamy takie d, że $ed \equiv 1 \bmod (p-1)(q-1)$.

- Szyfrowanie (weryfikacja podpisu):

$$c \equiv m^e \bmod N.$$

- Deszyfrowanie (podpisywanie):

$$m \equiv c^d \bmod N.$$

Bezpieczeństwo – problem faktoryzacji

Bezpieczeństwo RSA oparte jest na problemie rozkładu liczby N na czynniki pierwsze. Łatwo zauważyć, że jeśli ktoś zna liczby p i q takie, że $N = pq$, to z łatwością znajdzie klucz publiczny

$$d \equiv e^{-1} \bmod (p-1)(q-1).$$

Najszybszym znanym algorytmem faktoryzacyjnym jest *Sito Ciał Liczbowych* (NFS), którego złożoność określa poniższa formuła

$$exp\left(c_0 N^{1/3} \left(\log(N \log 2)\right)^{2/3}\right).$$

Do tej pory nie wykazano, czy problem faktoryzacji i złamania RSA są sobie równoważne.

Wydajność – generowanie kluczy

Najbardziej czasochłonną operacją podczas generowania klucza jest znalezienie dwóch liczb pierwszych p i q. Operacja ta ma złożoność $O(\log(p)^4)$ – o ile stosowane są probabilistyczne metody testowania pierwszości.

Dodatkowe warunki na czynniki pierwsze dla modułu RSA:

1. $p-1=2p'$, $\quad p+1=2p''$,
2. $q-1=2q'$, $\quad q+1=2q''$.

Wydajność – wykonywanie operacji

Znajomość czynników liczy N pozwala na przyspieszenie operacji prywatnej. Z twierdzenia chińskiego o resztach wynika bowiem izomorfizm

$$\mathbb{Z}/N\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Powyższy izomorfizm daje możliwość czterokrotnego przyspieszenia obliczeń

$$y \equiv x^d \bmod N \iff \begin{cases} y \equiv x^{d \bmod (p-1)} \bmod p, \\ y \equiv x^{d \bmod (q-1)} \bmod q. \end{cases}$$

Co to są punkty stałe

Punktem stałym przekształcenia RSA nazwiemy taką liczbę x, dla której zachodzi

$$x^e \equiv x \bmod N.$$

Łatwo zauważyć, że skoro $x^{ed} \equiv x \bmod N$, to

$$x^e \equiv x \bmod N \iff x^d \equiv x \bmod N.$$

Oznacza to, że punkt stały przekształcenia publicznego jest również punktem stałym przekształcenia prywatnego.

Czy duża liczba punktów stałych jest dobra?

Punkty stałe prowadzą do znalezienia czynników

$$x^e \equiv x \bmod N$$

$$x^{e-1} \equiv 1 \bmod N$$

$$x^{e-1} - 1 \equiv 0 \bmod N$$

$$(x^{\frac{e-1}{2}} - 1)(x^{\frac{e-1}{2}} + 1) \equiv 0 \bmod N$$

$$N \mid (x^{\frac{e-1}{2}} - 1)(x^{\frac{e-1}{2}} + 1)$$

Z dużym prawdopodobieństwem $NWD(N, (x^{\frac{e-1}{2}} \pm 1))$ będzie równe p lub q.

Oczekiwana liczba punktów stałych dla RSA (1)

Jeśli $(u, v) \in U^2$, to prawdopodobieństwo graniczne tego, że $NWD(u, v) = 1$ wynosi

$$P_1 = \lim_{|U| \to \infty} P(U) = \frac{6}{\pi^2}.$$

Jeśli ponadto przez P_B oznaczymy graniczne prawdopodobieństwo tego, że $NWD(u, v) \leq B$, to prawdziwa jest następująca zależność

$$P_B = P_1 \cdot \sum_{d=1}^{B} \frac{1}{d^2}.$$

Oczekiwana liczba punktów stałych dla RSA (2)

Prawdopodobieństwo wylosowania dwóch względnie pierwszych liczb ze zbioru $\{1, 2, \ldots, N\}$ możemy oszacować przez

$$P_1 + \varepsilon_N,$$

gdzie $\varepsilon_N < 4\frac{\ln N}{N}$. Na tej podstawie możemy wyrazić oczekiwaną liczbę punktów stałych RSA

$$\mathrm{ES} \leq \left(\frac{3(P_1 + \varepsilon_{\sqrt{N}})(2 + \ln N)}{2} \right)^2 = O(\ln^2 N)$$

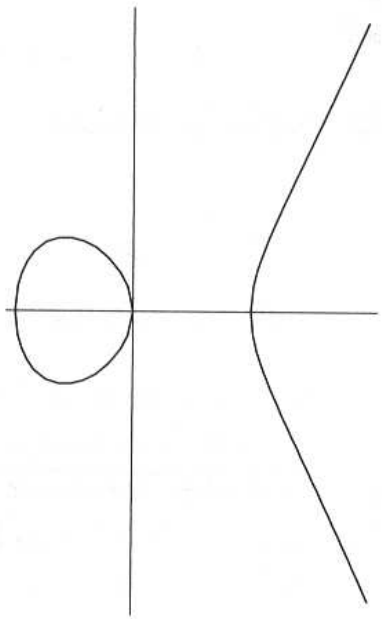
oraz oszacować prawdopodobieństwo trafienia w taki punkt

$$P = O\left(\frac{\ln^2 N}{N} \right).$$

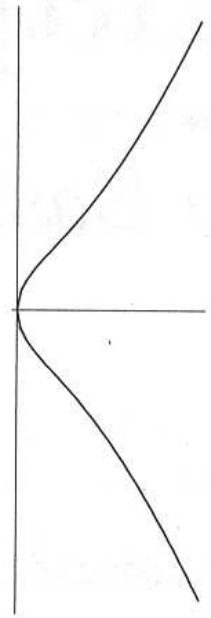
Krzywa eliptyczna

Jednorodne równanie Weierstrassa:

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$



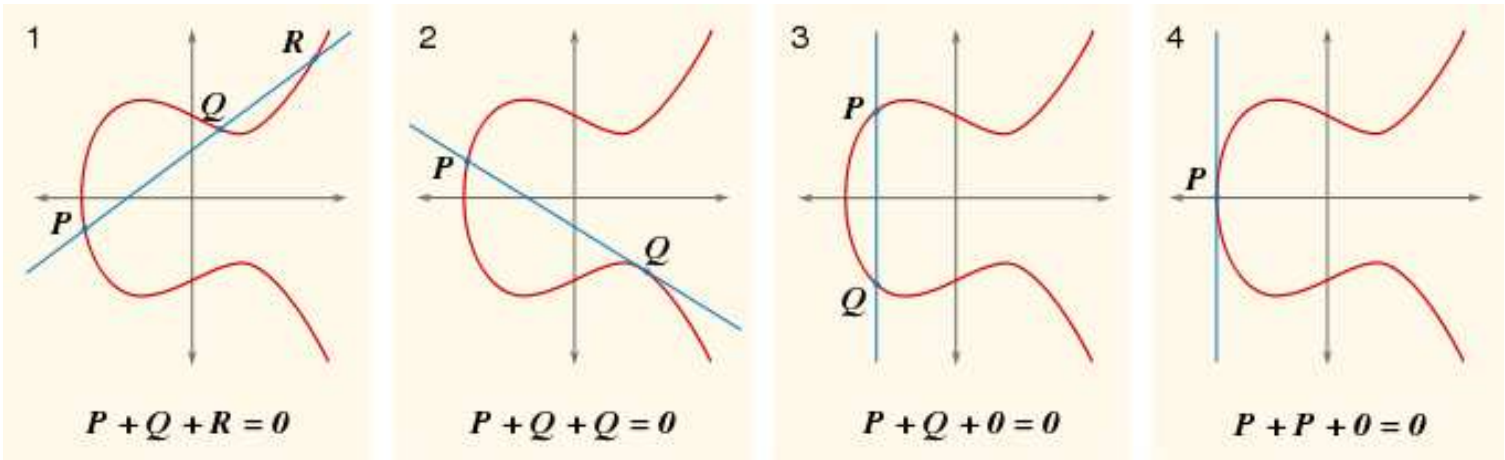
$(a) \quad y^2 = x^3 - x$



$(b) \quad y^2 = x^3 + x$

Grupa punktów krzywej eliptycznej

Punkty krzywej eliptycznej tworzą grupę.



Problem logarytmu dyskretnego

Niech G będzie grupą cykliczną, w której element g jest generatorem. Logarytmem dyskretnym z elementu $h \in G$ nazywamy taką liczbę x, dla której spełnione jest równanie

$$g^x = h.$$

Znalezienie logarytmu dyskretnego jest w ogólności zadaniem obliczeniowo trudnym. W szczególności najszybsza metoda pozwalająca na jego wyznaczenie w grupie punktów krzywej eliptycznej ma złożoność

$$2^{r/2},$$

gdzie r jest największym dzielnikiem pierwszym rzędu generatora.

Algorytm ECDH

Uzgadnianie wspólnego sekretu metodą Diffiego-Hellmana

A		B
g^a	$\rightarrow$	
	$\leftarrow$	g^b
$h = \left(g^b\right)^a = g^{ab}$		$h = \left(g^a\right)^b = g^{ab}$

Czy każdej krzywej można użyć do celów kryptograficznych?

Aby krzywa nadawała się do zastosowań kryptograficznych musi spełnić szereg warunków, które są weryfikowane na podstawie liczby jej punktów. Dlatego też zliczenie punktów krzywej jest pierwszą czynnością, jaka jest wykonywana podczas sprawdzania przydatności krzywej eliptycznej.

W szczególności wybierane są tylko te krzywe, których liczba punktów podzielna jest przez dużą liczbę pierwszą.

Algorytmy zliczania punktów

Zliczanie punktów krzywej zdefiniowanej nad ciałem charakterystyki 2

- algorytm Satoh,
- algorytm AGM (Algebraic Geometry Method).

Zliczanie punktów krzywej zdefiniowanej nad ciałem charakterystyki $p > 3$

- algorytm Schoofa,
- algorytm SEA (Schoof-Elkies-Atkin).

Operacje wykonywane podczas zliczania punktów

Znakomita większość operacji podczas zliczania punktów metodą SEA wykonywana jest na wielomianach lub formalnych szeregach potęgowych modulo p.

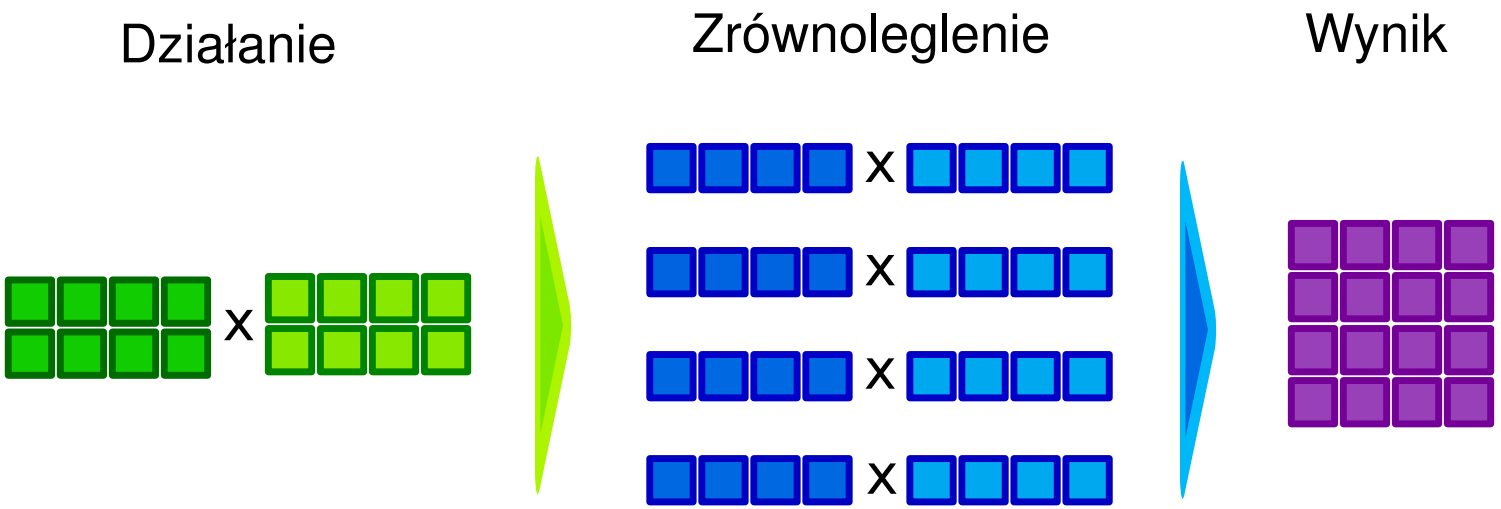
Najbardziej czasochłonna jest faza preobliczeń wstępnych podczas których konieczne jest operowanie na szeregach mających nawet po kilkaset tysięcy współczynników.

Dlatego warto zastosować techniki mnożenia bazujące na FFT oraz zastanowić się nad możliwością zrównoleglenia obliczeń.

Szybka arytmetyka w pierścieniu szeregów potęgowych (1)

$$\mathbb{Z}[[X]] \quad \rightarrow \quad \left| \begin{array}{c} \textbf{Równoległe FFT} \\ \mathbb{F}_{p_1}[[X]] \\ \vdots \\ \mathbb{F}_{p_i}[[X]] \\ \vdots \\ \mathbb{F}_{p_k}[[X]] \end{array} \right| \quad \rightarrow \quad \mathbb{Z}[[X]]$$

Szybka arytmetyka w pierścieniu szeregów potęgowych (2)



Szybka arytmetyka w pierścieniu szeregów potęgowych (3)

1. Współczynniki pojedynczej precyzji:
   - koszt klasycznego mnożenia FFT – n^2,
   - koszt mnożenia FFT-CRT – $2n^2$.
2. Współczynniki podwójnej precyzji:
   - koszt klasycznego mnożenia FFT – $4n^2$,
   - koszt mnożenia FFT-CRT – $4n^2$.
3. Współczynniki czterokrotnej precyzji:
   - koszt klasycznego mnożenia FFT – $16n^2$,
   - koszt mnożenia FFT-CRT – $8n^2$.
4. Współczynniki ośmiokrotnej precyzji:
   - koszt klasycznego mnożenia FFT – $64n^2$,
   - koszt mnożenia FFT-CRT – $16n^2$.

Szybka arytmetyka w pierścieniu szeregów potęgowych (4)

Jeśli przyjąć, że n jest liczbą współczynników, a k jest liczbą cyfr jaką ma największy współczynnik, to złożoność zaproponowanego algorytmu jest następująca:

$$c_1 k^2 n + kn(2 + 3\log(n)) + c_2 k^2 n$$

Jak widać dla dużych k bardziej opłacalne będzie zastosowanie również metody FFT do mnożenia poszczególnych współczynników. Wtedy złożoność wyniesie

$$O(k\log(k)n\log(n)).$$

Proponowana metoda jest zatem opłacalna jedynie w przypadku współczynników o umiarkowanym rozmiarze.

Podsumowanie (1)

Oszacowanie liczby punktów stałych dla losowych parametrów RSA.

- Pozwala na oszacowanie z jakim prawdopodobieństwem wylosujemy słaby klucz.
- Uzyskany wynik może być wykorzystany w praktyce do ograniczenia liczby dodatkowych warunków, które są nakładane na czynniki modułu (możliwość przyspieszenia procesu generowania kluczy).

Podsumowanie (2)

Szybka arytmetyka w pierścieniu szeregów potęgowych.

- Zwiększa szybkość algorytmu zliczania punktów krzywej. Daje to możliwość szybkiego generowania *własnych* krzywych eliptycznych.
- Opracowana technika może mieć zastosowanie również w innego typu obliczeniach, które wykorzystują operacje w pierścieniu szeregów potęgowych. Jej ogromną zaletą jest łatwość zrównoleglania obliczeń.