Cryptographic protocol for electronic auctions with extended requirements.

Bogdan Księżopolski[1], Zbigniew Kotulski[2]

[1]*Institute of Physics, M. Curie-Skłodowska University,*
Pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland
e-mail: bogdan@kft.umcs.lublin.pl
[2]*Institute of Fundamental Technological Research, Polish Academy of Sciences,*
Świętokrzyska ul. 21, 00-049 Warsaw, Poland
e-mail: zkotulsk@ippt.gov.pl

Abstract

In this paper we present a cryptographic protocol which is the realization of an electronic auction being the component of the e-government system. This cryptographic protocol fulfils all the functions of the classic auction and additionally, by use of cryptographic primitives, enhances the protection of information. The characteristic features of the protocol are: the incontrovertibility of participants and offers, data integrity, confidence of bids, anonymity of the winning bidder, public verification of the result of auction and confirmation of taking part in the auction.

1. Introduction

At present, traditional methods in public administration become insufficient, because they lead to the decision mechanisms that are time-consuming, expensive, inconvenient for customers as well as susceptible on abuse. The philosophy of modern state [1] founds that any information is being passed in a fast way. We mean: taking and transmitting the printings, quick correction of data, changes of legal controls, quicker treat of decision. Comparing classic computer solutions with traditional ones we can notice the considerable advantages from usage of the second variant. For example, classic execution auction carries behind the costs of notice of auction, mail of information, human costs (checking offers), filing, and moreover, it is then a time-consuming process as well as weakly resistant on abuse. In this new approach we can tell about low costs, whole process is being hold virtually, we save on filing of data, the whole process is being accelerated, it gathers transparency and applying cryptographic methods we can exclude every abuses, in cryptography considered as attacks.

In this paper we present the cryptographic protocol, which let us possible to realize the auction in a virtual way and, additionally, assures the high protection of information taking the part in this process.

2. Electronic auctions

Now, we can notice the development of e-commerce, which is extensively manifested in internet shops, e-banks, electronic auctions as well as many other forms. To realize services mentioned above we use different cryptographic protocols, which take care both about correctness and the safety of the information sent during the electronic communication process. Concerning e-auction, we should also pay attention to all mechanisms that must be used to make the auction possible.

We distinguish several different types of electronic auctions (analogously as in their traditional form). The most popular are: *English, 1st Price Sealed - Bid, Vickrey, Dutch.*

Type *English* is the most widespread. It consist in auctioning the price for a given good. The price grows till time when it will stay only one person taking part in auction, during when different will resign.

Type *1st Price Sealed-Bid* consist in declaring the price for given goods independently by every bidder. Person who will declare the highest price wins goods and he is obliged to pay the price introduced by himself.

Type *Vickrey*, alternatively called *2nd Price Sealed - Bid*, is very similar to the previous model. The difference consist in wining the auction by person, who declared the highest sum

for given goods, but he pays second highest in order.
Type *Dutch* consist in starting the auction with the highest possible price and decreasing the requested price until some bidder agrees to pay it. This bidder wins the auction with the price by which the auction was stopped.

Every of the introduced auction models possesses many cryptographic protocols realizing it, each characterized with different computation and communication complexity.

To realize the auction with extended properties we can use the *1st Price Sealed – Bid* auction model.

3. The 1st Price Sealed - Bid auction model.

Type *the 1st Price Sealed Bid* is the model, on the ground of which came into many cryptographic protocols [2,3,4,6], which present the different degree of complexity. Thanks to him we get the different level of protection of information. Protocols possess individual requirements, which are solved by different techniques.
In our case we should pay attention on some features.

3.1. The communication computational requirements

Cryptographic protocols consist with different phases, during which all operations are executed. They can base on the communication steps, that is the transmission of information among participants of given protocols. Different working is making calculations which need suitable computing power. Usually both methods are united, essential difference between cryptographic protocols is the relation of executed calculations to number of necessary connections between participants.

3.2 The way of the price settlement

Another essential element is the way of the settlement of the price. Some cryptographic protocols [2,7] possess the list of prices and the bidder can choose only concrete price value. Different [8] make possible the choice of prices but it is usually one criterion offer which means taking into account the standard of prices only.

3.3. Requirement in regard to the participants.

In electronic auctions main participants are: auctioneer or auctioneers as well as bidders. Tasks for auctioneer are different in dependence from concrete protocols, they generally control all phases of protocols. Bidders are participants which auction given offer. Important element is making possible for bidders to participate in auction, in some protocols [2,7,...] oneself does not tie large weight to it. Another [8], foresee special subprotocol which is responsible for assigning authorization numbers.

3.4. Practical techniques.

In current works to obtain demanded level of protection of information different techniques are used. In our case it is worth to turn our attention on two of them.

First of the techniques [2,6] bases its mechanism on the threshold scheme. In this method, we need several auctioneers, to whom bidders send their parts of offer. Main auctioneer links all parts and marks final price without exposing individual offers to all bidders. Danger of this technique is inherent in possible collusions between auctioneers, what in fact can bring to earlier disclosure of component prices or not to disclosure of final offer.

Second technique [3,4] excludes the possibility of collusions between auctioneers, this was achieved thanks to use of “trustworthy third person". However, in this method the restriction can arouse the credibility for this "third person".

4. Current e-auction and e-auction with extended requirements

The creation of electronic form of auction is the aim of presented cryptographic protocol.

Mechanisms applied in current e-auction are very similar to elements applied in presented e-auction, I think here particularly about communication processes between individual sides. In spite of many similarities, remembered earlier, our cryptographic protocol realizing e-auctions can not be applied in their present form.

The main difference consist in choosing of given offer, she does not only restrain to price, it is the choice of multicriterion, that is the composition of individual factors dependent of concrete case.

Another difference is the complexity of documents necessary to applying for possibility to participate in auction. As it was remembered earlier, in many protocols [2,7] oneself does not put attention on opportunity to obtain the rights to take part in auction but rather only to bidder's authorization. With realization of presented e-auction we have to turn special attention on this element.

With realization of particular phases of protocol we use both remembered above methods, that is: threshold scheme as well as third trustworthy person (TTP). Using those two methods is connected with complexity of requirements which presented protocol has to fulfil.

In presented protocol, the confidence of bids are achieved by using threshold scheme of dividing secret [5].

5. Description of the protocol.

5.1. Model.

Presented protocol of e-auction consists of four subprotocols: *certification, notification of auction, notification of offer as well as choice of offer.* In protocol take part *N* bidders (O_1, ... ,O_N), third trustworthy person that is *GAP* (main auction agency) as well as firm which wants to announce the auction.

The first step of protocol is verification by GAP, the participants taking part in e-auction, that is the bidders O_N as well as firm F which wants to announce the auction (the *subprotocol of certification*). The next step is notification to GAP the auction by verified firm F. GAP publishes the conditions of notified auction, giving all requirements notified by F (*the subprotocol of notification of auction*). In the next step, person wanting to take part in auction, after earlier verification, sends his offer to GAP (*the subprotocol of notification of offer*). The last subprotocol is executed after elapsing of time for notification of offers, then firm F as well as bidders O_N, send their parts of secret (needed to read offers) to GAP. After decoding them, they will be sent to firm F, where victorious offer will be chosen. In the same subprotocol, the firm F sends information about the victorious offer to GAP, then it will be published to (be generally known) public message (*the subprotocol of choice of offer*).

The communication between participants of protocol is safe. We achieve it thanks to using public key cryptography, where every participant of protocol possesses his private key (SK) as well as public key (PK). Those practical keys are not solid, their validity ends with the validity of registration number, which is achieved in subprotocol of certification.

Offers sent by O_N bidders are coded by public key of given auction. To can read them on account that we possess the private key, which in subprotocol of notification of auction, becomes divided into parts with the help of the suitable safe threshold scheme of division of secret. In protocol we also use the random numbers generator (KG). We use him to create the identification number of participants of auction as well as the numbers of auctions.

Auction ends after passing of definite time, to qualify this moment we will use the time stamp (T).

5.2. Proprieties of the protocol

The presented cryptographic protocol is characterized by the following features:

Incontrovertibility of participants: Only certificated persons can announce e-auction. Only

entitled persons can make auction's offers.

Integrity of data:. Both the content of sent offers as well as the final results of e-auction cannot be modified.

The incontrovertibility of offers: Bidder who won e-auction can not deny content of his offer as well as fact of making this offer.

Confidence of bids: Nobody can establish the content of the sent offers before the end of e-auction.

Anonymity of the winning bidder: The bidder who won the auction is not disclosed publicly.

Public verification: Everyone can check, which offer won e-auction. Participants of e-auction can check if their offers were taken into consideration.

6. Realization of the protocol

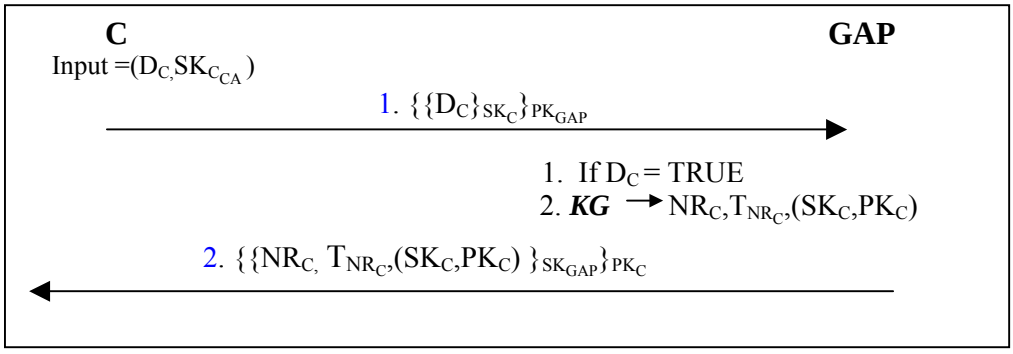
6.1. The certification subprotocol

The opportunity of participation in e-auction has to be preceded by obtaining suitable authorizations.

Person who apply for certificate, that is firm wanting to announce auction or bidder, should possess appropriate documents Dc as well as private key $SK_{C_{CA}}$ achieved from one of indicated earlier centres of authorization(CA). He digitally signs the documents mentioned above by using $SK_{C_{CA}}$ and then code with help of public key PK_{GAP} and later sends it to GAP.

GAP decodes documents and verifies then. After positive verification, generates them with the help of the generator of random numbers (KG), unique registration number for given person NR_C. Registration number is important during definite time, in order to this the time stamp of registration number T_{NR_C} is generated. GAP generates also private key (SK_C) and public key (PK_C) for given subject, which will be used in next subprotocol. Validity of these keys ends along with crossing the time showed by T_{NR_C}. It signs digitally generated data, it codes with the help of public key C and then sends it to C.

Table 1. Graf to the certification subprotocol.



6.2. The auction notification subprotocol

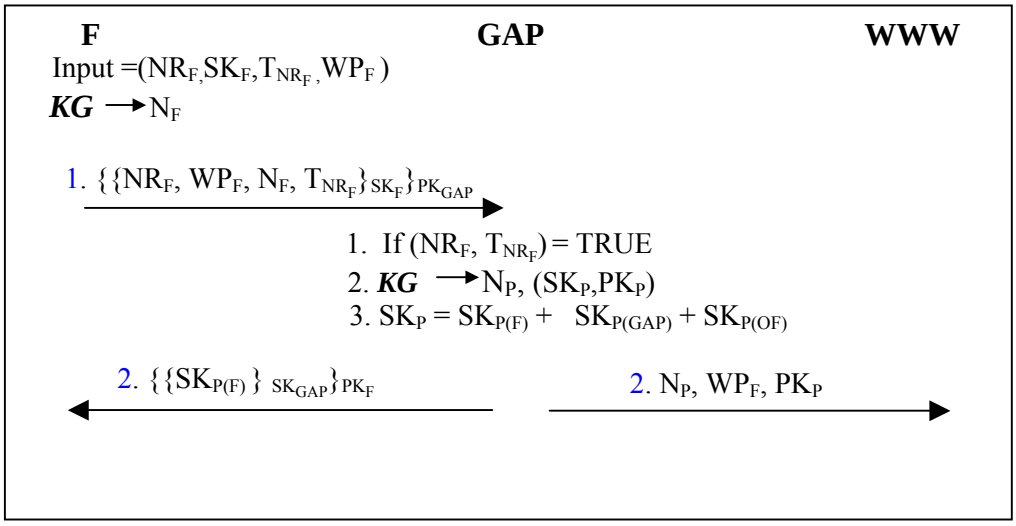
The protocol can be notified by any person, which got earlier in subprotocol of certification suitable authorizations.

Such a person, indicated as *F,* should possess the registration number NR_F, his time stamp T_{NR_F}, private key SK_F as well as conditions of notified auction WP_F . F generates with the help

of the generator of random numbers (KG), his individual number NF.

In the first step, F sends to GAP, signed digitally (SK_F) as well as coded (PK_{GAP}) following information: his registration number (NR_F), his time stamp (T_{NR_F}), the conditions of auction (WP_F) as well as his individual number (N_F).

Table 2. Graf to the auction notification subprotocol.



The main auction agency (GAP) verifies the registration number F (NR_F) as well as validity of his gauge of time. After positive authorization GAP generates the individual number of auction (N_P) as well as a few keys for concrete auction (SK_P,PK_P). The private key of auction (SK_P) is divided by use of the threshold scheme of dividing secret. Secret is divided into three parts, designed for F($SK_{P(F)}$), for GAP ($SK_{P(GAP)}$) as well as bidders in auction ($SK_{P(OF)}$). Each part is necessary to reproduce private key (SK_P).

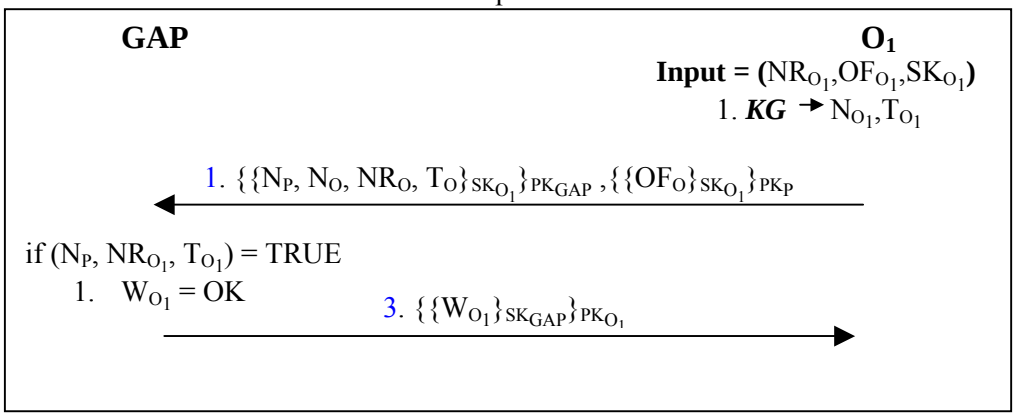
GAP sends digitally signed (SK_{GAP}) as well as coded (PK_F)) - the part of secret designed for F ($SK_{P(F)}$).

GAP publishes, for example on WWW site, the number of auction (N_P), conditions of it (WP_F) as well as its public key (PK_P).

6.3. The offer notification subprotocol

After the auction is notified and published, the interested parties can notify their offers. Bidder wanting to take part in auction should possess achieved earlier registration number (NR_{O_1}), private key (SK_{O_1}) as well as his offer (OF_{O_1}). Then bidder O_1, generates his individual number (N_{O_1}) and he marks his offer by time stamp (T_{O_1}).

Table 3. Graf to the offer notification subprotocol.



Next step consist in sending to GAP digitally signed (SK_{O_1}) as well as coded (PK_{GAP}) following information: N_P, N_O, NR_O, T_O. Offer (OF_{O_1}) is also digitally signed (SK_{O_1}) but it is coded by use of public key of given auction (PK_P), it is later sent to GAP.

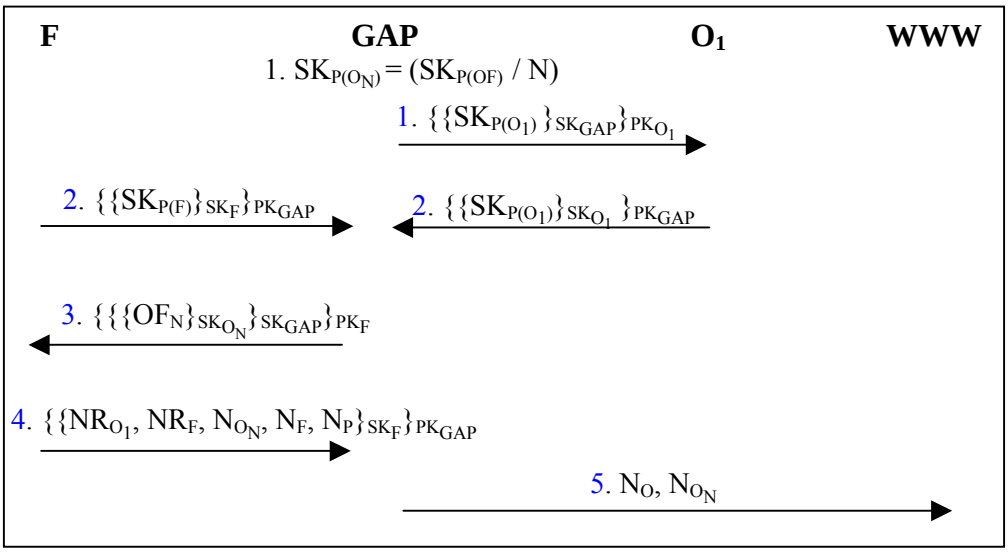
If sent data are correct, then GAP sends O_1 the confirmation of the notification of offer (W_{O_1}). Confirmation is digitally signed by GAP (SK_{GAP}) as well as coded (PK_{O_1}).

6.4. The offer choice subprotocol

Last subprotocol is executed after elapsing the time designed for making offers. This time is published with different conditions of auction (WP_F).

Knowing the number of bidders who sent their offers (N) GAP it divide earlier spitted part of main secret of auction ($SK_{P(OF)}$) into *N of* smaller parts. He uses the safe threshold scheme of dividing secret about profile (2,N). Created parts it signs digitally (SK_{O_1}), it codes (PK_{O_1}) and sends to all bidders O_N.

Table 4. Graf to the offer choice subprotocol.



In next step, the firm F as well as the bidders O_N send digitally signed and coded, their parts of secret to GAP, where they will become assembled in main secret of the auction (SK_P). Having the whole secret of given auction GAP can decode all sent offers (OF_N). After this action he sends all offers digitally signed by bidders to firm F, which is announcing auction. All offers are earlier undersigned digitally (SK_{GAP}) as well as coded (PK_F).

After having received offers firm F chooses the best offer and sends results to GAP in order to notify the winner. Sent information are the following: the bidder's who won auction registration number (NR_{O_1}), his registration number (NR_F), all bidders which offers were taken into account individual numbers (N_{O_N}), his individual number (N_F) as well as the number of auction (N_P). Exchanged information are digitally signed (SK_F) as well as coded (PK_{GAP}).

After having received information GAP publishes individual number (N_{O_1}) of the bidder whose offer won. To knowledge public all bidders which of offer be under All individual numbers of bidders whose offer were taken into account (N_{O_N}) are made public.

7. Security of the protocol

In this part of work, we will try to prove that the foundation shown in earlier part of work were fulfilled.

Participants' incontrovertibility. The subprotocol of certification is responsible for main

participant's verifications. GAP as third trustworthy person checks the required documents and assign the right to notify the own auction or the right of participation in auction. Registration assigned individual number is necessary in order to take part in remaining subprotocols.

Data integrity. Offers sent by bidders are digitally signed with the help of private keys received by every bidder after positive verification in subprotocol of certification. The results of auction, are also signed digitally by firm which announced auction, she also possesses the private key received in subprotocol of certification.

Confidence of the bids. The bidder can not deny the content of his offer because before it will be coded with the help of public key of auction it has to be signed digitally by him. The fact of making offer by bidder is noted down by GAP which archives every correct offer.

Anonymity of the offers. The offers sent by bidders are coded by use of public key of auction. Private key of auction is divided with use of safe threshold scheme of dividing secret into three parts from which every is necessary to composition of the whole secret. One part stays in GAP, second is sent to firm F which announce auction and third one is for bidders taking part in auction. Mentioned third part in subprotocol of offer's choice, is divided according to scheme (2,n) that is we fractionise secret for n parts but only two are necessary to second composition of secret. Scheme (2,n) is chosen because we need minimum two offers for auction to be important.

Winning bidder's anonymity. After choosing winning offer only bidder's individual number is passed to public message. This number shows winning bidder about victory.

Public verification. After finding the winner of e-auction, all bidder's individual numbers and the distinction number which won auction are published. Every participant can check if his number is on list what is equivalent with the fact of taking his offer under attention.

8. Conclusion

The presented cryptographic e-auction protocol can be used in any situation where requirements to its realization are very restrictive and complicated. The complexity can lie both in criteria of notified auctions and processes of the authentication of the participants.

The protocol was designed in support about possibility of today's computer applications, what gives him possibilities to use him in practice.

In future works it is worth to concentrate on the possibility of replacing third trustworthy person in the protocol by some additional calculation, which enlarge the burden of the given system but which allow to reduce considerably communication among parts of auction.

Bibliography

[1] P. Czarnecki. *Seminar e-Government in Poland - present and future.*

[2] W. Ham, K. Kim, H. Imai. Yet Another Strong Sealed - Bid Auctions. In *Proceedings of the Symposium on Cryptography and Information Security SCSI 2003*

[3] O. Baudron, J. Stern. Ninths - interactive Private Auctions. In: *Proceedings of the 5th Annual Conference he Financial Cryptography (FC), pp. 300-313, 2001.*

[4] A. Juels, M. Szydlo. And two - server, sealed - poverties auction protocol. In: *Proceedings of the 6th Annual Conference he Financial Cryptography (FC), volume 2357 of Lecture Notes in Computer Science. Springer, 2002.*

[5] K. Kulesza, Z. Kotulski, On Automatic Secret Generation and Sharing for Karin-Greene - Hellman Scheme, in: J. Sołdek, L. Drobiazgiewicz, [ed.], *Artificial Intelligence and Security in Computing Systems*, Kluwer 2003, pp. 281-292. ISBN: 1-4020-7396-8.

[6] M. Harkavy, J. D. Tygar, H. Kikuchi. Electronic auctions with private bids. In: *Proceedings of the 3rd USENIX Workshop he Electronic Commerce, pp. 61-74, 1998.*
[7] K. Suzuki, K. Kobayashi, H. Morita. Efficient sealed - poverties auction using hash chain. *ICISC 2000, LNCS, pp. 183-191, 2001.*
[8] K. Viswanathan, C. Boyd, E. Dawson. And three phased schema handicap sealed - poverties auction system design. In: *Australasian Conference Handicap Information Security and Privacy, ACISP " 2000, pp. 412-426. Lecture Notes in Computer Science, Springer-Verlag 2000.*