Annales UMCS Informatica AI 2 (2004) 391-400

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI

http://www.annales.umcs.lublin.pl/

Cryptographic protocol for electronic auctions with extended requirements

Bogdan Księżopolski[a*], Zbigniew Kotulski[b]

[a]*Institute of Physics, M. Curie-Skłodowska University, pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland*
[b]*Institute of Fundamental Technological Research, Polish Academy of Sciences, Świętokrzyska, 21, 00-049 Warszawa, Poland*

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 to 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 poorly resistant to 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 each abuse, in cryptography considered as attacks.

* Corresponding author: *e-mail address*: bogdan@kft.umcs.lublin.pl

In this paper we present the cryptographic protocol, which makes it 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 about both correctness and 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 to their traditional form). The most popular are: *English, 1st Price Sealed – Bid, Vickrey, Dutch.*

The type *English* is the most widespread. It consists in auctioning the price for given goods. The price grows until it only one person taking part in auction, remains while others give up.

Type *1st Price Sealed-Bid* consists in declaring the price for given goods independently by every bidder. The person who declares the highest price wins goods and he is obliged to pay the price sugested by himself.

The type *Vickrey*, alternatively called *2nd Price Sealed – Bid*, is very similar to the previous model. The difference consists in wining the auction by the person, who declared the highest sum for given goods, but he pays the second highest in order.

The type *Dutch* consists 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.

Each introduced auction model possesses many cryptographic protocols realizing it, each is characterized 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

The type *the 1st Price Sealed Bid* is the model, on the basis of which many cryptographic protocols [2-4,6], presenting different degrees of complexity came into being. Thanks to it we get different level of information protection. Protocols possess individual requirements, solved by different techniques.

In our case we should pay attention to some features.

3.1. The communication computational requirements

Cryptographic protocols consist of 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 activity is making calculations which need suitable computing power. Both methods are usually united, the essential difference between cryptographic protocols is the relation of executed calculations to the number of necessary connections between participants.

3.2 The way of the price settlement

Another essential element is the way of the price settlement. Some cryptographic protocols [2,7] possess the list of prices and the bidder can choose only a specific price value. Different [8] make it the choice of prices possible 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 the auctioneer are different depending on specific protocols, they generally control all phases of protocols. Bidders are the participants with the auction given offer. An important element is making it possible for bidders to participate in auction, in some protocols [2,7] not paying much attention to it. Another [8], foresee special subprotocol which is responsible for assigning authorization numbers.

3.4. Practical techniques

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

The first technique [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 the final price without exposing individual offers to all bidders. Danger of this technique is inherent in possible collusions between auctioneers, which, in fact, can bring to earlier disclosure of component prices or not to disclosure of final offer.

The second technique [3,4] excludes the possibility of collusions between auctioneers which is achieved thanks to the 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 the current e-auction are very similar to the elements applied in the presented e-auction, I think here particularly about communication processes between individual sides. In spite of many similarities, pointed out earlier, our cryptographic protocol realizing e-auctions can not be applied in its present form.

The main difference consists in choosing a given offer, it does not only restrain to price, it is the choice of multicriteria, that is the composition of individual factors dependent on given cases.

Another difference is the complexity of documents necessary for applying for participation in the auction. As discused earlier, in many protocols [2,7] attention is not paid to the opportunity to obtain the rights to take part in auction but rather only to bidder's authorization. With realization of the presented e-auction we have to pay a special attention to this element.

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

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

5. Description of the protocol

5.1. Model

The presented protocol of e-auction consists of four subprotocols: *certification, notification of auction, notification of offer as well as choice of offer*. In protocol there 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 are 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, a 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 the winning offer will be chosen. In the same subprotocol, the firm F sends

information about the winning offer to GAP, then it will be given to (be generally known) public knowledge (*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 permanent, 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 the public key of a given auction. They can be read on the condition that we possess the private key, which in the subprotocol of notification of auction becomes divided into parts with the help of the suitable safe threshold scheme of division of secret. In the protocol we also use the random numbers generator (KG). We use it to create the identification number of participants of auction as well as the numbers of auctions.

Auction ends when a given time passes. To determine it the time stamp (T) is used.

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 the content of his offer as well as the 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

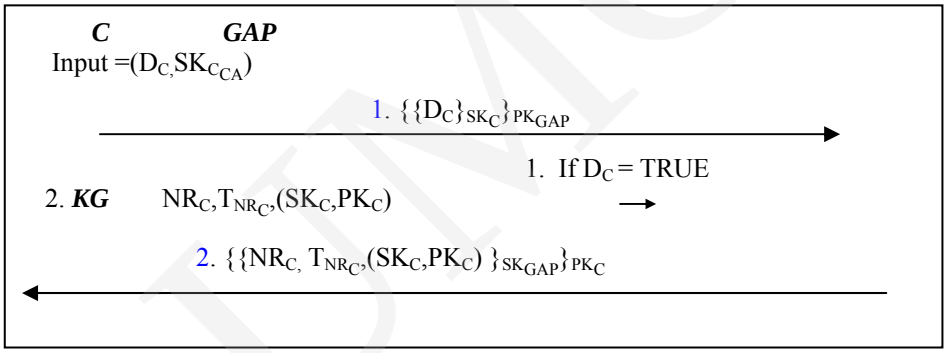
The opportunity of participation in e-auction has to be preceded by obtaining suitable authorizations.

A person who applies for certificate, that is a firm wanting to announce auction or bidder, should possess appropriate documents Dc as well as private key $SK_{C_{CA}}$ achieved from one of the earlier indicated centres of

authorization(CA). He signs the documents mentioned above digitally 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 them. After positive verification, it generates them with the help of the generator of random numbers (KG), unique registration number for a given person NR_C. The registration number is important for a definite time, so that the time stamp of registration number T_{NR_C} is generated. GAP generates also private key (SK_C) and public (PK_C) keys for a given subject, which will be used in the next subprotocol. Validity of these keys ends along with crossing the time shown by T_{NR_C}. It signs digitally the generated data, it codes with the help of the public key C and then sends it to C.

Table 1. Graph of the certification subprotocol



6.2. The auction notification subprotocol

The person certified subprotocol can be notified for the auction.

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

In the first step, F sends to GAP, signed digitally (SK_F) as well as coded (PK_{GAP}) the 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).

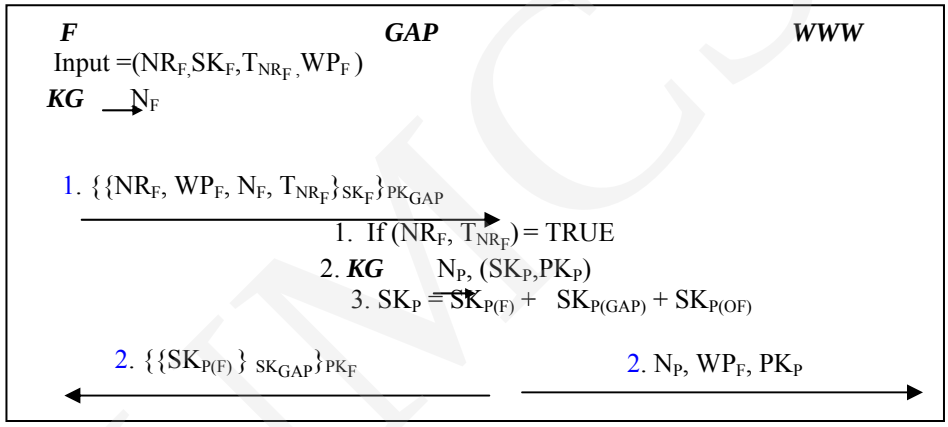
The main auction agency (GAP) verifies the registration number F (NR_F) as well as validity of his time gauge. After positive authorization GAP generates the individual number of auction (N_P) as well as a few keys for concrete auction (SK_P,PK_P). The private key of auction (SK_P) is divided by the 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 the private key (SK_P).

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

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

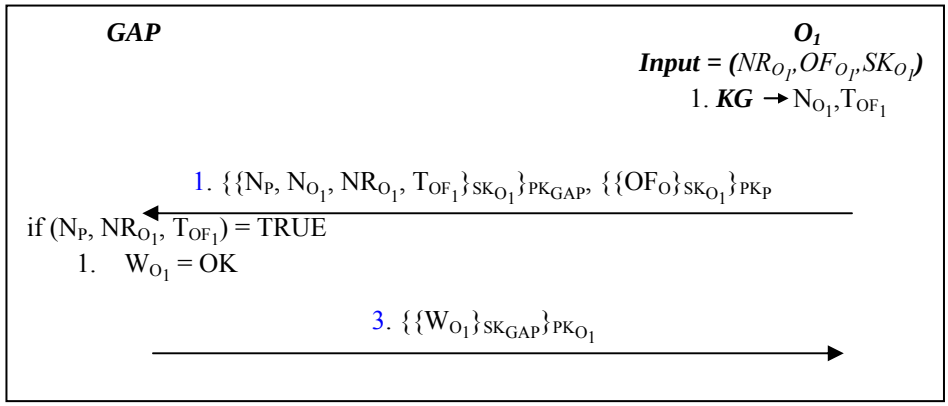
Table 2. Graph of the auction notification subprotocol



6.3. The offer notification subprotocol

After the auction is notified and published, the interested parties can notify their offers. A bidder wanting to take part in auction should possess the obtained earlier registration number (NR_{O_1}), private key (SK_{O_1}) as well as his offer (OF_{O_1}). Then a bidder O_1, generates his individual number (N_{O_1}) and he marks his offer by the time stamp (T_{OF_1}).

Table 3. Graph of the offer notification subprotocol



The next step consists in sending to GAP the digitally signed (SK_{O_1}) as well as the coded (PK_{GAP}) following information: N_P, N_O, NR_O, T_O. The 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), then it is sent to GAP.

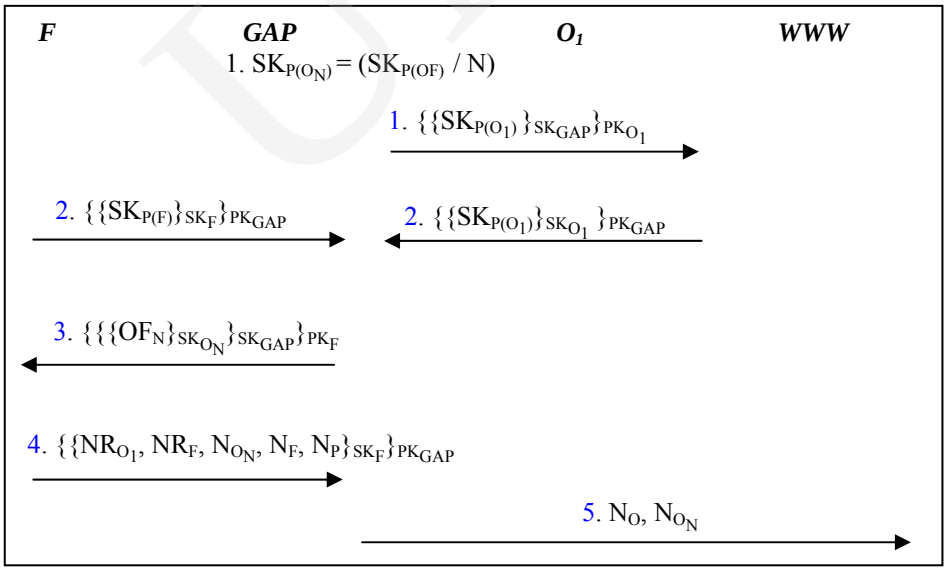
If the sent data are correct, then GAP sends O_1, the confirmation of the notification of offer (W_{O_1}). Confirmation is digitally signed by GAP (SK_{GAP}) as well as coded (PK_{O_1}).

6.4. The offer choice subprotocol

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

Knowing the number of bidders who sent their offers (N) GAP it divides the earlier split 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). The created parts are signed digitally (SK_{O_1}), coded (PK_{O_1}) and sent to all bidders O_N.

Table 4. Graph of the offer choice subprotocol



In the next step, the firm F as well as the bidders O_N send digitally their signed and coded parts of secret to GAP, where they are assembled in the main secret of the auction (SK_P). Having the whole secret of the given auction, GAP can decode all sent offers (OF_N). After this action he sends all offers digitally

signed by bidders to the firm F, which announces the auction. All offers are earlier undersigned digitally (SK_{GAP}) as well as coded (PK_F).

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

After having received information GAP publishes the individual number (N_{O_1}) of the bidder whose offer won. The individual numbers of the bidders whose offers considered are given to public knowledge (N_{O_N}).

7. Security of the protocol

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

Participants' incontrovertibility. The subprotocol of certification is responsible for main participants' verifications. GAP as the third trustworthy person checks the required documents and assigns the right to notify the own auction or the right of participation in the auction. Registration assigning the individual number is necessary in order to take part in the remaining subprotocols.

Data integrity. The offers sent by bidders are digitally signed with the help of private keys received by every bidder after the positive verification in subprotocol of certification. The results of auction, are also signed digitally by the firm which announced the auction. It also possesses the private key received in the 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 the auction public key, it has to be signed digitally by him. The fact of making the 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 the use of auction public key. The private key of auction is divided with the use of safe threshold scheme of dividing secret into three parts of which each is necessary for contents of the whole secret. One part stays in GAP, the second is sent to the firm F which announces auction and the third one is for the bidders taking part in the auction. The third part in the subprotocol of offer choice, is divided according to the scheme (2,n) that is the fractionise secret for n parts but only two are necessary for the second composition of secret. Scheme (2,n) is chosen because we need minimum two offers for the auction to be important.

Winning bidder's anonymity. After choosing the winning offer only bidder's individual number is passed to public knowledge. This number shows the winning bidder.

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

8. Conclusion

The presented cryptographic e-auction protocol can be used in any situation where requirements for 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 to give possibility of computer application.

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

References

[1] Czarnecki P., *Seminar e-Government in Poland – present and future*.
[2] Ham W., Kim K., Imai H., *Yet Another Strong Sealed – Bid Auctions*. In Proceedings of the Symposium on Cryptography and Information Security SCSI, (2003).
[3] Baudron O., Stern J., *Ninths – interactive Private Auctions*. In: Proceedings of the 5th Annual Conference he Financial Cryptography (FC), (2001) 300.
[4] Juels A., Szydlo M., *And two – server, sealed – poverties auction protocol*. In: Proceedings of the 6th Annual Conference he Financial Cryptography (FC), Lecture Notes in Computer Science. Springer, 2357 (2002).
[5] Kulesza K., Kotulski Z., *On Automatic Secret Generation and Sharing for Karin-Greene – Hellman Scheme*. In: Sołdek J., Drobiazgiewicz L., [ed.], Artificial Intelligence and Security in Computing Systems, Kluwer, ISBN: 1-4020-7396-8, (2003) 281.
[6] Harkavy M., Tygar J.D., Kikuchi H., *Electronic auctions with private bids*. In: Proceedings of the 3rd USENIX Workshop he Electronic Commerce, (1998) 61.
[7] Suzuki K., Kobayashi K., Morita H.. *Efficient sealed – poverties auction using hash chain*. ICISC 2000, LNCS, (2001) 183.
[8] Viswanathan K., Boyd C., Dawson E., *And three phased schema handicap sealed – poverties auction system design*. In: Australasian Conference Handicap Information Security and Privacy, ACISP"2000, Lecture Notes in Computer Science, Springer-Verlag, (2000) 412.