Development of the protocol «ELECTRONIC CASH» with inspection correction rules of the electronic e-cash number for e-Commerce systems

Igor Kalmykov. Writter
kia762@yandex.ru

Mariya Lapina. Writter
mlapina@ncfu.ru

Natalija Kononova. Writter
knv_fm@mail.ru

Maxim Kalmikov. Writter
kmi762@yandex.ru

Department of Information Security of Automated Systems
North-Caucasus Federal University
Stavropol, 355009

Abstract

The purpose of the research is to reduce the time to determine an intruder who tries to pay for a purchase with an electronic coin with a fake serial number by developing an algorithm which allows the seller to ensure that the buyer has correctly generated serial number S_i for electronic note i, as well as number T_i, which is used in the equation of checking for double payment of an electronic note. Various cryptographic protocols are utilized in modern e-commerce systems. Among them, it is possible to highlight the protocols of "withdrawal", "single coin payment" "whole wallet payment", "double-payment check for the same coin". Most of these protocols are built on the evidence of absolute non-disclosure of information. However, known protocols for "single coin payment" only allow a seller to determine presence of the electronic signature of the bank that issued an electronic wallet for a customer. The check of correct generation of an electronic coin serial number will allow a seller to determine an intruder prior to making a sell. Therefore, the development of a "single coin payment" protocol with checks for correct generation of an electronic note serial number which does not allow an intruder to pay using an electronic coin with a fake serial number is a significant task.

Keywords: electronic payments systems, cryptographic protocols data protection, pseudo-random function the zero-knowledge protocol, unauthorized access.

In: Marco Schaerf, Massimo Mecella, Drozdova Viktoria Igorevna, Kalmykov Igor Anatolievich (eds.): Proceedings of REMS 2018 – Russian Federation & Europe Multidisciplinary Symposium on Computer Science and ICT, Stavropol – Dombay, Russia, 15–20 October 2018, published at http://ceur-ws.org

1 Introduction

The explosive growth in the number of Internet users has become one of the main factors for the creation and rapid development of e-business. E-business is characterized by high dynamics of change of the environment in which economic activity is performed. Moreover, its organization and management in electronic form put a number of specific problems related to the correct functioning and ensuring its safety. A significant increase in the number of participants in economic activities and transferring of its part to the informational space leads to the fact that the business organization's security issues acquire extremely relevant content. Particularly great demands on information security systems apply to electronic payment systems (EPS) which use electronic cash [Can16, Cha16, Dre16].

It is obvious that one of the main properties of any system of cashless payments is safety of all its components at all stages of functioning of this system. At the same time the buyer who uses electronic cash, the seller, the issuer and the acquirer should be sure of protection of their investments. Unfortunately, the inclusive development of the Internet and mobile communications do not fully allow ensuring the required level of data protection. Therefore, the development of the protocols having high degree of data protection against unauthorized access (UA) and preventing an intruder from paying using an electronic coin with a fake serial number is an urgent task.

2 Research objective

The analysis of payment systems domestic market, which is still at the stage of its development, shows that it actually has several different solutions, ranging from traditional payment cards and ending with electronic cash. At the same time the last are becoming universal means of payment, due to the low cost of transaction execution, ease of divisibility and poolability, a higher degree of protection from theft, forgery, and denomination.

The carried-out analysis of studies [Can16, Cha16, Dre16] allowed allocating of a number of protocols, implementation of which will allow ensuring effective functioning of an autonomous electronic payment system. In study [Isl16] it is shown that the questions of protection of the electronic cash used by the modern EPS are assigned to protocols of cryptography protection. At the same time for effective functioning of these systems different cryptographic algorithms are used. Obviously, this approach increases the software size applied on an electronic cash media "electronic wallet".

However, known protocols for "payment" only allow a seller to determine presence of the electronic signature of the bank that issued an electronic wallet for a customer. Wherein, the procedure of checking correctness of the electronic coin serial number calculation is carried out at the end of the day. During this time, an intruder can purchase goods using fake coins. Therefore, sellers incur losses.

It is possible to eliminate this flaw by applying the procedure of serial number correctness check prior to making a sale. Thus, the purpose of the research is to reduce the time to determine an intruder who tries to pay for a purchase with an electronic coin with a fake serial number by developing an algorithm which allows the seller to make sure that the buyer has correctly generated serial number Si for electronic note i, as well as number Ti, which is used in the equation of checking for double payment of an electronic note.

3 Material and methods of research

In the process of investigation of the main types of reports have been carried out, which are used in today's BOT, working with e-money [about the protocols]. Studies have shown that the majority of EPA protocols use pseudo-random function. The majority of PSF using an algebraic system that has the property of rings and fields. This is due to the fact that such algebraic systems are widely used in various fields. So in the works [Moh07, Omo07, Moh16, Che95] shows the feasibility of using integral systems with the property of the ring, in the performance of information systems related to digital signal processing. In the papers [Kat16, Kat15, Mak17] shows the methods and algorithms for constructing error-correcting codes in the ring of integers and polynomials. In the work [Ste16] presented a way to correct the errors due to failures at the encoder AES algorithm based on modular codes. In the work [Kat13] is an example of the application of the modular code using the residue number system (RNS) in the secondary processing of navigation data systems. Using the CSR code has allowed to increase computing speed and reduce errors in determining the space-time coordinates of the consumer. Obviously, the use of an algebraic system possessing the property field, will develop a pseudorandom function which can be used in a variety of SOPs.

In the papers [Sar14, Yur17] presented protocols "withdrawals", "double-payment checks of the same coin."These protocols use a pseudo-random function, with the help of which the calculation of the number

of electronic coins and argument Si Ti, which is used to check the double coin payment protocol.

In this paper we will show the protocol developed by "payments of the same coin", which uses a similar function. For the organization of e-cash payment protocol user has two keys - public and private K KU public key is used by the bank when the electronic purse issuing its subscriber-buyer. The secret key buyers to participate in the process of payment of electronic money. But at the same time to to be in such a way that the seller is not able to his own computer. The public key is to develop a protocol calculates,

$$K_U = g^k mod\ q \tag{1}$$

where q - the order of the multiplicative group with the generating element g.

In [Sar14] showed that the protocol "withdrawals," the owner of the electronic cash, calculates the presentation, which depends on the secret key K, S parameter to generate a number of electronic bills, parameter T protocol for a "double payment. We use developed by RPA, the cryptographic resistance which is based on the -DDH problem to calculate λ proof of the complexity of the solutions the delivery. Let the secret key K, S and T parameters are the same length N bits. We divide them into m parts, so that

$$N_1 + N_2 + \ldots + N_m = N. \tag{2}$$

Then the presentation will be determined by

$$C = g^{\left(\prod_{j=1}^{m}(K_j+S_j+Tj)\right)^{-1}} \ mod\ q, \tag{3}$$

where K_j, S_j and T_j $-$ j-th block, resulting in the division numbers of the secret key K, the parameters S and T into m parts. To carry out the procedure of payment of the same coin, the buyer must be in presence of the W electronic wallet W, which contains the secret key holder K, S and T parameters, $\sigma_{K_B}(C)$ - the signature of the bank on presentation of C, which is used in the preparation of a purse buyer at the bank. So the buyer has a certain amount of coins in the electronic purse, he issued coins bank counter J. To purchase an electronic purse owner, contact the seller. At the same time he has to prove the latter the following points: - In the wallet W is the signature of the bank on presentation of C, ie,

$$\sigma_{K_B}(C) = \sigma_{K_B}(K, S, T) \tag{4}$$

- User generated S_i correct number of i-th e-bills;
- The buyer the right number generated T_i, which is used in the equation of the double payment of electronic bills.

Let us consider in more detail each stage of the "payment of the same coin" protocol. In the first phase, in order to prove to the seller that the electronic purse present signature bank issuing electronic bills, awarding the buyer calculates C according to expression (3). Then, using its private key, the buyer closes the data $E_K(C,\ \sigma_{K_B}(C))$ and sends the encrypted message to the seller. The seller, the buyer received a public key decrypts the message $D_{K_U}(C,\ \sigma_{K_B}(C))$.

After that, the seller goes to the bank and received his public key, decrypts his signature. The result of this procedure is the presentation of C, which was presented by the buyer to the bank to get the purse. Seller compares these values. In case of coincidence of these values the seller makes sure that the buyer has an electronic purse, which gave the bank.

At the second stage of the protocol "payment of the same coin" the seller must ensure that the buyer is properly generated S_i number i-th e-bills and the number of T_i, which is used in the equation of the double payment of electronic bills.

We use developed by the pseudo-random function of increased efficiency in the generation of S_i number of i-th e-bills,

$$S(i) = g^{\left(\prod_{j=1}^{m}(K_j+S_j)\right)^{-1}} \ mod\ q, \tag{5}$$

and where Sj and i_j - j-th block obtained by partitioning the parameters S_i and m part on. Thus the generation of T_i, which is used in Equation electronic bill payment double determined

$$T(i) = K_U g^{\left(\prod_{j=1}^{m}(T_j+K_j)\right)^{-1}} \ mod\ q, \tag{6}$$

where T_j and i_j - j-th block, resulting in the division of parameters T and i to m parts.

$$\prod_{j=1}^{m} \frac{1}{T_j + i_j + 1} mod\ q = a_T,$$

$$\prod_{j=1}^{m} \frac{1}{S_j + i_j + 1} mod\ q = a_S.$$

The seller sends the buyer a random number that is $r \in Z_q$.
After that, the buyer calculates the answers to the question r, ask the seller

$$a_S^* = (a_S - r) \bmod q, \tag{7}$$

$$a_T^* = (a_T - r) \bmod q. \tag{8}$$

The values obtained for the buyer uses to calculate the dark images of the serial number and denomination of the parameter for the equation of double payments,

$$S_i^* = g^{a_S^*} mod\ q \tag{9}$$

$$T_i^* = g^{a_T^*} mod\ q \tag{10}$$

After that, the buyer determines the product of true and dark images

$$S_i T_i\ mod\ q = g^{a_S} K_U g^{a_T}\ mod\ q = K_U g^{(a_S + a_T) mod \varphi(q)} mod\ q, \tag{11}$$

$$S_i^* T_i^*\ mod\ q = g^{a_S^*} K_U g^{^* a_T}\ mod\ q = K_U g^{(a_S^* + a_T^*) mod \varphi(q)} mod\ q. \tag{12}$$

The results obtained using expressions (11) and (12) is sent in encrypted form to the seller.
After that, the seller, the buyer using the public key of K_{OTK}, decrypts his signature. The seller then calculates the ratio.

$$A = \frac{S_i T_i}{S_i^* T_i^*} = \frac{K_U g^{(a_S + a_T) mod \varphi(q)}}{K_U g^{\left(a_S^* + a_T^*\right) mod \varphi(q)}} = g^{2r} mod\ q. \tag{13}$$

If the calculated value according to equation (13) corresponds to,

$$A = (g^r)^2 \bmod q, \tag{14}$$

this indicates that the provided e-Si i-th number of electronic bills and the corresponding parameter of Ti, which is used in Equation double payments are generated correctly.

Results and Discussion

Let $q = 43$. Then $g = 3$. Let the secret key value be $K = 37$.
Then the public key value, according to (1), equals to $K_U = g^k mod\ q = 3^{37} mod\ 43 = 20$.
To calculate the electronic coin number let us take $S(1) = 28$.
To prevent repetitive utilization of the same electronic coin number let us take $T(1) = 19$.
Let us present the secret key in binary code and divide it on two blocks with 3 digits each. We shall have

$$K = 37 = 100101 = 100101;\ K_2 = 100_2 = 4;\ K_1 = 101_2 = 5.$$

Let us present $S(0)$ in binary code and divide it on two blocks with 3 digits each. We shall have

$$S(1) = 24 = 011000 = 011000;\ S_2(1) = 011_2 = 3;\ S_1(1) = 000_2 = 0.$$

Let us present $T(0)$ in binary code and divide it on two blocks with 3 digits each. We shall have

$$T(1) = 19 = 010011 = 010011;\ T_2(1) = 010_2 = 2;\ T_1(1) = 011_2 = 3$$

Let us calculate the sums with modulo $= 43$.
We shall receive

$$(S_1(1) + K_1) \bmod p = (0 + 5) \bmod 43 = 5,$$

$$(S_2(1) + K_2) \bmod p = (3 + 4) \bmod 43 = 7,$$

$$(T_1(1) + K_1) \bmod p = (3 + 5) \bmod 43 = 8,$$

$$(T_2(1) + K_2) \bmod p = (2 + 4) \bmod 43 = 6.$$

Let us calculate the backward multiplicative elements for the received sums modulo $p = 43$. We shall receive

$$(S_1(1) + K_1)^{-1} \bmod p = 5^{-1} \bmod 43 = 26,$$

$$(S_2(1) + K_2)^{-1} \bmod p = 7^{-1} \bmod 43 = 37,$$

$$(T_1(1) + K_1)^{-1} \bmod p = 8^{-1} \bmod 43 = 27,$$

$$(T_2(1) + K_2)^{-1} \bmod p = 6^{-1} \bmod 43 = 36.$$

Let us calculate the values

$$a_S(1) = \prod_{j=1}^{2} \frac{1}{S_j + K_j} \bmod q = \Big|26 \cdot 37\Big|_{43}^{+} = 38,$$

and

$$a_T(1) = \prod_{j=1}^{m} \frac{1}{T_j + K_j} \bmod q = \Big|27 \cdot 36\Big|_{43}^{+} = 6.$$

Then, the actual values of parameters S(1) and T(1) equal to

$$S(1) = g^{a_S} \bmod q = 3^{38} \bmod 43 = 17,$$

$$T(1) = g^{a_T} \bmod q = 3^{6} \bmod 43 = 41.$$

The seller sends the buyer random number $r = 3$.
Afterwards, the buyer calculates the responses to question $r = 3$, according to (7) and (8)

$$a_S^*(1) = (a_S(1) - r) \bmod q = (38 - 3) \bmod 43 = 35,$$

$$a_T^*(1) = (a_T(1) - r) \bmod q = (6 - 3) \bmod 43 = 3.$$

These values are used by the buyer to determine the shadow samples of the note serial number and the parameter for the equation of double-payment checking, according to (9) and (10)

$$S^*(1) = g^{a_S^*(1)} \bmod q = 3^{35} \bmod 43 = 7$$

$$T^*(1) = g^{a_T^*(1)} \bmod q = 3^{3} \bmod 43 = 27$$

After that, the buyer determines the product of the actual and the shadow samples, according to (11) and (12)

$$S(1)T(1) \bmod q = \Big|17 \cdot 41 \cdot 20\Big|_{43}^{+} = 8,$$

$$S^*(1)T^*(1) \bmod q = \Big|7 \cdot 27 \cdot 20\Big|_{43}^{+} = 39.$$

The results obtained with expressions (11) and (12) are sent to the seller in the encrypted form $E_K(3, 41, 8, 39)$.
Following that, the seller, using public key of the buyer $_{pub} = 20$, decrypts $D_{K_U}(3, 41, 8, 39)$ Afterwards, the seller calculates the ratio, according to (13)

$$\Big|\frac{S(1)T(1)}{S^*(1)T^*(1)}\Big|_{43}^{+} = \Big|\frac{8}{39}\Big|_{43}^{+} = 41.$$

Knowing number r = 3, the seller checks, according to (14)

$$A' = (g^r)^2 \bmod q = (3^3)^2 \bmod 43 = 41.$$

Since value $A' = A = 41$, this allows us to conclude that the buyer is not an intruder, who tries to pay for the goods with an electronic coin with a fake serial number.

Thus, the protocol was developed "the payment of the same coin", which allows the seller to verify the presence of the electronic wallet of the buyer, as well as the correct generation number i-th e-bills Si, as well as the parameter T_i, which is used in the equation of the double payment of electronic coin.

4 Conclusion

The protocol of "single coin payment", which can be applied in e-commerce systems, is presented in the research. Unlike known "single coin payment" protocols, which only allow a seller to check the electronic signature of the bank that issued an electronic wallet for a buyer, the developed protocol allows to carry out a check for correct generation of an electronic coin serial number. The desired goal is achieved by developing the algorithm which allows the seller to ensure that the buyer has correctly generated serial number S_i for electronic note i, as well as number T_i, which is used in the equation of checking for double payment of an electronic note. The developed protocol allows a seller to determine an intruder prior to making a sell. Application of the developed protocol reduces the time required to determine an intruder who attempts to make a purchase with an electronic coin with a fake serial number compared to the protocols known before.

References

[Can16] Canard S., Pointcheval D., Sanders O., Traore J. *Divisible e-cash made practical.* Source of the Document IET Information Security, 10(6), 2016, pp. 332-347.

[Cha16] Chang C.-C., Chen W.-Y., Chang S.-C. *A highly efficient and secure electronic cash system based on secure sharing in cloud environment.* Security and Communication Networks 9 (14), 2016, pp. 2476-2483.

[Che95] Chervyakov N.I., Veligosha A.V., Kalmykov I.A., Ivanov P.E. *Digital filters in a system of residual classes* // Izvestiya Vysshikh Uchebnykh Zavedenij. Radioelektronika, 1995, 38(8), pp. 11-20.

[Dre16] Dreier J., Kassem A., Lafourcade P. *Automated verification of e-cash protocols.* Communications in Computer and Information Science 585, 2016, pp. 223-244.

[Isl16] Islam S.K., Amin R., Biswas G.P., Obaidat M.S., Khan M.K. *Pairing–Free Identity–Based Partially Blind Signature Scheme and Its Application in Online E-cash System.* Arabian Journal for Science and Engineering, 41(8), 2016, pp. 3163-3176.

[Kat13] Katkov K.A., & Kalmykov I.A. *Application of Parallel Technologies in Navigation Management under the Conditions of Artificial Ionospheric Disturbances.* World Applied Sciences Journal, 26(1), 2013, pp. 108-113.

[Kat16] Katkov K.A., Naumenko D.O., Sarkisov A.B., & Makarova A.V. *Parallel Modular Technologies in Digital Signal Processing.* Life Science Journal, 11(11s), 2014, pp. 435–438.

[Kat15] Katkov K.A., Timoshenko L.I., Dunin A.V., & Gish T.A. *Application of Modular Technologies in the Large-Scale Analysis of Signals.* Journal of Theoretical and Applied Information Technology, 80(3), 2016, pp. 391-400.

[Mak17] Makarova A.V., Stepanova E.P., Toporkova E.V. *The use of redundant modular codes for improving the fault tolerance of special processors for digital signal processing* // CEUR Workshop Proceedings 1837, 2017, pp. 115-122.

[Moh07] Mohan P.V. *Residue Number Systems. Algorithms and Architectures.* Springer, 2002. - 273 p.

[Moh16] Mohan P.V. *Residue Number Systems. Theory and Applications.* Springer, 2016. - 403 p.

[Omo07] Omondi A., Premkumar B. *Residue Number Systems: Theory and Implementation.* Imperial College Press. UK, 2007. - 342 p.

[Sar14] Sarkisov A., Makarova A. *Extension of the Methods of Protection of the E-commerce Systems Based on the Modular Algebraic Schemes.* Proceedings of the Southern Federal University. Technical sciences, 2(151), 2014, pp. 218-225.

[Ste16] Stepanova E.P., Toporkova E.V., Kalmykov M.I., Katkov R.A., Rezenkov D.N. *Application of the codes of a polynomial residue number system, aimed at reducing the effects of failures in the AES cipher* // Journal of Digital Information Management, 2016. Vol. 14. N.2., pp.114-123.

[Yur17] Yurdanov D., Kalmykov M., Gostev D. *The implementation of information and communication technologies with the use of modular codes.* // CEUR Workshop Proceedings 1837, 2017, pp. 206-212.