Impact Factor: 9.2 ISSN-L: 2544-980X

WAYS TO EXCHANGE INFORMATION THROUGH AN ELECTRONIC DIGITAL SIGNATURE

***M.M.Turdimatov* [1] *, S.S.Askarov* [2]**

[1] *Associate Professor of the Department of Information Security of the Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorezmi*
[2] *Master's student of the Department of Information Security of the Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi*

ANNOTATION: *This article presents methods of data exchange using electronic digital signature algorithms , classification of electronic digital signature algorithms based on the Schnor scheme and their comparative analysis, as well as classification by complexity. Problems with the ElGamal digital signature scheme are also being explored.*

Keywords: *electronic digital signature, electronic signature scheme, symmetrical, asymmetrical, parameter algebra , EEC, discrete logarithmization, electronic document, public key, private key.*

INTRODUCTION: To date, favorable conditions have been created for the introduction and use of modern information technologies in all spheres of society, to better satisfy the information needs of citizens, to enter the global information system and to expand the use of its resources. Taking this into account, all fields of the system include the concepts “Electronic document”, “Electronic digital signature” .

An electronic document is created, processed and stored using technical means and services of information systems and information technologies. Information recorded in electronic form, verified by ERI and having other details of an electronic document that allow it to be identified as an electronic document [1].

If we look at the history of ERI, it was in 1976 that Whitfield Diffie and Martin Hellman first proposed the concept of " Electronic Digital Signature", although they assumed that only digital signature schemes could exist.

In 1977, Ronald Rivest , Adi Shamir , and Leonard Adleman developed RSA , which can be used to create primitive digital signatures without further modification . Also in 1984, Shafi Goldwasser , Silvio Micali and Ronald Rivest were the first to rigorously define security requirements for digital signature algorithms. Models of attacks on GMP digital signature algorithms that meet the described requirements are described.

An important place in solving the problem of ensuring information security in electronic document management processes.

FORMULATION OF THE PROBLEM. An electronic digital signature algorithm based on the Schnor scheme is used as a cryptographic tool.

The problem with the ElGamal digital signature scheme is that it must be too large to hamper the discrete logarithm. It is recommended that the length be at least 1024 bits. You can enter a signature that is 2048 bits long. To reduce the signature size, Schnorr proposed a new scheme based on the ElGamal scheme, but with a reduced signature size. The figure below provides an overview of the Schnorr digital signature scheme[1].

General idea of the Schnorr digital signature scheme. During the signing process, two functions generate two signatures;

during verification, the output of one function is compared with the first signature to be verified.

ERI is also of great importance when submitting reports electronically at enterprises and trade organizations, as well as giving legal status to an electronic document.

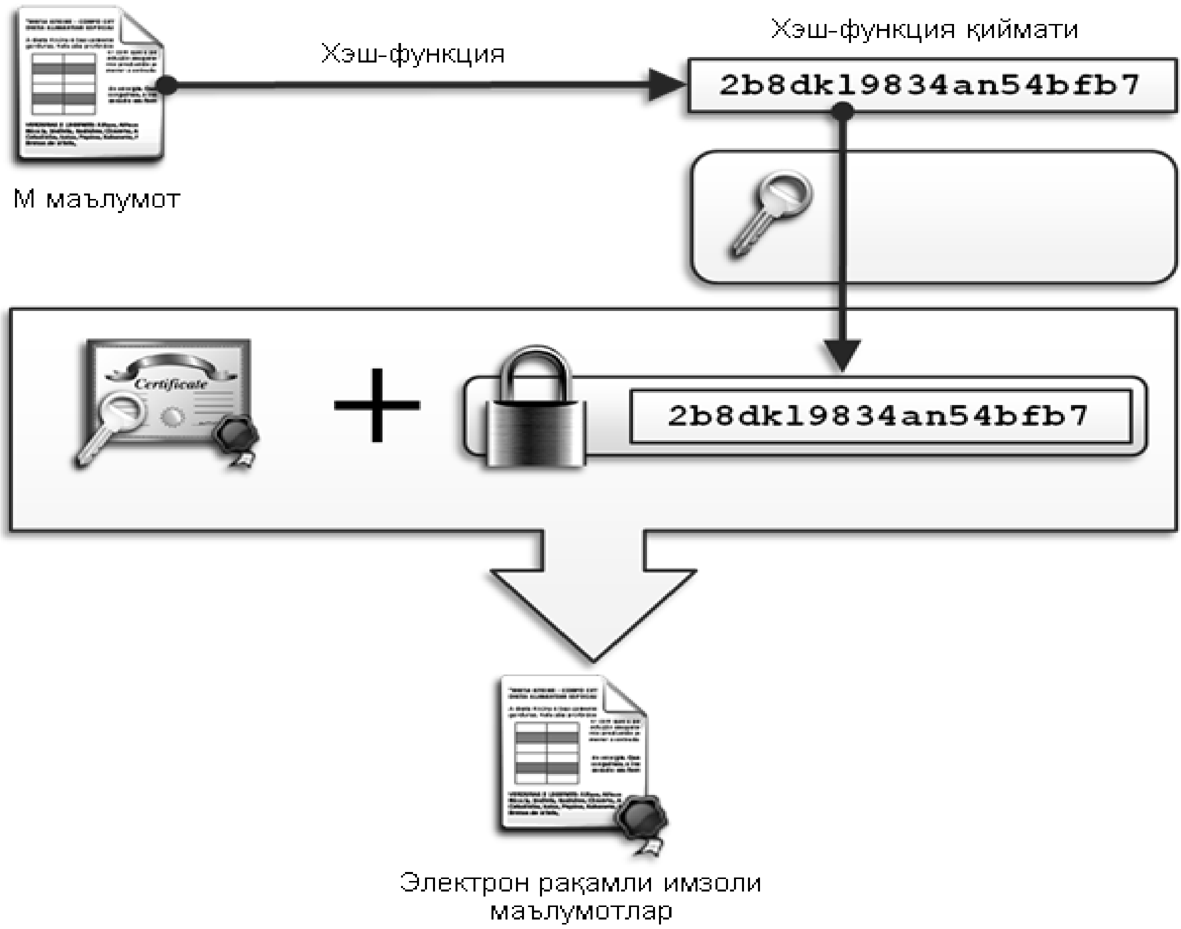

Figure 1. ERI formation process.

The generally accepted scheme (model) of ERI includes three processes:

- ERI key generation;

- Formation of ERI;
- ERI verification (confirmation of authenticity) [4].

The process of creating an electronic document using ERI is shown in Figure 1, and first the hash value of the information being sent is calculated. Then, according to the digital signature algorithm, the information is signed with the sender's private key.

ERI verification compares the hash value calculated from the sender's public key and the hash value of the data. See Figure 2 below. The ERI review process is presented.

The generation and testing of different ERI algorithms differ in their mathematical functions.

The mathematical functions of the ERI algorithms presented in this article are classified according to the complexity of the problems (Table 1):

- Factoring complexity problems based on the ERI Algorithms.
- Discrete logarithm problem. complexity based on HUSBAND algorithms.
- Elliptic bending linear discrete logarithm complexity problems based on the ERI Algorithm.
- ERI algorithms based on parameter algebra.
- For various problems (for example, quadratic discount, based on square root modulo *n*). ERI algorithms. Below, ERI algorithms are classified by task complexity.

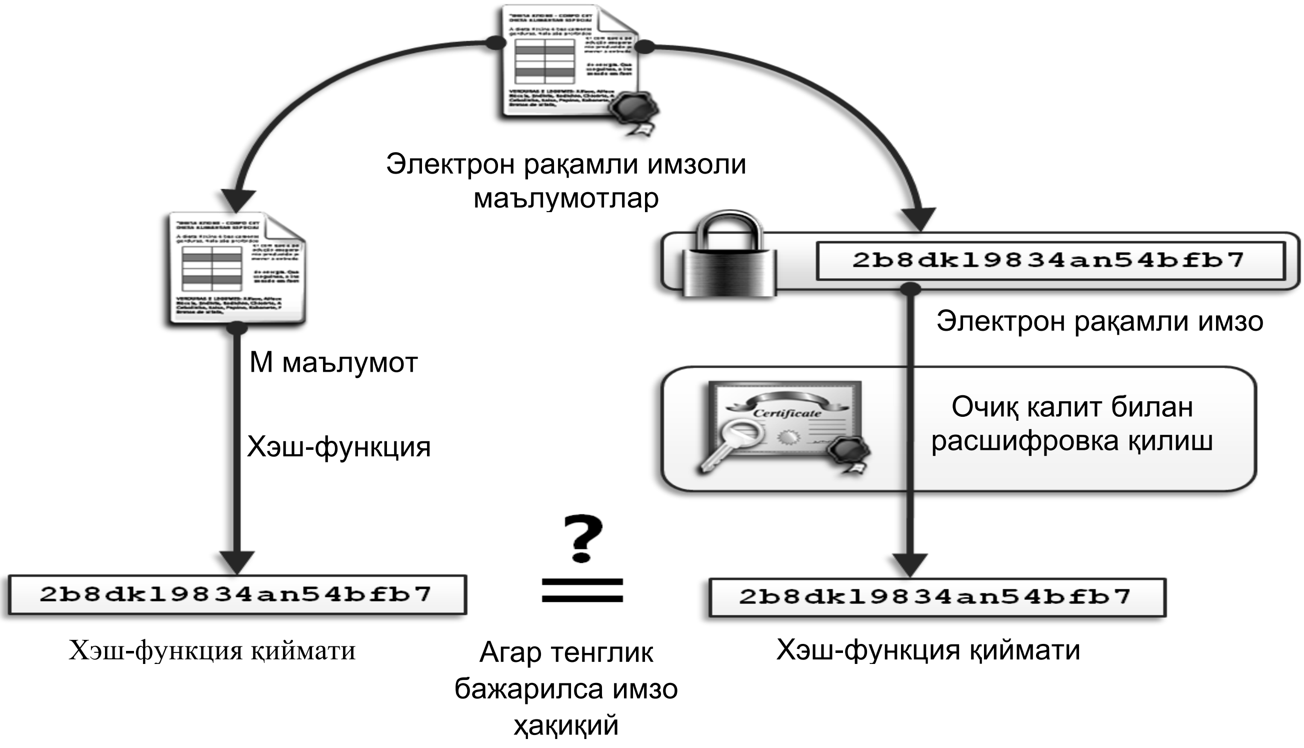

Figure 2. ERI verification process

was proposed by Japanese scientists in 1985. The main feature of this electronic digital signature is its speed. Compared to the RSA or ElGamal algorithms, the process of signing a document and verifying the signature using the ESIGN algorithm is several times faster.

Signature parameters include the following: In the ESIGN algorithm, a pair of large primes p and q is used as a secret key and is given by $n = p^{2} *q$. The pair (n, k) is accepted as the public key. Here k is the security parameter.

The generation and transmission of ERI using the ESIGN algorithm includes the following sequence of steps (Fig. 3):

1. m = H(M) - hash function for information M, 0< m < n -1 .

2. Number x is generated , p*q < x .

3. $w \equiv ((m - x^{k}) \pmod{n})/p*q$.

4. An electronic digital signature is formed:

$S \equiv x+((w/kx\ k^{-1} \pmod{p}))p*q$.

Using the received information M and the digital signature S, the receiving party performs the following sequence of actions:

1. hash function m = H(M);

^{k} (mod n) for S using public key (n, k) is;

3. A number a equal to or greater than twice the number of bits divided by 3 is much less than an integer, and $2^{\text{is a}}$;

4. m and $m+2^{a}$ with S^{k} (mod n) compared with:

$m = = s^{k} \pmod{n}$;

$m+2^{a} = = \sigma^{k} \pmod{n}$.

If S^{k} (mod n) equal to or greater than m and s^{k} (mod n) $m+2^{a}$ less than , ERI is considered valid, otherwise it is invalid. The fact that this algorithm has the ability to perform calculations related to x and k in advance allows the ERI generation process to be accelerated.

The digital Schnorr signature based on the discrete logarithm problem is calculated on the basis of the main module and a second radical module is used, which is significantly smaller than it. To generate Schnorr digital signature keys, the first two prime numbers p and q are chosen so that q is a multiple of p-1. Then a value greater than 1 is selected when $a^{q} \equiv 1 \pmod{p}$. r, q and a can be freely declared and applied to a user group [5].

To generate a key pair, a random number less than q is selected. This is the private key with which the public key is used.$v \equiv^{\text{this is -s}}$ (mod p) .

The main disadvantage of the Schnorr digital signature scheme is that when the attacker quite clearly sets the problem of discrete logarithm based on the cryptosystem and has enough resources to solve this problem, then in the case of forgery of the digital signature received by the recipient, the signer does not have any evidence and data proving that the signature was forged.

The digital signature length for the Schnorr scheme is much shorter than that of the RSA and ElGamal digital signature schemes when the security level is the same. The national standard UzDSt 1092:2009 also uses modules r and q based on the Schnorr algorithm.

Currently, ERI algorithms based on the discrete logarithm problem with elliptic curves, which are considered the most complex, are widely used. The advantage of elliptic cryptography is that at the moment there are no subexponential algorithms for solving discrete logarithm problems on a group of points on elliptic curves.

The most well-known algorithms based on this problem are the ECDSA ERI algorithms GOST 34.10-2001. In the ECDSA algorithm, as the key size increases, signature generation is much faster, and signature verification is much slower.

shows the speed of the ECDSA algorithm, based on the problem of discrete logarithm of an elliptic curve, in comparison with the RSA algorithm, based on the problem of factoring on short keys [5].

Table 1

Creation and verification of ERI based on RSA and ECDSA algorithms

Algorithms	**Signature create**	**Signature check**
RSA (2048 bit)	120 ms	5 ms
ECDSA (216 bit)	68 ms	70 ms

As can be seen from this table , the time required to create an ERI using the ECDSA algorithm with a length of 216 bits is approximately 2 times less than the time required to create an ERI using the RSA algorithm 2048 bits long .

One of the most difficult cryptographic problems today is parameter algebra. The UzDSt 1092:2009 standard, developed by Uzbek scientists, is based on this problem [4]. It uses a new one-way function with hidden modulo arithmetic . UzDSt 1092:2009 provides for the detection of forgery of an electronic digital signature by introducing the session key procedure used in the process of confirming the authenticity of an electronic digital signature into the process of creating an electronic digital signature.

Electronic document in the information and communication network ERI exchange

In the process, the following three problems are solved, giving the opportunity gives:

- determine the authenticity of the electronic document of the source ;

- electronic document integrity check (no changes);

- place an item from the author into the digital signature of the electronic document

he will not refuse to provide .

Electronic digital sign general recognize received circuit three

the process includes :

- electronic digital signature keys generation ;
- electronic digital signature formation;
- electronic digital signature authenticity confirmation

Signature should be placed by the author only by, only for him the personal was known

with key made increased . Check the authenticity of the sign for now welcome person author, author's signature open key with made can increase [3] . Electronic digital signature algorithms formation too gift of the day software , hardware and hardware from tools is used .

CONCLUSION. In conclusion, we can say that the advantage of ERI algorithms based on the complexity of the discrete logarithm of an elliptic curve problem is their speed due to the use of short keys, while the advantage of ERI algorithms based on parametric algebra is high cryptographic strength due to the use of a new one-way function. Due to the fact that when falsifying ERI based on parametric algebra, it is possible to determine the mechanism for its detection, the use of a counterfeit document is limited.

Electronic digital signature is traditional in the exchange of paper documents.

Binary number system, as opposed to private signature functions.

functions with specific memory registers into pieces related question.

The memory of bits is known to be one of a sequence consisting of an electron, which signature by copying something to the place to put or change computers based on Hello in systems, complexity does not give birth [5] .

Today's high level of development of the whole world in civilization

documents, including confidential documents also in electronic form use and Hello widely used in infection transmission systems electronic documents are in development and electronic signatures authenticity identify problems solutions importance reason

releases [6,7] .

Digital sign efficiency its basis organize doer cryptographic algorithm speed, endurance and counting Flexibility is a related issue for your machines.

Electronic documents in this article are exchanged in processes information security provide problem hi al in reaching important place occupied cryptographic tool Schnor to circuit based electron digital signature of the algorithm entity Recommended . The problem with the ElGamal digital signature scheme is that it must be too large to make it difficult to take a discrete logarithm; A length of at least 1024 bits is recommended. It is possible to make a signature with a size of 2048 bits, but to reduce the size of the signature it may be considered appropriate to create it based on the Schnorr El-Gamal scheme.

REFERENCES

1. Law of the Republic of Uzbekistan “On electronic document management”. 12/11/2003 y.
2. Law of the Republic of Uzbekistan “On Electronic Digital Signature”. 04/29/2003.
3. Own DST 1092:2009 “Information technologies. Cryptographic information protection. Processes of formation and verification of electronic digital signatures.”
4. Bruce Schneier. Applied cryptography. Protocols, algorithms, source texts and SI languages - Moscow: TRIUMPH, 2002.
5. Khasanov Kh.P. Methods and algorithms for creating cryptosystems based on improved diamatric algebras and parametric algebra. – Tashkent, 2008. 208 p.

6. Khudoynazarov U., Melikuziev A. (2023). IMPROVING THE RSA PUBLIC KEY ENCRYPTION ALGORITHM BASED ON PARAMETERS ALGEBRA. Research and implementation.

7. *Akbarov D., Khasanov P., Khasanov Kh., Akhmedova O. Mathematical foundations of cryptography. Textbook. - Tashkent, 2010 - 210 p.*

8. Akbarov D.E. Cryptographic methods of information protection and their applications. Tashkent. “Mark of Uzbekistan”, 2009. – 432 p.