Proposals of using chameleon-signature in Ukrainian prototype of combined PKI

Viktor Dolgov, Iuliia Ishchenko

Abstract – **in this thesis imparts a proposition to introduce a chameleon-signature in the prototype of Ukrainian combined PKI.**

Keywords – **combined PKI, chameleon-hash, chameleon-signature.**

I. INTRODUCTION

The rapid development of information technologies and the rapid growth of the Internet led to the formation of the information environment, an impact on all media of human activity. More and more paper documents are replaced by electronic information, which greatly facilitates the dissemination, copying, archiving and information management, promotes business process. Implementation of electronic document management systems can substantially reduce the financial costs and staff time in all areas of information activities. Almost all traditional forms of business, one way or another, are converted into electronic business. In this thesis are considered applicability and advantages of chameleon-signature in the prototype of combined PKI of Ukraine.

II. RATIONALE FOR CREATING OF COMBINED PKI

The most important condition for the existence of e-business is information security. The basis of modern information security systems is tools of cryptographic protection of information, in particular asymmetric systems. To date, the Ukrainian legislation as the basic architecture of a legitimate system of asymmetric cryptography, public key infrastructure (PKI) is defined, which is a combination of hardware and software, organizational and technical means for ensuring that the directional encryption and services of digital signature.

However, PKI has some disadvantages, such as:

– complexity and high cost of lifecycle maintenance of digital certificates;

– complexity of key recovery procedures, etc.

Most of the shortcomings inherent in PKI can be eliminated in an identity based encryption scheme (IBE - Identity based encryption) [1]. A distinctive feature of such schemes is that as the encryption key used by user ID. But this scheme has its own problems, which do not allow implementing the system in the electronic document management of large user communities. One of the most significant shortcomings IBE schemes is the need of high levels of confidence in the trusted third party. In order to unite the advantages of PKI and IBE, proposed to use a combined scheme, known as the combined PKI.

III. ADVANTAGES OF CHAMELEON-SIGNATURE

It should be noted that the increasing number of electronic document management systems, makes new requirements to protection of electronic documents. Implementation of PKI (and the combined PKI in the near future) will not be able to meet fully the requirements of individual systems, in particular e-commerce systems. Researches show that in such systems as, for example, a system of closed auctions, closed system of electronic voting, some banking transactions and other systems relating to electronic commerce, there is a need for additional properties. Such properties are the following: non-transferability signature and message hiding. Under non-transferability we understand the impossibility of proof of validity of digital signature to a third party without the participation of the signer. Message hiding meens no need to open the message content to a third party in the course of resolving disputes. Chameleon-signature [2] enables these properties by using a chameleon-hash, which is a one-way function with a secret. Mathematical basis of the chameleon- signature is a bilinear pairing in the group of points of an elliptic curve. General form of a chameleon-hash is shown in Fig. 1:

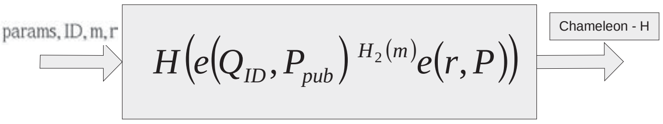
params, ID, m, r
$H\left(e\left(Q_{ID}, P_{pub}\right)^{H_2(m)} e(r, P)\right)$
Chameleon - H

Fig.1 General form of a chameleon-hash

Fig. 1 uses the following notation: trusted third party publishes $\text{params} = \left\langle G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H \right\rangle$ – system parameters, G_1 – cyclic additive group generated by P, q – order of P, G_2 – cyclic multiplicative group of the order q, $e : G_1 \times G_1 \rightarrow G_2$ – a bilinear pairing, $H_1 : \{0,1\} \rightarrow G_1$, $H_2 : \{0,1\} \rightarrow Z_q$, $H : G_2 \rightarrow \{0,1\}^n$ - hash functions (n - message length, Z_q – ring of integers of order q), $ID \in \{1,0\}^n$ – recipient identity information, m – message. Key pair of recipient: $Q_{ID} = H_1(ID) \in G_1$, $B = sQ_{ID}$ – recipient`s public and secret key respectively. Key pair of trusted third party: $P_{pub} = sP$ – public key, s – master-key.

IV. CONCLUSION

Thus a promising direction to improve electronic document management systems is the implementation of combined PKI, as well as its mechanism of chameleon-hash. Implementation of a chameleon-hash allows adding properties to the innovative nature of cryptographic protocols in a combined PKI, to ensure secure operation of electronic commerce systems.

REFERENCES

[1] D. Boneh and M. Franklin, "Identity-based Encryption from the Weil pairing", Proceedings of CRYPTO 2001, LNCS 2139, pages 213-229, Springer-Verlag, 2001.

[2] G. Ateniese and B. de Medeiros, "Identity-based Chameleon Hash and Applications", Financial Cryptography 2004, Lecture Notes in Computer Science 3110, pages 164 – 180, 2004.