New Public Key Signature Scheme

Gurgen Khachatrian
American University of Armenia
Yerevan, Armenia
e-mail: gurgenkh@aua.am

Melsik K. Kyureghyan
Institute for Informatics and
Automation Problems
Yerevan, Armenia
e-mail: melsik@ipia.sci.am

ABSTRACT

In this paper a new public-key signature scheme is presented based on discrete logarithm problem. The specific of presented scheme is that the signature is addressed from a given user with given public key to another user with the different public key so only that recipient will be able to verify the signature from a specified user. The complexity of implementation is similar to Digital Signature Standard Algorithm (DSA).

Keywords

Public-key signature, digital signature algorithm, complexity.

1. INTRODUCTION

Digital signature standard algorithm (DSA) [1,2] is based on discrete logarithm problem and is designed to sign a document in the way that each user knowing the public key of the signer g^s can verify the signature. In many applications it is important that the document is signed in the way that only intended recipient with the public key g^r will be able to verify the signature.

In [3] a new approach has been introduced dealing with key exchange for broadcast applications. In this paper we show how that approach can be used to design a new public-key signature scheme that is based on discrete logarithm problem.

2. NEW PUBLIC-KEY SIGNATURE SCHEME

DSA algorithm can be explained as follows: Let we have shared global public key values (p,q,g): a large prime $p = 2^L$ where $L = 512$ to 1024 bits and is a multiple of 64; choose q, a 160 bit prime factor of $p-1$; choose $g = h^{(p-1)/q}$ where $h < p-1$, $h^{(p-1)/q}(\mathbf{mod}\, p) > 1$. Users choose private key $x < q$ and compute $y = g^x(\mathbf{mod}\, p)$.

To *sign* a message M the sender: generates a random signature key k, $k < q$, k must be random, be destroyed after use, and never be reused, then computes signature pair:

$$r = \left(g^k(\mathbf{mod}\, p)\right)(\mathbf{mod}\, q)$$

$$s = k^{-1} \cdot \left(H(M) + x \cdot r\right)(\mathbf{mod}\, q),$$

sends signature (r,s) with message M. Having received M and signature (r,s) to *verify* a signature, recipient computes:

$$w = s^{-1}(\mathbf{mod}\, q),$$
$$u1 = \left(H(M) \cdot w\right)(\mathbf{mod}\, q),$$
$$u2 = (r \cdot w)(\mathbf{mod}\, q),$$
$$v = \left(g^{u1} \cdot y^{u2}(\mathbf{mod}\, p)\right)(\mathbf{mod}\, q).$$

If $v = r$, then signature is verified.

In the DSA scheme everyone who has signer's public key can verify the signature. In the presented scheme the signature is intended to a specified user with a given public key. So we will use x_s, x_r and g^{x_s}, g^{x_r} to denote private and public keys for sender and receiver, respectively.

To *sign* a message M the sender: generates a random key r, $r < q$, r must be random, be destroyed after use, and never be reused, then computes signature pair:

$$S_1 = \left(g^{(x_r)\times r}(\mathbf{mod}\, p)\right)(\mathbf{mod}\, q)$$

$$S_2 = r^{-1} \cdot \left(H(M) + (x_s + r) \cdot g^r\right)(\mathbf{mod}\, q).$$

Having received M and signature (S_1, S_2) to *verify* a signature, recipient with a public key $g^{(x_r)}$ computes:

$$\left(g^{(x_r)\times r}\right)^{r_k} = g^r = t \; where \; (x_r)^{-1} = r_k$$

(only known to him) so only he/she can get g^r and then computes:

$$w = S_2^{-1}(\mathbf{mod}\, q) \text{ and } H(M),$$

$$u1 = H(M)w\,(\mathbf{mod}\,q),$$
$$u2 = (tw)(\mathbf{mod}\,q),$$
$$v = \left(g^{u1}\left(tg^{x_s}\right)^{u2}(\mathbf{mod}\,p)\right)(\mathbf{mod}\,q).$$

The signature is verified if $v = t$.Why it works? Since

$$v = g^{u1} \cdot \left(t \cdot g^{x_s}\right)^{u2} = g^{H(M)S_2^{-1}} g^{(r+x_s)g^{r}_{S_2^{-1}}}$$
$$= g^{S_2^{-1}\left(H(M)+(r+x_s)g^{r}\right)} = g^{r} = t.$$

The computational complexity of the proposed scheme is equivalent to DSA scheme. The advantage of the scheme is that only intended recipient of the message will be able to verify if the signature is valid.

3. CONCLUSION

We have presented a new public-key digital signature scheme based on discrete logarithm problem. In this scheme only chosen recipient of the message will be able to verify the signature. For some important applications this feature will eliminate the need for message encryption.

REFERENCES

[1] Taher ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Transactions on Information Theory*, v. IT-31, n. 4, 1985, pp. 469–472 *or* CRYPTO 84, pp. 10–18, Springer-Verlag.

[2]Schnorr C. “Efficient Signatures for smart card” *Journal of Cryptology*, pp. 161–174,No3, 1991.

[3] G.Khachatrian and M.Kuregian, “Note on LUCAS Public-key Algorithms and Key Exchange for Broadcast Applications”- Proceedings of the Second INTAS International Seminar on Coding Theory and Combinatorics, Essen, Germany, April 9-11, pp. 11-17 (1997).