A SIGNATURE ALGORITHM BASED ON DLP AND COMPUTING SQUARE ROOTS

Ounasser Abid[1] and Omar Khadir[2]

[1, 2] Laboratory of Mathematics, Cryptography and Mechanics, FSTM
University Hassan II of Casablanca, Morocco

ABSTRACT

In this work, we present a new digital signature protocol based on the discrete logarithm problem and computing square roots modulo a large composite number. This method can be used as an alternative if known systems are broken.

KEYWORDS

Public key cryptography, ElGamal signature scheme, discrete logarithm problem, Rabin digital signature

1.INTRODUCTION

Cryptography has become one of the fundamental tools of information and communications technology since the end of the last century. When digital signature algorithms were introduced, scientists tried to construct more secure and resistant signing procedures. The most significant models are RSA [9], Rabin method [8], ElGamal scheme [2] and Elliptic Curve Digital Signature Algorithm (ECDSA) [5, 7].

In this work, we propose a protocol that is based on a variant of ElGamal signature [4] and Rabin method [8]. Our scheme benefits from the hardness of the discrete logarithm problem and computing square roots modulo a large composite number, both believed to be intractable.

The article is arranged as follows. In the next section, we expose ElGamal signature and one of its variants. We devote the third section to describe our contribution and to analyze the security issue. The conclusion is given in the fourth section.

In the sequel, we use ElGamal paper notation. $\mathbb{Z}$ is the set of integers. For every positive integer n, we denote by $\mathbb{Z}/n\mathbb{Z}$ the finite ring of modular integers and by $(\mathbb{Z}/n\mathbb{Z})^*$ the multiplicative group of its invertible elements. Let a, b and c be three integers, we write $a \equiv b \pmod{c}$ if c divides the difference $a - b$, and $a = b \bmod c$ when a is the remainder of the division of b by c.

2. VARIANT OF ELGAMAL SIGNATURE SCHEME

2.1. Elgamal Signature Protocol

In this section we recall ElGamal signature scheme [2], in three steps.

Step 1. Alice chooses three numbers:

-p, a large prime integer.
-α, a primitive root of the finite multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$.
-x, a random element of $\{1, 2, \ldots, p-1\}$.

Then she computes $y = \alpha^x \bmod p$. Parameters (p, α, y) and x are respectively Alice public and private key.

Step 2. To sign a message m , Alice needs to solve the equation:

$$\alpha^m \equiv y^r r^s \pmod{p} \quad (1)$$

where r, s are the unknown variables.

Alice fixes arbitrarily r to be $r = \alpha^k \bmod p$, where k is chosen randomly and invertible modulo $p-1$. Equation (1) is then equivalent to:

$$m \equiv xr + ks \pmod{p-1} \quad (2)$$

As Alice knows the secret key x, and as the integer k is invertible modulo $p-1$, she computes the other unknown variable $s \equiv \frac{m-xr}{k} \pmod{p-1}$.

Step 3. Bob can verify the signature by checking that congruence (1) is valid for the variables r and s given by Alice.

In the next section, we describe briefly a digital signature protocol that was conceived by one of the authors in 2011 [4].

2.2. Variant of ElGamal Signature Protocol

Let $m = h(M)$, where h is a secure hash function (e.g., SHA1 [6,10]), and M the message to be signed by Alice.

The modulo p is a large prime integer. Element α is a primitive root of the finite multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. Number y is calculated by $y = \alpha^x \bmod p$, where x is chosen randomly in $\{1, 2, \ldots, p-1\}$.

The variant [4] is based on the equation:

$$\alpha^t = y^r r^s s^m \pmod{p} \quad (3)$$

Parameters r, s, t are unknown and (p, α, y) is Alice public key. To Solve (3), Alice fixes arbitrarily r to be $r = \alpha^k \bmod p$, and s to be $s = \alpha^l \bmod p$, where k, l are selected randomly in $\{1,2, \ldots, p-1\}$. Equation (3) is then equivalent to:

$$t \equiv rx + ks + lm \pmod{p-1} \quad (4)$$

Alice knows the values of r, s, k, l, m and x, she can compute the third unknown variable t. Bob verifies the signature by checking the congruence (3).

This scheme has the advantage that it does not use the extended Euclidean algorithm for computing $k^{-1} \mod (p-1)$.

Now, we move to our contribution.

3. OUR SIGNATURE PROTOCOL

In this section we propose our contribution and analyze its security

3.1. Description of the Protocol

Let P be a prime integer in the form $P = 2pq + 1$, where p and q are two distinct primes such as $p \equiv -1 \pmod 4$ and $q \equiv -1 \pmod 4$. Alice public key is (P, α, y), where α is a primitive root of the finite multiplicative group $(\mathbb{Z}/P\mathbb{Z})^*$. Let $y \equiv \alpha^x \pmod P$, Alice must keep x secret. The parameters x, p and q constitute Alice private key. We propose the following new protocol:

To sign m the hash of a message M, Alice has to give a solution of the equation:

$$\alpha^{t^2} \equiv y^r r^s s^m \pmod P \quad (5)$$

Where r, s, t are the unknown parameters. To solve the congruence (5) Alice puts $r = \alpha^k \pmod P$ and $s = \alpha^l \pmod P$, where k and l are randomly chosen in $\{1, 2, \ldots, P-1\}$.

Equation (5) is equivalent to:

$$t^2 \equiv rx + ks + lm \pmod{P-1} \quad (6)$$

We have
$$(6) \Leftrightarrow \begin{cases} t^2 = rx + ks + lm \pmod 2 \\ t^2 = rx + ks + lm \pmod p \\ t^2 \equiv rx + ks + lm \pmod q \end{cases}$$

Alice will use the Chinese remainder theorem to calculate t from (6), provided that the expression $rx + ks + lm$ is a quadratic residue modulo p and modulo q, which can be verified by using Legendre symbol [10].

Let us illustrate the method by the following example.

3.2. Example

Suppose that Alice private key is $(p, q, x) = (43,107,281)$. So $P = 9203$. We take the primitive element modulo P as $\alpha - 2$ so $y \equiv \alpha^x \equiv 8970\ (mod\ P)$. Thus the public key is $(P, \alpha, y) - (9203,2,8970)$.

Let $k = 5025$ and $l = 1265$ be two random exponents chosen by Alice. We have $r \equiv 2^k \equiv 6092\ (mod\ P)$ and $s \equiv 2^l \equiv 5855\ (mod\ P)$.

To sign $m = h(M) = 432$ the hash of a message M, Alice will need equation (6) to get t the third element of the signature.

We have:

$$t^2 \equiv 6423\ (mod\ P-1) \Leftrightarrow \begin{cases} t^2 \equiv 1\ (mod\ 2) \\ t^2 \equiv 16\ (mod\ p) \\ t^2 = 3\ (mod\ q) \end{cases}$$

$$\Leftrightarrow \begin{cases} t \equiv 1\ (mod\ 2) \\ t \equiv +4\ (mod\ p) \\ t \equiv \pm 89\ (mod\ q) \end{cases}$$

By using the Chinese remainder theorem, Alice finds four valid values for t: $9077, 7615, 1587, 125$. Then, she chooses for example $t \equiv 1587\ (mod\ P-1)$.

If we replace r, s and t in equation (5) we can verify that (r, s, t) is a valid solution. Therefore, Alice signature for the message M is $(r, s, t) = (6092, 5855, 1587)$.

Now, we analyze the security of our protocol.

3.3. Security Analysis

In this section we discuss four possible attacks. Assume that Oscar is Alice opponent.

Attack 1:

a) If Oscar fixes r and s, he cannot obtain t from equation (5) because, knowing the right part of the equivalence, he has to solve discrete logarithm problem to get t^2. And if he succeeded, he would have to calculate the square root of t^2 modulo the large prime P. A task that seems to be as hard as factoring (see [6,8,10]).

b) If he fixes r and t in order to get s, then, formula (5) is equivalent to $\alpha^{t^2} y^{-r} = r^s s^m\ (mod\ P)$, for which, there is no known way to determine s. Oscar cannot use equation (6) as long as he ignores the value of x kept secret by Alice.

c) If he fixes s and t and wants to get r, then, from formula (5) we have $\alpha^{t^2} s^{-m} \equiv y^r r^s\ (mod\ P)$, and there is no known way to determine s from this equivalence. Oscar cannot use equation (6) as long as he ignores the value of x kept secret by Alice.

Attack 2: If Oscar takes Alice's signature (r, s, t) of a message M, and tries to acquire x. From equation (6) we have $t^2 \equiv rx + ks + lm \ (mod\ P-1)$, calculating x from this equivalence is impossible, because k and l remain unknown.

Attack 3: Assuming Oscar is able to solve the discrete logarithm problem [2]. So he can find Alice private exponent x, therefore, computes $X \equiv t^2 \ (mod\ P-1)$ from equation (6). However, calculating t from the modular equation $t^2 \equiv X \ (mod\ P-1)$ is believed to be as hard as factoring the large composite number $(P-1)$ (see [6,8,10])

Attack 4: Assuming Oscar is able to solve Rabin modular equation $t^2 = a \ (mod\ P \quad 1)$, where t is the unknown variable. He would like to exploit relation (6) to find t. But, he needs x, and to have x he must solve a discrete logarithm problem, since $y = a^x \ mod\ P$.

3.4. Complexity of our Scheme

As in reference [3], let T_{mult}, T_{exp} and $T_h$be respectively the time to perform a modular multiplication, a modular exponentiation and to compute the hash of a message M. The time needed for operations such as comparison, modular addition and substraction is ignored. We make the conversion $T_{exp} = 240T_{mult}$.

Generating a signature requires six modular exponentiations, three modular multiplications and one hash function computation. The estimated time for signing a message is:

$$T_s = 6T_{exp} \ | \ 12T_{mult} \ | \ T_h = 1452T_{mult} \ | \ T_h$$

To verify a message, Bob needs to perform five modular exponentiations, two modular multiplications and one hash function computation. The estimated verification time is:

$$T_v = 5T_{exp} + 2T_{mult} + T_h = 1202T_{mult} + T_h$$

4. CONCLUSION

In this paper we presented a new digital signature method. It is based on two hard equations: discrete logarithm problem and computing square root modulo a large integer. We also discussed its security and complexity.

5. ACKNOWLEDGEMENTS

This work is supported by MMSy e-Orientation project.

REFERENCES

[1] W. Diffie and M. E. Hellman: New directions in cryptography. IEEE Transactions on Information Theory, vol. IT-22, (1976), pp. 644-654.

[2] T. ElGamal: A public key cryptosystem and a signature scheme based on discrete logarithm problem. IEEE Trans. Info. Theory, IT-31, (1985), pp. 469-472.

[3] E. S. Ismail, N. M. F. Tahat and R. R. Ahmad: A new digital signature scheme based on factoring and discrete logarithms. J. of Mathematics and Statistics (4): (2008), pp. 222-225.

[4] O. Khadir: New variant of ElGamal signature scheme. Int. J. Contemp. Math. Sciences, Vol. 5, no. 34, (2010), pp. 1653-1662.

[5] N. Koblitz: Elliptic curve cryptosystem. Math. Comp. 48 (1987), pp. 203-209.

[6] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone: Handbook of applied cryptography. CRC Press, Boca Raton, Florida, 1997. Available at http://www.cacr.math.uwaterloo.ca/hac/

[7] V. Miller: Uses of elliptic curves in cryptography. In: H.C. Williams (Ed.), Advances in Cryptology: Proceedings of Crypto'85, Lecture Notes in Computer Science, Vol. 218, Springer, Berlin, 1985, pp. 417-426.

[8] M. O. Rabin: Digitalized signatures and public key functions as intractable as factoring. MIT/LCS/TR, Vol. 212, (1979).

[9] R. Rivest, A. Shamir and L. Adeleman: A method for obtaining digital signatures and public key cryptosystems, Communication of the ACM, Vol. no 21, (1978), pp. 120-126.

[10] D. R. Stinson: Cryptography, theory and practice, Third Edition, Chapman & Hall/CRC, 2006.