Journal of Universal Mathematics
Vol.1 No.2 pp.104-109 (2018)
ISSN-2618-5660

A SECURE VARIANT OF SCHNORR SIGNATURE USING THE RSA ALGORITHM

L. ZAHHAFI AND O. KHADIR

Abstract. In this paper we propose a topic on cryptography. It is a digital signature protocol. Indeed, we have improved the signature of Schnorr based on the problem of the discrete logarithm to make it more secure. We integrated the RSA algorithm into our scheme, which secures the signature process even if the signer uses the same signature key.

1. Introduction

Since the creation of the Internet, communications between people and most of their transactions have become automatic and take place via this network. However, any information transferred via the Internet may be intercepted by a non-honest entity. Hence, the security of this information needs to be strengthened. And this is the role of cryptography that allows to encrypt all secret data to guarantee its confidentiality.

Public key cryptography protects the process of message exchange between two parties using secret and public keys. It must guarantee the confidentiality, integrity and authentication.

Many topics are studied in cryptography. In particular digital signature is an important research area. This concept guarantees the integrity of an electronic document and authenticates its author.

To sign a message M, the signer begins with the creation of its private and public keys respectively K_{pr} and K_{pb}. He then calculates the signature of its message by an encryption function using its secret key K_{pr}. The verifier can check the signature validity using the decryption function and the public key of the signer K_{pb}.

As all cryptographic protocols, the digital signature is based on hard mathematical problems. Among them, the discrete logarithm problem [3,11]. It allows to solve modular exponentiation $a^x \equiv b\,[p]$ with p is a large prime, a a primitive root of the finite multiplicative group $\mathbb{Z}/p\mathbb{Z}$ and x is the unknown. Several digital signature protocols are based on this kind of mathematical problems. We quote the signature of ElGamal [4] proposed in 1985, and its variant [5] which are among the most known schemes.

Factorization of large numbers [1,2,7,11] is also a tool used in the digital signatures.

Date: June 1, 2018, accepted.
2000 *Mathematics Subject Classification.* 11T71, 94A60.
Key words and phrases. Digital signature, Discrete logarithm problem, Factorization.

Since we need to execute factorization to solve a modular polynomial equation like: $x^k \equiv b\,[n]$ with: k is an integer, x the unknown and n is a large composite integer. It presents the basic for several encryption systems used in the exchange of sensitive informations. In 1978, Rabin [8] proposed a signature scheme using the equation: $x^2 \equiv b\,[n]$ where n is large composite number. In the same year, Rivest, Shamir and Adleman published a paper in which they proposed a new cryptosystem and a strong digital signature scheme based on the factorization of large numbers.

In this article, we present a new digital signature scheme. We are inspired by the work of Schnorr [10]. Indeed, We have improved this protocol to make it more stronger by integrating the RSA algorithm.

The paper is organized as follows: We recall in section 2 the Schnorr signature. In section 3, we presents the algorithm of RSA. Then, we show the steps of our signature protocol in section 4. We end by a conclusion in section 5.

We denote by $\mathbb{Z}/n\mathbb{Z}$ the finite ring of modular integers for every positive integer n. We write $x \equiv y\,[n]$ if n divides the difference $x - y$ with: x, y and n are three integers. $||$ presents the concatenation operator.

2. Schnorr signature

The Schnorr signature [10] is a cryptographic algorithm proposed in 1990. It's based on the difficulty of solving a discrete logarithm problem.
To generate signature parameters, a trusted center chooses a large prime p, a primitive root a of the finite multiplicative group $\mathbb{Z}/p\mathbb{Z}$ and a one way hash function h. It selects randomly $x \in \{1, 2, 3..., p-1\}$ and computes $y \equiv a^x\,[p]$. The center gives x to Alice as her private key and y as her public key.

2.1. Signature generation.

To sign a message M, Alice follows the steps:

(1) She chooses a random $k \in \{1, 2, 3..., p-1\}$ and calculates: $r \equiv a^k\,[p]$.
(2) She computes $b = h(r||M)$ where $||$ is the concatenation operator.
(3) Finally, Alice generates: $s = k - xb$.

So, the signature is the pair: (s, b).

2.2. Signature verification.

To verify Alice signature, the verifier Bob performs the following operations:

(1) He calculates: $r_v \equiv a^s y^b\,[p]$.
(2) Then, Bob computes $b_v = h(r_v||M)$.

Bob checks if $b = b_v$ and accepts or rejects the Alice's signature.
Indeed, to sign the message, we have: $r_v \equiv a^s y^b \equiv a^{k-xb} y^b\,[p]$. As $y \equiv a^x\,[p]$, $r_v \equiv a^{k-xb} a^{xb} \equiv a^k \equiv r\,[p]$. Finally, $b_v = h(r_v||M) = h(r||M) = b$. The result was then proven.

Example 2.1. Suppose that the trusted center generates the prime $p = 4608587$ and $a = 2$, a primitive root of the finite multiplicative group $\mathbb{Z}/p\mathbb{Z}$. It chooses $x = 105$ as Alice's secret key. So, $y \equiv a^x \equiv 1284681\,[p]$ is her public key.
Alice selects $k = 3876528$. Then, she calculates: $r \equiv a^k \equiv 582965\,[p]$. Assume that she wants to sign the message M, where: $b = h(r||M) = 13211$. So, Alice generates $s = k - xb = 2489373$.The signature is the pair $(2489373, 13211)$.

Bob verifies Alice signature as follows:
He calculates: $r_v \equiv a^s y^b \equiv 582965\,[p]$. Then, he computes $b_v = h(r_v||M) = 13211$.
While $b = b_v = 13211$, Bob accepts this signature.

Remark 2.2. If Alice signs two messages M_1 and M_1 using the same signature key k, then her private key x will be disclosed.
Indeed, to sign the messages M_1 and M_2, Alice calculates: $s_1 = k - xb_1$ and $s_2 = k - xb_2$. By subtracting, we find: $s_1 - s_2 = k - xb_1 - k + xb_2$. So, $x = \dfrac{s_1 - s_2}{b_2 - b_1}$.

3. RSA algorithm (1977)

RSA's signature algorithm is the same as encryption. It is based on the problem of factorization of large numbers.
To generate the RSA keys, a trusted center chooses two large primes p and q and calculates their product $n = pq$. Then, it finds $\varphi(n)$ and selects an integer e where $gcd(e, \varphi(n)) = 1$. Now, the trusted center can calculate the value of d that verifies: $d \equiv \dfrac{1}{e}\,[\varphi(n)]$ as the private key of Alice.
To sign a message M Alice have to solve the fallowing equation: $M \equiv X^e\,[n]$.
Using her private key d, Alice finds: $X \equiv M^d\,[n]$. So, the verifier Bob checks Alice signature by replacing the value X in the above equation. Then, he accepts or rejects her signature.

Example 3.1. Let's take $p = 1319$ and $q = 1747$, $n = pq = 2304293$. Alice chooses $e = 7$ prime with $\varphi(n) = 2301228$. She calculates her private key $d \equiv \dfrac{1}{e} \equiv \dfrac{1}{7} \equiv 328747\,[2301228]$.
Suppose that Alice wants to sign the message $M = 1234$. So, she solves this equation: $1234 \equiv X^7\,[2304293]$ using her secret key.
$X \equiv M^d \equiv 1234^{328747} \equiv 152888\,[2304293]$
While $M \equiv X^e \equiv 152888^7 \equiv 1234\,[2304293]$, Bob accepts Alice signature.

4. Our contribution

In this section, we present our new signature protocol. We describe the different steps to sign a message M.

4.1. **Description of the protocol.** We will insert the RSA algorithm into the signature presented in section 2. We start by generating the signature keys.
The trusted center generates the keys for both Schnorr and RSA signatures as follows:

- $P = 2pq + 1$ where P, p and q are primes.
- A primitive root a of the finite multiplicative group $\mathbb{Z}/P\mathbb{Z}$.
- A one way hash function h.
- A Schnorr private key $x \in \{1, 2, 3..., P - 1\}$.
- The public key $y \equiv a^x\,[P]$.
- A public RSA exponent e that verifies $gcd(e, \varphi(P - 1)) = 1$.
- The RSA secret key of Alice is: $d \equiv \dfrac{1}{e}\,[\varphi(P - 1)]$.

Parameters P, a, y and e are Alice public key. Elements x and d are Alice secret key. Observe that p and q must be destroyed for security reasons.

4.2. **Signature generation.** To sign a message M, Alice follows the steps:

(1) She chooses a random $k \in \{1, 2, 3..., P-1\}$. Then, she calculates: $r \equiv a^k \,[P]$.
(2) She computes $b' = h(r||M)$ with $||$ is the concatenation operator.
(3) Finally, She generates: $s' = k - xb'$.

Now, Alice calculates s and b using the RSA private key d. She executes this two modular equations: $s \equiv s'^d \,[P-1]$ and $b \equiv b'^d \,[P-1]$. So, the signature is the pair (s, b).

4.3. **Signature verification.** To verify Alice signature, Bob executes these operations using the pair (s, b) and Alice public keys:

(1) He calculates: $r_v \equiv a^{s^e} y^{b^e} \,[P]$.
(2) Then, he computes $b_v = h(r_v||M)$.

Bob checks if $b_v \equiv b^e \,[P-1]$. He accepts Alice signature if and only if the modular equation is valid.

Example 4.1. Suppose that the trusted center generates the primes $p = 1319, q = 1747$ and $P = 4608587$, $a = 2$, a primitive root of the finite multiplicative group $\mathbb{Z}/P\mathbb{Z}$. Then, it chooses $x = 105$ as Alice Schnorr secret key. So, $y \equiv a^x \equiv 1284681 \,[P]$ is her public key. About the RSA keys, we fix $e = 7$ and $d \equiv \dfrac{1}{e} \equiv 328747 \,[\varphi(P-1)]$, with $\varphi(P-1) = \varphi(2pq) = (p-1)(q-1) = 2301228$.
Alice selects $k = 3876528$. Then, she calculates: $r \equiv a^k \equiv 582965 \,[P]$. Assume that she wants to sign the message M where: $b\prime = h(r||M) = 13211$. So, Alice have to generate $s\prime = k - xb\prime = 2489373$. Then, she finds $s \equiv s\prime^d \equiv 2489373^{328747} \equiv 2856453 \,[P-1]$ and $b \equiv b\prime^d \equiv 13211^{328747} \equiv 3937057 \,[P-1]$.
The signature is the pair, $(2856453, 3937057)$.
Bob verifies Alice signature as follows:
He calculates: $r_v \equiv a^{s^{e[P-1]}} y^{b^{e[P-1]}} \equiv 582965 \,[P]$. Then, he computes: $b_v = h(r_v||M) = 13211$.
As $b_v \equiv b^e \equiv 3937057 \,[P-1]$, Bob accepts this signature.

4.4. **Security analysis.** Before describing possible attacks we have the next fact:

Theorem 4.2. *If an attacker can break our scheme, then he can also break Schnorr protocol.*

Proof. If the attacker can solve the equation $h(a^{s^e} y^{b^e}||M) = b^e \,[P-1]$, where s and b are the unknown variables, then he will be able to solve the Schnorr signature equation $h(a^s y^b||M) = b \,[P-1]$. The protocol that we proposed depends simultaneously on discrete logarithm problem and factorization. But the Schnorr scheme is based only on discrete logarithm problem. So, our method is stronger then that of Schnorr. □

Assume that Oscar is an attacker.

- **Attack 1:** Using the public key y, Oscar will not be able to find the Schnorr private key of Alice x. Indeed, he must solve the discrete logarithm problem: $y \equiv a^x \,[P]$.
- **Attack 2:** Using the public key e, Oscar will not be able to find the RSA private key of Alice: $d \equiv \dfrac{1}{e} \,[\varphi(P-1)]$. Indeed, he must factor the large number $P-1 = 2pq$ to calculate the Euler function: $\varphi(P-1) = (p-1)(q-1)$.

- **Attack 3:** As we have already seen above, if Alice signs two messages M_1 and M_2, by Schnorr method, using the same signature key k, then her private key x will be disclosed. So, the attacker Oscar will be able to propose s^e and b^e instead of Alice that verify the signature equation: $r \equiv a^{s^e} y^{b^e} [P]$. However, he can't find the values of s and b since he does not hold Alice RSA private key. So, even if Alice signs two messages using the same signature key k the protocol will not be broken.

Remark 4.3. Breaking this signature is very difficult for attackers as there are no algorithm to solve a modular polynomial equation or a discrete logarithm problem in an acceptable time.

4.5. **Complexity.** In this paragraph, we discuss the complexity of our method. So, let T_{exp}, T_{mult} and T_h the times necessary to calculate respectively an exponentiation, a multiplication and a hash function. To generate her keys y and d, Alice needs to execute one modular exponentiation and one modular multiplication. In the signature step, she performs 3 modular exponentiations, one multiplication and one hash function. To verify Alice signature, Bob calculates 6 modular exponentiations, one multiplication and one hash function. So, there are 9 modular exponentiations, 3 multiplications and two hash function. In other words, the total time T_{tot} required to execute all the signature operations is:

$$T_{tot} = 9T_{exp} + 3T_{mult} + 2T_h$$

We have: $T_{exp} = O((\log n)^3)$ and $T_{mult} = O((\log n)^2)$, (see [7]). And we suppose that: $T_h = O((\log n)^2)$. So, the final complexity of our signature scheme is as follows:

$$T_{tot} = O((\log n)^2 + (\log n)^3)$$

Finally, we assume that the protocol works on a polylogarithmic time.

5. Conclusion

In this paper, we presented an amelioration of the Schnorr signature that makes it more secure against different possible attacks. With our change, Schnorr protocol becomes more efficient and secure. Our contribution allows Alice to sign several messages with the same signature key.

Acknowledgements

This work is supported by the MMS e-orientation project.

References

[1] Adleman, L. M., Pomerance, C., & Rumely, R. S. (1983), On distinguishing prime numbers from composite numbers, *Ann. Math*, pp 173−206.
[2] Agrawal, M., Kayal, N., & Saxena, N. (2004), Primes in P, *Annals of Mathematics* , pp 781−793.
[3] Den Boer, B. (1988), Diffie-Hellman is as strong as discrete log for certain primes, *In Crypto*.
[4] ElGamal, T. (1985), A public key cryptosystem and a signature scheme based on discrete logarithm problem, *IEEE Trans. Info. Theory , IT-31*.
[5] Khadir, O., (2010), New variant of ElGamal signature scheme, *Int. J. Contemp. Math. Sciences*Vol. 5, no. 34.
[6] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996) *Handbook of applied cryptography*, pp 72.

[7] Pollard, J. M. (1975), A Monte Carlo method for factorization, *BIT Numerical Mathematics*, pp 331−334.
[8] Rabin, M.O., (1978), Digital signatures and public-key functions as intractable as factorization, *Technical Report MIT/LCS/TR-212*.
[9] Rivest, R., Shamir, A., & Adeleman, L. (1978), A method for obtaining digital signatures and public key cryptosystems, *Communication of the ACM*,Vol. no 21.
[10] Schnorr, C.P., (1991), Efficient Signature Generation by Smart Cards, *Journal of Cryptology*, pp 161−174.
[11] Shor & Peter (1997), Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM Journal on Computing*, pp 1484−1509.

Laboratory of Mathematics, Cryptography, Mechanics and Numerical Analysis.
Current address: University Hassan II of Casablanca, fstm, 146, Mohammedia, Morocco.
E-mail address, L. Zahhafi: `leila.zahhafi@gmail.com`
E-mail address, O. Khadir: `khadir@hotmail.com`