Int. J. Adv. Appl. Math. and Mech. 3(1) (2015) 92 – 97 (ISSN: 2347-2529)

Journal homepage: www.ijaamm.com

IJAAMM

International Journal of Advances in Applied Mathematics and Mechanics

New variant of Guillou-Quisquater digital signature scheme

Research Article

J. Ettanfouhi, O. Khadir *

Laboratory of Mathematics, Cryptography and Mechanics, Fstm, University Hassan II of Casablanca, Morocco

Received 20 May 2015; accepted (in revised version) 14 August 2015

Abstract: In this work, we present a new digital signature protocol. The scheme, derived from Guillou-Quisquater signature method, is an alternative protocol if existing systems are broken. We discuss its efficiency and security.

MSC: 94A60 • 90C90

Keywords: Public key cryptography • RSA • Guillou-Quisquater signature scheme

1. Introduction

The security of electronic communication has been extensively studied since the invention of the public key cryptography [1–3]. Other subjects as authentication, zero-knowledge and digital signature were explored. One of the most known cryptosystem is RSA algorithm [2]. A signature protocol allows to sign an electronic contract. Let us review the principle of the method. The signer Alice has two kinds of keys. A private one, must be kept secret and the second is public. If she likes to sign a document M, she has to solve a hard mathematical equation. It depends of the message M, and of her public key. With the help of her private key, Alice can give a solution to the problem. The verifier Bob checks if the answer calculated by Alice is valid. Nobody is able to imitate her signature, even the interrogator himself.

Existing signatures schemes were designed by developing hard problems, like discrete logarithm and factoring [2–9]. These algorithms, for the time being, appear safe and secure. But in a near future they can be broken. Hence, the need of creating new alternatives.

At Eurocrypt'88 Guillou and Quisquater introduced first, an interactive zero-knowledge protocol. In 1990, they published a paper [6] where they exposed a remarkable digital signature system. Their technique was based on RSA algorithm.

In this work, we present a variant of Guillou-Quisquater scheme and create a new signature method. We analyze its efficiency and security. For its theoretical interest, we also give a general form of our system equation.

The paper is organized as follows: In section 2 we recall the basic Guillou-Quisquater signature scheme. We review some possible attacks. Then we present our new variant with a theoretical generalization in section 3. Section 4 is devoted to the conclusion.

In the sequel, we will respect Guillou-Quisquater paper notations [6]. $\mathbb{N}$, $\mathbb{Z}$ are respectively the sets of integers and non-negative 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,c be three integers. The great common divisor of a and b is denoted by $gcd(a,b)$. We write $a \equiv b \ (mod\ c)$ if c divides the difference $a-b$, and $a = b \mod c$ if a is the remainder in the division of b by c. The bit-length of an integer n is the number of bits in its binary representation. $a||b$ is the concatenation of a and b.

We start by describing the Guillou-Quisquater signature method.

* Corresponding author.

E-mail addresses: ettanfouhi@gmail.com (J. Ettanfouhi), khadir@hotmail.com (O. Khadir)

2. Guillou-Quisquater signature scheme

In this section we review Guillou-Quisquater signature system[6]. We Also discuss some known attacks. The protocol needs three short steps: generating parameters, signing message and verifying signature.

2.1. Guillou-Quisquater algorithm

Let h be a secure public hash function like SHA1 [10, chap.9] or [11, chap.5].

1. To generate the keys:
   - Alice chooses randomly two large primes P and Q, then she calculates $n = PQ$.
   - She takes an integer $0 < v < \varphi(n)$, where $\varphi(n)$ is the phi-Euler function.
   - She selects randomly an identification variable B and computes:

$$J = B^v \mod n \tag{1}$$

   We consider then that (n, v, J) and B are respectively Alice public and private key.

2. Assume that Alice wants to sign the message $M < n$. She must solve the following modular equation:

$$t^v \equiv T J^{h(M||T)} (mod\ n) \tag{2}$$

   where t, T are unknown variables.

   To solve equation (2), Alice fixes arbitrary T to be $T = r^v\ mod\ n$, where r is chosen randomly. Then she finds:

$$t \equiv r B^{h(M||T)} (mod\ n) \tag{3}$$

As Alice knows the secret key B, she computes the second unknown variable t by congruence (3). Note that there are many couples (t, T) solutions of the relation (2).
3. Bob can verify the signature by checking if equation (2) is valid for the variables t and T furnished by Alice.
Now, we discuss some possible attacks.

2.2. Main known attacks

In this subsection we present situations where the dishonest Oscar is able to forge Alice signature.

Attack 1:
The first attack is cited in the "handbook of applied cryptography" ([10] , chap.11). In Guillou-Quisquater system, the integer v must be sufficiently large. This choice excludes the possibility of forging Alice signature. We briefly describe this attack.
Oscar chooses a message M. He computes $l = h(M||T)$ where

$$T \equiv J^{-s} (mod\ n) \tag{4}$$

for many values of s, until obtaining $l \equiv s\ (mod\ v)$ He determines an integer x, such as

$$s = xv + l \tag{5}$$

then he calculates

$$t = J^{-x} \mod n \tag{6}$$

To sign the document M, Oscar must solve the following congruence with the unknowns T and t:

$$t^v \equiv T.J^l (mod\ n) \tag{7}$$

He uses (4), (5) and (6) to prove (7) as follows :

$$T J^l \equiv J^{-s} J^l \equiv J^{-s+l} \equiv (J^{-x})^v \equiv (t)^v (mod\ n)$$

So in this case, Oscar has forged Alice signature. Hence the need of using a large value of the integer v.
We move to the second possible attack.

Attack 2:

Let (n_A, v_A, J_A, B_A) and (n_O, v_O, J_O, B_O) be respectively Alice and Oscar keys in a Guillou-Quisquater signature protocol. Suppose that Oscar tries to forge fraudulently Alice signature for the message M. He replaces, in the key server distribution, Alice's public key by (n_O, v_O, J_O). He signs the message M by giving (T_O, t_O) to the verifier Bob. As consequence, it is recommended to use a very secure key server distribution.
There is another possible attack.

Attack 3:
Let (n, v, J) be Alice public key. If Oscar obtains the signature of two messages M_1 and M_2 he can make the following operations:

$$\begin{cases} t_1^v \equiv T_1 J^{h(M_1||T_1)} (mod\ n) \\ t_2^v \equiv T_2 J^{h(M_2||T_2)} (mod\ n) \end{cases}$$

so

$$(t_1 t_2)^v \equiv T_1 T_2 J^{h(M_1||T_1)+h(M_2||T_2)} (mod\ n) \tag{8}$$

If Oscar finds an interesting message M where:

$$h(M||T_1 T_2) = h(M_1||T_1) + h(M_2||T_2)$$

congruence (8) becomes:

$$(t_1 t_2)^v \equiv T_1 T_2 J^{h(M||T_1 T_2)} (mod\ n)$$

As Oscar knows T_1, t_1, T_2 and t_2, he proves illegally that Alice has signed the document M. Now, we propose our Guillou-Quisquater signature variant.

3. Our Protocol and its Theoretical Generalization

In this section we describe a new variant of Guillou-Quisquater signature scheme based on an equation with three unknown variables.

3.1. Our protocol

Assume that h is a secure public hash function like SHA1 ([10] , chap. 9) or ([11], chap. 5).

1. To generate the parameters:
   - Alice chooses randomly two large primes P and Q, then she calculates $n = PQ$.
   - She takes an integer $0 < v < \varphi(n)$.
   - She selects randomly two identifications messages B_1 and B_2, then computes:

$$\begin{cases} J_1 = B_1^v \mod n \\ J_2 = B_2^v \mod n \end{cases}$$

   We consider then that (n, v, J_1, J_2) is Alice public key, and (B_1, B_1) her private one.

2. If Alice wants to sign the contract $M < n$. She must solve the following modular equation:

$$Z^v \equiv T t J_1^{h(M||T)} J_2^{h(M||t)} \ (mod\ n) \tag{9}$$

   where T, t and Z are the unknown variables.
   To solve equation (9), Alice fixes arbitrary T to be $T = r_1^v\ mod\ n$ and t to be $t = r_2^v\ mod\ n$, where r_1 and r_2 are chosen randomly. Then she finds:

$$Z \equiv r_1 r_2 B_1^{h(M||T)} B_2^{h(M||t)} (mod\ n) \tag{10}$$

   As Alice detains the secret key (B_1, B_2), she can find the third unknown variable Z by congruence (10).

3. Bob checks if the signature (T, t, Z) is valid for the relation (9).

Our system has the advantage that Oscar must solve two hard problems instead of one. To illustrate this algorithm, we give an example.

3.2. Example

Let (n, v, J_1, J_2)=(12393217, 127, 9468104, 631477) and (B_1, B_2)=(4536, 19519) be respectively Alice public and private key. Suppose that she wants to sign the message M=2015. To simplify, we assume that the hash function $h(x)$ result the sum of the digits of the integer x modulo 100. Alice chooses randomly (r_1, r_2)=(119, 205). She starts by computing $T = r_1^v \mod n = 6581159$ and $t = r_2^v \mod n = 6301624$. Then $h(M||T) = h(20156581159) = 43$ and $h(M||t) = h(20156301624) = 30$. Hence

$$Z \equiv r_1 r_2 B_1^{h(M||T)} B_2^{h(M||t)} \mod n = 9322383.$$

To validate the signature, we check that

$$Z^v \mod n = T t J_1^{h(M||T)} J_2^{h(M||t)} \mod n = 1018378$$

Now, we study the security of our method.

3.3. Security analysis

Assume that Oscar is Alice's opponent.

Attack 1:

As in Guillou-Quisquater system, in our protocol the integer v must be sufficiently large. This choice excludes the possibility of imitating Alice signature. We briefly describe this attack.
The fraudulent Oscar chooses a message M. He computes

$l_1 = h(M||T)$ and $l_2 = h(M||t)$ where

$$T \equiv J_1^{-s_1} (mod\ n) \tag{11}$$

$$t \equiv J_2^{-s_2} (mod\ n) \tag{12}$$

for many values of s_1 and s_2, until obtaining $l_1 \equiv s_1 (mod\ v)$ and $l_2 \equiv s_2 (mod\ v)$. He determines two integers x and y, such as

$$s_1 = xv + l_1 \tag{13}$$

$$s_2 = yv + l_2 \tag{14}$$

then he calculates

$$Z \equiv J_1^{-x} J_2^{-y} (mod\ n) \tag{15}$$

To sign the document M, Oscar must solve the following congruence with T, t and Z as unknown variables:

$$Z^v \equiv T t J_1^{l_1} J_2^{l_2} (mod\ n) \tag{16}$$

He uses (11), (12), (13), (14) and (15) to prove (16) as follows:

$$T t J_1^{l_1} J_2^{l_2} \equiv J_1^{-s_1} J_2^{-s_2} J_1^{l_1} J_2^{l_2} \equiv (J_1^{-x} J_2^{-y})^v = Z^v (mod\ n)$$

So in this case, Oscar has forged Alice signature.
As a recommendation, cryptography designers must always use a large value of the integer v.

Attack 2:

Knowing All public signature parameters for a document M, Oscar tries to find Alice secret keys B_1 and B_2. He is confronted to two hard modular equations instead of one in Guillou-Quisquater scheme.

Attack 3:

Oscar wants to imitate Alice signature for a contract M. He fixes arbitrary two unknown variables and tries to find the third parameter.
(1) Suppose that he fixes T and t, and likes to solve the modular congruence (9). But here, he will face a modular polynomial equation. We don't know a method for solving that kind of problems.
(2) Suppose that he fixes (T, Z) or (t, Z), and wants to solve equation (9). But here, we have a weird equation and today there is no way to find its solution.

3.4. Complexity of our algorithm

As in [12], let T_{exp}, T_{mult} and T_h be respectively the time to perform a modular exponentiation, a modular multiplication and hash function computation of a message M. We ignore the time required for modular additions, substraction, comparisons and make the conversion $T_{exp} = 240T_{mult}$.
From subsection 3.1, we see that the signer Alice needs to perform six modular exponentiations, three modular multiplications and two hash functions computation. The global required time is:

$$T_s = 6T_{exp} + 3T_{mult} + 2T_h = 1443T_{mult} + 2T_h$$

The verifier Bob needs to perform three modular exponentiations, three modular multiplications and two hash functions computation. The global required time is:

$$T_v = 3T_{exp} + 3T_{mult} + 2T_h = 723T_{mult} + 2T_h$$

Now, for its theoretical interest, we give a general form.

3.5. Theoretical generalization

Assume that h is a secure public hash function like SHA1 [10, chap.9] and [11, chap.5].

1. To generate the parameters:
   - Alice chooses randomly two large primes P and Q, then she calculates $n = PQ$.
   - She takes an integer $0 < v < \varphi(n)$.
   - She selects randomly N identifications variables B_1,B_2,B_3,...,B_N then computes:

$$\begin{cases} J_1 = B_1^v \mod n \\ J_2 = B_2^v \mod n \\ J_3 = B_3^v \mod n \\ \ldots \\ J_N = B_N^v \mod n \end{cases}$$

   We consider then that $(n, v, J_1, J_2, J_3, ..., J_N)$ is Alice public key, and $(B_1, B_1, B_3, ..., B_N)$ her private one.

2. If Alice wants to sign the contract $M < n$. She must solve the following modular equation:

$$Z^v \equiv T_1 T_2 T_3 ... T_N J_1^{h(M||T_1)} J_2^{h(M||T_2)} J_3^{h(M||T_3)} ... J_N^{h(M||T_N)} \ (mod\ n) \tag{17}$$

   where $T_1, T_2, T_3, ..., T_N$ and Z are unknown variables.
   To solve equation (17), Alice fixes arbitrary T_1 to be $T_1 = r_1^v \ mod\ n$, T_2 to be $T_2 = r_2^v \ mod\ n$, T_3 to be $T_3 = r_3^v \ mod\ n$, ... and T_N to be $T_N = r_N^v \ mod\ n$, where r_1, r_2, r_3,... and r_N are chosen randomly. Then she finds:

$$Z = r_1 r_2 r_3 ... r_4 B_1^{h(M||T_1)} B_2^{h(M||T_2)} B_3^{h(M||T_3)} ... B_N^{h(M||T_N)} \mod n \tag{18}$$

   As Alice detains the secret key $(B_1, B_1, B_3, ..., B_N)$, she can find the last unknown variable Z by congruence (18).

3. Bob checks whether or not the signature $(T_1, T_2, T_3, ..., T_N, Z)$ is valid for the relation (17).

Although the signature schemes are based on solving hard mathematical problems, there are many attempts to investigate other directions[13–15].

4. Conclusion

In this work, we presented a new protocol that can be useful if the old signature systems are broken. Our method is derived from Guillou-Quisquater signature. The proposed scheme requires a moderate time complexity in signing and verifying algorithm. Also some possible attacks have been discussed and we have shown that our algorithm is secured against them.

Acknowledgments

This work is supported by the MMSyOrientation project.

References

[1] W.Diffie, M.E.Hellman , New directions in cryptography, IEEE Transactions on information theory IT-22 (1976) 644–654.

[2] R. Rivest, A. Shamir, L. Adeleman, A method for obtaining digital signatures and public key cryptosystems, Communication of the ACM, 21 (1978) 120–126.

[3] M. O. Rabin, Digitalized signatures and public key functions as intractable as factoring, MIT/LCS/TR 212, 1979.

[4] J. Buchmann, Introduction to Cryptography,(Second Edition), Springer, 2000.

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

[6] L.C. Guillou, J.J. Quisquater, A Paradoxial Identity-based SIgnature Scheme Resulting from Zero-Knowledge, Advances in cryptography, LNCS 403 (1990) 216–231.

[7] H. Ong, C .P . Schnorr, A. Shamir, Efficient signature schemes on polynomial equations, Advances in Cryptology, Crypto'84, LNCS 196, Springer-Verlag, (1985) 37–46.

[8] C. P. Schnorr, Efficient signatures generation by smart cards, Advances in Cryptology, Crypto'89, LNCS 435, Springer-Verlag, (1990) 239–252.

[9] A. Shamir, How to prove yourself : practical solutions to identification and signature problems, Advances in Cryptology, Crypto'86, LNCS 196, Springer-Verlag (1987) 186–194.

[10] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of applied cryptography, CRC Press, Boca Raton, Florida, 1997.

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

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

[13] Michael Gr. Voskoglou, Solving problems with the help of computers: A fuzzy logic approach, International Journal of Advances in Applied Mathematics and Mechanics 2(2) (2014) 62–71.

[14] T. Jenitha Premalatha, S. Jothimani, Intuitionistic fuzzy π g β closed sets, International Journal of Advances in Applied Mathematics and Mechanics 2(2) (2014) 92–101.

[15] Kirtiwant P Ghadle, Yogesh M Muley, Travelling salesman problem with MATLAB programming, International Journal of Advances in Applied Mathematics and Mechanics. 2(3) (2015) 258–266.