Int. J. Open Problems Compt. Math., Vol. 10, No. 2, June 2018
ISSN 1998-6262;
www.i-csrs.org

Variant of Guillou-Quisquater zero-knowledge scheme

S. Ezziri and O. Khadir

Laboratory of Mathematics, Cryptography, Mechanics and Numerical Analysis
Fstm, University Hassan II of Casablanca, Morocco
e-mail: Salma.ezziri@gmail.com
Laboratory of Mathematics, Cryptography, Mechanics and Numerical Analysis
Fstm, University Hassan II of Casablanca, Morocco
e-mail: Khadir@hotmail.com

Received 12 January 2018; Accepted 28 February 2018

Abstract

In cryptography, a zero-knowledge proof is the process allowing Alice, the customer or the client to prove herself to Bob, a bank or a server. Without obtaining any secret information from the prover, the verifier must be convinced that the statement given is true. In this work we propose a new identification protocol inspired by Guillou-Quisquater scheme, and stronger than it. The security analysis is studied.

Keywords: *Zero-knowledge proof, Guillou-Quisquater protocol, identification.*
2010 Mathematics Subject Classification: 03F55, 46S40.

1 Introduction

Zero-knowledge proof is an important issue in public key cryptography. It is used in various situations. Such as authorization to access to a server, digital signatures, exchange of communication between a customer and the bank. The method is generally based on a hard mathematical equation. The verifier Bob checks if the answer given by Alice is valid. It is very complexe for anyone else other than Alice to imitate her identification. These schemes are usually used

in microprocessor-based devices such as smart cards, personal computers, and remote control systems, due to their simplicity and security. The best known identification protocols, relies on developing the solutions of difficult problems. Among these hard equations in cryptography we find: discrete logarithm, factoring and computing square root modulo a large composite number.
In 1985, S. Goldwasser, S. Micali and C. Rackoff [3] have introduced the concept of zero-knowledge proof in cryptography. In 1986 authors A. Fiat and A. Shamir [2,14] proposed a first practical scheme of indentification, based on factoring and computing square root modulo a large composite number. In 1988, Guillou and Quisquater [4] published a paper where they exposed a remarkable interactive identification. Their technique was based on the RSA algorithm [11,12]. In 1989, Schnorr [13,16 pp. 371-374] created a method serving to prove the knowledge of a discrete logarithm. In 1993, Okamoto [8,16 pp. 378-383] proposed a scheme which is provably secure against active attacks under the discrete logarithm assumption. In 2005, E. Bangerter, J. Camenisch, and U. Maurer [1] published a paper where they presented an efficient zero-knowledge proof for exponentiation and multi-exponentiation based on a discrete logarithm. All these algorithms are claimed to be secure by their authors. But, perhaps one day they will be broken. Hence, the need of designing new alternatives.
In this work we present a new identification protocol inspired by the Guillou-Quisquater scheme, and stronger than it. We analyze its security. It is known that the Guillou-Quisquater protocol is based on the RSA algorithm [11,12]. Our method relies simultaneously on RSA and on Rabin cryptosystem [10,16 pp. 211-213]. Hence the effectiveness of our protocol.
The paper is organized as follows: In section 2 we recall the basic Guillou-Quisquater scheme. Then we present new variant in section 3. We conclude and present an open problem in section 4.
In the sequel, for every positive integer n , we denote by $\mathbb{Z}/n\mathbb{Z}$ the finite ring of modular integers. Let a, b, c be three integers. We write $a \equiv b\,[c]$ if c divides the difference $a - b$, and $a = b \bmod c$ if a is the remainder in the division of b by c.
In all of the following, we will respect Guillou-Quisquater paper notations [4] . We start by describing the classical Guillou-Quisquater scheme.

2 Guillou-Quisquater scheme

2.1 Description of the protocol [4]

A trusted center chooses a RSA integer n, product of two large and distinct primes p and q. It also selects a public RSA exponent v, that is an integer relatively prime with $\varphi(n) = (p-1)(q-1)$. We can assume that v is a small

prime, for example $v = 3$ is acceptable. As usual the confidence authority publishes n,v and keeps p and q secret.
In the Guillou-Quisquater scheme, Alice proves to Bob that she knows the v^{th} root $\frac{1}{B}$ modulo n of a given number $J \in \mathbb{Z}/n\mathbb{Z}$. In other words : $(\frac{1}{B})^v \equiv J\,[n]$. Alice's public key is (J, v, n) and B is her private key.
The protocol works as follows :

1. Alice chooses a random number $r \in \{1, 2, ..., n-1\}$ and computes $T \equiv r^v\,[n]$. She sends the result T to the verifier Bob.

2. Bob chooses a random number $d \in \{0, 1, .., v-1\}$ and sends it to Alice.

3. Alice replies by sending $t \equiv r.B^d\,[n]$.

Theorem 1 [4] *Bob accepts the identification if and only if* $t^v.J^d \equiv T\,[n]$.

Proof. We first have : $(\frac{1}{B})^v \equiv J\,[n]$, $T \equiv r^v\,[n]$ and $t \equiv r.B^d\,[n]$. Then : $t^v \equiv r^v.B^{v.d} \equiv T.(\frac{1}{J})^d\,[n]$. Thus : $t^v.J^d \equiv T\,[n]$. ■

2.2 Example

Suppose that the trusted source selects: $n = p.q = 47.59 = 2773$, and $v = 157$. The number v is prime with $\varphi(n) = (47-1)(59-1) = 2668$. The trusted source keeps secret the factors p and q.
Alice, in order to begin, will first generate a personal public key J, using a secret key $B = 920$ such that : $J \equiv (\frac{1}{B})^v\,[n]$. This would result in: $J \equiv (\frac{1}{920})^{157} \equiv 1892\,[n]$.
The identification procedure works as follows :

1. Alice chooses a random number $r = 1874$ and computes $T \equiv r^v \equiv 1874^{157} \equiv 933\,[n]$. She sends the result T to Bob.

2. Bob chooses $d = 135$ and sends it to Alice.

3. Alice replies by sending $t \equiv r.B^d \equiv 1874.920^{135} \equiv 1138\,[n]$.

Bob checks the validity of the response by the equation : $t^v.J^d \equiv 1138^{157}.1892^{135} \equiv 933 \equiv T\,[n]$.

2.3 Security analysis

Assume that Oscar is an attacker.

- **Attack 1** : Knowing Alice public key. If Oscar intercepts the value of d and t, then he can computes the scalar T using the equation $t^v.J^d \equiv T\,[n]$. But it does not work, because he must send the value of T at the beginning of the procedure.
- **Attack 2** : Even if the attacker intercepts the value of t he is not able to find Alice secret key, because he must solve the equation $t \equiv r.B^d\,[n]$ with two unknowns B and r.
- **Attack 3** : Suppose that the attacker intercepts the value of T and t. If he tries to imitate the identification of Alice, then he will be blocked at the challenge number d which is changeable with each identification.

In the next section we present our result.

3 Our contribution

3.1 Description of the protocol

We first have a confidence center, which is trusted by everyone. This authority distributes to all interested parties a secret based on their identity, that he only can compute. The trusted center chooses an RSA integer n product of two large and distinct primes p, q, a public RSA exponent v an integer relatively prime with $\varphi(n) = (p-1)(q-1)$. As usual the trusted source publishes n and v, keeping p and q secret.

Alice's public key is (J, v, n) and B is her private key with $J \equiv (\frac{1}{B})^{2v}\,[n]$.

The protocol works as follows :

1. Alice chooses a random number $r \in \{1, 2, ..., n-1\}$ and computes : $T \equiv r^v\,[n]$.
   She sends the result T to the verifier Bob.
2. Bob chooses a random number $d \in \{0, 1, .., v-1\}$ and sends it to Alice.
3. Alice replies by sending $t \equiv r.B^d\,[n]$.

Theorem 2 *Bob accepts the identification if and only if :* $t^{2v}.J^d \equiv T^2\,[n]$.

Proof. Indeed : $J \equiv (\frac{1}{B})^{2v}\,[n]$, $T \equiv r^v\,[n]$ and $t \equiv r.B^d\,[n]$. Then : $t^{2v} \equiv r^{2v}.B^{2v.d} \equiv T^2.(\frac{1}{J})^d\,[n]$. Thus : $t^{2v}.J^d \equiv T^2\,[n]$. ■

3.2 Example

Let $n = 101.113 = 11413$. Alice's secret key is $B = 9726$ and her public key is (J, v, n) with $v = 3533$ and $J \equiv (\frac{1}{B})^{2v} \equiv (\frac{1}{9726})^{7066} \equiv 5170\,[n]$.
Alice wants to identify herself to Bob. The protocol works as follows:

1. Alice chooses a random number $r = 1861$, computes $T \equiv r^v \equiv 1861^{3533} \equiv 8709\,[n]$ and sends T to Bob.
2. Bob chooses a random number $d = 3145$ and sends it to Alice.
3. Alice replies by sending $t \equiv r.B^d \equiv 1861.9726^{3145} \equiv 6185\,[n]$.

Bob checks that :
$t^{2v}.J^d \equiv 6185^{7066}.5170^{3145} \equiv 7296\,[n]$ and $T^2 \equiv 8709^2 \equiv 7296\,[n]$.
Bob accepts Alice's identification.

3.3 Security analysis

Assume that Oscar is an attacker.

- **Attack 1** : Knowing Alice public key. If Oscar intercepts the value of d and t, then he can computes the scalar T using the equation $t^{2v}.J^d \equiv T^2\,[n]$. But it does not work, because he must send the value of T at the beginning of the procedure.
- **Attack 2** : Even if the attacker intercepts the value of t he is not able to find Alice secret key, because he must solve the equation $t \equiv r.B^d\,[n]$ with two unknowns B and r.
- **Attack 3** : Suppose that the attacker intercepts the value of T and t. If he tries to imitate the identification of Alice, then he will be blocked at the challenge number d which is changeable at each identification.

From the security point of view, the protocol that we have suggested is stronger than that proposed by Guillou-Quisquater. Indeed:

Theorem 3 *An attacker capable of breaking our protocol, can also break the Guillou-Quisquater identification system.*

Proof. We first have : $t^{2v}.J^d \equiv T^2\,[n]$ the verification equation of our protocol; If an attacker Oscar finds a way to calculate T and t, then he can easily breaks the protocol proposed by Guillou-Quisquater. Set : $T' = T^2\,[n]$ and $t' = t^2\,[n]$; The verification equation becomes $t'^v.J^d \equiv T'\,[n]$. It is similar to that suggested by Guillou-Quisquater. Hence the effectiveness of our protocol. Note that, even if an attacker breaks the protocol proposed by Guillou-Quisquater, we don't know anyway that he can break ours. Then, from point of security our method is stronger than that suggested by Guillou-Quisquater. ■

4 Conclusion

In this paper, we described a new identification scheme inspired by the work of Guillou-Quisquater, stronger than it, and we analyzed its security. We relied on the concept of zero-knowledge proof.

Open Problem

Factoring large integers is a well established problem in number theory and particulary in public key cryptography. In 2010, several researchers concluded that, to factor a 232-digit number [6] utilizing hundreds of machines, took two years. In 2003, authors estimated that a 1024-bit RSA modulus [7] would be about a thousand times harder. However, it has not been proven that no efficient algorithm for factoring exists. The security of many cryptosystems is based on the presumed factorization difficulty. It is the case for RSA [11,12], Paillier [9], Okamoto-Uchiyama [8] or Rabin cryptosystem [10]. Many other areas of computer science and mathematics have been brought to bear on the same problem. Here we find quantum computing, algebraic number theory, and elliptic curves. There exists also other kinds of systems that depend on the factorization problem. As an exemple we have the cloud computing data store using RSA encryption algorithm [5,15] to provide privacy and security for users.
Let $n = pq$ be a fixed large composite integer where p and q are two unknown primes. Let v coprime with $\varphi(n)$. Breaking RSA, say by Oscar for example, means that for any ciphertext C, Oscar is able to solve the equation $M^v \equiv C\ [n]$ and to find the secret message M. It is well known [12,16 pp. 173-177] that we ignore if Oscar can factor the modulus n. On an other hand, if Oscar can factor n, of course he breaks the RSA protocol.
Suppose now that Oscar is able to solve the general modular equation $t^{2v}\, J^d \equiv T^2\ [n]$ where the unknown variables are t and T and all the other parameters $n, v, J, d \neq 1$ are given. Can he factor the modulus n ? More precisely :

Open problem: Is solving the equation $t^{2v}\, J^d \equiv T^2\ [n]$ sufficient to make possible the factorization of n ?

The problem is not difficult when the exponent d is equal to 1. Indeed, if Oscar can solve the equation $t^{2v}\, J \equiv T^2\ [n]$, he then easily breaks the Rabin cryptosystem. But we know [10] that as a consequence he will determine the factorization of n.

ACKNOWLEDGEMENTS.

The authors are greatly indebted to the referees for their helpful comments

and suggestions that led to the improvement of this paper.
This work was supported by the MMS e-orientation project.

References

[1] E. Bangerter, J. Camenisch, U. Maurer, Efficient proofs of knowledge of discrete logarithms and representations in groups with hidden order. In: Vaudenay S. (eds) Public Key Cryptography, 2005. Lecture notes in computer science, v.3386. Springer, Berlin, Heidelberg.

[2] A. Fiat and A. Shamir, How to prove yourself: practical solutions to identification and signature problems. Springer-Verlag, Lecture notes in computer science, No 263, Advances in cryptology, Proceedings of Crypto '86, pp. 186-194, 1987.

[3] S. Goldwasser, S. Micali and C. Rackoff, The knowledge of interactive proof systems, 17^{th} ACM symposium on theory of computing, pp. 291-304, 1985.

[4] L. Guillou and J.-J. Quisquater : A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory, Proc. of Euro Crypt '88, Springer Verlag LNCS series.

[5] P. Kalpana ,et al, Data Security in Cloud Computing using RSA Algorithm, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, v.1, Issue 4, September 2012.

[6] Kleinjung, Factorization of a 768-bit RSA modulus, International Association for Cryptologic Research, 2010.

[7] A.K. Lenstra, E. Tromer, A. Shamir, W. Kortsmit, B. Dodson, J. Hughes, P. Leyland, Factoring estimates for a 1024-bit RSA modulus, Proceedings Asiacrypt 2003, Springer-Verlag, LNCS 2894 (2003) 55-74.

[8] T. Okamoto, Provably secure and practical identification schemes and corresponding signature schemes. In : Brickell E.F. (eds) Advances in Cryptology Crypto '92. Crypto 1992. Lecture notes in computer science, v.740. Springer, Berlin, Heidelberg.

[9] Paillier, Pascal, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, Eurocrypt. Springer. pp. 223-238, 1999.

[10] M. Rabin, Digitalized Signatures and Public-Key Functions as Intractable as Factorization, MIT Laboratory for Computer Science, 1979.

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

[12] R. Rivest, A. Shamir and L. Adleman, The original RSA patent as filed with the U.S. patent office, 1977, U.S. Patent 4,405,829.

[13] Schnorr, Efficient identification and signatures for smart cards, in G Brassard, ed. Advances in cryptology - Crypto '89, pp. 239-252, Springer-Verlag, 1990. Lecture Notes in Computer Science, v.435.

[14] A. Shamir, Identity-based cryptosystems and signatures schemes, Springer-Verlag, Lecture notes in computer science, No 196, Advances in cryptology, Proceedings of Crypto '84, pp. 47-53, 1985.

[15] H. A. Shehadeh, Q. Y. Obeidat, and D. Darwish, Comprehensive Study on Data Security in Cloud Data Store, International Journal of Open Problems in Computer Science and Mathematics, ISSN 1998 - 6262, v.7, December 2014.

[16] D. R. Stinson, Cryptography: Theory and practice, third Edition (Discrete mathematics and its applications), 1995.