I. J. Computer Network and Information Security, **2016, 9, 27-33**
Published Online September 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.09.04

Alternative Equations for Guillou-Quisquater Signature Scheme

J. Ettanfouhi, O. Khadir
Laboratory of Mathematics, Cryptography and Mechanics, Fstm, University Hassan II of Casablanca, Morocco
E-mail: ettanfouhi@gmail.com, khadir@hotmail.com

Abstract—In 1990, Guillou and Quisquater published an article where they described a new digital signature system. Their technique was based on the RSA algorithm. In this paper, we present several modified Guillou-Quisquater digital signature protocols. We discuss their security and complexity. These schemes can be seen as alternative signature methods if existing systems are completely broken.

Index Terms—Public key cryptography, RSA, Guillou-Quisquater signature scheme.

I. Introduction

Since its invention, the public key cryptography[3, 9, 8] offers many possibilities to share information in a safe way. As one of the most used subjects in this field, we have digital signature protocols. To sign a contract, Alice begins by publishing her public key in a secure server distribution. If she decides to sign a document, she must use her private key. Generally she has to solve a hard mathematical equation. The verifier Bob checks if the answer given by Alice is valid. Since only Alice knows the private key, it is impossible for anybody to imitate her signature.

The principle of the most known signatures schemes, relies on developing the solutions of hard problems, like discrete logarithm, factoring and computing square root modulo a large composite number [9, 5, 11, 10, 8, 7, 4, 2]. These algorithms are claimed to be secure by their authors. But it, perhaps one day they will be broken. Hence, the need of designing new alternatives.

In 1990, Guillou and Quisquater published a paper [5] where they exposed a remarkable digital signature system. Their technique was based on the RSA algorithm.

In this work, we present several new types of Guillou-Quisquater signature scheme. We also analyze their security and complexity.

The paper is organized as follows: In section 2 we recall the basic Guillou-Quisquater signature scheme and review the main known attacks. Then we present new variants in section 3. Section 4 is devoted to a summary table and we conclude in section 5.

In the sequel, we will respect Guillou-Quisquater paper notations [5]. N, Z are respectively the sets of integers and non-negative integers. For every positive integer n, we denote by $\mathsf{Z}/n\mathsf{Z}$ the finite ring of modular integers and by $(\mathsf{Z}/n\mathsf{Z})^*$ 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 $a \equiv b \pmod{c}$ if c divides the difference $a-b$, and $a = b \bmod c$ if a is the remainder in the division of b by c. 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 classical Guillou-Quisquater signature method.

II. Guillou-Quisquater Signature Scheme

In this section we review Guillou-Quisquater signature system[5]. We also discuss the most known attacks.

The protocol needs three steps: generating parameters, signing message and verifying signature.

2.1. Guillou-Quisquater algorithm

Let h be a secure public hash function like SHA1 [6, chap.9] or [12, 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 $0 < v < \phi(n)$, where $\phi(n)$ is the phi-Euler function.
   - She selects randomly an identification variable B and computes:

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

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:

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

where t, T are the unknown variables.

To solve equation (2), Alice fixes arbitrary T to be $T = r^v \quad mod \quad n$, where r is chosen randomly in 2,3,..., $n-2$. Then she finds:

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

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 relation (2).

Bob can verify the signature by checking if equation (2) is valid for the variables t and T furnished by Alice.

2.2. Example

Let ($n, v, J,$)=(24035009 , 65537 , 18390631) and $B = 2178584$ be respectively Alice public and private key. Suppose that she wants to sign the message M =865704. To simplify, we assume that the hash function $h(x)$ is the sum of the digits of the integer x modulo 100. Alice chooses randomly $r = 79483$. She starts by computing $T = r^v \bmod n = 4194323$. Then $h(M \| T) = h(8657044194323) = 56$. Hence

$$t \equiv rB^{h(M\|T)}(mod \quad n) = 1894978$$

To validate the signature, we check that

$$t^v \bmod n = TJ^{h(M\|T)} \bmod n = 2260066$$

Now, we discuss the most known attacks.

2.3. Main attacks

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

Attack 1: The first attack is indicated in the "handbook of applied cryptography" [6, 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

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

for many values of s , until obtaining $l \equiv s \quad (mod \quad v)$. This is possible because parameter v is supposed to be not too large. He next determines the integer x, such that

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

and then calculates

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

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

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

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

$$TJ^l \equiv J^{-s}J^l \equiv t^v(mod \quad n)$$

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 known attack.

Attack 2: Let (n, v, J) be Alice public key. If Oscar obtains the signatures of two messages M_1 and M_2 he can write the following operations:

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

so

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

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:

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

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 new variants of Guillou-Quisquater signature.

III. Our Variants of Guillou-Quisquater Signature Scheme

In this section we describe seven new variants of Guillou-Quisquater signature scheme. They are based on multiple hard problems.

The following parameters will be used throughout of this section:

- h is a secure public hash function like SHA1 [6, chap.9] or [12, chap.5];
- P and Q are large primes choosen randomly by

Alice, and $n = PQ$.

- v is an integer $0 < v < \varphi(n)$, where $\varphi(n)$ is the phi-Euler function. Integers v and $\varphi(n)$ are co-prime.
- As in [1], 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 suppose that we the equivalence $T_{exp} = 240T_{mult}$.

3.1. First Variant

3.1.1. The Protocol

1. Alice start by choosing randomly an identification message B and computes:

$$J = B^v \bmod n$$

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

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

$$t^v \equiv T^{h(M\|T)} J \quad (mod \quad n) \tag{9}$$

where t, T are unknown variables.

To solve equation (9), Alice fixes arbitrary T to be $T = r^v \quad mod \quad n$, where r is chosen randomly in 2,3,..., $n-2$. Then she finds:

$$t \equiv r^{h(M\|T)} B \quad (mod \quad n) \tag{10}$$

As Alice knows the secret key B, she computes the second unknown variable t by congruence (10). Note that there are many couples (t, T) solutions of the relation (9).

3. Bob can verify the signature by checking if equation (9) is valid for the variables t and T furnished by Alice.

Now, we study the security of this method.

3.1.2. Security analysis

Assume that Oscar is Alice's opponent.

Attack 1: Knowing Alice public keys, Oscar tries to find the secret key B. He is confronted to a hard modular equation based on the discrete logarithm problem.

Attack 2: Oscar wants to imitate Alice signature for a contract M. He fixes arbitrary one unknown variable and tries to find the second parameter.

(1) Suppose that he fixes 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 and wants to solve equation (9). But here also we have a weird equation and today there is no way to find its solution.

Attack 3: Even if Bob gets the solutions t and T, he is not able to find Alice secret key, because he must solve the equation (10) with two unknowns parameters B and r.

Attack 4: This variant is resistant to the first attack mentioned in subsection 2.2. Even with a small value of the exponent v Bob is not able to forge Alice signature. In fact, we use (4), (5) and (6), and we have:

$$T^l J \equiv J^{-sl} J \equiv J^{-sl+1} \neq t^v (mod \quad n)$$

3.1.3. Complexity of the algorithm

From subsection 3.1.1, we see that the signer Alice needs to perform three modular exponentiations, one modular multiplication and one hash function computation. The global required time is:

$$T_s = 3T_{exp} + T_{mult} + T_h = 721T_{mult} + T_h$$

The verifier Bob needs to perform two modular exponentiations, one modular multiplication and one hash function computation. The global required time is:

$$T_v = 2T_{exp} + T_{mult} + T_h = 481T_{mult} + T_h$$

For all the following Guillou-Quisquater variants, the complexity is summarized in a table in section 4.

Now, we move to our second variant.

3.2. Second Variant

3.2.1. The Protocol

1. Alice starts by choosing randomly an identification message B and computes:

$$J = B^v \bmod n$$

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:

$$t^v \equiv T^2 J^{h(M\|T^2)} (mod \quad n) \qquad (11)$$

where t, T are unknown variables.

To solve equation (11), Alice fixes arbitrary T to be $T = r^v \ mod \ n$, where r is chosen randomly. Then she finds:

$$t \equiv r^2 B^{h(M\|T^2)} (mod \quad n) \qquad (12)$$

As Alice knows the secret key B, she computes the second unknown variable t by congruence (12).

3. Bob can verify the signature by checking if equation (11) is valid for the variables t and T furnished by Alice.

3.2.2. Security analysis

This variant can be seen as more secured that the original Guillou-Quisquater signature. Indeed, solving (11) implies breaking congruence (2).

Attack 1: Even if Bob gets the solutions t and T he is not able to find Alice secret key, because he must solve the equation (12) with two unknowns B and r.

Attack 2: Oscar wants to imitate Alice signature for a contract M. He fixes arbitrary one unknown variable and tries to find the second parameter.

(1) Suppose that he fixes T, and likes to solve the modular congruence (11). 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 and wants to solve equation (11). But here we have a weird equation and today there is no way to find its solution.

Attack 3: The first attack mentioned in subsection 2.2 is valid for this variant, if we take $T \equiv J^{-s/2} (mod \quad n)$. In this case Bob can forge Alice signature. So we must choose a large value for the exponent v.

Now, we move to the third variant.

3.3. Third Variant

3.3.1. The Protocol

1. Alice start by choosing randomly an identification message B and computes:

$$J = B^v \bmod n$$

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:

$$t^v \equiv T^{2h(M\|T^2)} J \quad (mod \quad n) \qquad (13)$$

where t, T are unknown variables.

To solve equation (13), Alice fixes arbitrary T to be $T = r^v \ mod \ n$, where r is chosen randomly. Then she finds:

$$t \equiv r^{2h(M\|T^2)} B \quad (mod \quad n) \qquad (14)$$

As Alice knows the secret key B, she computes the second unknown variable t by congruence (14).

3. Bob can verify the signature by checking if equation (13) is valid for the variables t and T furnished by Alice.

3.3.2. Security analysis

Attack 1: Even if Bob gets the solutions t and T he is not able to find Alice secret key, because he must solve the equation (14) with two unknown parameters B and r.

Attack 2: Oscar wants to imitate Alice signature for a contract M. He fixes arbitrary one unknown variable and tries to find the second parameter.

(1) Suppose that he fixes T, and likes to solve the modular congruence (13). 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 and wants to solve equation (13). But here we have a weird equation and today there is no way to find its solution.

Attack 3: This variant is resistant to the first attack mentioned in subsection 2.2. Even with a small value of the exponent v Bob is not able to forge Alice signature. In fact, we use (4), (5) and (6), and we have:

$$T^{2l} J \equiv J^{-2sl} J \neq t^v (mod \quad n)$$

Now, we move to the fourth variant.

3.4. Fourth Variant (Rabin scheme)

3.4.1. The Protocol

1. Alice start by choosing randomly an identification message B and computes:

$$J = B^2 \bmod n$$

We consider then that (n, 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:

$$t^2 \equiv TJ^{h(M\|T)}(mod \quad n) \tag{15}$$

where t, T are unknown variables.

To solve equation (15), Alice fixes arbitrary T to be $T = r^2 \quad mod \quad n$, where r is chosen randomly in 2,3,..., $n-2$. Then she finds:

$$t \equiv rB^{h(M\|T)}(mod \quad n) \tag{16}$$

As Alice knows the secret key B, she computes the second unknown variable t by congruence (16).

3. Bob can verify the signature by checking if equation (15) is valid for the variables t and T furnished by Alice.

3.4.2. Security analysis

Attack 1: Knowing Alice public keys, Oscar tries to find the secret key B. He is confronted to a hard problem: computing the square root modulo a large number n. It is proved that it is hard as factoring the number n.

Attack 2: Even if Bob gets the solutions t and T he is not able to find Alice secret key, because he must solve the equation (16) with two unknowns B and r.

Attack 3: Oscar wants to imitate Alice signature for a contract M. He fixes arbitrary one unknown variable and tries to find the second parameter.

(1) Suppose that he fixes T, and likes to solve the modular congruence (15). But here, he will face a square root modulo a large number. We don't know a method for solving that kind of problems.

(2) Suppose that he fixes t and wants to solve equation (15). But here we have a weird equation and today there is no way to find its solution.

Now, we move to the fifth variant.

3.5. Fifth Variant (Rabin scheme)

3.5.1. The Protocol

1. Alice start by choosing randomly an identification message B and computes:

$$J = B^2 \bmod n$$

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:

$$t^2 \equiv T^{h(M\|T)}J(mod \quad n) \tag{17}$$

where t, T are unknown variables.

To solve equation (17), Alice fixes arbitrary T to be $T = r^2 \quad mod \quad n$, where r is chosen randomly in 2,3,..., $n-2$. Then she finds:

$$t \equiv r^{h(M\|T)}B(mod \quad n) \tag{18}$$

As Alice knows the secret key B, she computes the second unknown variable t by congruence (18). Note that there are many couples (t, T) solutions of the relation (17).

3. Bob can verify the signature by checking if equation (17) is valid for the variables t and T furnished by Alice.

3.5.2. Security analysis

Attack 1: Knowing Alice public keys, Oscar tries to find the secret key B. He is confronted to a hard problem: computing the square root modulo a large number n. It is proved that it is hard as factoring the number n.

Attack 2: Even if Bob gets the solutions t and T he is not able to find Alice secret key, because he must solve the equation (18) with two unknowns B and r.

Attack 3: Oscar wants to imitate Alice signature for a contract M. He fixes arbitrary one unknown variable and tries to find the second parameter.

(1) Suppose that he fixes T, and likes to solve the modular congruence (17). 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 and wants to solve equation (17). But here we have a weird equation and today there is no way to find its solution.

Now, we move to the sixth variant.

3.6. Sixth Variant

3.6.1. The Protocol

1. Alice start by choosing randomly two identification messages B_1 and B_2, then computes:

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

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:

$$Z^v \equiv tTJ_1^{h(M\|t)} J_2^{h(M\|T)} \quad (mod \quad n) \tag{19}$$

where t, T and Z are the unknown variables.

To solve equation (19), 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 in 2,3,..., $n-2$. Then she finds:

$$Z \equiv r_1 r_2 B_1^{h(M\|t)} B_2^{h(M\|T)} (mod \quad n) \tag{20}$$

As Alice detains the secret key (B_1 , B_2), she can find the third unknown variable Z by congruence (20).

3. Bob checks if the signature (T, t, Z) is valid for the relation (19).

This system has the advantage that Oscar must solve two hard problems instead of one.

3.6.2. Security analysis

Attack 1: Knowing Alice public keys, 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 2: Even if Bob gets the solutions t, T and Z he is not able to find Alice secret key, because he must solve the equation (20) with four unknowns B_1, B_2, r_1 and r_2.

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 (19). 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 (19). But here, we have a weird equation and today there is no way to find its solution.

Attack 4: The first attack mentioned in subsection 2.2 is valid for this variant, if we take $l_1 = h(M \| T)$ and $l_2 = h(M \| t)$, where $T \equiv J_1^{-s_1} (mod \quad n)$ and $t \equiv J_2^{-s_2} (mod \quad n)$ for many values of s_1 and s_2, until obtaining $l_1 \equiv s_1 (mod \quad v)$ and $l_2 \equiv s_2 (mod \quad v)$. In this case Bob can forge Alice signature. So we must choose a large value for the integer v.

Now, we move to the seventh variant.

3.7. Seventh Variant

3.7.1. The Protocol

1. Alice start by choosing randomly two identifications messages B_1 and B_2, then computes:

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

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:

$$Z^v \equiv t^{h(M\|t)} T^{h(M\|T)} J_1 J_2 \quad (mod \quad n) \tag{21}$$

where t, T and Z are the unknown variables.

To solve equation (21), 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 in 2,3,..., $n-2$. Then she finds:

$$Z \equiv r_1^{h(M\|T)} r_2^{h(M\|t)} B_1 B_2 (mod \quad n) \tag{22}$$

As Alice detains the secret key (B_1 , B_2), she can find the third unknown variable Z by congruence (22).

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

relation (21).

This system has the advantage that Oscar must solve two hard problems instead of one.

3.7.2. Security analysis

Attack 1: Knowing Alice public keys, 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 2: Even if Bob gets the solutions t, T and Z he is not able to find Alice secret key, because he must solve the equation (22) with four unknowns B_1, B_2, r_1 and r_2.

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 (21). 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 (21). But here, we have a weird equation and today there is no way to find its solution.

IV. CONCLUSION

In this work, we presented seven protocols that can be useful if the old signature systems are completely broken. These variants are all derived from Guillou-Quisquater signature scheme. We analyzed the time complexity in signing and verifying algorithm. Also most possible attacks have been discussed.

ACKNOWLEDGEMENT

This work is supported by the MMSy e-Orientation project.

REFERENCES

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

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

[3] W.Diffie and M.E.Hellman, *New directions in cryptography*, IEEE Transactions on information theory, vol. IT-22,(1976), pp. 644-654..

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

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

[6] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, Florida, (1997).

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

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

[11] 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.

[12] D. R. Stinson, *Cryptography, theory and practice*, Third Edition, Chapman & Hall/CRC, (2006).

[13] *D.P. Franco, F.D. Barboza, N. M. Cardoso*, *A Secure Method for Authenticity Verification of Handwritten Signatures Through Digital Image Processing and Artificial Neural Networks*, International Journal of Communication Networks and Information Security (IJCNIS), Vol 5, No 2 (2013).

[14] H. TOUMI, A. TALEA, B. MARZAK, A. EDDAOUI, M. TALEA, *Cooperative Trust Framework for Cloud Computing Based on Mobile Agents,* International Journal of Communication Networks and Information Security (IJCNIS), Vol 7, No 2 (2015).

Authors' Profiles

Dr Omar Khadir received his Ph.D. degree in Computer Science from theUniversity of Rouen, France (1994). Co-founder of the Laboratory of Mathematics, Cryptography and Mechanics at the University of Hassan II Mohammedia, Morocco, where he is now the head of the Department of Mathematics. He teaches cryptography for graduate students preparing a degree in computer science.

His current research interests include public key cryptography, digital signature, primality, factorisation of large integers and more generally, all subjects connected to the information technology.

Jaouad Ettanfouhi holds an engineer degree in Computer Science from the University of Hassan II Mohammedia (2011). Member of the laboratory of Mathematics, Cryptography and Mechanics, he is preparing a thesis in public key cryptography.