Journal of Mathematics Research; Vol. 11, No. 6; December 2019
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

Provable Security of The Generalized ElGamal Signature Scheme

Demba Sow[1] & Mamadou Ghouraissiou Camara[2]

[1] Faculté des Sciences et Techniques, Département de Mathématiques et Informatique, Université Cheikh Anta Diop de Dakar, Sénégal

[2] Institut Supérieur de Technologie de Mamou (ISTM), Département de Génie Informatique, Republic of Guinea

Correspondence: Demba Sow, Faculté des Sciences et Techniques, Département de Mathématiques et Informatique, Université Cheikh Anta Diop de Dakar, Sénégal. Tel: 00221776084855. E-mail: sowdembis@yahoo.fr

Received: October 23, 2019 Accepted: November 15, 2019 Online Published: November 19, 2019

doi:10.5539/jmr.v11n6p77 URL: https://doi.org/10.5539/jmr.v11n6p77

Abstract

A new variant of the ElGamal signature scheme called ”a Generalized ElGamal signature scheme” is proposed in 2011. The Generalized ElGamal signature scheme is a modified ElGamal signature scheme. In this paper, we propose the security proof of the Generalized ElGamal signature scheme in the random oracle model. First, we recall some security notions of signature schemes and show the security of the modified ElGamal Signature scheme.

Keywords: signature scheme, ElGamal, DSA signature, provable security

1. Introduction

Digital signatures perform an important role in verifying the identity of a sender of a document. A digital signature is represented as a string of binary digits. The signature is a process using a set of rules and parameters (algorithm) to ensure the identity of the sender of a document and the originality of the data. The signature is generated by the owner of a private key. A private key is known only by its owner. A signature is verified using a public key associated with a private key.

1.1 Related Work

In 1985, the ElGamal signature scheme (ElGamal, 1985) is presented by Taher ElGamal. But, it is existentially forgeable (Pointcheval & Stern, 1996).

In August of 1991, the U.S. National Institute of Standards and Technology (NIST) proposed a Digital Signature Algorithm (DSA).

In 1994, the DSA has become a U.S. Federal Information Processing Standard (FIPS 186) called the Digital Signature Standard (DSS), and is the first digital signature scheme recognized by any government (NIST, 1994).

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures, based on the mathematical concept of modular exponentiations and the discrete logarithm problem.

In November 1996, David Pointcheval and Serge Vaudenay presented the security proof for slight variants of DSA in their paper titled ”On Provable Security for Digital Signature Algorithm” in (Pointcheval & Vaudenay, 1996).

David Pointcheval and Jacques Stern study the security proofs for signature schemes in the random oracle model in (Pointcheval & Stern, 1996). Then, they generalized this technique against attacks of adaptively chosen messages. Finally, they applied this technique in a new variant of the ElGamal signature scheme.

In (Sow & Sow, 2011), some variants of ElGamal Signature Schemes were proposed. The variants of the signature schemes proposed in (Sow & Sow, 2011) are resistant to certain vulnerabilities shown in the ElGamal signature schemes. Moreover, in (Sow & Sow, 2011), there are many more signature variants than the ElGamal signature schemes.

1.2 Our Contribution

In this article, first, we show the modified ElGamal Signature scheme and its security, and we propose the provable security of the Generalized ElGamal signature scheme (Sow & Sow, 2011).

1.3 Organization of the Paper

This paper is organized as follow:

- In **section 2**: we recall the Discrete Logarithm Problem and security notions about signatures schemes.
- In **section 3**: we present the slight variant of the ElGamal signature scheme and its security proposed by Pointcheval and Stern in (Pointcheval & Stern, 1996).
- In **section 4**: we show the provable security of the Generalized ElGamal signature scheme proposed in (Sow & Sow, 2011).

2. Preliminaries

In this section, we recall the Discrete Logarithm Problem, the Diffie-Hellman problems (CDH and DDH), the signature scheme and security notions about signatures schemes.

2.1 Diffie-Hellman Problems

In this subsection, we recall the Discrete Logarithm Problem, the Computational and the Decisional Diffie-Hellman problems.

2.1.1 The Discrete Logarithm Assumption

Let $\mathbb{G}$ be a finite multiplicative group of order q with a generator g. The Discrete Logarithm Problem (DLP) asks x given a group element $h = g^x$.

The DLP is intractable in the underlying group $\mathbb{G}$. We formally show this via adversarial view as the following: For any polynomial time adversary A, the probability that

$$Pr[x = A(\mathbb{G}, q, g, h) : g^x = h]$$

is negligible.

2.1.2 The Computational Diffie-Hellman Assumption

Recall that the computational Diffie-Hellman problem is defined as follows:

Let $\mathbb{G}$ be a finite multiplicative group of order q with a generator g. Given two elements of $\mathbb{G}$, g^x and g^y, it is required to find g^{xy}.

The Computational Diffie-Hellman problem (CDH) is intractable in the underlying group $\mathbb{G}$.

2.1.3 The Decisional Diffie-Hellman Assumption

We state the Decisional Diffie-Hellman problem (DDH) as the following:

Let $\mathbb{G}$ be a finite multiplicative group of order q with a generator g. Find whether $xy = z \mod q$ if the three elements (g^x, g^y, g^z) of $\mathbb{G}$ are given.

The DDH problem is computationally hard in the underlying group $\mathbb{G}$.

2.2 Provable Secure and Signature Schemes

2.2.1 Signature Scheme

Definition 1

The definition of a signature scheme $\Sigma = (KeyGen, Sig, Ver)$ is as follows:

1. The **The key generation algorithm** $KeyGen \xrightarrow{\$} (sk, vk)$. The algorithm takes on input 1^k, which is a formal notation for a machine with running time polynomial in k (the security parameter) , the algorithm *KeyGen* outputs a key pair (pk, sk) where pk is the public key and sk is the secrete key. Algorithm *KeyGen* is probabilistic.

2. The **The signature algorithm** $Sig(sk, m) \xrightarrow{\$} \sigma$. The signing algorithm Sig takes on input a message m and a key pair (pk, sk) and outputs a signature σ. It need be probabilistic.

3. The **The verification algorithm** $Ver(vk, m, \sigma) \xrightarrow{\$} \{0, 1\}$. The verification algorithm Ver takes on input a signature σ, a message m and a public key pk and tests whether σ is a valid signature of m with respect to pk. Ver outputs either 0 (invalid) or 1 (valid). It need not be probabilistic.

Definition 2 (Correctness).

A digital signature scheme Σ is correct if for all message m, all $(sk, vk) \longleftarrow KeyGen()$, and all $\sigma \longleftarrow Sig(sk, m)$, we have that $Ver(vk, m, \sigma) = 1$.

2.2.2 Security Notions

Definition 3(Security goals).

There are several possible security goals for the attacker:

- **Key recovery:** Calculate sk, then allow the attacker to act as a signer.
- **Universal forgery:** For any message m, compute a valid signature for m. Make an efficient algorithm that can sign messages with a good probability of success.
- **Existential forgery:** For any message m, calculate σ which is a valid signature. And in this case, we are talking about **Existential unforgeability (EUF)** for the corresponding security level.

Definition 4 (Attack scenarios).

We can give the attacker different powers:

- **Key-only attack** or **No-Message Attack (NKA):** The attacker receives vk.
- **Known-message attack (KMA):** The attacker receives a list of message/signature pairs for a pre-selected list of messages.
- **Adaptive chosen-message attack (CMA):** The attacker may adaptively obtain signatures for messages of his choosing.

Remark 1

The ”best” security notion is existential unforgeability under adaptive chosen message attack (EUF-CMA). We want to bound

$$Succ_{\Sigma}^{euf-cma}(\mathcal{A}) = Pr\left(Exp_{\Sigma}^{euf-cma}(\mathcal{A}) = 1\right).$$

3. The Slight Variant of the ElGamal Signature Scheme

In this section, we present the ElGamal signature scheme (ElGamal, 1985), the security of the new variant of the ElGamal signature scheme (Pointcheval & Stern, 1996).

3.1 The ElGamal Signature Scheme

We start this section with a reminder of the ElGamal signature scheme (ElGamal, 1985):

3.1.1 Algorithm

- **Key generation:** it generates a random large prime p of size n and a generator g of $(\mathbb{Z}/p\mathbb{Z})^*$. Then, it computes the public key $y = g^x \mod p$ where $x \in \mathbb{Z}/(p-1)\mathbb{Z}$ is the random secret key.
- **Signature:** to sign a message m, a pair (r, s) is generated where $g^m = y^r r^s \mod p$. In order to achieve the goal, a random $k \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ is chosen, the exponentiation $r = g^k \mod p$ is computed and the linear equation $m = xr + ks \mod (p-1)$ is solved. Finally the output is (r, s).
- **Verification:** to verify the signature (r, s), one checks the equation $g^m = y^r r^s \mod p$.

3.1.2 Security

The complete security of the ElGamal signature scheme can not be proven since it is vulnerable to existential forgery (see (Pointcheval & Stern, 1996)).

Theorem 1 *The ElGamal signature scheme is not secure against Existential forgery.*

Proof see (Pointcheval & Stern, 1996).

3.2 The Slight Variant of the ElGamal Signature Scheme

This variant of the ElGamal signature scheme is proposed by Pointcheval and Stern in (Pointcheval & Stern, 1996). The hash value of the integer part named $f(m,r)$ is used to substitute that of the message m in this new variant.

3.2.1 Algorithm

- **Key generation:** the algorithm has not changed.
- **Signature:** to sign a message m, a pair (r, s) is generated where $g^{f(m,r)} = y^r r^s \mod p$. The generation of the k and r values and the resolution of the equation $f(m,r) = xr + ks \mod (p-1)$ will achieve the goal. We have as an output $(r, f(m,r), s)$.
- **Verification:** the signature is checked with the changes made by the hash function.

3.2.2 Security of the Generalized ElGamal Signature Scheme

First, we recall some definitions and lemmas (see (Pointcheval & Stern, 1996)).

Lemma 1 ***(the forking lemma).*** *We suppose that $\mathcal{A}$ is a Turing machine that is also probabilistic and resolving in polynomial time. Suppose as input only public data is given. With a not insignificant probability, if A can output a valid signature $(m, \sigma_1, h, \sigma_2)$, then by repeating the execution of this machine with a not insignificant probability and with a different oracle, one generates two valid signatures $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$ where $h \neq h'$.*

Lemma 2 *Suppose that $F \subset A \times B$ and* $\Pr[F(a,b)] \geq \varepsilon$. *So, there exists $\Lambda \subset A$ such that*

- $\Pr[a \in \Lambda] \geq \varepsilon/2$
- *whenever $c \in \Lambda$,* $\Pr[F(c,b)] \geq \varepsilon/2$

Let $|p|$ be the length of an integer p.

Definition 5

We fix a real λ. If the factorization of $p-1$ is $p-1 = UV$ with U a prime number and V verifies $V \leq |p|^\lambda$ then we say that p is an λ-hard prime number.

Lemma 3 *An indistinguishable distribution can be simulated by the the signer for prime numbers λ-hard.*

The following theorems prove the security of the slight variant ElGamal signature scheme presented by Pointcheval and Stern in (Pointcheval & Stern, 1996).

- **Security against a no-message attack.**

  Let us recall some assumptions before stating the theorem.

  Consider a no-message attack against schemes using λ-hard prime moduli in the random oracle model. Consider also the probabilities are studied over random tapes, public keys and random oracles.

  Theorem 2 *The light variant ElGamal signature scheme is secure against a no-message attack. This means the discrete logarithm problem with λ-hard prime moduli is able to solve in polynomial time, if the light variant ElGamal signature scheme is existential forgeable.*

- **Security against an adaptively chosen message attack.**

  Let us recall some assumptions before stating the theorem.

  In the random oracle model, we consider an adaptively chosen message attack against schemes using λ-hard prime moduli. We consider also the probabilities are studied over random tapes, public keys and random oracles.

  Theorem 3 *In the random oracle model, the light variant ElGamal signature scheme is secure against an adaptively chosen message attack. This means the discrete logarithm problem with λ-hard prime moduli is able to solve in polynomial time, if the light variant ElGamal signature scheme is existential forgeable.*

4. Security of the Generalized ElGamal Signature Scheme

First, we show the Generalized ElGamal signature scheme (Sow & Sow, 2011): key generation, signature and verification algorithms. After, we propose its security against an adaptively chosen message attack.

4.1 The Generalized ElGamal Signature Scheme

In this subsection, we give a key generation mechanism and a signature and verification algorithms (Sow & Sow, 2011), which can be view as a light modification of ElGamal's signature schemes (see (ElGamal, 1985) and (Menezes, Van Oorschot & Vanstone, 1997)).

4.1.1 Key Generation Algorithm

1. Select a group $G = (\mathbb{Z}/p\mathbb{Z})^*$ (where p is a large prime number) with sufficiently large order: $n = \#G$ and select an element $g \in G$ with sufficiently large (prime) order: $d = o(g)$ [g and d can be optionally kept secret];
2. Select two random integers $2 < k < s < d$ sufficiently large, (s and k are coprime with $n = \#G$) and compute kd; Compute with euclidian division algorithm, the pair (r, t) such that $kd = rs + t$ where $t = kd \mod s$ and $r = \left\lfloor \frac{kd}{s} \right\rfloor < d$;

   [Note that $r = \left\lfloor \frac{kd}{s} \right\rfloor, \left\lfloor \frac{s}{t} \right\rfloor, \gcd(r, n) = 1, \gcd(t, n) = 1, d - r$, and t must be sufficiently large, if not, return to step 2]
3. Compute $\gamma = g^s$ and $\delta = g^t$ in G; [Note that $\gamma \neq 1$ and $\delta \neq 1$];

   Bob's public key is $((\gamma, \delta), G, n = \#G)$ and Bob's private key is $((r, s, t), G, n = \#G)$;

Remark 2 *Note that only r is used in decryption process. But* (r, s, t) *are used in signature mechanism.*

4.1.2 Signature Algorithm

Let h' an element of G which can be represented in binary i.e there exists an injective map $h : G \to \{0, 1\}^*$. Assume also that there exists a cryptographic hash function $H : \{0, 1\}^* \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ where $n = \#G$.

Let m be the message to sign.

1. Choose a random integer $2 < \beta < n = \#G$ such that $\gcd(\beta, n) = 1, \beta$ and $d - \beta$ must be sufficiently large;
2. Calculate $R = (g^s)^{r\beta}$ in G, $H(h(R))$, $(r\beta)^{-1} \mod n$ and $s^{-1}t \mod n$;
3. Calculate $S = (r\beta)^{-1}\{H(h(m)) - s^{-1}tH(h(R))\} \mod n$; if $S = 0$ or $S = 1$, return to stage 2;
4. Output (R, S) as the signature of m.

4.1.3 Verification Algorithm

1. Take $(\gamma, \delta, G) = ((g^s, g^t), G)$ the public key and (R, S) the signature of m;
2. Calculate $V_1 = (g^t)^{H(h(R))}R^S$ and $V_2 = (g^s)^{H(h(m))}$ in G;
3. The signature is valid if $V_1 = V_2$;

4.2 Security of the Generalized ElGamal Signature Scheme

In this section, we study the resistance of the Generalized ElGamal Signature scheme against an adaptively chosen message attack, at least for a large variety of modulus.

4.2.1 Security Against a No-Message Attack

Let us recall some assumptions before stating the theorem.

In the random oracle model, we consider a no-message attack against schemes using λ-hard prime moduli. We consider also the probabilities are studied over random tapes, public keys and random oracles.

Theorem 4 *The Generalized ElGamal Signature scheme is secure against a no-message attack. This means the discrete logarithm problem with* λ*-hard prime moduli is able to solve in polynomial time, if the Generalized ElGamal Signature scheme is existential forgeable.*

Proof By **lemma 1**, we have two valid signatures (m, H, R, S) and (m, H', R, S') such that $(g^s)^H = \gamma^H = R^S \delta^R \mod n = R^S (g^t)^R \mod n$ and $(g^s)^{H'} = \gamma^{H'} = R^{S'} \delta^R \mod n = R^{S'} (g^t)^R \mod n$. Then, we have $g^{sHS' - sH'S} = g^{tR[S' - S]} \mod n$ and $g^{s[H - H']} = R^{S - S'} \mod n$. There exist i such that $g^i = R \mod n$ because g is a generator of $(\mathbb{Z}/n\mathbb{Z})^*$. Thus,

$$s[HS' - H'S] = tR[S' - S] \mod n - 1 \qquad (1).$$

$$s[H' - H] = i[S - S'] \mod n - 1 \qquad (2).$$

We know that H and H' are produced from a "repeated oracle", so we assume that $H - H'$ is prime to U (where U is a prime number), so that $\gcd[S - S', U] = 1$. But, we know for R, no hypothesis can be made, hence, the following two cases:

case 1: R and U are primes between them. So, the equation (1) gives the modular value U of t, $t = s[HS' - H'S][R[S' - S]]^{-1} \mod U$. An adequate t (that is, a t that checks $\delta = g^t \mod n$) can be computed if we perform an exhaustive search over the V modular value of t.

case 2: $R = bU$ where b is small. Then the equation (2) gives the modular value U of i, $i = s[H - H'][S - S']^{-1} \mod U$. An adequate i (that is, a i that checks $bU = g^i \mod n$) can be computed if we perform an exhaustive search over the V modular value of i.

We note that i is prime to U.

Using the proof of **theorem 10** in (Pointcheval & Stern, 1996) and **lemma 2**, we prove the theorem.

Juste take in input $(g, \delta = g^t)$ and outputs, with non-negligible probability, $t \in \mathbb{Z}/(n-1)\mathbb{Z}$ or take in input $(g, \gamma = g^s)$ and outputs, with non-negligible probability, $s \in \mathbb{Z}/(n-1)\mathbb{Z}$.

4.2.2 Security Against an Adaptively Chosen Message Attack

Let us recall some assumptions before stating the theorem.

In the random oracle model, we consider an adaptively chosen message attack against schemes using λ-hard prime moduli. We consider also the probabilities are studied over random tapes, public keys and random oracles.

Theorem 5 *In the random oracle model, the Generalized ElGamal Signature scheme is secure against an adaptively chosen message attack. This means the discrete logarithm problem with λ-hard prime moduli is able to solve in polynomial time, if the Generalized ElGamal Signature scheme is existential forgeable.*

Proof Assuming that a simulator $\mathcal{S}$ requests the signatures (S_i, R_i) and obtains a new random value H_i for each simulated signature (R_i, H_i, S_i) of the messages m_i. It is noted that a significant collision of requests occurs. Thus, the attacker cannot distinguish the legitimate signature from the simulator. Hence, like **Theorem 4**, discrete logarithms can be solved from a collusion of the simulator and the attacker.

5. Conclusion

We have successfully proved the existentially unforgery of the Generalized ElGamal signature scheme, under an adaptively chosen message attack, in the random oracle model.

References

Elgamal, T. (1985). *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. CRYPTO, IT-31*(4), 469-472. https://doi.org/10.1109/TIT.1985.1057074

Menezes, A. J., & Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*. CRC Press, Boca Raton.

Pointcheval, D. (2005, June). *Advanced Course on Contemporary Cryptology, chapter Contemporary Cryptology Provable Security for Public Key Schemes*, pp. 133-189. Advanced Courses CRM Barcelona. Birkhuser.

Pointcheval, D., & Stern, J. (1996, May). *Security Proofs for Signature Schemes.* Advances in Cryptology ? Proceedings of EUROCRYPT '96, Zaragoza, Spain) U. Maurer, Ed. Springer-Verlag, LNCS 1070, 387-398. https://doi.org/10.1007/3-540-68339-9_33

Pointcheval, D., & Vaudenay, S. (1996). *On Provable Security for Digital Signature Algorithms.* Technical report LIENS 96-17, Ecole Normale Superieure.

Sow, D., & Sow, D. (2011). A new variant of El Gamal's encryption and signatures schemes. *JP Journal of Algebra, Number Theory and Applications, 20*(1), 21-39.

U.S. Department of Commerce, NIST. (1994, Aug). *Digital Signature Standard.* Federal Information Processing Standard Publication 186.

Copyrights