Digital Signatures: Status and Challenge

Jin Li and Kwangjo Kim
International Research center for Information Security (IRIS)
Information and Communications University (ICU)
103-6 Munji-Dong, Yuseong-Gu, Daejeon, 305-732, Korea
82-42-866-6192
{jjl,kkj}@icu.ac.kr

Abstract Digital signature is a central cryptographic primitive. Since the standard definition on the security of signature schemes was given [19], there have been many attempts to design practical and provably secure signature schemes in this security model. Different assumptions and tools have been used in these constructions. In this work, we give a survey on these signature schemes and show the status and challenge in signatures.

Keywords Signature, Provable Security, Random Oracle Model, Assumption

Section 1 Introduction

In cryptography, one of the breakthroughs is the proposal of public key cryptosystem. It can not only be used for encryption, but also can be used in authentication and undeniability. Before this notion, all cryptosystems have only one secret key for two parties to communicate secretly. In public key cryptosystem, pulic key and secret key are divided. The two parites need not agree with the same secret key before communication. As one of the methods for authentication, the notion of signature was proposed in [19]. The digital signature has the same function as the traditional writing signature. And, it becomes more and more important in e-commerce. The signature can be used to realize completeness, authentication and undeniability. It has found many applications since it was proposed, such as in e-cash, e-auction and e-voting etc.

Many variants of signature have also been proposed.

1. Blind signature [7]: There is a case in e-cash and e-auction as follows: The signer should sign some document without knowing the content of the message. In 1982, Chaum introduced the notion of blind signature to solve this problem;
2. Group signature [10]: In group signature, one of members in some group wants to sign on behalf of this group. At the same time, the identity of the signer is anonymous in the group. There are many applications for group signature, such as e-auction and e-voting, for anonyminity and undeniability.
3. Threshold signature [13]: In some cases, the secret key should be shared among several users. Only enough members agree with the computation, the secret key could be recovered. In 1991, Desmedty and Frankely introduced this notion in signature, namely, threshold signature.
4. Undeniable signature [9]: The digital signature can be duplicated and anyone could verify the validity of the signature. But in some case, the signer would not like to allow anyone to verify its signature. He/she only wants the receiver could verify its signature with his/her permission and cooperation. In 1989, Chaum and Antwerpen introduced the notion of undeniable signature [9] to solve this problem.
5. On-line/Off-line signature [15]: In many cases, such as smart card and mobile device, they have only small storage and computational ability. So, it will be very slow if signature generation required in these devices. In order to solve this problem, on-line/off-line signature was proposed by Even, Goldreich and Micali [15]. In this kind of signature, most of the computation for signature could be pre-computed (off-line) before the message is received. So, only small computation is required for on-line computation.
6. Proxy signature [26]: In proxy signature, one entity could delegate its signing ability to another entity. This kind of signature was proposed by Mambo, Usuda and Okamoto in 1996. And, the delegation could be

divided into many kinds such as partial delegation and full delegation etc.

7. Ring signature [30]: Ring signature was proposed to keep signer's anonymity when it signs messages on behalf of a ``ring'' of possible signers. Different from group signature, its anonymity is unconditional.
8. Designated verifiable signature [20]: In this kind of signature, only the designated verifier could verify the correctness of signature.

There are also many other kinds of signature, such as secret signature [23], designated confirmer signature [8], homorphic signature [21], chameleon signature [25], etc. They can be used in many different applications.

The security model for ordinary digital signature was first given [19] in 1984. In this model, the adversary's attack abilities and goals were given. However, the security of many signature schemes can not be proven in this model because the difficulty of signing oracle simulation. One milestone for provable security is the proposal of random oracle model by Bellare and Rogaway [2]. In the random oracle model, hash function was viewed as an ideal random function, *i.e*., perfect randomly function. However, in the actual implementation, user can compute the value of hash function by themselves. So, there are some gaps in ideal function and actual implementation, which was also pointed out in [6].

There are many signature schemes have been proved under this security model, for example, RSA signature scheme [3], Schnorr signature [31] *etc*.

However, because of the controversy of random oracle [6], how to prove and propose efficient signature in standard seucurity model without random oracle is very important. There are many attempts to design signature. Some of them are generic methods from one-way function [22]. However, these schemes are not efficient. Recently, there are several efficient signature schemes have been proposed and proved without random oracle model , such as [4,17,27,34] .

Section 2 Definitions and Security Model

Definition 2.1. There are three algorithms in an ordinary digital signature:

1. Key generation algorithm Gen: On input security parameter k, output secret key sk and public key pk.
2. Signature generation algorithm Sign: On input message m, secret key sk, output signature σ.
3. Signature verification algorithm Verify: On input signature σ, message m and public key pk, output 1/0 for valid or invalid.

The security of signature could be analyzed from two aspects: Ability of adversary and goal of adversary. And, according to different abilities and goals, many combinations, *i.e*., security models could be derived.

According to the goals of the adversary, it can be divided into four categories [19]:

1. Total break: This is the most serious attack, in which the adversary is able to disclose the secret key of the signer;
2. Universal forgery: The adversary is able to sign any given messages;
3. Existential forgery: The adversary is able to provide a signature on a new message whose signature has not been seen;
4. Strong Existential forgery: The adversary is able to provide a new message-signature pair.

On the other hand, various resources can be made available to the adversary, helping into his/her forgery [19]. We focus ourselves on two kinds of message attacks:

1. Weakly chosen message attack: The adversary is allowed to obtain signatures from the signer for a chosen list of messages before it attempts to break the scheme. These messages chosen by the adversary must be given to the signer before seeing the signer's public key;

2. Adaptively chosen message attack: The adversary is allowed to request signatures of messages chosen by it. These messages may not only depend on signer's public key, but also depend on the previous obtained signatures.

By combining the different goals of the adversary and various resources available to the adversary, many security notions for signature schemes can be derived. The standard notion of security for a signature scheme is called existential unforgeability under adaptively chosen message attacks (fully-secure signatures) [19], which is defined through the following game between a challenger *C* and an adversary *A*:

Setup: A public/private key pair (pk, sk) ← Gen(1^k) is generated and adversary *A* is given the public key pk.

Query: *A* runs for time t and issues q signing queries to a signing oracle in an adaptive manner, that is, for each i, $1 \leq i \leq q$, *A* chooses a message m_i based on the message-signature pairs that *A* has already seen, and obtains in return a signature σ_i on m_i from the signing oracle.

Forge: *A* outputs a forgery (m*, σ*) and halts. *A* wins the game if σ* is a valid signature on message m* under the public key pk, *i.e.*, Verify(pk, m*, σ*)=1; and m* has never been queried.

Definition 2.2 **Unforgeability**: A signature scheme S =(Gen, Sign, Verify) is (t, q, ϵ)-fully-secure, if any adversary with run-time t wins the above game with probability at most ϵ after issuing at most q signing queries.

Section 3 Efficient Signature Schemes

3.1 RSA Signature scheme [29]

Definition 3.1 (RSA Assumption) Let n=pq, where p and q are safe primes, and random elements e, h, where (e, φ(n))=1. It is infeasible to compute $h^{\frac{1}{e}} \bmod n$.

We describe the RSA signature scheme as follows:

1. **Gen**: Pick two safe primes p and q, compute n=pq as RSA modulus. Choose an integer e and compute d, such that ed≡1 mod φ(n). Furthermore, a collision resistant hash function H: {0,1}*→ Zn. The public key is (n,e) and the secret key is (φ(n),d).
2. **Sign**: To sign a message m, the signer computes H(m), and outputs the signature as $\sigma = H(m)^d \bmod n$.
3. **Verify**: On input verification key (n, e), message m, and σ, output 1 if and only if $\sigma^e = H(m) \bmod n$. Otherwise, output 0.

3.2 Schnorr Signature scheme [31]

Definition 3.2 (Discrete Logarithm Assumption) Given a randomly large group G with order prime q, and a random element g,y∈ G, it is infeasible to find x such that $g^x = y$.

All users share a group G with size q. Let g be the generator of this group, and H: {0,1}*→ Z_q be a cryptographic hash function.

1. **Gen**: Choose a private key *x* such that $0 < x < q$. The public key is *y* where $y = g^x$.
2. **Sign**: To sign a message m:Choose a random *k* such that $0 < k < q$. Let $r = g^k$ and compute e=H(m‖r) and s=k-xe mod q. The signature is the pair (*e*,*s*).
3. **Verify**: Given signature (e,s), verifiy if the following two equations hold: Let $r_v = g^s y^e$ and $e_v = H(m \| r_v)$. Output 1 if e_v =e. Otherwise, output 0.

3.3 GHR Signature [17].

Gennaro, Halevi and Rabin proposed a secure signature scheme [17] without random oracle, under the assumption that hash function is division intractable and a non-standard randomness-finding oracle.

Definition 3.3 (Strong-RSA Assumption) Given a randomly chosen RSA modulus n, and a random element s∈ Z_n^*, it is infeasible to find a pair (e,r) with e>1 such that $r^e = s \pmod n$.

We describe the GHR signature scheme as follows:

1. **Gen**: Pick two safe primes p and q, compute n=pq as RSA modulus, a hash

function H, and select s$\in Z_n^*$. The public key is (n,s) and the secret key is (p, q).

2. **Sign**: To sign a message m, the signer computes e=H(m) and outputs the signature as $\sigma = s^{\frac{1}{e}} \bmod n$.

3. **Verify**: On input verification key (n, s), message m, and σ, output 1 if and only if $\sigma^{H(m)}$=s mod n. Otherwise, output 0.

Later, another similar signature scheme was proposed by Cramer and Shoup [12], which was also based on Strong-RSA assumption.

3.4 Boneh-Boyen Signature [4].

Before the description of Boneh-Boyen signature, we first introduce some preliminaries on bilinear maps and an assumption used in [4].

Let G be a multiplicative group generated by g, whose order is a prime p, and G_1 also be a multiplicative group with the same order p. Let e: $G \times G \rightarrow G_1$ be a map with the following properties: Bilinearity, Non-degeneracy and Computability.

As shown in [4,35], such non-degenerate bilinear maps over cyclic groups can be obtained from the Weil or the Tate pairing over algebraic curves.

Definition 3.4 (q-Strong Diffie-Hellman Assumption (q-SDH in short)) The q-SDH assumption in G is defined as follows: given a (q+1)-tuple $(g, g^x, g^{x^2}, \dots, g^{x^q}) \in G^{q+1}$ as input, it is hard to output a pair (c, $g^{\frac{1}{x+c}}$), where $c \in Z_p$.

Next, we describe the Boneh-Boyen signature [4]. Actually, the scheme in random oracle was also proposed by Zhang et al. in [35]. Let G, G_1 be bilinear groups where the order of G and G_1 is p. As usual, g is a generator of G. Let H be a cryptographic hash function.

1. **Gen**: Pick $x \in Z_p$, compute $y = g^x$. The public key is y and the secret key is x.

2. **Sign**: Given message m, the signer outputs the signature on m as $\sigma = g^{\frac{1}{x+H(m)}}$.

3. **Verify**: On input verification key y, message m, and the signature σ, output 1 if and only if $e(yg^{H(m)}, \sigma)=e(g, g)$. Otherwise, output 0.

3.5 Waters Signature Scheme [34]

Definition 3.5 (Computational Diffie-Hellman Assumption) Given a randomly large group G with order prime p, and random elements $g^x, g^y \in G$ for unknown x,y, it is infeasible to compute g^{xy}.

In EUROCRYPT'05, Waters [34] proposed an identity-based encryption scheme. From the private key extraction algorithm, a signature scheme without random oracles has been constructed [34].

1. **Gen**: Choose $x \in Z_p$, compute $g_1 = g^x$. Additionally, two random values$g_2, u' \in$ G are chosen. Furthermore, and a random n-length vector $U=(u_1, \dots, u_n)$, whose elements are chosen at random from G. The public key is pk = (g_1, g_2, u', U) and the secret key is g_2^x.

2. **Sign**: To generate a signature on message $m=(\mu_1, \dots, \mu_n) \in \{0,1\}^n$, pick $s \in Z_p^*$ and output the signature as $\sigma = (g_2^x(u'\prod_{i=1}^n u_i^{\mu_i})^s , g^s)$ with his secret key g_2^x.

3. **Verify**: Given a signature σ on message $m=(\mu_1, \dots, \mu_n)$, it first parses $\sigma =(\sigma_1, \sigma_2)$. Output 1 if the following equation holds: $e(\sigma_1, g)=e(g_2, g_1)\ e(u'\prod_{i=1}^n u_i^{\mu_i}, \sigma_2)$. Otherwise, output 0.

Section 4 Analysis of the Signature Schemes

The signature schemes described above have the following properties:

1. Security relied on random oracles: The signature schemes [4,17,29,31,35] were proved to be secure in random oracle model;
2. Security proof without random oracles: As described in the paper of [4, 17], these two schemes could be transformed into schemes without random oracles. The

method in [4] is to use a chameleon hash function H(x)=a+bx. However, in order to avoid random oracles, in [17], it has to introduce another strong assumption as random-findness hash function. Actually, this assumption is really strong, which is similar to random oracle model. Many papers [11, 27] gave security analysis to this construction；

3. Security proof based on standard assumption: [29,31,34]；
4. Security proof based on strong assumption: [4,12,17,35];

From the above analysis, only Waters signature scheme [34] is based on standard assumption, and without random oracles. However, the scheme is not so efficient because it requires more than n public keys, where n is the number of bits from hash function.

So, it is still an open problem to construct an efficient signature scheme, based on standard assumption. Meanwhile, its security proof should not be based on random oracles.

Recently, we gave some suggestions [24] to solve this open problem. In [24], two new paradigms were proposed to get fully-secure signatures from only weakly-secure signature schemes. Based on this, the open problem could be reduced to find such a weakly-secure signature scheme, which is easier to construct compared to fully-secure signature scheme.

Section 5 Conclusion

A signature survey was given in this work. We showed the most efficient signature schemes in literature. And, comparison among these signature schemes was given. We analyzed the advantages and problems of these signature schemes. We also showed the open problem in the construction of signature and some steps towards solving this problem.

References

[1] M. Bellare and S. Micali. How to sign given any trapdoor function. J. of the ACM 39,1992, pp. 214-233.

[2] M. Bellare and P. Rogaway. Random oracle are practical: A paradigm for designing efficient protocols. In Proceedings of the First ACM Conference on Computer and Communications Security, pp. 62-73, 1993.

[3] M. Bellare and P. Rogaway. The exact security of digital signatures: How to sign with RSA and Rabin. EUROCRYPT'96, LNCS 1070, pp. 399-416. Springer,1996.

[4] D. Boneh and X. Boyen. Short signatures without random oracles. EUROCRYPT'04, LNCS 3027, pp. 56-73, Springer, 2004.

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. ASIACRYPT'01, LNCS 2248, pp. 514-532. Springer, 2001.

[6] R. Canetti, O. Goldreich, and S. Halevi. The Random Oracle Methodology, Revisited. STOC'98, ACM, pp. 207-221, 1998.

[7] D. Chaum. Blind signatures for untraceable payments, CRYPTO'82, pp.199-203, Springer,1983.

[8] D. Chaum. Designated confirmer signatures. EUROCRYPT'94, LNCS 950, pp. 86-91. Springer, 1994.

[9] D.Chaum, H. V. Antwerpen. Undeniable Signatures. CRYPTO'89, LNCS 435, pp. 212-216, Springer, 1990.

[10] D. Chaum and E. van Heyst. Group signatures. EUROCRYPT'91, LNCS 547, pp. 257-65, Springer, 1991.

[11] J.-S. Coron and D. Naccache. Security analysis of the Gennaro-Halevi- Rabin signature scheme. EUROCRYPT'00, pp. 91-101, Springer, 2000.

[12] R. Cramer and V. Shoup. Signature schemes based on the strong RSA assumption. ACM TISSEC, 3(3):161-185, 2000. Extended abstract in Proc. 6th ACM CCS, 1999.

[13] Y. Desmedt and Y. Frankel. Threshold cryptosystems. CRYPTO'89, pp. 307-315. LNCS 435, Springer, 1989.

[14] W. Diffie and M. E. Hellman. New Directions in Cryptography. In IEEE

Transactions on Information Theory, volume IT-22(6), pp. 644-654, 1976.

[15] S. Even, O. Goldreich, and S. Micali. On-line/Off-line digital signatures, Journal of Cryptology, vol 9, pp. 35-67, 1996.

[16] A. Fiat and A. Shamir. How to prove yourself: Practical Solutions to Identification And Signature Problems, CRYPTO'86, LNCS 263, pp. 641-654, , Springer, 1987.

[17] R. Gennaro, S. Halevi, and T. Rabin. Secure hash-and-sign signatures without the random oracle. EUROCRYPT'99, pp. 123-139, Springer, 1999.

[18] Eu-Jin Goh and S. Jarecki. A signature scheme as secure as the Diffie-Hellman Problem, EUROCRYPT'03, LNCS 2656, pp. 401-415, Springer, 2003.

[19] S.Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. SIAM J. Computing, 17(2):281-308, 1988.

[20] M. Jakobsson, K. Sako, and R. Impagliazzo, Designated verifier proofs and their applications, EUROCRYPT'96, LNCS 1070, pp. 321-331, Springer, 1996.

[21] R. Johnson, D. Molnar, D. Song, and D. Wagner. Homomorphic Signature Schemes. RSA Conference -Cryptographers' Track, 2002.

[22] L. Lamport. Constructing digital signatures from a one way function. Technical Report CSL-98, SRI International, October 1979.

[23] B. Lee, K. R. Choo, J. Yang, and S. Yoo. Secret Signatures: How to Achieve Business Privacy Efficiently? WISA 2007, LNCS 4867, pp. 30-47, Springer, 2007.

[24] J. Li, K. Kim, F. Zhang, and D. S. Wong. Generic security-amplifying methods of ordinary digital signatures. ACNS 2008, LNCS 5037, pp. 224-241, Springer, 2008.

[25] H. Krawczyk and T. Rabin. Chameleon signatures. In Proceedings of NDSS 2000. Internet Society, 2000. http://eprint.iacr.org/1998/010/.

[26] M.Mambo, K.Usuda, E.Okamoto. Proxy signatures for delegating signing operation, Proceedings of the 3rd ACM Conference on Computer and Communications Security (CCS), ACM, pp. 48-57, 1996.

[27] D. Naccache and D. Pointcheval and J. Stern, Twin Signatures: an Alternative to the Hash-and-Sign Paradigm, CCS 2001, pp. 20-27, ACM, 2001.

[28] A. Perrig. The BiBa one-time signature and broadcast authentication protocol. In Eighth ACM Conference on Computer and Communication Security, pp. 28-37. ACM, 2001.

[29] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signature and pulbic key cryptosystems, Comm. of ACM, 21, 1978, pp. 120-126.

[30] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to Leak a Secret. ASIACRYPT'01, LNCS 2248, pp.552-565, Springer, 2001.

[31] C.-P. Schnorr. Efficient identification and signatures for smart cards. CRYPTO 1989, pp. 239-252, Springer, 1989.

[32] A. Shamir. Identity-based cryptosystems and signature schemes. CRYPTO'84, LNCS 196, pp. 47-53, Springer, 1984.

[33] A. Shamir and Y. Tauman. Improved online/offline signature schemes, CRYPTO 2001, LNCS 2139, pp. 355--367, Springer, 2001.

[34] B.Waters. Efficient Identity based Encryption without random oracles, EuroCrypt 2005, pp. 114-127, LNCS 3494, Springer, 2005.

[35] F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications, PKC 2004, LNCS 2947, pp. 277-290, Springer, 2004.