International Journal of Cryptology Research 1 (1): 11-19 (2009)

A New Online/Offline Signature Scheme without Key Exposure in the Standard Model

Zhiwei Wang, Shihui Zheng, Yixian Yang
Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876
Email: zhwwong2007@yahoo.com.cn

ABSTRACT

The notion of online/offline signature schemes was introduced in 1990 by Even, Goldreich and Micali. In 2001, Shamir and Tauman proposed an efficient generic construction method for building online/offline signature schemes, which is called "hash-sign-switch". In this paper, we utilize the "hash-sign-switch" paradigm to build a new online/offline signature scheme provably secure under the $k+1$ square roots assumption in the standard model. The trapdoor hash function designed for our scheme is a double-trapdoor hash function, which can avoid the key exposure problem.

Keywords: signature schemes, online/offline, trapdoor hash function

INTRODUCTION

Digital signatures are important and fundamental cryptographic primitives. Besides oblivious applications in electronic commerce, they are as important building blocks for various kinds of cryptographic protocols. Up to now, many signature schemes have been proposed [8,9,10].

The notion of *online/offline signature scheme* was first introduced by Even, Goldreich and Micali [1,7]. The signature generation procedure of online/offline signature scheme is divided into two phases. The first phase is performed offline (before the message to be signed is given) and the second phase is performed online (after the message to be signed is given). *Online/offline signature schemes* are useful, since in many application the signer has very limited response once the message is presented, but he can carry out costly computation between consecutive signing requests.

Even, Goldreich and Micali presented a general method for converting any signature scheme into an online/offline signature scheme, which uses a one-time signature scheme[1,7]. In 2001, Shamir and Tauman proposed a more efficient generic construction method for building online/offline signature schemes[2], which is called "hash-sign-switch". In 2006, Kurosawa et al. [3] proposed the first provably secure online/offline signature scheme under strong RSA assumption in the standard model. However, we note that the stronger RSA assumption is easier than the standard RSA assumption. So it is worthwhile to design provably secure online/offline signature schemes based on different hard problems. Furthermore, Kurosawa et al.'s scheme suffer from key exposure problem due to the design of the trapdoor hash function. In [11], Chen et al. first

introduce a double-trap door hash family based on the discrete logarithm assumption to solve the problem of key exposure.

In this paper, we utilize Shamir and Tauman's "hash-sign-switch" paradigm to build a new online/offline signature scheme, which is EF-CMA (existentially unforgeable under adaptive chosen message attacks) secure [6] in the standard model. The newly designed trapdoor hash function of our scheme can avoid the key exposure problem. The basic signature scheme is EF-KMA (existentially unforgeable under known message attacks) secure under the $k+1$ square roots assumption[4] in the standard model (without random oracles).

SHAMIR-TAUMAN'S "HASH-SIGN-SWITCH" PARADIGM

Shamir and Tauman introduced the following "hash-sign-switch" paradigm [2] to get a generic online/offline signature scheme.

- **System Parameters Generation:**
  Let (I,H) be any trapdoor hash function (A special type of hash functions, called *trapdoor hash functions,* were introduced by Krawczyk and Rabin[5], who used them to construct *chameleon signatures*) and (G,S,V) be any provably secure signature scheme. The system parameters are $SP=\{(I,H),(G,S,V)\}$.

- **Key Generation Algorithm:**
  1. Run the key generation algorithm of the original signature scheme G to obtain signing/verification key pair (SK,VK).
  2. Run the key generation algorithm of the trapdoor hash function (I,H) to obtain a trapdoor /hash key pair (TK,HK).

  The signing key is (SK,VK) and the verification key is (VK,HK)

- **The Signing Algorithm**:
  Offline phase:
  1. Choose at random $(m_i,r_i)\in_R M\times R$, and compute the hash value $h_i=H_{HK}(m_i,r_i)$.
  2. Run the signing algorithm S with the signing key SK to sign the message h_i. Let the output be $\sigma_i=S_{SK}(h_i)$.
  3. Store the pair (m_i,r_i), and the signature σ_i.

  Online phase:
  1. For a given message m, retrieve from the memory a random pair (m_i,r_i), and the signature σ_i.
  2. Compute $r\in R$ such that $H_{HK}(m,r)=H_{HK}(m_i,r_i)$.

3. Send (r, σ_i) as the signature of the message m.

- **The Verification Algorithm:**
  1. Compute $h_i = H_{HK}(m, r)$.
  2. Verify that σ_i is indeed a signature of the hash value h_i with respect to the verification key VK.

In the Shamir and Tauman's online/offline signatures [2], a limitation is that the signature for different messages must use different hash values. Otherwise, if the signer uses the same hash value twice to obtain two different messages, the recipient can obtain a hash collision and use it to recover the signer's trapdoor information.

A DOUBLE-TRAPDOOR HASH FUNCTION

In this section, we propose a new trapdoor hash function based on factoring assumption, which is a main ingredient for designing our efficient online/offline signature scheme.

- **The key generation Algorithm** I.
  Choose at random a safe primes $n \in \{0,1\}^k$ ($n = 2n'+1$, n' is also prime). Choose at random an element $g \in Z_n^*$ of order $\phi(n)$. Choose random element $x, y \in_R Z_{\phi(n)}$, and compute $X = g^x \bmod n, Y = g^y \bmod n$. The public hash key is (n, g, X, Y) and the private trapdoor key is (x, y).

- **The hash function** H **.**
  Given the public hash key $HK = (n, g, X, Y)$, the new trapdoor hash function $h_{HK} : Z_{\phi(n)} \times Z_{\phi(n)} \to Z_n^*$ is defined as $h_{HK}(m, r) = X^m Y^r \bmod n$.

Theorem 1. *The construction above is a trapdoor hash function under the assumption of that factoring problem is in tractable.*

Proof. 1. *Efficiency*: Given the public hash key $HK = (n, g, X, Y)$ and a pair $(m, r) \in Z_{\phi(n)} \times Z_{\phi(n)}$, the function $h_{HK}(m, r) = X^m Y^r \bmod n$ is computable in polynomial time.

2. *Collision resistance:* Assume to the contrary, there exists a probabilistic polynomial time algorithm A that on input HK outputs, with a probability which is non-negligible, two pairs $(m_1, r_1), (m_2, r_2) \in Z_{\phi(n)} \times Z_{\phi(n)}$ that satisfy $m_1 \neq m_2$ and

$h_{HK}(m_1, r_1) = h_{HK}(m_2, r_2)$. Then we can use A to solve the discrete logarithm problem as follows: For a randomly given instance $(a, g^a \bmod n)$, choose a random element $b \in_R Z_{\phi(n)}$ and define $X = g^a \bmod n, Y = g^b \bmod n$ .Therefore if $g^{am_1} g^{br_1} = g^{am_2} g^{br_2}$, we can compute $a = (m_1 - m_2)^{-1}(r_2 - r_1)b$.

3. *Trapdoor collisions*: Given the public hash key $HK = (n, g, X, Y)$ and a corresponding trapdoor key (x, y). Given a pair $(m_1, r_1) \in Z_{\phi(n)} \times Z_{\phi(n)}$, and an additional message $m_2 \in Z_{\phi(n)}$, we want to find $r_2 \in Z_{\phi(n)}$ such that $g^{xm_1} g^{yr_1} = g^{xm_2} g^{yr_2}$, the value of r_2 can be computed in polynomial time as follows:
$r_2 = r_1 + xy^{-1}(m_1 - m_2) \bmod(\phi(n))$.

It remains to note that if r_1 is uniformly distributed in $Z_{\phi(n)}$ then r_2 is also uniformly distributed in $Z_{\phi(n)}$.

In this hash function, there are two trapdoors. The trapdoor/hash key pair of the first one is $(y)/(n, g, Y)$, which is used to build *long-term* trapdoor . The trapdoor/hash key pair of the second one is $(x)/(n, g, X)$, which is used to build *one-time* trapdoor . The concept of multi-trapdoor function has been introduced in [12], while a concrete double-trapdoor function was proposed in [13]. This kind of function is very helpful to the construction of Online/Offline signature without key exposure.

A WEAKLY SECURE SIGNATURE SCHEME BASED ON THE $k+1$ SQUARE ROOTS ASSUMPTION

In 2006, Zhang et al. [4] proposed a new complexity assumption, which is called $k+1$ square roots assumption.

Definition 1 ($k+1$**-Square Roots Problem).** For an integer k, and $x \in_R Z_q, g \in G$, given

$$\{g, \alpha = g^x, h_1, \cdots, h_k \in Z_q, g^{(x+h_1)^{1/2}}, \cdots, g^{(x+h_k)^{1/2}}\},$$

compute $g^{(x+h)^{1/2}}$ for some $h \notin \{h_1, \cdots, h_k\}$.

Definition 2 ($k+1$**-Square Roots Assumption).** We say that the $(k+1, t, \varepsilon)$-Square Roots assumption holds in (G, G_T) if no t-time algorithm has advantage at least ε in solving the $k+1$-Square Roots

Problem in (G, G_T), i.e., $k+1$-Square Roots Problem is (t, ε)-hard in (G, G_T).

Zhang et al. constructed a EF-CMA (existentially unforgeable under adaptive chosen message attacks) secure short signature scheme based on this assumption in the standard model.

We consider the following two types of attacks:

- **Adaptive chosen message attack:** The attacker is given signature for a list of messages of his adaptive choice. In particular, the choice of each message can depend on the verification key and on the signature produced for previous messages.
- **Known message attack:** The attacker has access to an oracle that signs a list of known message, which should be produced before any signature is given, and should be independent of the verification key.

We call a signature scheme is *adaptive secure* if it is existentially unforgeable under adaptive chosen message attacks (EF-CMA), while we call a signature scheme is *weakly secure* if it is existentially unforgeable under known message attacks (EF-KMA). From Shamir and Tauman's result [2], we can conclude that the online/offline signature scheme is adaptive secure, if the basic signature scheme is only weakly secure.

In this section, we design a weakly secure signature scheme based on the $k+1$ square roots assumption in the standard model. We describe the weakly secure signature as follows:

Let $e: G \times G \to G_T$ be the bilinear pairing where $|G| = |G_T| = v$ for some prime v, and $\phi(v) = n$. The system parameters are (G, G_T, e, v, g'), here $g' \in G$ is a random generator. We assume that $v \equiv 3 \bmod 4$ (so that -1 is a non-quadratic residue modulo v).

Key Generation. Randomly select $z \in_R Z_v^*$, and compute $u = g'^z$. The public key is u. The secret key is z.

Signing. Given a secret key z, and a message m, computes $\sigma = g'^{(m+z)^{1/2}}$. If $(m+z)$ is a non-quadratic residue modulo v, compute $\sigma = g'^{(-(m+z))^{1/2}}$.

Verification. Given a public key (G, G_T, e, v, g'), a message m, and a signature σ, verify that $e(\sigma, \sigma) = e(g'^m u, g')$ or $e(\sigma, \sigma) = e(g'^m u, g')^{-1}$.

Theorem 2. *Suppose the* $(k+1,t',\varepsilon)$ *square roots assumption holds in* G, *then the basic signature scheme above is* (t,q_S,ε) *-secure against existentially forgery under known message attacks (EF-KMA) provide that* $t \le t'-O(k)$ *and* $q_S < k+1$.

Proof. Assume A is a forger that (t,q_S,ε) -breaks the signature scheme. We construct an algorithm B that, by interacting with A, solves the (q_S+1,t',ε) square roots problem (also $(k+1,t',\varepsilon)$ square roots problem, if $k > q_S$) in time t' with advantage ε. Algorithm B is given an instance
"For a integer q_S, *and* $z \in_R Z_v$, $g' \in G$, *given*
$\left\{ g', u = g'^{z}, m_1, \cdots, m_{q_S} \in Z_v, g'^{(z+m_1)^{1/2}}, \cdots, g'^{(z+m_{qS})^{1/2}} \right\}$
to compute $g'^{(z+m^*)^{1/2}}$ *for some* $m^* \notin \{m_1, \cdots, m_{q_S}\}$. *"*

Algorithm B does so by interacting with the forger A as follows:

Query: Algorithm A outputs a list of distinct q_S messages $m_1, \cdots, m_{q_S} \in Z_v^*$, and A must reveal its queries up front.

Response: B must respond signatures on the q_S messages from A with $g'^{(z+m_1)^{1/2}}, \cdots, g'^{(z+m_{qS})^{1/2}}$.

Output: Eventually, A outputs a forgery (m^*, σ^*). Here $m^* \notin \{m_1, \cdots, m_{q_S}\}$. Since (m^*, σ^*) is a valid forgery, it satisfies:
$e(\sigma^*, \sigma^*) = e(g'^{m^*} u, g')$
So, $\sigma^* = g'^{(z+m^*)^{1/2}}$. B outputs (m^*, σ^*) as a solution to B's challenge.
The claimed bounds are obvious by construction of the reduction.

NEW ONLINE/OFFLINE SIGNATURE SCHEME WITHOUT KEY EXPOSURE IN THE STANDARD MODEL

In this section, we eventually combine the primitives described in the section above using Shamir and Tauman's approach, and get a new online/offline signature scheme.

- **Key Generation:**
  1. Run the key generation algorithm of the weakly secure signature to obtain the signing/verification key pair $(z)/(u, g')$.
  2. Run the key generation algorithm of double-trapdoor hash function to obtain the *long-term* trapdoor/hash key pair $(y)/(n, g, Y)$.
  3. Choose at random $x^* \in_R Z_{\phi(n)}$, and compute the double-trapdoor hash value $h = Y^{x^*} \bmod n$.
  4. Run the signing algorithm of the weakly secure signature to sign the hash value h. Let output be $\sigma = g'^{(h+z)^{1/2}}$ or $\sigma = g'^{(-(h+z))^{1/2}}$.

- **Signing:**
  1. Offline phase:
     i. Choose at random $x_i \in_R Z_{\phi(n)}$, and compute $X_i = g^{x_i} \bmod n$ and $x_i y^{-1} \bmod \phi(n)$.
     ii. Store the one-time trapdoor/hash key pair $(x_i y^{-1})/(X_i, g)$.
  2. Online phase:
     i. For a given signed message m_i, retrieve from the memory a random key pair $(x_i y^{-1})/(X_i, g)$.
     ii. Compute $r_i = x^* - x_i y^{-1} m_i (\bmod \phi(n))$.
     iii. Send (r_i, X_i, σ) as the signature of the message m_i.

- **Verification:**
  1. Compute $h = X_i^{m_i} Y^r \bmod n$.
  2. Verify that σ is indeed a signature of the hash value h.

***Remark**:* In our proposed online/offline signature scheme, the *one-time* trapdoor hash key $X_i = g^{x_i} \bmod n$ is used only once for signing the message m_i. Hence, the hash value and the corresponding signature are always identical and can be viewed as the public key of the signer. So there is no key exposure problem in our online/offline signature scheme.

Theorem 3. *If the $k+1$ square roots assumption is valid, then the online/offline signature scheme above is existentially unforgeable under adaptive chosen message attacks (EF-CMA).*

Proof. From Theorem 1 we have that the trapdoor hash family used in the construction above is secure trapdoor hash function. Theorem 2 states that

the basic signature used to sign the hash value h is weakly secure under the $k+1$ square roots assumption We prove it in the standard model. Hence, using the result from Shamir and Tauman [2], we can conclude that the online/offline signature scheme above is existentially unforgeable under adaptive chosen message attacks (EF-CMA).

CONCLUSION

In this paper, we utilize the Shamir and Tauman's paradigm to construct a new online/offline signature scheme based on the $k+1$ square roots assumption. Our proposal is existentially unforgeable under adaptive chosen message attacks in the standard model. In our scheme, we design a double-trapdoor hash family, which can avoid the key exposure problem. So the signer need not compute and store plenty of different hash values and the corresponding signatures on the hash value in the offline phase.

ACKNOWLEDGEMENTS

This work is supported by National Basic Research Program of China (No 2007CB310704), National Natural Science Foundation of China (No 60673098) and NSFC-RGC Joint Research Foundation (No 60731160626).

REFERENCES

[1] S. Even, O. Goldreich, and S. Micali. 1990. On-line/off-line Digital Signatures. *In Advances in Cryptology: Crypto'89, LNCS 2442*, Springer, pp. 263-277.

[2] A. Shamir and Y. Tauman. 2001. Improved Online/Offline Signature Schemes. *In Advances in Cryptology: Crypto'01, LNCS 2139*, pp. 355-367.

[3] K. Kurosawa and K. Schmidt-Samoa. 2006. New Online/Offline Signature Schemes without Random Oracles. *PKC 2006, LNCS* 3958, pp. 330-346.

[4] F. Zhang, X. Chen, W. Sulio and Y. Mu. 2006. A New Signature Scheme without Random Oracles from Billinear Pairings. *VIETCRYPT 2006, LNCS 4341*, pp. 67-80.

[5] H. Krawczyk and T. Rabin. 2000. Chameleon Signatures. *In Symposium on Network and Distribute Systems Security (NDSS'00)*, Internet Society, pp. 143-154.

[6] S. Goldwasser, S. Micali and R. Rivest. 1988. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. *SIAM J. on Computing*, 17, pp. 281-308.

[7] S. Even, O. Goldreich, and S. Micali. On-line/Off-line Digital Signatures. *Journal of Cryptology*, 9(1), pp. 35-67, Springer-Verlag, 1996.

[8] A. Fiat and A. Shamir. 1986. How to prove yourself: Practical solutions to identification and signature problems. *Crypto'86, LNCS 263*, pp. 186-194.

[9] C.P. Schnorr. 1991. Efficient signature generation for smart cards. *Journal of Cryptology*, 4(3), pp. 239-252.

[10] T. Elgamal. 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4), pp. 469-472.

[11] X.Chen, F. Zhang, S. Willy, and Y. Mu. 2007. Efficient Generic On-line/Off-line Signatures without Key Exposure. *ACNS'07, LNCS 4521*, pp. 18-30.

[12] R. Gennaro. 2004. Multi-trapdoor Commitments and Their applications to Proofs of Knowledge Secure Under Concurrent Man-in-the-Middle Attacks. *Crypto'04, LNCS 3152*, pp. 220-236.

[13] E. Bresson, D. Catalano, R. Gennaro. 2007. Improved On-Line/Off-Line Threshold Signatures. *PKC'07, LNCS 4450*, pp. 217-232.