A Novel k-Times Short Digital Signature Scheme using Pairing

Jianhong Zhang
College of Sciences
North China University of Technology
Beijing, 100144 China
jhzhangs@163.com

Jianjun Xie
College of Mathematics and Information Science
Hebei Normal University,
Shijiazhuang 050016,China
jj_xie@sohu.com

***Abstract*—Digital signature schemes allow a signer to transform any arbitrary message into a signed message, such that anyone can verify the validity of the signed message by the signer's public key. But, sometimes, we need to constrain the signer's signature times. In this letter, we propose a $k-$times short signature scheme and show that the scheme is secure without random oracle. The scheme makes that the signer can only produce k times signature, and only need one time point multiplication operator in whole signing phase, and the size of the signature is only one element in a finite field. Thus the scheme is very suitable to mobile agent.**

***Index Terms*—short signature, $k-$times, random oracle, security analysis**

I. Introduction

Digital signature schemes are an important cryptographical tool and allow a signer to transform any arbitrary message into a signed message, such that anyone can verify the validity of the signed message by the signer's public key. In general, digital signature can be divided int two classes. The first class includes one-time signatures and their variants based on one-way functions. These scheme can be used to sign a predetermined number of messages, we call them *multiple-time signature schemes*. The other class is based on public-key cryptography and they can be used to sign unlimited number of message.

Despite the limit imposed on the number of messages signed, multiple-time signature have found many applications. for example, in the design of public-key signature scheme[6], on-line/off-line signature[7] and broadcast authentication protocol[8].

To adapt to practice demand, short digital signature had been put forward. Short Signature are always desirable. They are necessary in some situation where people need to enter the signature manually, such as PDA that is not equipped with a keyboard. Additionally, short digital signatures are essential to ensure the authenticity of message in low-bandwidth communication channels. In general, short signatures are used to reduce the communication complexity of any transmission. as noted in [1], when one need sign a postcard, it is desirable to minimize the total length of the original message and the appended signature.

We know, the size of DSA signature is about 320 bits long, but A 320-bits signature is too long to be keyed in by a human. To Construct a short signature scheme, several proposals show how to shorten DSA while preserving the same level of security. Naccache and Stern[1] propose a variant of DSA where the signature length is approximately 240 bits. Subsequently, Mironov [2] suggests a DSA variant with a similar length and gives a concrete security of analysis of the construction in the random oracle model. Another technique proposed for reducing DSA signature length is a signature with message recovery[3]. In such systems one encodes a part of the message into the signature thus shortening the total length of the message-signature pair. For a long message, one can then achieve DSA signature overhead of 160 bits.

Because the 160-bits elliptic curve key size can provide the security of 1024-bits RSA key size. Recently, some efficient cryptosystems based on elliptic curve have been proposed. In particular, the signature schemes based on the bilinear pairing of elliptic curve have been proposed, and some scheme can realize short signature, such as D.Boneh et.al 's short signature[4]. Based on the above problems, in this letter, we propose a k-times short signature scheme and show that the scheme is secure under the Square Decisional Diffie-Hellman assumption, and the size of the signature is the same as D.Boneh's short signature.

The paper is organized as follows. In section 2, we review the preliminary knowledge. In section 3, we propose our k-times short signature scheme. In section 4, the security of the scheme is discussed. Finally, we conclude the paper in section 5.

II. Preliminaries

In this section, we first review a few concept related proposed short signature scheme.

A. Bilinear Pairing

Let $\mathbb{G}_1$ be additive group whose order is a prime q, and $\mathbb{G}_2$ be a multiplicative group of the same order q. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$ be the bilinear pairing with the following properties, please refer to [5,4] for the detail content.

- Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1, a, b \in \mathbb{Z}_q$

- Non-degeneracy: There exists $P, Q \in \mathbb{G}_1$ such that $e(P,Q) \neq 1$, in other words, the map doesn't send all pairs in $\mathbb{G}_1 \times \mathbb{G}_1$ to the identity in $\mathbb{G}_2$
- Computability: There is an efficient algorithm to compute $e(P,Q)$ for $P, Q \in \mathbb{G}_1$.

For example, Weil pairing and Tate pairing satisfy the above three properties. We would like to suggest adopt the Tate pairing for implementation since the current research indicates that there exist quite a few efficient algorithms to compute the Tate pairing.

B. Square Decisional Diffie-Hellman Assumption (SDDH Assumption)[10]

Let G_1 be a large cyclic group of prime order q. P is a generator of the group G_1, then $e(P,P)$ is a generator of the group G_2. Let $g = e(P,P)$, we consider the following two distributions:

- Given a square Diffie-Hellman triple (g, g^x, g^{x^2}), where $x \in Z_q$ is a random string chosen uniformly at random;
- Given a random triple (g, g^x, g^r), where $x, r \in Z_q$ are two random strings chosen uniformly at random.

We say that the Square Decisional Diffie-Hellman Assumption holds in G_2 if no t-time algorithm has advantage at least ϵ to distinguish the above two triple distributions in G_2.

C. Generalized Square Decisional Diffie-Hellman Assumption (Generalized SDDH Assumption)[10]

For any k, the following distributions are indistinguishable:

- The distribution R^k of any random k+1-tuple $(g, g^{x_1}, g^{x_2}, \cdots, g^{x_k}) \in G_2^k$, where $x_1, x_2, \cdots, x_k \in Z_q$ are uniformly distributed in G_2^k
- The distribution D^k of k+1-tuples $(g, g^x, g^{x^2}, \cdots, g^{x^k}) \in G_2^k$, where $x \in Z_q$are uniformly distributed in G_2^k.

III. Our Proposed Signature Scheme

In this section, we are ready to present our new k-times short signature scheme. For simplicity, without loss of generality,we set $k = 2$ to discuss our k-times short signature scheme. We use the following notations:

- S: a signer,
- V: a verifier ,
- m : a message to be signed by S.
- $H(\cdot)$: a hash function, s.t H: $\{0,1\}^* \rightarrow Z_q$

[Key Generation]

1) S chooses a generator P at random, and randomly selects $r, s \in Z_q$.
2) S computes $V_1 = sP, g = (P,P)$ and for $(1 \leq i \leq k)$ the signer S computes $v_i = g^{r^i}$.

[Key Parameter]

- the public key of the signer is $(g, V_1, v_1, v_2, \cdots, v_k)$ and the corresponding secret key is (r, s).

(Note that when $k = 2$, the public key is $(V_1, v_1 = g^r, v_2 = g^{r^2})$)

[Signature Generation]

To produce a signature on the message m, the signer S executes as follows:

- the signer sets $S = \frac{1}{s}P$;
- the signer S computes
  $e = H(m)$ and
  $\alpha = (r+e)^k S$ (Note that when $k = 2, \alpha = (r+e)^2 S$)
- send message-signature pair (m, α) to the verifier.

[Verification]

- the verifier V first computes $e = H(m)$.
- V then checks whether $e(V_1, \alpha) = \prod_{i=1}^{k} (v_i)^{C_k^i} e^{k-i} g^{e^k}$ (Note that when $k = 2$, the verifier checks $e(V_1, \alpha) = v_2 v_1^{2e} \cdot g^{e^2}$)

Note that the exponentiation operations in G_2 are significantly faster than pairing operations.

IV. Security Analysis

In the section, we will discuss the security of the proposed scheme and show that the scheme can only provide k signatures. At the same time, we also show the security of the scheme is based on Square decisional Diffie-Hellman assumption.

Theorem1: *Our proposed k-times Short signature scheme can only provide k signatures on k different messages.*

proof: According to the above signing process, we know the signature of message m is $\alpha = (r+e)^k S$. However, in fact, $\alpha = (r^k + C_k^1 e r^{k-1} + C_k^2 r^{k-2} e^2 + \cdots + e^k)S$. Since r, S are two unknown numbers, we set $y_1 = r^k S, y_2 = r^{k-1} S, y_3 = r^{k-2} S, \cdots, y_{k+1} = S$, then we can obtain

$$\alpha = y_1 + C_k^1 e y_2 + \cdots + C_k^{k-1} y_k e^{k-1} + e^k y_{k+1}$$

To solve the above $k+1$ unknown numbers $y_1, y_2, \cdots, y_{k+1}$, we must obtain at least $k+1$ signatures. Namely,

$$\begin{aligned}
\alpha_1 &= y_1 + C_k^1 e_1 y_2 + \cdots + C_k^{k-1} y_k e_1^{k-1} + e_1^k y_{k+1} \\
\alpha_2 &= y_1 + C_k^1 e_2 y_2 + \cdots + C_k^{k-1} y_k e_2^{k-1} + e_2^k y_{k+1} \\
&\vdots \quad\quad \vdots \\
\alpha_{k+1} &= y_1 + C_k^1 e_{k+1} y_2 + \cdots + C_k^{k-1} y_k e_{k+1}^{k-1} + e_{k+1}^k y_{k+1}
\end{aligned}$$

By the transformation, the $k+1$ signatures can been written as follows:

$$(\alpha_1, \cdots, \alpha_{k+1}) =$$

$$(y_1, \cdots, y_{k+1}) \begin{pmatrix} 1 & 0 & \cdots & 1 \\ 0 & C_k^1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \cdots & 1 \\ e_1 & \cdots & e_{k+1} \\ \vdots & \vdots & \vdots \\ e_1^k & \cdots & e_{k+1}^k \end{pmatrix}$$

the numbers of the catercorner is non-zero in first matrix. The second matrix is a Vandermonde matrix, when the signer produces signatures on k different messages, then $e_i = H(m_i)$ $for 1 \leq i \leq k$ is different. Therefore, we obtain that the

two matrixes are singularity, the two matrixes exist reversible matrixes.

According to the state above, we obtain to solve $(y_1, y_2, \cdots, y_{k+1})$ by k signatures on k different messages. That is to say, our proposed scheme can only provide k signatures on different messages. □.

Theorem2: *Let A be a forger against our k -times Short signature scheme, where the group G_1 has prime order q. Then the SDDH problem can be solved in G with probability ε' and within T'.*

Proof: We are going to construct a probabilistic polynomial time Turing machine F which will use the attacker A as a sub-routine in order to solve a given instance of the Square Decisional Diffie-Hellman problem. Therefore, F will try to perfectly simulate the environment of A.

The machine F receives the two distributions $(q, G_1, P, x_1P, x_2P, \cdots, x_kP) \in G_1^k$, where $x_1, x_2, \cdot, x_k \in Z_q$ and $(q, G_1, P, xP, x^2P, \cdots, x^kP) \in G_1^k$, where $x \in Z_q$, and its goals is to distinguish the above two distributions. For simplicity to discuss, we set $(a_1P, a_2P, \cdots, a_kP)$, where $(a_1, a_2, \cdots, a_k) = (x, x^2, \cdots, x^k)$ or $(a_1, a_2, \cdots, a_k) = (x_1, x_2, \cdots, x_k)$.

The machine F randomly chooses a number $s \in Z_q$ and computes $V_1 = sP$, then sets the public key as follows: for $(1 \leq i \leq k)$

$$v_i = e(a_iP, P)$$

then, the machine F sends $(V_1, v_1, v_2, \cdots, v_k)$ as the public key to the forger A. If the forger A can forge a signature on the message m with probability ε' and within T', then the machine F can distinguish the above two distributions with probability ε' and within T'. □

As the size of signature, the signature of our proposed scheme is only one element in a finite field. While standard signature based on discrete log such as DSA require two elements. Therefore,our signatures are much shorter than all current variants of DSA for the same security. When we adopt a supersingular elliptic curve over finite field F_{p^n} with embedding degree $k = 6$ and the modified Weil pairing[4], the length of an element in Z_q^* and G_1 can be approximately $log_2 q$ bits, therefore the total signature length is approximately $log_2 q$ bits. Thus, our proposed scheme is very suitable to mobile agent.

V. Conclusion

As a special signature, ring signature is an anonymous signature which allows a user to anonymously sign on behalf of a group. In real life, we often work in the multi-user setting and hope only the designated users can check our signatures, such as hospital records. In the work, by combining ring signature and designated verifier signature scheme, a ring signature scheme with Multi-designated verifiers are proposed to satisfy the multi-user setting. And the proposed scheme is proven to be secure in a novel assumption: the Chosen-Target-Inverse-CDH problem under the random oracle model.

Acknowledgement

This work is supported by Natural Science Foundation of China (NO:60703044,90604010), the New Star Plan Project of Beijing Science and Technology (NO:2007B001), the PHR, Program for New Century Excellent Talents in University(NCET-06-188), The Beijing Natural Science Foundation Programm and Scientific Research Key Program of Beijing Municipal Commission of Education (NO:KZ2008 10009005) and 973 Program (No:2007CB310700).

References

[1] D.Naccache and J.Stern, and S.Takano, *Signing on a postcard*, In Y.Frankel, editor, Proceedings of Financial Cryptography 2000, vol 1962 of LNCS, pp121-135, springer-verlag, Berlin 2000 .

[2] I. Mironov. A Short Signature as Secure as DSA. Unpublished manuscript, 2001.

[3] L.Pintsov and S.Vanstone. Postal revenue collection in the digital age. In Y.Frankel, editor, Proceedings of Financial Cryptography 2000, vol 2000 of LNCS, pp 105-125, Springer-verlag, Berlin 2000.

[4] Dan Boneh, Ben Lynn, and Hovav Shacham, Short Signature from the Weil Paring, editor, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp 514-532, Springer-verlag, 2001.

[5] D.Boneh and M.Franklin, Identity-based encryption from the weil pairing, Advances in Cryptology-Crypto 2001, LNCS 2139, pp 213-229, Springer-verlag, 2001.

[6] C.Dwork and M.Naor, An efficient existentially unforgeable signature scheme and its applications, Advances in Cryptology-Crypto'94, LNCS 839, 1994, pp 234-246.

[7] J.Zhang, W.Zou,D.Chen and Y.Wang,On the Security of a Digital Signature with Message Recovery Using Self-certified Public Key,Informatica, Vol.29 (3), pp 343-346.

[8] S.Even, O.Goldreich and S.Micali. On-line/off-line digital signatures, Journal of Cryptology, Vol(9) 1996, pp 35-67

[9] A.Perrig. The BiBa one-time signature and broadcast authentication. the 8th ACM Conference on Computer and Communication security, ACM, 2001, pp 28-37

[10] T.Okamoto, A.Inomata and E.Okamoto, A proposal of short proxy signature using pairing, In the proceedings of the International Conference on Information Technology: Coding and Computing, pp. 631-635, 2005

[11] F.Bao, R.H.Deng, and H.F.Zhu, Variations of Diffie-Hellman Problem, ICICS 2003, LNCS 2836, pp 301-312, 2003