On-line/Off-line Identity-based Signature Scheme with Strong Unforgeability in the Standard Model

Xiaodong Yang, Chunlin Chen, Tingchun Ma, Yutong Li and Likun Xiao

College of Computer Science and Engineering Northwest Normal University Lanzhou, Gansu 730070, China
Email: y200888@163.com

Abstract. To solve the problems of low efficiency of the strong unforgeable identity-based signature scheme, a new strong unforgeable on-line/off-line identity-based signature scheme in standard model is proposed. Our new scheme uses the chameleon hash function and divides the signature algorithm into two stages: on-line stage and off-line stage. Our scheme generates signatures in a very short time, which efficiently improves the performance of the signature. The analysis results show that the proposed scheme not only has higher security, but also has lower computation cost.

1. Introduction
In 1984, Shamir proposed an identity-based public key cryptosystem [1]. The advantage of identity-based cryptosystem is that it reduces users’ dependence on public key certificates. Since 1984, many identity-based signature schemes have been proposed. At present, there are mainly two models: random oracle model and standard model. Some signature and encryption schemes are secure in the random oracle model, but not in the standard model [2]. Therefore, it is of significance to design a provable security signature scheme in the standard model. The references [3, 4] are identity-based signature schemes in the standard model, but these schemes are only existential unforgeable.

Since some existentially unforgeable identity-based schemes are malleable [5], it is easy to modify the previous valid signature to a new legal signature on the same message. Thus, strong unforgeability has been introduced [6]. Yang et al. proposed a strong unforgeable identity-based signature scheme [7]. However, the efficiency of Yang’s scheme is low and can not be applied to devices with limited computing power.

Even et al. first proposed the concept of on-line/off-line signature scheme in 1989 [8]. The advantage of on-line/off-line signature is to reduce the signature overhead. Based on the scheme of Yang et al., combined with the chameleon hash function, we propose an on-line/off-line identity-based signature scheme with strong unforgeability in the standard model that can generate legal signatures of messages in a very short time.

2. Preliminaries
2.1. Discrete Logarithm Problem
Let $G$ be a cyclic group whose order is $p$, $p$ is a large prime number, and $g$ is a generator of $G$. The discrete logarithm (DL) problem on group $G$ is to compute $a$ given $(g, g^a) \in G$ for $a \in \mathbb{Z}_p^*$.

Definition 1 A DL problem is $(t, \varepsilon_{DL})$-hard if no $t$-polynomial time adversary has advantage at least probability $\varepsilon_{DL}$ in solving the DL problem.
2.2. **Computational Diffie-Hellman Problem**

Let $G$ be a cyclic group whose order is $p$, $p$ is a large prime number, and $g$ is a generator of $G$. The computational Diffie-Hellman (CDH) problem on group $G$ is to compute $g^{ab}$ given $(g, g^a, g^b) \in G^3$ for $a, b \in \mathbb{Z}_p^*$.

**Definition 2** A CDH problem is $(t, \epsilon_{CDH})$-hard if no $t$-polynomial time adversary has advantage at least probability $\epsilon_{CDH}$ in solving the CDH problem.

2.3. **Chameleon Hash Function**

The chameleon hash function $CH(\cdot, \cdot)$ is a special hash function [9], which has a threshold key $TK$ and a public key $HK$ and satisfies the following properties:

1. **Efficiency:** Given the public key $HK$, a message $m$ and a random number $r$, there exists a polynomial time algorithm to compute $CH_{HK}(m,r)$.
2. **Collision resistance:** Enter the public key $HK$, there is no probability polynomial time algorithm outputs $11(m,r)$ and $22(m,r)$ with a non-negligible probability, such that $12mm \neq 1122(m,r)$.
3. **Trapdoor collisions:** Given a threshold key $TK$, a public key $HK$, two different messages $(m_1, m_2)$ and a random number $r_i$, there exists a probabilistic polynomial time algorithm that outputs a value $r_2$, such that $1122(m_1, r_i) = CH_{HK}(m_1, r_i)$. If $r_i$ is uniformly distributed, then the distribution of $r_2$ is computationally indistinguishable from uniform.

3. **Our Scheme**

Based on chameleon hash function $CH(m,r) = h^r y^r$, an identity-based on-line/off-line signature scheme with strong unforgeability in the standard model is designed. The scheme is described as follows:

3.1. **Setup**

The PKG selects two large prime numbers $p$ and $q$, satisfying $q \mid p - 1$, two cyclic groups $G_1, G_2$ of prime order $p$, a generator $g$ in $G_1$, and a bilinear pairing $e: G_1 \times G_2 \rightarrow G_3$. Also, the PKG randomly selects $\alpha, \beta \in \mathbb{Z}_p$, and computes $g^\alpha$ and $msk = g^\beta$. Furthermore, the PKG selects a $q$-order element $h \in \mathbb{Z}_p^*$.

3.2. **Extract**

For a user’s identity $ID$, the PKG randomly selects $r \in \mathbb{Z}_p^*$ and computes $K(ID) = (v_1, \ldots, v_m)$, $U = \prod_{i=1}^{m} v_i$ and $sk_{ID} = (sk_1, sk_2) = (g^\alpha U^{r_i}, g^{r_i})$. Then, the PKG transmits the private key $(sk_{ID}, x, X)$ to the user through a secure channel.

3.3. **Sign**

In order to generate the signature of the message $m$, the signer performs the following steps:

(1) **Off-line stage:** Generate status information $St$ using the private key $(sk_{ID}, x, X)$.

   ① Randomly choose $m', r' \in \mathbb{Z}_q^*$, compute $CH(m', r') = h^r y^r \mod p$ and $R = X m' + r' \mod q$. 
② Randomly choose \( r_m \in \mathbb{Z}_p^* \), compute \( \sigma_3 = g^{r_m} \).

③ Using \( sk_{ID} = (sk_1, sk_2) \) to set \( \sigma_2 = sk_2 \), and to compute \( F(CH(m', r')) = (M_1, \ldots, M_n) \), \( W = \prod_{j=1}^n w_j^M_j \), \( s = H(M, ID, sk_2, g^{r_m}) \) and \( \sigma_1 = sk_1 \cdot (v^W)^{r_m} \).

④ Save the status information \( St = \{m', r', CH(m', r'), \sigma_1, \sigma_2, \sigma_3, R\} \).

(2) On-line stage: For the message \( m \) to be signed, the signature of \( M \) is generated by using the private key \( (sk_{ID}, x, X) \) and the state information \( St \).

① Extract the status information \( St = \{m', r', CH(m', r'), \sigma_1, \sigma_2, \sigma_3, R\} \).

② Compute \( r = R - Xm \pmod{q} \), it indicates \( CH(m', r') = CH(m, r) \).

③ Output a signature \( \sigma = (\sigma_1, \sigma_2, \sigma_3, r) \) of message \( m \).

3.4. Verify

Given an identity \( ID \) and the signature \( \sigma = (\sigma_1, \sigma_2, \sigma_3, r) \) of a message \( m \), the verifier performs the following steps:

(1) Compute \( s = H(m, ID, \sigma_2, \sigma_3) \) and \( CH(m, r) = h^n y^r (\pmod{p}) \).

(2) Compute \( K(ID) = (v_1, \ldots, v_n) \), \( U = \prod_{i=1}^n u_i^{v_i} \), \( F(CH(m, r)) = (M_1, \ldots, M_n) \) and \( W = \prod_{j=1}^n w_j^{M_j} \).

(3) A verifier checks the following verification equation:

\[
e(\sigma_1, g) = e(g_2, g_1) e(U, \sigma_2) e(v^W, \sigma_3)
\]

If the above equation holds, it means that \( \sigma \) is a legal signature of identity \( ID \) and message \( m \). Otherwise, \( \sigma \) is illegal.

4. Analysis Of The Scheme

In this section, we analyze the correctness, security and performance of the proposed scheme.

4.1. Correct Analysis

Because of \( r = R - Xm \pmod{q} \), we have

\[
CH(m, r) = h^n y^r = h^n y^{R - Xm} = h^n y^{(Xm + r) - Xm} = h^n h^{(x m + r - Xm)} = h^n h^{x m + r - m} = h^n h^{w} = h^n y^r (\pmod{p}) = CH(m', r').
\]

Since \( (\sigma_1, \sigma_2, \sigma_3) \) is the legal signature of \( CH(m', r') \), \( (\sigma_1, \sigma_2, \sigma_3) \) is also the legal signature of \( CH(m, r) \).

4.2. Security Analysis

**Theorem 1** In the standard model, the on-line/off-line identity-based signature scheme proposed in this paper is strongly unforgeable against the adaptive chosen-message attacks.

**Proof:** The method of document [10] is used to prove the security of our new scheme. Suppose that the attacker \( A \) can successfully break the strong unforgeability of the above scheme with a non-negligible probability \( \varepsilon \). The following proves that there is a polynomial time algorithm \( B \), which can solve an instance of discrete logarithm problem with a probability of at least \( \varepsilon / 2 \), or successfully forge the signature of our scheme with a probability of at least \( \varepsilon / 2 \).
Suppose that the attacker $A$ asks for the signature of $q$ messages $\{m_i\}_{i=1}^q$ and obtains the corresponding signatures $\{(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, r_i)\}_{i=1}^q$. After the signature query, the attacker $A$ outputs a forgery $(\sigma_1^*, \sigma_2^*, \sigma_3^*, r^*)$ of the message $m^*$. The forgery of $A$ can be divided into the following two types.

**Type 1** There is an $i \in \{1, 2, \cdots, q\}$ that satisfies $CH(m_i, r_i) = CH(m^*, r^*)$.

**Type 2** For any $i \in \{1, 2, \cdots, q\}$, satisfy $CH(m_i, r_i) \neq CH(m^*, r^*)$.

If the first type holds, a probability polynomial time algorithm $B$ is defined, which uses the forgery of the attacker $A$ to find a collision of the chameleon hash function, thus solving an instance of the DL problem.

Suppose that the instance of DL problem received by $B$ is $(h, y) \in Z_p^*$, the goal of $B$ is to determine the discrete logarithm of $y$: $\log_h y = x$. $B$ simulates an on-line/off-line signature security game according to the following procedure.

**Setup:** $B$ runs the Setup algorithm to generate parameters, sends the generated system parameter $cp$ to the attacker $A$. The private key $\alpha$ is known to $B$, but $x$ is unknown to $B$.

**Queries:** $A$ asks for the signature of message $m_i$, $B$ first selects a random number $r_i \in Z_p^*$, calculates $CH(m_i, r_i)$, then runs signature generation algorithm $Sign$ to generate the signature $(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, r_i)$ of $CH(m_i, r_i)$, and returns the signature value to the attacker $A$.

**Forgery:** The attacker $A$ outputs a forged signature $(\sigma_1^*, \sigma_2^*, \sigma_3^*, r^*)$ of the message $m_i$, then there exists an $i \in \{1, 2, \cdots, q\}$ that makes $CH(m_i, r_i) = CH(m^*, r^*)$. So $B$ computes $h^m y^{-i} = h^m y^i (mod q)$ and obtains $x = (m - m_i)(r_i - r^*)^i (mod q)$.

Therefore, the attacker $A$ solves an instance of discrete logarithm with a probability of at least $\varepsilon/2$.

If the second type holds, given the system parameter $cp$, a probabilistic polynomial time algorithm $C$ is constructed. $C$ forges a signature of our scheme under the adaptive chosen-message attacks. $C$ performs the following operations.

**Setup:** $C$ runs the Setup algorithm and sends the generated system parameter $cp$ to the attacker $A$, the private key $x$ is known to $C$, but $\alpha$ is unknown to $C$.

**Queries:** $C$ selects $q$, messages $m_i' \in Z_p^*$, $q$, random numbers $r_i' \in Z_p^*$ and computes $CH(m_i', r_i')$. $C$ also makes a query of our scheme for the signature $(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3})$ of $CH(m_i', r_i')$. When $A$ asks for the signature of message $m_i'$, $C$ first computes $r_i = (m_i' - m_i)x^{-i} + r_i'(mod q)$ such that $CH(m_i', r_i) = CH(m_i, r_i)$, and then returns the signature $(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, r_i)$ of $m_i'$ to $A$.

**Forgery:** The attacker $A$ outputs a forgery $(\sigma_1^*, \sigma_2^*, \sigma_3^*, r^*)$ of the message $m$ with a probability of $\varepsilon$, for any $i \in \{1, 2, \cdots, q\}$, satisfying $CH(m_i, r_i) = CH(m^*, r^*)$. This means that $C$ never asked $CH(m_i', r_i')$ from the signature oracle of our scheme. So $C$ obtains a message $CH(m^*, r^*)$ and the corresponding legal signature $(\sigma_1^*, \sigma_2^*, \sigma_3^*)$.

Therefore, $C$ successfully forges a signature of our scheme with a probability of at least $\varepsilon/2$.

### 4.3. Performance Analysis

We compare our scheme with the existing identity-based signature schemes in the standard model [3, 4, 7] from performance and security. The results are shown in Table 1, in which $n$, $|G_1|$, $|G_2|$ and $|Z_p^*|$ donate the bit length of a message, an element in $G_1$, $G_2$ and in $Z_p^*$, respectively. Also, we compare the number of exponential, multiplication and subtraction operations in the signature generation algorithms of these schemes.
Table 1. Performance comparison of signature generation algorithms

| Scheme           | Length | Exponentiation | Multiplication | Subtraction | Strong Unforgeability |
|------------------|--------|----------------|----------------|-------------|-----------------------|
| Li’s scheme [3]  | $2|G_1|+|G_2|$ | 2              | 1             | 0           | NO                    |
| Zhang’s scheme [4]| $3|G_1|$ | 3              | 0             | 0           | NO                    |
| Yang’s scheme [7]| $3|G_1|$ | 3              | n/2           | 0           | YES                   |
| Our scheme       | $3|G_1|+|Z^*_p|$ | 0              | 1             | 1           | YES                   |

From Table 1, we can see that in our proposed scheme, the signature algorithm only needs one modular subtraction operation and one modular multiplication operation. When the signature message arrives, the online signature of the message can be generated in a very short time. While, the computation of subtraction and multiplication is negligible relative to exponential operation. In addition, our scheme satisfies strong unforgeability. Therefore, the proposed scheme greatly improves the performance of the identity-based strong unforgeable signature scheme in the standard model.

5. Conclusions
In this paper, we propose an identity-based on-line/off-line signature scheme using chameleon hash function. It is proved that the new scheme is strongly unforgeable against adaptive chosen-message attacks. The performance of the scheme is compared with that of the several existing identity-based signature schemes in the standard model. The results show that the new scheme has higher signature efficiency and is suitable for environments with limited time or limited computing. The future work is to design identity-based on-line/off-line signature schemes with shorter signature length.

6. Acknowledgments
This work was partially supported by the National Natural Science Foundation of China (61662069), China Postdoctoral Science Foundation (2017M610817), Science and Technology Project of Lanzhou City of China (2013-4-22), Foundation for Excellent Young Teachers by Northwest Normal University (NWNU-LKQN-14-7).

7. References
[1] Shamir A. Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology. Springer Berlin Heidelberg, 1984:47-53.
[2] Ran C, Goldreich O, Halevi S. The random oracle methodology, revisited (preliminary version). Proc. ACM Symposium on Theory of Computing, 1998:209-218.
[3] Li J, Jiang P. An Efficient and Provably Secure Identity-based Signature Scheme in the Standard Model. Chinese Journal of Computer, 2009, 32(11):2130-2136.
[4] Zhang L, Hu Y, et al. Identity-based Provably Secure Signature Scheme in the Standard Model. Journal of Xidian University (Natural Science Edition), 2008, 33(1):1076-1079.
[5] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model. Australasian Conference on Information Security and Privacy. Springer Berlin Heidelberg, 2006:207-222.
[6] Boneh D, Shen E, Waters B. Strongly unforgeable signatures based on computational Diffie-Hellman. International Workshop on Public Key Cryptography. Springer Berlin Heidelberg, 2006:229-240.
[7] Yang X, Yang P, An F, et al. Cryptanalysis and Improvement of a Strongly Unforgeable Identity-Based Signature Scheme. 2017.
[8] Even S, Goldreich O, Micali S. On-line/off-line digital signatures. Journal of Cryptology, 1996, 9(1):35-67.
[9] Xiaofeng Chen, Fangguo Zhang, Willy Susilo, et al. Efficient Generic On-Line/Off-Line Signatures Without Key Exposure. Information Sciences, 2008, 178(21):4192-4203.
[10] Shamir A, Tauman Y. Improved Online/Offline Signature Schemes. *Advances in Cryptology-CRYPTO 2001. Springer Berlin Heidelberg*, 2001:355-367.