2009

Is the notion of divisible on-line/off-line signatures stronger than on-line/off-line signatures?

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Man Ho Allen Au
University of Wollongong, aau@uow.edu.au

Publication Details

Au, M., Susilo, W. & Mu, Y. (2009). Is the notion of divisible on-line/off-line signatures stronger than on-line/off-line signatures?. Lecture Notes in Computer Science, 5848 129-139.

Is the notion of divisible on-line/off-line signatures stronger than on-line/off-line signatures?

Abstract
On-line/Off-line signatures are useful in many applications where the signer has a very limited response time once the message is presented. The idea is to perform the signing process in two phases. The first phase is performed off-line before the message to be signed is available and the second phase is performed on-line after the message to be signed is provided. Recently, in CT-RSA 2009, Gao et al. made a very interesting observation that most of the existing schemes possess the following structure. In the off-line phase, a partial signature, called the off-line token is computed first. Upon completion of the on-line phase, the off-line token constitutes part of the full signature. They considered the "off-line token exposure problem" in which the off-line token is exposed in the off-line phase and introduced a new model to capture this scenario. While intuitively the new requirement appears to be a stronger notion, Gao et al. cannot discover a concrete attack on any of the existing schemes under the new model. They regard clarifying the relationship between the models as an open problem. In this paper, we provide an affirmative answer to this open problem. We construct an On-line/Offline signature scheme, which is secure under the ordinary security model whilst it is insecure in the new model. Specifically, we present a security proof under the old model and a concrete attack of the scheme under the new model. This illustrates that the new model is indeed stronger.

Keywords
notion, divisible, line, off, line, signatures, stronger, line, off, line, signatures

Disciplines
Physical Sciences and Mathematics

Publication Details
Au, M., Susilo, W. & Mu, Y. (2009). Is the notion of divisible on-line/off-line signatures stronger than on-line/off-line signatures?. Lecture Notes in Computer Science, 5848 129-139.

Is the Notion of Divisible On-line/Off-line Signatures Stronger than On-line/Off-line Signatures?*

Man Ho Au, Willy Susilo and Yi Mu

Center for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong, Australia
{aau,wsusilo,ymu}@uow.edu.au

Abstract. On-line/Off-line signatures are useful in many applications where the signer has a very limited response time once the message is presented. The idea is to perform the signing process in two phases. The first phase is performed *off-line* before the message to be signed is available and the second phase is performed *on-line* after the message to be signed is provided. Recently, in CT-RSA 2009, Gao *et al.* made a very interesting observation that most of the existing schemes possess the following structure. In the off-line phase, a partial signature, called the off-line token is computed first. Upon completion of the on-line phase, the off-line token constitutes part of the full signature. They considered the "off-line token exposure problem" in which the off-line token is exposed in the off-line phase and introduced a new model to capture this scenario. While intuitively the new requirement appears to be a stronger notion, Gao *et al.* cannot discover a concrete attack on any of the existing schemes under the new model. They regard clarifying the relationship between the models as an open problem. In this paper, we provide an affirmative answer to this open problem. We construct an On-line/Off-line signature scheme, which is secure under the ordinary security model whilst it is insecure in the new model. Specifically, we present a security proof under the old model and a concrete attack of the scheme under the new model. This illustrates that the new model is indeed stronger.

Keywords: on-line/off-line signatures, divisible on-line/off-line signatures, OS-EU-CMA, DOS-EU-CMA

1 Introduction

The notion on-line/off-line signatures (OS) was put forth by Even, Goldreich and Micali in 1990 [11]. Their main idea is to split the signature generation algorithm into two phases, namely, off-line phase and on-line phase. To achieve efficient signing when a message is presented, they utilized an off-line phase to handle the most costly computations. When a message is available, the on-line phase can then be performed efficiently in order to generate the required signature. Some of the signature schemes naturally fit into the framework of an on-line/off-line signature. The list includes the schemes from Fiat-Shamir (or any signature scheme obtained from Σ-Protocol using the Fiat-Shamir heuristics) [12], Schnorr [19], El-Gamal [13] and Boneh-Boyen [4].

Based on the work from Even, Goldreich and Micali, Shamir and Tauman [20] proposed an improved online/offline signature scheme utilizing the hash-sign-switch paradigm . The online signing phase of their scheme maintains the efficiency of Even *et al.*, while key size and signature size are largely reduced. Since then, many subsequent works have been done [15, 24, 16, 22, 23, 7, 9, 6].

1.1 Divisible of OS Schemes

Recently, in CT-RSA 2009, Gao *et al.* [26] made an interesting observation that most of the existing on-line/off-line signature schemes [13, 22, 23, 7, 16, 9, 6] share the following *divisibility* structure. A

* This work is supported by ARC Discovery Grant DP0877123.

partial signature, called an off-line token, is first computed in the off-line phase. The remaining part of the signature is generated in the on-line phase when the message is known. OS schemes satisfying this framework is said to be *divisible*.

Although the signature generation process is split into two stages, the transmission of the signature is a one-time process. The complete signature is sent to the recipient at the end of the on-line phase. Gao *et al.* studied an interesting problem: *can the off-line token be transmitted to the recipient prior to the on-line phase while maintaining the security of the OS scheme?* The significance of the question is that, the signer could send the signature in stages (during the off-line phase), possibly when the channel is less busy. This can make better utilization of the bandwidth. Another scenario is when the off-line tokens are unavoidably exposed to others (they referred this case as the "token exposure problem"), in case of on-line/off-line threshold signatures [9, 6].

Gao *et al.* studied this off-line token exposure problem and proposed a new security model to capture it. In this paper, we referred the new model as DOS-EU-CMA[1] to distinguish it from the traditional (or 'regular') model of OS-EU-CMA [11]. The standard notion of security for a signature scheme is existential unforgeability under chosen message attack (EU-CMA) [14]. Informally speaking, an attacker in this notion can request signatures on messages of its choice, possibly adaptively, before outputting a forged signature on any message, provided that it has not been given a signature on that message. Definition of DOS-EU-CMA and OS-EU-CMA shall be reviewed in Section 2.5. Looking ahead, it is fair to say the notion OS-EU-CMA closely follows the requirement of EU-CMA in which the OS is treated as an ordinary signature. Additionally, an attacker in DOS-EU-CMA is allowed to separate his query of signature into two phases. Specifically, the attacker is allowed to decide the querying message after receiving the off-line token.

Gao *et al.* presented a new scheme secure under their new model. They also analyzed several existing schemes and observed that some of them are secure under the new model as well. Furthermore, the security of the remaining schemes under their examination is less clear. While they are not able to derive security proof under the new model, they also cannot discover any concrete attack on these schemes. Hence, they left the problem of finding the potential gap between the model of DOS-EU-CMA and OS-EU-CMA as an open problem. Specifically, they questioned whether a scheme that is secure in OS-EU-CMA but it is not secure in DOS-EU-CMA can be constructed at all, as an open problem.

1.2 Our Contribution

In this paper, we provide an affirmative answer to the aforementioned open problem. Specifically, we construct an on-line/off-line signature
scheme[2] and prove its security under the model of OS-EU-CMA. Then, we present a concrete attack on our scheme under the model of DOS-EU-CMA. Consequently, our construction illustrates the gap between to two models. In summary, we provide an affirmative answer to the open problem raised by Gao *et al.* in [26] and show that the new model is indeed *stronger* than the traditional model. We would like to stress that the sole purpose of our construction is to demonstrate the theoretical gap between the models. Thus, efficiency is not of our concern and indeed our scheme is by no means practical compared with existing On-line/Off-line signatures.

1.3 Organization of The Paper

The rest of this paper is organized as follows. In Section 2, we review preliminaries including the models of OS-EU-CMA and DOS-EU-CMA. Next, we present our OS scheme, its security analysis under the model of OS-EU-CMA and an attack in the model of DOS-EU-CMA in Section 3. Finally, we conclude the paper in Section 4.

[1] The abbreviation DOS refers to divisible on-line/off-line signatures.

[2] We note that we are not concentrating on developing a practical or efficient scheme. Rather, we are interested to show a scheme that is secure under OS-EU-CMA but it is not secure under DOS-EU-CMA, and hence, it provides an answer to the open problem raised by Gao et al. [26].

	Secure under the traditional model?	Secure under the new model [26]?
[12, 13, 4, 20, 22, 7]	✓	?
[19, 9, 6, 26]	✓	✓
Our scheme	✓	×

Table 1. Summary of the separation between the traditional model and the new model

2 Preliminaries

2.1 Miscellaneous Notations

If S is a set, $|S|$ represents its cardinality. If S is a non-empty set and $a \in_R S$, then a is an element in S drawn uniformly at random from S. We denote by $\mathbb{Z}$ the set of integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ and by $\mathbb{Z}_p$ we denote the set $\{0, \ldots, p-1\}$.

We say that a function $\mathsf{negl}(k)$ is a negligible function [1], if for all polynomials $f(k)$, for all sufficiently large k, $\mathsf{negl}(k) < 1/f(k)$.

2.2 Bilinear Map

A pairing is a bilinear mapping from a pair of group elements to a group element. Specifically, let $\mathbb{G}_1, \mathbb{G}_T$ be cyclic groups of order p. Let g be a generator of $\mathbb{G}_1$. A function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$ is said to be a pairing if it satisfies the following properties:

- (Bilinearity.) $\hat{e}(u^x, v^y) = \hat{e}(u, v)^{xy}$ for all $u, v \in \mathbb{G}_1$ and $x, y \in \mathbb{Z}_p$.
- (Non-Degeneracy.) $\hat{e}(g, g) \neq 1_{\mathbb{G}_T}$, where $1_{\mathbb{G}_T}$ is the identity element of $\mathbb{G}_T$.
- (Efficient Computability.) $\hat{e}(u, v)$ can be computed efficiently (that is, in polynomial time) for all $u, v \in \mathbb{G}_1$.
- (Unique Representation.) All elements in $\mathbb{G}_1$ and $\mathbb{G}_T$ have unique binary representation.

2.3 Number-Theoretic Assumptions

Security of our proposed signature scheme is related to the hardness of the following problems.

The Discrete Logarithm Assumption The discrete logarithm problem (DLP) [5] forms the basis in the security of many cryptosystems.

Definition 1. *The Discrete Logarithm Problem in $\mathbb{G} = \langle g \rangle$ is defined as follows: On input a tuple $(g, Y) \in \mathbb{G}^2$, output x such that $Y = g^x$.*

Shoup [21] derived a lower bound on any algorithms that solve DLP without exploiting any special properties of the encoding of the group element. Such algorithms are known as generic algorithms. Specifically, the lower bound is $\Omega(\sqrt{d})$, where d is the largest prime dividing the order of the group. Indeed, such bound is met by the well-known Pollard's rho algorithm [18] that works in arbitrary groups. The discrete logarithm assumption stated that there is no PPT algorithm solves DLP with non-negligible probability.

Computational Diffie-Hellman Assumption If we can solve DLP in $\mathbb{G}$, we can also solve the computational Diffie-Hellman (CDH) [10] problem although whether the converse is true or not is still an open problem.

Definition 2. *The Computational Diffie-Hellman Problem in $\mathbb{G} = \langle g \rangle$ such that $|\mathbb{G}| = p$ is defined as follows: On input a tuple $(g, g^x, g^y) \in \mathbb{G}^3$, output g^{xy}.*

The CDH assumption states that no PPT solves CDHP with non-negligible probability.

The Pairing Pre-Image Assumption

Definition 3. *The Pairing Pre-Image Problem (PPIP) in* $\mathbb{G}_1, \mathbb{G}_T$ *such that* $\mathbb{G} = \langle g \rangle$, $|\mathbb{G}_1| = |\mathbb{G}_T| = p$ *with pairing* $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ *is defined as follows: On input a tuple* $(g, Z) \in \mathbb{G}_1 \times \mathbb{G}_T$, *output* $X \in \mathbb{G}_1$ *such that* $\hat{e}(X, g) = Z$.

This problem is often implicitly assumed to be hard in many cryptosystems employing bilinear maps. Indeed , it is straightforward to show PPIP is no harder than DLP in $\mathbb{G}_T$ and no easier than CDHP in $\mathbb{G}_1$.

Specifically, suppose DLP in $\mathbb{G}_T$ is easy. Given a PPIP instance (g, Z), compute x such that $Z = \hat{e}(g, g)^x$ by solving DLP in $\mathbb{G}_T$ of Z to base $\hat{e}(g, g)$. Output g^x as the solution to PPIP instance. On the other hand, assume PPIP is easy. Given a CDHP instance (g, g^a, g^b) in $\mathbb{G}_1$, compute X such that $\hat{e}(X, g) = \hat{e}(g^a, g^b)$ by solving PPIP with input $\big(g, \hat{e}(g^a, g^b)\big)$. Output X as the solution of the CDHP instance.

Thus, we have the following relationship between CDHP in $\mathbb{G}_1$, PPIP and DLP in $\mathbb{G}_T$.

$$\text{CDHP in } \mathbb{G}_1 <= \text{PPIP} <= \text{DLP in } \mathbb{G}_T$$

The PPI assumption states that no PPT solves PPIP with non-negligible probability.

2.4 On-line/Off-line Signatures

In the following, we review the syntax of an OS scheme.

Definition 4. *An OS scheme consists of four algorithms, namely,* KeyGen, OffSign, OnSign *and* Verify *for generating keys, signing in the online and offline phase, and verifying signatures, respectively.*

- $(pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda)$. *On input security parameter* 1^λ, *the key generation algorithm outputs a public/private key pair.*
- $(\Sigma^{\mathtt{off}}, St) \leftarrow \mathsf{OffSign}(sk)$. *On input the secret key, the off-line signing algorithm outputs an off-line token* $\Sigma^{\mathtt{off}}$ *and some state information* St.
- $(\Sigma^{\mathtt{on}}) \leftarrow \mathsf{OnSign}(sk, St, m)$. *On input the secret key, a state information* St *and a message, the on-line signing algorithm outputs an on-line token* $(\Sigma^{\mathtt{off}}, \Sigma^{\mathtt{on}})$. *The signature of* m *is defined as* $\sigma = (\Sigma^{\mathtt{off}}, \Sigma^{\mathtt{on}}))$.
- $0/1 \leftarrow \mathsf{Verify}(pk, m, \sigma)$. *On input a public key, a message and a signature, the verification algorithms output* 1 *if the signature is valid and* 0 *otherwise.*

As mentioned by Gao *et al.*, every OS scheme is trivially *divisible* under their definition by setting $\Sigma^{\mathtt{off}}$ as *null*[3]. Those schemes are called trivially divisible. Throughout this paper, we are interested in OS scheme that is non-trivially *divisible*, that is, $\Sigma^{\mathtt{off}}$ is not *null*.

2.5 Security Requirements

The standard notion of security for an OS scheme is existential unforgeability under chosen message attack (OS-EU-CMA) [14], which can be defined formally by the following game between a challenger $\mathcal{C}$ and a PPT adversary $\mathcal{A}$.

Definition 5 (Game OS-EU-CMA).

Setup: A challenger $\mathcal{C}$ *runs algorithm* KeyGen *to obtain a public key* pk *and a private key* sk. $\mathcal{C}$ *gives* pk *to* $\mathcal{A}$.

Queries: For the i*-th query,* $\mathcal{A}$ *requests a signature on message* m_i. $\mathcal{C}$ *responses by computing* $(\Sigma_i^{\mathtt{off}}, St_i) \leftarrow \mathsf{OffSign}(sk)$ *followed by* $\Sigma_i^{\mathtt{on}} \leftarrow \mathsf{OnSign}(sk,\ St_i,\ m_i)$. $\sigma_i = (\Sigma_i^{\mathtt{off}}, \Sigma_i^{\mathtt{on}})$ *is returned to* $\mathcal{A}$.

[3] Or more generally, any dummy offline token.

Output: $\mathcal{A}$ *outputs a pair* (m^*, σ^*). $\mathcal{A}$ *wins the game if* $m^* \notin \{m_1, \ldots, m_q\}$ *and* $1 \leftarrow \mathsf{Verify}(pk, m^*, \sigma^*)$.

An OS scheme is OS-EU-CMA secure if no PPT adversary can win in Game OS-EU-CMA with non-negligible probability.

In the following, we will review the new model proposed by Gao *et al.*. Looking ahead, the major difference between the two notions is that attacker in the new model is allowed to adaptively choose the query messages based on the off-line token. This is to capture the off-line token exposure problem. Specifically, the following game between a challenger $\mathcal{C}$ and a PPT adversary $\mathcal{A}$ formally defines the security requirement for a divisible on-line/off-line (DOS) scheme, as defined by Gao *et al.*

Definition 6 (Game DOS-EU-CMA).

Setup: $\mathcal{A}$ *challenger* $\mathcal{C}$ *runs algorithm* KeyGen *to obtain a public key* pk *and a private key* sk. $\mathcal{C}$ *gives* pk *to* $\mathcal{A}$.

Off-Sign Queries: For the i*-th query,* $\mathcal{A}$ *requests an off-line token.* $\mathcal{C}$ *responses by computing* $(\Sigma_i^{\mathtt{off}}, St_i) \leftarrow \mathsf{OffSign}(sk)$. $\Sigma_i^{\mathtt{off}}$ *is given to* $\mathcal{A}$ *while* $(\Sigma_i^{\mathtt{off}}, St_i)$ *is stored in set* $\mathcal{U}$.

On-Sign Queries: $\mathcal{A}$ *submits a message* m_i *and an off-line token* $\Sigma_i^{\mathtt{off}}$ *such that there exists an entry* $(\Sigma_i^{\mathtt{off}}, St_i) \in \mathcal{U}$. $\mathcal{C}$ *computes* $\Sigma_i^{\mathtt{on}} \leftarrow \mathsf{OnSign}(sk, St_i, m_i)$. $\Sigma_i^{\mathtt{on}}$ *is returned to* $\mathcal{A}$ *and* $(\Sigma_i^{\mathtt{off}}, St_i)$ *is removed from* $\mathcal{U}$.

Output: $\mathcal{A}$ *outputs a pair* (m^*, σ^*). $\mathcal{A}$ *wins the game if* $m^* \notin \{m_1, \ldots, m_q\}$ *and* $1 \leftarrow \mathsf{Verify}(pk, m^*, \sigma^*)$.

An OS scheme is DOS-EU-CMA secure if no PPT adversary can win in Game DOS-EU-CMA with non-negligible probability.

2.6 Relationship of OS-EU-CMA and DOS-EU-CMA

DOS-EU-CMA is at least no weaker than OS-EU-CMA as a security notion. However, it is unclear whether there is a separation between the two. Gao *et al.* [26] analyzed a number of existing schemes and proved that several of which are in fact DOS-EU-CMA, as shown in Table 2. Of the remaining schemes that cannot be proven secure in the new model, they are not able to devise any concrete attack. The following table is obtained from their results in [26]. The symbol "?" indicates that it cannot be proven secure under the security notion while no explicit attack can be found either. The word "Sig" in the assumption represents the security also depends on the security of the underlying standard signature scheme. For the introduction to the q-SDH assumption and the one-more discrete log assumption, we refer the readers to [3, 8] and [2], respectively.

	OS-EU-CMA?	DOS-EU-CMA?	Assumption
Fiat-Shamir [12]	✓	?	
El-Gamal [13]	✓	?	
DSS [17]	✓	?	
Boneh-Boyen [4]	✓	?	
Shamir-Tauman (generic) [20]	✓	?	
Xu *et al.* [22]	✓	?	
Chen *et al.* (generic) [7]	✓	?	
Schnorr-OS [19]	✓	✓	one-more-discrete log
Crutchfield *et al.* (generic) [9]	✓	✓	Sig + one-more-discrete log
Bresson *et al.* (generic) [6]	✓	✓	Sig + discrete log
Gao *et al.* [26]	✓	✓	q-SDH

Table 2. Summary of existing OS schemes

3 Our Result

3.1 An On-line/Off-line Signature

In this section, we present our OS construction. We note that the goal of our construction is to demonstrate the gap between the security notions of OS-EU-CMA and DOS-EU-CMA and thus efficiency is not of prime concern.

KeyGen. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ be a bilinear map. Note that $|\mathbb{G}_1| = |\mathbb{G}_T| = p$ for some prime p. Let g be a generator of $\mathbb{G}_1$. Let $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$ be a collision-resistant hash function. Let $X \in_R \mathbb{G}_1$ and $Z = \hat{e}(X, g)$. The secret key sk is (X) while the public key pk is $(\hat{e}, \mathbb{G}_1, \mathbb{G}_T, p, g, Z, H)$. The message space $\mathcal{M}$ is $\mathbb{G}_1$.

OffSign. Randomly generate $R \in \mathbb{G}_1$, $s \in_R \mathbb{Z}_p^*$, output $(\Sigma^{\mathtt{off}}, St)$ as (R, s).

OnSign. On input $M \in \mathbb{G}_1$, $(\Sigma^{\mathtt{off}}, St) = (R, s)$, compute $\varsigma = X(R/M)^s$. Further, generate $r \in_R \mathbb{Z}_p$, compute $T = \hat{e}(\frac{R}{M}, g)^r$, $c = H(T||R||\varsigma||M)$ and $z = r - cs$. Output $\Sigma^{\mathtt{on}}$ as (ς, c, z).

Verify. Given a public key $(\hat{e}, \mathbb{G}_1, \mathbb{G}_T, p, g, Z, H)$, a message $M \in \mathbb{G}_1$, a signature $\sigma = (\Sigma^{\mathtt{off}}, \Sigma^{\mathtt{on}}) = \big(R, (\varsigma, c, z)\big)$, verify that $c = H\big((\hat{e}(\varsigma, g)Z^{-1})^c \hat{e}(\frac{R}{M}, g)^z || R || \varsigma || M\big)$. If the equality holds, output 1. Otherwise, output 0.

Correctness of the scheme is straightforward. Note that

$$\begin{aligned}
\big(\hat{e}(\varsigma, g)Z^{-1}\big)^c \hat{e}(\frac{R}{M}, g)^z &= \big(\hat{e}(X(\frac{R}{M})^s, g)\hat{e}(X, g)^{-1}\big)^c \hat{e}(\frac{R}{M}, g)^z \\
&= \big(\hat{e}(X, g)\hat{e}(X, g)^{-1}\hat{e}((\frac{R}{M})^s, g)\big)^c \hat{e}(\frac{R}{M}, g)^z \\
&= \hat{e}(\frac{R}{M}, g)^{cs}\hat{e}(\frac{R}{M}, g)^z \\
&= \hat{e}(\frac{R}{M}, g)^r \\
&= T
\end{aligned}$$

□

3.2 Security Analysis

We prove that our construction is a secure OS scheme by reduction. Suppose there is a forger $\mathcal{A}$ that wins in Game OS-EU-CMA with probability ϵ, we construct a simulator $\mathcal{S}$, having black-box access to $\mathcal{A}$, that solves the pairing pre-image problem in the random oracle model with success probability $\frac{\epsilon}{q_H^2}$, assuming $\mathcal{A}$ makes q_H queries to the hash oracle.

Proof. $\mathcal{S}$ is given a problem instance $(\hat{e}, \mathbb{G}_1, \mathbb{G}_T, p, g, Z)$ where g is a generator of $\mathbb{G}_1$ with prime order p, its task is to compute X such that $\hat{e}(X, g) = Z$.

Setting up the public key. $\mathcal{S}$ sets the public key pk of the signer as $(\hat{e}, \mathbb{G}_1, \mathbb{G}_T, p, g, Z)$. In the random oracle model, $\mathcal{S}$ also gets control over Hash function H. pk is given to the adversary $\mathcal{A}$.

Simulating the Oracles. For the i-th query, $\mathcal{A}$ requests a signature on message $m_i \in \mathbb{G}_1$. $\mathcal{S}$ responses by randomly generates $R, \varsigma \in_R \mathbb{G}_1$, $c, z \in_R \mathbb{Z}_p$, computes $T = (\hat{e}(\varsigma, g)Z^{-1})^c \hat{e}(\frac{R}{m_i}, g)^z$ and backpatch the output of the random oracle $H(T||R||\varsigma||m_i)$ as c. Returns $\sigma_i = (R, \varsigma, c, z)$ to $\mathcal{A}$.

Hash Queries. $\mathcal{S}$ randomly chooses one of the q_H hash queries with input $T^*||R^*||\varsigma^*||M^*$ and fork the adversary. The two copies of the adversary receives the hash output as c^* and c' such that $c^* \neq c'$ respectively.

The Forgery and Reduction. Finally, the two copies of $\mathcal{A}$ output two forged signatures. With probability at least $\frac{1}{q_H^2}$ the two forged signatures are $(R^*,\ \varsigma^*,\ c^*,\ z^*)$ on message M^* such that $c^* = H\big((\hat{e}(\varsigma,\ g)Z^{-1})^{c^*}\ \hat{e}(\frac{R^*}{M^*},\ g)^{z^*}\ ||\ R^*\ ||\ \varsigma^*\ ||\ M^*\big)$ and $(R^*, \varsigma^*, c', z')$ on the same message M^* such that $\big(\hat{e}(\varsigma^*, g)Z^{-1}\big)^{c^*}\hat{e}(\frac{R^*}{M^*}, g)^{z^*} = \big(\hat{e}(\varsigma^*, g)Z^{-1}\big)^{c'}\hat{e}(\frac{R^*}{M^*}, g)^{z'}$.

$\mathcal{S}$ computes X as $\varsigma(\frac{R^*}{M^*})^{\frac{z'-z^*}{c'-c^*}}$. Indeed,

$$\begin{aligned}
\big(\hat{e}(\varsigma^*, g)Z^{-1}\big)^{c^*}\hat{e}(\frac{R^*}{M^*}, g)^{z^*} &= \big(\hat{e}(\varsigma^*, g)Z^{-1}\big)^{c'}\hat{e}(\frac{R^*}{M^*}, g)^{z'} \\
\big(\hat{e}(\varsigma^*, g)Z^{-1}\big)^{c^*-c'} &= \hat{e}(\frac{R^*}{M^*}, g)^{z'-z^*} \\
Z^{c'-c^*} &= \hat{e}(\frac{R^*}{M^*}, g)^{z'-z^*}\hat{e}(\varsigma^*, g)^{c'-c^*} \\
\hat{e}(X, g)^{c'-c^*} &= \hat{e}((\frac{R^*}{M^*})^{z'-z^*}\varsigma^{c'-c^*}, g) \\
\hat{e}(X, g) &= \hat{e}\big((\frac{R^*}{M^*})^{\frac{z'-z^*}{c'-c^*}}\varsigma, g\big) \\
X &= \varsigma(\frac{R^*}{M^*})^{\frac{z'-z^*}{c'-c^*}}
\end{aligned}$$

Consequently, the success probability of $\mathcal{S}$ is at least $\frac{\epsilon}{q_H^2}$. □

3.3 An Attack of Our OS under Definition 6 (DOS-EU-CMA)

While our scheme is OS-EU-CMA secure, there is an attack under Definition 6 (DOS-EU-CMA), i.e. the new model proposed by Gao *et al.* Specifically, the attacker first obtains an off-line token R. Upon receiving R, the attacker chooses the message to query as $M = R$. ς in the corresponding signature $\big(R, (\varsigma, c, z)\big)$ will have the form of X since $\varsigma = X(\frac{R}{M})^r$. Thus, the scheme is totally broken with the secret key revealed when the attacker can choose the message after knowing the off-line token.

The weakness of the scheme under Definition 6 is obvious: it is insecure when the off-line token R is equal to the message M to be signed. This, however, will happen with negligible probability when R is hidden from the attacker before message M to be signed is presented and thus the scheme is still secure under Definition 5. This clearly illustrates that DOS-EU-CMA is a stronger security notion compared with OS-EU-CMA.

4 Conclusion

We presented a new OS scheme and proved that it is secure under the traditional model of on-line/off-line signatures (OS-EU-CMA). Next, we presented a concrete attack of our scheme under the newly-proposed model by Gao *et al.* [26], DOS-EU-CMA. This scheme exemplifies a case that the model in [26] is indeed stronger than the traditional one. Hence, it provides an affirmative answer to to the open problem in [26].

References

1. M. Bellare. A Note on Negligible Functions. *Journal of Cryptology*, 15(4):271–284, 2002.
2. M. Bellare and A. Palacio. Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In M. Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 162–177. Springer, 2002.
3. D. Boneh and X. Boyen. Short Signatures without Random Oracles. In C. Cachin and J. Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 2004.

4. D. Boneh and X. Boyen. Short signatures without random oracles and the sdh assumption in bilinear groups. *Journal of Cryptology*, 21(2):149–177, 2008.
5. D. Boneh and R. J. Lipton. Algorithms for Black-Box Fields and their Application to Cryptography (Extended Abstract). In N. Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*, pages 283–297. Springer, 1996.
6. E. Bresson, D. Catalano, and R. Gennaro. Improved on-line/off-line threshold signatures. In T. Okamoto and X. Wang, editors, *Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, April 16-20, 2007, Proceedings*, volume 4450 of *Lecture Notes in Computer Science*, pages 217–232. Springer, 2007.
7. X. Chen, F. Zhang, W. Susilo, and Y. Mu. Efficient generic on-line/off-line signatures without key exposure. In J. Katz and M. Yung, editors, *Applied Cryptography and Network Security, 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007, Proceedings*, volume 4521 of *Lecture Notes in Computer Science*, pages 18–30. Springer, 2007.
8. J. H. Cheon. Security Analysis of the Strong Diffie-Hellman Problem. In S. Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 1–11. Springer, 2006.
9. C. Crutchfield, D. Molnar, D. Turner, and D. Wagner. Generic on-line/off-line threshold signatures. In Yung et al. [25], pages 58–74.
10. W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
11. S. Even, O. Goldreich, and S. Micali. On-line/off-line digital schemes. In G. Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 263–275. Springer, 1989.
12. A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In A. M. Odlyzko, editor, *CRYPTO 1986*, volume 263 of *LNCS*, pages 186–194. Springer, 1986.
13. T. E. Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.
14. S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.*, 17(2):281–308, 1988.
15. F. Guo and Y. Mu. Optimal online/offline signature: How to sign a message without online computation. In J. Baek, F. Bao, K. Chen, and X. Lai, editors, *Provable Security, Second International Conference, ProvSec 2008, Shanghai, China, October 30 - November 1, 2008. Proceedings*, volume 5324 of *Lecture Notes in Computer Science*, pages 98–111. Springer, 2008.
16. K. Kurosawa and K. Schmidt-Samoa. New online/offline signature schemes without random oracles. In Yung et al. [25], pages 330–346.
17. N. I. of Standards and T. (NIST). The digital signature standard, 186. *Federal Information Processing Standards Publication (FIPS PUB)*, 1994.
18. J. M. Pollard. Monte Carlo Methods for Index Computation (mod p). *Mathematics of Computation*, 32(143):918–924, 1978.
19. C.-P. Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, 4(3):161–174, 1991.
20. A. Shamir and Y. Tauman. Improved online/offline signature schemes. In J. Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 355–367. Springer, 2001.
21. V. Shoup. Lower bounds for discrete logarithms and related problems. In W. Fumy, editor, *Advances in Cryptology - EUROCRYPT 1997, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer, 1997.
22. S. Xu, Y. Mu, and W. Susilo. Online/offline signatures and multisignatures for aodv and dsr routing security. In L. M. Batten and R. Safavi-Naini, editors, *Information Security and Privacy, 11th Australasian Conference, ACISP 2006, Melbourne, Australia, July 3-5, 2006, Proceedings*, volume 4058 of *Lecture Notes in Computer Science*, pages 99–110. Springer, 2006.
23. P. Yu and S. R. Tate. An online/offline signature scheme based on the strong rsa assumption. In *AINAW '07: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, pages 601–606, Washington, DC, USA, 2007. IEEE Computer Society.

24. P. Yu and S. R. Tate. Online/offline signature schemes for devices with limited computing capabilities. In T. Malkin, editor, *Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008, San Francisco, CA, USA, April 8-11, 2008. Proceedings*, volume 4964 of *Lecture Notes in Computer Science*, pages 301–317. Springer, 2008.
25. M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors. *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings*, volume 3958 of *Lecture Notes in Computer Science*. Springer, 2006.
26. C. zhi Gao, B. Wei, D. Xie, and C. Tang. Divisible on-line/off-line signatures. In M. Fischlin, editor, *Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings*, volume 5473 of *Lecture Notes in Computer Science*, pages 148–163. Springer, 2009.