Remark on Yu et al.’s Online/Offline signature scheme in CT-RSA 2008

Ma Xiao-Long, Wang Zhi-Wei, Gu Li-Ze, Yang Yi-xian
Information Security Center, State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications, Beijing, China
{balicmxl@yahoo.com, zhiweiWang@163.com, glz_bupt@263.net, yyx@bupt.edu.cn}

Abstract—In CT-RSA 2008, Yu et al. proposed a family of three efficient Online/Offline signature schemes, which are especially suitable for the devices with limited computing capabilities. In this paper, we propose a new security model of Online/Offline signature. We find that Yu et al.’ basic scheme is insecure under our model. We repair Yu et al.’s loophole by proposing a modified scheme.

Keywords—Online/offline signature, Security mode, Devices with limited computing capabilities

I. INTRODUCTION

The notion of Online/Offline signature was first introduced by Even, Goldreich and Micali[1], and the idea is to perform the signature generation in two phases. The first phase is performed offline, after the message to be signed becomes available. The computational cost in online phase is usually very low. In CT-RSA 2008, Yu et al. proposed a family of three efficient Online/Offline signature schemes (OOSIG1, OOSIG2 and OOSIG3)[2] based on strong RSA assumption [3,4], in which OOSIG1 is the basic scheme. Since the computational cost of the online phase is very low, Yu et al believe that their schemes are very suitable for the devices with limited computing capabilities.

The notion of Online/Offline signature was first introduced by Even, Goldreich and Micali[1], and the idea is to perform the signature generation in two phases. The first phase is performed offline, after the message to be signed becomes available. The computational cost in online phase is usually very low. In CT-RSA 2008, Yu et al. proposed a family of three efficient Online/Offline signature schemes (OOSIG1, OOSIG2 and OOSIG3)[2] based on strong RSA assumption [3,4], in which OOSIG1 is the basic scheme. Since the computational cost of the online phase is very low, Yu et al believe that their schemes are very suitable for the devices with limited computing capabilities.

The rest of the paper is organized as follows. In Section 2, we review the OOSIG1 scheme. In Section 3, we depict our new security model of Online/Offline signature. In Section 4, we analyze the OOSIG1 scheme. In Section 5, we propose a modified scheme, and in Section 6, the conclusion is given.

II. REVIEW OF YU ET AL.’S BASIC SCHEME (OOSIG1)

Online/Offline signature is defined to be a 4-tuple of algorithms, namely, ParamGen, KeyGen, Sign and Verify. S-offline denotes the sub-algorithm for the offline phase of Sign algorithm and S-online denotes the sub-algorithm for the online phase of Sign algorithm. In OOSIG1, these algorithms are constructed as follows:

ParamGen: Let \( k \) be the security parameter, then defines some parameters as follows: \( l_m \) is the length of the message to be signed. \( l \) is a security parameter that controls the statistical closeness of distributions, and should be polynomial in \( k \). \( l_m \geq l_m + 2 \) is the length of an exponent in the signature algorithm. \( l_2 = 2k \) is the length of the public modulus. \( l = l_m + l + 1 \) is the length of another exponent used in the signing algorithm. Finally, outputs the system parameter \( \text{param}= (k, l_m, l, l_m, l_1) \).

KeyGen: On input \( l_i \), selects two \( k \)-bit safe primes \( p = 2^p + 1 \) and \( q = 2q + 1 \), where \( p \) and \( q \) are also primes. Compute \( n = pq \), and pick a random generator of \( QR_n \) (Quadratic Residue Group). Then select \( \alpha, \beta \in [0, p'q') \) and compute \( a = b^\alpha \mod n \) and \( c = b^\beta \mod n \). Let \( K = [2^i/p'q'] \). Output the public key \( PK= (n, a, b, c) \) and the private key \( SK = (p'q', \alpha, \beta, K) \).

The signing algorithm is composed by offline phase (S-offline) and online phase (S-online).

S-offline: The signer selects a random \( r \in [0, p'q') \), a random \( l_m \)-bit prime number \( e \), and a random \( k \in [0, K) \), and then computes:

\[
\begin{align*}
& v = b^r \mod n, \\
& \lambda = kp'q' + ye - \beta \mod Kp'q' \\
& V_{\text{offline}} = (v, \lambda, e, \gamma, k)
\end{align*}
\]

\( V_{\text{offline}} \) should be kept for the signer himself.

S-online: The signer computes:

\[
s = \lambda - \alpha m \mod Kp'q'
\]

Outputs the signature \( \sigma = (v, e, s) \) on the message \( m \).

Verify: Given a signature \( \sigma = (v, e, s) \) on the message \( m \), a verifier first checks that \( e \)'s length is \( l_m \), and then checks whether \( v' = a^\alpha b^e c \mod n \) holds or not. If holds, output “valid”, otherwise, output “invalid”.

978-0-7695-3744-3/09 $25.00 © 2009 IEEE
DOI 10.1109/IAS.2009.318
III. NEW SECURITY MODEL OF ONLINE/OFFLINE SIGNATURE

Our new security model of Online/Offline signature can be defined by using the following game between a challenger C and an adversary A.

Setup: The challenger C runs the algorithm ParamGen, KeyGen to obtain param, PK and SK. The adversary A is given param and PK. Then, the challenger C runs the S-offline algorithm to get V_{offline}, and keeps it for himself.

Queries: The adversary A only needs to make S-online Queries. Proceeding adaptively, A can make at most q_{s-online} S-online queries. For each S-online query m_i \in \{m_1, \cdots, m_{q_{s-online}}\}, the challenger C returns \sigma_i as response by running S-online algorithm.

Output: The adversary A will output a pair \((m^*, \sigma^*)\), and wins the game if:
1. \(m^* \notin \{m_1, \cdots, m_{q_{s-online}}\}\); and
2. Verify(param, \(m^*, \sigma^*, PK\)) = Valid.

We define \(ADV'_A\) to be the probability that A wins in the above game. We say an Online/Offline signature scheme is secure if \(ADV'_A\) is negligible.

IV. ANALYSIS OF OOSIG1

The following shows how the adversary A in our security model can break OOSIG1:

1. The adversary A issues \(q_{s-online}\) S-online queries on \(\{m_1, \cdots, m_{q_{s-online}}\}\). For each S-online query, the challenger C returns \(\sigma_i\) as response by running the S-online algorithm.
2. Eventually, A outputs a forged signature \(\sigma^* = (v, e, s^* = s_k - (s_i - s_j))\) on \(m^* = m_k + m_j - m_i (i, j, k \in \{1, \cdots, q_{s-online}\})\). Checks that \(m^* \notin \{m_1, \cdots, m_{q_{s-online}}\}\) (this probability is non-negligible), and Verify(param, \(m^*, \sigma^*, PK\)) = Valid must hold. So A can win the game with non-negligible probability.

Note that: Since
\[
s^* = s_k - (s_i - s_j) = \gamma e - \beta - \alpha (m_i + m_j - m_k)
\]
\[
= \gamma e - \beta - \alpha m^*, \quad \text{then } v^* = a^w b^c \mod n \text{ must hold.}
\]
Thus, it is clear that OOSIG1 is insecure under our model. We also can find that OOSIG2 and OOSIG3 are both insecure by the similar idea.

V. A MODIFIED SCHEME BASED ON OOSIG1

This will enable us to maintain uniformity in the conference proceedings as well as in the post-conference luxurious books by WSES Press.

In this section, we depict our modified scheme as follows:

ParamGen: This algorithm is the same as OOSIG1.

KeyGen: This algorithm is also the same as OOSIG1.

Sign: This algorithm is small modified.

S-offline: The signer selects a random \(\gamma \in \mathbb{Z}_p [0, p' q')\), a random \(l\)-bit prime number e, and a random \(k^i \in \mathbb{Z} [0, K]\), and then computes:
\[
v = b' \mod n, \lambda = kp' q' + \gamma e - \beta \mod Kp' q'.
\]
\[
V_{offline} = (v, \lambda, e, \gamma, k) \text{ should be kept for the signer himself.}
\]

S-online: The signer computes
\[
s = \lambda - \alpha m^2 \mod Kp' q'
\]
for the message \(m \in [0, 2^l\)\). Outputs the signature \(\sigma = (v, e, s)\) on the message m.

Verify: Given a signature \(\sigma = (v, e, s)\) on the message m, a verifier first checks that e’s length is \(l_1\), and then checks whether \(v^* = (a^w b^c \mod n)\) holds or not. If holds, output ”valid”, otherwise, output ”invalid”.

Remark: Since \(s = \lambda - \alpha m^2 \mod Kp' q'\), then our modified scheme can resist the attack in Section 4. Moreover, compared with the original scheme, the online phase of our scheme needs only one more multiplication. Thus, it is also very efficient.

VI. CONCLUSION

In this paper, we propose a new security model of Online/Offline signature. We find that Yu et al’s basic scheme is not secure under our model, and we present a modified scheme.

REFERENCES