Abstract—In 2002, Wu and Hsu proposed two new ID-based multisignature schemes that are suitable for the sequential and the broadcasting architectures, respectively. They claimed that these two schemes cannot be broken due to the difficulty of factorization. In this paper, we prove that the Wu-Hsu multisignature schemes can be broken by Euclidean algorithm with known signature attack.

Keywords—multisignature; distinguished signing authorities; Euclidean algorithm;

I. INTRODUCTION

In 2002, Wu and Hsu proposed two new ID-based multisignature schemes with distinguished signing authorities [1]. One scheme is suitable for the sequential architecture and the other is suitable for the broadcasting architecture. For the sequential architecture, the issuer initiates the whole document and defines the signing order. Each group member signs the partial content he is responsible for in predefined order. The multisignature is completed after the last signer finished his signing process. For the broadcasting architecture, the issuer initiates the whole document and broadcasts it to all signers. Each participant signer independently signs the partial content he is responsible for and then broadcasts and transmits his partial signature to the collector. After receiving all the partial signatures, the collector can produce the multisignature with respect to all participant signers.

In this paper, we present a known signature attack on the above two multisignature schemes for the sequential and broadcasting architectures. An attacker can efficiently obtain each signer’s private key and produce a valid group signature for any message by using our analysis. In other words, the Wu-Hsu multisignature schemes are insecure.

II. REVIEW OF WU-HSU’S MULTISIGNATURE SCHEMES

In this section, we briefly review the related multisignature schemes for the sequential and broadcasting architecture. Each scheme consists of three phases: the initialization phase, the multisignature generation phase and multisignature verification phase. The initialization and multisignature verification phases are the same in both schemes. Each scheme for different architecture has its own multisignature generation phase.

1) Initialization phase

In both schemes, the system generates two primes \( p_1 \) and \( p_2 \) of about 100 digits such that \( p_1 = \pm 1 \pmod{8} \) and \( p_2 = \pm 3 \pmod{8} \), where \( (p_1-1)/2 \) and \( (p_2-1)/2 \) are relatively prime [3]. The system publishes four public parameters \( N \), \( g \), \( h(\cdot) \) and \( e \), where \( N \) is equal to \( p_1 \times p_2 \) and the Jacobi symbol \( \left( \frac{N}{p_1} \right) \) is \(-1\). \( g \) is primitive in both \( \mathbb{GF}(p_1) \) and \( \mathbb{GF}(p_2) \), \( h(\cdot) \) is a one-way hash function, and \( e \) and \( d \) in \( \mathbb{ZL}^* \) are used as the system’s public and secret keys such that \( e \times d = 1 \pmod{L} \), where \( L = \text{lcm}(p_1-1,p_2-1) \). Each signer \( U_i \), \( i = 1, 2, \cdots, n \), whose identity information is \( D_i \), holds a secret key \( S_i \) such that

\[
g^{-S_i} = ID_i \pmod{N}, \text{ where } ID_i = \begin{cases} \text{D}_i \pmod{N} & \text{if } \left( \frac{D_i}{N} \right) = 1 \\ 2D_i \pmod{N} & \text{if } \left( \frac{D_i}{N} \right) = -1 \end{cases}
\]

2) Multisignature generation phase

a) The sequential structure: Assume that there are \( n \) signers in this predefined order, \( U_1, U_2, \cdots, U_n \), who want to sign \( m_1, m_2, \cdots, m_n \), respectively. The document issuer sends \( \{m, SG_0 = 1\} \) to the first signer \( U_1 \). After receiving \( \{m, SG_{i-1}\} \), \( U_i \) executes the following steps:

i) Signer \( U_i \), \( i = 2, 3, \cdots, n \) checks the following equality:

\[
(SG_{i-1})^e \cdot \prod_{j=1}^{i-1} ID_j^{h(m_j)} = 1 \pmod{N} \quad (1)
\]

If the above equation holds, the partial multisignature \( SG_{i-1} \) generated by the preceding signers is valid. It can continue to the next steps. Otherwise, it needs to stop the procedure and make an announcement.

ii) Each signer \( U_i \), \( i = 1, 2, \cdots, n \) signs the partial documents \( m_i \) which he is responsible for:

\[
M_i = g^{S_i \cdot h(m_i)} \pmod{N} \quad (2)
\]

\[
SG_i = SG_{i-1} \cdot M_i \pmod{N} \quad (3)
\]
iii) Signer \( U_i, \ i = 1, 2, \cdots, n - 1 \), sends \( \{m, SG_{i-1}\} \) to the next signer \( U_{i+1} \). If the last signer \( U_n \) completes Step 1 and Step 2, the multisignature \( SG_n \) for \( m \) is then sent to the verifier. Note that Eq. 3 can be rewritten as
\[
SG = \prod_{j=1}^{n} M_j \mod N \quad (4)
\]

b) The broadcasting structure: The document issuer broadcasts \( m \) to all the signers \( U_1, U_2, \cdots, U_n \). Each signer \( U_i \) computes \( M_i \) by Eq. 2, and then delivers \( \{m, M_i\} \) to \( U_c \). \( U_c \) can check the validity of each individual partial signature \( M_i \) by the following equation:
\[
M_i^a \cdot ID_i^{h(m_i)} \equiv 1 \pmod{N} \quad (5)
\]

Once all the individual signatures have been received and verified, \( U_c \) computes the multisignature \( SG \) as
\[
SG = \prod_{j=1}^{n} M_j \mod N \quad (6)
\]

After that, \( U_c \) sends \( \{m, SG\} \) to the verifier.

3) Multisignature verification phase
The multisignature \( SG \) is verified by
\[
SG^a \cdot \left( \prod_{j=1}^{n} I D_i^{h(m_i)} \right) \equiv 1 \pmod{N} \quad (7)
\]

If it holds, \( SG \) is regarded as a valid multisignature for \( m \) with respect to the group \( G \).

III. THE PROPOSED KNOWN SIGNATURE ATTACK

The security issues are considered for above two schemes in the following:

1) It is difficult to deduce the system’s parameters and signer’s secret key from the public information.

2) It is difficult to deduce the signer’s secret key from partial multisignature(s).

3) It is difficult to forge a multisignature for any sets of signers without knowing their secret keys.

The security of above two schemes is mainly based on the difficulty of factorization. In this section, we propose a known signature attack on above two multisignature schemes. The signer’s secret key can be deduced without solving the problem of factorization by choosing two known signer’s valid partial signature and solving the Euclidean algorithm. Then, the attacker can forge any valid multisignature \( SG^{m''} \) for any message \( m'' \).

In this attack, it is assumed that the attacker can obtain two known valid partial signature \( M_i \) and \( M_i' \) for \( h(m_i) \) and \( h(m_i') \) in Eq. 2, and also assumed that \( h(m_i) \) and \( h(m_i') \) are relatively prime in high chances. For the sake of convenience, we define \( g_i = g^{m_i} \pmod{N} \). The known signature attack is performed below:

1) By the Euclidean algorithm, the attacker can solve two integers, \( a \) and \( b \), to satisfy the equation: \( ah(m_i) + bh(m_i') = 1 \).

2) \( g_i \) can be obtained by the following equation:
\[
M_i^a \cdot M_i'^b \equiv \left( g_i^{S_i h(m_i)} \right)^a \cdot \left( g_i^{S_i'h(m_i')} \right)^b \pmod{N}
\]
\[
= g_i^{ah(m_i)} \cdot g_i^{bh(m_i')} \pmod{N}
\]
\[
= g_i^{ah(m_i)+bh(m_i')} \pmod{N}
\]
\[
= g_i \pmod{N}
\]

3) The attacker can forge any partial signature \( M_i'' \) for any partial message \( m_i'' \):
\[
M_i'' = g_i^{h(m_i'')} = g_i^{S_i h(m_i'')} \pmod{N}
\]

If the attacker collects the \( n \) secret keys of the signer \( U_1, U_2, \cdots, U_n \) by above steps, he can forge a valid multisignature \( SG'' \) for any message \( m'' \) for sequential and broadcasting architectures. In [2], Wu and Hsu also proposed two ID-based multisignatures with distinguished signing authorities for sequential and broadcasting architectures. Both ID-based multisignature schemes are similar to each other in the structure of multisignature generation and verification except using different ID-based system. The above known signature attack can also successfully be applied to these schemes.

IV. CONCLUSION

We have presented a known signature attack on Wu-Hsu’s ID-based multisignatures with distinguished signing authorities for sequential and broadcasting architectures. In this attack, any malicious attacker can solve any signer’s secret key from two known valid partial signatures. Then, the attacker can forge a valid group multisignature for any message for sequential and broadcasting architectures. The attack cannot be detected by the verifier except in the rollover period of signer’s secret key. The main complexity of the attack is equivalent to the complexity of computing approximately \( n \) times the Euclidean algorithm. Obviously, the above computational task is not hard to carry out, so the known signature attack method is very efficient. Particularly, we would like to point out that the known signature attack is also successful for the similar Wu-Hsu’s ID-based multisignature schemes with distinguished signing authorities for sequential and broadcasting architectures.

ACKNOWLEDGMENT

This work was supported by the National Science Council, Taiwan, under contracts NSC 96-2221-E-214-071-MY3.
REFERENCES

