On the Security of a New Efficient Group Signature
with Forward Security

C. Y. Gun¹,², H. F. Lin³, C. Y. Chen⁴, S. H. Liao⁴

¹Department of Communications Engineering,
Feng Chia University, Taichung 40724, Taiwan, R.O.C.

²Department of Finance,
Nan Kai Institute of Technology, Nantou 54210, Taiwan, R.O.C

E-mail: moon384@nkc.edu.tw

³Department of Information Engineering and Computer Science,
Feng Chia University, Taichung 40724, Taiwan, R.O.C.

E-mail: hflin@fcu.edu.tw

⁴Department of Communications Engineering,
Feng Chia University, Taichung 40724, Taiwan, R.O.C.

E-mail: chihchen@fcu.edu.tw,M9406251@fcu.edu.tw

Abstract

A Group signature means that any member in a group may sign a message anonymously on behalf of the group. The group manager can trace the actual signer whenever a debate regarding signing occurs. Based on Song’s practical forward secure group signature scheme, Zhang, Wu, and Wang proposed “A Novel Efficient Group Signature Scheme with Forward Security” in 2003 and, two years later, the same group proposed “A New Efficient Group Signature with Forward Security” in Informatica aiming to improve the security of their previous method. In this paper, we show that the “Exculpability” and the “Revocability” properties claimed in Zhang, Wu, and Wang’s new scheme are both not secure because (1) the
group manager himself can achieve forging a valid signature without being traced; (2) once one group member is expelled from the group, all group signatures produced thereafter could be assumed a revoked signature.

**Keywords:** Group signature, forward security, anonymity, exculpability, revocability, traceability.

1. **Introduction**

   Digital signatures play an important role in the electronic society nowadays, since it takes advantage of its integrity property to prevent modification of the received message and its authentication property to verify the validity of the user. Group signatures, blind signatures, threshold signatures, undeniable signatures are all digital signatures. Chaum and Heyst [5] proposed the first group signature in 1991. They described in their scheme that a group signature means that any group member may sign document on behalf of the group anonymously. Everyone can check the validity of the signature, but due to its anonymity and unlinkability properties, none except the group manager is able to trace the actual signer. Accordingly, a group signature satisfies three conditions. (1) Only members of the group can sign documents on behalf of the group. (2) Any receiver may verify the validity of the signature, but none except the group manager can discover which group member was the signer. (3) Whenever disputes occur, the group manager can “OPEN” the signature to reveal the actual signer.

   Many group signature schemes have been subsequently proposed [1, 2, 3, 5, 6, 7, 9]. In 2003, Zhang, Wu and Wang [10] proposed a novel efficient group signature scheme with forward security. This scheme has ID-based property and broadcasts on the CRL whenever a group member is revoked. In the same year, Wang [8] showed that Zhang, Wu and Wang’s method [10] is vulnerable such as being forgeable, untraceable, and linkable.

   In 2005, Cao [4] also pointed out the untraceability of Zhang, Wu and Wang’s method [10] by using simpler methods. Though Zhang, Wu and Wang [11] proposed “A New Efficient Group Signature with Forward Security” in 2005 aiming to improve their previous scheme, we shall point out that the “Exculpability” and the “Revocability” properties are both not secure in their new scheme. This is because the group manager himself can achieve forging a valid signature without being traced. If any group member, say Bob, is expelled from the
group starting from the time period \( j \), then any group signature at time period \( i \), for \( i \geq j \), could be assumed a revoked signature. This is a serious flaw.

This paper is organized as follows. Section 2 overviews the informal definitions of a forward-secure group signature scheme and the security requirements. Section 3 gives a brief review of Zhang, Wu and Wang’s new scheme [11]. Then, in Section 4, we show the exculpability and the revocability properties are both not secure in their new scheme. Finally, in Section 5, we conclude this paper.

2. Preliminaries

**Definition 1.** [4, 8, 10, 11] A group signature scheme consists of the procedures listed below:

- **SETUP**: Obtain the group public key and secret key through an algorithm.
- **JOIN**: An interactive protocol between the group manager and a user which allows the user to become a group member.
- **SIGN**: Any group member may sign documents on behalf of the group.
- **VERIFY**: Determine the validity of a group signature by using the group public key.
- **OPEN**: Track down the actual signer, given the signed message and the group secret key.

**Definition 2.** [4, 8, 10, 11] We say that a group signature is secure if it meets the following properties:

- **Correctness**: A signature generated by any member of the group must be accepted by the “VERIFY” procedure.
- **Unforgeability**: Only group members may represent the group when signing messages.
- **Anonymity**: Identifying the actual signer is computationally hard for all except the group manager.
- **Unlinkability**: It is computationally hard to decide whether two different signatures were
signed by the same group member.

Exculpability: Even if the group manager and some of the group members collude, they cannot sign on behalf of non-involved group members.

Traceability: The group manager can always trace the actual signer of a valid signature.

Coalition-resistance: Colluding group members cannot generate a valid signature that is untraceable.

Revocability: Whenever a group member leaves the group, he can no longer generate a valid group signature.

Forward security: Whenever a group signing key is exposed, previously generated group signatures remain valid and do not need to be re-signed.

3. A brief review of Zhang, Wu and Wang’s scheme

Zhang, Wu and Wang’s group signature scheme [11] is comprised of the following procedure:

3.1 SETUP. The group manager (GM) randomly chooses two large primes \( p_1 \) and \( p_2 \), with the same size such that \( p_1 = 2p_1' + 1 \), \( p_2 = 2p_2' + 1 \), both \( p_1' \) and \( p_2' \) also being primes.

Let \( n = p_1p_2 \), and \( G = \langle g \rangle \) be a cyclic subgroup of \( Z_n^* \) where \( Z_n^* = \{x \in Z_n \mid \gcd(x, n) = 1\} \), \( g \)'s order is \( 
\text{ord}<g> = p_1'p_2' \). GM randomly chooses an integer \( e \) satisfying \( \gcd(e, \phi(n)) = 1 \), and then computes \( d \) such that \( de = 1 \mod \phi(n) \) where \( \phi(n) \) is the Euler Totient function. Let \( h(\cdot) \) be a coalition-resistant hash function. The expected system lifetime period is divided into \( T \) intervals and they are publicly known. GM randomly chooses an integer \( x \) as his secret key and computes the corresponding public key \( y = g^x \mod(n) \). \( (c,s) = SPK \{y : y = g^r\}() \) denotes the signature of knowledge of \( \log_g y \) in \( G \). Finally, the group manager publishes the public key \((y,n,g,e,h(\cdot), ID_{GM}, T)\), where \( ID_{GM} \) is the identity of the group manager.
3.2 JOIN. If a user, say Bob, wants to join the group, he executes an interactive protocol with GM. First, Bob chooses a random number \( k \in Z_n^* \) as his secret key, and computes his identity \( ID_B \equiv g^k \pmod{n} \). Then he generates the signature of knowledge \( (c, s) = SPK\{\gamma': ID_B = g^\gamma\} \) to show that he knows a secret value \( k \) to meet \( ID_B \equiv g^k \pmod{n} \). Finally, Bob keeps \( k \) private and sends \((ID_B, (c, s))\) to the group manager.

Upon receiving \((ID_B, (c, s))\), GM first verifies the signature of knowledge \((c, s)\). If the verification holds, GM stores \((ID_B, (c, s))\) in his group member database and then generates membership certificate for Bob. Thereby, GM randomly chooses a number \( \alpha \in Z_n^* \) and computes the triple \((s_B, r_B, \omega_{B_0})\) as follow:

\[
\begin{align*}
r_B &\equiv g^\alpha \pmod{n}, \\
s_B &\equiv \alpha + r_B x, \\
\omega_{B_0} &\equiv (r_B ID_{GM} ID_B)^{-d^\gamma} \pmod{n}.
\end{align*}
\]

Then GM sends this membership certificate \((s_B, r_B, \omega_{B_0})\) to Bob via a private channel and stores \((s_B, r_B, \omega_{B_0})\) together with \((ID_B, (c, s))\) in his local database.

After Bob receives \((s_B, r_B, \omega_{B_0})\), he verifies the following relations:

\[
\begin{align*}
g^{s_B} &\equiv r_B^\gamma \pmod{n}, \\
r_B ID_{GM} ID_B &\equiv \omega_{B_0}^{-\gamma} \pmod{n}.
\end{align*}
\]

If both the above equations hold, Bob stores \((s_B, r_B, \omega_{B_0})\) as his resulting initial membership certificate.

3.3 EVOLVE. Assume that Bob has the group membership certificate \((s_B, r_B, \omega_{B_j})\) at time period \( j \). Then at time period \( j+1 \), he updates his group membership certificate as \((s_B, r_B, \omega_{B_{j+1}})\) via Evolving function \( f(x) = x^\epsilon \pmod{n} \) and compute

\[
\omega_{B_{j+1}} \equiv (\omega_{B_j})^\epsilon \pmod{n}, \text{ where } \omega_{B_j} \equiv (r_B ID_{GM} ID_B)^{-d^{\epsilon-j}} \pmod{n}.
\]
3.4 SIGN. Let \( (s_B, r_B, \omega_B) \) be Bob’s group membership certificate at time period \( j \), to sign a message \( m \), Bob randomly chooses three numbers \( q_1, q_2, q_3 \in \mathbb{Z}_n^* \), and computes \( z_1, u, r_1, r_2, r_3 \) as follows:

\[
\begin{align*}
z_1 & \equiv g^{q_1} q_2^{s_B} \equiv u \mod n, \\
u & = h(z_1, m), \\
r_1 & = q_1 + (s_B + k)u, \\
r_2 & \equiv q_3 \omega_B^u \mod n, \\
r_3 & = q_2 - r_B u.
\end{align*}
\]

The group signature on \( m \) is \( \sigma = (u, r_1, r_2, r_3, m, j) \).

3.5 VERIFY. Given a group signature \( \sigma = (u, r_1, r_2, r_3, m, j) \), a verifier accepts it as a valid group signature on \( m \) if and only if \( u = h(z_1', m) \), where \( z_1' \) is computed by

\[
z_1' \equiv ID_{GM}^{x_B} g^x r_2^{s_B} \equiv y^n \mod n.
\]

3.6 OPEN. Given \( \sigma = (u, r_1, r_2, r_3, m, j) \), in case of a dispute, GM can open it to reveal the actual identity of the signer who produced the signature. GM executes the following steps:

1. Check the validity of signature \( \sigma \) via VERIFY procedure.
2. Compute \( \eta \equiv 1/u \mod \phi(n) \).
3. Compute \( z_1' \equiv ID_{GM}^{x_B} g^x r_2^{s_B} \equiv y^n \mod n \).
4. Search his database to find a pair \( (ID_B, r_B) \) that satisfies the following equality:

\[
r_3/\omega_B^u = (z_1'/g^x y^n)^{d_{s_B}^{-1}} \mod n.
\]
5. If there is a duple \( (ID_B, r_B) \) satisfying the above equation, GM concludes that \( ID_B \) is the identity of the actual signer.
3.7 REVOKE. If GM wants to revoke Bob’s membership certificate at time period $j$, he publishes a revocation duple $(R_j, j)$ in the CRL (the Certificate Revocation List), where $R_j$ is computed by:

$$R_j = \omega_{b_j}(r_b ID_b)^{d_{r-j}} \mod n,$$

we explain as below:

Given a valid group signature $\sigma = (u, r_1, r_2, r_3, m, j)$, a verifier can identify whether $\sigma$ is produced by a revoked group member or not. He computes the following:

(i) $z' \equiv ID_{GM}^u g^n r_2^{r-j} y^n \mod n$.

(ii) $z'(r_2^{-1} R_j)^{r-j} \equiv g^n y^n \mod n$.

If the signature satisfies the equation (1), then the verifier concludes that the signature $\sigma$ is revoked.

Assume a verifier has a signature for period $i$, where $i \geq j$. To check whether the membership certificate of the group member has been expelled, the verifier simply computes $R_j = (R_j)^{r-j} \mod n$ and checks whether the equation $z'(r_2^{-1} R_j)^{r-j} = g^n y^n \mod n$ holds or not. If it holds, it means that the signature has been revoked.

4. Cryptanalysis of Zhang, Wu and Wang’s Scheme

In 2003, Zhang, Wu and Wang [10] proposed a novel efficient group signature scheme with forward security. Unfortunately, the scheme was pointed out to have flaws such as being linkable, untraceable and universally forgeable by Guilin Wang in [8]. Furthermore, Cao [4] has also shown the untraceability by a simpler attack.

Though Zhang, Wu and Wang [11] proposed, in 2005, a new scheme “A New Efficient Group Signature with Forward Security” aiming to improve their previous scheme [10], we shall point out that the “Exculpability” and the “Revocability” properties in their new scheme are still insecure.
4.1 Unexculpability

In this subsection, we shall propose an attack aimed at the Exculpability property of Zhang, Wu and Wang’s new scheme [11].

ATTACK 1. The group manager (GM) can forge a signature on behalf of any group member for a message \( m \) at “any time period \( j \)”, he can do the processes by himself as follows.

1. Randomly choose three integers \( q_1, q_2, q_3 \in Z_n^\ast \).

2. Compute \( z = g^{q_0} y^{q_2} q_3^{e_j} \mod n \).

3. Compute \( u = h(z, m) \).

4. Choose one group member’s record \( ((s_B, r_B, \omega_{B_i}, (ID_B, (c, s))) \) from his database and compute

\[
\begin{align*}
  r_1 &= s_B u + q_1, \\
  r_2 &= q_3 \omega_B^{e_j} ID_B^{e_j} \\
  r_3 &= q_2 - r_B u.
\end{align*}
\]

The manager claims that \( (u, r_1, r_2, r_3, j) \) is a valid group signature on \( m \) because it can pass the verify procedure as follows.

(i) Compute \( z' \equiv ID_G^{\ast} g^{q_0} r_2^{e_j} y^{q_2} \mod n \).

(ii) \( h(z', m) = u \) holds because

\[
\begin{align*}
  z' &= ID_G^{\ast} g^{q_0} r_2^{e_j} y^{q_2} \mod n \\
  &= ID_G^{\ast} g^{q_0} r_2^{e_j} y^{q_2} (r_B ID_G^{\ast} ID_B^{e_j})^{e_j} \mod n \\
  &= g^{q_0} r_2^{e_j} y^{q_2} ID_G^{\ast} ID_B^{e_j} r_B^{e_j} \mod n \\
  &= g^{q_2} r_3^{e_j} \mod n \\
  &= z \mod n.
\end{align*}
\]

ATTACK 2. The group manager or any group member can forge a valid signature without being traced as follows.

1. Randomly choose three integers \( q_1, q_2, q_3 \in Z_n^\ast \).
(2) Compute \( z \equiv g^h r^t q_1^x \mod n \).

(3) Compute \( u = h(z, m) \).

(4) Compute \( r_1 = q_1, \)
\( r_2 = q_3 ID_{GM}^{\omega t^{-j}}, \)
\( r_3 = q_2. \)

Then he claims that \((u, r_1, r_2, r_3, j)\) is a valid group signature on \( m \) because it can pass the verifying procedures as follows:

(i) Compute \( z' \equiv ID_{GM}^u g^x r_2 y^o \mod n \).

(ii) \( h(z', m) = u \) holds because
\[
z' \equiv ID_{GM}^u g^x r_2 y^o \mod n
\equiv ID_{GM}^u (q_1 ID_{GM}^{\omega t^{-j}})^r y^o \mod n
\equiv g^h r^t ID_{GM}^u q_3 ID_{GM}^{\omega t^{-j} r^{-j}} \mod n
\equiv g^h r^t q_3 r^{-j} \mod n
\equiv z.
\]

Observing the two attacks displayed above, since the GM can forge signatures independently, then the security of the “Exculpability” property, which the authors claim to have, is flawed.

4.2 Untraceable problem

In Step 3 of the “Open Procedure” located in the authors’ article, \( r_2 / \omega_{B_j}^y \equiv (z'_j / g^x y^o)^{r^{-j}} \mod n \) does not hold and is apparently wrong. We have attempted to modify the original equality, yet unsuccessfully, therefore we will not further discuss the “Traceability” property.

4.3 Unrevocability

If GM revokes Bob’s membership certificate at time period \( j \), he publishes a revocation
token \((R_j, j)\) in the CRL (the Certificate Revocation List), where \(R_j = \omega_B \left( r_B ID_B \right)^{d_j} \mod n\).

Since

\[
R_j = \omega_B \left( r_B ID_B \right)^{d_j} \mod n = (r_B ID_{GM} ID_B)^{-d_j} \cdot (r_B ID_B)^{d_j} \mod n = ID_{GM}^{-d_j} \mod n,
\]

\(R_j\) is independent of Bob. So the unrevocability attack can be applied by any group member, and any group member are also assumed to be revoked by the GM from the time period \(j\), therefore their signatures are assumed invalid. Because once \((R_j, j)\) is declared, given a group signature \((u, r_1, r_2, r_3, m, j + i)\) for \(i = 0, 1, 2, \ldots, T - (j + 1)\), when a verifier identifies whether the signature is produced by a revoked group member or not, he computes the following quantification:

**Step 1:**

\[
z' = ID_{GM}^{u} g^{\tilde{r}_2} y^{\tilde{r}_1} \mod n
\]

**Step 2:** \((R_j)_{\tilde{R}} = R_{j+i} = ID_{GM}^{-d_\tilde{r}_{j+i}} \mod n\) for \(i = 0, 1, 2, \ldots, T - (j + 1)\)

Check \(z'(r_2^{-1} R_{j+i}^{\tilde{w}})^{d_\tilde{r}_{j+i}} = g^\tilde{y} \mod n \cdots \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \·}
We have presented two simple and direct attacks to show that the “Exculpability” property is insecure. The “Revocability” property is still fragile in their scheme.

References


