LETTER

A Universal Forgery on Araki *et al.*'s Convertible Limited Verifier Signature Scheme

Fangguo ZHANG[†], ***Nonmember and*** **Kwangjo KIM**[†], ***Member***

SUMMARY In 1999, Araki *et al.* [1] proposed a convertible limited verifier signature scheme. In this letter, we propose a universal forgery attack on their scheme. We show that any one can forge a valid signature of a user U_A on an arbitrary message.
key words: *Signature scheme, Convertible limited verifier signature, Universal forgery.*

1. Introduction

The digital signature provides the function of integration, authentication, and non-repudiation for the signing message. In ordinary digital signature schemes, anyone can verify the signatures with signer's public key. However it is not necessary for anyone to be convinced a justification of signer's dishonorable message such as a bill. It is enough for a receiver only to prove a justification of the signature if the signer does not execute a contract. The undeniable signature schemes [2] [3] and the limited verifier signature scheme[1] can solve this problem. There exists a message such as official documents which will be first treated as limited verifier signatures but after a few years as ordinary digital signatures. So the limited verifier signature scheme should be convertible. In 1999, Araki *et al.* [1] proposed a convertible limited verifier signature scheme. In this paper, we show that Araki *et al.*'s scheme is universally forgeable, that is, any one can forge a valid signature of a user U_A on an arbitrary message.

2. Araki *et al.*'s Convertible Limited Verifier Signature Scheme

In this section, we give a short description of Araki *et al.*'s convertible limited verifier signature scheme and refer to the original paper [1] for more details.

Araki *et al.*'s convertible limited verifier signature scheme can be divided into three phases: the signing, the 1st verification, and the 2nd verification (or conversion) phases. In the signing and the 1st verification phases, a signer can generate a signature with message recovery [4] to some specified recipient. In the conversion phase, the signer is requested to submit one more parameter for converting the signature into an ordinary one and then any verifier can verify the converted signature. Initially, the system publishes the following parameters:

- p : a large prime,
- q : a large prime satisfying $p = 2q + 1$,
- g : an element of order q in Z_p^*,
- $H(\cdot)$: a one-way hash function.

Each user U_i owns a secret key $x_i \in Z_q^*$ and a public key $y_i = g^{x_i} \bmod p$. Let U_A be the signer, U_B the recipient, and m the message to be signed.

[*Signing Phase*]

For signing the message m, the signer U_A first chooses an integer $k \in Z_q^*$ and computes $j = H(k)$, $r_1 = y_B^{k+j} \bmod p$ and $r_2 = m(r_1 + g)^{-1} \bmod p$. He then verifies whether $r_1 + g \neq 0 \pmod p$ and $r_2 < q$. If both of the two inequalities hold, he computes

$$J = g^j \bmod p$$

$$s = (r_2 k - 1 - r_2)(1 + x_A)^{-1} \bmod q.$$

The signature for m is (r_2, s, J) which will be sent to the recipient U_B.

[1*st Verification Phase*]

The recipient U_B can recover the message as

$$m = (y_B^{(1+r_2+s)r_2^{-1}} (y_A^{sr_2^{-1}} J)^{x_B} + g) r_2 \bmod p.$$

It is easy to see that only U_B can recover m and check its validity, since the recovery equation involves U_B's secret key x_B.

[*Conversion Phase*]

To convert the signature into an ordinary one, the signer U_A is requested to release a further parameter $u = (s x_A r_2^{-1} + j) \bmod q$. Upon receiving u, U_B first verifies its validity with the equality $g^u = y_A^{sr_2^{-1}} J \bmod p$. If holds, U_B can reveal the converted signature for m as (r_2, s, J, u) in case of the signer's repudiation. For verifying the converted signature, the verifier first verifies the equality $g^u = y_A^{sr_2^{-1}} J \bmod p$. If it does not hold, the signature is invalid; otherwise, the verifier verifies the signature with the equality

$$m = (y_B^{(1+r_2+s)r_2^{-1}+u} + g) r_2 \bmod p.$$

If it holds, the signature is valid.

[†]The authors are with International Research center for Information Security (IRIS), Information and Communications University (ICU), 58-4 Hwaam-dong Yusong-ku, Taejeon, 305-732 KOREA. E-mail: {zhfg, kkj}@icu.ac.kr

3. A Universal Forgery on Araki *et al.*'s Signature Scheme

In this section, we propose a universal forgery attack on Araki *et al.*'s convertible limited verifier signature scheme.

Assume that **Adv** is an adversary, and he want imitate U_A to sign a message to U_B. **Adv** will do as follows:

[*Forge Signing Phase*]

For any message m, **Adv** first chooses a random integer $c \in Z_q^*$ and computes $r_2 = m(y_B^c + g)^{-1} \bmod p$. He then verifies whether $y_B^c + g \neq 0 \pmod p$ and $r_2 < q$. If both of the two inequalities hold, he chooses another random integer $s \in Z_q^*$ and computes

$$t = c - r_2^{-1}(1 + r_2 + s) \bmod q.$$

$$J = y_A^{-sr_2^{-1}} g^t \bmod p$$

The signature for m is (r_2, s, J) which is sent to the recipient U_B.

Then (r_2, s, J) is a valid signature of m since

$$\begin{aligned}
&(y_B^{(1+r_2+s)r_2^{-1}}(y_A^{sr_2^{-1}} J)^{x_B} + g)r_2 \bmod p \\
&= (y_B^{(1+r_2+s)r_2^{-1}}(y_A^{sr_2^{-1}} y_A^{-sr_2^{-1}} g^t)^{x_B} + g)r_2 \bmod p \\
&= (y_B^{(1+r_2+s)r_2^{-1}} y_B^t + g)r_2 \bmod p \\
&= (y_B^{(1+r_2+s)r_2^{-1}+t} + g)r_2 \bmod p \\
&= (y_B^c + g)r_2 \ mod\ p \\
&= m
\end{aligned}$$

When U_B wants to convert the signature into an ordinary one, he asks **Adv** to release a further parameter. **Adv** sends t to U_B. Upon receiving t, U_B can first verifies its validity with the equality $g^t = y_A^{sr_2^{-1}} J \bmod p$. Then, U_B can reveal the converted signature for m as (r_2, s, J, t) in case of the signer U_A's repudiation. For verifying the converted signature, the verifier first verifies the equality $g^t = y_A^{sr_2^{-1}} J \bmod p$. If it does not hold, the signature is invalid; otherwise, the verifier further verifies the signature with the equality

$$m = (y_B^{(1+r_2+s)r_2^{-1}+t} + g)r_2 \bmod p.$$

If it holds, the signature is valid.

From above, we see that Araki *et al.*'s convertible limited verifier signature scheme is universally forgeable.

4. Conclusion

In this letter, we have shown that Araki *et al.*'s convertible limited verifier signature scheme is universally forgeable. Since the convertible limited verifier signature is very useful in electronic commerce, designing a secure and efficient convertible limited verifier signature scheme against this attack remains an open problem.

References

[1] S. Araki, S. Uehara and K. Imamura, *The limited verifier signature and its application*, IEICE Transactions on Fundamentals E82-A (1), pp. 63-68, 1999.

[2] J. Boyar, D. Chaum, I. Damgard and T. Pedersen, *Convertible undeniable signatures*, Advances in Cryptology-Crypt0'90, LNCS 537, pp.189-205, Springer-Verlag,1990.

[3] D. Chaum and H. van Antwerpen, *Undeniable signatures*, Advances in Cryptology-Crypt0'89, LNCS 435, pp.212-216, Springer-Verlag,1990.

[4] K. Nyberg and R.A. Rueppel, *Message recovery for signature schemes based on the discrete logarithm problem*, Advances in Cryptology-EuroCrypt'94, LNCS 950, pp.182-193, Springer-Verlag,1995.