Comment on "Improvement of the Miyazaki-Takaragi Threshold Digital Signature Scheme"

Zuhua Shao

Department of Computer and Electronic Engineering, Zhejiang University of Science and Technology
No. 85, XueYuan Road, Hangzhou, Zhejiang 310012, P.R. of China (Email: zhshao_98@yahoo.com)

(Received Sept 16, 2005; accepted Oct. 28, 2005)

Abstract

To enhance applications of smart cards, Miyazaki and Takaragi proposed a (t, n) threshold digital signature scheme based on the security of elliptic curve discrete logarithm (ECDLP). The advantages of their scheme are low communication bandwidth and computational complexity, which provides critical benefits for the use of smart cards in distributed environments. Recently Wu et al. pointed out that the Miyazaki-Takaragi threshold digital signature scheme cannot withstand the insider forgery attack. Then they further amended the scheme against the attack with a simple improvement. However, this paper will show that the attack proposed by Wu et al. is wrong, since they confused the point addition of elliptic curve with the vector addition on a finite field. Finally, we will point out that a general coalition attack can be also applied to both of the Miyazaki-Takaragi scheme and the Wu's improvement.

Keywords: Coalition attack, elliptic curve, forgery attack, threshold digital signature

1 Introduction

With digitalized documents, hand-written signatures are replaced by digital signatures to provide the functions of integrity, authentication and non-reputation in the compute systems [2, 7]. In group-orientated applications, a group signature can be generated by one member, some members, or all members according to the group's signing policy. A (t, n) threshold signature scheme allows any t or more signers to cooperatively sign messages on behalf of the group, but $t - 1$ or fewer signers cannot [1, 3].

Smart cards are produced for their easy carrying and ease of use [4]. Because smart cards can only be equipped with a processor with a slight computing power and a very limited memory capability, the required computational complexity and the memory storage are concerned the most in the use of smart cards. To enhance the applications of smart cards, Miyazaki and Takaragi [6] proposed a (t, n) threshold digital signature scheme based on the security of elliptic curve discrete logarithm (ECDLP). The advantages of their scheme are low communication bandwidth and computational complexity, which provides critical benefits for the use of smart cards in distributed environments.

Recently Wu et al. [9] pointed out that the Miyazaki-Takaragi threshold digital signature scheme cannot withstand insider forgery attacks. They thought that a malicious signer could cheat other signer into signing messages chosen by the malicious signer. Then they further amended the scheme against the attack with a simple improvement. However, this paper will show that the attack proposed by Wu et al. is wrong, since they confused the point addition of elliptic curve with the vector addition on a finite field. Finally, we will point out that a general coalition attack can be also applied to both of the Miyazaki-Takaragi scheme and the Wu's improvement. Though we can improvement their scheme against the coalition attack, resulting scheme is perhaps not applicable for smart cards.

2 Brief Review of the Miyazaki-Takaragi Scheme

The scheme consists of three phases: the initialization phase, the signing phase and the verification phase.

Initialization phase:
Let the n members in the group be $\{u_1, u_2, \ldots, u_n\}$. Initially, the dealer of the phases determines the following parameters:

p: a prime;

$E(Z_p)$: an elliptic curve manipulated over Z_p;

G: the base point on $E(Z_p)$;

q: the order of G on $E(Z_p)$, which is also a prime;

$h(\cdot)$: one-way hash function;

d: the group's private key, which is chosen from Z_q;

$Y = d \cdot G$: the group's public key, which is a point on $E(Z_p)$;

$f(x) = d + d_1 x + \cdots + d_{t-1} x^{t-1}$, where d_i's are random integers in Z_q.

The secret key for u_i is computed as $x_i = f(i)$ which is then securely delivered to u_i (for $i = 1$ to n). The corresponding public key for u_i is $Y_i = x_i \cdot G$.

Signing phase:
Without loss of generality, let $S = \{u_1, u_2, \ldots, u_t\}$ be the set of t signers who want to cooperatively generate a group signature for the message m. Each signer u_i performs the following steps:

Step 1. Compute $e_i = c_i \cdot x_i \bmod q$, where $c_i = \Pi_{u_j \in s \setminus \{u_i\}} j/(j-i)$ is the Lagrange coefficient.

Step 2. Choose a random integer $k_i \in Z_q$.

Step 3. Compute $R_i = k_i \cdot G$, which is then broadcasted to all other signers.

Step 4. Compute

$$(x, y) = \sum_{u_j \in S} R_j \tag{1}$$

After receiving all R_j's from other co-signers, the signer u_i performs the following steps:

Step 5. Compute

$$\begin{aligned} r &= x - h(m) \bmod q, \qquad (2)\\ v_i &= e_i \cdot r + k_i \bmod q, \qquad (3) \end{aligned}$$

then broadcast v_i to all other co-signers.

Step 6. Validate v_j with the equality $R_j = v_j \cdot G - r \cdot c_j \cdot Y_j$ for $u_j \in S \setminus \{u_i\}$. If the verification for some v_j does not hold, u_j is requested to resubmit it again. When all v_j's are valid, the signer u_i proceeds to the next step.

Step 7. Compute

$$v = \sum_{u_j \in S} v_j \bmod q \tag{4}$$

The group signature for message m is (r, v).

Verification phase:
The verifier can verify the group signature with the following equality:

$$x = r + h(m) \bmod q \tag{5}$$

where

$$(x, y) = v \cdot G - r \cdot Y. \tag{6}$$

If it holds, the group signature is a valid group signature.

3 Wu et al.'s Cryptanalysis and Improvement

Wu et al. demonstrated a forgery attack plotted by some insider. Let $u_a \in S$ be the malicious signer who attempts to forge a valid group signature for his arbitrarily chosen message m'. He first chooses a random integer $k_a \in Z_q$ and computes $R'_a = k_a \cdot G$, then waits until receiving all other signers' R_i's without broadcasting R'_a. When all R_i's sent from other signers are collected, u_a first computes

$$(x', y') = R'_a + \sum_{u_j \in S \setminus \{u_a\}} R_j. \tag{7}$$

And assigns

$$R' = (x' - h(m') + h(m), y') \tag{8}$$

where m is the original message to be signed by S. Then, u_a computes and broadcasts

$$R_a \;=\; R' - (x', y') + R'_a \tag{9}$$

to all co-signers instead of R'_a. Following the normal procedure, each participant signer obtains

$$(x, y) = (x' - h(m') + h(m), y'),$$

which would be shown in Theorem 1. Then, by Equation (2), each participant signer computes

$$r' = x - h(m) = x' - h(m') \bmod q. \tag{10}$$

That is, the individual signature v_i in Equation (3) is generated with respect to the message m' chosen by u_a. After collecting all v_i's in Step 6, u_a disrupts the process with some suitable excuse. Then u_a computes v' as Equation (4). In Theorem 2, Wu et al. confirmed that the forged signature (r', v') is a valid group signature for m'.

Theorem 1 *With the broadcasted R_a of Equation (9), each participant signer will obtain $(x, y) = (x' - h(m') + h(m),\ y')$ by Equation (1).*

Proof.

$$\begin{aligned} (x, y) &= \sum_{u_j \in S} R_j \qquad \text{(by Equation (1))}\\ &= R_a + \sum_{u_j \in S \setminus \{u_a\}} R_j\\ &= R' - (x', y') + R'_a + (x', y') - R'_a\\ &= R' \qquad \text{(by Equations (9) and (7))}\\ &= (x' - h(m') + h(m),\ y') \quad \text{(by Equation (8))} \end{aligned}$$

□

Theorem 2 *The forged signature (r', v') for m' will pass the signature verification.*

Proof. From Equation (6), the verifier first computes

$$\begin{aligned} & V' \cdot G - r' \cdot Y \\ = & \sum_{u_i \in S} v_i \cdot G - r' \cdot Y \qquad \text{(by Equation (4))} \\ = & \sum_{u_i \in S} (e_i \cdot r' + k_i \bmod q) \cdot G - r' \cdot Y \\ & \qquad \text{(by Equation (3))} \\ = & r' \cdot d \cdot G + \sum_{u_i \in S} k_i \cdot G - r' \cdot Y \\ & \qquad \text{(by Lagrange Formula)} \\ = & \sum_{u_i \in S} k_i \cdot G \qquad (\because Y = d \cdot G) \\ = & R'_a + \sum_{u_i \in S \setminus \{u_a\}} R_i \qquad (\because R_i = k_i \cdot G) \\ = & (x', y') \qquad \text{(by Equation (7))} \end{aligned}$$

Since $r' = x' - h(m') \bmod q$ by Equation (10). That is, as compared to Equation (5) and (6), the verifier will be convinced that (r', v') is a valid group signature for m'. □

By stated above, Wu et al. thought that the Miyazaki-Takaragi scheme is insecure against the forgery attack. To strengthen security, they suggested that $h(m)$ should be replaced by $h(m||(x, y))$.

4 Comment on Wu's Cryptanalysis

The Miyazaki-Takaragi scheme is over on elliptic curve [5]. An elliptic curve $E(Z_p)$ defined by the parameters $a, b \in Z_p$ (satisfy $4a^3 + 27b^2 \neq 0 \bmod p$) consists of the set of solutions or points $P = (x, y)$ for $x, y \in Z_p$ to the equation:

$$y^2 = x^3 + ax + b \bmod p$$

together with extra point O called the point at infinity. The equation $y^2 = x^3 + ax + b \bmod p$ is called the defining equation of $E(Z_p)$. For a given point $P = (x_p, y_p)$, x_p is called the x-coordinate of P, and y_p is called the y-coordinate of P.

By defining an addition rule to add points on $E(Z_p)$, the set of points on $E(Z_p)$ forms an abelian group. The addition rule is specified as follows:

1) $O + O = O$.

2) $(x, y) + O = O + (x, y) = (x, y)$ for all $(x, y) \in E(Z_p)$.

3) $(x, y) + (x, -y) = O$ for all $(x, y) \in E(Z_p)$, that is, $-(x, y) = (x, -y)$.

4) $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ for all $(x_1, y_1), (x_2, y_2) \in E(Z_p)$ and $x_1 \neq x_2$, where $x_3 = \lambda^2 - x_1 - x_2 \bmod p$, $y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$, and $\lambda = (y_2 - y_1)/(x_2 - x_1) \bmod p$.

5) $(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$ for all $(x_1, y_1) \in E(Z_p)$ and $y_1 \neq 0$, where $x_3 = \lambda^2 - 2x_1 \bmod p$, $y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$, and $\lambda = (3x_1^2 + a)/(2y_1) \bmod p$.

Note that, not all vectors in $Z_p \times Z_p$ are the point on $E(Z_p)$ and the vector addition is different from the point addition of $E(Z_p)$. However, in the Wu's cryptanalysis, the two kinds of the additions are confused.

In Equation (7), $(x', y') = R'_a + \sum_{u_i \in S \setminus \{u_a\}} R_j$ is a point on $E(Z_p)$, since R'_a is a point on $E(Z_p)$.

In Equation (8), $R' = (x' - h(m') + h(m), y')$ is not a point on $E(Z_p)$, since at most only three points on $E(Z_p)$ have the same y-coordinate. Then there are some problem in the calculation of Equation (9) $R_a = R' - (x', y') + R'_a$, the vector addition or the point addition of $E(Z_p)$?

By guessing, the meaning of Wu et al. is the point addition of $E(Z_p)$. However, by using the addition rule of the point addition of $E(Z_p)$, the resulting R_a is not a point on $E(Z_p)$. Following the Wu's forgery attack, u_a broadcasts R_a to all co-signers instead of R'_a.

Following the normal procedure, each participant signer obtains (x, y) which is not $(x' - h(m') + h(m), y')$, since the Theorem 1 is wrong.

The prerequisite of the proof of the Theorem 1 is that the point (x, y) forms an abelian group. Certainly, we can define this addition rule to add vectors on $Z_p \times Z_p$. However, the vectors in $Z_p \times Z_p$ do not form an abelian group with respect to the addition rule. The conditions of the equations of

$$\begin{aligned} & R_a + \sum_{j \in S \setminus \{u_a\}} R_j \\ = & (R' - (x', y') + R'_a) + (x', y') - R'_a \\ = & R' \end{aligned}$$

are that commutative law, associative law and cancellation law hold in the defined algebra system. Therefore, the forged (r', v') is not a valid group signature for m'.

One anonymous referee thinks that this error is only one typo. "In Equation (8), one can see that if y' is changed into y'', Wu et al.'s attack is also effective".

However, we do not agree with him for the following reasons:

To satisfy Theorem 1, $R' = (x' - h(m') + h(m), y'')$ must be a point on $E(Z_p)$. Then $(x, y) = (x' - h(m') + h(m), y'')$ satisfies the equation $y^2 = x^3 + ax + b \bmod p$. Hence $x' - h(m') + h(m)$ is a quadratic residue modulo p. This probability is $1/2$ for arbitrarily chosen message m'.

Moreover, to satisfy Theorem 2, the malicious signer u_a must compute $v_a = e_a \cdot r' + k_a \bmod q$ as Equation (3) in Step 5.

Then, in Step 6, other signers should validate with the equality $R_a = v_a \cdot G - r' \cdot c_a \cdot Y_a$.

Note that the malicious signer u_a computes and broadcasts

$$R_a = R' - (x', y') + R'_a \qquad (9)$$

to all co-signers instead of R'_a.

Hence, other signer would find this forgery since $R'_a = k_a \cdot G = v_a \cdot G - r' \cdot c_a \cdot Y_a \neq R'_a$.

Therefore, the Wu et al.'s attack is not also effective even if correcting the so-called typo.

5 A General Coalition Attack Against Threshold Signature Schemes

In the original Miyazaki-Takaragi scheme, the group's private key is d. Each signer u_i has the secret share $x_i = f(i)$. If t or more malicious signers pool their secret shares together, they can recover $f(0)$ by applying Lagrange interpolating polynomial. Then each of them can alone compute valid signatures for new messages on behalf of the group afterwards, without the cooperation of other signers and without being detected by verifiers. Obviously, this violates the group's signing policy. Otherwise, if such coalition is permissive, other signers would follow this kind of dishonesty. Thus, each signer can also alone compute valid group signatures after one coalition. It is terrible for the threshold signature scheme.

In the improvement of Wu et al., there also exists the same kind of coalition attack.

This coalition attack is inherent in many threshold signature schemes [4] using threshold secret share scheme, as long as the private key can be recovered from secret shares.

The other paper of mine [8] provided an approach of withstanding this kind of coalition attack. However, resulting scheme is perhaps not applicable for smart cards since it requires some more communications and computations.

6 Conclusions

In this paper, we have shown that the cryptanalysis proposed Wu et al. against the Miyazaki-Takaragi threshold digital signature scheme is not correct, since they confused the point addition of elliptic curve with the vector addition on a finite field. Then, we have pointed out that a general coalition attack can be also applied to both of the Miyazaki-Takaragi scheme and the Wu's improvement. Though we have proposed an approach to overcome the security flaw inherent in some threshold signature schemes using threshold secret share scheme, resulting scheme is perhaps not applicable for smart cards.

7 Acknowledgements

The author would like to thank the anonymous referees for their valuable comments and suggestions that improve the presentation of this paper. This material is based upon work funded by Zhejiang Provincial Natural Science Foundation of China under Grant No.Y104201.

References

[1] Y. Desmedt, "Society and group oriented cryptography: A new concept," in *CRYPTO'87*, pp. 120-127, Berlin, Springer-Verlag, 1987.

[2] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transaction on Information Theory*, vol. IT-31, no. 4, pp. 469-472, 1985.

[3] L. Harn, "Group-oriented (t, n) threshold signature and multisignature," *IEE Proceedings of Computer Digital Techniques*, vol. 141, no. 5, pp. 307-313, 1994.

[4] M. Hendry, *Smart Card Security and Applications*, Artech House, Inc., 1997.

[5] A. Menezes and S. Vanstone, *Elliptic Curve Systems*, Proposed IEEE P1363 Standard, pp. 1-42, 1995.

[6] K. Miyazaki and K. Takaragi, "A threshold digital signature scheme for a smart card based system," *IEICE Transactions on Fundamental*, vol. E84-A, no. 1, pp. 205-213, 2001.

[7] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems," *Communications of ACM* vol. 21, no. 2, pp. 120-126, 1978.

[8] Z. Shao, "Improvement of threshold proxy signature scheme", *Computer Standard and Interface*, vol. 27, no. 1, pp. 53-59, 2004.

[9] T. S. Wu, C. L. Hsu, H. Y. Lin, and P. S. Huang, "Improvement of the Miyazaki-Takaragi threshold digital signature scheme," *Information Processing Letters*, vol. 88, pp. 183-186, 2003.

Zuhua Shao was born in Shanghai, People's Republic of China, On 30 April 1948. He received B.S. degree in mathematics and M.S. in algebra from the Northeastern Normal University, People's Republic of China in 1976 and 1981 respectively. Since 1990 he has taught computer science as an associated professor in the Hangzhou Institute of Financial Managers, The Industrial and Commerce Bank of China. Now he is a professor at the Zhejiang University of Science and Technology. His current research interests are cryptography and financial data security.