Two Simple Attacks on a Blind Signature Scheme

Miaomiao Tian[1,2], Youwen Zhu[3], and Zhili Chen[1,2]
(Corresponding author: Miaomiao Tian)

School of Computer Science and Technology, University of Science and Technology of China, Hefei, China[1]
Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou, China[2]
Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan[3]
(Email: miaotian@mail.ustc.edu.cn)

(Received Aug. 6, 2012; revised and accepted Mar. 7, 2013)

Abstract

A blind signature scheme allows a user to obtain a signature on a given message without revealing any information about the message to the signer. The idea of blind signature was first introduced by Chaum at CRYPTO 1982. Blind signatures can be used in many applications, such as e-voting. Recently, Chakraborty and Mehta proposed a new blind signature scheme (Chakraborty-Mehta scheme) based on the elliptic curve discrete logarithm problem. They asserted that their blind signature scheme is secure. In this paper, however, we will present two simple but powerful attacks on their blind signature scheme. The attacks show Chakraborty-Mehta blind signature scheme is not secure.

Keywords: Cryptanalysis, blind signature, elliptic curve

1 Introduction

Blind signature scheme is one of cornerstones of modern cryptography. A blind signature scheme allows a user to obtain a signature on a given message without revealing any information about the message to the signer. A secure blind signature scheme should satisfy three properties, i.e., blindness, untraceability and unforgeability.

1) Blindness. It allows a user to obtain a signature on a given message without revealing the message to the signer.

2) Untraceability. It means that the signer is not able to trace the signature-message pair after the user has revealed the signature to the public.

3) Unforgeability. It means that only the signer can generate a valid signature. This property is the most important one and must be satisfied for all signature schemes.

Because of the blindness and untraceability properties, blind signature schemes have been employed extensively in privacy oriented applications, such as e-voting systems (e.g. [5, 8]).

The first blind signature scheme was invented by Chaum [3] in 1982 and the security of that scheme is based on the hardness of factoring large composite integers. Since then, a number of blind signature schemes have been proposed, e.g., [1, 2, 6, 7]. Recently, Chakraborty and Mehta [2] proposed a new blind signature scheme, Chakraborty-Mehta blind signature scheme, based on the elliptic curve discrete logarithm problem. They asserted that their blind signature scheme is secure. In this paper, however, we will show that an adversary $\mathcal{A}$ can easily forge a valid signature on any message, and after receiving a valid signature from a signer, $\mathcal{A}$ is also able to obtain the signer's secret key. Therefore, Chakraborty-Mehta blind signature scheme is not secure and cannot be used in e-voting systems.

The rest of this paper is organized as follows. Section 2 will introduce the definition of elliptic curve group and the general security notions for digital signatures. In Section 3, we briefly review Chakraborty-Mehta blind signature scheme. Two attacks on their blind signature scheme will be given in Section 4. Finally, Section 5 concludes this paper.

2 Preliminaries

2.1 Elliptic curve group

Let $p > 3$ be a large prime and F_p be a finite field. An elliptic curve G over F_p is the set of all points $P = (x, y)$ that satisfy the equation

$$y^2 = x^3 + ax + b \pmod{p},$$

where $a, b \in F_p$ are constants such that $4a^3 + 27b^2 \neq 0$, together with an infinity point O. The elliptic curve G can form a cyclic group under the point addition operation $R = P + Q$ which is defined according to a chord-andtangent rule. Particularly, we define $x \cdot P = P + P + \cdots + P$ (x times).

2.2 General security notions of digital signature scheme

As mentioned previously, a digital signature scheme must satisfy unforgeability. But what is its concrete meaning? Here, we list all types of forgeries of signature schemes (ordered by their risk) [4].

1) The most serious attack on a signature scheme is called *total break*, which means an adversary can obtain the secret key of the signer.

2) *Universal forgery* means an adversary can construct an efficient algorithm functionally equivalent to the signing algorithm of the signature scheme.

3) *Selective forgery* means an adversary can forge a signature for a particular message chosen by himself.

4) *Existential forgery* means an adversary can forge a signature for at least one message, but the adversary cannot control over the message whose signature he obtains.

3 Review of Chakraborty-Mehta blind signature scheme

In this section, we briefly review Chakraborty-Mehta blind signature scheme.

Let G be a elliptic curve group and P be a generator of G with order q. The Chakraborty-Mehta blind signature scheme runs as follows.

Setup. On input G, P and q, the algorithm outputs a cryptographic hash function $h : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. The signer chooses $x \in \mathbb{Z}_q^*$ uniformly at random and sets $(Q = xP, x)$ as its public/secret key pair.

Blind. The user with message M wants to get a blind signature on M. He first computes $m = h(M)$ and $r = mQ$, then sends r to the signer.

Sign. On input r and the secret key x, the signer does the following steps:

1) Compute $r' = x^{-1}r = mP$.
2) Generate a stamp of the blind signature $z = \langle nounce \| date \| place \rangle$.
3) Compute $R = r' + h(z)P$ and $s = x - h(z)$.
4) Output the signature (R, s, z).

Verify. On input the message M and the signature (R, s, z), the verifier accepts the signature if and only if the equality $sP - Q + R = h(M)P$ holds.

The correctness of the scheme can be verified as follows.

$$\begin{aligned} & sP - Q + R \\ = \;& (x - h(z))P - Q + r' + h(z)P \\ = \;& xP - Q + r' \\ = \;& r' \\ = \;& h(M)P \end{aligned}$$

4 Cryptanalysis of Chakraborty-Mehta signature scheme

In this section, we show two simple but powerful attacks on Chakraborty-Mehta signature scheme. The first attack is a total break of their signature scheme and the second attack is a universal forgery.

4.1 Attack 1

Suppose that a malicious user $\mathcal{A}$ wants to get the signer's secret key x, then he can do the following steps:

1) $\mathcal{A}$ queries a blind signature on message M. Then the signer will compute and output a signature (R, s, z) as a response.

2) After receiving the signature (R, s, z), $\mathcal{A}$ computes $h(z)$.

3) Finally, $\mathcal{A}$ obtains the signer's secret key $x = s + h(z)$.

According to the algorithm **Sign** of Section 3, we know that $s = x - h(z)$. By the above process, we can see that the user $\mathcal{A}$ will obtain the signer's secret key x. Thus, the attack 1 will be successful. Then the user $\mathcal{A}$ armed with the signer's secret key x will be able to generate valid signatures on any messages.

4.2 Attack 2

Suppose that a malicious user $\mathcal{A}$ wants to get a valid signature on message M, then he can do the following steps:

1) $\mathcal{A}$ first produces a stamp of the signature $z = \langle nounce \| date \| place \rangle$.

2) Then $\mathcal{A}$ computes $h(z)$ and $h(M)$.

3) $\mathcal{A}$ selects $s \in \mathbb{Z}_q^*$ uniformly at random.

4) Finally, $\mathcal{A}$ computes $R = h(M)P + Q - sP$, where Q is the signer's public key.

The forged signature on M is (R, s, z). We can see that

$$sP - Q + R = sP - Q + h(M)P + Q - sP = h(M)P.$$

Therefore, the signature (R, s, z) will pass the the verifier's checking. That is, the signature (R, s, z) forged by $\mathcal{A}$ is valid.

5 Conclusion

In this paper, we have analyzed a new blind signature scheme proposed by Chakraborty and Mehta. We presented two simple but very powerful attacks on their scheme. The results show that Chakraborty-Mehta signature scheme is vulnerable and insecure.

Acknowledgements

Miaomiao Tian and Zhili Chen are supported by the National Grand Fundamental Research 973 Program of China (No. 2011CB302905), the National Natural Science Foundation of China (No. 61202407), the Fundamental Research Funds for the Central Universities (No. WK0110000033), and the Scientific and Technical Plan of Suzhou (No. SYG201010). Youwen Zhu is supported by the JSPS Postdoctoral Fellowship (No. P12045).

References

[1] J. Camenisch, J. Piveteau, and M. Stadler, "Blind signatures based on the discrete logarithm problem," in *Eurocrypt '94*, LNCS 950, pp. 428–432, Springer-Verlag, 1995.

[2] K. Chakraborty and J. Mehta, "A stamped blind signature scheme based on elliptic curve discrete logarithm problem," *International Journal of Network Security*, vol. 14, no. 6, pp. 316–319, 2012.

[3] D. Chaum, "Blind signatures for untraceable payments," in *Crypto '82*, pp. 199–203, 1983.

[4] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptative chosen-message attacks," *SIAM Journal of Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[5] I. Lin, M. Hwang, and C. Chang, "Security enhancement for anonymous secure e-voting over a network," *Computer Standards and Interfaces*, vol. 25, no. 2, pp. 131–139, 2003.

[6] T. Okamoto, "Efficient blind and partially blind signatures without random oracles," in *The 3rd Theory of Cryptography Conference*, LNCS 3876, pp. 80–99, Springer-Verlag, 2006.

[7] M. Rückert, "Lattice-based blind signatures," in *Asiacrypt '10*, LNCS 6477, pp. 413–430, Springer-Verlag, 2010.

[8] F. Rodríguez-Henríquez, D. Ortiz-Arroyo, and C. García-Zamora, "Yet another improvement over the Mu-Varadharajan e-voting protocol," *Computer Standards and Interfaces*, vol. 29, no. 4, pp. 471–480, 2007.

Miaomiao Tian is a Ph.D. student in School of Computer Science and Technology at University of Science and Technology of China. His research interests include cryptography and information security.

Youwen Zhu is currently a postdoctoral fellow at Kyushu University, Fukuoka, Japan. He received the B.A. in science communication in 2007 and Ph.D. degree in computer science in 2012, respectively, both from University of Science and Technology of China. His research interests include applied cryptography, network security, secure outsourcing and privacy preservation in cloud computing, and distributed computation.

Zhili Chen received his Ph.D. degree in computer science from University of Science and Technology of China in 2009. He is currently a postdoctoral fellow of School of Computer Science and Technology at University of Science and Technology of China. His research interests include information security and information hiding.