Breaking A Proxy Signature Scheme From Lattices

Miaomiao Tian and Liusheng Huang
(Corresponding author: Miaomiao Tian)

School of Computer Science and Technology, University of Science and Technology of China
Hefei 230026, P.R. China (Email: miaotian@mail.ustc.edu.cn)

(Received Dec. 07, 2011; revised and accepted Feb. 01, 2012)

Abstract

A proxy signature scheme allows a proxy signer to sign messages on behalf of an original signer. Proxy signature schemes have found numerous practical applications such as grid computing, mobile agent systems and cloud applications. Recently, Jiang et al. proposed the first lattice-based proxy signature scheme and claimed that their scheme provides all the security properties of a secure proxy signature scheme. However, in this paper, we disprove their claim and show that an original signer is able to forge a proxy signature on any message. Finally, we also discuss other possible alternative schemes.

Keywords: Cryptanalysis, proxy signature, lattices

1 Introduction

Lattices are currently enjoying great interest in cryptography, due to provable security reductions and implementation simplicity. Furthermore, lattice-based cryptography is believed to be secure even in the quantum era. Up to now, a number of lattice-based signature schemes have been constructed including proxy signatures [2, 4, 5, 6, 11, 12, 13].

The concept of proxy signature was introduced by Mambo *et al.* [9] in 1996. Proxy signatures allow an original signer to delegate a proxy signer to sign messages on its behalf. Proxy signature schemes have found numerous practical applications such as grid computing [3] and mobile agent systems [7, 10]. There are three types of delegation in proxy signatures, i.e., full delegation, partial delegation and delegation by warrant. Partial delegation also covers proxy-unprotected proxy signature and proxy-protected proxy signature. In a proxy-protected proxy signature scheme only the proxy signer is able to generate a valid proxy signature, while in a proxy-unprotected proxy signature scheme either the proxy signer or the original signer can generate a valid proxy signature on a message. Obviously, the proxy-protected proxy signature schemes are more interesting since they avoid the potential disputes between the original signer and the proxy signer. Recently, Jiang et al. [6] presented the first proxy signature scheme from lattices. They claimed that their scheme is a secure proxy-protected proxy signature scheme. Unfortunately, in this paper, we show that an original signer is able to forge a proxy signature on any message. Other possible alternative schemes are also discussed.

The remainder of this paper is organized as follows. Section 2 introduces some preliminaries needed in this paper. In Section 3, we review Jiang et al.'s lattice-based proxy signature scheme. Two attacks and possible improvements on their scheme will be presented in Section 4. Finally, Section 5 concludes this paper.

2 Preliminaries

For a positive integer d, $[d]$ denotes the set $\{1, \cdots, d\}$. For a string s, we refer to $|s|$ as its length. For a matrix $A = [a_1, \cdots, a_m] \in \mathbb{Z}^{n \times m}$, let $\widetilde{A}$ denote its Gram-Schmidt orthogonalization. Define $||A|| = \max_{i \in [m]} ||a_i||$, where $|| \cdot ||$ is the ℓ_2 norm. The function $\text{negl}(n)$ is negligible in n if it vanishes faster than all polynomial fractions for large n.

Let X and Y be two distributions over some finite set F. The *statistical distance* between them is defined as $\Delta(X; Y) = \max_{e \in F} |X(e) - Y(e)|$. We say that X and Y are statistically close if $\Delta(X; Y) \leq \text{negl}(n)$.

2.1 Lattices and Discrete Gaussian

In this work, we are concerned only with m-dimensional integer lattices.

Definition 2.1. *Let a basis $B = [b_1, \ldots, b_m] \in \mathbb{Z}^{m \times m}$ consist of m-linearly independent vectors. The lattice generated by B is defined as*

$$\Lambda = \mathcal{L}(B) = \{Bc : c \in \mathbb{Z}^m\}.$$

For a positive integer q, a matrix $A \in \mathbb{Z}^{n\times m}$ and a vector $y \in \mathbb{Z}_q^n$, the following two sets will be heavily used in this paper. The first set is a lattice and the other one is its generalization.

$$\Lambda^{\perp}(A) = \{e \in \mathbb{Z}^m : Ae = 0 \pmod q\}$$

$$\Lambda^{y}(A) = \{e \in \mathbb{Z}^m : Ae = y \pmod q\}.$$

Definition 2.2. *For any $\sigma > 0$, the Gaussian function on $\mathbb{R}^m$ centered at c with parameter σ is*

$$\rho_{\sigma,c}(x) = \exp(-\pi||x-c||^2/\sigma^2)$$

The discrete Gaussian distribution over Λ with center c and parameter σ is

$$\forall x \in \Lambda, \quad D_{\Lambda,\sigma,c} = \rho_{\sigma,c}(x)/\rho_{\sigma,c}(\Lambda).$$

2.2 Hardness Assumption

Security of Jiang et al.'s scheme is based on the hardness of the short integer solution (SIS) problem [1] which is described as follows.

Definition 2.3. *Given a positive integer q, a real β and a matrix $A \in \mathbb{Z}_q^{n\times m}$, the short integer solution problem (q, m, β)-SIS is: find a non-zero vector $e \in \Lambda^{\perp}(A)$ such that $||e|| \le \beta$.*

Micciancio and Regev [8] showed that, for appropriate parameters, solving SIS on the average is as hard as approximating certain lattice problems in the worst case.

2.3 Trapdoor Functions and Lattice Basis Delegation

Let $A \in \mathbb{Z}_q^{n\times m}$ be a uniformly random matrix. Gentry *et al.* [4] introduced an one-way function $f_A(x) = Ax \pmod q$ with domain $D_n = \{e \in \mathbb{Z}^m : ||e|| \le \sigma\sqrt{m}\}$ and showed how to use a trapdoor to sample a preimage of any element in $\mathbb{Z}_q^n$. Some facts about this kind of function are listed below.

Theorem 2.1. *Let $q \ge 3$ and $m \ge 6n\log q$, there is a probabilistic polynomial-time (PPT) algorithm **TrapGen**(1^n) that outputs a matrix $A \in \mathbb{Z}_q^{n\times m}$ statistically close to uniform and a basis T_A for $\Lambda^{\perp}(A)$ satisfying $||\widetilde{T_A}|| \le O(\sqrt{n\log q})$ with overwhelming probability.*

Lemma 2.1. *Let $q \ge 3$ and $m > 5n\log q$. Let $A \in \mathbb{Z}_q^{n\times m}$, T_A be a basis for $\Lambda^{\perp}(A)$ and $\sigma \ge \|\widetilde{T_A}\| \cdot \omega(\sqrt{\log m})$. Then for any $y \in \mathbb{Z}_q^n$, there is a PPT algorithm **SamplePre**(A, T_A, σ, y) that outputs a vector $e \in \Lambda^y(A)$ such that $||e|| \le \sigma\sqrt{m}$ with all but negl(n) probability.*

From Lemma 2.1, we can see that a short basis T_A for $\Lambda^{\perp}(A)$ is a trapdoor of f_A. In 2010, Cash *et al.* [2] presented a lattice basis delegation algorithm. Here we show one of their findings which will be used in this work.

Lemma 2.2. *Let $A_1, A_2 \in \mathbb{Z}_q^{n\times m}$ and T_{A_1} be a basis of $\Lambda^{\perp}(A_1)$. The algorithm **ExtBasis**$(T_{A_1}, A = A_1||A_2)$ takes as input T_{A_1}, A_1 and A_2, and outputs a short basis T_A for $\Lambda^{\perp}(A)$ such that $||\widetilde{T_A}|| = ||\widetilde{T_{A_1}}||$.*

2.4 Proxy Signature Scheme

A proxy signature scheme is specified by the following four algorithms:

Setup. This algorithm takes as input a security parameter n and outputs the system public parameters PP. And the original signer S_o selects its key pair (pk_o, sk_o) and the proxy signer S_p selects its key pair (pk_p, sk_p), respectively.

Proxy generation. This algorithm takes as input the private keys sk_o and sk_p. It outputs a proxy secret key psk for the proxy signer S_p.

Proxy sign. This algorithm takes as input the proxy secret key psk and a message m. It outputs a proxy signature θ.

Proxy verify. This algorithm takes as input a proxy signature θ on the massage m and outputs 1 if the signature is valid. Otherwise, it outputs 0.

A secure proxy signature scheme should fulfill the following properties [7, 9]:

Verifiability. From proxy signatures, a verifier can be convinced of the original signer's agreement on the signed messages.

Strong unforgeability. Only the proxy signer can produce a valid proxy signature on behalf of the original signer.

Strong identifiability. Anyone can determine the identity of the corresponding proxy signer from a proxy signature.

Strong undeniability. Once the proxy signer creates a valid proxy signature on behalf of the original signer, he cannot repudiate his signature creation against anyone else.

Prevention of misuse. The proxy signer cannot use the proxy key for other purposes than generating a valid proxy signature.

3 Review of Jiang et al.'s Proxy Signature Scheme from Lattices

In this section, we briefly review Jiang et al.'s lattice-based proxy signature scheme [6], which is stated as follows:

Setup. Given a security parameter n, the PKG picks a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^n$, a prime $q \geq 3$ and $m \geq 6n \log q$. The original signer runs $\mathbf{TrapGen}(1^n)$ twice to generate two matrices $A_1, A_2 \in \mathbb{Z}_q^{n\times m}$ and the corresponding short bases $T_{A_1}, T_{A_2} \in \mathbb{Z}_q^{m\times m}$ for $\Lambda^{\perp}(A_1)$ and $\Lambda^{\perp}(A_2)$, respectively. The system public parameters is $PP = (n, q, m, A_1, A_2, H)$ and the original signer's key pair is (A_1, T_{A_1}).

Proxy generation. The original signer sends T_{A_2} to the proxy signer via a secure channel. The proxy signer then runs ExtBasis$(T_{A_2}, A = A_1||A_2)$ to generate a basis T_A for $\Lambda^{\perp}(A)$. The public key of the proxy signer is A.

According to Lemma 2.2, we know that $||\widetilde{T_A}|| = ||\widetilde{T}_{A_2}||$. Therefore, T_A is short and is suited as a private key of the proxy signer.

Proxy sign. Given $\sigma \geq \|\widetilde{T_A}\| \cdot \omega(\sqrt{\log 2m})$, a new message $M \in \{0,1\}^*$ and the key pair (A, T_A), the proxy signer runs $\mathbf{SamplePre}(A, T_A, \sigma, H(M))$ to generate a signature θ such that $A\theta = H(M) \pmod q$.

Proxy verify. Given the system parameters PP, a proxy signature θ and a massage M, the verifier accepts the signature if and only if $A\theta = H(M) \pmod q$ and $||\theta|| \leq \sigma\sqrt{m}$.

Correctness. By Lemma 2.1, we know that the signature θ satisfies $A\theta = H(M) \pmod q$ and $||\theta|| \leq \sigma\sqrt{m}$ with 1−negl(n) probability.

4 Cryptanalysis of Jiang et al.'s Proxy Signature Scheme

In this section we will show that Jiang et al.'s proxy signature scheme is insecure and discuss other alternative schemes.

The following two simple attacks show that Jiang et al.'s proxy signature scheme is not secure:

Attack 1. To sign a message M', the original signer runs ExtBasis$(T_{A_1}, A = A_1||A_2)$ to generate a short basis T'_A for $\Lambda^{\perp}(A)$. According to Lemma 2.2, we know that T'_A is also short. Then the original signer runs $\mathbf{SamplePre}(A, T'_A, \sigma, H(M'))$ to generate a signature θ' such that $A\theta' = H(M') \pmod q$. By Lemma 2.1, we can see that the signature θ' satisfies $A\theta' = H(M') \pmod q$ and $||\theta'|| \leq \sigma\sqrt{m}$ with 1−negl(n) probability. Therefore, the original signer creates a valid proxy signature on M'.

Attack 2. As we know, the original signer also has the value of T_{A_2}. Therefore, he can also create a valid proxy signature on any message according to the signing algorithm in Section 3. That is Jiang et al.'s proxy signature scheme is insecure and does not satisfy strong unforgeability and strong undeniability.

To prevent the second attack, we can change the **Setup** algorithm simply. Specifically, the original signer and the proxy signer can generate (A_1, T_{A_1}) and (A_2, T_{A_2}), respectively. However, in this case, similar to the first attack process, both the original signer and the proxy signer is able to independently produce a valid proxy signature on any message. In other words, the modified proxy signature scheme will violate verifiability, strong unforgeability and strong undeniability. Therefore, the modified proxy signature scheme is also insecure.

Of course, we are indeed able to construct a secure lattice-based proxy signature scheme by using the following approach.

1) An original signer with key pair (A_1, T_{A_1}) can sign a delegation warrant W which records the delegation police and the identities of the original signer and the proxy singer. Concretely, the original signer runs $\mathbf{SamplePre}(A_1, T_{A_1}, \sigma, H(W))$ to generate a signature θ such that $A_1\theta = H(W) \pmod q$ and $||\theta|| \leq \sigma\sqrt{m}$.
2) To sign message M, the proxy signer with key pair (A_2, T_{A_2}) runs $\mathbf{SamplePre}(A_2, T_{A_2}, \sigma, H(M||W))$ to generate a signature ϑ such that $A_2\vartheta = H(M||W) \pmod q$ and $||\vartheta|| \leq \sigma\sqrt{m}$. The proxy signature is (θ, ϑ).
3) Verifiers check $A_1\theta = H(W) \pmod q$, $||\theta|| \leq \sigma\sqrt{m}$, $A_2\vartheta = H(M||W) \pmod q$ and $||\vartheta|| \leq \sigma\sqrt{m}$.

It's clear that the new lattice-based proxy signature is secure, but it's trivial. As a result, it's fair to say that constructing a secure and non-trivial lattice-based proxy signature scheme is not an easy task.

5 Conclusion

Recently, Jiang et al. [6] presented the first lattice-based proxy signature scheme. In this paper, we have demonstrated that Jiang et al.'s proxy signature scheme is insecure. We have also discussed other possible alternatives and have indicated that constructing a secure and non-trivial proxy signature scheme from lattices is an open problem.

Acknowledgements

This work is supported by the Major Research Plan of the National Natural Science Foundation of China (No. 90818005) and the National Natural Science Foundation of China (No. 60903217).

References

[1] M. Ajtai, "Generating hard instances of lattice problems," *STOC 1996*, pp. 99–108, 1996.

[2] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai Trees, or How to Delegate a Lattice Basis," *Eurocrypt 2010*, LNCS 6110, Springer-Verlag, pp. 523–552, 2010.

[3] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke, "A security architecture for computational grids," *The 5th ACM Conference on Computers and Communications Security*, pp. 83–92, 1998.

[4] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for Hard Lattices and New Cryptographic Constructions," *STOC 2008*, pp. 197–206, 2008.

[5] D. Gordon, J. Katz, and V. Vaikuntanathan, "A group singnature scheme from lattice assumptions," *Asiacrypt 2010*, LNSC 6477, Springer-Verlag, pp. 395–412, 2010.

[6] Y. Jiang, F. Kong, and X. Ju, "Lattice-based Proxy Signature," *The 6th International Conference on Computational Intelligence and Security*, pp. 382-385, 2010.

[7] B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its applications," *Proceedings of Symposium on Cryptography and Information Security*, pp. 603–608, 2001.

[8] D. Micciancio, and O. Regev, "Worst-case to average-case reductions based on gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007.

[9] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature for delegating signing operation," *The 3rd ACM Conference on Computer and Communications Security*, pp. 48–57, 1996.

[10] H. Park, and I. Lee, "A digital nominative proxy signature scheme for mobile communication," *The 3rd International Conference on Information and Communications Security*, LNCS 2229, Springer-Verlag, pp. 451–455, 2001.

[11] M. Rückert, "Lattice-based Blind Signatures," *Asiacrypt 2010*, LNSC 6477, Springer-Verlag, pp. 413–430, 2010.

[12] M. Rückert, "Strongly unforgeable signatures and hierarchical identitybased signatures from lattices without random oracles," *PQCrypto 2010*, LNCS 6061, Springer-Verlag, pp. 182–200, 2010.

[13] M. Tian, L. Huang, and W. Yang, "A new hierarchical identity-based signature scheme from lattices in the standard model," *International Journal of Network Security*, In Press.

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.

Liusheng Huang is a professor in School of Computer Science and Technology at University of Science and Technology of China. His research interests include information security, wireless sensor network and distributed computing. He is author or coauthor of more than 100 research papers and 6 books.