Cryptanalysis on ‘An efficient identity-based proxy signcryption using lattice’

Zi-Yuan Liu, Yi-Fan Tseng, Raylin Tso*

Department of Computer Science, National Chengchi University, Taipei 11605, Taiwan
{zyliu, yftseng, raylin}@cs.nccu.edu.tw

March 18, 2021

Abstract

In this note, we conduct a cryptanalysis of the paper published by Zhu *et al.* on Future Generation Computer Systems in 2021. We demonstrate that their quantum-resistant identity-based proxy signcryption scheme cannot achieve the confidentiality as they claimed.

Keywords— Cryptanalysis, Identity-based, Proxy signcryption, Lattice-based cryptosystem

1 Introduction

Identity-based proxy signcryption (IDPSC), at a high level, combines the benefits and capabilities of identity-based cryptography [JN09], proxy signature [MUO96], and signcryption [Zhe97] in the same time.

Zhu *et al*. [ZWWC21] recently introduced the first quantum-resistant IDPSC based on lattices and claimed that the scheme achieves confidentiality under the lattice hard assumption–learning with error assumption. That is, it remains secure from the indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2).

In this note, we first point out the flaws of the security proof in [ZWWC21], and then demonstrate how an adversary can break the confidentiality to obtain the plaintext without using any private information.

The remainder of this note is organized as follows: Section 2 provides preliminaries. Section 3 introduces the system model and security requirement of IDPSC. Section 4 describes the IDPSC scheme proposed by Zhu *et al*. Section 5 points out the flaws in security proof and provides a cryptanalysis to Zhu *et al*.’s scheme. Finally, Section 6 concludes this note.

2 Preliminaries

2.1 Notations

Let $\mathbb{Z}$ and $\mathbb{R}$ denotes a set of integer and real, respectively. For prime q, $\mathbb{Z}_q$ denotes a finite field (or Galois field) with order q. For an element e and finite set S, $e \leftarrow S$ indicates that e is selected uniformly and randomly from S. Finally, for a vector v, $\|v\|$ represents the l_2 norm of v.

2.2 Lattice and discrete Gaussian distribution

Given $n, m, q \in \mathbb{Z}$, $A \in \mathbb{Z}_q^{n\times m}$, and $u \in \mathbb{Z}_q^n$, two lattices and a coset are defined as follows:

- $\Lambda_q(A) := \{y \in \mathbb{Z}_q^m \mid \exists z \in \mathbb{Z}_q^n, y = A^\top z \bmod q\}$;

*Corresponding author

- $\Lambda_q^{\perp}(A) := \{e \in \mathbb{Z}_q^m \mid Ae = 0 \bmod q\}$;
- $\Lambda_q^{u}(A) := \{e \in \mathbb{Z}^m \mid Ae = u \bmod q\}$.

We define the Gaussian function on $\Lambda \subset \mathbb{Z}^n$ centered at $c \in \mathbb{R}^n$ with parameter real $s > 0$ as follows:

$$\forall x \in \Lambda, \;\; \rho_{s,c}(x) := \exp\left(-\pi \frac{\|x-c\|^2}{s^2}\right).$$

Let $\rho_{s,c}(\Lambda) := \sum_{x\in\Lambda} \rho_{s,c}(x)$, we can further define the discrete Gaussian distribution over Λ with center $c \in \mathbb{R}^n$ and parameter $s > 0$ as:

$$\forall y \in \Lambda, \;\; D_{\Lambda,s,c}(y) := \frac{\rho_{s,c}(y)}{\rho_{s,c}(\Lambda)}.$$

For convenience, we omit s and c when $s = 1$ and $c = 0$, respectively.

2.3 Hard assumption and useful theorems

Definition 1 (Learning with errors (LWE) assumption [Reg05, Reg09]). *Let $n \in \mathbb{Z}, q = q(n)$, and $\alpha > 0$. Define $A_{s,\alpha} \subseteq \mathbb{Z}_q^n \times \mathbb{Z}_q$ as the distribution of the tuple $(a, a^{\top}s + x)$, where $a \leftarrow \mathbb{Z}_q^n, x \leftarrow D_{\mathbb{Z}^n,\alpha}$. Given m samples from $A_{s,\alpha}$ generated from the same $s \leftarrow \mathbb{Z}_q^n$, the search version of LWE problem is to output s.*

Theorem 1 (Rejection sampling [Lyu12]). *Let $V \subset \mathbb{Z}^m$ where the norms of all elements are less than some T, $\sigma = \omega(T\sqrt{\log m})$ be a real, $\psi : V \to \mathbb{R}$, and $M = O(1)$. Then, the distribution of the algorithm $Samp_1$ is within statistical distance $\frac{2^{-\omega(\log m)}}{M}$ from the distribution of the algorithm $Samp_2$.*
$Samp_1$:

- $c \leftarrow \psi$;
- $z \leftarrow D_{\mathbb{Z}^m,\alpha,c}$;
- *outputs* (c, z) *with probability* $\min\left(\frac{D_{\mathbb{Z}^m,\alpha}(z)}{MD_{\mathbb{Z}^m,\alpha,c}(z)}\right)$.

$Samp_2$:

- $c \leftarrow \psi$;
- $z \leftarrow D_{\mathbb{Z}^m,\alpha}$;
- *outputs* (c, z) *with probability* $1/M$.

Theorem 2 (Gaussian sample preimage [GPV08] and matrix [TH16]). *Given a matrix $A \in \mathbb{Z}_q^{n\times m}$, basis $B \in \mathbb{Z}_q^{m\times m}$ of $\Lambda_q^{\perp}(A)$, vector $u \in \mathbb{Z}_q^n$, and parameter $s \geq \|\tilde{B}\| \cdot \omega(\sqrt{\log m})$, there is an algorithm $SamplePre(A, B, s, u) \to v \in \mathbb{Z}^m$ such that $Av = u$ and the distribution of v is statistically close to $D_{\mathbb{Z}^m,s}$. Then, given a matrix $U = [U_1|\cdots|U_k] \in \mathbb{Z}_q^{n\times k}$, there is another algorithm $SampleMat(A, B, s, U) \to V \in \mathbb{Z}^{m\times k}$ that, for $i = 1, \cdots, k$, calls $SamplePre(A, B, s, U_i) \to V_i$ such that $AV = U$, where $V = [V_1|\cdots|V_k]$.*

3 System model and security requirement of IDPSC

Here, we recall the system and security requirement of IDPSC defined in [ZWWC21]. An IDPSC consists of three entities: original-signcrypter $\mathcal{O}$, proxy-signcrypter $\mathcal{P}$, and unsigncrypter $\mathcal{R}$, and along with six polynomial-time algorithms described as follows:

- $ST(1^{\lambda}) \to (parms, mk)$: This algorithm takes a security parameter λ as its input and outputs system parameters $parms$, and a master-key mk.
- $EX(parms, mk, id_i) \to sk_{id_i}$: This algorithm takes the system parameters $parms$, the master-key mk, and an identity id_i as its inputs and outputs identity id_i's private key sk_{id_i}.

- $DG(parms, id_{\mathcal{O}}, sk_{id_{\mathcal{O}}}, \omega) \to \eta$: This algorithm is executed by the original-signcrypter that takes the system parameters $parms$, $\mathcal{O}$'s identity $id_{\mathcal{O}}$, $\mathcal{O}$'s private key $sk_{id_{\mathcal{O}}}$, and a warrant ω as its inputs and outputs a warrant-signature η to the proxy signcrypter.

- $PSK(parms, \eta, id_{\mathcal{P}}, sk_{id_{\mathcal{P}}}) \to sk_{\mathcal{P}}$: This algorithm is executed by the proxy-signcrypter that takes the system parameters $parms$, a warrant-signature η, and $\mathcal{P}$'s identity $id_{\mathcal{P}}$ and the corresponding private key $sk_{id_{\mathcal{P}}}$ as its inputs and outputs a proxy signcrypted private key $sk_{\mathcal{P}}$ for warrant ω.

- $PSC(parms, id_{\mathcal{R}}, t, sk_{\mathcal{P}}) \to \delta$: This algorithm is executed by the proxy-signcrypter that takes the system parameters $parms$, $\mathcal{R}$'s identity $id_{\mathcal{R}}$, a message t, and a proxy signcrypted private key $sk_{\mathcal{P}}$ as its inputs and outputs a ciphertext δ on message t.

- $US(parms, id_{\mathcal{P}}, sk_{id_{\mathcal{R}}}, \delta, \eta) \to t/\perp$: This algorithm is executed by the unsigncrypter that takes the system parameters $parms$, $\mathcal{P}$'s identity $id_{\mathcal{P}}$, $\mathcal{R}$'s private key $sk_{id_{\mathcal{R}}}$, a ciphertext δ, and a warrant-signature η as its inputs and outputs a message t or a reject symbol $\perp$.

Similar to a common signcryption schemes [Zhe97], IDPSC must satisfy confidentiality to ensure that there is no adversary can obtain any information from the ciphertext. This property is modeled by the following IND-CCA2 game that is interacted between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$:

Game IND-CCA2:

- **Initialization**: After inputting a security parameter λ, $\mathcal{C}$ executes $ST(1^{\lambda})$ to generate system parameters $parms$ and the master-key mk. Finally, $\mathcal{C}$ sends $parms$ to $\mathcal{A}$ and keeps mk secret.

- **Phase 1**: In this phase, $\mathcal{A}$ is allowed to adaptively perform a polynomial-time bounded query to the following oracles:
  - **Extraction oracle**: $\mathcal{A}$ can issue this oracle with an identity id to $\mathcal{C}$, $\mathcal{C}$ returns id's private key $sk_{id} \leftarrow EX(parms, mk, id)$ to $\mathcal{A}$.
  - **Delegation oracle**: $\mathcal{A}$ can issue this oracle with a warrant ω, a proxy identity $id_{\mathcal{P}}$, and an original identity $id_{\mathcal{O}}$ to $\mathcal{C}$, $\mathcal{C}$ returns a warrant-signature $\eta \leftarrow DG(parms, id_{\mathcal{O}}, sk_{id_{\mathcal{O}}}, \omega)$ to $\mathcal{A}$, where $sk_{id_{\mathcal{O}}}$ is generated by running $EX(parms, mk, id_{\mathcal{O}})$.
  - **Proxy secret key oracle**: $\mathcal{A}$ can issue this oracle with a warrant-signature η, and a proxy identity $id_{\mathcal{P}}$ to $\mathcal{C}$, $\mathcal{C}$ returns a proxy signcrypted private key $sk_{\mathcal{P}} \leftarrow PSK(parms, \eta, id_{\mathcal{P}}, sk_{id_{\mathcal{P}}})$ to $\mathcal{A}$, where $sk_{id_{\mathcal{P}}}$ is generated by running $EX(parms, mk, id_{\mathcal{P}})$.
  - **Signcryption oracle**: $\mathcal{A}$ can issue this oracle with a unsigncrypter's identity $id_{\mathcal{R}}$, a message t, and a proxy-signcrypter's identity $id_{\mathcal{R}}$ to $\mathcal{C}$, $\mathcal{C}$ returns a ciphertext $\delta \leftarrow PSC(parms, id_{\mathcal{R}}, t, sk_{\mathcal{P}})$ to $\mathcal{A}$.
  - **Unsigncryption oracle**: $\mathcal{A}$ can issue this oracle with a proxy-signcrypter's identity $id_{\mathcal{P}}$, a unsigncrypter's identity $id_{\mathcal{R}}$, a ciphertext δ, and a warrant-signature η to $\mathcal{C}$, $\mathcal{C}$ returns $t/\perp \leftarrow US(parms, id_{\mathcal{P}}, sk_{id_{\mathcal{R}}}, \delta, \eta)$ to $\mathcal{A}$, where $sk_{id_{\mathcal{R}}} \leftarrow EX(parms, mk, id_{\mathcal{R}})$.

- **Challenge**: After **Phase 1**, $\mathcal{A}$ outputs $id^*_{\mathcal{O}}, id^*_{\mathcal{P}}, id^*_{\mathcal{R}}$, and two messages t_0, t_1 with the same length to $\mathcal{C}$, $\mathcal{C}$ first randomly chooses a bit $b \in \{0, 1\}$. Then, $\mathcal{C}$ generates $\eta^* \leftarrow DG(parms, id^*_{\mathcal{O}}, sk_{id^*_{\mathcal{O}}}, w^*)$ for some w^*, $sk^*_{\mathcal{P}} \leftarrow PSK(parms, \eta, id^*_{\mathcal{P}}, sk_{id^*_{\mathcal{P}}})$, $\delta^* \leftarrow PSC(parms, id^*_{\mathcal{R}}, t_b, sk^*_{\mathcal{P}})$, and then returns (η^*, δ^*) to $\mathcal{A}$.

- **Phase 2**: In this phase, $\mathcal{A}$ can keep do as in **Phase 1** with the additional restriction that he/she cannot query $id^*_{\mathcal{R}}$ to **Extraction oracle** and query δ^* to **Unsigncryption oracle**.

- **Guess**: Finally, $\mathcal{A}$ outputs a bit b' as its answer. The advantage of $\mathcal{A}$ is defined as

$$Adv_{\mathcal{A}}^{\text{IND-CCA2}} := \Pr[b = b'] - \frac{1}{2}.$$

Definition 2 (IND-CCA2 security of IDPSC)**.** *An IDPSC scheme is said to be IND-CCA2 secure if there is no probabilistic polynomial-time adversary $\mathcal{A}$ can win the IND-CCA2 game with a non-negligible advantage.*

4 Zhu *et al.*'s IDPSC

In this section, we revisit the IDPSC scheme proposed by Zhu *et al.* [ZWWC21].

- $ST(1^\lambda)$:
    1. choose $q \geq 3$, real M, $m > 5n \log q$, and $k \in \mathbb{N}$ are positive integers.
    2. $\tilde{L} = O(\sqrt{n \log q})$, Gaussian parameter $s = \tilde{L} \cdot \omega(\sqrt{\log n})$, and $\sigma = 12s\lambda m$.
    3. generates $(A \in \mathbb{Z}_q^{n\times m}, B \in \mathbb{Z}_q^{m\times m})$ by using $TrapGen(q, n)$, where $\|\tilde{B}\| \leq \tilde{L}$.
    4. selects three secure cryptographic hash functions:
        - $H : \{0,1\}^* \to \mathbb{Z}_q^k$;
        - $H_1 : \{0,1\}^{\ell_1} \to \mathbb{Z}_q^{n\times k}$;
        - $H_2 : \{0,1\}^* \to \{v : v \in \{-1,0,1\}^k, \|v\|_1 \leq \lambda\}$.
    5. outputs the system parameters and master-key

$$parms := (q, n, m, k, s, \sigma, A, H, H_1, H_2);\ mk := B.$$

- $EX(parms, mk, id_i)$:
    1. runs $S_{id_i} \leftarrow SampleMat(A, B, s, H_1(id_i))$, where $AS_{id_i} = H_1(id_i)$ and $\|S_{id_i}\| \leq s\sqrt{m}$.
    2. outputs identity id_i's private key $sk_{id_i} := S_{id_i}$.

- $DG(parms, id_{\mathcal{O}}, sk_{id_{\mathcal{O}}}, \omega)$:
    1. selects a random $\alpha \leftarrow D_\sigma^m$ and computes $\mu = H_2(A\alpha, \omega)$.
    2. computes $\nu = S_{id_{\mathcal{O}}}\mu + \alpha$.
    3. outputs warrant-signature $\eta := (\omega, \mu, \nu)$ with probability $\min\left(\frac{D_\sigma^m(\nu)}{MD^m_{S_{id_{\mathcal{O}}}\mu,\sigma}(\nu)}\right)$.

- $PSK(parms, \eta, id_{\mathcal{P}}, sk_{id_{\mathcal{P}}})$:
    1. checks whether $\mu = H_2(A\nu - H_1(id_{\mathcal{O}})\mu, \omega)$ and $\|\nu\| \leq 2\sigma\sqrt{m}$.
    2. $S_{\mathcal{P}} \leftarrow SampleMat(A, B, s, H_1(id_{\mathcal{P}}|\nu|\omega|AS_{id_{\mathcal{P}}}))$, where $AS_{\mathcal{P}} = H_1(id_{\mathcal{P}}|\nu|\omega|AS_{id_{\mathcal{P}}})$.
    3. outputs proxy signcrypted private key $sk_{\mathcal{P}} := S_{\mathcal{P}}$.

- $PSC(parms, id_{\mathcal{R}}, t, sk_{\mathcal{P}})$:
    1. random selects $\beta \leftarrow D_\sigma^m$ and computes $\phi = H_2(A\beta, H_1(id_{\mathcal{R}}))$.
    2. computes $\chi = H(\phi, AS_{\mathcal{P}}) \oplus t$.
    3. computes $\xi = S_{\mathcal{P}}\phi + \beta$.
    4. outputs ciphertext tuple $\delta := (\chi, \xi, \phi)$ with probability $\min\left(\frac{D_\sigma^m(\xi)}{MD^m_{S_{\mathcal{P}}\phi,\sigma}(\xi)}\right)$.

- $US(parms, id_{\mathcal{P}}, sk_{id_{\mathcal{R}}}, \delta, \eta)$:
    1. computes $h = H_2(A\xi - H_1(id_{\mathcal{P}}|\nu|\omega|H_1(id_{\mathcal{P}}))\phi, AS_{id_{\mathcal{R}}})$.
    2. computes $t = H(h, H_1(id_{\mathcal{P}}|\nu|\omega|H_1(id_{\mathcal{P}}))) \oplus \chi$.
    3. if $\|\xi\| \leq 2\sigma\sqrt{m}$ and $h = \phi$, outputs t. Otherwise, outputs $\perp$.

5 Cryptanalysis of Zhu *et al.*'s IDPSC

In this section, we first point out the flaw of the security proof in [ZWWC21], and then give a cryptanalysis to show that Zhu *et al.*'s IDPSC cannot resist IND-CCA2 adversary.

5.1 Flaw of the security proof

In the security proof in [ZWWC21], at the beginning, the challenger is given an LWE instance $(\tilde{S}, \tilde{\xi} = \tilde{S}\tilde{\phi} + \tilde{\beta})$. As mentioned in Definition 1, we have $(\tilde{S}, \tilde{\xi}) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$. Then, in the **Challenge** phase, the challenger selects $\phi^* \leftarrow \{0,1\}^*$, $\chi^* \leftarrow \{0,1\}^*$, sets $\xi^* = \tilde{\xi}$, and returns challenged ciphertext tuple (ϕ^*, χ^*, ξ^*) to the adversary. Therefore, ξ^* is a $\mathbb{Z}_q$ element and $\|\xi^*\| \leq q$.

However, as the described in algorithm PSC in Section 4, $\|\xi\|$ is generated from rejection sampling (Theorem 1) and therefore ξ is a m-dimension vector (*i.e.*, $\xi \in \mathbb{Z}^m$) and $\|\xi\|$ is less than $2\sigma\sqrt{m}$.

Therefore, the challenger does not give a perfect simulation, and the adversary can easily distinguish the view given by the challenger from a real scheme.

5.2 Breaking the IND-CCA2 security

Theorem 3. *The confidentiality of Zhu et al.'s IDPSC scheme does not hold.*

Proof. In this proof, we describe how the adversary can distinguish which message t_b, where $b \in \{0,1\}$, is signcrypted by the challenger, without using the private key of unsigncryptor, after receiving the challenged tuple (η^*, δ^*).

The adversary performs as follows:

1. parses $\eta^* = (\omega^*, \mu^*, \nu^*)$ and $\delta^* = (\chi^*, \xi^*, \phi^*)$.
2. computes $t^* = H(\phi^*, H_1(id_{\mathcal{P}}^*|\nu^*|\omega^*|H_1(id_{\mathcal{P}}^*))) \oplus \chi^*$.
3. if $t^* = t_0$, returns $b' = 0$. Otherwise, returns $b' = 1$.

The following we analyze why the attack work. Because

$$\begin{aligned}
t^* &= H\left(\phi^*, H_1(id_{\mathcal{P}}^*|\nu^*|\omega^*|H_1(id_{\mathcal{P}}^*))\right) \oplus \chi^* \\
&= H(\phi^*, H_1(id_{\mathcal{P}}^*|\nu^*|\omega^*|AS_{id_{\mathcal{P}}^*})) \oplus \chi^* \\
&= H(\phi^*, AS_{\mathcal{P}})) \oplus \chi^* \\
&= t_b \oplus \chi^* \oplus \chi^* \\
&= t_b.
\end{aligned}$$

□

6 Conclusion

In this note, we give a cryptanalysis on the identity-based proxy signcryption scheme proposed by Zhu *et al.* [ZWWC21]. We pointed out the flaw in their security proof in detail and show that their scheme does not satisfy IND-CCA2 security requirement.

Acknowledgment

This research was supported by the Ministry of Science and Technology, Taiwan (ROC), under Project Numbers MOST 108-2218-E-004-001-, MOST 108-2218-E-004-002-MY2, MOST 109-2218-E-011-007-, MOST 109-2221-E-004-011-MY3, and MOST 109-3111-8-004-001-

References

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Cynthia Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 197–206. ACM, 2008.

[JN09] Marc Joye and Gregory Neven, editors. *Identity-based cryptography*, volume 2 of *Cryptology and Information Security Series*. IOS Press, 2009.

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 738–755. Springer, 2012.

[MUO96] Masahiro Mambo, Keisuke Usuda, and Eiji Okamoto. Proxy signatures for delegating signing operation. In Li Gong and Jacques Stearn, editors, *CCS '96, Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Delhi, India, March 14-16, 1996*, pages 48–57. ACM, 1996.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93. ACM, 2005.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.

[TH16] Miaomiao Tian and Liusheng Huang. Identity-based signatures from lattices: Simpler, faster, shorter. *Fundam. Informaticae*, 145(2):171–187, 2016.

[Zhe97] Yuliang Zheng. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption). In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 1997.

[ZWWC21] Hongfei Zhu, Ye Wang, Chonghua Wang, and Xiaochun Cheng. An efficient identity-based proxy signcryption using lattice. *Future Gener. Comput. Syst.*, 117:321–327, 2021.