Future Generation Computer Systems 95 (2019) 100–103

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Cryptoanalysis on 'A round-optimal lattice-based blind signature scheme for cloud services'

Jung Hee Cheon [a], JinHyuck Jeong [a], Ji Sun Shin [b,*]

[a] Seoul National University, Seoul, Republic of Korea
[b] Sejong University, Seoul, Republic of Korea

HIGHLIGHTS

- Zhu et al. proposed a blind signature in Future Generation Computer Systems in 2017.
- Zhu et al.'s is extended from Plantard et al.'s signature scheme in PKC 2008.
- Zhu et al.'s scheme either does not provide the blindness or not correctly work.

ARTICLE INFO

Article history:
Received 26 July 2018
Received in revised form 16 November 2018
Accepted 29 December 2018
Available online 8 January 2019

Keywords:
Blind signatures
Lattice-based cryptosystem
Cryptoanalysis

ABSTRACT

In this note, we review the article published by Zhu et al. in Future Generation Computer Systems in 2017. We show that their construction of a blind signature does not hold the correctness requirement or the blindness requirement.

© 2018 Published by Elsevier B.V.

1. Introduction

In [1], a lattice-based blind signature scheme is proposed by Zhu et al. Their blind signature scheme is extended from Plantard et al.'s digital signature scheme [2] based on the Closest Vector Problem CVP_∞.

1.1. Paper organization

In Section 2, we introduce preliminaries, and in Section 3, we briefly describe the blind signature scheme by Zhu et al.'s [1]. In Section 4, we present our cryptoanalysis on the Zhu et al.'s scheme. In Section 5, we discuss the difficulties of building a provably secure blind signature and future work. Finally, in Section 6, we conclude.

2. Preliminaries

2.1. Blind signature

A blind signature scheme consists of three PPT algorithms, $(KG_\epsilon, SG_\epsilon, VF_\epsilon)$ and involves three entities of the signer $\mathcal{S}$, the user $\mathcal{U}$ and the verifier $\mathcal{V}$. The key generation algorithm KG_ϵ is run by the signer or a trusted authority. The signing algorithm SG_ϵ is run by the signer $\mathcal{S}$ and the user $\mathcal{U}$ interactively. The verification algorithm VF_ϵ is run by the verifier $\mathcal{V}$. The algorithms are defined as follows [1,3].

- KG_ϵ generates secret key k_s and public key k_p.
- $SG_\epsilon(k_s, m)$ executes an interaction between $\mathcal{S}$ and $\mathcal{U}$ where $\mathcal{S}$ has a secret key k_s and $\mathcal{U}$ has a message m. Finally, $\mathcal{U}$ obtains and outputs a signature σ of m.
- $VF_\epsilon(k_p, \sigma, m)$ accepts it if σ is valid, otherwise it rejects it.

Correctness requirement. The correctness requirement is as follows. If k_s, k_p are generated from KG_ϵ, and a signature σ on a message m is generated from $SG_\epsilon(k_s, m)$, then $VF_\epsilon(k_p, \sigma, m)$ accepts it with probability 1. If we allow a negligible error ε, then the correctness requirement holds with probability $1 - \varepsilon$.

Security requirement. A blind signature scheme requires two security properties, blindness and one-more unforgeability [1,3,4]. The blindness captures message hiding from a malicious signer. In particular, a malicious cannot determine which message is queried to sign from the signing execution. The one-more unforgeability captures the inability of the adversary accessing to the signing oracle to obtain one-more valid signature that is not from the

* Corresponding author.
E-mail address: jsshin@sejong.ac.kr (J.S. Shin).

https://doi.org/10.1016/j.future.2018.12.067
0167-739X/© 2018 Published by Elsevier B.V.

signing oracle. In particular, no adversary controlling the user can generate $l+1$ valid signatures given l valid signatures from the signer. For formal definitions, we refer to [1,3,4].

2.2. Notations and definitions [1,2]

We briefly review the notions and definitions from [1,2].

Notations. Let $\lfloor x \rceil$ be rounded down to the closest integer vector of $x \in \mathbb{R}^n$. l_2-norm and l_∞-norm are the Euclidean norm and the infinity norm, respectively. $\|A\|$ and $\|A\|_p$ are the l_2 matrix norm and the l_p matrix norm, respectively. Finally, let $\rho(C)$ denote the spectral radius of C, i.e., $\rho(C) = max\{|\lambda|, Cx = x\lambda\}$ for $C \in \mathbb{C}^{n,n}$. We denote the identity matrix of dimension n by Id_n, or Id simply.

Definition 1 (*l_p-norm*)**.** Let w be a vector of $\mathbb{R}^n$.

1. For $p = \infty$, $\|w\|_\infty$ is defined by $\|w\|_\infty = \max\{|w_i|, \leq i < n\}$.
2. For $p \geq 2$, $\|w\|_p$ is defined by $\|w\|_p = \left(\sum_{i=0}^{n-1} |w_i|^p\right)^{1/p}$.

Definition 2 (***CVP**$_p$*)**.** Let B be a given basis of a lattice $\mathcal{L}$ and w a vector. The Closest Vector Problem (**CVP**) is to find a vector u such that $\|w-u\|_p \leq \|w-v\|_p$ for all $v \in \mathcal{L}$

Moreover, we introduce some definitions and notations related to matrices.

Definition 3 (*Hermite Normal Form, HNF*)**.** Let $\mathcal{L}$ be a full-rank lattice of dimension n with $H = (h_{i,j}) \in \mathbb{R}^n$ a basis. H is a Hermite Normal Form basis of $\mathcal{L}$ if and only if

$$h_{i,j} \begin{cases} = 0 & \text{if } \ i < j \\ \geq 0 & \text{if } \ i \geq j \ \text{ for all } \ 0 \leq i, j < n. \\ < h_{j,j} & \text{if } \ i > j \end{cases}$$

Definition 4 (*Polytope Norm*)**.** Given a non-singular matrix P of dimension n, we define $\|w\|_P = \|wP^{-1}\|_\infty$ for $w \in \mathbb{R}^n$.

3. The blind signature scheme by Zhu et al.

$\mathcal{H}$ is a hash function family mapping $\{0,1\}^* \to \{x \in \mathbb{Z}^n, \|x\|_{P2} < 1\}$. The blind signature scheme $\epsilon = (KG_\epsilon, SG_\epsilon, VF_\epsilon)$ works as follows:

1. KG_ϵ chooses a random hash function h from $\mathcal{H}$ and a random matrix $S \in$. Then, compute $P = \lfloor 2\rho(S)+1 \rceil Id$ and the HNF basis H of $P - S$. Finally, output the public key $k_p = (P, H)$, and the secret key $k_s = S$.
2. SG_ϵ defines the interactive protocol between $\mathcal{U}$ and $\mathcal{S}$ (described in Fig. 1) as follows.
   (a) $\mathcal{U}$ chooses a random $r \leftarrow \{0,1\}^*$
   (b) $\mathcal{U}$ computes $v = h(m,r) \in \mathbb{Z}^n$.
   (c) $\mathcal{U}$ selects a random blinding vector e where e is a linear combination of H and H's integral coefficients are chosen from uniform distribution.
   (d) $\mathcal{U}$ chooses a blinding matrix $T = B^{-1}NB$ where B is generated from H, N is a permutation matrix. T maps a lattice point to another lattice point while keeping the vector's length.
   (e) $\mathcal{U}$ computes $u = (v+e) * T$ and sends it to $\mathcal{S}$.
   (f) $\mathcal{S}$ repeatedly computes $\delta' = u - \lceil uP^{-1} \rfloor (P - S)$ until $\|\delta'\|_P < 1$.
   (g) $\mathcal{S}$ sends δ' to $\mathcal{U}$.
   (h) Finally, upon receiving δ', $\mathcal{U}$ compute $\delta = \delta' * T^{-1} - e$, and outputs the message and signature pair, $\langle m, r, \delta \rangle$.

$\mathcal{S}(S)$		$\mathcal{U}(P,H,m)$
		$v = h(m,r)$
	$\xleftarrow{\quad u \quad}$	$u = (v+e)*T$
repeatedly compute		
$\delta' = u - \lceil uP^{-1} \rfloor (P-S)$		
until $\|\delta'\|_P < 1$	$\xrightarrow{\quad \delta' \quad}$	$\delta = \delta' * T^{-1} - e$
		output signature tuple (m, r, δ)

Fig. 1. The signing procedure in the blind signature scheme proposed by Zhu et al. [1].

3. VG_ϵ verifies δ as follows.
   (a) $\mathcal{V}$ checks if $\|\delta\|_P < 1$. If it is not, rejects it.
   (b) Otherwise, if it is. Then, check if $h(m,r) - \delta$ is a lattice point of $\mathcal{L}$ with basis H. If it is, accept it, otherwise, reject it.

4. Cryptoanalysis on Zhu et al.'s blind signature scheme

4.1. Correctness and blindness

In the Zhu et al.'s blind signature scheme [1], it is argued that the correctness of their blind signature scheme is obvious since their scheme is a variant of Plantard et al.'s signature scheme [2]. However, the final signature δ, unblinded by the user $\mathcal{U}$ is not δ' generated by the signer $\mathcal{S}$. Therefore, even if $\|\delta'\|_P < 1.$, it does not guarantee that $\|\delta\|_P < 1$ where $\delta = (\delta' * T^{-1} - e)$. In particular, if $\|e\|_P$ is larger than or equal to 2, $\|\delta\|_P$ can be larger than 1.

Otherwise, if $\|e\|_P$ is not large enough but smaller than 2, then, the blindness can be broken since given two message-signature pairs (m_0, r_0, δ_0), (m_1, r_1, δ_1), the malicious signer can check which u_i is close to v_j for $i, j \in \{0,1\}$, where $v_j = h(m_j, r_j)$. Since T is length preserving and $\|e\|_P$ is small, $|u_j| = |v_j + e| \approx |v_j|$.

In the next, we formally show our argument described in the above as follows.

Theorem 1. *In Zhu et al.'s blind signature scheme, if $\|e\|_P \geq 2$, the correctness does not hold. Otherwise, if $\|e\|_P < 2$, the blindness property does not hold with non-negligible probability.*

We prove Theorem 1 by showing each case of $\|e\|_P \geq 2$, or $\|e\|_P < 2$. The former yields an incorrect scheme, and the latter breaks the blindness property with non-negligible probability.

Showing incorrectness. We first prove the incorrectness of the scheme in the following theorem.

Theorem 2. *Suppose that $\|\delta'\|_P < 1$ and T is a linear transformation preserving the norm $\| \|_P$, that is, $\|\mathbf{v} * T\|_P = \|\mathbf{v}\|_P$ for every vector $\mathbf{v} \in \mathbb{Z}^n$. If $\|e\|_P \geq 2$, then $\|\delta\|_P \geq 1$ where $\delta = \delta' * T^{-1} - e$.*

Proof. The proof is easily done using the triangle inequality.

$$\begin{aligned} \|\delta\|_P &= \|\delta' * T^{-1} - e\|_P \\ &\geq \left| \|\delta' * T\|_P - \|e\|_P \right| = \left| \|\delta'\|_P - \|e\|_P \right| > 2 - 1 \geq 1. \quad \square \end{aligned}$$

Breaking the blindness property. As shown in Theorem 2, to guarantee the correctness of Zhu et al.'s scheme, $\|e\|_P$ must be smaller than 2. However, this bound on e leads the blindness to be totally broken. We show it formally in the next.

Lemma 1.

1. *If $\|e\|_P < 2$ and $P = \lfloor 2\rho(S)+1 \rceil Id$, then $\|e\|_\infty < 2\left(\lfloor 2\rho(S)+1 \rceil\right)$*

2. *If* $v \in \mathbb{Z}^n$ *satisfying* $\|v\|_{P^2} < 1$, *then* $\|v\|_\infty < (\lfloor 2\rho(S)+1 \rfloor)^2$

Proof. Now we have $1 \le \lfloor 2\rho(S)+1 \rfloor \le 2n+1$ meaning

$$\frac{\|e\|_\infty}{\lfloor 2\rho(S)+1 \rfloor} = \|(\lfloor 2\rho(S)+1 \rfloor)^{-1} e\|_\infty = \|eP^{-1}\|_\infty = \|e\|_P < 2.$$

Thus, $\|e\|_\infty$ should be smaller than $2(\lfloor 2\rho(S)+1 \rfloor)$. Similarly, $\|v\|_{P^2} < 1$ gives us $\|v\|_\infty < (\lfloor 2\rho(S)+1 \rfloor)^2$. □

Lemma 2. *Assume that the distribution of the outputs of the hash function* $h : \{0,1\}^* \to \{x \in \mathbb{Z}^n, \|x\|_{P^2} < 1\}$ *and* $N = \lfloor 2\rho(S)+1 \rfloor \ge 4$ *. Then the probability that* $\|x_1 - x_2\|_\infty$ *is larger than* $4N$ *is at least* $1 - \frac{16}{N^2}$.

Proof. By Lemma 1, the space of outputs of h is $\{x \in \mathbb{Z}^n, \|x\|_\infty < N^2\}$ which is represented by the square with size of $2N^2$ centered at origin in Euclidean plane. On this range, the $4N$-neighborhood of x_1 has at most $(2 \cdot 4N)^2$ area which tends to get smaller as x_1 is close to the boundary. Thus, the probability that x_2 lies outside of this area is at least $1 - \frac{(2\cdot 4N)^2}{(2\cdot N^2)^2} = 1 - \frac{16}{N^2}$. □

From Lemma 2, we can construct an adversary attacking the blindness of this scheme as in the following theorem.

Theorem 3. *If* $\|e\|_P < 2$, *the blindness of Zhu et al.'s scheme is broken with non-negligible probability.*

Proof. We construct an PPT adversary $\mathcal{A}$ trying to break the blindness of this scheme.

1. The adversary $\mathcal{A}$ uses the algorithm KG_ϵ to generate a key pair $(k_s = S, k_p = (P, H))$ of this blind signature scheme. The public key k_p is made public, while $\mathcal{A}$ keeps k_s as his private key.
2. The adversary $\mathcal{A}$ outputs two messages m_0 and m_1, which might depend on k_s and k_p.
3. Let U_0 and U_1 be users with access to the public key k_p but not to the secret key k_s. For a random bit b that is unknown to $\mathcal{A}$, user U_0 is given the message m_b, while the message m_{1-b} is sent to user U_1. Both users engage in the interactive signing protocol (with $\mathcal{A}$ as signer), obtaining blind signatures δ_0 and δ_1 for the messages m_0 and m_1 with random r_0 and r_1, respectively.
   - In this procedure, $\mathcal{A}$ is given $u_b = (v_b + e_b) * T$ and $u_{1-b} = (v_{1-b} + e_{1-b}) * T$ where $v_i = h(m_i, r_i)$ for $i = b, 1-b$.
   - $\mathcal{A}$ can get $\|u_i\|_P = \|v_i + e_i\|_P$ for $i = b, 1-b$ since T preserves the norm.
4. The message/signature pairs (m_0, r_0, δ_0) and (m_1, r_1, δ_1) are given to the adversary $\mathcal{A}$.
5. $\mathcal{A}$ computes $\|v_i\|_P$ where $v_i = h(m_i, r_i)$ for $i = 0,1$ and outputs a bit $\bar{b}$ such that $\|v_{\bar{b}}\|_P - \|u_b\|_P| = min\{|\|v_0\|_P - \|u_b\|_P|, |\|v_1\|_P - \|u_b\|_P|\}$.

In the scheme [1], $P := \lfloor 2\rho(S)+1 \rfloor Id$. Therefore, by Lemma 2, the probability that $\|v_0 - v_1\|_\infty$ is larger than $4N$ is at least $1 - \frac{16}{N^2}$. Furthermore, here we are considering the case $\|e\|_P < 2$. Therefore, for two bits $b, b' \in \{0,1\}$, we have:

$$\|v_b - u_{b'}\|_\infty \le \|e_{b'}\|_\infty < 2N, \text{ with probability 1, if } b = b', \text{ and}$$

$$\|v_b - u_{b'}\|_\infty > 4N - 2N = 2N, \text{ with probability at least } 1 - \frac{16}{N^2}, \text{ if } b \ne b'.$$

Now, let L denote the case when $\|v_0 - v_1\|_\infty > 4N$. Clearly, $\Pr[\mathsf{L}] \ge 1 - \frac{16}{N^2}$. Also, in the event of L, $\bar{b} = b$ with probability 1-ϵ for a negligible function ϵ, since $\mathcal{A}$ can perfectly determine it by the distance of $\|v_{\bar{b}}\|_P - \|u_b\|_P$. In the event of $\bar{\mathsf{L}}$ (L's complement case), without loss of generality, we can say the probability that $\bar{b} = b$ is $\frac{1}{2} + \zeta$ for a function $\zeta \in [0, \frac{1}{2})$.[1]

Then, we have the advantage of this adversary $\mathcal{A}$:

$$\mathsf{Adv}_\mathcal{A} = \left|\Pr[\bar{b} = b] - \frac{1}{2}\right| = \left|\Pr[\bar{b} = b|\mathsf{L}]\Pr[\mathsf{L}] + \Pr[\bar{b} = b|\bar{\mathsf{L}}]\Pr[\bar{\mathsf{L}}] - \frac{1}{2}\right| > \frac{1}{2}\Pr[\mathsf{L}] + \varepsilon,$$

for a negligible function ε.

Moreover, an average approximation of $\rho(S)$ is about $\sqrt{\frac{2n}{3}}$ [2, Chapter 7.3]. Therefore, an average approximation of N is about $2\sqrt{\frac{2n}{3}} + 1$, and we can obtain the advantage of $\mathcal{A}$,

$$\mathsf{Adv}_\mathcal{A} > \frac{1}{2}\left(1 - \frac{16}{N^2}\right) + \varepsilon \approx \frac{1}{2} - \frac{8}{\left(2\sqrt{\frac{2n}{3}} + 1\right)^2} + \varepsilon > \frac{1}{2} - \frac{8}{n} + \varepsilon,$$

which is not negligible in n for $n > 16$. Therefore, the blindness is broken with non-negligible probability. □

5. Discussion

In this section, we briefly describe the difficulties of building *provably secure* blind signatures and future work. To our best knowledge, from lattices, there is one known *provably secure* blind signature [3]. In [3], it is well described why building a provably secure blind signature is difficult in general and why it is more difficult when it comes to working with lattices. Here is a quick summary and we refer to [3] for details. First, building a provably secure blind signature is non-trivial in general since two security requirements of a blind signature scheme, the blindness and the one-more unforgeability have somewhat conflicting characteristics. To provide the blindness, the user is given an ability to modify the signature from the signer. However, the ability must be limited only to the single signature. Otherwise, it hurts the one-more unforgeability.

Secondly, building a probably secure blind signature *from lattices* becomes harder because in lattices, the completeness is not naturally followed. In particular, the blind signature by Rückert [3] makes use of a commitment scheme and additional interactions to overcome the incompleteness. Moreover, in lattices, RSA-style design does not work [3]: the RSA-style using preimage trapdoor functions consists of the following procedures, (1) hash, (2) blind, (3) invert, then (4) unblind. In lattice, such a style does not work due to the linearity of the function (For details, we refer to [3]).

As summarized in the above, building a blind signature that is provably secure in lattices requires a careful design and rigorous security analysis. Often plausible designs fail to be provably secure [1,5,6]. Since the problem becomes harder in lattices, a rigorous study is required. One possible approach is improving the scheme by Rückert [3] by lessening the number of interactions. One might try to lessen them by sending two or more commitments at a time. Another possible approach is building a lattice-based witness indistinguishability primitive first and then applying it as a building block like in [5,6]. The aforementioned methods require further research to ensure provable security analysis and concrete scheme design. In this paper, we focus on providing cryptoanalysis of the particular scheme. We will continue the further research as a future work.

[1] For $\zeta \in (-\frac{1}{2}, 0]$, we can similarly obtain the same lower bound.

6. Conclusion

In this paper, we present cryptoanalysis on the blind signature scheme by Zhu et al. [1]. We formally prove that either the scheme is incorrect, or the blindness property is not preserved with high probability.

Acknowledgments

This work was supported by Samsung Research Funding Center of Samsung Electronics under Project Number SRFC-TB1403-52, and also by Institute for Information and communications Technology Promotion (IITP) grants funded by the Korea government (MSIT) (No. 2016-6-00599, A Study on Functional Signature and Its Applications, and No. IITP-2018-0-01423, the ITRC (Information Technology Research Center) support program).

References

[1] H. Zhu, Y.a. Tan, X. Zhang, L. Zhu, C. Zhang, J. Zheng, A round-optimal lattice-based blind signature scheme for cloud services, Future Gener. Comput. Syst. 73 (C) (2017) 106–114.
[2] T. Plantard, W. Susilo, K.T. Win, A digital signature scheme based on CVP_∞, in: R. Cramer (Ed.), Public Key Cryptography – PKC 2008, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 288–307.
[3] M. Rückert, Lattice-Based blind signatures, in: M. Abe (Ed.), Advances in Cryptology - ASIACRYPT 2010, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 413–430.
[4] A. Juels, M. Luby, R. Ostrovsky, Security of blind digital signatures, in: B.S. Kaliski (Ed.), Advances in Cryptology — CRYPTO '97, Springer Berlin Heidelberg, Berlin, Heidelberg, 1997, pp. 150–164.
[5] D. Pointcheval, J. Stern, Provably secure blind signature schemes, in: K. Kim, T. Matsumoto (Eds.), Advances in Cryptology — ASIACRYPT '96, Springer Berlin Heidelberg, Berlin, Heidelberg, 1996, pp. 252–265.
[6] D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures, J. Cryptol. 13 (3) (2000) 361–396.

Jung Hee Cheon is a Professor in the department of Mathematical Sciences and the director of the Cryptographic Hard problems Research Initiatives (CHRI) at Seoul National University (SNU). He received his B.S. and Ph.D. degrees in mathematics from KAIST in 1991, and 1997, respectively. Before joining SNU, he worked for Electronics and Telecommunications Research Institute, Brown University, and Information and Communications University, Korea. He received the best paper award in Asiacrypt 2008 and Eurocrypt 2015. His research focuses on computational number theory, cryptology and their applications to practical problems. He is an associate editor of DCC (Designs, Codes and Cryptography) and JCN (Journal of Communications and Networks), and served as program committee members for various conferences including Crypto, Eurocrypt, Asiacrypt. He was a PC co-chair of ANTS-XI and Asiacrypt 2015/2016.

Jinhyuck Jeong, received his B.S. degree in Education of Mathematics from Seoul National University, Seoul, Korea in 2012. He is currently pursuing the Ph.D. degree in Mathematical Sciences from Seoul National University, Seoul, Korea. His current research interests include biometrics authentication, fuzzy extractor, and homomorphic encryption with its applications.

Ji Sun Shin received her B.Sc. degree in Computer Science from Seoul National University, Seoul, Korea in 2001 and her Ph.D. degree from the University of Maryland, College Park, USA in 2009. From 2009 to 2012, she was a Senior Engineer at Samsung SDS, Seoul, Korea, where she was involved in the development of network access control systems. From 2012, she is working as an Assistant Professor of Computer and Information Security at Sejong University. Her research interests are computer network security, cryptographic protocols and applied cryptography.