Contents lists available at ScienceDirect

Future Generation Computer Systems

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

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

Hongfei Zhu[a], Yu-an Tan[a,b], Xiaosong Zhang[a,c], Liehuang Zhu[a,b], Changyou Zhang[d], Jun Zheng[a,b,*]

[a] *School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China*
[b] *Research Center of Massive Language Information Processing and Cloud Computing Application, Beijing 100081, China*
[c] *Department of Computer Science and Technology, Tangshan University, Tangshan 063000, China*
[d] *Institute of Software, Chinese Academy of Science, Beijing 100190, China*

HIGHLIGHTS

- We propose a novel CVP_∞ blind signature scheme based on lattice, which can guarantee trustworthy of Big Data.
- Our scheme can resist brute-force attacks, theoretical-timing attacks, and Nguyen–Regev attacks.
- Our scheme can offer statistical blindness and one-more unforgeability.
- Our round-optimal scheme outperforms the RSA, the Schnorr, and the ECC blind signature schemes in terms of efficiency and security.
- Our scheme outperforms the Rückert's lattice-based blind signature scheme in terms of signature length, moves, security, and energy cost.

ARTICLE INFO

Article history:
Received 18 November 2016
Received in revised form
24 January 2017
Accepted 28 January 2017
Available online xxxx

Keywords:
Big data and veracity
Blind signature
Quantum computer attack
CVP infinity
Trustworthy

ABSTRACT

To process rapidly growing Big Data, many organizations migrate their data and services such as e-voting and e-payment systems to the cloud. In these two systems, blind signature has become an essential cryptographic primitive since it allows the signer to sign a message without learning what he signs. Thus, it can guarantee trustworthy of Big Data. However, most blind signature schemes based on factoring and discrete logarithm problems cannot resist quantum computer attacks. The alternative blind signature schemes are based on lattice. Here, we present a round-optimal lattice-based blind signature scheme constructed on the closest vector problem using infinity norm. Firstly, our scheme is proven blind and one-more unforgeable, and is resistant to brute-force attacks, theoretical-timing attacks, and Nguyen–Regev attacks. Secondly, our scheme outperforms the RSA, the Schnorr, and the ECC blind signature schemes in terms of efficiency and security. Also, it outperforms the Rückert's blind signature in terms of signature length, moves, and security. Finally, our scheme outperforms the Rückert's blind signature in terms of communication and computation energy costs. Additionally, it outperforms the RSA blind signature in terms of communication energy cost.

1. Introduction

Current technologies have difficulty in processing huge data due to Big Data's high volume, high velocity, variety, veracity, and complexity value [1,2]. An alternative method is to store Big Data in the cloud for its major advantages such as on-demand self-service, resource pooling, rapid elasticity, utility-based pricing etc. [3–5]. Thus, many companies, governments and banks migrate their data and services, such as e-voting and e-payment systems to the cloud. However, if Big Data is mandated by untrusted cloud providers, its security can become a severe problem [6–13].

To guarantee the security in the e-voting and the e-payment systems, blind signature has become an essential cryptographic primitive since a signer is allowed to sign a message without learning what he actually signs. As expected, blind signature can guarantee trustworthy of Big Data [2,14]. Many blind signature

[*] Corresponding author at: School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China.
E-mail addresses: Hongfei010@gmail.com (H. Zhu), tan2008@bit.edu.cn (Y.-a. Tan), zxs0224@163.com (X. Zhang), liehuangz@bit.edu.cn (L. Zhu), changyou@iscas.ac.cn (C. Zhang), zhengjun_bit@163.com (J. Zheng).

http://dx.doi.org/10.1016/j.future.2017.01.031
0167-739X/© 2017 Elsevier B.V. All rights reserved.

schemes have found their wide use in e-payment, e-voting and oblivious transfer.

As blind signature was initially proposed by D. Chaum [15] in 1983, many blind signature schemes were constructed on RSA, ElGamal, ECC, DSA, etc.

According to their hardness problems, traditional blind signature schemes have the factoring blind signature, the discrete logarithm (DLP) blind signature and the pairing blind signature. Their development dates back to 1984 when D. Chaum initiated the RSA blind signature scheme [16]. In this scheme, even if the bank and the payee are conspiring against the payer, they can learn nothing from their participation in the payments protocol about the payer. Unfortunately, Chaum only described the blindness property of the blind signature scheme without proving its security. Although its security was proven by Bellare et al. [17], the random oracle was still in doubt. J. Camenisch et al. presented a new blind signature scheme based on RSA in the standard model. Their scheme was proven secure [18], but it needs long keys to achieve sufficient security.

To overcome the disadvantage of long keys, alternatively, in 1992, D. Chaum et al. initiated the blind signature scheme constructed on DLP [19]. Unfortunately, they did not prove its security, since there is a gap between cryptography and computation complexity. Later, T. Okamoto presented an efficient blind signature based on Schnorr scheme [20]. Similarly, this scheme was not provably secure as well. In 1994, J.L. Camenisch et al. presented two DLP blind signature schemes [21]. Apart from lack of rigid proof of security, all of these blind signature schemes only had the blindness property.

The property of unforgeability was not considered until 1996, when D. Pointcheval et al. firstly defined the security concepts for blind signature by presenting the Okamoto–Schnorr blind signature [22]. Subsequently, A. Boldyreva presented a blind signature based on pairing, which was both blind and one-more unforgeable, and potentially available to robustness and proactiveness [23]. However, this scheme still needs to be proven secure in the random oracle. To improve the security, Okamoto T. presented a blind signature in 2006. Though this scheme was secure in the standard model [24], it is not round-optimal. In 2011, O. Blazy et al. presented a provable secure blind signature scheme based on pairing [25] in the standard model. Its advantage is round-optimal. However, blind signature schemes based on pairing are usually inefficient.

To make blind signature schemes practical, researchers proposed concurrency and round-optimal. Concurrency means that a signer entity can execute many sessions from users at the same time [26–32], while the round-optimal property means that a blind signature scheme needs only two moves [33].

Concurrent blind signature is a concern since nearly all the schemes discussed above need more than three moves. In 1997, A. Juels et al. proposed the concept of concurrency in an adaptive interleaved chosen-message attack firstly, in which an adversary can execute many concurrent sessions. But his scheme is inefficient. After that, some concurrent blind signature schemes were proposed without the random oracle model [33–35]. However, they are not efficient enough. In 2011, Garg S et al. initially constructed a round-optimal blind signature, i.e. two-moves, in the standard model. Unfortunately, it was inefficient [36]. To improve the efficiency, S. Garg and D. Gupta constructed two efficient blind signature schemes, both of which were provably secure and round-optimal in the standard model [37,38]. Since most concurrent blind signature and round-optimal blind signature schemes were constructed on the factoring or the DLP, these schemes were nonresistant to quantum-computer attacks [39].

The demand for strong resistance to quantum computer attacks and high efficiency leads to the alternative blind signature schemes based on lattice. In 2010, a lattice-based blind signature was initially proposed by M. Rückert, whose security relies on the ideal-lattice shortest vector problem (ISVP) [40]. Their scheme outperforms the RSA and the Okamoto–Schnorr blind signature schemes in terms of efficiency, when its dimension exceeds 8192. However, it is not concurrent and round-optimal.

As discussed above, previous blind signature schemes are either insecure or inefficient. To integrate both security and efficiency, we present a novel CVP_∞ blind signature based on lattice. Our contributions are three-fold:

(1) Inspired by [41], we propose a novel lattice-based CVP_∞ blind signature scheme. Our scheme can guarantee trustworthy of Big Data. Different from most lattice-based signature schemes, which currently use l_2 norm, our scheme is more secure since the approximation problems for l_∞ norm are more difficult than for l_2 norm.
(2) In terms of resistance and security, our CVP_∞ blind signature scheme can resist brute-force attacks, theoretical-timing attacks, and Nguyen–Regev attacks. Furthermore, we prove that our scheme is secure on the properties of blindness and one-more unforgeability.
(3) The comparison between our blind signature scheme and the others shows that our scheme outperforms the others as it is more efficient than the RSA, the Schnorr and the ECC blind signature schemes. Its signature size is shorter than the Rückert's blind signature scheme. Its communication and computation energy consumptions are less than the Rückert blind signature scheme and it is round-optimal.

The remainder of the paper is organized as follows. Section 2 reviews the background of e-payment, e-voting, lattice and blind signature. Section 3 presents the construction of the CVP_∞ blind signature. Section 4 evaluates our scheme's resistance and security, also compares the performance and energy cost of five blind signature schemes. Section 5 concludes this paper.

2. Preliminaries

Let $x \in \mathbb{R}^n, C \in \mathbb{C}^{n,n}$, then $\lfloor x \rceil$ is rounded down to the closest integer vector of x. l_2-norm and l_∞-norm are respectively the Euclidean norm and the infinity norm, $\|A\|$ and $\|A\|_p$ are respectively the l_2 matrix norm and the l_p matrix norm. $\rho(C)$ is C's spectral radius, which can be got from $\rho(C) = \max\{|\lambda|, Cx = x\lambda\}$.

2.1. Blind signature in e-payment and e-voting systems for cloud services

In an e-payment system [15] for Big Data, we denote the payer as Alice, the payee as Bob, and the trusted third part as Trusted Third Part (TTP). Then we consider this situation: Alice wants to buy goods from Bob. To keep the security of the e-payment system, Alice's services are deployed in her personal cloud, the bank and Bob's services and data are deployed in the public cloud. As depicted in Fig. 1, firstly, TTP generates the key pairs for Alice, Bob, and the bank, then sends the private key to them respectively. Secondly, Alice withdraws money from the bank. Thirdly, Alice sends the money to Bob like spending real cash. Finally, Bob deposits the money in the bank. Then the e-payment process is described as follows:

(1) TTP generates and distributes the key:
- TTP generates the key pairs for Alice, Bob, and the bank.
- TTP sends the corresponding private key to Alice, Bob, and the bank respectively.

(2) Alice withdraws money from the bank:
- Alice logs in her account in the personal cloud.