Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **1**, January **2014**

Improvement of a Lattice-based Signature Scheme

Yan Xu[1,2], Miaomiao Tian[1,*], Liusheng Huang[1] and Wei Yang[1]

University of Science and Technology of China[1]
443 Jinzhai Road, Hefei 230026, China

Anhui University[2]
3 Feixi Road, Hefei 230039, China

Corresponding author*
xuyan@ahu.edu.cn, miaotian@mail.ustc.edu.cn, lshuang,qubit@ustc.edu.cn

Xiaochen Shen[3]

Mount Saint Vincent University[3]
166 Bedford Highway, Halifax B3M 2J6, Canada
shenxiaochen8729@hotmail.com

Recevied May, 2013; revised September, 2013

Abstract. *Recently, Boyen at PKC 2010 proposed a lattice-based signature scheme in the standard model. In this paper, we show that his signature scheme does not satisfy strong unforgeability. In other words, an adversary can produce a new signature for a message M after seeing a signature of the message M. Then we present an improved scheme and prove that the improved scheme satisfies strong unforgeability. Furthermore, the improved signature scheme is as efficient as Boyen's signature scheme.*

Keywords: Cryptography, Digital Signature, Lattice, Strong Unforgeability

1. Introduction.

Digital signature is the cornerstone of e-commerce, e-government and so on. A digital signature scheme is said to be *strongly unforgeable* if (1) it is existentially unforgeable under a chosen-message attack, and (2) any adversary cannot generate a different signature for a massage which has been signed [1]. Strongly unforgeable signatures are very useful and can be used to construct group signatures [2] as well as chosen-ciphertext secure encryption systems [3, 4].

Lattice-based signature schemes are enjoying great popularity in signature field due to the operations involved in lattices are very simple, the security of these schemes is based on the worst-case hardness of lattice problems and lattice-based cryptography is hard even for quantum computers [5,6]. In 2008, Gentry, Peikert and Vaikuntanathan [7] introduced a family of trapdoor functions based on small integer solution (SIS) problem and then designed a lattice-based signature scheme using these functions. The signature scheme is proven to be strongly unforgeable in the random oracle model. In 2010, Cash et al. [8] proposed a new signature scheme from lattices which is secure in the standard model but is not strongly unforgeable. By revising Cash et al.'s scheme, Rückert [9] constructed the first strongly unforgeable lattice-based signature scheme in the standard model. Later on, strongly unforgeable lattice-based signature schemes received great attentions and several new strongly unforgeable lattice-based signature schemes are proposed. For example, Tian et al. in [10] constructed a strongly unforgeable lattice-based ring signature scheme in the standard model and in [11, 12] constructed two hierarchical identity-based signature schemes from lattices that are strongly unforgeable in the standard model and in the random oracle model, respectively.

In this paper we analyze a novel lattice-based signature scheme in the standard model presented by Boyen [13]. The scheme is more efficient than other lattice-based signature schemes in the standard model (e.g. [8, 9]). However, we show that the scheme does not meet strong unforgeability. Namely, an adversary $\mathcal{A}$ can produce a new message-signature pair $(M, \mathbf{s}')$ after seeing a valid message-signature pair $(M, \mathbf{s})$. We then based on Rückert's construction present an improved scheme and prove that the improved scheme satisfies strong unforgeability. The performance of our improved scheme is almost the same as that of Boyen's scheme.

The rest of this paper is organized as follows. Section 2 introduces some useful definitions and results used throughout this work. In Section 3, we review and analyze Boyen's signature scheme. The improved scheme and its analysis will be provided in Section 4. Finally, Section 5 concludes this paper.

2. **Preliminaries.** In this section, we first give some definitions and then recall how to sample lattice points with short length and how to delegate a short basis. They will be used as building blocks of this paper.

Definition 1. Let q be a positive integer and $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ be a matrix, define a mdimensional full-rank integer lattice as:

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

Definition 2. Given a positive integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a real β, the SIS problem (q, m, β)-SIS is finding a vector $e \in \Lambda^{\perp}(\mathbf{A})$ such that $\|\mathbf{e}\| \leq \beta$.

For some parameters the SIS problem is hard [5,14]. Security of our improved signature scheme will rest on the hardness assumption of the SIS problem.

Definition 3. For any $\sigma > 0$, define the Gaussian function on $\mathbb{R}^m$ centered at $\mathbf{c}$ with parameter σ as:

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

The discrete Gaussian distribution over lattice Λ with center $\mathbf{c}$ and parameter σ is defined as:

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

2.1. **Trapdoor functions.** Here we will review the trapdoor functions introduced by Gentry, Peikert and Vaikuntanathan [7]. Let $D_n = \{\mathbf{e} \in \mathbb{Z}^m : \|\mathbf{e}\| \leq \sigma\sqrt{m}\}$ be domain and $R_n = \mathbb{Z}_q^n$ be range, the trapdoor functions determined by $\mathbf{A}$ are

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{Ax}(mod\ q).$$

where $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is a uniformly random matrix.

Sampling from $f_{\mathbf{A}}^{-1}(\mathbf{y})$ for any $\mathbf{y} \in R_n$ without a trapdoor is as hard as solving some lattice problems in the worst-case. A short basis $\mathbf{T_A}$ for $\Lambda^{\perp}(\mathbf{A})$ is a trapdoor of the function $f_{\mathbf{A}}$. According to [7], we can get a vector $\mathbf{v} \in D_n$ with overwhelming probability using $\mathbf{T_A}$. Here we briefly review the sampling algorithm:

- **TrapGen(1^n):** Let $q \geq 2$ and $m \geq 5n \log q$, the probabilistic polynomial-time algorithm TrapGen(1^n) outputs a matrix $\mathbf{A} \in \mathbf{Z}_q^{n\times m}$ statistically close to uniform and a basis $\mathbf{T_A}$ for $\Lambda^{\perp}(\mathbf{A})$ with overwhelming probability such that $\left\|\widetilde{\mathbf{T_A}}\right\| \leq O(\sqrt{n \log q})$, where $\widetilde{\mathbf{T_A}}$ denotes the Gram-Schmidt orthogonalization of $\mathbf{T_A}$.

- **SampleDom(1^n, σ):** The algorithm samples an $\mathbf{x}$ from distribution $D_{\mathbb{Z}^m,\sigma,0}$ such that $\mathbf{x} \in D_n$ with overwhelming probability.
- **SamplePre(A, $\mathbf{T_A}$, σ, y):** On input $\mathbf{y} \in R_n$, the algorithm samples a vetoer $\mathbf{e} \in D_n$ such that $\mathbf{A_e} = \mathbf{y}(mod\ q)$. In order to do this, we first choose an arbitrary $\mathbf{c} \in \mathbb{Z}^m$ such that $\mathbf{A_c} = \mathbf{y}(mod\ q)$ and next sample an $\mathbf{x}$ from distribution $D_{\Lambda^{\perp}(\mathbf{A}),\sigma,-c}$ using **SampleDom(1^n, σ)**. Finally, output $\mathbf{e} = \mathbf{x} + \mathbf{c}$.

2.2. **Basis Delegation.** Recently, Cash et al. [8] introduce an effective way to delegate a short basis for $\Lambda^{\perp}(\mathbf{A})$ into one for $\Lambda^{\perp}(\mathbf{A}||\mathbf{B})$, where $\mathbf{A}||\mathbf{B}$ is a new matrix whose rows are the junction of each row of matrices $\mathbf{A}$ and $\mathbf{B}$. The result is described below.

Lemma 2.1. *For $q \geq 2$, $m \geq 5n \log q$, let $\mathbf{T_A}$ be an arbitrary basis of $\Lambda^{\perp}(\mathbf{A})$ and let $\mathbf{B} \in \mathbb{Z}_q^{n\times m'}$ be arbitrary, there is a polynomial-time algorithm **ExtBasis**($\mathbf{T_A}$, $\mathbf{A}' = \mathbf{A}||\mathbf{B}$) outputs a basis $\mathbf{T_{A'}}$ of $\Lambda^{\perp}(\mathbf{A}')$ such that $\left\|\widetilde{\mathbf{T_{A'}}}\right\| = \left\|\widetilde{\mathbf{T_A}}\right\|$.*

3. **Analysis of Boyen's signature scheme.** In this section we briefly review the latticebased signature scheme proposed by Boyen and show the scheme is not strongly unforgeable.

3.1. **Boyen's signature scheme.** Let a massage M be an l-bit string indexed from 1 to l. The Boyen's signature scheme is described in the following.

- **KeyGen(1^n):** Given a security parameter n, run **TrapGen(1^n)** to generate a matrix $\mathbf{A} \in \mathbf{Z}_q^{n\times m}$ with a short basis $\mathbf{T_A}$ for $\Lambda^{\perp}(\mathbf{A})$. Choose $l + 1$ independent matrices $\mathbf{C}_0, \mathbf{C}_1, \ldots, \mathbf{C}_l \in \mathbb{Z}_q^{n\times m}$. Output the verification key $\mathbf{VK} = (\mathbf{A}, \mathbf{C}_0, \mathbf{C}_1, \ldots, \mathbf{C}_l) \in (\mathbb{Z}_q^{n\times m})^{l+2}$.
- **Sign($\mathbf{T_A}$, M):**On input the signing key $\mathbf{T_A}$ and a massage $M \in \{0,1\}^l$, one does the following:
  1. Let $\mathbf{C}_M = \mathbf{C}_0 + (-1)^{M[1]}\mathbf{C}_1 + \cdots + (-1)^{M[l]}\mathbf{C}_l$.
  2. Define $\mathbf{A}' = (\mathbf{A}||\mathbf{C}_M) \in \mathbb{Z}_q^{n\times 2m}$.
  3. Run **ExtBasis**($\mathbf{T_A}$,$\mathbf{A}'$) to generate a short basis $\mathbf{T_{A'}}$ for $\Lambda^{\perp}(\mathbf{A}')$.
  4. Compute $\mathbf{d} \leftarrow$ **SamplePre**($\mathbf{A}'$, $\mathbf{T_{A'}}$, σ, $\mathbf{0}$).
  5. Output the signature $\mathbf{d}$.
- **Verify(VK, d, M):**Given the verification key $\mathbf{VK}$, a signature $\mathbf{d} \in \mathbb{Z}^{2m}$ and a massage $M \in \{0,1\}^l$, output "Accept" if and only if $0 \leq \|\mathbf{d}\| \leq \sigma\sqrt{2m}$ and $(\mathbf{A}||\mathbf{C}_M)\mathbf{d} = \mathbf{0}(mod\ q)$; output "Reject", otherwise.

3.2. **An attack on Boyen's signature scheme.** It is clear that, for any integer $k \neq 1$, the vector $\mathbf{v} = k \cdot \mathbf{d}$ is a new solution of the linear system $(\mathbf{A}||\mathbf{C}_M)\mathbf{x} = \mathbf{0}(mod\ q)$. If there exists an integer k_0 such that $0 \leq \|k_0 \cdot \mathbf{d}\| \leq \sigma\sqrt{2m}$, then, for each k such that $0 < |k| \leq |k_0|$, $\mathbf{v} = k \cdot \mathbf{d}$ is a valid signature of M. In particular, $-\mathbf{d}$ is a different signature of M since $-\mathbf{d} \neq \mathbf{d}$, $0 < \|-\mathbf{d}\| = \|\mathbf{d}\| \leq \sigma\sqrt{2m}$ and $(\mathbf{A}||\mathbf{C}_M)(-\mathbf{d}) = \mathbf{0}(mod\ q)$. Thus, anyone can easily forge a new signature for M after seeing the message-signature pair (M, $\mathbf{d}$). It implies that Boyen's signature scheme does not satisfy strong unforgeability. (Here we would like to stress that Boyen did not prove the signature scheme to be strongly unforgeable.)

4. **Our improved signature scheme.** In this section, based on Rückert's construction [9], we propose an improved signature scheme of Boyen's cheme and prove the improved scheme is strongly unforgeable in the standard model. We also compare the performance of our improved scheme with those of the schemes in [8] and [13].

Table 1. Performance comparison of several lattice-based signature schemes.

Scheme	Verification key size	Secret key size	Signature size
[8]	$(2l+1)nm$	m^2	$(l+1)m$
[13]	$(l+1)nm$	m^2	$2m$
This work	$(l+1)nm+n$	m^2	$2m$

4.1. Construction.

Our improved signature scheme is described as follows.

- **KeyGen(1^n):** Given a security parameter n, run **TrapGen(1^n)** to generate a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ with a short basis $\mathbf{T_A}$ for $\Lambda^{\perp}(\mathbf{A})$. Choose $l+1$ independent matrices $\mathbf{C}_0, \mathbf{C}_1, \ldots, \mathbf{C}_l \in \mathbb{Z}_q^{n\times m}$ and a random vector $\mathbf{y} \in R_n \backslash \{\mathbf{0}\}$. Output the verification key $\mathbf{VK} = (\mathbf{A}, \mathbf{y}, \mathbf{C}_0, \mathbf{C}_1, \ldots, \mathbf{C}_l)$.
- **Sign($\mathbf{T_A}$, M):**On input the signing key $\mathbf{T_A}$ and a massage $M \in \{0,1\}^l$, the signer does the following:
  1. Let $\mathbf{C}_M = \mathbf{C}_0 + (-1)^{M[1]}\mathbf{C}_1 + \cdots + (-1)^{M[l]}\mathbf{C}_l$.
  2. Define $\mathbf{A}' = (\mathbf{A}||\mathbf{C}_M) \in \mathbb{Z}_q^{n\times 2m}$.
  3. Run **ExtBasis**($\mathbf{T_A}$,$\mathbf{A}'$) to generate a short basis $\mathbf{T}_{\mathbf{A}'}$ for $\Lambda^{\perp}(\mathbf{A}')$.
  4. Compute $\mathbf{s} \leftarrow$ **SamplePre**($\mathbf{A}'$, $\mathbf{T}_{\mathbf{A}'}$, σ, $\mathbf{y}$).
- **Verify(VK, s, M):**Given the verification key **VK**, a signature s and a massage $M \in \{0,1\}^l$, output "Accept" if and only if $0 \leq \|\mathbf{s}\| \leq \sigma\sqrt{2m}$ and $(\mathbf{A}||\mathbf{C}_M)\mathbf{s} = \mathbf{y}(mod\ q)$; output "Reject", otherwise.

4.2. Analysis.

Now we analyze the performance and security of our improved scheme successively.

Performance Comparisons. To make a more comprehensive conclusion, we make a comparison between our scheme and some related lattice-based signature schemes. Table I shows the details. Obviously, the performance of our improved scheme is almost the same as that of Boyen's scheme [13] and better than that of the scheme proposed in [8].

The following theorem reveals that our improved scheme is strongly unforgeable in the standard model.

Theorem 4.1.*(Strong unforgeability) For a prime modulus q and a polynomial function $\beta = poly(n)$, if there is an adversary $\mathcal{A}$ that outputs a forgery, with probability ϵ and making $Q \leq q/2$ adaptive chosen-message queries, then there is an algorithm $\mathcal{B}$ that solves the (q, m, β)-SIS problem with probability $\epsilon' > (1+Q/q)\epsilon(6q)^{-1}$.*

Proof. Suppose there exists such an adversary $\mathcal{A}$, we show that an algorithm $\mathcal{B}$ is able to be constructed to solve the SIS problem.

- **Setup.** For a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathcal{B}$ picks a random matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$ with a short basis $\mathbf{T_B}$, $l+1$ short random matrices $\mathbf{R}_0, \mathbf{R}_1, \ldots, \mathbf{R}_l \in \mathbb{Z}_q^{n\times m}$, l uniformly random scalars $h_1, h_2, \ldots, h_l \in \mathbb{Z}_q$ and a short vector $\mathbf{x}$. The algorithm $\mathcal{B}$ selects a massage M^* such that $h_{M^*} = 0\ (mod\ q)$ and sets $\mathbf{y} = (\mathbf{A}||\mathbf{A}\mathbf{R}_{M^*})\mathbf{x}\ (mod\ q)$ (The h_{M^*} and $\mathbf{R}_{M^*}$ are defined below). Output the verification key $\mathbf{VK} = (\mathbf{A}, \mathbf{y}, \mathbf{C}_0 = \mathbf{A}\mathbf{R}_0 + \mathbf{B}(mod\ q), \mathbf{C}_1 = \mathbf{A}\mathbf{R}_1 + h_1\mathbf{B}(mod\ q), \ldots, \mathbf{C}_l = \mathbf{A}\mathbf{R}_1 + h_1\mathbf{B}(mod\ q))$.
- **Signature queries.** $\mathcal{B}$ answers signature queries from $\mathcal{A}$ on any message $M (M \neq M^*)$ as follows:
  1. Set $\mathbf{R}_M = \mathbf{R}_0 + \sum_{i=1}^{l}(-1)^{M[i]}\mathbf{R}_i$.
  2. Set $h_M = 1 + \sum_{i=1}^{l}(-1)^{M[i]}h_i$.

3. $\mathcal{B}$ aborts the algorithm if $h_M = 0\ (mod\ q)$
4. Let $\mathbf{F}_M = (\mathbf{A}||\mathbf{AR_M} + h_M\mathbf{B}) \in \mathbb{Z}_q^{n\times 2m}$
5. Find a short vector $\mathbf{d} \in \mathbb{Z}^{2m}$ such that $\mathbf{F}_M\mathbf{d} = \mathbf{y}(mod\ q)$ using the trapdoor $\mathbf{T_B}$. $\mathcal{B}$ can find the vector $\mathbf{d}$ as follows: First of all, $\mathcal{B}$ selects a vector $\mathbf{d}_1 \in D_n$. Then, he computes $\mathbf{d}_2 \leftarrow \mathbf{SamplePre}(h_M\mathbf{B}, \mathbf{T_B}, \sigma, \mathbf{y} - \mathbf{Ad}_1)$. The vector $\mathbf{d}^T = [\mathbf{d}_1^T - (\mathbf{R}_M\mathbf{d}_2)^T||\mathbf{d}_2^T]$ meets $\mathbf{F}_M\mathbf{d} = \mathbf{y}(mod\ q)$.
6. Output the signature $\mathbf{d}$.
If $M = M^*$, $\mathcal{B}$ outputs $\mathbf{x}$.

- **Output.** Finally, $\mathcal{A}$ outputs a forgery $\mathbf{s}^T = [\mathbf{s}_1^T||\mathbf{s}_2^T]$ on message M'. $\mathcal{B}$ computes $h_{M'}$ and restarts the simulation process if $h_{M'} \neq 0$.

If $h_{M'} = 0$, then we have $(\mathbf{A}||\mathbf{AR}_{M'})\mathbf{s} = \mathbf{y}\ (mod\ q)$. It is clear that $\mathcal{B}$ gets a solution $\mathbf{e} = \mathbf{s}_1 + \mathbf{R}_{M'}\mathbf{s}_2 - \mathbf{x}_1 - \mathbf{R}_{M^*}\mathbf{x}_2$ of the (q, m, β)-SIS problem since

$$\begin{aligned}\mathbf{Ae} &= \mathbf{A}(\mathbf{s}_1 + \mathbf{R}_{M'}\mathbf{s}_2 - \mathbf{x}_1 - \mathbf{R}_{M^*}\mathbf{x}_2)\\ &= (\mathbf{A}||\mathbf{AR}_{M'})\mathbf{s} - (\mathbf{A}||\mathbf{AR}_{M^*})\mathbf{x}\\ &= \mathbf{y} - \mathbf{y}\\ &= \mathbf{0}\ (mod\ q)\end{aligned}$$

where $\mathbf{x}^T = [\mathbf{x}_1^T||\mathbf{x}_2^T]$ is a signature of the massage M^*.

The above simulation process works well no matter whether M' is a fresh message or not. We now need to compute the probability of $\mathbf{e} \neq \mathbf{0}$. Similar to [13], $Prob[\mathbf{e} \neq 0] \geq 2/3$. Therefore, the total success probability of the algorithm $\mathcal{B}$ is $\epsilon' = \epsilon Q(2q)^{-1}(1 - Q/q + 1/q)(q^{-1} + Q^{-1})Prob[\mathbf{e} \neq 0] > (1 + Q/q)\epsilon(6q)^{-1}$. This completes the proof.

5. **Conclusions.** In this paper, we have shown that Boyen's lattice-based signature scheme does not satisfy strong unforgeability. Then, we have proposed an improved lattice-based signature scheme which is strongly unforgeable in the stranded model. A formal proof on the security of the improved scheme and a performance analysis have also been provided.

Acknowledgement. This work is supported by the National Grand Fundamental Research 973 Program of China (No. 2011CB302905), the National Natural Science Foundation of China (Nos. 61202407, 61173188, 61173187), the Fundamental Research Funds for the Central Universities (No. WK01100s00033), the Natural Science Foundation of Anhui Province of China (No. 11040606M141), and the Special Foundation for Young Scientists of Anhui Province of China (No. 2012SQRL015).

REFERENCES

[1] S. Goldwasser, S. Micali, and R. L. Rivest, A digital signature scheme secure against adaptive chosenmessage attacks, *Journal of SIAM Journal on Computing*, vol. 17, no. 2, pp. 281-308, 1988.

[2] D. Boneh, X. Boyen, and H. Shacham, Short group signatures, *Proc. of the 24th Annual International Cryptology Conference*, vol. 4. no. 4, pp. 345-370, 1998.

[3] R. Canetti, S. Halevi, and J. Katz, Chosen-ciphertext security from identity-based encryption, *Proc. of the 23th International Conference on the Theory and Applications of Cryptographic Techniques*, LNCS 3027, springer, pp. 207-222, 2004.

[4] T. T. Tsai, Y. M. Tseng, and T. Y. Wu, A fully secure revocable ID-based encryption in the standard model, *Journal of Informatica*, vol. 23, no. 3, pp. 487-505, 2012.

[5] M. Ajtai, Generating hard instances of the short basis problem, *Proc. of the 26th International Colloquium on Automata, Languages and Programming*, pp. 1-9, 1999.

[6] O. Regev, Lattice-based cryptography, *Proc. of the 26th annual international conference on Advances in Cryptology*, pp. 131-141, 2006.

[7] C. Gentry, C. Peikert, and V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, *Proc. of the 40th annual ACM symposium on Theory of computing*, pp. 197-206, 2008.

[8] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, Bonsai trees, or how to delegate a lattice basis, *Proc. of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques*, pp. 523-552, 2010.

[9] M. Rückert, Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles, *Proc. of the Third international conference on Post-Quantum Cryptography*, pp. 182-200, 2010.

[10] M. Tian, L. Huang, and W. Yang, Efficient lattice-based ring signature scheme, *Chinese Journal of Computers*, vol. 35, no. 4, pp. 712-718, 2012.

[11] 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*, vol. 14, no. 6, pp. 310-315, 2012.

[12] M. Tian, L. Huang, and W. Yang, Efficient hierarchical identity-based signatures from lattices, *International Journal of Electronic Security and Digital Forensics*, vol. 5, no. 1, pp. 1-10, 2013.

[13] X. Boyen, Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more, *Proc. of the 13th international conference on Practice and Theory in Public Key Cryptography*, pp. 499-517, 2010.

[14] J. Alwen, and C. Peikert, Generating shorter bases for hard random lattices, *Journal of Theory of Computing Systems*, vol. 48, no. 3, pp. 535-553, 2011.