A Novel Nonlinear Network Coding Signature Scheme Determined by the SIS problem

Yanqing Yao, Zhoujun Li, Hua Guo
State Key Laboratory of Software Development Environment,
Beihang University, Beijing 100191, China
School of Computer Science and Engineering, Beihang University, Beijing, China
Beijing Key Laboratory of Network Technology, Beihang University, Beijing, China
yaoyanqing1984@sina.com, lizj@buaa.edu.cn, hguo@buaa.edu.cn

Abstract

Network coding signature schemes can be employed to pre- vent malicious modification of data in network transition. But existing network coding signature schemes are only suitable for linear network coding. To adapt to nonlinear network coding, in this paper we introduce the concept of nonlinear network coding signature scheme and its un- forgeability, and propose a unforgeable nonlinear network coding scheme based on the hardness of the small integer solution (SIS) problem in lattice-based cryptography. We first present an improvement on the theorem which presented the unforgeability of a signature scheme without identifiers proposed by David Cash et.al. in EUROCRYPT 2010. Then a nonlinear network coding signature scheme is designed, and its unforgeability is proved by employing the Chinese remainder theorem. Thus the scheme can be used to provide cryptographic protection in nonlinear network coding.

Keywords: *nonlinear network coding signature scheme, the small integer solution problem, lattice-based cryptography, the Chinese remainder theorem*

1. Introduction

Signature scheme is a basic cryptographic tool in network security. In contrast to traditional "store-and-forward" routing, network coding [2] is related to a general class of routing mechanisms where intermediate nodes modify data packets in transit. In a signature scheme, every file is bound with an identifier $\mathbf{id}$ that is chosen by the sender when the first packet associated with the file is transmitted. The identifier provides a mechanism for honest nodes, and especially the receiver, to distinguish packets associated with different files [2]. Nowadays, network coding has been suggested for applications in wireless and/or ad-hoc networks, it has also been proposed as an efficient tool for content distribution in peer-to-peer networks [5] as well as improving the performance of large scale data dissemination over the Internet [1]. In [2], the concept of network coding signature scheme was presented. However, it's only suitable for linear network coding with homomorphic signature scheme [2, 3] because of its strong verification requirement. Dougherty et al. [7] showed that linear network coding is insufficient for non-multicast networks. Nowadays, nonlinear network

coding has aroused scholars' interest [6, 8]. To provide cryptographic protection against pollution attacks, we will propose the concepts of nonlinear network coding signature scheme and its unforgeability and present a secure nonlinear network coding scheme.

The rest of this paper is organized as follows. In the following section, we recall some terms and theories, and introduce the concepts of nonlinear network coding signature scheme and its unforgeability to be used in the paper. In Section 3, we improve the theorem about the unforgeability of the signature scheme in [4]. Based on the result, we design a novel nonlinear network coding signature scheme based on the hardness of the **SIS** problem, and prove its unforgeability. Section 4 concludes the paper.

2. Preliminaries

In this section, we propose the concepts of nonlinear network coding signature scheme and its unforgeability. The scheme can be used to prevent adversary's attacks such as corrupting an arbitrary number of nodes in the network, eavesdropping on all network traffic, and inserting or modifying an arbitrary number of packets.

Definition 1. A nonlinear network coding signature scheme for a message space $\mathcal{M}$ is defined by a triple of probabilistic, polynomial time algorithms, $(\mathbf{Gen}, \mathbf{Sign}, \mathbf{Verify})$ with the following functionality:

• $\mathbf{Gen}$: On input a security parameter 1^n (in unary) and additional public parameters $\mathbf{params}$ that include the length of a vector to be signed, this algorithm outputs a public key pk and a secret key sk.

• $\mathbf{Sign}(sk, \mu, \mathbf{id})$: On input a secret key sk, an identifier $\mathbf{id}$ that is an element of a randomly samplable set $\mathcal{I}$, and a vector $\mu \in \mathcal{M}$, this algorithm outputs a signature σ.

• $\mathbf{Verify}(pk, \mathbf{id}, \mu, \sigma)$: On input verification key pk, an identifier $\mathbf{id} \in \mathcal{I}$, a message μ, and a signature σ, this algorithm outputs either 0 (reject) or 1 (accept).

We require that for each (pk, sk) output by $\mathbf{Gen}$, the following holds: for all $\mu \in \mathcal{M}$ and for all $\mathbf{id} \in \mathcal{I}$, if $\sigma \leftarrow \mathbf{Sign}(sk, \mu, \mathbf{id})$, then $\mathbf{Verify}(pk, \mathbf{id}, \mu, \sigma)$ should accept with overwhelming probability.

Remark 1. It should be noticed that the scheme above is very different from the network coding signature scheme in [2]. In [2], the signature scheme should satisfy that for all subspaces $V \subseteq M$ and for all $\mathbf{id} \in \mathcal{I}$, if $\sigma \leftarrow \mathbf{Sign}(sk, \mathbf{id}, V)$, then $\mathbf{Verify}(pk, \mathbf{id}, \mathbf{y}, \sigma) = 1$ for all $\mathbf{y} \in V$. For linear network coding, the homomorphic scheme can be employed to protect the files' security. We only need to define $\mathbf{Sign}(sk, \mathbf{id}, V) = (\mathbf{Sign}(sk, \mathbf{id}, \mathbf{v}_1), \mathbf{Sign}(sk, \mathbf{id}, \mathbf{v}_2), \cdots, \mathbf{Sign}(sk, \mathbf{id}, \mathbf{v}_m))$ where $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}$ is a basis of the subspace V. Then the signature of the vector $\mathbf{v} = \Sigma_{i=1}^{m} \alpha_i \mathbf{v}_i \in V$ can be defined as $\Sigma_{i=1}^{m} \alpha_i \mathbf{Sign}(sk, \mathbf{id}, \mathbf{v}_i)$. But for nonlinear network coding like the negate-or (NOR) function [9], it's difficult to define $\mathbf{Sign}(sk, \mathbf{id}, V)$. To remedy this flaw, we present the above concept about nonlinear network coding signature scheme.

Definition 2. A nonlinear network coding signature scheme $\mathcal{S} = (\mathbf{Gen}, \mathbf{Sign}, \mathbf{Verify})$ is unforgeable if the advantage of any probabilistic, polynomial-time adversary $\mathcal{A}$ in the following security game is negligible in the security parameter 1^n:

$\mathbf{Gen}$: The challenger runs $\mathbf{Gen}(1^n, \mathbf{params})$ to obtain (pk, sk), and gives pk to $\mathcal{A}$.

$\mathbf{Queries}$: Proceeding adaptively, $\mathcal{A}$ specifies a vector $\mu_i \in \mathcal{M}$. The challenger chooses an identifier $\mathbf{id}_i$ uniformly at random from the set of identifiers $\mathcal{I}$, and sends $\mathbf{id}_i$ and $\sigma \leftarrow \mathbf{Sign}(sk, \mu_i, \mathbf{id}_i)$ to $\mathcal{A}$.

$\mathbf{Output}$: $\mathcal{A}$ outputs $\mathbf{id}^* \in \mathcal{I}$, a vector μ^*, and a nonzero signature σ^*.

The adversary wins if $\mathbf{Verify}(pk, \mathbf{id}^*, \mu^*, \sigma^*) = 1$, and either (1) $\mathbf{id}^* \neq \mathbf{id_i}$ for all i where $\mathbf{id_i}$ has been appeared in the $\mathbf{Queries}$ process (a type 1 forgery), or (2) $\mathbf{id}^* = \mathbf{id_i}$ but $\mu^* \neq \mu_i$ for some i(a type 2 forgery).

3. The nonlinear network coding signature scheme based on the SIS problem and its unforgeability

3.1. The nonlinear network coding signature scheme

In this section, based on the signature scheme in [4], we construct a nonlinear network coding signature scheme. Compared to the signature scheme in [4], the identifiers are added. Accordingly, the prime q in [4] has been changed into $2q$ in the corresponding positions, and the verification items have been changed.

In addition to the main $\mathbf{SIS}$ parameters n and q, the parameters of our signature scheme also involves:

- a dimension $m = O(n \log 2q)$ and a bound $\widetilde{L} = O(\sqrt{n \log 2q})$.
- a (hashed) message length k, which induces a 'total dimension' $m' = m \cdot (k+1)$;
- a Gaussian parameter $s = \widetilde{L} \cdot \omega(\sqrt{\log n})$.

The nonlinear network coding signature scheme(NSIG) is defined as follows:

- $\mathbf{Gen}$: generate $(\mathbf{A}_0; \mathbf{S}_0) \leftarrow \mathbf{GenBasis}(1^n; 1^m; 2q)$, where $\mathbf{A}_0 \in \mathbb{Z}_{2q}^{n \times m}$ is negligibly close to uniform and $\mathbf{S}_0$ is a basis of $\Lambda^{\perp}(\mathbf{A}_0)$ with $||\tilde{\mathbf{S}}_0|| \leq \widetilde{L}$. Let $F : \{0,1\}^n \to \mathbb{Z}_2^n$ be a one to one mapping. Then for each $(b, j) \in \{0,1\} \times [k]$, choose uniformly random and independent $\mathbf{A}_j^{(b)} \in \mathbb{Z}_{2q}^{n \times m}$. Output $pk = (\mathbf{A}_0, \{\mathbf{A}_j^{(b)}\}, F)$ and $sk = (\mathbf{S}_0; pk)$.
- $\mathbf{Sign}(sk, \mu \in \{0,1\}^k, \mathbf{id} \in \{0,1\}^n)$: Let $\mathbf{A}_\mu = \mathbf{A}_0 || \mathbf{A}_1^{(\mu_1)} || \cdots || \mathbf{A}_k^{(\mu_k)}$. Output $\sigma \leftarrow \mathcal{D}_{\Lambda^{\perp}_{q \cdot F(\mathbf{id})}(\mathbf{A}_\mu), s}$, via $\sigma \leftarrow \mathbf{SampleD}(\mathbf{ExtBasis}(\mathbf{S}_0, \mathbf{A}_\mu); q \cdot F(\mathbf{id}); s)$.

(In the rare event that $||\sigma|| > s \cdot \sqrt{m'}$, resample σ.)

- $\mathbf{Verify}(pk, \mathbf{id}, \mu, \sigma)$: let $\mathbf{A}_\mu$ be as above. Accept if $||\sigma|| \leq s \cdot \sqrt{m'}$, and $\mathbf{A}_\mu \cdot \sigma \equiv q \cdot F(\mathbf{id}) (mod\ 2q)$; else, reject.

$\mathbf{Correctness}$: Denote the output of $\mathbf{ExtBasis}(\mathbf{S}_0, \mathbf{A}_\mu)$ as $\mathbf{S}$, from Lemma 2, we have $||\widetilde{\mathbf{S}}|| = ||\widetilde{\mathbf{S}_0}||$. Combining $s = \widetilde{L} \cdot \omega(\sqrt{\log n})$ and $||\widetilde{\mathbf{S}_0}|| \leq \widetilde{L}$, we have $s \geq ||\widetilde{\mathbf{S}}|| \cdot \omega(\sqrt{\log n})$. Then from Lemma 2.4 of [4] we conclude that the vector σ output by the $\mathbf{Sign}$ algorithm satisfies $\mathbf{A}_\mu \cdot \sigma \equiv q \cdot F(\mathbf{id}) (mod\ 2q)$ and is drawn from a distribution statistically close to $\mathbf{A}_\mu \cdot \sigma \equiv q \cdot F(\mathbf{id}) (mod\ 2q)$.

By Lemma 2.4 of [4] we conclude that $||\sigma|| \leq s \cdot \sqrt{m'}$ with overwhelming probability.

3.2. Unforgeability

Now we prove unforgeability of our nonlinear network coding signature scheme. Given an adversary that breaks the signature scheme for a message space $\{0,1\}^k$ and an identity space $\{0,1\}^n$, we construct an adversary that simulates the signature scheme and solves the $\mathbf{SIS}_{q,\beta}$ problem.

Lemma 1. *Let B be a finite subset of $\{0,1\}^k$. Denote P_B as the set of all strings $p \in \{0,1\}^{\leq k}$ having the property that p is a shortest string for which p is not a prefix of any $\mu^{(j)} \in B$. Denote $|P_i| = \max\{|P_B| : B \subseteq \{0,1\}^k and |B| = i\}$. Let $g_i^- = k \cdot i - |P_i|$. Then*

- $g_1^- = 0$,
- $g_2^- = 2$,

• $g_i^- = \min_{1 \le l \le i-1} \{i + g_{i-l}^- + g_l^-\}$ *for* $i \ge 3$.

proof. Omitted.

Remark 2. It should be noticed that the maximum cardinality of the set P in the proof about the unforgeability of a signature scheme [4] was not exact. The above Lemma is the exact result.

Theorem 1. *Let $\mathcal{N}$ be the nonlinear network coding signature scheme described above. Suppose that $\beta = s \cdot \sqrt{m'}$. Then $\mathcal{N}$ is unforgeable assuming that the $\mathbf{SIS}_{q,\beta}$ problem is infeasible.*

In particular, let $\mathcal{A}$ be a polynomial-time adversary as in Definition 2 and make at most Q signature queries. Then there exists a probabilistic polynomial- time algorithm $\mathcal{B}$ that solves the $\mathbf{SIS}_{q,\beta}$ problem, such that

$$\mathbf{Adv}_{\mathbf{SIS}_{q,\beta}}(\mathcal{B}) \ge [1 - \frac{1}{2}(\frac{Q}{2^k} + \frac{Q-1}{2^k - 1})] \cdot \frac{1}{k \cdot Q - g_Q^-} \mathbf{Adv}_{NSIG}(\mathcal{A}) - negl(n).$$

proof. Let $\mathcal{A}$ be an adversary as in Definition 2 that makes at most Q signature queries. We construct an probabilistic polynomial-time algorithm $\mathcal{B}$ that takes as input $m'' = m \cdot (2k+1)$ uniformly random and independent samples from $\mathbb{Z}_q^n$ in the form of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m''}$. Let $\mathbf{A} = \mathbf{U}_0 || \mathbf{U}_1^{(0)} || \mathbf{U}_1^{(1)} || \cdots || \mathbf{U}_k^{(0)} || \mathbf{U}_k^{(1)}$, where $\mathbf{U}_0, \mathbf{U}_i^{(b)} \in \mathbb{Z}_q^{n \times m}$.

Algorithm $\mathcal{B}$ simulates the $\mathbf{Gen}$ and $\mathbf{Sign}$ algorithms of NSIG, and works as follows. First, $\mathcal{B}$ invokes $\mathcal{A}$ to receive Q messages $\mu^{(1)}, \mu^{(2)}, \cdots, \mu^{(Q)} \in \{0,1\}^k$ as signature queries. Then $\mathcal{B}$ computes the set P of all strings $p \in \{0,1\}^{\le k}$ having the property that p is a shortest string for which no $\mu^{(j)}$ has p as a prefix. From Lemma 1, there are at most $k \cdot Q - g_Q^-$ strings in the set P. By the proof of Lemma 1, we have that only polynomial time is needed to find the set P.

Next, $\mathcal{B}$ chooses some p from P uniformly at random, let $t = |p|$, and parse p as $p = p_1 || p_2 || \cdots || p_t$ where $|p_i| = 1$ for $1 \le i \le t$. Let F be a one to one mapping $F : \{0,1\}^n \to \mathbb{Z}_2^n$. It then provides a NSIG verification key $pk = (\mathbf{A}_0, \{\mathbf{A}_j^{(b)}\}, F)$ to $\mathcal{A}$, generated as follows:

• Uncontrolled growth: choose a uniformly random matrix $\mathbf{V}_0 \leftarrow^R \mathbb{Z}_2^{n \times m}$. Use the Chinese remainder theorem to compute $\mathbf{A}_0 \in \mathbb{Z}_{2q}^{n \times m}$ such that $\mathbf{A}_0 \equiv U_0 (mod\ q)$ and $\mathbf{A}_0 \equiv \mathbf{V}_0 (mod\ 2)$.

• Uncontrolled growth: for each $i \in [t]$, choose a uniformly random matrix $\mathbf{V}_i^{(0)} \leftarrow^R \mathbb{Z}_2^{n \times m}$. Use the Chinese remainder theorem to compute $\mathbf{A}_i^{(p_i)} \in \mathbb{Z}_{2q}^{n \times m}$ such that $\mathbf{A}_i^{(p_i)} \equiv U_i^{(0)} (mod\ q)$ and $\mathbf{A}_i^{(p_i)} \equiv \mathbf{V}_i^{(0)} (mod\ 2)$.

• Controlled growth: for each $i \in [t]$, invoke $\mathbf{GenBasis}(1^n, 1^m, 2q)$ to generate $\mathbf{A}_i^{(1-p_i)}$ and basis $\mathbf{S}_i$ of $\Lambda^\perp(\mathbf{A}_i^{(1-p_i)})$ such that $||\tilde{\mathbf{S}}_i|| \le \widetilde{L}$.

• Uncontrolled growth: for $i = t+1, \cdots, k$, and $b \in \{0,1\}$, choose a uniformly random matrix $V_i^{(b)} \leftarrow^R \mathbb{Z}_2^{n \times m}$. Use the Chinese remainder theorem to compute $\mathbf{A}_i^{(b)} \in \mathbb{Z}_{2q}^{n \times m}$ such that $\mathbf{A}_i^{(b)} \equiv \mathbf{U}_i^{(b)} (mod\ q)$ and $\mathbf{A}_i^{(b)} \equiv \mathbf{V}_i^{(b)} (mod\ 2)$.

Next, $\mathcal{B}$ generates signatures for each queried message $\mu = \mu^{(j)}$ as follows: let $i \in [t]$ be the first position at which $\mu_i \ne p_i$ where μ_i denote the ith bit of the string μ. Then $\mathcal{B}$ selects an identifier $\mathbf{id}_j$ uniformly at random from the set of identitifiers $\{0,1\}^n$ and generates

$$\sigma_j \leftarrow \mathbf{SampleD}(\mathbf{ExtBasis}(\mathbf{S}_i, \mathbf{A}_\mu), q \cdot F(\mathbf{id}_j), s),$$

where $\mathbf{A}_\mu = \mathbf{A}_L || \mathbf{A}_i^{(1-p_i)} || \mathbf{A}_R$ (for some matrices $\mathbf{A}_L, \mathbf{A}_R$). (In the event that $||\mathbf{v}|| > \beta$, resample $\mathbf{SampleD}$.) $\mathcal{B}$ sends the pair $(\sigma_j, \mathbf{id}_j)$ to the adversary $\mathcal{A}$.

Eventually $\mathcal{A}$ outputs an identifier $\mathbf{id}^*$, a vector $\mu \in \{0,1\}^k$, and a none-zero signature σ^*.

If ($\mathbf{id}^*$, μ^*, $\sigma^* \neq \mathbf{0}$) is a valid forgery, then we have $A_{\mu^*} \cdot \sigma^* \equiv q \cdot F(\mathbf{id}^*)(mod\ 2q)$, $||\sigma^*|| \leq \beta$. Thus $\mathbf{A}_{\mu^*} \cdot \sigma^* \equiv \mathbf{0}(mod\ q)$. $\mathcal{B}$ checks whether p is a prefix of μ^*. If not, $\mathcal{B}$ aborts; otherwise, note that $\mathbf{A}_{\mu^*} = \mathbf{A}_0||\mathbf{A}_1^{(p_1)}||\cdots||\mathbf{A}_t^{(p_t)}||\mathbf{A}_{t+1}^{(\mu_{t+1}^*)}||\cdots||\mathbf{A}_k^{(\mu_k^*)}$. Therefore, by inserting zeros into σ^* at the corresponding positions, we get $\sigma'^* \in \mathbb{Z}^{m''}$. Consequently, we have $\mathbf{A}\sigma'^* \equiv \mathbf{0}(mod\ q)$ and $0 < ||\sigma'^*|| \leq \beta$.

Finally, $\mathcal{B}$ outputs $\sigma'^* \in \mathbb{Z}^{m''}$ as a solution to the $\mathbf{SIS}_{q,\beta}$ problem.

Now we analyze that if the simulator $\mathcal{B}$ does not abort, the distribution of the simulator's outputs is (statistically) indistinguishable from the distribution of the outputs in the real signature scheme. It is observed that conditioned on any choice of $p \in P$, $\mathbf{A}_0$ and $\{\mathbf{A}_j^{(b)}\}$ in the verification key pk given to $\mathcal{A}$ are negligibly close to uniform. Furthermore, by $s = \widetilde{L} \cdot \omega(\sqrt{\log n})$ and $||\widetilde{\mathbf{S}}_i|| \leq \widetilde{L}$, we have $s \geq ||\widetilde{\mathbf{S}}_i|| \cdot \omega(\sqrt{\log n})$. Consequently, by Lemma 2.4 of [4] we have that the signatures given to $\mathcal{A}$ are distributed exactly as in the real attack (up to negligible statistical distance). Therefore, $\mathcal{A}$ outputs a valid forgery ($\mathbf{id}^*$, μ^*, $\sigma^* \neq \mathbf{0}$) with probability at least $\mathbf{Adv}_{NSIG}(\mathcal{A}) - negl(n)$.

Next, we observe the situations where the simulator doesn't abort and show that the probability that this happens is at least $[1 - \frac{1}{2}(\frac{Q}{2^k} + \frac{Q-1}{2^k-1})] \cdot \frac{1}{k \cdot Q - g_Q^-}$. When ($\mathbf{id}^*$, μ^*, $\sigma^* \neq \mathbf{0}$) is a valid forgery, we have that (1) $\mathbf{id}^* \neq \mathbf{id}_i$ for all i, or (2) $\mathbf{id}^* \neq \mathbf{id}_{i_0}$ but $\mu^* \neq \mu_{i_0}$. If a valid forgery has been given, assume that the probabilities of type 1 forgery and type 2 forgery are both $1/2$. Thus the probability that $\mu^* \neq \mu_i$ for $i = 1, 2, \cdots, Q$ is $\frac{1}{2} \cdot (1 - \frac{Q}{2^k}) + \frac{1}{2} \cdot (1 - \frac{Q-1}{2^k-1})$. When $\mu^* \neq \mu_i$ for $i = 1, 2, \cdots, Q$, we conclude that a prefix of μ^* must be in the set P. Since p is chosen from P uniformly at random, we have that p is a prefix of μ^* with probability $[\frac{1}{2} \cdot (1 - \frac{Q}{2^k}) + \frac{1}{2} \cdot (1 - \frac{Q-1}{2^k-1})] \cdot \frac{1}{|P|} \geq [1 - \frac{1}{2}(\frac{Q}{2^k} + \frac{Q-1}{2^k-1})] \cdot \frac{1}{k \cdot Q - g_Q^-}$ conditioned on the valid forgery.

Consequently, we have that

$$\mathbf{Adv}_{\mathbf{SIS}_{q,\beta}}(\mathcal{B}) \geq [1 - \frac{1}{2}(\frac{Q}{2^k} + \frac{Q-1}{2^k-1})] \cdot \frac{1}{k \cdot Q - g_Q^-} \mathbf{Adv}_{NSIG}(\mathcal{A}) - negl(n).$$

4. Conclusion

Recently, nonlinear network coding and lattice-based cryptography have aroused great interest in the information security field. But existing network coding signature schemes are only suitable for linear network coding. In this paper we have studied nonlinear network coding signature scheme based on the hardness of the small integer solution (**SIS**) problem and its unforgeability. Our contribution is three-fold. Firstly, we have introduced the concepts of nonlinear network coding signature scheme and its unforgeability. Secondly, we have improved the theorem which presented the unforgeability of a signature scheme without identifiers proposed by David Cash et.al. in EUROCRYPT 2010. Finally, based on the result, by adding identifiers to the former scheme and modifying the corresponding parameter as well as the verification items, we have designed a nonlinear network coding signature scheme, and the unforgeability has been proved by employing the Chinese remainder theorem and the technique proposed by David Cash et.al. in EUROCRYPT 2010.

5. Acknowledgments

This work is supported by the Natural Science Foundation of China (60973105 and 60963006), the Research Fund for the Doctoral Program of Higher Education of China (20101303110004 and

20111102130003), the Fund of the State Key Laboratory of Software Development Environment under Grant No. SKLSDE-2011ZX-03, the Innovation Foundation of Beihang University for Ph.D. Graduates under Grant No. 2011106014, and the Fund of the Scholarship Award for Excellent Doctoral Student granted by Ministry of Education under Grant No.400618.

References

[1] Gkantsidis, C., Rodriguez, P.: Network coding for large scale content distribution. In Proc. of IEEE INFOCOM 2005, 2235-2245, 2005.

[2] Boneh, D., Freeman, D., Katz, J., Waters, B.: Signing a Linear Subspace: Signature Schemes for Network Coding. In Public-Key Cryptography-PKC'09. LNCS, vol. 5443, pp. 68-87. Springer, Heidelberg (2009).

[3] Boneh, D., Freeman, D.: Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures. In Public Key Cryptography-PKC 2011. LNCS, vol. 6571, pp. 1-16. Springer, Heidelberg (2011).

[4] Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai Trees, or How to Delegate a Lattice Basis. In Proceedings of EUROCRYPT'2010, 523-552, 2010.

[5] Krohn, M., Freedman, M., Mazieres, D.: On the-fly verification of rateless erasure codes for efficient content distribution. In Proc. of IEEE Symposium on Security and Privacy 2004, 226-240, 2004.

[6] Kosut, O., Tong, L., Tse, D.: Nonlinear Network Coding is Necessary to Combat General Byzantine. In Proc. 47th Allerton Conf. Commun., Control, and Comput., 593-599, 2009.

[7] Dougherty, R., Freiling, C., Zeger, K.: Insufficiency of linear coding in network information flow. IEEE Transactions on Information Theory, V51, N8, pp. 2745-2759 (2005).

[8] Shadbakht, S., Hassibi, B.: MCMC methods for entropy optimization and nonlinear network coding. In proc. of IEEE Int. Sym. on Inf. Theory (ISIT), Austin, TX, pp. 2383-2387 (2010).

[9] Koike-Akino, T., Larsson, P., Popovski, P., Tarokh, V.: Non-linear network coding in two-way relaying discrete channels. Wireless Communications and Signal Processing, pp. 1-5 (2009).

Authors :

Yanqing Yao: Yanqing Yao received her B.S. degree and M.S. degree in the College of Mathematics and Information Science, Hebei Normal University, China in 2007 and 2010 respectively. She is currently a PhD candidate of Beihang University in China. Her research interest includes Cryptography, Information Security, and the Mathematical Basis of Artificial Intelligence.

Zhoujun Li: Zhoujun Li received his B.S. degree in Computer Science from Wuhan University, China, in 1984. He received the M.S. and Ph.D. degrees in Computer Science from National University of Defense Technology, China, in 1986 and 1999, respectively. He is currently a professor of Beihang University. His research interest includes Information Security.

Hua Guo: Hua Guo received her B.S. degree in Computer Science from Information Engineer University, China, in 2003. She received the M.S. degrees in Computer Science from Zhengzhou University, China, in 2006. She is currently a lecture at Beihang University in China. Her research interest includes Cryptography and Information Security.