Practical Schemes for Tunable Secure Network Coding

Guangjun Liu
School of Mathematics and Computer Engineering, Xi'an University
Xi'an, 710065 – China
[e-mail: liuguangjuns@gmail.com]
*Corresponding author: Guangjun Liu

Received August 2, 2014; revised October 10, 2014; revised November 21, 2014; revised January 19, 2015; accepted January 26, 2015; published March 31, 2015

Abstract

Network coding is promising to maximize network throughput and improve the resilience to random network failures in various networking systems. In this paper, the problem of providing efficient confidentiality for practical network coding system against a global eavesdropper (with full eavesdropping capabilities to the network) is considered. By exploiting a novel combination between the construction technique of systematic Maximum Distance Separable (MDS) erasure coding and traditional cryptographic approach, two efficient schemes are proposed that can achieve the maximum possible rate and minimum encryption overhead respectively on top of any communication network or underlying linear network code. Every generation is first subjected to an encoding by a particular matrix generated by two (or three) Vandermonde matrices, and then parts of coded vectors (or secret symbols) are encrypted before transmitting. The proposed schemes are characterized by tunable and measurable degrees of security and also shown to be of low overhead in computation and bandwidth.

Keywords: Network security, network coding, wiretapping, MDS code, Vandermonde matrix, encryption

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61271174, 11371290 and 61301178) and the Science and Technology Innovation Foundation of Xi'an (Grant No. CXY1352WL28).

http://dx.doi.org/10.3837/tiis.2015.03.020 **ISSN : 1976-7277**

1. Introduction

Network coding is an elegant and novel routing approach that generalizes traditional routing where each node simply stores and forwards the incoming packets [1]. It has been proved that network coding can potentially maximize network capacity, improve transmission efficiency, and increase network robustness [2], [3], [4]. Recently, network coding has received a large number of applications in wired and wireless networks [5]. Moreover, an often noted advantage of network coding over traditional packet forwarding protocols is the inherent protection that it provides against eavesdropping [6]. This inherent security is an important issue of general interest to the research community, and has been attracting much attention.

In [7], Cai and Yeung first studied an information theoretic secure network code over a wiretap network for single source multicast, where a wiretapper can eavesdrop any one but not more than one set of channels, called a wiretap set, unknown by the transmitter and receivers, from a given collection of all possible wiretap sets of a fixed size r. For this special case, they also proved some tight fundamental performance bounds. Subsequently, Feldman et al. [8] pointed out a tradeoff between the size of the message set and the size of the transmission alphabet. The scheme, as well as the scheme in [7], is essentially a coset coding scheme that uses the message to select a coset of a Maximum Distance Separable (MDS) code and transmits a random codeword within the coset. Both can be considered as a generalization of wiretap channel II [9]. A similar equivalent problem was covered in [10]. However, these security schemes with perfect security are only designed for some specific network codes, each also requires coding over a large field and thus shows inefficiency in applications. To address this issue, Silva and Kschischang [11] exploited a universal perfectly secure network coding scheme independent of any linear codes, but involves expensive arithmetic operations over a large extension field. More recently, Cheng et al. [12] extensively investigated the wiretap channel II [9] when the wiretap sets consists of arbitrary subsets of channels and obtained some more general performance bounds comparing to the existing schemes.

For practical consideration, Bhattad and Narayanan [13] proposed a relaxed model of security whose goal is also to get rid of the loss of information rate in the secure network coding and maximally secure against guessing. Herein, security is defined as wiretappers not being able to obtain any meaningful information of source messages without trading off the throughput. However, the scheme incurs complicated construction of an encoding matrix which also depends on the network topology and the specific network code. Thereafter, another weakly secure scheme was introduced by Silva et al. [14] based on rank-metric codes, it can be applied on top of any linear network code seamlessly. Unfortunately, they also showed the existence of universal weakly secure network code, but have not shown an explicit construction. Besides, their code construction involves expensive arithmetic operations over a large extension field at the source, while incurring the similar inefficiency as the scheme in [13]. Furthermore, this practical security was then explored for trusted storage based on a secret sharing technique [15], where part of blocks are protected by the remaining parts, and vice versa. Interestingly, another parallel work with imperfect secrecy under a generalization of wiretap channel II [9] was presented in [16] where the wiretapper can obtain some partial information about the private message which is measured by the equivocation of the message given the symbols obtained by the wiretapper. They also proved a tight region of the achievable rate tuples.

The most attractive advantage of these information theoretic based secure schemes includes that no secret sharing is needed between the source and receivers. Moreover, these schemes also provide measurable or quantifiable privacy-preserving viewing from the angle of information theory. However, the major disadvantage or impracticality of these schemes is that they must restrict the eavesdropping capacity, which is not the case in some realistic scenarios. Actually, as for wireless network, it is possible that a wiretapper can access global network linkages because of the broadcast nature of the wireless interface. To address this problem, securing network coding in conjunction with traditional cryptographic approaches emerges in general applications.

As we all know, traditional encryption has been broadly employing in military or commercial systems. It means that the wiretapper cannot obtain the protected information without the secret key. An intuitive approach based on traditional cryptography is to employ link-to-link encryptions on coded packets. However, this method is not feasible as it will bring heavy computational overhead to each node, and result in significant performance degradation. Hence, it is indeed unwise to encrypt all confidential messages without regard to the intrinsic security properties of network coding in network coding settings.

The mixing feature of network coding can be used to ensure confidentiality more efficiently by protecting much shorter coding vector instead of the long message content. By viewing the network code as a cipher, it is possible to create a lightweight cryptographic scheme that reduces the overall computational complexity. As a practical example, Vilela et al. [17] proposed a computationally secure network coding scheme by means of hidding the precoding matrix. However, the scheme is actually insecure when some plaintext are disclosed unless one-time-pad/precoding is adopted, which will incur heavy bandwidth overhead for transmitting precoding information. Another elegant solution is to protect the coding vectors using Homomorphic Encryption Functions [18], but substantial homomorphic cryptographic operations greatly degrade the communication efficiency. As a variant and extension of the scheme in [17], Lima et al. [19] designed a secure solution by additionally encrypting partial vector packets. However, the same bandwidth overhead occupied as that of global coding vector will be used to transmit the precoding vector. In addition, Zhang et al. [20] proposed a scheme called P-Coding, which would be more inefficient than traditional full encryption since all the information symbols of each generation (even including the global coding vectors) have to be protected.

Mostly, the existing traditional cryptographic based schemes always realize the security by means of the encryption or protection to the global coding vectors. On one hand, the security of this kind cannot be proven to satisfy or guarantee the practical applications; On the other hand, these schemes show to be inefficient in either computation or bandwidth, as the security feature provided by random linear network coding (RLNC) is not fully exploited. More importantly, it is hard to evaluate the degree of security provided by these schemes. Therefore, how to provide efficient and exact security against wiretapping is still an open issue in practical applications for network coding, which becomes the main contribution of our work.

In sum, both kinds of solutions suffer from various drawbacks as mentioned above. In this paper, we further exploit the practically appealing security and propose two efficient weakly secure network coding schemes in terms of bandwidth overhead and security requirement. Both schemes are inspired by the idea of [13], and rely on the novel combination of traditional cryptographic approach and the construction technique of systematic MDS erasure coding by the Vandermonde matrices as presented in [22]. The following are some features of our scheme:

1) It ensures practical security against global eavesdropper and can be applied on top of any network codes.

2) The implementation is computationally efficient and incurs low communication overhead.

3) It provides measurable and tunable confidential service without taking the network topology or specific network code into account, while the tradeoff is easily achieved between security complexity and communication overhead.

The remainder of this paper is organized as follows. Section 2 describes the system model and adversary model, as well as some preliminaries behind this paper. The proposed basic scheme and security analysis are then presented in Section 3 and 4. An alternative scheme with low encryption overhead is shown in Section 5. The performance evaluation of the proposals is exhibited in Section 6. Section 7 surveys some related work. Finally we conclude this paper in Section 8.

2. Models and Preliminaries

2.1 Network Model

We adopt the general random linear network coding model introduced in [4]. A network can be represented as an acyclic directed graph, and each edge is assumed to transport a row vector defined in a finite field F_q in unit time. The transmitted message is firstly divided into a sequence of vector groups of the same size called generations (or sessions), each can be also represented as a matrix containing m (row) vectors $\boldsymbol{v}_i = (v_{i1}, v_{i2}, ..., v_{in}) \in \mathrm{F}_q^n (i = 1, 2, ..., m)$ which span an m-dimensional linear space F_q^n. Here consider a general multicast case in which one source needs to deliver a series of generations to a set of sinks.

Before sending, the source first creates m augmented vectors $\bar{\boldsymbol{v}}_i \in \mathrm{F}_q^{m+n} (i = 1, 2, ..., m)$ for each generation by prefixing $\boldsymbol{v}_i$ with the i^{th} unit vector of dimension m, i.e,

$$\bar{\boldsymbol{v}}_i = (\overbrace{\underbrace{0, \ldots, 0, 1}_{i}, 0, \ldots, 0}^{m}; \boldsymbol{v}_i).$$

For each intermediate node, it receives the vectors $\bar{\boldsymbol{w}}_1, \bar{\boldsymbol{w}}_2, ..., \bar{\boldsymbol{w}}_l$ from its l inputting links respectively, and forwards a linear combination formed by $\bar{\boldsymbol{w}} = \sum_{i=1}^{l} \alpha_i \bar{\boldsymbol{w}}_i$ into each outgoing link, where the coefficients $\alpha_1, \alpha_2, ..., \alpha_l$ are selected in F_q for the outgoing link. Note that only vectors from the same generation are encoded. Obviously, the first m symbols of $\bar{\boldsymbol{w}}$ are termed as global encoding coefficients.

Different methods for selecting the coefficients yield different types of network coding. When the $\{\alpha_i\}$ are deterministic for each intermediate node, the resulting code is referred as deterministic network coding. If the $\{\alpha_i\}$ are chosen randomly and independently by each intermediate node, the resulting code is termed as RLNC.

At the network terminals, every sink performs decoding operations to the received generations. As stated in [4], one generation can be recovered with a high probability if a proper large coding field is utilized in multicast. For example, a sink has received *m* legitimate independent vectors $\bar{\boldsymbol{c}}_i = (\boldsymbol{e}_i ; \boldsymbol{c}_i) \in \mathrm{F}_q^{m+n} (i = 1, 2, ..., m)$ belonging to the generation represented as a matrix $\boldsymbol{F}$ at the source, the sink can recover $\boldsymbol{F}$ using Gaussian Elimination as

$$\boldsymbol{F} = \boldsymbol{U}^{-1} \cdot \boldsymbol{V} ,$$

where $\boldsymbol{U} = (\boldsymbol{e}_1^T, \boldsymbol{e}_2^T, ..., \boldsymbol{e}_m^T)^T$ and $\boldsymbol{V} = (\boldsymbol{c}_1^T, \boldsymbol{c}_2^T, ..., \boldsymbol{c}_m^T)^T$.

2.2 Adversary Model

In this paper, the adversary considered is an internal or external wiretapper with computation bounded power, aims at intercepting packets and decoding them to extract meaningful information. Moreover, the wiretapper has the capabilities to wiretapping all the network transmissions (excluding the secret keys) and possesses full knowledge of encoding and decoding schemes at each node. The eavesdropper with these characteristics is called as global wiretapper, which can be achieved in real practice. Without loss of generality, we assume the source and terminals are always trusted and can never be compromised by an adversary. The wiretapper can be always aware of the existence of the proposed schemes, even also the intermediate nodes can be monitored or compromised.

2.3 Practical Security

Let us denote by *M* the multicast information, and *C* a set of ciphertext messages observed by a wiretapper.

We first recall the Shannon security, where the ciphertext *C* is considered to be secure against wiretapping with regard to *M* if the mutual information between *C* and *M* equals 0, i.e., $I(C; M) = 0$. The security criterion considered by [7], [8], [10], [11] fall in this category.

Compared to the Shannon security, the weakly secure network coding proposed by [13] is a different information theoretic security model with more practically appealing. We term this type of security in this paper as practical security.

Under practical secrecy criterion, the ciphertext *C* is considered to be secure with regard to *M* if *C* has no meaningful information with regard to *M*, that is, $I(x_i; M)=0$, $\forall x_i \in M$. For example, if a wiretapper can only observe the message of the form $c = 4x + 3y$ over F_q, a practical secure scheme guarantees that $I(x;c) = I(y;c) = 0$, but $I(x, y; c) \neq 0$. Naturally, the goal of an adversary is to recover as much meaningful information with regard to the plaintext data as possible.

Practical security is more suitable for energy-constrained networks where network coding applications may not have perfect secure requirements in practice. The most appealing advantage of the practical security is that it allows communication at maximum rate while ensuring that only meaningless information is leaked to the adversary.

2.4 Matrices with No Singular Square Submatrices

In practical applications, the matrices over F_q with no singular square submatrices are used to build systematic MDS erasure codes. Over a given finite field, the matrices with this property can be constructed according to the following theorem.

Theorem 1 ([21]): Let us denote by $\boldsymbol{A}$ and $\boldsymbol{B}$ two $r \times r$ matrices of rank *r* over a given field such that any $r \times r$ submatrix of the $r \times 2r$ matrix $(\boldsymbol{A} | \boldsymbol{B})$ has a rank r, the matrix $\boldsymbol{A}^{-1} \cdot \boldsymbol{B}$ is such that any of its square submatrices is nonsingular.

Among the matrices with this property, the class constructed by two Vandermonde matrices is an excellent candidate to build systematic MDS codes principally since matrix-vector multiplications can be performed very efficiently, especially when fast Fourier transform (FFT) can be used [23].

3. Proposed Secure Network Coding Scheme

In this section, we introduce the basic secure scheme for RLNC over wireless networks. The scheme can be naturally used for deterministic network coding over wired networks.

The plaintext of the generation is represented as an $m \times n$ matrix $\boldsymbol{M} = (\boldsymbol{v}_1^T, \boldsymbol{v}_2^T, \ldots, \boldsymbol{v}_m^T)^T$, where $\boldsymbol{v}_i = (v_{i1}, v_{i2}, \ldots, v_{in}) \in \mathrm{F}_q^n (i = 1, 2, \ldots, m)$ are termed as source vectors. Also, the Vandermonde matrix $(a_i^{j-1})_{i,j=1}^m$ is denote by $V(a_1, a_2, ..., a_m)$ in following text. To make concise presentation, a transmitting instance for only one generation is presented below.

3.1 Secure Source Coding

Before source coding, the proposed scheme needs a one-time key pre-distribution to begin with, the relevant technique of key distribution is complemented later. To achieve security, the key idea is to encrypt the crucial information by which the plaintext can be easily recovered. Under this idea, the following operation steps need to be performed:

1) The source generates two public $m \times m$ Vandermonde matrices $\boldsymbol{V}_1 = V(a_1, a_2, ..., a_m)$ and $\boldsymbol{V}_2 = V(b_1, b_2, ..., b_m)$ over F_q, and computes

$$\boldsymbol{A} = \boldsymbol{V}_1^{-1} \cdot \boldsymbol{V}_2,\ \boldsymbol{W} = \boldsymbol{A} \cdot \boldsymbol{M} = (\boldsymbol{w}_1^T, \boldsymbol{w}_2^T, \ldots, \boldsymbol{w}_m^T)^T .$$

2) The vectors $\boldsymbol{w}_{i_1}, \boldsymbol{w}_{i_2}, ..., \boldsymbol{w}_{i_r}$ are encrypted to be the vectors $\boldsymbol{z}_1, \boldsymbol{z}_2, ..., \boldsymbol{z}_m$ using an encryption mechanism E (such as, AES in a stream cipher mode), where the integer set $\{i_1, i_2, ..., i_r\} \subset \{1, 2, ..., m\}$ is pre-determined and $\boldsymbol{z}_{i_k} = E(\boldsymbol{w}_{i_k})(k = 1, 2, ..., r)$.

3) The source constructs the packets $\boldsymbol{p}_i (i = 1, 2, ..., m)$ which are composed by prefixing $\boldsymbol{z}_i$ with the i^{th} unit vector of dimension m. The packets are then sent out to the network.

For simplicity, the case without loss of generality that the first r vectors, i.e., $\boldsymbol{w}_1, \boldsymbol{w}_2, ..., \boldsymbol{w}_r$, are encrypted is considered herein. Let us consider a scenario such as the one when m = 3, r = 1 at the source coding depicted in **Fig. 1**.

3.2 Packets Relay

The network forwarder (or encoder) is an important component of the wireless relays of the network coded system. Every forwarder linearly combines the received packets according to the rules of standard RLNC protocol [4].

3.3 Decoding at Sinks

A sink (or recipient) first applies Gaussian elimination on the global encoding matrix to decode $\boldsymbol{z}_1, \boldsymbol{z}_2, ..., \boldsymbol{z}_m$ and then decrypts $\boldsymbol{z}_1, \boldsymbol{z}_2, ..., \boldsymbol{z}_r$ with the corresponding key as to recover the vectors $\boldsymbol{w}_1, \boldsymbol{w}_2, ..., \boldsymbol{w}_r$. Using the publicly constructed matrix ***A***, the sink obtains the plaintext vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, ..., \boldsymbol{v}_m$ by $\boldsymbol{M} = \boldsymbol{A}^{-1} \cdot \boldsymbol{W}$.

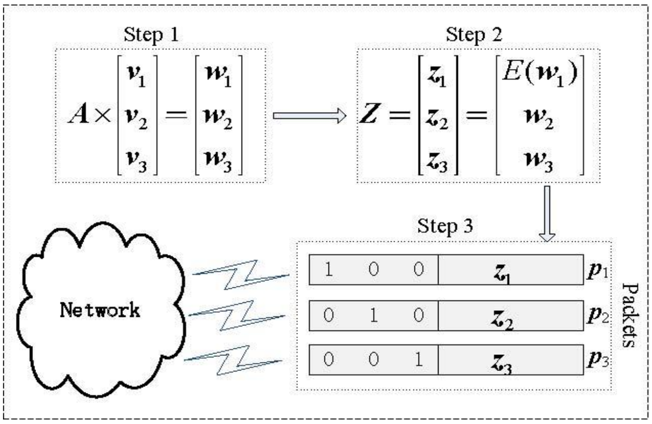
Step 1
$A \times \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix}$
Step 2
$Z = \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{bmatrix} E(w_1) \\ w_2 \\ w_3 \end{bmatrix}$
Step 3
Network
1 0 0 z_1 p_1
0 1 0 z_2 p_2
0 0 1 z_3 p_3
Packets

Fig. 1. Illustration of the operations at the source when $m = 3, r = 1$. The source vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, ..., \boldsymbol{v}_m$ are encoded to be $\boldsymbol{z}_1, \boldsymbol{z}_2, ..., \boldsymbol{z}_m$ at the step 1 and 2. One row of identity matrix is generated for each coded source vector. Each packet is composed by a header which includes a row of identity matrix $\boldsymbol{I}_3$. Then the packets are sent into the network using standard network coding protocol.

4. Security Analysis

In this section, the proposed scheme is shown to be secure against wiretapping attacks under the following feasible constraints. Each element of the original data, or plaintext, is uniformly distributed and mutually independent over $\mathbb{F}_q$. Actually, it can always be satisfied by applying entropy coding on the source vectors. Besides, we assume that the used cipher *E* such that the output is independent of the plaintext and uniform distributed over $\mathbb{F}_q$.

Theorem 2: For a computational bounded adversary, the proposed scheme can achieve practical security to protect the plaintext ***M*** even if the entire ciphertext ***Z*** has been wiretapped.

Proof*:** Consider that each plaintext symbol is mutually independent and uniformly distributed over $\mathbb{F}_q$, we can easily conclude that the same statistical properties is satisfied among the columns of any one generation plaintext matrix ***M. Therefore, the security discussion to the first column of ***M*** (donoted as $\boldsymbol{s} = (v_{11}, v_{21}, ..., v_{m1})$) is enough in the following.

Assume that a wiretapper has collected as many packets to recover all $\boldsymbol{z}_i (i = 1, 2, ..., m)$, but he cannot obtain any meaningful information about $w_{11}, w_{21}, ..., w_{r1}$ which are encrypted by a secure cipher *E*. Although $w_{r+1,1}, w_{r+2,1}, ..., w_{m1}$ and ***A*** can be observed by the wiretapper, they do not help him to solve the plaintext vector ***s*** with *m* unknowns by *m-r* linear equations.

From the statement of Theorem 2 in [13], if a secure scheme is considered to be weakly secure, it must resist a certain number of guesses, which is also a threshold against wiretapping. If more guesses beyond the threshold can be done by the wiretapper, he can also recover all plaintext vectors.

Next, we will show that our scheme can effectively resist r-1 guesses with regard to $\boldsymbol{s}$, i.e., the security threshold to recover $\boldsymbol{s}$ is r-1.

There exists a wiretapper that has the ability to guess any subset of r-1 elements of $\boldsymbol{s}$. Without loss of generality, we assume that the guessed plaintext subset Φ consists of the first r-1 elements of $\boldsymbol{s}$. To recover the content of $\boldsymbol{s}$, the wiretapper must construct and try to solve the following system of equations according to the known information, i.e.,

$$\begin{pmatrix} a_{r+1,1} & a_{r+1,2} & \cdots & a_{r+1,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} v_{11} \\ \vdots \\ v_{r-1,1} \\ v_{r1} \\ \vdots \\ v_{m1} \end{pmatrix} = \begin{pmatrix} w_{11} \\ \vdots \\ w_{r-1,1} \\ w_{r1} \\ \vdots \\ w_{m1} \end{pmatrix}. \tag{1}$$

When the wiretapper sets $v_{i1} = \hat{v}_{i1} (i = 1,2,...,r\text{-}1)$ after r-1 guesses, we have that

$$\begin{pmatrix} a_{r+1,r} & a_{r+1,r+1} & \cdots & a_{r+1,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{mr} & a_{m,r+1} & \cdots & a_{mm} \end{pmatrix} \begin{pmatrix} v_{r1} \\ v_{r+1,1} \\ \vdots \\ v_{m1} \end{pmatrix} = \begin{pmatrix} \varpi_{r+1,1} \\ \vdots \\ \varpi_{m1} \end{pmatrix}, \tag{2}$$

where $\varpi_{i1} = w_{i1} - \sum_{l=1}^{r-1} a_{r+1,l} \cdot \hat{v}_{l1} (i = r+1, \ldots, m)$.

It is easily to show that the system (2) always exists a free variable for each equation. Note that any square submatrices of $\boldsymbol{A}$ is nonsingular, the coefficient matrix (denoted by $\boldsymbol{A'}$) of (2) should be full row rank according to Theorem 1. Therefore, when we put the coefficient matrix $\boldsymbol{A'}$ in the reduced row echelon form $(\boldsymbol{I}_{m-r}; \boldsymbol{h}^T)$, the last column $\boldsymbol{h}^T$ cannot include 0. Otherwise, we assume the first element is 0, the square matrix composed by all the columns of $\boldsymbol{A'}$ except the first one is an exact singular matrix, which is a contradiction.

From the information-theoretical aspect, we have that the mutual information between the ciphertext and the guessed plaintext subset equals to 0, i.e., $I(\boldsymbol{z}_1, \boldsymbol{z}_2, \ldots, \boldsymbol{z}_m; \Phi) = 0$. The result always implies that $I(\boldsymbol{z}_1, \boldsymbol{z}_2, \ldots, \boldsymbol{z}_m; v_{i1}) = 0 (i = 1,2,...,m)$ in conjunction with the above statements, which obviously meets the practical security criterion in this paper.

Generally, the security analysis to the case that Φ is any arbitrary r-1 plaintext symbol guessed set is similar to the discussion above. Particularly, if the r-1 guesses to the unknown symbols of the chosen subset Φ are exact what values of they are, then one more successful guess would result in full disclosure of the plaintext data. □

Theorem 2 shows that the algebraic property of $\boldsymbol{A}$ guarantees that the proposed scheme is always practical secure against any r-1 successful guesses to the plaintext data. Although the wiretapper can observe the other *n-r* packets that are not encrypted, he cannot recover any value(s) of the plaintext symbol(s) unless all encrypted packets have been revealed.

But have to say, the efficiency of the source coding is even more important than security in some scenarios such as real-time or resource-constrained networks. We observe that the proposed scheme may consume much computation resource for encryption operation and the resulting coding complexity maybe still a burden for some resource-constrained systems. To overcome this issue, an alternative smarter scheme is designed for more general circumstances, and particularly features lower encryption overhead for those special applications in the following section.

5. An Alternative Scheme With Low Encryption Overhead

Recall the proposed basic scheme just described can achieve the maximum possible rate for transmission. In reality, the tradeoff between security overhead and bandwidth usage is feasible to improve the system efficiency for practical requirement. It is possible that a little bandwidth sacrifice would be exchanged for greatly reduce the security overhead, under which a lightweight scheme is obtained with low encryption overhead based on the basic scheme.

5.1 Construction

As the basic scheme, the key pre-distribution is first performed in advance. The details of this scheme performed at the source and sinks are described as follows:

(1) Secure Source Coding

1) Generates two public $m \times m$ Vandermonde matrices $\boldsymbol{V}_1 = V(a_1, a_2, ..., a_m)$, $\boldsymbol{V}_2 = V(b_1, b_2, ..., b_m)$ over F_q, and r vectors $\Delta_i = (\sigma_i, \sigma_i^2, \ldots, \sigma_i^m)(i = 1, 2, \ldots, r)$, where σ_i are chosen uniformly at random from all non-zero elements of F_q.

2) Computes $\boldsymbol{A} = \boldsymbol{V}_1^{-1} \cdot \boldsymbol{V}_2 = (\boldsymbol{a}_1^T, \boldsymbol{a}_2^T, \ldots, \boldsymbol{a}_m^T)^T$.

3) Chooses a pre-determined integer set $\{i_1, i_2, ..., i_r\} \subset \{1, 2, ..., m\}$ and constructs an encoding matrix $\boldsymbol{A}^* = (\boldsymbol{a}_1^*, \boldsymbol{a}_2^*, ..., \boldsymbol{a}_m^*)$ where $|\boldsymbol{A}^*| \neq 0$ and

$$\boldsymbol{a}_j^* = \begin{cases} \Delta_j & j = i_1, i_2, \ldots, i_r, \\ \boldsymbol{a}_j & otherwise. \end{cases}$$

4) Computes $\boldsymbol{W} = \boldsymbol{A}^* \cdot \boldsymbol{M} = (\boldsymbol{w}_1^T, \boldsymbol{w}_2^T, \ldots, \boldsymbol{w}_m^T)^T$.

Obviously, the encoding matrix $\boldsymbol{A}^*$ is generated by three Vandermonde matrices $\boldsymbol{V}_1$, $\boldsymbol{V}_2$ and $\boldsymbol{V}_3 = (\Delta_1^T, \Delta_2^T, \ldots, \Delta_r^T)^T$.

5) Encrypts σ_k to be $\beta_k = E(\sigma_k), k = 1, 2, \ldots, r$. When $k = i_1, i_2, ..., i_r$, β_k is attached to be the prefix of the vector $\boldsymbol{w}_k$; Otherwise, an arbitrary element β_k over F_q is padded to be the prefix of $\boldsymbol{w}_k (k \neq i_1, i_2, \ldots, i_r)$.

6) Generates the packet $\boldsymbol{p}_i (i = 1, 2, ..., m)$ as the following form, which is composed by prefixing $\boldsymbol{z}_i = \boldsymbol{w}_i$ with the i^{th} unit vector of m dimension, i.e.,

$$\boldsymbol{p}_i = (\overbrace{\underbrace{0,\ldots,0,1}_{i},0,\ldots,0}^{m};\beta_i;\boldsymbol{z}_i).$$

The packets $\boldsymbol{p}_1, \boldsymbol{p}_2,..., \boldsymbol{p}_m$ are then sent into the network using standard RLNC protocol. Another operation instance when m = 3, r = 1 for secure source coding is illustrated in Fig. 2.

(2) Decoding at Sinks

Every sink first decodes the packets $\boldsymbol{p}_1, \boldsymbol{p}_2,..., \boldsymbol{p}_m$ using Gaussian elimination, and then decrypts $\beta_k (k = i_1, i_2, \ldots, i_r)$. Finally, the plaintext generation matrix $\boldsymbol{M}$ is recovered at the sink through the matrix $\boldsymbol{A}^*$.

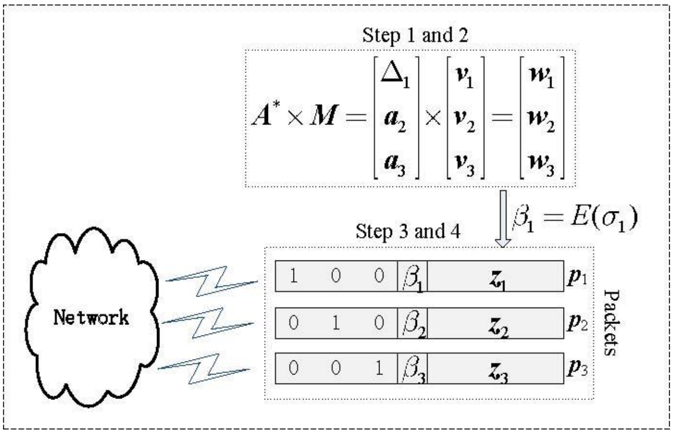
Step 1 and 2
$\boldsymbol{A}^* \times \boldsymbol{M} = \begin{bmatrix} \Delta_1 \\ \boldsymbol{a}_2 \\ \boldsymbol{a}_3 \end{bmatrix} \times \begin{bmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \boldsymbol{v}_3 \end{bmatrix} = \begin{bmatrix} \boldsymbol{w}_1 \\ \boldsymbol{w}_2 \\ \boldsymbol{w}_3 \end{bmatrix}$
$\beta_1 = E(\sigma_1)$
Step 3 and 4
Network
1 0 0 β_1 $\boldsymbol{z}_1$ $\boldsymbol{p}_1$
0 1 0 β_2 $\boldsymbol{z}_2$ $\boldsymbol{p}_2$
0 0 1 β_3 $\boldsymbol{z}_3$ $\boldsymbol{p}_3$
Packets

Fig. 2. Illustration of the operations at the source when $m = 3, r = 1$ and i_1=1. Note that $\Delta_1 = (\sigma_1, \sigma_1^2, ..., \sigma_1^m)$, $\boldsymbol{z}_i$=$\boldsymbol{w}_i$ but β_2, β_3 are padded by two arbitrary elements from F_q.

5.2 Security Analysis

The alternative scheme is a variant and extension of the basic scheme, and characterized by a lightweight security with less encryption operations is performed. Under the same assumption, the security of the alternative scheme is discussed similarly as the basic scheme.

First, a lemma is first shown in the following.

Lemma 1: Let the plaintext data be a vector m= $(m_1, m_2,..., m_m)$ whose components m_i, i = 1, 2,…, m, are random symbols independently and uniformly distributed over F_q, β is a random symbol chosen from F_q. If $\boldsymbol{\eta} = (\eta_1, \eta_2, \ldots, \eta_m) = (\beta, \beta^2, \ldots, \beta^m)$ and $\delta = \boldsymbol{\mu} \cdot \boldsymbol{\eta}$, the mutual information between $\boldsymbol{\mu}$ and δ is zero.

Proof: The lemma is easy to follow. Actually, we have that

$$\begin{aligned} I(\boldsymbol{\mu};\delta) &= H(\boldsymbol{\mu}) - H(\boldsymbol{\mu} \mid \delta) \\ &= H(\mu_1, \mu_2, ..., \mu_m) - H(\mu_1, \mu_2, ..., \mu_m \mid \delta). \end{aligned} \tag{3}$$

According to the chain rule of entropy, we have

$$H(\mu_1, \mu_2, ..., \mu_m \mid \delta) = \sum_{j=1}^{m} H(\mu_j \mid \delta, \hat{\mu}_1, \hat{\mu}_2, ..., \hat{\mu}_{j-1}), \tag{4}$$

where $\hat{\mu}_i$ means a observation or realization of the random variable μ_i. In the following, we only analyze the case $H(\mu_m \mid \delta, \hat{\mu}_1, \hat{\mu}_2, ..., \hat{\mu}_{m-1})$. Note that $\delta = \boldsymbol{\mu} \cdot \boldsymbol{\eta}$, so we have

$$\begin{aligned} & H(\mu_m \mid \delta, \hat{\mu}_1, \hat{\mu}_2, ..., \hat{\mu}_{m-1}) \\ &= H(\mu_m \mid \beta, \hat{\mu}_1, \hat{\mu}_2, ..., \hat{\mu}_{m-1}) \qquad (5) \\ &= H(\mu_m \mid \beta) \qquad (6) \\ &= H(\mu_m). \qquad (7) \end{aligned}$$

where (5) and (6) follows from $\delta = \eta_m \mu_m + \sum_{i=1}^{m-1} \eta_i \hat{\mu}_i$ and $\eta_i = \beta^i$. Eq. (7) is valid because β is independent from μ_m.

Furthermore, the random symbols $\eta_i (i = 1, 2, ..., m)$ are independently and uniformly distributed over F_q, we have that

$$H(\mu_j \mid \delta, \hat{\mu}_1, \hat{\mu}_2, ..., \hat{\mu}_{j-1}) \geq H(\mu_m \mid \delta, \hat{\mu}_1, \hat{\mu}_2, ..., \hat{\mu}_{m-1}) \text{ for } j = 1, 2, ..., m-1.$$

On the other hand, the mutual information $I(\boldsymbol{\mu}; \delta)$ is not always less than 0, then it follows that $I(\boldsymbol{\mu}; \delta) = 0$ from Eq. (3) and Eq. (4).

Theorem 3: For a computational bounded wiretapper, the alternative scheme satisfies the criterion of practical security.

Proof: Without loss of generality, we set $r_i = i (i=1, 2, ..., r)$ and assume the wiretapper has the ability to guess at most r-1 plaintext symbols. We only analyze two typical cases that are the most conducive to the wiretapper. As the same reason in Theorem 2, only the first column of the generation plaintext matrix ***M***, i.e., $\boldsymbol{s} = (v_{11}, v_{21}, ..., v_{m1})$, is considered herein.

1) Case 1: If the wiretapper tries to reveal the secrets set $\beta_1, \beta_2, \ldots, \beta_r$, he has the only way to guess any r-1 secret symbols of the set (here for $\beta_1, \beta_2, \ldots, \beta_{r-1}$ as an example). However, there still exists a free unknown variable β_r, which means that the wiretapper cannot collect any meaningful information to construct $\boldsymbol{A}^*$.
2) Case 2: The wiretapper chooses to distill the plaintext information of the vector $\boldsymbol{s}$. According to Lemma 1, he has no ability to get any meaningful information to $\boldsymbol{s}$ even if $\boldsymbol{z}_1, \boldsymbol{z}_2, ..., \boldsymbol{z}_m$ are all known to the wiretapper. By the discussion in Theorem 2, we can conclude that the alternative scheme can resist any r-1 guesses to any one plaintext vector.

Generally, we can similarly conclude that the wiretapper can also guess any r-1 symbols out of $\beta_1, \beta_2, \ldots, \beta_r$ and $\boldsymbol{s}$. In a nutshell, the alternative scheme satisfies the practical security criterion, and guaranteed practical security against wiretapping in the general scenarios.

6. Performance Analysis

In this section, we discuss the performance of the proposed schemes in term of computational complexity and communication overhead. Besides, the main security characteristics of both schemes are elaborated on as well.

6.1 Computational Complexity

The analysis to the computation overhead of both schemes consists of three parts: (1) matrix-vector multiplication; (2) encryption; (3) decoding at the sinks. As part of public transmitted message, the matrices V_1 and V_2 can be generated offline, so the computation cost to construct them can be neglected in the following discussion.

(1)Matrix-vector multiplication

1) Analysis to the basic scheme

Compared to the standard rule of matrix-vector multiplication, the Vandermonde or inverse of Vandermonde matrix-vector multiplication can be more efficient. As pointed out in [23], the computation complexity is at most $O(m\log^2 m)$ rather than $O(m^2)$ in generic ones. For reducing the computation overhead, the encoding to one generation plaintext matrix $\boldsymbol{M}$ by left multiplying $\boldsymbol{A}$, i.e., $\boldsymbol{A}\cdot\boldsymbol{M}$, can be computed by multiplying $\boldsymbol{M}$ using two matrices, i.e., $\boldsymbol{V}_1^{-1}\cdot(\boldsymbol{V}_2\cdot\boldsymbol{M})$. Since one generation plaintext data is composed by n column vectors, we can conclude that the computational complexity of this part in the basic scheme is $O(mn\log^2 m)$.

Also, the complexity of this part can be further improved considering the case when m is a divisor of q-1 and the two Vandermonde matrices are generated by two elements of $\mathbb{F}_q$ of order m respectively [23]. Under this setting, the encoding operations in this phase can be performed at most $O(mn\log m)$ by using Fast Fourier Transform (FFT).

2) Analysis to the alternative scheme

Different from the basic scheme, the source in the alternative scheme needs to perform standard matrix-vector multiplication, so the computational complexity for matrix-vector multiplication is $O(m^2n)$ as well as $O(rm)$ for generating the Vandermonde matrix $\boldsymbol{V}_3$. In network coded applications, the scheme does not increase the overall compution overhead, because Gaussian elimination is already required for the decoding of network coding, which always performs the same computational complexity, i.e., $O(m^2n)$.

In sum, the proposed schemes present several advantages in source coding complexity. In [13], [14], it is not a easy task of finding a suitable source coding matrix over a large coding field that exactly satisfies the practical security, which greatly lowers the coding efficiency. More seriously, the issue with lack of scalability is primary reason is restraining the existing schemes of this kind applications. As stated in [13], the choice of the source coding matrix is also dependent on the particular network topology and the underlying network code, which severely impacts on the applications of network coding. In contrast, the coding matrix at the source in this paper can be easy and efficient in construction. Due to no adaptation to encode the plaintext data using random matrix as used in [17], [18], the proposed schemes can be more efficiently to prevent the global wiretapping.

(2)Encryption

The encryption to the secret symbols can be efficient implemented using symmetric cipher, such as a block cipher constructed in the counter (CTR) mode [24]. The parameters of the adopted cipher should be adjusted to approximate these criteria [25].

Different from the schemes in [17], [18], the proposals do not additional hide the encoding matrix itself, thus greatly reduce the encryption overhead. In contrast, the encryption volume per generation of the proposals is minimized from nr in the basic scheme to r in the alternative scheme, while this volume in [17], [18] is even up to $m(m+n)$. Obviously, both proposals are characteristic by manageable complexity and lightweight encryption overhead.

(3)Decoding at the sinks

Based on the above discussion, a sink needs to take at most $O(mn\log^2 m)$ or $O(m^2 n)$ algebraic operations in both proposed schemes respectively after decoding using Gaussian Elimination and decryption.

6.2 Communication Overhead

Since the encoding matrix $\boldsymbol{A}$ can be public, so the maximum rate can be achieved using the basic scheme without trading off the throughput. Unlike the schemes in [13], [14], the implementations of the proposed schemes do not require a large field or extension field for secure coding, which makes the computation and bandwidth resource can be further saved. Compared to the basic scheme, the alternative scheme also features lower security overhead, while the ability to reduce the encryption volume comes at the cost of little bandwidth penalty. Luckily, this communication overhead is still far less than that of the schemes in [17], [19], where the precoding matrix must be online exchanged securely therein between the source and sinks.

As stated in Section 3, it is necessary that the proposed schemes require shared secret keys between the source and several legitimate destinations. There has been considerable research that provides security solutions to the key pre-distribution mechanism in multicast. while the specifics of the key pre-distribution mechanism are not the central topic of this paper, but excellent solutions including offline key pre-distribution or broadcast encryption [26] can be commonly recommended in this paper. Before the proposals running, the secret key has been generated and shared among all authorized participates in advance, which would bring to some bandwidth overhead of which the amount is about $O(\log_2 n)$ during the start-up time (n denotes the number of authorized participates in the network). Notice that the key distribution does not pertain to the main body of the proposed scheme itself, so it is easily seeing that the additional overhead brought by the key distribution actually does not affect the light-weight specificity of the proposed schemes in traffic. Thus, the overhead for secret key sharing is omitted in the following analysis.

Table 1 shows that the proposed schemes enjoys important advantages compared to the existing schemes.

Table 1. Comparisons between the proposals and the existing typical schemes

Scheme	Selected field size	Encryption volume per generation (symbols)	Bandwidth overhead
Vilela et al. [17]	Small	m^2	m
Lima et al. [19]	Small	$0.5m(m+1)+rn$	m
Fan et al. [18]	Large	m^2+mn	0
Zhang et al. [20]	Small	m^2+mn	0
Basic proposal	Small	$r(m+n)+m$	0
Alternative proposal	Small	r	1

6.3 Measurable and Tunable Security

From the proofs of Theorem 2 and 3, both schemes can provide the security against global wiretapping with measurable degree which is evaluated by the metric “mutual information” [27]. Actually, both schemes can effectively resist up to *r*-1 guesses to any column vector of any generation plaintext. Furthermore, the security degrees provided by the proposed schemes can be finely tuned since *r* is a tunable systematic parameter, which can characterize different security configurations. Therefore, the proposals can realize and offer a tunable and efficient security service without taking environment and/or application characteristics explicitly into account. Meanwhile, the optimal tradeoff between the security requirement and computational complexity can be achieved easily.

6.4 An Implementation Example

To support our discussion, this section presents a practical implementation using AES. Herein, the source wants to transmit a file of 200 megabytes to the receivers. The file is encoded into 655.360 generations of 320 bytes. Every generation is represented as an 8×20 matrix $\boldsymbol{V}$ in $\mathbb{F}_{2^{16}}$, i.e., $m=8,n=20$. For securing the communication, the source performs the proposed basic scheme for each generation in the same way.

According to the statements in Section 3 and 5, the example needs to encrypt 20 and 1 plaintext symbols per generation respectively when $r=1$ in the basic and alternative schemes, the corresponding encryption ratios are $\frac{20}{160}=12.5\%$ and $\frac{1}{160}=0.625\%$, thus the encryption volumes for the transmission of the file are 25 and 1.25 megabytes. In contrast, the amounts are high up to 80 megabytes and 49 megabytes in [17] and [19] respectively.

7. Discussion

In this paper, we mainly address the issue of designing practical-oriented security for network coded systems. Meanwhile, some other indispensable issues should be paid attention to in real applications.

The information-mixing nature of network coding also renders it highly susceptible to “pollution attacks” in which some faked packets are injected into network information flow. The polluted data packets will propagate quickly that even worse the receivers cannot decode any original plaintext data. As a necessary assistance of our scheme, the techniques in [28], [29] can be used to effectively mitigate pollution attacks whereas at some cost of delay and overhead.

In order to achieve reliable communication over unstable or extreme networks, the alternative solutions, such as resilient network coding [30] or network error-correcting codes [31], should be introduced to improve the robustness for network failure and packet losses/errors. Besides, all the forwarders (including the intermediate nodes and the receivers) should reserve a storing buffer for collecting or decoding the coded packets for network coding.

Which one of the proposals in this paper is selected for concrete applications needs a comprehensive consideration towards the tradeoff between the security complexity and communication overhead. From the above analysis, the basic scheme features low communication overhead, while the alternative scheme is characterized by lightweight security complexity. Although the first can achieve the maximum network throughput, the second one shows a more promising potential for applications due to its lower security penalty.

8. Conclusion

In this paper, we focus on how to achieve practically secure network coding against global wiretapping in an efficient way instead of encrypting all transmitted symbols. The basic idea is to exploit the algebraic structures of systematic MDS erasure codes and Vandermonde matrices by means of the traditional cryptographic technique. Under this idea, we propose two effective schemes with low complexity that can provide measurable and tunable security levels for different requirements. Under the assumption of zero-error communication, the basic scheme is showed to achieve the maximum possible rate, while the alternative scheme is characterized by low encryption overhead. Both can be deployed on top of any communication network without requiring knowledge of the underlying network code.

Our work only focused on wiretapping attacks. We note that systematic MDS codes built from the matrices with no singular submatrices have been widely used in practical applications to cope with losses of data packets [32]. Intuitively, the proposed scheme has the promising potential to be an alternative solution to design secure error-correcting codes (such as the scheme in [33]) against global attackers, which becomes part of our future work.

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol.46, no.4, pp.1204-1216, 2000. Article (CrossRef Link).

[2] R. Koetter, M. Medard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol.11, no.5, pp.782-795, 2003. Article (CrossRef Link).

[3] Y. Chen, G. Feng, L. Zhou, "Using network coding to improve robustness and persistence for data transmission in sensor networks," in *Proc. of 6th International ICST Conference on Communications and Networking in China (CHINACOM)*, pp.1170-1175 , 2011. Article (CrossRef Link).

[4] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol.52, no.10, pp.4413-4430, 2006. Article (CrossRef Link).

[5] C. Fragouli, E. Soljanin, "Network Coding Applications," *Journal of Foundations and Trends in Networking*, vol.2, no.2, pp.135-269, 2007. Article (CrossRef Link).

[6] R. Du, C. Zhao, F. Zhao, S. Li, "Strategies of network coding against nodes conspiracy attack," *Security and Communication Networks*, 2013. Article (CrossRef Link).

[7] N. Cai, R. W. Yeung, "Secure network coding," *in Proc. of International Symposium in Information Theory*, 2002. Article (CrossRef Link).

[8] J. Feldman, T. Malkin, C. Stein, R. A. Servedio, "On the capacity of secure network coding," in *Proc. of 42nd Annual Allerton Conference on Communication, Control, and Computing*, 2004. http://people.csail.mit.edu/jonfeld/pubs/sflow_Allerton04_final.pdf.

[9] L. H. Ozarow, A. D. Wyner, "Wire-tap channel II," *AT&T Bell Labs. Tech. J.*, vol.63, pp.2135-2157, 1984. Article (CrossRef Link).

[10] S. Y. E. Rouayheb, E. Soljanin, A. Sprintson, "Secure network coding for wiretap networks of type II," *IEEE Transactions on Information Theory*, vol.58, no.3, pp.1361-1371, 2012. Article (CrossRef Link).

[11] D. Silva, F.R. Kschischang, "Universal Secure Network Coding via Rank-Metric Codes," *IEEE Transactions on Information Theory*, vol.57, no.2, pp.1124-1135, 2011. Article (CrossRef Link).

[12] F. Cheng, R. W. Yeung, "Performance Bounds on a Wiretap Network with Arbitrary Wiretap Sets," *IEEE Transactions on Information Theory*, vol 60, no.6, 2014. Article (CrossRef Link).

[13] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," in *Proc. of 1st Workshop on Network Coding, Theory, and Applications (NetCod05)*, 2005. http://netcod.org/papers/06BhattadN-final.pdf.

[14] D. Silva, F. R. Kschischang, "Universal weakly secure network coding," in *Proc. of IEEE Information Theory Workshop on Networking and Information Theory*, pp.281-285, 2009. Article (CrossRef Link).

[15] P. F. Oliveira, L. Lima, T. T. V. Vinhoza, M. Médard, J. Barros, "Trusted Storage over Untrusted Networks," in *Proc. of IEEE Global Telecommunications Conference (GLOBECOM)*, pp.1-5, 2010. Article (CrossRef Link).

[16] F. Cheng, R. W. Yeung, K. W. Shum, "Imperfect Secrecy in Wiretap Channel II," in *Proc. of IEEE International Information Theory (ISIT)*, 2012. Article (CrossRef Link).

[17] J. P. Vilela, L. Lima, J. Barros, "Lightweight Security for Network Coding," in *Proc. of the IEEE International Conference on Communications (ICC)*, pp.1750-1754, 2008. Article (CrossRef Link).

[18] Y. Fan, Y. Jiang, H. Zhu, X. Shen, "An efficient privacy-preserving scheme against traffic analysis in network coding," in *Proc. of IEEE INFOCOM'09*, pp.2213-2221, 2009. Article (CrossRef Link).

[19] L. Lima, J. Barros, M. Médard, A. Toledo, "Towards Secure Multiresolution Network Coding," in *Proc. of IEEE Information Theory Workshop on Networking and Information Theory (ITW)*, pp.125-129, Jun.10-12, 2009. Article (CrossRef Link).

[20] P. Zhang, Y. Jiang, C. Lin, Y Fan, X. Shen, "P-Coding: Secure Network Coding against Eavesdropping Attacks," in *Proc. of IEEE INFOCOM'10*, pp.1-9, 2010. Article (CrossRef Link).

[21] J. Lacan, J. Fimes, "A construction of matrices with no singular square submatrices," in *Proc. of the 7th International Conference on Finite Fields and Applications*, *Lecture Notes in Computer Science*, vol.2948, pp.145-147, 2003. Article (CrossRef Link).

[22] J. Lacan, J. Fimes, "Systematic MDS erasure codes based on Vandermonde matrices," *IEEE Communications Letters*, vol.8, no.9, pp.570-572, 2004. Article (CrossRef Link).

[23] I. Gohberg, V. Olshevsky, "Fast algorithms with preprocessing for matrix-vector multiplication problems," *Journal of Complexity*, vol.10, no.4, pp.411-427, 1994. Article (CrossRef Link).

[24] R. A. Mollin, "*An Introduction to Cryptography*," *CRC Press*, 2006.

[25] M. Bellare, A. Desai, E. Jokipii, P. Rogaway, "A concrete security treatment of symmetric encryption," in *Proc. of the 38th Annual Symposium on Foundations of Computer Science,* pp.394-403, 1997. Article (CrossRef Link).

[26] M. J. Moyer, J. R. Rao, P. Rohatgi, "A survey of security issues in multicast communications," *IEEE Network*, vol.13, no.6, pp.12-23, 1999. Article (CrossRef Link).

[27] T. M. Cover, J. A. Thomas, "*Elements of Information Theory*," 2009.

[28] C. Cheng, T. Jiang, "An efficient homomorphic MAC with small key size for authentication in network coding," *IEEE Transactions on Computers*, vol.2, no.10, pp.2096-2100, 2013. Article (CrossRef Link).

[29] P. Zhang, Y. Jiang, C. Lin, H. Yao, A. Wasef, and X. Shen, "Padding for orthogonality: Efficient subspace authentication for network coding," in *Proc. of IEEE INFOCOM*, pp.1026-1034, 2011. Article (CrossRef Link).

[30] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Médard, "Resilient Network Coding in the Presence of Byzantine Adversaries," in *Proc. of IEEE INFOCOM*, pp.616-624, 2007. Article (CrossRef Link).

[31] Z. Zhang, "Linear network error correction codes in packet networks," *IEEE Transactions on Information Theory*, vol.54, no.1, pp.209-218, 2008. Article (CrossRef Link).

[32] F. J. MacWilliams, N. J. A. Sloane, "The Theory of Error-Correcting Codes," New York: North-Holland, 1977.

[33] C. K. Ngai, "Network Coding for Security and Error Correction," *Ph.D. Thesis*, 2008. http://iest2.ie.cuhk.edu.hk/~whyeung/post/thesis/Ngai.pdf.

Guangjun Liu received his M.S. degree in applied mathematics and Ph.D degree in cryptography from Xidian University, Xi'an, China, in 2009 and 2013, respectively. He is currently a lecturer at the school of mathematics and computer engineering in Xi'an University, Xi'an, China. His research interests include cryptography and information security, secure network coding and applications.