Secure Network Coding on a Wiretap Network

Ning Cai, *Senior Member, IEEE,* and Raymond W. Yeung, *Fellow, IEEE*

***Abstract*—In the paradigm of network coding, the nodes in a network are allowed to encode the information received from the input links. With network coding, the full capacity of the network can be utilized. In this paper, we propose a model, call the *wiretap network*, that incorporates information security with network coding. In this model, a collection of subsets of the channels in the network is given, and a wiretapper is allowed to access any one (but not more than one) of these subsets without being able to obtain any information about the message transmitted. Our model includes secret sharing in classical cryptography as a special case. We present a construction of secure linear network codes that can be used provided a certain graph-theoretic condition is satisfied. We also prove the necessity of this condition for the special case that the wiretapper may choose to access any subset of channels of a fixed size. The optimality of our code construction is established for this special case. Finally, we extend our results to the scenario when the wiretapper is allowed to obtain a controlled amount of information about the message.**

***Index Terms*—Algebraic coding, cryptography, multicast, network coding, secret sharing, wiretap channel.**

I. Introduction

The first *information-theoretically secure* communication system, the so-called *Shannon cipher system* studied by Shannon in his celebrated paper [25], is formulated as follows. Suppose a sender wants to send the output of a random source message M with alphabet $\mathcal{M} = \{0, 1, \ldots, p-1\}$ to a receiver. The sender can send information via a "public" channel, whose output can be accessed by the receiver as well as a wiretapper who tries to obtain some information about M, or the sender can send information via a "secure" channel, whose output can be accessed only by the receiver. The usual way to protect M from the wiretapper is that the sender generates a "secret key" K independent of the source message M according to the uniform distribution over $\mathcal{M}$. Let m be the outcome of M, and let k be the outcome of K. Then the sender sends the key k to the receiver via the secure channel, and sends $m+k$ (mod p) via the public channel. Upon receiving both k and $m+k$, the receiver as the legal user can recover m because $m = (m+k)-k$. On the other hand, the wiretapper cannot obtain any information about m by knowing $m+k$ alone because what he/she knows is a total randomization of the message m. In other words, M and K are statistically independent. This notion of security is often referred to as *information-theoretic security* in the literature. In this work, we will refer to it as *perfect security* so as to distinguish from a few other notions of security to be discussed.

The main idea in the above scheme is that the sender has to randomize the message in order to protect it from the wiretapper, where in this case the alphabets of the random key and of the information source have the same size (the two alphabets are the same). Shannon showed in [25] that this protocol is optimal in the sense of minimizing the size of the random key. This result, known as the *perfect secrecy theorem*, has been generalized to the *imperfect secrecy theorem* by Yeung [27] (p. 116).

In the above scheme, if another wiretapper observes k but cannot observe $m+k$, he/she again

The work of N. Cai was partially supported by grants from the National Natural Science Foundation of China (Ref. No. 60832001 and No. 60672119). The work of R. W. Yeung was partially supported by a grant from the Research Grant Committee (RGC Ref. No. CUHK 2/06C) and a grant from the University Grants Committee (Project No. AoE/E-02/08) of the Hong Kong Special Administrative Region, China.

N. Cai is with The State Key Lab. of ISN, Xidian University, Xi'an, Shaanxi, 710071, China. He was with Department of Information Engineering, The Chinese University of Hong Kong, N.T., Hong Kong when this work was done. Email: caining@mail.xidian.edu.cn

R. W. Yeung is with the Institute of Network Coding and Department of Information Engineering, The Chinese University of Hong Kong, N.T., Hong Kong. Email: whyeung@ie.cuhk.edu.hk

cannot obtain any information about M. Thus the only thing we have to do for security is to ensure that an illegal user cannot obtain the outputs of both the public and the secure channels. This observation tells us that there is logically no difference between the public channel and the secure channel. The Shannon cipher system can be regarded as a secure code defined for the simple network in Fig. 1 with two nodes, a source and a sink nodes, connected by two channels, such that a wiretapper can obtain no information about the "secure message" M by accessing any single channel. Based on this observation, in the conference version of the current paper [5], we proposed a model for secure network coding called the *wiretap network*. A wiretap network consists of a communication network and a collection of subsets of wiretap channels in the network. A network code is secure for a wiretap network if a wiretapper can obtain no information about the secure message by accessing any wiretap subset, while all the sink nodes in the network as legal users can decode the secure message with zero error. In particular, a wiretap network is called an r-WN (WN stands for "wiretap network") if the collection of wiretap subsets are all subsets of channels with cardinalities not larger than r. A network code is r-secure if it is secure for an r-WN. That is, for an r-secure network code, a wiretapper can obtain no information about the secure message by accessing any r channels. The Shannon cipher system is the simplest 1-secure network code.

Obviously, for the existence of r-secure network codes, it is necessary that r is strictly smaller than the value of maximum flow from the source node to every sink node, because otherwise a wiretapper accessing all the channels at a minimum cut between the source node and a sink node would have all the information received by the sink node and therefore can correctly decode the secure message. This reveals the fact that for security, a legal user must know more than an illegal one.

Another well-known model of a cipher system is the *secret sharing* model proposed independently by Blakley [3] and Shamir [24] (see also Ozarow and Wyner's wire-tap channel II [22], a special case of secret sharing). This model subsumes the Shannon cipher system. We will show in Section II that our model subsumes secret sharing and in fact, the threshold secret sharing scheme is a special r-secure network code.

One of the main results in [5] was a construction of linear secure network codes, which will be presented in Section III. In the construction, we use a special matrix to transform a non-secure linear network code into a secure network code. The optimality of this construction (discussed in Section IV) was presented in [30]. Subsequent to [5], Feldman *et al.* [11] pointed out that the condition required for the special matrix is equivalent to a Hamming distance property of a certain type of codes. They also derived a tradeoff between the size of the message set $\mathcal{M}$ and the size of the transmission alphabet F. In [10], El Rouayheb and Soljanin presented a construction of secure network codes by using secure codes for wiretap channel II [22]. They first encode the source message by a secure code based on an MDS code for a wiretap channel II and then send the resulting codeword by a linear network code through the network. They derived a secure condition for the described coding schemes and accordingly proposed a code construction. Their bound on the alphabet size for the construction is smaller than ours. Moreover, they showed that their construction is actually equivalent to ours.

Bhattad and Narayanan [2] introduced *weakly secure network coding*, where security is defined as wiretappers not being able to decode any part of source messages correctly. They showed that one can use a weakly secure network code without trading off the throughput.

The r-secure linear network code was strengthened to the *strongly r-secure linear network code* by Harada and Yamamoto [14]. For a strongly r-secure network code, a wiretapper can obtain no information about any s components of the source message by accessing $n - s$ channels provided that the maximum flows to all the sink nodes are at least n, where $s \leq n - r$. They presented a polynomial-time algorithm to construct strongly secure linear network codes. They pointed out that strong security in fact contains weak security in [2] as a special case. In [4], Cai showed that a random linear network code [15] is strongly secure with high probablity, provided that the order of coding field is sufficiently large.

In a recent paper by Ngai *et al.* [20], the gener-

alized Hamming weight for linear error correction codes, introduced by Wei [26], was generalized to linear network codes. They called it the *network generalized Hamming weight* and studied its basic properties. Using these properties, they obtained a complete a characterization of the security performance of a linear block code when it is used in conjunction with a given linear network code.

The model of wiretap network was extended to multiple sources by the authors [6], where the randomness for protecting the source messages can be generated at a set of nodes instead of one node. A necessary and sufficient condition for the security of a linear network code was derived by the authors in this work for the case that all the source messages have positive probability and then by Zhang and Yeung [32] for the general case.

Perhaps the most general model of multi-source secure network coding was due to Chan and Grant [8]. They considered the case of multiple sources and multiple wiretappers. Each wiretapper is interested in a particular subset of the source messages and can access an arbitrary subset of channels in his/her *own* collection of wiretap subsets. Again the security they considered is perfect security, i.e., a wiretapper can obtain no information about the messages he/she is interested in. They obtained a lower bound and an upper bound on the capacity region in term of Γ^*, the region of all entropy functions [28]. In the sequel, we will refer to the model as the general wiretap network.

There have been several alternative models for secure network coding. Among them, Jain [17] focused on the relation between security and network topology. In their model, there is a single source node and a single sink node in the network, and all the nodes may generate randomness to help the secure transmission. They asked when messages can be transmitted with perfect security and did not consider the cost incurred. A necessary and sufficiently condition was derived. The tradeoff between security and the cost of network coding was studied by Tan and Médard [23]. In their model, with certain probability, each channel may be accessed by a wiretapper and the wiretapper is interested in the messages from a subset of sources. Their criterion of security is the probability for the wiretapper to be able to decode the message of interest correctly. They proposed two heuristic solutions and compared their performances with traditional routing by simulation. Their results showed that coding may be more effective for both reducing the cost and increasing the security. In the above literature, security is measured by information quantities (mutual information or entropy) or decoding probability, whereas Lima *et al.* [19] proposed an algebraic secure criterion. They considered the security of random linear network codes and assume that all intermediate nodes are potentially wiretappers who completely comply with the communication protocols in random coding but want to decode the source message transmitted over the network. To measure security they used the number of symbols that an intermediate node has to guess in order to be able to decode one of the transmitted symbols in terms of the rank of the partial global encoding matrix. With this security measure, they analyzed the security of random linear network codes over complete directed acyclic graphs.

Network coding for error correction was studied by [29], [7], where the fundamental coding bounds were obtained. Secure network coding with error correction was studied by Ngai and Yeung [21]. In this work, they presented a construction of secure error-correcting (SEC) network codes that can protect the source message from wiretapping, random errors, and errors injected by the wiretapper. They also proved the optimality of their construction.

In the next section, we present our model of a wiretap network and define a secure network code, which in our terminology is called an admissible code. The difference between our model and some other models are explained in two examples. In Section 3, we first construct a class of linear codes based on the work of Li *et al*. [18] on linear network coding. Then we present a sufficient condition for the construction to be admissible. The proof of the sufficiency of this condition is deferred to Section 5. In Section 4, we prove the optimality of our construction in Section 3 for r-secure network codes. In Section 6, we extend our results to the scenario when the wiretapper is allowed to obtain a controlled amount of information about the message. The paper is concluded in Section 7.

II. Communication System on a Wiretap Network

In this section, we first present our model of the wiretap network. Then we define secure or admissible network codes for a wiretap network.

A wiretap network consists of the following components:

1) *Directed multigraph* $\mathcal{G}$: The pair $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is called a directed multigraph[1], where $\mathcal{V}$ and $\mathcal{E}$ are the node set and the edge set of $\mathcal{G}$, respectively. In our model, we assume that $\mathcal{G}$ is acyclic, i.e., it does not contain a directed cycle.

2) *Source node* s: The node set $\mathcal{V}$ contains a node s, called the source node, where a random message M taking values in an alphabet $\mathcal{M}$ is generated.

3) *Set of user nodes* $\mathcal{U}$: A user node is a node in $\mathcal{V}$ which is fully accessed by a legal user who is required to receive the random message M with zero error. There is generally more than one user node in a network. The set of user nodes is denoted by $\mathcal{U}$.

4) *Collection of sets of wiretap edges* $\mathcal{A}$: $\mathcal{A}$ is a collection of subsets of the edge set $\mathcal{E}$. Each member of $\mathcal{A}$ may be fully accessed by a wiretapper, but no wiretapper may access more than one member of $\mathcal{A}$.

We refer to the quadruple $(\mathcal{G}, s, \mathcal{U}, \mathcal{A})$ as a wiretap network. We also refer to the multigraph $\mathcal{G}$ as a network and the edges in $\mathcal{E}$ as channels. The random message M is generated at the source node s according to an arbitrary distribution on an alphabet $\mathcal{M}$, called the *message set*. On each channel in $\mathcal{E}$, an index taken from an alphabet F called the *transmission alphabet* can be transmitted. We are interested in the maximum value of $|\mathcal{M}|$ for which the message M can be multicast from the source node s to the set of user nodes $\mathcal{U}$ while being protected from *a wiretapper* who can access any set of channels in $\mathcal{A}$.

The system has been extended to *multiple sources* and *multiple wiretapper* in [8], where each wiretapper is interested in the messages from *a subset* of the multiple sources and has his/her own collection of wiretap subsets. In other words, different wiretappers may be interested in different subsets of the sources and may have different collections of wiretap subsets.

The current work is a generalization of the work by Ahlswede *et al*. [1] and Li *et al*. [18] on network coding. In the paradigm of network coding, the nodes in a communication network are allowed to encode the information received from the input links before it is transmitted on the output links. The advantage of network coding is that it can utilize the full capacity of a network for multicasting information.

In the model we study in the current paper, in the absence of a wiretapper, i.e., $\mathcal{A} = \emptyset$, the wiretap network is reduced to the model studied in [1] and [18]. It was proved in [1] that information can be multicast from the source node s to all the user nodes in $\mathcal{U}$ at rate τ if and only if the value of a maximum flow from s to each user node is at least τ in the graph $\mathcal{G}$. In general, information can be multicast from the source node to the user nodes at a higher rate with network coding than without network coding when there are at least two user nodes (see the example in [1], called the *butterfly network*). Subsequently, it was proved in [18] by an explicit construction that this can be achieved by linear network codes. For a comprehensive treatment of network coding, we refer the reader to [28].

As we have discussed earlier, it is necessary to randomize the message in order to protect it from the wiretapper. This can be explained as follows. If there is no randomness in the network, the index transmitted on any channel is a function of the message M and hence is not independent of M unless the index takes a constant value. If this is the case, the channel becomes degenerate as it transmits no useful information. Thus for a wiretap network, without randomness, a wiretapper would be able to obtain some knowledge about the source message by accessing any single "non-degenerate" channel.

Introducing randomness in the network to protect the source message inevitably reduces the throughput because additional bandwidth is needed to transmit different randomized versions of the source message. Note that our secure criterion is that the wiretappers may obtain absolutely no information about *the whole source message*. In the case of the general wiretap network in [8] where there are multiple sources and multiple wiretappers interested

[1]In a multigraph, there can be more than one edge from one node to another node.

in different subsets of the sources, or in the case that the secure criterion is relaxed, it is not always necessary to reduce the throughput for security. This will be shown in Example 2 at end of the section. But first let us define an admissible code for a wiretap network.

Let K be an independent random variable, called the key, that takes values in an alphabet $\mathcal{K}$ according to the uniform distribution. To facilitate our discussion, we denote the sets of input and output channels of a given node $a \in \mathcal{V}$ by $\mathrm{In}(a)$ and $\mathrm{Out}(a)$, respectively. A code for a wiretap network consists of a set of local encoding mappings $\{\phi_e : e \in \mathcal{E}\}$ such that for all e, ϕ_e is a function from $\mathcal{M} \times \mathcal{K}$ to F if $e \in \mathrm{Out}(s)$, and is a function from $F^{|\mathrm{In}(t)|}$ to F if $e \in \mathrm{Out}(t)$ for $t \neq s$. For $e \in \mathcal{E}$, let Y_e be the random symbol in F transmitted on channel e, i.e., the value of ϕ_e. For a subset B of $\mathcal{E}$, denote $(Y_e : e \in B)$ by Y_B.

To complete the description of a code, we have to specify the order in which the channels send the indices, called the *encoding order*. Since the graph $\mathcal{G}$ is acyclic, it defines a partial order on the node set $\mathcal{V}$. Then the nodes in $\mathcal{V}$ can be indexed in a way such that for two nodes t and t', if there is a channel from node t to node t', then $t < t'$. According to this indexing, node t sends indices in its output channels before node t' if and only if $t < t'$. The order in which the channels within the set of output channels of a node send the indices is immaterial. The important point here is that whenever a channel sends an index, all the indices necessary for encoding have already been received. A code defined as such induces a function Φ_u from $\mathcal{M}\times\mathcal{K}$ to $F^{|\mathrm{In}(u)|}$ for all user nodes $u \in \mathcal{U}$, where the value of Φ_u denotes the indices received by the user node u in its input channels.

A code $\{\phi_e : e \in \mathcal{E}\}$ is admissible for a wiretap network $(\mathcal{G}, s, \mathcal{U}, \mathcal{A})$ if the following conditions are satisfied:

1) For all user nodes $u \in \mathcal{U}$ and all $\mathbf{m}, \mathbf{m}' \in \mathcal{M}$ with $\mathbf{m} \neq \mathbf{m}'$,

$$\Phi_u(\mathbf{m}, \mathbf{k}) \neq \Phi_u(\mathbf{m}', \mathbf{k}')$$

for all $\mathbf{k}, \mathbf{k}' \in \mathcal{K}$, where $\mathbf{k}$, and $\mathbf{k}'$ may or may not be the same. This guarantees that any two messages are distinguishable at every user node because the formula ensures that for every user node $u \in \mathcal{U}$, there exist no $\mathbf{k}, \mathbf{k}' \in \mathcal{K}$, be they the same or different, that can produce from two different messages $\mathbf{m}$ and $\mathbf{m}'$ the same set of indices at the input channels of the user node u. This is referred to as *the decodable condition*.

2) For all $A \in \mathcal{A}$

$$H(M|Y_A) = H(M).$$

Here $H(\cdot|\cdot)$ and $H(\cdot)$ denote conditional entropy and entropy, respectively. In other words, M and Y_A are independent. This is referred to as the *secure condition*.

We call a wiretap network an r-WN if $\mathcal{A}$ is the collection of all subsets of channels with cardinalities not exceeding r. An admissible code for an r-WN is called an r-secure network code. For an r-secure network code, a wiretapper can obtain absolutely no information about the source messages by accessing any r channels in the network. Obviously, the Shannon cipher system is a 1-secure network code for the network with a source node s and a user u and two parallel channels from s to u.

In a secret sharing scheme, a random secret message M taken from a finite set $\mathcal{M}$ is shared among n participants in $[n] := \{1, 2, \ldots, n\}$ in such a way that only the so-called qualified subsets of $[n]$ are able to reconstruct M, whereas any other subsets of $[n]$ should know absolutely nothing about M. To share the secret M, a dealer with full access to the secret source sends a random "share" Y_i to every participant $i \in [n]$ according to the value m of the secret message M. A basic problem in secret sharing is

(*) at most how many bits of secret can be shared if each participant i receives at most r_i bits of share, where the non-negative real vector $(r_1, r_2, \ldots, r_n)$ is given.

We can easily see that this is equivalent to asking whether there exists an admissible code for the wiretap network to be described in the next paragraph, and an admissible code for this particular wiretap network is exactly a secret sharing scheme. In this sense, secure network coding contains secret sharing as a special case.

Let a secret sharing scheme be given. Denote by $\mathcal{Q}$ the collection of qualified subsets in $[n]$ and let $\mathcal{Q}_0$ be its minimal sets (i.e., $Q \in \mathcal{Q}_0$ if and

only if $Q \in \mathcal{Q}$ and no other subset of Q is in $\mathcal{Q}$). We now construct a wiretap network which has three layers of nodes: top, middle, and bottom. The only node on the top layer is the source node s and it corresponds to the dealer in the secret sharing scheme. There are n intermediate nodes on the middle layer, each of them corresponding to a participant in the secret sharing scheme. For every $i \in [n]$, the source node s is connected to the intermediate node i by a channel (s, i) with capacity r_i. There are $|\mathcal{Q}_0|$ user nodes labelled by $\mathcal{Q}_0$ on the bottom layer. An intermediate node i is connected to a user node $Q \in \mathcal{Q}_0$ if and only if $i \in Q$. Finally, the collection of wiretap subsets is defined as $\mathcal{A} = \{\{(s, i), i \in A\} : A \in 2^{[n]} \setminus \mathcal{Q}\}$, where $2^{[n]}$ is the power set of $[n]$. Obviously, for the given secret sharing scheme, the network code sending the random share Y_i to the intermediate node i for all $i \in [n]$ is admissible, because each user node on the bottom layer can decode the secret message by virtue of the secret sharing scheme. On the other hand, an admissible code for the network defines a secret sharing scheme.

An (r, n)-threshold secret sharing scheme [3][24], where $r \leq n$, is a secret sharing scheme such that any r of the n participants can correctly recover the secret message but any $r-1$ or less participants can have no information about the secret message. Then obviously an (r, n)-threshold secret sharing scheme is equivalent to an $(r-1)$-secure network code for the network described in the last paragraph. As in general the problem (*) is extremely hard, to find optimal admissible codes for an arbitrary wiretap network is a very difficult problem.

Example 1 (Secret Sharing): Consider the wiretap network shown in Fig. 1 with

$$\mathcal{U} = \{u_1, u_2, u_3\}$$

and

$$\mathcal{A} = \{\{(s, a_1)\}, \{(s, a_2)\}, \{(s, a_3)\}\}.$$

This wiretap network represents the $(2, 3)$-threshold secret sharing scheme.

In the definition of our admissible code, we use perfect security as the secure condition. To achieve this level of security, however, a relatively high price needs to be paid in terms of the throughput as well as the amount of randomness used in the scheme. As such, some weaker secure conditions have been proposed. The following example gives a comparison between perfect secrecy and these secure conditions.

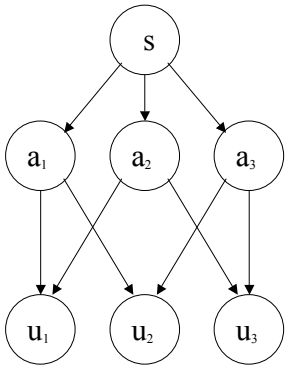

Fig. 1. A wiretap network representing the $(2, 3)$-threshold secret sharing scheme.

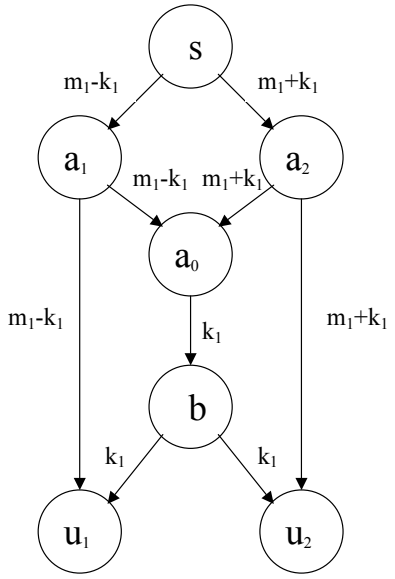

Fig. 2. An example of an admissible code for a wiretap network.

Example 2: Consider the wiretap network shown in the Fig. 2 with

$$\mathcal{U} = \{u_1, u_2\}$$

and

$$\mathcal{A} = \{\{e\} : e \in \mathcal{E}\}.$$

That is, the wiretap network is obtained by adding

a collection $\mathcal{A}$ of subsets of wiretap channels to the well-known butterfly network in [1], where the wiretapper can access any single channel in the network. To simplify our discussion, we assume that the source message M is generated according to the uniform distribution on $\mathcal{M}$. In the wiretap network, there are exactly two disjoint paths from the source node s to each of the user nodes u_1 and u_2. For each $A \in \mathcal{A}$, which contains exactly one channel, there is one path that starts at the source node s and has that channel in A as the last channel on the path. Such a path will be called a path from the source node s to A. For example,

$$(s, a_1), (a_1, a_0), (a_0, b)$$

is a path from the source node s to $A = \{(a_0, b)\}$.

We now describe a linear network code for this wiretap network over $GF(3)$. Let M be a ternary source taking values in $GF(3)$. At the source node s, an independent random key K is also generated according to the uniform distribution on $GF(3)$. Denote the values taken by M and K by m_1 and k_1, respectively. Then Figure 2 shows a linear network code on the wiretap network. It is easy to check that such a code satisfies the decodable condition and the secure condition, and is therefore admissible. In fact, as we will see, the existence of such an admissible code is guaranteed by Theorem 3.

Weak security introduced by Bhattad and Narayanan [2] is defined as that a wiretapper cannot decode any component of the source message correctly. It was shown that there is no extra cost for weak security provided that the coding field is sufficiently large and that the wiretapper is not allowed to obtain all the information received by any single user. This can be done over $GF(q)$ with $q \geq 4$ in the butterfly network as follows. Let $M = (M_1, M_2)$ be generated at the source node s, where M_1 and M_2 are two independent random symbols taking values in $GF(q)$ according to the uniform distribution. Denote by m_i the value of $M_i, i = 1, 2$. Let α_0, α_1, and α_2 be three distinct non-zero elements in $GF(q)$. The source node s sends $m_1 + \alpha_1 m_2$ to u_1 and a_0 through a_1, and sends $m_2 + \alpha_2 m_2$ to u_2 and a_0 through a_2. Upon receiving $m_1 + \alpha_1 m_2$ and $m_1 + \alpha_2 m_2$, a_0 then sends $m_1 + \alpha_0 m_2$ to u_1 and u_2 through b. Obviously, the code is weakly secure if the wiretapper cannot access any two channels transmitting linearly independent information simultaneously. In this scheme, the number of symbols that can be sent to the users is equal to the maximum flow from the source node to the each of the user node, so that there is no sacrifice in throughput. Also, no randomness is needed for protecting the message.

Let us again assume that a wiretapper can assess at most one channel in the butterfly network. Then the same code is also secure for the following general wiretap network [8]. In this general wiretap network, we assume that M_1 and M_2 are generated from different sources, and two wiretappers, who are able to access any single channel, are interested in M_1 and M_2, respectively. Then the code in last paragraph is secure for this general wiretap network. To see this, we note that $H(M_1|Y) = H(M_1) = \log q$ for the random output Y of any single channel. Thus for this general wiretap network, the required security can be achieved at no extra cost. The reason is quite clear, because M_2 serves as the "randomness" to protect M_1, and vice versa. The same phenomenon can also be found in the analysis of the strongly r-secure code in [4].

However, for this network code, we have $I(M_1; M_2|Y) = \log q > 0$. This yields that a wiretapper interested in *the whole message* (M_1, M_2) can gain $\log q$ bits of information upon accessing any single channel if we use mutual information as the security measure. Following [27, Example 6.15], we call this *imperfect secrecy*. We will see in Section VI that this is indeed the best possible security that can be achieved if one does not pay extra for security.

Recall that the original linear code on the butterfly network in [1] is over $GF(2)$. Here we let $M = (M_1, M_2)$ be two independent random bits taking values in $GF(2)$ according to the uniform distribution. In their coding scheme, the source node s sends m_1 to u_1 and a_0 through a_1, and sends m_2 to u_2 and a_0 through a_2. Upon receiving m_1 and m_2, a_0 sends $m_1 + m_2$ to u_1 and u_2 through b. Lima *et al.* in [19] partitioned $\mathcal{V} \setminus \{s, u_1, u_2\}$ into three subsets, $V_0 = \{b\}, V_1 = \{a_1, a_2\}$, and $V_2 = \{a_0\}$, and observed that a node in V_i is able to decode exactly i bit(s) in $m = (m_1, m_2)$. Thus from the wiretapper's point of view, node a_0 is the best node and node b is the worst node to access in

the sense of the number of bits the wiretapper can correctly decode. In the same sense, it is better for the wiretapper to access (a_1, u_1) or (a_2, u_2) than (a_0, b).

The discussion in [19] is based on the assumption that the wiretapper is interested in decoding as many symbols in the message as possible. However, if security is measured by the mutual information $I(M; Y_A)$ (or equivalently $H(M|Y_A)$ since $I(M; Y_A) = H(M) - H(M|Y_A)$), it makes no difference for the wiretapper to access any one of the channels (a_1, u_1), (a_2, u_2), and (a_0, b). In any of these cases, the remaining uncertainty to the wiretapper about M is equal to 1 bit. In the case that the wiretapper is interested in the parity of the two bits m_1 and m_2, then it is of course better for him/her to access (a_0, b) than any other single channel.

III. Construction of a Class of Admissible Linear Codes for Communication Systems on a Wiretap Network

In this section, we propose a class of admissible linear codes for a wiretap network. In defining a linear network code, we let the transmission alphabet F be a finite field $GF(q)$, where q is a sufficiently large power of a prime. In other words, a symbol in $GF(q)$ can be transmitted on each channel in the network.

In the rest of the paper, we adopt the terminology for linear network codes in [31]. In defining an n-dimensional linear network code on $\mathcal{G}$, we let $\mathrm{In}(s)$ consist of n imaginary channels terminating at the source node s.

Definition 1: (Global description of a linear network code) An n-dimensional linear network code on $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ consists of a column n-vector $\mathbf{f}_e$ for every channel $e \in \mathcal{E} \cup \mathrm{In}(s)$ such that:

1) for $e \in \mathrm{Out}(t)$, $\mathbf{f}_e$ is a linear combination of $\mathbf{f}_d$, $d \in \mathrm{In}(t)$.
2) $\mathbf{f}_e$, $e \in \mathrm{In}(s)$, form the standard basis of the vector space F^n.

The vector $\mathbf{f}_e$ is called the global encoding kernel for channel e.

We use $\langle \cdot \rangle$ to denote the linear span of a set of vectors. For $t \in \mathcal{V}$, let

$$V_t = \langle \{ \mathbf{f}_e : e \in \mathrm{In}(t) \} \rangle.$$

For $T \subset \mathcal{V}$, let

$$V_T = \langle \{ \cup_{t \in T} V_t \} \rangle,$$

and for $B \in \mathcal{E}$, let

$$V_B = \langle \{ \mathbf{f}_e : e \in B \} \rangle.$$

For a node $t \in \mathcal{V}$ where $t \neq s$, let $\mathrm{maxflow}(t)$ denote the value of a maximum flow from the source node s to node t.

The following existence theorem of a linear network code with the prescribed property is due to Jaggi *et al.* [16], who proposed a polynomial-time algorithm for constructing such a code.

Theorem 1: If $\mathrm{maxflow}(u) \geq n$ for all $u \in \mathcal{U}$, then there exists an n-dimensional linear network code on $\mathcal{G}$ over $GF(q)$ for $q > |\mathcal{U}|$ such that $\dim(V_u) = n$ for all $u \in \mathcal{U}$.

We now define a class of linear codes for a wiretap network by the following construction.

Construction 1

1) Choose suitable positive integers n and r, where $r < n$. The message M is randomly chosen from $GF^{(n-r)}(q)$ (not necessarily uniformly distributed), while the independent random key K is distributed uniformly on $GF^r(q)$. Let the outcome $\mathbf{m}$ of M be a row vector in $GF^{(n-r)}(q)$ and the outcome $\mathbf{k}$ of K be a row vector in $GF^r(q)$. Let $X = (M, K)$.

2) Choose a suitable n-dimensional linear network code on $\mathcal{G}$.

3) Encode the vector X by transmitting in each channel e the value $X\,\mathbf{f}_e$.

We will show later how n, r and the linear network code can be chosen to make the code admissible, i.e., decodable and secure.

Theorem 2 in below states that if a certain condition is satisfied, then it is possible to obtain an admissible code by Construction 1. The proof of this theorem is deferred to Section V. The sufficient condition in Theorem 2 depends on a linear network code satisfying certain properties whose existence is hard to verify. Nevertheless, a more explicit sufficient condition will be obtained.

Theorem 2: There exists an admissible code on $\mathcal{G}$ over $GF(q)$ for $q > |\mathcal{A}|$ by Construction 1 if

there exists an n-dimensional linear network code over $GF(q)$ such that for all user nodes $u \in \mathcal{U}$,

$$\dim(V_u) = n, \tag{1}$$

and for all wiretap sets of channels $A \in \mathcal{A}$,

$$\dim(V_A) \leq r. \tag{2}$$

In the directed graph $\mathcal{G}$, a path is a sequence of channels $e_1, e_2, \ldots, e_l$ such that for $1 \leq i \leq l-1$, there exists $t_i \in \mathcal{V}$ such that $e_i \in \mathrm{In}(t_i)$ and $e_{i+1} \in \mathrm{Out}(t_i)$. Two paths are disjoint if they do not share a common channel (but they may share a common node). For a collection of channel $A \subset \mathcal{E}$, a path from the source node s to the channels in A refers a path that starts at the source node s and has one of the channels in A as the last channel on the path. The following theorem is similar to Theorem 2 except that the condition therein depends only on the graph $\mathcal{G}$ and the collection of wiretap channels $\mathcal{A}$. This condition is easy to check and is more explicit than the condition in Theorem 2.

Theorem 3: Let $\mathcal{G}^* = (\mathcal{V}, \mathcal{E}^*)$, where $\mathcal{E}^* \subset \mathcal{E}$, be a subgraph of $\mathcal{G}$ satisfying the following:

i) For any $u \in \mathcal{U}$, there are n disjoint paths in $\mathcal{G}^*$ from the source node s to the user node u.

ii) For any $A \in \mathcal{A}$, there are at most r disjoint paths in $\mathcal{E}^*$ from the source node s to the channels in A.

If such a subgraph $\mathcal{G}^*$ exists, then there exists an admissible code on $\mathcal{G}$ over $GF(q)$ by Construction 1 for $q > \max\{|\mathcal{U}|, |\mathcal{A}|\}$.

This theorem is a simple consequence of Theorems 1 and 2 and the following lemma ([28, Theorem 19.10]).

Lemma 1: For any $A \in \mathcal{A}$, let $\mathrm{maxflow}(A)$ denote the maximum number of disjoint paths from the source node s to the channels in A. For any linear network code defined on $\mathcal{G}$, $\dim(V_A) \leq \mathrm{maxflow}(A)$.

Proof of Theorem 3 Assume the existence of the subgraph $\mathcal{G}^*$ as prescribed and let $q > \max\{|\mathcal{U}|, |\mathcal{A}|\}$. We will confine our discussion to $\mathcal{G}^*$. The condition i) in the theorem implies that $\mathrm{maxflow}(u) \geq n$ for all $u \in \mathcal{U}$, and the condition ii) in the theorem implies that $\mathrm{maxflow}(A) \leq r$ for all $A \in \mathcal{A}$. Since $q > |\mathcal{U}|$, by Theorem 1, there exists an n-dimensional linear network code on $\mathcal{G}^*$ such that $\dim(V_u) = n$ for all $u \in \mathcal{U}$. Now for this network code, for any $A \in \mathcal{A}$, by Lemma 1, $\dim(V_A) \leq \mathrm{maxflow}(A) \leq r$. Since $q > |\mathcal{A}|$, by invoking Theorem 2, we see the existence of an admissible code on $\mathcal{G}^*$ by Construction 1. The theorem is proved. □

By applying Theorem 3 to an r-WN, we have

Corollary 1: There exists an r-secure network code on any $\mathcal{G}$ over $GF(q)$ by Construction 1 for $q > \max\left\{|\mathcal{U}|, \binom{|\mathcal{E}|}{r}\right\}$ if r is smaller than the minimum value of a maximum flow from the source node to a user node.

An immediately consequence of the corollary is the main result in [3][24] that for $r \leq n$, an (r, n)-threshold secret sharing scheme always exists when $r_i = c$ for all $1 \leq i \leq n$, where c is a sufficiently large constant.

IV. Optimality of r-secure Network Codes

By Corollary 1 at the end of last section, we have that for all $\mathcal{G}$ and all $r < n$, one can obtain an r-secure network code over $GF(q)$ by Construction 1 by taking q to be a sufficiently large power of any prime number. We note that the code constructed by Construction 1 can transmit a message M consisting of $n-r$ symbols in $GF(q)$ to all user nodes $u \in \mathcal{U}$ securely. To achieve this, a key consisting of r symbols in $GF(q)$ is used. In this section, we will establish the optimality of the code so constructed by proving two fundamental performance bounds and showing that the tightness of these bounds are achieved by the code.

Consider any r-secure network code for a given network $\mathcal{G}$. Let $u \in \mathcal{U}$ be such that $\mathrm{maxflow}(u) = n$ and (W, W^c) be a minimum cut between the source node s and node u. Denote the set of channels on (W, W^c) by E_W. Then $|E_W| = n$. Since the message M can be decoded at node u and the symbols received at node u are functions of Y_{E_W}, we have

$$H(M|Y_{E_W}) = 0. \tag{3}$$

On the other hand, for any subset J of E_W with cardinality r, since the code is secure, we have

$$H(M|Y_J) = H(M). \tag{4}$$

It follows that

$$\begin{aligned} H(M) &= H(M|Y_J) - H(M|Y_{E_W}) \\ &= I(M; Y_{E_W \setminus J}|Y_J) \\ &\leq H(Y_{E_W \setminus J}|Y_J) \\ &\leq H(Y_{E_W \setminus J}) \\ &\leq (n-r)\log q. \end{aligned}$$

This tightness of this upper bound on $H(M)$ is achieved by the r-secure network code constructed by Construction 1 when M is distributed uniformly on $GF^{(n-r)}(q)$. In other words, the code multicasts the maximum possible amount of information to the user nodes securely.

In the rest of the section, we will prove that the code uses the minimum amount of randomness to achieve the required security when the message M is distributed uniformly. In establishing this result, we need a set of inequalities stated in the next lemma due to Han [13] (see also [9], Theorem 17.6.3).

Lemma 2: For a subset α of $\mathcal{N} = \{1, 2, \ldots, n\}$, let $\overline{\alpha} = \mathcal{N} \setminus \alpha$ and denote $(X_i, i \in \alpha)$ by X_α. For $1 \leq r \leq n$, let

$$h_r = \frac{1}{\binom{n-1}{r-1}} \sum_{\alpha:|\alpha|=r} H(X_\alpha|X_{\overline{\alpha}}). \tag{5}$$

Then

$$h_1 \leq h_2 \leq \cdots \leq h_n.$$

Let $u \in \mathcal{U}$ be any user node and consider any cut (W, W^c) between the source node s and node u. Let $|E_W| = n' \geq n$. For any $J \subset E_W$ such that $|J| = r$, consider

$$\begin{aligned} H(M) &= H(M|Y_{E_W}) + I(Y_{E_W}; M) \\ &= I(Y_J; M) + I(Y_{E_W \setminus J}; M|Y_J) \quad (6) \\ &= I(Y_{E_W \setminus J}; M|Y_J), \end{aligned}$$

where the second and the third equalities follow from (3) and (4), respectively. Summing over all J, we have

$$\begin{aligned} &\binom{n'}{r} H(M) \\ &= \sum_J I(Y_{E_W \setminus J}; M|Y_J) \\ &\leq \binom{n'-1}{n'-r-1} \left[\frac{1}{\binom{n'-1}{n'-r-1}} \sum_J H(Y_{E_W \setminus J}|Y_J) \right] \\ &\leq \binom{n'-1}{n'-r-1} H(Y_{E_W}), \end{aligned}$$

where the last inequality follows from Lemma 2. Hence,

$$H(Y_{E_W}) \geq \frac{n'}{n'-r} H(M). \tag{7}$$

Finally,

$$\begin{aligned} H(M) + H(K) &\geq H(M, K) \quad (8) \\ &= H(M, K, Y_{E_W}) \quad (9) \\ &\geq H(Y_{E_W}) \\ &\geq \frac{n'}{n'-r} H(M), \end{aligned}$$

where (9) follows from

$$H(Y_{E_W}|M, K) = 0, \tag{10}$$

or Y_{E_W} is a function of M and K. This implies

$$H(K) \geq \frac{r}{n'-r} H(M). \tag{11}$$

This lower bound on $H(K)$ applies to every cut between the source node s and any user node u, in particular to a cut with size equal to n. Therefore, we conclude that

$$H(K) \geq \frac{r}{n-r} H(M). \tag{12}$$

The tightness of this lower bound on $H(K)$ is achieved by the code constructed by Construction 1 when both M and K are uniformly distributed, i.e., $H(M) = (n-r)\log q$ and $H(K) = r \log q$. Under this condition, the code uses the minimum amount of randomness to achieve the required security. In Appendix A, we prove that

$$H(K) \geq H(Y_J).$$

This lower bound on $H(K)$ gives further insight into the problem.

We note that the inequality in (8) holds regardless of whether the message M and the key K are

independent. In fact, toward establishing (12), this assumption in Construction 1 has not been invoked. Hence, (12) is valid even when M and K are not independent.

In obtaining (9) in the above, we have used the fact Y_{E_W} is a function of M and K. Close examination of the steps in our proof reveals that K can be more generally interpreted as the randomness introduced into the network at the "upstream" of the set of channels E_W. When $n' > n$, (11) is a looser lower bound on $H(K)$ than (12). This means that it is not necessary for all the randomness K to be generated at the source node s as in Construction 1. As long as all the randomness K is generated at the "upstream" of any cut of size n between the source node s and any user node u, it is already good enough. This observation would be useful if the source node s does not have enough resource to generate all the required randomness.

Hence, we have proved that when the message is uniformly distributed, the code obtained by Construction 1 is optimal in terms of both the amount information that can be multicast in the network securely and the amount of randomness used for achieving the required security. In this case, by (12), K has to be uniformly distributed if we want the size of the size of the alphabet of K to be minimal, i.e., $|\mathcal{K}| = r \log q$.

V. Proof of Theorem 2

Assume the existence of the n-dimensional linear network code as prescribed in the theorem. Denote the code by $\mathcal{C}$ and let $\mathbf{f}_e, e \in \mathcal{E}$ be the global encoding kernels. For all $A \in \mathcal{A}$, let $\dim(V_A) = r_A$, and let $\{\mathbf{a}_1(A), \mathbf{a}_2(A), \ldots, \mathbf{a}_{r_A}(A)\}$ be a maximally independent set of vectors in $\{\mathbf{f}_e, e \in A\}$. Note that $r_A \le r$ by (2).

Lemma 3: If $q > |\mathcal{A}|$, there exist column n-vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-r}$ such that for all $A \in \mathcal{A}$,

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-r}, \mathbf{a}_1(A), \mathbf{a}_2(A), \ldots, \mathbf{a}_{r_A}(A)$$

are linearly independent.

Proof If suffices to show that for $1 \le i \le n-r$, if $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}$ have been chosen such that for all $A \in \mathcal{A}$,

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}, \mathbf{a}_1(A), \mathbf{a}_2(A), \ldots, \mathbf{a}_{r_A}(A) \quad (13)$$

are linearly independent, then it is possible to choose $\mathbf{b}_i$ such that for all $A \in \mathcal{A}$,

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}, \mathbf{b}_i, \mathbf{a}_1(A), \mathbf{a}_2(A), \ldots, \mathbf{a}_{r_A}(A) \quad (14)$$

are linearly independent. Specifically, $\mathbf{b}_i$ is chosen such that it is linearly independent of the set of vectors in (13) for all $A \in \mathcal{A}$, i.e., we require that

$$\mathbf{b}_i \in GF^n(q) \backslash \bigcup_{A\in\mathcal{A}} \langle \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}, \mathbf{a}_1(A), \mathbf{a}_2(A), \ldots, \mathbf{a}_{r_A}(A)\rangle.$$

Thus we need to show that the set above is nonempty. Since the vectors in (13) are linearly independent,

$$\begin{aligned}
&\left|\bigcup_{A\in\mathcal{A}} \langle \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}, \mathbf{a}_1(A), \mathbf{a}_2(A), \ldots, \mathbf{a}_{r_A}(A)\rangle\right| \\
&\le \sum_{A\in\mathcal{A}} |\langle \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}, \mathbf{a}_1(A), \mathbf{a}_2(A), \\
&\quad \ldots, \mathbf{a}_{r_A}(A)\rangle| \\
&= \sum_{A\in\mathcal{A}} q^{r_A+i-1} \\
&\le \sum_{A\in\mathcal{A}} q^{r+i-1} \\
&= |\mathcal{A}| q^{r+i-1}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\left|GF^n(q) \backslash \bigcup_{A\in\mathcal{A}} \langle \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}, \mathbf{a}_1(A), \mathbf{a}_2(A), \right. \\
&\qquad \left. \ldots, \mathbf{a}_{r_A}(A)\rangle\right| \\
&\ge q^n - |\mathcal{A}| q^{r+i-1} \\
&= q^{r-i+1}(q^{n-r-i+1} - |\mathcal{A}|) \\
&\ge q^{r-i+1}(q - |\mathcal{A}|) \\
&> 0
\end{aligned}$$

since $i \le n-r$ and $q > |\mathcal{A}|$. Hence, $\mathbf{b}_i$ can be chosen for all $1 \le i \le n-r$. □Subsequent to [5], Feldman *et al.* [11] pointed out that the condition for $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-r}$ in Lemma 3 is equivalent to a Hamming distance property of a certain type of codes. They also derived a tradeoff between the size of the message set $\mathcal{M}$ and the size of the transmission alphabet F. Specifically, they showed that it is sufficient to take $q > |\mathcal{A}|^{\frac{1}{r\epsilon+1}}$ if we want to

send a message consisting of $\lfloor n-r(1+\epsilon)\rfloor$ instead of $(n-r)$ q-ary symbols through the network. We note that this tradeoff can readily be obtained by replacing $i \le n-r$ and $q > |\mathcal{A}|$ by $i \le n-r(1+\epsilon)$ and $q^{r\epsilon+1} > |\mathcal{A}|$, respectively in the above proof.

Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-r}$ be chosen according to the above lemma. Extend $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-r}$ to a basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-r}, \mathbf{b}_{n-r+1}, \ldots, \mathbf{b}_n$ for $GF^n(q)$, and define the $n \times n$ matrix

$$Q = [\ \mathbf{b}_1\ \mathbf{b}_2\ \ldots\ \mathbf{b}_n\ ]. \tag{15}$$

Evidently, Q is nonsingular.

Let $\mathcal{T} : GF^n(q) \to GF^n(q)$ be the linear transformation represented by the matrix Q^{-1}. Now transform the linear network code $\mathcal{C}$ into another linear network code $\mathcal{C}'$ with global encoding kernels $\mathbf{f}'_e, e \in \mathcal{E}$ by $\mathcal{T}$, i.e., $\mathbf{f}'_e = Q^{-1}\mathbf{f}_e$ for all $e \in \mathcal{E}$. For $u \in \mathcal{U}$ and $A \in \mathcal{A}$, the vector spaces V_u and V_A for the linear network code $\mathcal{C}$ become $V'_u = \mathcal{T}V_u$ and $V'_A = \mathcal{T}V_A$ for the linear network code $\mathcal{C}'$, respectively. Since Q is invertible, by (1) and (2),

$$\dim(V'_u) = \dim(V_u) = n \tag{16}$$

and

$$\dim(V'_A) = \dim(V_A) \le r. \tag{17}$$

With the global encoding kernels $\mathbf{f}'_e$, $e \in \mathcal{E}$, we obtain a linear network code $\mathcal{C}_s$ for a wiretap network by Construction 1. It follows from (16) by a straightforward argument that $\mathcal{C}_s$ is decodable because at each user node $u \in \mathcal{U}$, both $\mathbf{m}$ and $\mathbf{k}$ can be decoded with zero error.

To complete the proof, we only have to check that $\mathcal{C}_s$ is secure. For $1 \le j \le r_A$, let $\mathbf{a}'_j(A) = Q^{-1}\mathbf{a}_j(A)$. Let F_A and F'_A be $n \times r_A$ matrices whose jth columns are $\mathbf{a}_j(A)$ and $\mathbf{a}'_j(A)$, respectively. Then

$$F'_A = Q^{-1}F_A. \tag{18}$$

Let Y_A be the vector of symbols transmitted on the channels in the wiretap set A. Let $\mathbf{y}_A$ be the value of Y_A when $X = \mathbf{x}$, i.e.,

$$\mathbf{y}_A = \mathbf{x}F'_A. \tag{19}$$

In other words, upon observing $\mathbf{y}_A$, the knowledge of the wiretapper is that $\mathbf{x}$ is a solution of the above equation. For a row r_A-vector $\mathbf{y} \in GF^{r_A}(q)$, let

$$C(\mathbf{y}) = \{\mathbf{x} : \mathbf{x} \in GF^n(q), \mathbf{y} = \mathbf{x}F'_A\}. \tag{20}$$

Then the solution set of (19) is given by $C(\mathbf{y}_A)$, which is seen to be a coset of the null space $C(\mathbf{0})$ under the linear transformation represented by F'_A. Therefore, $GF^n(q)$ is partitioned into $\{C(\mathbf{y}) : \mathbf{y} \in GF^{r_A}(q)\}$.

For $\mathbf{m} \in GF^{(n-r)}(q)$, let

$$D(\mathbf{m}) = \{(\mathbf{m}, \mathbf{k}) : \mathbf{k} \in GF^r(q)\}.$$

We now show that for all $\mathbf{m} \in GF^{(n-r)}(q)$ and $\mathbf{y} \in GF^{r_A}(q)$,

$$|D(\mathbf{m}) \cap C(\mathbf{y})| = q^{r-r_A}, \tag{21}$$

which does not depend on $\mathbf{m}$. Let

$$G_A = [\ \mathbf{e}_1\ \mathbf{e}_2\ \cdots\ \mathbf{e}_{n-r}\ F'_A\ ],$$

where $\mathbf{e}_j$ is the column n-vector whose jth component is 1 and all other components are 0. If follows from the definition of $D(\mathbf{m})$ and $C(\mathbf{y})$ that if a vector $\mathbf{x}$ is in their intersection, then

$$\mathbf{x}G_A = [\ \mathbf{m}\ \mathbf{y}\ ]. \tag{22}$$

Therefore, by (15) and (18), we have

$$QG_A = [\ \mathbf{b}_1\ \mathbf{b}_2\ \cdots \mathbf{b}_{n-r}\ \mathbf{a}_1(A)\ \mathbf{a}_2(A)\ \cdots\ \mathbf{a}_{r_A}(A)\ ].$$

By construction, the columns of QG_A are linearly independent, so that $\mathrm{rank}(QG_A) = n - r + r_A$. Since Q is nonsingular, $\mathrm{rank}(G_A) = \mathrm{rank}(QG_A) = n - r + r_A$. It follows that for any $(\mathbf{m}, \mathbf{y}) \in GF^{(n-r+r_A)}(q)$, the solution set of (22) is nonempty and is an affine subspace with cardinality

$$\frac{q^n}{q^{n-r+r_A}} = q^{r-r_A}.$$

This proves (21). In other words, for each $\mathbf{y} \in GF^{r_A}(q)$ observed by the wiretapper, every message $\mathbf{m} \in GF^{(n-r)}(q)$ is possible, and for each $\mathbf{m}$, the total number of keys $\mathbf{k} \in GF^r(q)$ that can produce $\mathbf{y}$ is equal to q^{r-r_A}.

For all $A \in \mathcal{A}$, $\mathbf{y} \in GF^{r_A}(q)$, and $\mathbf{m} \in GF^{(n-r)}(q)$ with $\Pr\{M = \mathbf{m}\} > 0$,

$$\begin{aligned}
&\Pr\{Y_A = \mathbf{y} | M = \mathbf{m}\} \\
&\quad = \Pr\{(\mathbf{m}, K) \in D(m) \cap C(y) | M = \mathbf{m}\} \\
&\quad = \Pr\{(\mathbf{m}, K) \in D(m) \cap C(y)\},
\end{aligned}$$

because for any fixed $\mathbf{m}$, $Y_A = \mathbf{y}$ if and only if $(\mathbf{m}, K) \in D(m) \cap C(y)$, and K is independent of

M. Since K is uniformly distributed, by (21), we obtain

$$\Pr\{Y_A = \mathbf{y} | M = \mathbf{m}\} = q^{-r} q^{r-r_A} = q^{-r_A},$$

which does not depend on $\mathbf{m}$. Hence, Y_A is independent of M, and so the linear network code $\mathcal{C}_s$ we have constructed by Construction 1 is secure.

We end this section with two remarks.

Remark 1: Since G_A has full rank, each column of F'_A cannot be a linear combination of $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_{n-r}$, or equivalently, the lower r components cannot be all zero. In other words, the key K is involved in each of the symbols transmitted on the channels of a wiretap set. In fact, if F'_A contains a column such that the lower r components are all zero, then the wiretapper receives a symbol which is a known linear combination of the symbols in the message M, making the code not secure.

Remark 2: In Construction 1, we obtain a secure network code by taking a linear transformation represented by the matrix Q^{-1} of any given non-secure network code. An advantage of this technique is that in the course of making the network code secure, we do not need to change the local encoding kernels. Rather, we only need to pre-encode the input of the network $\mathbf{x} = (\mathbf{m}, \mathbf{k})$ by the matrix Q^{-1} and then send the codeword $\mathbf{x}Q^{-1}$ through the network. This is very convenient in practice because once a (non-secure) linear network code is in place, the decision on the level of security to be used can be deferred. Subsequent to [5], the same idea was used in [10], where they obtained a secure network code by taking a linear transformation of a secure linear code for wiretap channel II. The validity of this technique hinges on the assumption that all the randomness for protecting the source message is generated at the source node. In general, this randomness may be generated at a set of nodes instead of the source node as discussed in [6] and [32]. Finally, we remark that this paper and almost all other papers in the same direction consider only acyclic networks. In principle, secure network coding can also be discussed for cyclic networks, but the formulation would be considerably more complicated because convolutional network code instead of block network code is involved.

VI. Imperfect Secrecy

In this section, we extend our results in the previous sections for the special case that the collection $\mathcal{A}$ of wiretap sets consists of all the r-subsets of $\mathcal{E}$ by allowing the wiretapper to obtain a controlled amount of information about the message. Specifically, the secure condition is replaced by the condition that for all $A \in \mathcal{A}$,

$$I(M; Y_A) \le i \log q, \tag{23}$$

where i is a fixed integer satisfying $0 \le i \le r$. We will refer to this as the *imperfectly secure condition*. The integer i specifies how much information can be leaked to the wiretapper. When $i = 0$, the imperfectly secure condition reduces to the secure condition.

The study of imperfect secrecy can be motivated in more than one way. First, it is a natural generalization of perfect secrecy from the information theory point of view. Second, the mutual information $I(M; Y_A)$ is a useful measure of the amount of information leaked to the wiretapper. For a linear network code, when $I(M; Y_A) = i \log q$, where $0 < i \le r$, the size of the set of all possible values that can be taken by M according to the wiretapper is reduced by a factor of q^i. For some applications, such security can be regarded as sufficient as long as the size of the set is not too small. As we will see, the benefit of accepting a lower level of security is that a larger source message can be transmitted. This will be made precise in the sequel.

We first show that under the imperfectly secure condition, the message M can consist of at most $(n - r + i)$ q-ary symbols. Consider any code on a wiretap network satisfying both the decodable condition and the imperfectly secure condition. Let $u \in \mathcal{U}$ be such that $\mathrm{maxflow}(u) = n$ and (W, W^c) be a minimum cut between the source node s and node u. Consider

$$\begin{aligned} H(M) &= I(Y_J; M) + I(Y_{E_W \setminus J}; M | Y_J) && (24)\\ &\le I(Y_J; M) + H(Y_{E_W \setminus J}) && (25)\\ &\le (n - r + i) \log q, && (26) \end{aligned}$$

where (24) follows from (6), and (26) follows from (23) and $|E_W \setminus J| = n - r$, proving the claim. Note that (25) is equivalent to the imperfect secrecy theorem in [27] (p. 116).

Next, we show that tightness in (26) can be achieved by an "imperfectly secure" code obtained via Construction 1. In Construction 1, let $K = (M^*, K')$, where M^* is chosen randomly from $GF^i(q)$, and K' is independent of (M, M^*) and distributed uniformly on $GF^{r-i}(q)$. The input pair (M, K) in Construction 1 now becomes the triple (M, M^*, K'), where $M' = (M, M^*)$ is regarded as the message of our imperfectly secure code which consists of $(n - r + i)$ q-ary symbols, and K' is regarded as the key of the code which consists of $(r - i)$ q-ary symbols. Since the code obtained by Construction 1 is secure when the input pair is (M, K), we have

$$I(M; Y_A) = 0$$

for all $A \in \mathcal{A}$. Thus

$$\begin{aligned} I(M'; Y_A) &= I(M; Y_A) + I(M^*; Y_A|M) \\ &\le H(M^*) \\ &= i \log q, \end{aligned}$$

i.e., the imperfectly secure condition is satisfied by the code we have constructed. Evidently, node u can decode the message $M' = (M, M^*)$ because in the code obtained by Construction 1, the pair (M, K) can be recovered. Hence, we have obtained a code that multicasts the maximum possible amount of information while satisfying the imperfect secure condition with the prescribed i.

Finally, we prove that the imperfectly secure code we have constructed above uses the minimum amount of randomness to achieve the required level of security when the message M' is uniformly distributed. The proof is a generalization of the corresponding proof in Section 4, so we only present the sketch here. Let $u \in \mathcal{U}$ be such that $\mathrm{maxflow}(u) = n$ and (W, W^c) be a minimum cut between the source node s and node u. For any $J \subset E_W$ such that $|J| = r$, by (6) and (23) with M replaced by M', we have

$$H(M') \le i \log q + I(Y_{E_W \setminus J}; M'|Y_J).$$

Summing over all J, we have

$$\binom{n}{r} H(M') \le \binom{n}{r} i \log q + \binom{n-1}{n-r-1} H(Y_{E_W}),$$

which implies

$$H(Y_{E_W}) \ge \frac{n}{n-r}(H(M') - i \log q).$$

It follows that

$$\begin{aligned} & H(M') + H(K') \\ &\quad \ge H(Y_{E_W}) \\ &\quad \ge \frac{n}{n-r}(H(M') - i \log q), \end{aligned}$$

or

$$H(K') \ge \frac{r}{n-r} H(M') - \frac{n}{n-r}(i \log q).$$

When the message M' is uniformly distributed, $H(M') = (n - r + i) \log q$ and $H(K') = (r - i) \log q$, and it can readily be checked that the inequality above is tight. This completes the proof.

VII. Conclusion

In this paper, we have introduced the wiretap network as a model for multicasting on a network with information-theoretic security. Our model subsumes secret sharing in classical cryptography. We have proposed a construction of a secure linear network code for a wiretap network. The optimality of our construction is proved for the special case that the wiretapper may choose to access any subset of channels of a fixed size. Moreover, we have extended this construction to the scenario when the wiretapper is allowed to obtain a controlled amount of information about the message. This extended construction is also shown to be optimal.

Appendix A
A Lower Bound on $H(K)$

Assume that the collection $\mathcal{A}$ of wiretap sets consists of all the r-subsets of $\mathcal{E}$. Let $u \in \mathcal{U}$ be any user node and consider any cut (W, W^c) between the source node s and node u. Let $|E_W| = n' \ge n$. We will prove that

$$H(K) \ge H(Y_J). \tag{27}$$

for any $J \subset E_W$ such that $|J| = r$. Consider

$$H(Y_J|M, K) \le H(Y_{E_W}|M, K) = 0,$$

which implies

$$H(Y_J|M, K) = 0.$$

Together with

$$H(Y_J) = H(Y_J|M)$$

from the secure condition, we have

$$\begin{aligned} H(Y_J) &= H(Y_J|M) - H(Y_J|M,K) \\ &= I(Y_J;K|M) \\ &\leq H(K|M) \\ &= H(K), \end{aligned}$$

proving (27).

ACKNOWLEDGMENT

Raymond Yeung would like to thank Prof. Ueli Maurer for the useful discussion. Both authors would like to thank Prof. Te Sun Han for pointing out the references for his inequalities and for his comments on the draft.

REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Info. Theory*, IT-46: 1204-1216, 2000.

[2] K. Bhattad and K. R. Narayanan, Weakly secure network coding, First Workshop on Network Coding, Theory, and Applications (NetCod05), Apr. 2005.

[3] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, 48: 313-317, 1979.

[4] N. Cai, "Valuable Messages and Random Outputs of Channels in Linear Network Coding," IEEE International Symposium on Information Theory 2009, Seoul, Korea, June 28-July 3, 2009.

[5] N. Cai and R. W. Yeung, "Secure network coding," IEEE International Symposium on Information Theory, Lausanne, Switzerland, Jun 30-Jul 5, 2002.

[6] N. Cai and R. W. Yeung, "A Security Condition for Multi-Source Linear Network Coding," IEEE International Symposium on Information Theory, Nice, France, June 24-29, 2007.

[7] N. Cai and R. W. Yeung, "Network error correction, Part II: Lower bounds," *Comm. Info. and Syst.*, 6: 37-54, 2006 (http://www.ims.cuhk.edu.hk/˜cis/).

[8] T. Chan and A. Grant, "Capacity Bounds for Secure Network Coding," Australian Commun. Theory Workshop, (Christchurch, NZ), 30 Jan - 1 Feb, 2008.

[9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed., Wiley, 2006.

[10] S. Y. El Rouayheb and E. Soljanin On wiretap networks II, IEEE International Symposium on Information Theory, Nice, France, June 24 C June 29, 2007.

[11] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, "On the capacity of secure network coding," 42nd Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sept 29-Oct 1, 2004.

[12] L. K. Ford, Jr. and D. K. Fulkerson, *Flows in Networks*, Princeton University Press, Princeton, New Jersey, 1962.

[13] T. S. Han, "Nonnegative entropy measures of multivariate symmetric correlations," *Info. Contr.,* 36: 133-156, 1978.

[14] K. Harada and H. Yamamoto, "Strongly Secure Linear Network Coding," *EICE Transactions on Fundamentals,* vol. E91-A, No.10, pp.2720-2728, Oct. 2008.

[15] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, A random linear network coding approach to multicast, *IEEE Trans. on Inform. Theory,* vol. 52, pp. 4413-4430, Oct. 2006.

[16] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Trans. Info. Theory*, IT-51: 1973-1982, 2005.

[17] K. Jain, Security based on network topology against the wiretapping attack, IEEE Wireless Communications, pp. 68C71, Feb. 2004.

[18] S.-Y. R. Li, R. W. Yeung and N. Cai, "Linear network coding," *IEEE Trans. Info. Theory*, IT-49: 371-381, 2003.

[19] L. Lima, M. Médard, and J. Barros, "Random Linear Network Coding: A free cipher?" IEEE International Symposium on Information Theory, Nice, France, June 24 C June 29, 2007.

[20] C.-K. Ngai, R. W. Yeung, and Z. Zhang, "Network Generalized Hamming Weight," 2009 Workshop on Network Coding, Theory and Applications, Lausanne, Switzerland, 2009.

[21] C.-K. Ngai and R. W. Yeung, "Secure error-correcting (SEC) network codes," 2009 Workshop on Network Coding, Theory and Applications, Lausanne, Switzerland, 2009.

[22] L. H. Ozarow and A. D. Wyner, "Wire-tap Channel II," *AT&T Bell Labs. Tech. J.*, 63: 2135-2157, 1984.

[23] J. Tan and M. Médard, "Secure Network Coding with a Cost Criterion,"

[24] A. Shamir, "How to share a secret," *Comm. ACM*, 22: 612-613, 1979.

[25] C. E. Shannon, "Communication theory of secrecy systems", Bell Sys. Tech. Journal 28, pp. 656-715,1949,

[26] V. K. Wei, "Generalized Hamming Weight for Linear Codes," *IEEE Trans. Inform. Theory,* vol. 37 , no. 5, pp 1412-1418, Sep.1991.

[27] R. W. Yeung, *A First Course in Information Theory*, Kluwer Academic/Plenum Publishers, 2002.

[28] R. W. Yeung, *Information Theory and Network Coding*, Springer 2008.

[29] R. W. Yeung and N. Cai, "Network error correction, Part I: Basic concepts and upper bounds," *Comm. Info. and Syst.*, 6: 19-36, 2006 (http://www.ims.cuhk.edu.hk/˜cis/).

[30] R. W. Yeung and N. Cai, "On the Optimality of a Construction of Secure Network Codes", IEEE International Symposium on Information Theory, Toronto, Canada, July 6 - 11, 2008.

[31] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, "Network coding Theory," *Foundations and Trends in Comm. and Info. Theory*, vol. 2, nos. 4 and 5, 241-381, 2005.

[32] Z. Zhang and R. W. Yeung, "A General Security Condition for Multi-Source Linear Network Coding," IEEE International Symposium on Information Theory 2009, Seoul, Korea, June 28-July 3, 2009.

Ning Cai (M'08-SM'09) received the B.S. degree in mathematics from the Normal College of Beijing, Beijing, China in 1982, the M.S. degree in mathematics from Academia Sinica, Beijing, China, in 1984, and the Dr. degree in mathematics from the University of Bielefeld, Bielefeld, Germany, in 1988.

During 1984-1986, he worked in the Institute of Systems Sciences, Academia Sinica, Beijing, China. During 1988-1989, he was with the Department of Mathematics, Statistics and Computer Science, the University of Illinois, Chicago, USA. From 1989 to 1998, he was a Miss. Mitarbeiter in the Department of Mathematics, the University of Bielefeld, Germany and from 1998 to 1999, he was with the School of Computing, the National University of Singapore, Singapore. From 2000 to 2001, he was with the Department of Information Engineering, The Chinese University of Hong Kong. From 2002 to 2004 he was with the Department of Mathematics, the University of Bielefeld, Germany. In 2005 he visited Department of Information Engineering, The Chinese University of Hong Kong. Since 2006, he has been a distinguished professor of the State Key Lab. of Integrated Services Networks (ISN), Xidian University, China.

Dr. Cai is a recipient of the 2005 IEEE Information Theory Society Paper Award (for his paper "Linear network coding" co-authored with S.-Y. R. Li and R. W. Yeung).

He has served on the committees of a number of information theory symposiums and workshops. His research interests include network coding and information theory.

Raymond W. Yeung (S'85-M'88-SM'92-F'03) was born in Hong Kong on June 3, 1962. He received the B.S., M.Eng., and Ph.D. degrees in electrical engineering from Cornell University, Ithaca, NY, in 1984, 1985, and 1988, respectively.

He was on leave at Ecole Nationale Supérieure des Télécommunications, Paris, France, during fall 1986. He was a Member of Technical Staff of AT&T Bell Laboratories from 1988 to 1991. Since 1991, he has been with the Department of Information Engineering, The Chinese University of Hong Kong, where he is now a chair professor. He is also a Changjiang Chair Professor at Xidian University (2009-12) and an Advisory Professor at Beijing University of Post and Telecommunications (2008-11). He has held visiting positions at Cornell University, Nankai University, the University of Bielefeld, the University of Copenhagen, Tokyo Institute of Technology, and Munich University of Technology. He was a Consultant in a project of Jet Propulsion Laboratory, Pasadena, CA, for salvaging the malfunctioning Galileo Spacecraft and a Consultant for NEC, USA.

He is the author of the textbooks *A First Course in Information Theory* (Kluwer Academic/Plenum 2002) and its revision *Information Theory and Network Coding* (Springer 2008). His research interests include information theory and network coding.

Dr. Yeung was a member of the Board of Governors of the IEEE Information Theory Society from 1999 to 2001. He has served on the committees of a number of information theory symposiums and workshops. He was General Chair of the First and the Fourth Workshop on Network, Coding, and Applications (NetCod 2005 and 2008), a Technical Co-Chair for the 2006 IEEE International Symposium on Information Theory, and a Technical Co-Chair for the 2006 IEEE Information Theory Workshop, Chengdu, China. He currently serves as an Editor-at-Large of *Communications in Information and Systems*, an Editor of *Foundation and Trends in Communications and Information Theory* and of *Foundation and Trends in Networking*, and was an Associate Editor for Shannon Theory of this Transactions from 2003 to 2005. He was a recipient of the Croucher Foundation Senior Research Fellowship for 2000/2001, the Best Paper Award (Communication Theory) of the 2004 International Conference on Communications, Circuits and System (with C. K. Ngai), the 2005 IEEE Information Theory Society Paper Award (for his paper "Linear network coding" co-authored with S.-Y. R. Li and N. Cai), and the Friedrich Wilhelm Bessel Research Award of the Alexander von Humboldt Foundation in 2007. He is a Fellow of the IEEE and the Hong Kong Institution of Engineers.

Since January 2010, Dr. Yeung has been serving as Co-Director of the Institute of Network Coding at The Chinese University of Hong Kong.