On Secure Network Coding with Uniform Wiretap Sets

Wentao Huang and Tracey Ho
California Institute of Technology

Michael Langberg
The Open University of Israel

Joerg Kliewer
New Mexico State University

Abstract—This paper studies secure unicast communication over a network with uniform wiretap sets, and shows that, when network nodes can independently generate randomness, determining the secrecy capacity is at least as difficult as the $k$-unicast network coding problem. In particular, we show that a general $k$-unicast problem can be reduced to the problem of finding the secrecy capacity of a corresponding single unicast network with uniform link capacities and any one wiretap link. We propose a low-complexity linear optimization-based construction involving global random keys that can be generated anywhere in the network, and a greedy algorithm that can further improve the achievable rate by adding local random keys.

I. INTRODUCTION

The secure network coding problem, introduced by Cai and Yeung [1], concerns information theoretically secure communication over a network where an unknown subset of network links may be wiretapped. A secure code prevents the wiretapper from obtaining information about the message being communicated. The secrecy capacity of a network, with respect to a given collection of possible wiretap sets, is the maximum rate of communication such that for any one of the wiretap sets the secrecy constraints are satisfied. Types of secrecy constraints studied in the literature include perfect secrecy, strong secrecy and weak secrecy. In the uniform setting, i.e. equal capacity links of which any one link can be wiretapped, [1] showed that when only the source can generate randomness, the secrecy capacity is given by the cut-set bounds and linear codes suffice to achieve capacity.

This paper considers the problem of finding the secrecy capacity of a network when we allow network nodes in addition to the source to generate independent randomness (i.e. randomness generated at different nodes is statistically independent). We show that a general $k$-unicast problem can be reduced to a corresponding single unicast secrecy capacity problem with uniform link capacities where any single link can be wiretapped. This implies that determining the secrecy capacity, even in the simple case of a single unicast and uniform wiretap sets of size 1, is at least as difficult as the long-standing open problem of determining the capacity region of multiple-unicast network coding, which is not presently known to be in P, NP or undecidable [2].

The secure network coding problem in the non-uniform setting, i.e. restricted wiretap sets and/or non-uniform link capacities, has been considered by Cui et al. [3], and by Chan and Grant [4], who showed that determining multicast secrecy capacity with restricted wiretap sets is at least as difficult as determining capacity for multiple-unicast network coding. Our reduction is similar to the core ideas appearing in [4] with the following differences which significantly strengthen the result. First, by introducing the idea of key cancellation and replacement at intermediate nodes, our construction does not need to impose restrictions on which links can be wiretapped. Secondly, unlike the reduction in [4] which involves multiple terminals, ours only needs a single destination. Thirdly, while [4] studies perfect secrecy, our results apply to perfect, strong and weak secrecy constraints.

While finding secure unicast capacity in the uniform setting is difficult, for this case we show a low-complexity linear optimization-based achievable strategy in which any network node may generate global random keys, i.e. random keys that are decoded by both the source and the sink. This approach generalizes the strategy in [1], [5] where only the source generates global keys, and has lower complexity than the linear optimization-based strategies in [3] designed for the non-uniform case. Performance can be further improved by exploiting local keys. We propose an efficient algorithm that greedily searches for places where local keys can be introduced in place of global keys, thereby increasing the secure communication rate.

II. MODEL

A network is represented by a directed graph $G = (V, E)$, where $V$ is the set of vertices representing network nodes, and $E$ the set of edges representing network links. Links have unit capacity (unless otherwise specified) and there may be multiple links between a pair of nodes. Each node $i \in V$ can generate a random variable $K_i$ which is independent of random variables generated at other nodes (the rate of $K_i$ can be upper bounded by the sum of outgoing link capacities of $i$). Transmissions on the outgoing links of node $i$ can be functions of $K_i$ as well as transmissions received on incoming links of $i$.

There is a source node $S \in V$ and a destination node $D \in V$. $S$ wants to communicate a message $M$, uniformly drawn from a finite alphabet set $S_n$, to $D$ using a code with length $n$. Then the rate of the code is $n^{-1} \log |S_n|$. We say that a communication rate $R$ is feasible if there exists a sequence of length-$n$ codes such that $|S_n| = 2^{nR}$ and the probability of decoding error tends to 0 as $n \to \infty$.

For the secure network coding problem, we specify additionally a collection $A$ of wiretap link sets, i.e., $A$ is a collection of subsets of $E$ such that an eavesdropper can...
wiretap any set in \( \mathcal{A} \). We consider three kinds of secrecy constraints: the requirement, for all \( A \in \mathcal{A} \), that 
\[ I(M; X^n(A)) = 0 \] corresponds to perfect secrecy; that 
\[ I(M; X^n(A)) \to 0 \] as \( n \to \infty \) corresponds to strong secrecy; and that 
\[ I(M; X^n(A)) \to 0 \] as \( n \to \infty \) corresponds to weak secrecy, where \( X(A) = \{ X(a, b) : (a, b) \in A \} \), and \( X(a, b) \) is the signal transmitted on the link \( (a, b) \). We say a secrecy rate \( R \) is feasible if the communication rate \( R \) is feasible and the prescribed secrecy condition is satisfied. The secrecy capacity of the network is defined as the supremum of all feasible secrecy rates. In the rest of the paper we study the case that \( \mathcal{A} \) is uniform, i.e., \( \mathcal{A} = \{ A \subset E : |A| \leq z \} \), where \( z \) is a specified maximum number of links that can be wiretapped.

### III. MULTIPLE UNICAST REDUCTION

#### A. Reduction of multiple unicast to secure communication

![Fig. 1: Source \( S \) wants to communicate with destination \( D \) secretly (with either weak secrecy, strong secrecy or perfect secrecy), \( \mathcal{N} \) is an embedded general network. Links are labeled by the signals transmitted on them.](image)

The following theorem reduces the open problem of multiple unicast network coding capacity to the secure network coding problem with only a single unicast and uniform wiretap sets of size \( 1 \).

**Theorem 1.** Given any unit rate \( K \)-unicast problem with source-destination pairs \( \{(S_i, T_i), i = 1, ..., K\} \) on a network \( \mathcal{N} \), the corresponding secure communication problem in Figure 1 with unit capacity links, any one of which can be wiretapped, has secrecy capacity \( K \) (under perfect, strong or weak secrecy requirements) if and only if the \( K \)-unicast problem is feasible.

**Proof.** The secrecy capacity is upper bounded by the capacity \( K \) of the min cut from \( S \) to \( D \).

"\( \Rightarrow \)" We show that feasibility of a weak secrecy rate of \( K \) implies feasibility of the \( K \)-unicast problem. Note that the result extends immediately to the cases of strong and perfect secrecy because they are even stronger conditions implying weak secrecy.

Suppose a secrecy rate of \( K \) is achieved by a code with length \( n \). Let \( M \) be the source input message, then 
\[ H(M) = Kn. \]

By the chain rule,
\begin{align*}
H(M|e^n_1, d^n_1, f^n_2, ..., f^n_K) &= H(M|e^n_1, d^n_1, f^n_2, ..., f^n_K) \\
&= H(M|e^n_1, d^n_1, f^n_2, ..., f^n_K) \\
&\leq H(M|e^n_1, d^n_1, f^n_2, ..., f^n_K).
\end{align*}

So
\begin{align*}
H(M|e^n_1, d^n_1, f^n_2, ..., f^n_K) &\geq H(M|d^n_1, f^n_2, ..., f^n_K) \\
&- H(e^n_1|d^n_1, f^n_2, ..., f^n_K) \\
&\geq (K-1)n,
\end{align*}

where the last inequality holds because of (1) and 
\[ H(e^n_1|d^n_1, f^n_2, ..., f^n_K) \leq H(e^n_1) \leq n. \] Similarly,
\begin{align*}
H(M|e^n_2, d^n_2, f^n_3, ..., f^n_K) &\leq H(M|e^n_2, d^n_2, f^n_3, ..., f^n_K) \\
&\leq n\epsilon_n + H(e^n_2, ..., e^n_K|d^n_1, f^n_2, ..., f^n_K) \\
&\leq n\epsilon_n + (K-1)n,
\end{align*}

where \( \epsilon_n \to 0 \) as \( n \to \infty \) and (4) is due to the cut set \( \{e^n_1, d^n_1, f^n_2, ..., f^n_K; e^n_2, ..., e^n_K\} \) from \( S \) to \( D \) and Fano’s inequality. Hence it follows
\begin{align*}
H(e^n_1) &\geq H(e^n_1|d^n_1, f^n_2, ..., f^n_K) \\
&\geq H(M|d^n_1, f^n_2, ..., f^n_K) \\
&- H(M|e^n_1, d^n_1, f^n_2, ..., f^n_K) \\
&\geq n - n\epsilon_n,
\end{align*}

where (6) holds because of (2), and (7) follows from (1) and (5). Also notice that
\begin{align*}
H(M|e^n_1, d^n_1, f^n_2, ..., f^n_K) &\geq H(M|e^n_1, f^n_2, ..., f^n_K) - H(d^n_1|e^n_1, f^n_2, ..., f^n_K),
\end{align*}

where
\[ H(M|e^n_1, f^n_2, ..., f^n_K) = H(M|e^n_1) \geq Kn - n\delta_n. \] with \( \delta_n \to 0 \) as \( n \to 0 \). Here the first equality holds because \( \{M, e^n_1\} \) is independent with \( \{f^n_i, i = 1, ..., K\} \) and the second inequality holds due to the weak secrecy constraint. Therefore by (5), (8) and (9) we have
\begin{align*}
H(d^n_1) &\geq H(d^n_1|e^n_1, f^n_2, ..., f^n_K) \\
&\geq H(M|e^n_1, f^n_2, ..., f^n_K) - H(M|e^n_1, d^n_1, f^n_2, ..., f^n_K) \\
&\geq n - n\epsilon_n - n\delta_n.
\end{align*}

Furthermore, by the independency between the sets of \( \{M, e^n_1, d^n_1\} \) and \( \{f^n_i, i = 1, ..., K\} \) we also have
\[ H(M|e^n_1, d^n_1, f^n_2, ..., f^n_K) = H(M|e^n_1, d^n_1). \]

According to (2) and (5), it is bounded by
\[ (K-1)n \leq H(M|e^n_1, d^n_1) \leq n\epsilon_n + (K-1)n. \]

Now consider the joint entropy of \( M, d^n_1, c^n_i \) and expand it in two ways
\begin{align*}
H(M, d^n_1, e^n_1) &= H(e^n_1|M, d^n_1) + H(M|d^n_1) + H(d^n_1) \\
&= H(M|e^n_1, d^n_1) + H(d^n_1) \\
&\leq (K+1)n + n\epsilon_n,
\end{align*}
where the last inequality holds because of (11) and
\[ H(d_i^n | c_i^n) \leq n, \quad H(c_i^n) \leq n. \]
Therefore
\[ H(e_i^n | M, d_i^n) \leq (K + 1)n + n\epsilon_n - H(M[d_i^n]) - H(d_i^n) \leq 2n\epsilon_n + n\delta_n. \]
where (10) and \( H(M[d_i^n]) = Kn \) (because \( M \) and \( d_i^n \) are independent by construction) are used to establish the inequality. And so by observing the Markov chain \( (M, d_i^n) \to (M, b_i^n) \to e_i^n \), it follows
\[ H(e_i^n | M, b_i^n) = H(e_i^n | M, b_i^n, d_i^n) \leq H(e_i^n | M, d_i^n) \leq 2n\epsilon_n + n\delta_n. \]
Then expand the joint entropy of \( M, b_i^n, c_i^n \) in two ways
\[ H(M, b_i^n, c_i^n) = H(b_i^n | M, c_i^n) + H(M | c_i^n) + H(e_i^n) \]
\[ = H(c_i^n | M, b_i^n) + H(M | b_i^n) + H(b_i^n) \]
\[ \leq (K + 1)n + 2n\epsilon_n + n\delta_n, \]
where the last inequality holds due to (13) and \( H(M|b_i^n) = Kn, \ H(b_i^n) \leq n \). Therefore by (7) and the weak secrecy constraint \( H(M|c_i^n) \geq Kn - n\delta_n \), we have
\[ H(b_i^n | M, c_i^n) \leq (K + 1)n + 2n\epsilon_n + n\delta_n - H(M|c_i^n) - H(e_i^n) \leq 3n\epsilon_n + 2n\delta_n. \]
So
\[ H(b_i^n | M, d_i^n) \leq H(b_i^n | M, c_i^n, d_i^n) \leq H(b_i^n | M, c_i^n) + H(c_i^n | M, d_i^n) \leq H(b_i^n | M, c_i^n) + H(M | b_i^n) + H(e_i^n) \]
\[ \leq (K + 1)n + 2n\epsilon_n + n\delta_n, \]
where the last inequality invokes (14) and (12). Notice that \( M \) is independent with \( b_i^n, d_i^n \), so
\[ H(b_i^n | d_i^n) = H(b_i^n | M, d_i^n) \leq 5n\epsilon_n + 3n\delta_n. \]
Now we bound the entropy of \( b_i^n \). Consider the joint entropy,
\[ H(M, b_i^n, c_i^n) = H(e_i^n | M, b_i^n) + H(M | b_i^n) + H(b_i^n) \]
\[ = H(b_i^n | M, b_i^n) + H(M | c_i^n) + H(e_i^n) \]
\[ \geq (K + 1)n - n\epsilon_n - n\delta_n, \]
where the last inequality holds because of (7), the secrecy condition \( H(M|c_i^n) \geq Kn - n\delta_n \), and \( H(b_i^n | M, c_i^n) \geq 0 \). So by (13) and because \( H(M | b_i^n) = Kn \), we have
\[ H(b_i^n) \geq (K + 1)n - n\epsilon_n - n\delta_n - H(c_i^n | M, b_i^n) - H(M | b_i^n) \geq n - 3n\epsilon_n - 2n\delta_n. \]
Finally, by (15) and (16),
\[ I(b_i^n ; d_i^n) \geq H(b_i^n) - H(b_i^n | d_i^n) \geq n - 8n\epsilon_n - 5n\delta_n, \]
The above argument extends to all other paths naturally (by renumbering the notations accordingly), so
\[ I(b_i^n ; d_i^n) \geq n - 8n\epsilon_n - 5n\delta_n, \forall i = 1, ..., K. \]
Therefore \( \forall i = 1, ..., K \), by the channel coding theorem, if we employ an outer code of length \( n \) by encoding \( b_i^n \) as a supersymbol, then there exists an inner code that achieves a rate of \( n - 8n\epsilon_n - 5n\delta_n \) from \( B_i \) to \( T_i \), and so the overall rate is
\[ R_i \geq \frac{n - 8n\epsilon_n - 5n\delta_n}{n} \to 1 \quad \text{as} \quad n \to \infty. \]
Because \( B_i \) can be viewed as a virtual source of \( S_i \), so \( \forall i = 1, ..., K \), the unicast from node \( S_i \) to \( T_i \) of rate 1 is feasible.

Conversely to the reduction above, for any weakly or strongly secure communication problem where any one link can be wiretapped, we can construct a communication problem without security constraints (which can in turn be reduced to an equivalent multiple unicast problem [6]) that is feasible if

Fig. 2: A scheme to achieve secrecy rate \( K \). \( V_x \) is the local key injected by node \( x \), with \( H(V_x) = 1 \), \( \forall x \). \( M_i, i = 1, ..., K \) are source input messages, with \( H(M_i) = 1 \), \( i = 1, ..., K \).
and only if the secure communication problem is feasible. The constructed communication network, called the $A$-enhanced network and described in [7] has an additional virtual sink node corresponding to each wiretapped set. Due to space limit we refer readers to [8], [7] for details in the case of weakly secure communication. The result for strongly secure communication follows from the equivalence of the capacity region for weak and strong security, shown in [9].

IV. ACHIEVABLE STRATEGIES

A. Global Key Schemes

We consider a class of achievable secure coding schemes in which all random keys are global, i.e. decodable with zero error by both the source and the sink, and perfect secrecy is ensured by having global keys of total rate equal to $z$, the number of wiretapped links.

Let $\Lambda_i(U)$ denote the collection of all cuts between $U \subset V$ and $t \in V \in G$. For any cut $C$, let $I_C$ be the corresponding cut-set. The following linear program characterizes the rate of the optimal coding scheme within this class.

$$\max R_S \quad \text{(LP1)}$$

s.t. $|I_C| \geq \sum_{i \in U} r_i$, $\forall U \in 2^V \setminus (S)$

$$|I_C| \geq \sum_{i \in U} r_i$, $\forall U \in 2^V \setminus (D)$

$$r_i = k_i, \forall i \in V, i \neq S$$

$$r_S = R_S + R_S$$

$$\sum i \in V k_i \geq z$$

Corollary 1. $\forall z \in \mathbb{R}$, let $R^*_S$ be the solution of LP1, $R_S$ the rate of any global key scheme which injects total key rate $z' = \sum_{i \in V} k_i$ with $z' \geq z$, then $R^*_S \geq R_S$.

Proof. By definition any global key scheme of rate $R_S$ is a solution to the multi-source multicast problem such that any node $i \in V$ is a source with rate $r_i = k_i$, $i \neq S$; $r_i = R_S + k_S$, $i = S$ and the sinks are $S$ and $D$. This rate vector is in the capacity region upper bounded by the cut-set bounds (17), (18) imposed in LP1. Hence $R^*_S \geq R_S$. □

The number of constraints in LP1 grows exponentially in the size of $V$. The following linear program formulated as a multi-source multicast problem is equivalent to LP1, but with number of constraints linear in $|E|$. For every $(u,v) \in E$, let $c(u,v)$ be the number of edges connecting $u$ and $v$.

$$\max R_S \quad \text{(LP2)}$$

s.t.

$$\sum_{w:(u,w) \in E} f_D(u,v) - \sum_{w:(v,u) \in E} f_D(v,u) = \begin{cases} R_S + k_S & u = S \\ -R_S - k_S & u = D \\ 0 & \text{o.w.} \end{cases}$$

$$\sum_{w:(u,w) \in E} f^D_i(u,v) - \sum_{w:(v,u) \in E} f^D_i(v,u) = \begin{cases} k^D_i & u = i \\ -k^D_i & u = D \\ 0 & \text{o.w.} \end{cases}$$

$$\sum_{w:(u,w) \in E} f_S(u,v) - \sum_{w:(v,u) \in E} f_S(v,u) = \begin{cases} k_D & u = D \\ -k_D & u = S \\ 0 & \forall u \neq S, D \end{cases}$$

Here $f_D$ and $\{f^D_i\}$ represent a multi-commodity flow to $D$; $f_S$ and $\{f^S_i\}$ represent a multi-commodity flow to $S$. Equations (22), (23), (24) and (25) are flow conservation constraints; (26) and (27) are link capacity constraints; (28) and (29) are secrecy constraints. LP1 and LP2 are equivalent due to [10, Theorem 2.3], i.e., the multi-source multicast problem specified in LP1 has a solution if and only if there exist corresponding multi-commodity flows to each of the sinks specified in LP2. Therefore the two linear programs have the same feasible region and the same optimal solution $R^*_S$.

Theorem 2. Let $R^*_S$ be the solution of LP2, there exists global key scheme that achieves message rate $R^*_S$ and perfect secrecy.

Proof. The proof is constructive. First augment $G$ to $G'$ as follows: 1) For every node $i \in V$, create a virtual key source $v_i$ and connect it to $i$ with edge $(v_i, i)$ of capacity $k_i$. Also create a virtual message source $v_M$ which is connected to $S$ by edge $(v_M, S)$ of capacity $R^*_S$. 2) Connect each subset $A \in A$ to a virtual node $t^A$. Specifically, $\forall (i, j) \in E$, create node $v_{ij}$ and replace $(i, j)$ by two edges $(i, v_{ij})$ and $(v_{ij}, j)$, then $\forall (i, j) \in A$, create edge $(v_{ij}, t^A)$, all of unit capacity. 3) For every $A \in A$, let $R_{v \rightarrow A}$ be the max sum of flows from $\{v_i : i \in V\} \cup \{v_M\}$ to $t^A$. Create virtual sink $D^A$ connected by $(t^A, D^A)$ of capacity $R_{v \rightarrow A}$, and by edge $(v_M, D^A)$ of capacity $R^*_S$. 4) Create a super key source $v_K$, connected by edges $(v_i, v_K)$ of capacity $k_i$, $\forall i \in V$. Let $R_{w} = \sum_{i \in V} k_i$ be the sum key rate, and connect the super key source to every virtual sink $D^A$ with edge $(v_K, D^A)$ of capacity $R_w - R_{v \rightarrow A}$.

Then consider the multi-source multicast problem where $S$, $D$ and the virtual sinks $\{D^A\}$ each demands the source messages and all the random keys from $\{v_i : i \in V\} \cup \{v_M\}$. The constraints in LP2 guarantee that the flows to $S$ and $D$ exist. Furthermore, note $R_{w \rightarrow t^A}$ equals the max sum of flows from $\{v_i : i \in V\}$ to $t^A$ because all keys are global and $R_{w \rightarrow t^A} \leq z \leq R_w$. Together with the additional capacity $R_w - R_{v \rightarrow A}$ in the augmented network, the max flow from the message and random key sources to each virtual sink $D^A$ is sufficient to ensure that the multicast problem is feasible [10]. A capacity-achieving code for this multisource multicast problem in the augmented graph corresponds to a code achieving rate $R^*_S$ for the original secrecy problem. Perfect secrecy is ensured because the information received by each virtual sink $D^A$ from each set $A \in A$ of original network edges must be independent of information received from the
In this case local keys can be injected at \( v \). Hence each gadget is associated with two nodes, and it is able to protect the sub-path of \( P_k \) between these two nodes. Furthermore, \( E_k \) is introduced so that the sub-paths may overlap. The virtual local key sources and additional links are introduced for reusing local keys on multiple paths. Intuitively if Algorithm 1 returns a local key chain \( L_1 \) on \( P_k \) then path \( P_k \) is protected by a series of local keys. If Algorithm 1 returns local key chains on \( R_S + 1 \) paths among \( \{ P_1, \cdots, P_{R_S+k_S} \} \), then we can transmit one less global key and one unit more message. Without loss of generality (by renumbering if necessary) we assume the algorithm returns \( L_1, \cdots, L_{R_S+1} \) on the first \( R_S + 1 \) paths \( P_1, \cdots, P_{R_S+1} \).

Below we introduce a secure code that achieves rate \( R_S + 1 \). We first construct a code \( C' \) that transmits \( R_S + 1 \) units of message and \( z - 1 \) global keys as described in Section IV-A. Hence \( C' \) achieves perfect secrecy if up to \( z - 1 \) links are wiretapped. Note because the coding subgraph of \( C' \) is acyclic, any edges incident with \( \bigcup \{ P_i \setminus \{ S, D \} \} \) are used for the unicast to \( D \) only, hence it suffices for \( C' \) to perform routing on \( \bigcup \{ P_i \setminus \{ S, D \} \} \). For the path-based approach in [12] suffices to construct \( C' \), and one can reuse the same coding coefficient for any edge outgoing from \( \bigcup \{ P_i \setminus \{ S, D \} \} \) as the coding coefficient of the incoming edge on a path. Next we construct a code \( C \) on top of \( C' \) as follows. \( C \) is identical to \( C' \) except on \( P = \{ P_1, \cdots, P_{R_S+1} \} \). For \( P_k \in P \), consider the gadgets in \( L_k \), each of them generates an independent local key and deliver the key to two nodes \( i, j \in P_k \). Assuming that \( i \) is upstream and \( j \) is downstream, \( i \) adds this local key to the incoming signal and send the sum as the outgoing signal along \( P_k \). This signal travels downstream and when it reaches \( j \), the key is canceled. Because \( C' \) performs routing on \( P \), the local keys indeed stay local and are completely canceled within \( P \). Therefore \( D \) can successfully decode the source messages, i.e., the communication requirement is accomplished.

Next we show \( C \) achieves perfect secrecy. Denote \( E_P' \) as the set of edges of the paths \( \{ P_1, \cdots, P_{R_S+k_S} \} \), \( E_P \) as the set of edges used by any flows in LP2 except \( E_P' \). Recalled the augmented graph \( G'_S \) used to construct \( C' \), and consider the subgraph \( G'_S \) of \( G' \) by deleting all edges in \( E_P \) and all unused edges (edges that carry no flows). Because \( R_S + k_S \) is the max flow from \( S \) to \( D \), there are no out-going edges from \( S \) (otherwise contradicts the fact that \( R_S + k_S \) is the max flow). So the min cut from the set of sources \( \{ v_i : i \in \mathcal{V} \} \cup \{ V_M \} \) to any \( t^A \) in \( G'_S \) is at most \( z - k_S \), and therefore by the construction of \( C' \), any wireset set \( A \) that does not include at least \( k_S \) edges in \( E_P \) is not effective, i.e., not leaking source message information. Hence without loss of generality we assume an effective wiretap set \( A \) include at least \( k_S \) edges in \( E_P \). By the construction of \( C' \), \( E_P \) consists of \( R_S + k_S \) disjoint routing paths. Clearly \( A \) must eavesdrop distinct paths, and therefore by the pigeonhole principle, at least one path in \( P \) is wiretapped. Denote the wiretapped signal on this path as \( X_1 + V_1 \), where \( X_1 \) is the original signal sent in \( C' \), and \( V_1 \) is one local key or a combination of them. Denote the remaining wiretapped signals as \( X_2 + V_2, \cdots, X_z + V_z \), where \( V_i, i \geq 2 \) is either zero or a function of local keys. Note \( L \) is a random variable uniformly drawn from a finite field and is independent of \( \{ M, X_2, \cdots, X_z \} \). Therefore \( X_1 + L \) also follows uniform
Algorithm 1 Local Key Chain Search for $P_k$

▷ Initialization

set $E_k := \{\text{reversal of the edges of } P_k\}$

unlabel all nodes

set $\text{pred}_0(j) := 0$, $\text{pred}_\text{out}(j) := 0$, $\forall j \in V \setminus P_k$

set $\text{LIST}_\text{in} := \emptyset$, $\text{LIST}_\text{out} := \emptyset$

label $S$ and set $\text{LIST}_P := \{S\}$

▷ Label nodes that can be reached by gadgets

while $D$ is unlabelled and LIST$_P$, LIST$_\text{in}$ and LIST$_\text{out}$ are not all empty do

remove a node $i$ from either LIST$_P$, LIST$_\text{in}$ or LIST$_\text{out}$

if $i$ is removed from LIST$_P$ or LIST$_\text{out}$ then

for all $(i, j) \in \mathcal{E}_L$, $j \notin P_k$ do

if $j$ is not labeled IN then label $j$ IN, set

$\text{pred}_\text{in}(j) := i$ and add $j$ to LIST$_\text{in}$

end for

for all $(j, i) \in \mathcal{E}_L$, $j \notin P_k$ do

if $j$ is not labeled OUT then label $j$ OUT, set

$\text{pred}_\text{out}(j) := i$ add $j$ to LIST$_\text{out}$

end for

for all $(i, j)$ or $(j, i) \in \mathcal{E}_L$, $j \in P_k$ do

if $j$ is not labeled $P$ then label $j$ $P$

if $(i, j) \in \mathcal{E}_k$ then set $\text{pred}(j) := (i, \text{IN})$

else set $\text{pred}(j) := (i, \text{OUT})$

end if

add $j$ to LIST$_P$

end if

end for

if $i \in P_k$ then

for all $(i, j) \in \mathcal{E}_k$ do

if $j$ is not labeled $P$ then label $j$ $P$, set

$\text{pred}(j) := (i, \text{IN})$ and add $j$ to LIST$_P$

end for

end if

end if

if $i$ is removed from LIST$_\text{in}$ then

for all $(i, j) \in \mathcal{E}_L$, $j \notin P_k$ do

if $j$ is not labeled IN then label $j$ IN, set

$\text{pred}_\text{in}(j) := i$ and add $j$ to LIST$_\text{in}$

end for

for all $(i, j) \in \mathcal{E}_L$, $j \in P_k$ do

if $j$ is not labeled $P$ then label $j$ $P$, set $\text{pred}(j) := (i, \text{IN})$ and add $j$ to LIST$_P$

end for

end if

end if

end while

distribution and is independent of $\{M, X_2, \ldots, X_z\}$. So

$I(M; X_1 + V_1, \ldots, X_z + V_z) \leq I(M; X_1 + V_1, X_2, \ldots, X_z) = I(M; X_2, \ldots, X_z) = 0$,

and perfect secrecy is achieved.

Figure 4 shows an example in which global key schemes achieve at most unit rate. With local key enhancement rate 2 is achieved. For path $(S, A, D)$ the two (not overlapping) gadgets are $(\{S, A\})$ and $(\{B, A\}, \{B, D\})$; for path $(S, C, E, D)$ the two overlapping gadgets are $(\{E, S\})$ and $(\{B, C\}, \{B, D\})$. Note local key $V_2$ and edge $(B, D)$ are reused for both paths.

Finally, message rate can be inductively increased by repeating the above procedure. Specifically, at the $\alpha$-th iteration of local key enhancement, $\alpha < k_S$, if Algorithm 1 finds $k_S + \alpha$ local keys chains protecting $k_S + \alpha$ paths, then rate $R_S + \alpha$ is feasible. Due to space limit we defer details to [8].

REFERENCES


