Private Network Coding without Secret Keys

Fabio Pasqualetti and Alberto Padoan

Abstract— **This paper studies the problem of private network coding, where a server aims to establish simultaneous private communications with multiple clients. We propose a control-theoretic approach to private (linear) network coding. We develop a server coding scheme ensuring privacy of information and maximum communication throughput without dedicated privacy mechanisms, such as data encryption, randomization and secret keys. Our coding scheme relies on the knowledge of the communication network. For our setup, we derive graph-theoretic and algebraic conditions for the existence of private coding schemes. Finally, we characterize the complexity of our private coding scheme and we discuss an illustrative example.**

I. Introduction

Network coding enables efficient transmission of data over networks. In contrast with classic communication networks where nodes reroute incoming packets, in network coding nodes transmit a weighted combination of their incoming packets [1], [2]. While improving communication efficiency [3], [4], [5], [6], network coding is inherently not secure against misbehaving nodes polluting or replaying packets [7] – due to mixing of information, corrupted packets may contaminate the information received by a destination – and it does not guarantee privacy of the transmitted data – with knowledge of a decoding key, a wiretapper may decode messages destined to legitimate clients [8].

In this work we study the problem of private network coding, where a server aims to establish private communications over a public network. We model the communication network as a directed graph, and we let the server (clients) inject (receive) packets at specific network nodes. By leveraging the formalism of network coding, linear iteration over finite fields [3], [9], and control-theoretic techniques [10], we develop a transmission strategy for the server to communicate arbitrary messages to a client, while preventing other clients from decoding the transmitted data. Our method assumes the knowledge of the communication network, yet it does not rely on dedicated privacy mechanisms, such as data encryption, randomization and private keys.

Related work Security and privacy of distributed systems and communication networks have been extensively studied in the last decades. An early work concerned with secure communication is due to Shannon [11], where the author proposes the use of a secret key shared through a secure communication channel to prevent a wiretapper from decoding the transmitted message. This strategy is further developed in the secret sharing model proposed in [12], [13] and more recently in [8], [14], to name a few. With respect to these works, our method does not rely upon randomization in the coding, nor on the presence of secret communication channels or secret keys. Instead, our code ensures privacy of information by exploiting the structure and dynamic behavior of the communication network. Secure network coding without secret keys has been recently investigated in [15], where it is shown that a secure network code can be designed for a given network if the cardinality of the alphabet is sufficiently large. Our method is fundamentally different, as it relies on a specific transmission scheme, which we design, and it assumes the coding mechanism to be given.

Cryptographic approaches to detect and correct corrupted packets are presented in [16], [17], [18]. These approaches rely on augmenting the network coded packets with additional verification information. This allows intermediate nodes to verify the validity of coded packets and filter out polluted packets at the expenses of a high computational overhead. Information theoretic approaches tolerate polluted packets by encoding enough redundant information to allow the receiver to recover native messages [19], [20]. With these approaches, the maximum transmission throughput is usually not achieved due to the presence of redundant information. Instead, our code does not transmit redundant information, achieves maximum throughput, and requires minimal computations from the server and the receivers.

Networks with adversaries have been considered in different scenarios and with various adversarial models. The resilience against Byzantine adversaries is characterized in [21], [22] for networks transmitting binary messages, and in [23], [24] for consensus networks over the field of real numbers. The problem of correcting adversarial errors is considered for instance in [25], [26]. These works constitute a complementary line of research: our transmission method does not correct the errors introduced by adversaries and, instead, it exploits the network dynamics to prevent adversaries from eavesdropping the message directed to the clients.

Paper contributions The main contribution of this work is the design of a communication protocol for private network coding, where a server aims to establish private communication channels with multiple clients. The proposed communication protocol achieves maximum communication throughput, ensures privacy of information without relying on dedicated privacy mechanisms, and is computationally efficient. Our analysis combines the formalism of linear network coding and finite-field iterations with control-theoretic notions. Based on our framework, we derive graph-theoretic and algebraic conditions on the communication network for the applicability of our private communication protocol, and we thoroughly characterize its performance.

Paper organization The remainder of the paper is organized as follows. In Section II we present the problem setup and some preliminary results. Section III contains our main

Fabio Pasqualetti is with the Mechanical Engineering Department, University of California at Riverside, `fabiopas@engr.ucr.edu`. Alberto Padoan is with Department of Electrical and Electronic Engineering, Imperial College, London, `alberto.padoan13@imperial.ac.uk`.

Preprint submitted to 53rd IEEE Conference on Decision and Control.
Received March 20, 2014.

results, including the design of a private network code and its applicability conditions. Finally, Section IV contains an illustrative example, and Section V concludes the paper.

II. Problem Setup and Preliminary Concepts

In this section we present our network and communication models, which are applicable to both wired and wireless scenarios. We model a network as a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{1, \dots, n\}$ and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denote the set of nodes and edges, respectively. Each directed edge $(i, j) \in \mathcal{E}$ corresponds to a communication channel from node j to node i. We assume the presence of at most one communication channel between any two nodes, and we let each communication channel have unit capacity and transmission delay (only one symbol can be transmitted on a channel at each time, and each symbol is delivered with unit time delay). We denote the sets of out-neighbors and in-neighbors of node i with $\mathcal{N}_i^{\text{out}} = \{j \,:\, (j,i) \in \mathcal{E},\, j \in \mathcal{V}\}$ and $\mathcal{N}_i^{\text{in}} = \{j \,:\, (i,j) \in \mathcal{E},\, j \in \mathcal{V}\}$, respectively.

Following the paradigm of linear network coding [3], we allow each node to transmit linear combinations of its incoming packets. In particular, let $a_{ij} \in \mathbb{F}_{\text{p}}$ be the weight associated with the edge (i, j), and let $x_i(t) \in \mathbb{F}_{\text{p}}$ be the *state* of node i at time t.[1] At each time t, each node i performs the following operations in order:

(i) transmit the state $x_i(t)$ to its out-neighbors $\mathcal{N}_i^{\text{out}}$,
(ii) receive the state $x_j(t)$ from its in-neighbors $\mathcal{N}_i^{\text{in}}$,
(iii) update its state to the value $\sum_{j \in \mathcal{N}^{\text{in}}} a_{ij} x_j(t)$.

We assume all operations to be performed in the field $\mathbb{F}_{\text{p}}$ with addition and multiplication defined as in *modular arithmetic*, that is, by performing the operation in the set of integers $\mathbb{Z}$, dividing by p, and taking the remainder. Let $x : \mathbb{N}_{\geq 0} \to \mathbb{F}_{\text{p}}^n$ be the map describing the state of the nodes over time, where $x(t)$ is the vector of the states at time t. The evolution of the states is described by the linear iteration over $\mathbb{F}_{\text{p}}$

$$x(t+1) = Ax(t),$$

where $a_{ij} = 0$ whenever $(i, j) \notin \mathcal{E}$, and $A = [a_{ij}]$.

In this work we the problem of *private network coding*, where the server aims to establish a private communication with some clients. We let the network behave as a transmission media, in which packets are injected by the server at some nodes, and received by the clients at different nodes. To be specific, let $\mathcal{U} \subseteq \{1, \dots, n\}$, with $m = |\mathcal{U}|$, be the set of nodes where the server injects its packets, and let $\mathcal{Y}_i \in \{1, \dots, n\}$ be the node observed by the i-th client and let $q \in \mathbb{N}$ denote the number of clients. Let B (resp. C_i^{T}) be the submatrix of I_n with columns indexed by $\mathcal{U}$ (resp. $\mathcal{Y}_i$), where I_n is the n-dimensional identity matrix. The recursive relation between the packets received by the i-th client and the packets transmitted by the server reads as

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t), \\ y_i(t) &= C_i x(t), \end{aligned} \tag{1}$$

where $u : \mathbb{N}_{\geq 0} \to \mathbb{F}_{\text{p}}^m$ denotes the sequence of packets transmitted by the server, $y_i : \mathbb{N}_{\geq 0} \to \mathbb{F}_{\text{p}}$ denotes the sequence of packets received by the i-th client, and where we assume $x(0) = 0$. Let

$$C = [C_1^{\mathsf{T}} \ \dots \ C_q^{\mathsf{T}}]^{\mathsf{T}} \text{ and } y = [y_1^{\mathsf{T}} \ \dots \ y_q^{\mathsf{T}}]^{\mathsf{T}}.$$

We say that the i-th communication channel is *private* if the server is able to transmit, possibly with delay, an arbitrary message to the i-th client while preventing other clients from decoding any part of the message.

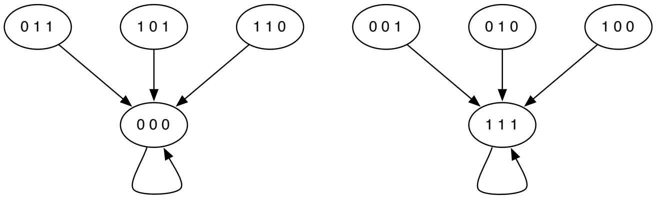


Fig. 1. This figure shows the transition graph associated with the network in Example 1 over the field $\mathbb{F}_2$. Notice that the transition graph has p^n vertices, and that each vertex has unit out-degree. See [29] for a study of the consensus properties of networks over finite fields.

Lemma II.1 ***(Private communication channel)*** *For the network model* (1)*, the i-th communication channel is private if and only if for every message $s : \{0, \dots, T\} \to \mathbb{F}_{\text{p}}$ there exists a sequence $u : \mathbb{N}_{\geq 0} \to \mathbb{F}_{\text{p}}^m$ satisfying*

$$\begin{cases} y_i(t) = 0, & \textit{for } t \notin \{\delta, \dots, \delta + T\}, \\ y_i(t) = s(t - \delta), & \textit{for } t \in \{\delta, \dots, \delta + T\}, \\ y_j(t) = 0, & \textit{for } t \in \{0, 1, \dots\}, \end{cases} \tag{2}$$

for some delay $\delta \in \mathbb{N}$ and for all clients $j \neq i$.

Proof: From the first two equations, the i-th client receives the message s. Moreover, since y_j is identically zero, the j-th client cannot reconstruct the input sequence u injected by the server, and hence the sequence y_i. On the other hand, if y_j is not identically zero, then the j-th client may exploit the network dynamics to reconstruct some parts of the message y_i received by the i-th client. ■

Remark 1 ***(Non-interacting control)*** *Our approach is inspired and motivated by the classic problem of non-interacting control [10]. With respect to the classic setup, our results are specialized to systems evolving on finite fields rather than the field of real numbers. As discussed for instance in [28], control-theoretic properties and techniques for real-valued systems may not extend to systems over finite fields, and their validity needs to be proven.* □

III. Private Network Coding

In this section we design a transmission scheme for a server to communicate privately with clients without using private keys. For convenience of analysis we define the *transition graph* associated with the network (1) as $\mathcal{G}_{\text{t}} = (\mathcal{V}_{\text{t}}, \mathcal{E}_{\text{t}})$, where $\mathcal{V}_{\text{t}} = \{v \;:\; v \in \mathbb{F}_{\text{p}}^n\}$ and $(v_i, v_j) \in \mathcal{E}_{\text{t}}$ if and only if $v_i = Av_j$. The transition graph contains p^n vertices, and each vertex has unit out-degree. Moreover, it can be shown that the transition graph is composed of disjoint weakly-connected subgraphs, that each subgraph contains

[1] The field $\mathbb{F}_{\text{p}}$, with p a prime number, consists of the integers $\{0, \dots, p-1\}$, with addition and multiplication defined as in modular arithmetic [27].

Preprint submitted to 53rd IEEE Conference on Decision and Control.
Received March 20, 2014.

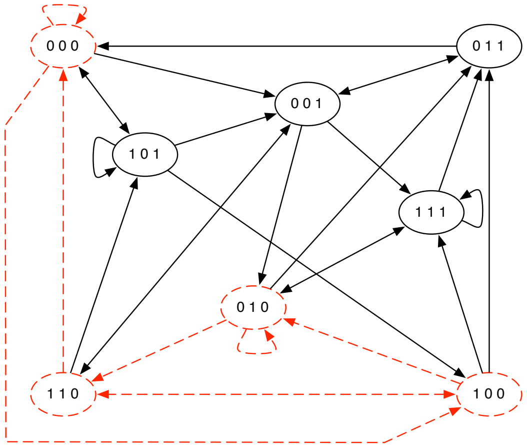


Fig. 2. This figure shows the forced graph associated with the network in Example 1 (solid black). The subgraph $\mathcal{G}_{\mathrm{f}}^1$ is also reported (dashed red). The first communication channel is private; see Theorem III.1.

exactly one cycle, possibly of unit length, and that each disjoint subgraph contains a globally reachable node [30], [29]. An example of transition graph is reported in Fig. 1. We additionally define the *forced graph* associated with the network (1) as $\mathcal{G}_{\mathrm{f}} = (\mathcal{V}_{\mathrm{f}}, \mathcal{E}_{\mathrm{f}})$, where $\mathcal{V}_{\mathrm{f}} = \{v \ : \ v \in \mathbb{F}_{\mathrm{p}}^n\}$ and $(v_i, v_j) \in \mathcal{E}_{\mathrm{t}}$ if and only if $v_i = Av_j + Bu$ for some $u \in \mathbb{F}_{\mathrm{p}}^m$. Notice that the transition graph is a subgraph of the forced graph, that the forced graph has p^n vertices, and that each vertex of the forced graph has out-degree equal to p^m. An example of forced graph is reported in Fig. 2. Finally, we define the sets of *observable states* as

$$\mathcal{O}_i = \{v \ : \ C_i v \neq 0, \ v \in \mathbb{F}_{\mathrm{p}}^n\} \text{ for } i \in \{1, \dots, q\},$$

and the i-th set of *unobservable states* as

$$\mathcal{C}_i = \mathcal{V}_{\mathrm{f}} \setminus \bigcup_{j \neq i} \mathcal{O}_j. \tag{3}$$

Theorem III.1 ***(Graph conditions for private channel)*** *Let $\mathcal{G}_{\mathrm{f}}$ be the forced graph of the network (1), and let $\mathcal{G}_{\mathrm{f}}^i$ be the subgraph of $\mathcal{G}_{\mathrm{f}}$ with vertices $\mathcal{C}_i$ defined as in (3). The i-th communication channel is private if and only if, for every message $s : \{0, \dots, T\} \to \mathbb{F}_{\mathrm{p}}$, there exists a path on $\mathcal{G}_{\mathrm{f}}^i$, say $p : \{0, 1, \dots\} \to \mathcal{V}_{\mathrm{f}}$, and $\delta \in \mathbb{N}$ satisfying*

$$\begin{aligned} C_i p(t+\delta) &= s(t), \text{ for } t \in \{0, \dots, T\} \\ C_i p(t) &= 0, \text{ otherwise.} \end{aligned}$$

Proof: The statement follows from Lemma II.1 and the fact that state trajectories of network (1) are in one-to-one correspondence with paths on its associated forced graph. ■

Example 1 ***(Transition and forced graphs)*** *Consider the network (1) over the field $\mathbb{F}_2$ with matrices*

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, C_1^{\mathsf{T}} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, C_2^{\mathsf{T}} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

The transition graph associated with A is reported in Fig. 1, while the forced graph associated with A and B is in Fig. 2. Notice that the transition graph is a subgraph of the forced graph, and that the first communication channel is private. In fact, let $s : \{0, \dots, T\} \to \mathbb{F}_{\mathrm{p}}$ be a sequence to be transmitted to client 1, and consider a path satisfying

$$\begin{cases} p(t+\delta) = (0,0,0) & \text{if } s(t) = 0 \text{ and } s(t+1) = 0, \\ p(t+\delta) = (1,0,0) & \text{if } s(t) = 0 \text{ and } s(t+1) = 1, \\ p(t+\delta) = (0,1,0) & \text{if } s(t) = 1 \text{ and } s(t+1) = 1, \\ p(t+\delta) = (1,1,0) & \text{if } s(t) = 1 \text{ and } s(t+1) = 0, \end{cases}$$

for some delay $\delta \in \mathbb{N}$. Notice that $y_1(t) = s(t)$ and $y_2(t) = 0$, so that the first communication channel is private. □

Theorem III.1 provides a necessary and sufficient condition for the existence of private communications between a server and its clients. Unfortunately, a verification of the graph condition in Theorem III.1 may be prohibitive for large networks, because the size of the forced graph grows exponentially with the number of nodes in the network (the forced graph contains p^n vertices and p^{n+m} edges; see Fig. 2). In what follows we derive algebraic conditions for private communication channels based on the network matrices.

We start by defining the necessary notation. For the network (1), an index $N \in \mathbb{N}$, and a positive integer $0 < \delta < N$, let

$$L_N = \begin{bmatrix} A^{N-1}B & \cdots & AB & B \end{bmatrix},$$

$$T_N = \begin{bmatrix} 0_{q\times m} & 0_{q\times m} & \cdots & 0_{q\times m} \\ CB & 0_{q\times m} & \cdots & 0_{q\times m} \\ CAB & CB & \ddots & 0_{q\times m} \\ \vdots & \ddots & \ddots & \vdots \\ CA^{N-2}B & \dots & CB & 0_{q\times m} \end{bmatrix}, \tag{4}$$

$$D_{i,N,\delta} = \Big[\underbrace{0_q \ \cdots \ 0_q}_{\delta} \ \ e_i \ \ \underbrace{0_q \ \cdots \ 0_q}_{N-\delta-1} \Big]^{\mathsf{T}},$$

$$Y_N = \begin{bmatrix} y^{\mathsf{T}}(0) & y^{\mathsf{T}}(1) & \cdots & y^{\mathsf{T}}(N-1) \end{bmatrix}^{\mathsf{T}},$$

$$U_N = \begin{bmatrix} u^{\mathsf{T}}(0) & u^{\mathsf{T}}(1) & \cdots & u^{\mathsf{T}}(N-1) \end{bmatrix}^{\mathsf{T}},$$

where 0_q denotes the q-dimensional zero row vector, $0_{q\times m}$ denotes the $(q \times m)$-dimensional zero matrix and e_i is the i-th row of the q-dimensional identity matrix. Observe that

$$Y_N = T_N U_N.$$

For $k \in \{1, \dots, N\}$, define the block-diagonal matrix

$$H_k = \text{blk-diag}(\underbrace{0_{m\times m}, \dots, 0_{m\times m}}_{k-1}, I_m, \underbrace{0_{m\times m}, \dots, 0_{m\times m}}_{N-k-1}),$$

where each diagonal submatrix is zero except for the k-th, which is the m-dimensional identity matrix. Finally, let

$$U_{N+T}^{\tau} = \Big[\underbrace{0_m \ \cdots \ 0_m}_{\tau} \ \ U_N^{\mathsf{T}} \ \ \underbrace{0_m \ \cdots \ 0_m}_{T-\tau} \Big]^{\mathsf{T}}.$$

Theorem III.2 ***(Algebraic condition for private communication)*** *For the network model (1), the i-th communication* *channel is private if and only if there exists $\delta \in \mathbb{N}$ such that, for every $N > \delta$ and for some vector $U_N \in \mathbb{F}_{\mathrm{p}}^{mN}$,*

$$T_N U_N = D_{i,N,\delta},$$

where T_N and $D_{i,N,\delta}$ are as in (4).

Proof: We start by showing the necessity of the statement. Let $s : \{0\} \to \mathbb{F}_{\mathrm{p}}$ be the message to be transmitted by the server to the i-th client. From Lemma II.1 the unit length message s can be privately transmitted to the i-th client only if there exists δ such that $y_i(\delta) = s(0)$, $y_i(\tau) = 0$ for $\tau \neq \delta$, and $y_j(t) = 0$ for all $t \in \mathbb{N}$ and clients $j \neq i$. It follows from the definition of the matrices in (4) that the message s can be privately transmitted to the i-th client only if $T_N U_N = D_{i,N,\delta}$ for some δ and for every $N > \delta$.

Sufficiency of the statement follows from the linearity of the network (1). Consider the message $s : \{0, \dots, T-1\} \to \mathbb{F}_{\mathrm{p}}$. Notice that the assumption $T_N U_N = D_{i,N,\delta}$ implies that the unit length message $\{1\}$ is privately transmitted to the i-th client, that is $y_i(\delta) = 1$, $y_i(\tau) = 0$ for $\tau \neq \delta$, and $y_j(t) = 0$ for all $t \in \mathbb{N}$ and clients $j \neq i$. Due to linearity we have $T_{N+T} U_{N+T}^{\tau} = D_{i,N+T,\delta+\tau}$ for all $\tau < T$, and

$$T_{N+T} \sum_{\tau=0}^{T-1} U_{N+T}^{\tau} s(\tau) = \sum_{\tau=0}^{T-1} D_{i,N+T,\delta+\tau}\, s(\tau),$$

so that s is privately transmitted to the i-th client. ■

In Theorem III.2 we state a necessary and sufficient algebraic condition for private communication. Note that the server input u may be nonzero at all times in the transmission interval, independently of the length of the message. In fact, when N grows, the transmission of a finite-length message may require an arbitrarily long input sequence. In the next Theorem we provide a condition to ensure that every finite-length message is transmitted with a finite-length input sequence, and we specify the server transmission code.

Theorem III.3 ***(Private communication with finite transmission)*** *Consider the network* (1) *with $x(0) = 0$. The i-th communication channel is private if there exist $N \in \mathbb{N}$ and $0 < \delta < N$ satisfying*

$$T_N U_N = D_{i,N,\delta}, \text{ and} \tag{5a}$$

$$L_N U_N = 0, \tag{5b}$$

where T_N, $D_{i,N,\delta}$, and L_N are as in (4), *and $U_N \in \mathbb{F}_{\mathrm{p}}^{mN}$.*

Moreover, let $s : \{0, \dots, T\} \to \mathbb{F}_{\mathrm{p}}$ be the message to be transmitted to the i-th client, and let $u : \mathbb{N}_{\geq 0} \to \mathbb{F}_{\mathrm{p}}^{m}$ be the sequence of packets transmitted by the server, where

$$u(t) = \sum_{\tau=0}^{N-1} H_{\tau+1} U_N\, w(t-\tau), \tag{6}$$

with $w(t) = s(t)$ for $t \in \{0, \dots, T\}$, and $w(t) = 0$ otherwise. Then, the sequence u achieves private communication of the message s, that is,

$$\begin{cases} y_i(t) = 0, & \text{for } t \notin \{\delta, \dots, \delta + T\}, \\ y_i(t) = s(t-\delta), & \text{for } t \in \{\delta, \dots, \delta + T\}, \\ y_j(t) = 0, & \text{for } t \in \{0, 1, \dots\}. \end{cases}$$

Proof: We prove the theorem by showing that the sequence (6) achieves private communication of the message s. Note that the first elements of the sequence u read as $u(0) = H_1 U_N s(0)$, $u(1) = H_1 U_N s(1) + H_2 U_N s(0)$, and $u(2) = H_1 U_N s(2) + H_2 U_N s(1) + H_3 U_N s(0)$. In particular, the sequence u can be written as

$$\begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(N-1) \\ \vdots \\ \vdots \\ u(N+T-1) \end{bmatrix} = \begin{bmatrix} H_1 U_N & 0_m & \cdots & 0_m \\ H_2 U_N & H_1 U_N & \ddots & \vdots \\ \vdots & H_2 U_N & \ddots & 0_m \\ H_N U_N & \vdots & \ddots & H_1 U_N \\ 0_m & H_N U_N & \ddots & H_2 U_N \\ \vdots & \ddots & \ddots & \vdots \\ 0_m & \cdots & 0_m & H_N U_N \end{bmatrix} \begin{bmatrix} s(0) \\ s(1) \\ \vdots \\ s(T) \end{bmatrix},$$

with $u(t) = 0$ for all $t \geq N + T$. The statement then follows from (5) and by applying the superposition principle due to the linearity of (1). ■

From Theorem III.3 the sequence (6) ensures the transmission of a message to a client via private communication. Hence, we call the sequence (6) *private code*. It should be observed that condition (5b) is convenient for the implementation of a private code, as it ensures that the private transmission of a finite-length message is achieved with a finite-length transmission by the server.

Remark 2 ***(Properties of the private code*** **(6)*)*** *Consider the private code* (6) *for the transmission of the message $s : \{0, \dots, T\} \to \mathbb{F}_{\mathrm{p}}$. Let N and δ satisfy equations* (5a) *and* (5b). *Observe that:*

(i) *the message is delivered with finite delay $\delta < N$,*
(ii) *the private code has finite complexity, since the server transmits $N + T$ packets,*
(iii) *no private key or encryption mechanism is needed to ensure private communication,*
(iv) *the server is required to know the network structure, and*
(v) *clients receive private messages without the use of any decoding scheme.* □

We conclude this section with the following result on the possibility of establishing simultaneous private communications. We say that a network is *private* if private communications with all clients can be simultaneously established.

Theorem III.4 ***(Private network)*** *The network* (1) *is private if every communication channel is private, that is, if there exist $N_i \in \mathbb{N}$ and $0 < \delta_i < N$ satisfying*

$$T_{N_i} U_{N_i} = D_{i,N_i,\delta_i}, \text{ and}$$

$$L_{N_i} U_{N_i} = 0, \text{ for all } i \in \{1, \dots, q\},$$

where T_{N_i}, D_{i,N_i,δ_i}, L_{N_i} are as in (4), *and $U_{N_i} \in \mathbb{F}_{\mathrm{p}}^{mN_i}$.*

Moreover, let $u_i : \mathbb{N}_{\geq 0} \to \mathbb{F}_{\mathrm{p}}^{m}$ be the private code defined in (6) *for the private transmission of the message*

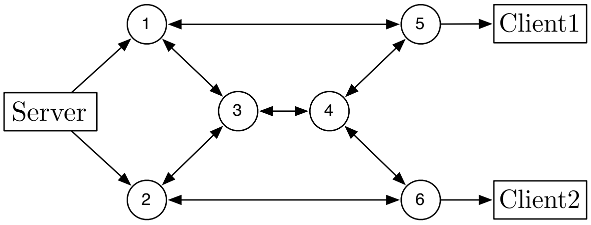


Fig. 3. Butterfly communication network with one server and two clients.

$s_i : \{0, \dots, T_i\} \to \mathbb{F}_{\mathrm{p}}$ *to the i-th client. Then, the private code* $u : \mathbb{N}_{\geq 0} \to \mathbb{F}_{\mathrm{p}}^m$,

$$u(t) = \sum_{i=1}^{q} u_i(t),$$

achieves private communication of every message s_i.

Proof: Let $y_i(u, t)$ be the sequence received by the i-th client when the server injects the sequence u. Since each sequence $u_i : \mathbb{N}_{\geq 0} \to \mathbb{F}_{\mathrm{p}}^m$ achieves private communication of the message $s_i : \{0, \dots, T_i\} \to \mathbb{F}_{\mathrm{p}}$ to the i-th client, it follows from Theorem III.3 that $y_i(u_j, t) = 0$ at all times. Due to linearity of the network (1), we have $y_i(u, t) = y_i(u_i, t)$ at all times. To conclude the proof notice that the i-th client cannot determine whether the server transmits the sequence $u = u_i$ or $u = u_i + \sum_{j \in K} u_j$, for any $K \subseteq \{1, \dots, q\} \setminus \{i\}$. Hence, the i-th client cannot decode any part of the message transmitted to the other clients. ■

From Theorem III.4, it is possible for the server to transmit private messages at network capacity. In fact, under the assumption of Theorem III.4 and after a finite delay, each client receives a private packet at each communication round (maximum communication rate). See Section IV for an illustrative example.

IV. An Illustrative Example

In this section we demonstrate the effectiveness of the private code (6) for private client-server communication. Consider the network in Fig. 3 over the field $\mathbb{F}_3$. Following our network model in Section II, the packets received by the clients are determined by the iteration

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t), \\ y_1(t) &= C_1 x(t), \\ y_2(t) &= C_2 x(t), \end{aligned}$$

where $x : \mathbb{N}_{\geq 0} \to \mathbb{F}_3^6$, $u : \mathbb{N}_{\geq 0} \to \mathbb{F}_3^2$, $y_i : \mathbb{N}_{\geq 0} \to \mathbb{F}_3$, with $i = 1, 2$, and

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 2 & 2 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 2 \\ 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix},$$

$$C_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \; C_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Notice that the server injects packets at the nodes 1 and 2, and that the two clients receive packets from the nodes 5 and 6, respectively. Let $N = 4$ and $\delta = 2$. It can be verified that

$$T_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}, \; D_{1,4,2} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

$$L_4 = \begin{bmatrix} 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \; D_{2,4,2} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

and that, with a convenient abuse of notation, the vectors

$$\begin{aligned} U_1 &= \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \end{bmatrix}^{\mathsf{T}}, \\ U_2 &= \begin{bmatrix} 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}^{\mathsf{T}}, \end{aligned}$$

satisfy

$$T_4 U_1 = D_{1,4,2}, \; T_4 U_2 = D_{2,4,2}, \; \text{ and } L_4 U_1 = L_4 U_2 = 0.$$

As discussed in Theorem III.3, there exist private codes for the first and second communication channels. In particular, let $s_1 : \{0, \dots, 18\} \to \mathbb{F}_3$ and $s_2 : \{0, \dots, 18\} \to \mathbb{F}_3$ be the messages to be transmitted to the first and second client, respectively. As in (6), define the private codes

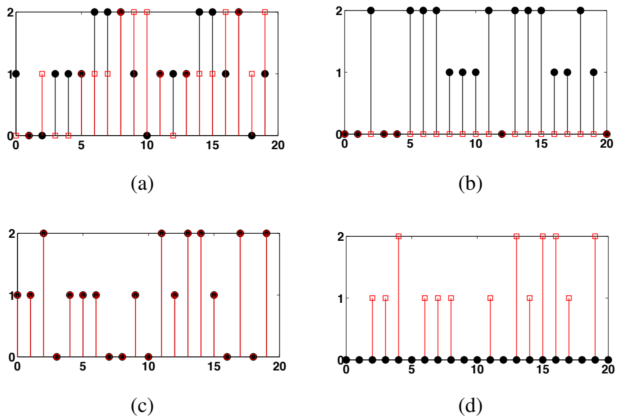
$$u_1(t) = \sum_{\tau=0}^{3} H_{\tau+1} U_1 w_1(\tau), \text{ and } u_2(t) = \sum_{\tau=0}^{3} H_{\tau+1} U_2 w_2(\tau),$$

where $w_i(t) = s_i(t)$ for $t \in \{0, \dots, 18\}$ and $w_i(t) = 0$ otherwise, with $i \in \{1, 2\}$. In Fig. 4 we show that the inputs u_1 and u_2 allow private transmission of messages s_1 and s_2. Finally, in Fig. 5 we show that the two private codes can be combined to achieve private multicasting at maximum rate.

V. Conclusion and Future Work

In this paper we propose a control-theoretic method for private network coding, where a server establishes simultaneous communications with multiple clients, while ensuring privacy of the transmitted data. Our method combines the paradigm of linear network coding with established control-theoretic techniques. We derive necessary and sufficient conditions on the communication network for the existence of private codes, and we discuss an illustrative example.

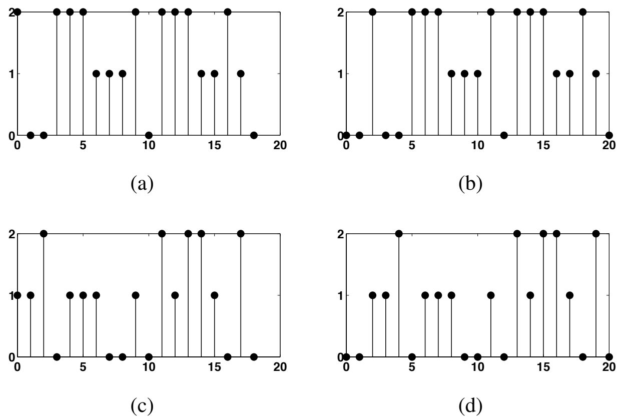
Our method assumes the server to know the structure of the communication network. The design of private codes requiring local network knowledge and capable of adapting to network changes is the subject of ongoing research.



(a) (b)

(c) (d)

Fig. 4. In this figure we show an example of private communication. In Fig. 4(a) we report the sequence of packets injected by the server. Notice that the server injects two packets at each time, represented as a black circle and a red square. In Fig. 4(b) we report the packets received by the first client (black circle) and by the second client (red square). All the packets received by the second client are identically zero, whereas the first client received the correct message. We conclude that the second client cannot reconstruct the message sent by the server to the first client, and hence the communication is private. The case in which the server establishes a private connection with the second client is reported in Fig. 4(c) and Fig. 4(d).



(a) (b)

(c) (d)

Fig. 5. In this figure we show an example of private multicasting. The network parameters are described in Section IV. In Fig. 5(a) and Fig. 5(c) we report the messages to be transmitted to the first and second client, respectively. Fig. 5(b) and Fig. 5(d) contain the messages received by the first and second client, respectively. Notice that the messages are correctly delivered to the clients with delay 2. Notice that the message received by the first client in Fig. 5(b) is the same as the message received in Fig. 4(b). We conclude that the first client cannot distinguish from whether the second clients received a nonzero message, as in Fig. 5(d), or an identically zero message, as in Fig. 4(b). As the same reasoning applies to the second client, we conclude that communication is private.

References

[1] C. Fragouli, J.-Y. Le Boudec, and J. Widmer, "Network coding: an instant primer," *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 1, pp. 63–68, 2006.

[2] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[3] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, 2003.

[4] S.-Y. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, 2003.

[5] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 789–804, 2006.

[6] D. S. Lun, M. Médard, R. Koetter, and M. Effros, "On coding for reliable communication over packet networks," *Physical Communication*, vol. 1, no. 1, pp. 3–20, 2008.

[7] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Secure network coding for wireless mesh networks: Threats, challenges, and directions," *Computer Communications*, vol. 32, no. 17, pp. 1790–1801, 2009.

[8] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 424–435, 2011.

[9] B. Elspas, "The theory of autonomous linear sequential networks," *IRE Transactions on Circuit Theory*, vol. 6, no. 1, pp. 45–60, 1959.

[10] G. Basile and G. Marro, *Controlled and Conditioned Invariants in Linear System Theory*. Prentice Hall, 1991.

[11] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[12] G. R. Blakley, "Safeguarding cryptographic keys," in *National Computer Conference*, vol. 48, 1979, pp. 313–317.

[13] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[14] N. Cai and R. W. Yeung, "Secure network coding," in *IEEE International Symposium on Information Theory*, 2002, p. 323.

[15] Z. Cao, Y. Tang, and X. Huang, "Against wiretappers without key – security is an intrinsic property of network coding," in *International Conference on Information, Communications and Signal Processing*, 2009, pp. 1–5.

[16] C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," in *IEEE Conf. on Computer Communications*, vol. 6, 2006, pp. 1–13.

[17] E. Kehdi and B. Li, "Null keys: Limiting malicious attacks via null space properties of network coding," in *IEEE Conf. on Computer Communications*, 2009, pp. 1224–1232.

[18] M. N. Krohn, M. J. Freedman, and D. Mazieres, "On-the-fly verification of rateless erasure codes for efficient content distribution," in *IEEE Symposium on Security and Privacy*, 2004, pp. 226–240.

[19] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient network coding in the presence of byzantine adversaries," in *IEEE Conf. on Computer Communications*, 2007, pp. 616–624.

[20] T. Ho, B. Leong, R. Koetter, M. Médard, M. Effros, and D. R. Karger, "Byzantine modification detection in multicast networks with random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2798–2803, 2008.

[21] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[22] D. Dolev, "The Byzantine generals strike again," *Journal of Algorithms*, vol. 3, pp. 14–30, 1982.

[23] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90–104, 2012.

[24] S. Sundaram and C. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Transactions on Automatic Control*, vol. 56, no. 7, pp. 1495–1508, 2011.

[25] R. W. Yeung and N. Cai, "Network error correction I: Basic concepts and upper bounds," *Communications in Information & Systems*, vol. 6, no. 1, pp. 19–35, 2006.

[26] N. Cai and R. W. Yeung, "Network error correction II: Lower bounds," *Communications in Information & Systems*, vol. 6, no. 1, pp. 37–54, 2006.

[27] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, 1996.

[28] S. Sundaram and C. Hadjicostis, "Structural controllability and observability of linear systems over finite fields with applications to multi-agent systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 1, pp. 60–73, 2013.

[29] F. Pasqualetti, D. Borra, and F. Bullo, "Consensus networks over finite fields," *Automatica*, vol. 50, no. 2, pp. 349–358, 2014.

[30] R. A. H. Toledo, "Linear finite dynamical systems," *Communications in Algebra*, vol. 33, no. 9, pp. 2977–2989, 2005.