Anonymous and Secure Network Coding

E. Gabidulin, O. Trushina

Moscow Institute of Physics and Technology
(State University)

2013

Dedicated to the memory of
Stefan Dodunekov (1945-2012)

Content

Models of anonymity

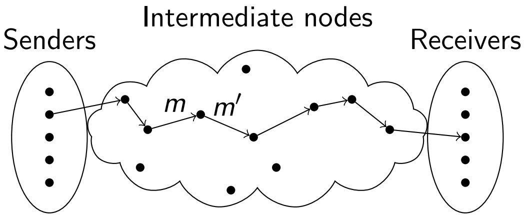
proposed by A. Pfitzmann and M. Hansen

1. *Unobservability*: impossibility to ascertain whether a communication exists
2. *Sender/receiver anonymity*: impossossobility to identify the sender/receiver of data flow
3. *Relationship anonymity*: impossibility to relate a sender and a receiver of a communication

Our interest is relationship anonymity.

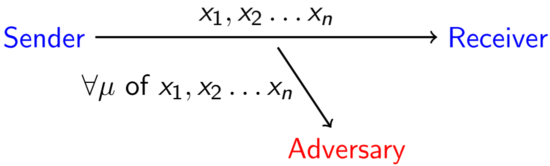
Anonymous communication task

Anonymous transmission: to guarantee a forwarding to be untraceable



Adversary: Are m and m' the same?
Can I reveal the previous and next path nodes of m'?

Coset coding overview



$$S = HX$$

source symbols $S = (s_1, s_2 \dots s_k)$ - syndrome

$(x_1, x_2 \dots x_n) = X \in$ corresponding coset

S is secret under μ observations, $k \leq n - \mu$

Model

Network

- error free links
- multiple sources and multiple receivers
- packet $x \in \mathbb{F}_{q^m}$
- message $X = (x_1, x_2, \ldots x_n) \in \mathbb{F}_{q^m}^n$
- coherent network coding: transmiting the linear combinations of packets, fixed coefficients.

Adversary

- passive, wiretapping not more than μ packets of earch source
- traffic analysis abilities

Silva-Kschischang scheme

$C - [n, n-k]$ maximun-rank-distance (MRD) code,
parity check matrix $H \in \mathbb{F}_{q^m}^{k \times n}, m \geq n$

$\phi : \mathbb{F}_{q^m}^{k} \to \mathbb{F}_{q^m}^{n}$

$\phi(S) = X = T \begin{pmatrix} S \\ V \end{pmatrix}$, random $V \in \mathbb{F}_{q^m}^{n-k}$

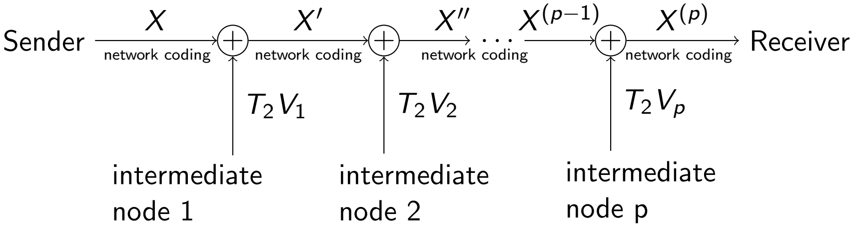
$T^{-1} = \begin{pmatrix} H \\ L \end{pmatrix}$, T is nonsingular, $T \in \mathbb{F}_{q^m}^{n \times n}$, $L \in \mathbb{F}_{q^m}^{(n-k) \times n}$

perfect secrecy:
$I(S; Z) = 0$, adversary observation $Z \subset X$, $Z \in \mathbb{F}_{q^m}^{\mu}$, $\mu \leq n - k$

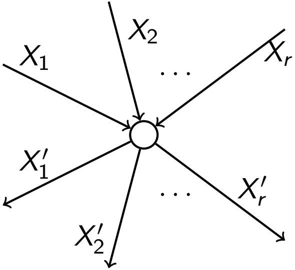
Anonymous and secure network coding scheme

$T = \begin{pmatrix} T_1 & T_2 \end{pmatrix}$,
T_1 - sender and receiver secret,
T_2 - public

$$X = \begin{pmatrix} T_1 & T_2 \end{pmatrix} \begin{pmatrix} S \\ V \end{pmatrix} = T_1 S + T_2 V \quad \Longrightarrow \quad X_{out} = X_{in} + T_2 V_{rand}$$



Anonymous and secure network coding scheme



uniform distribution

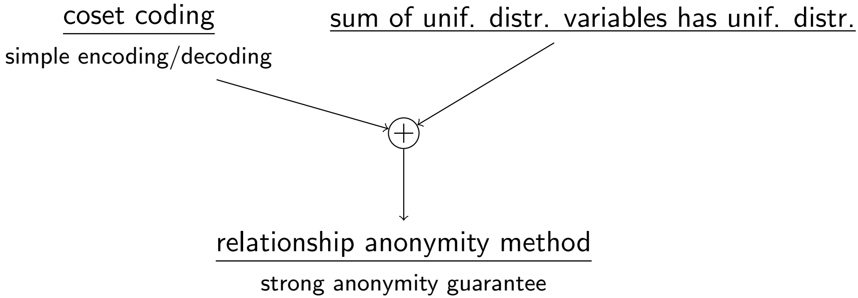
$$X' = X + T_2 V_{rand}$$

uniform distribution

perfect anonymity:
$I(X_i; X'_j) = 0,\ i, j = 1, 2, \ldots r$

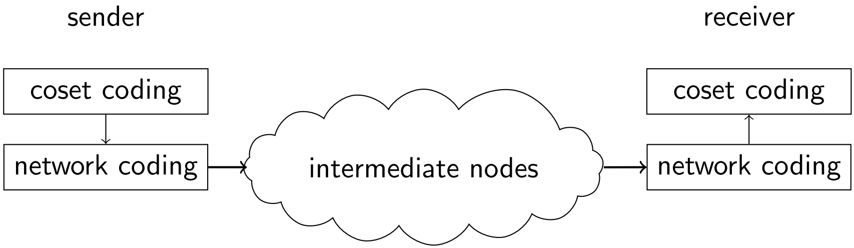
perfect secrecy under μ observations:
$I(S_i; Z_i) = 0,\ i = 1, 2, \ldots r$

Summary


coset coding
simple encoding/decoding
sum of unif. distr. variables has unif. distr.
relationship anonymity method
strong anonymity guarantee

Q&A

Communication process



Decoding process

Sender: $T^{-1} = \begin{pmatrix} H \\ L \end{pmatrix}$ for some L

$$T^{-1}T = \begin{pmatrix} H \\ L \end{pmatrix} \begin{pmatrix} T_1 & T_2 \end{pmatrix} = \begin{pmatrix} I_k & 0 \\ 0 & I_{n-k} \end{pmatrix} \Rightarrow HT_1 = I_k,\ HT_2 = 0$$

$$\xrightarrow{X^{(p)}} \text{Receiver}$$

$$X^{(p)} = \begin{pmatrix} T_1 & T_2 \end{pmatrix} \begin{pmatrix} S \\ V_1 + V_2 + \ldots + V_p \end{pmatrix}$$

Receiver: $\tilde{T}^{-1} = \begin{pmatrix} H \\ \tilde{L} \end{pmatrix}$ for some $\tilde{L}$

$$\tilde{T}^{-1}X^{(p)} = \begin{pmatrix} I_k & 0 \\ \tilde{L}T_1 & \tilde{L}T_2 \end{pmatrix} \begin{pmatrix} S \\ V_1 + V_2 + \ldots + V_p \end{pmatrix} \Rightarrow S$$

MRD code contribution

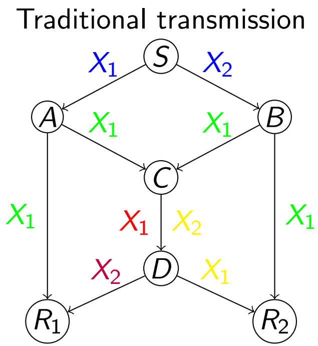
$S = HX$
adversary observation $Z \subset X,\ Z = WX$

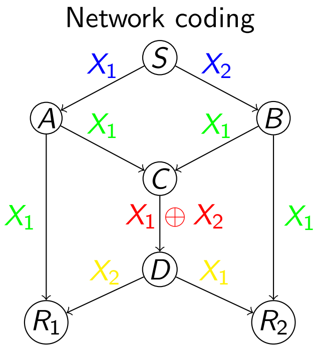
S and Z are linearly independent $\Longleftrightarrow$
$\mathrm{Rk}\begin{pmatrix} H \\ W \end{pmatrix} = \mathrm{Rk}H + \mathrm{Rk}W \Longleftrightarrow \langle H \rangle \cap \langle W \rangle = 0$

C $-[n, n-k]$ linear code, $H \in \mathbb{F}_{q^m}^{k \times n}$. If C is MRD code, $\mu \leq n-k$, then

$$\mathrm{Rk}\begin{pmatrix} H \\ W \end{pmatrix} = \mathrm{Rk}H + \mathrm{Rk}W, \text{ for all } W \in \mathbb{F}_q^{\mu \times n}$$

Network coding





State of Art

Method	Description	Overhead
Proposed method	overhead $O(n^2)$ per message, total relay node overhead $O(tn^2)$, t - number of flows, n - size of message	increase ↓
ALNCode	obfuscating the messages, constructing intersection of basis of incoming coding vectors, overhead $O(tn^3)$	
Homomorphic encryption based method	exponentiations and multiplications on each relay node, overhead $O(n^3)$ per message	
Adapting Onion Routing	encryption/decryption on each relay node + additional key sharing + additional decryption	