# Anoymous Network Coding Against Active Adversary

Oksana Trushina

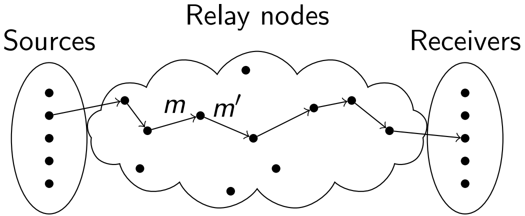
Moscow Institute of Physics and Technology

2016

# Outlines

# Anonymous Transmission

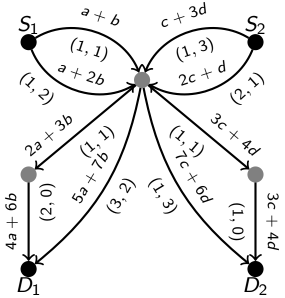
To guarantee a message forwarding to be untraceable




Are $m$ and $m'$ transfer the same information message?
Is it possible to reveal the previous and next nodes of a message $m'$?

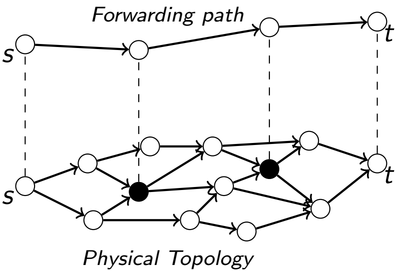
# Network Model

Coherent network coding




Received message $\mathcal{Y} = A\mathcal{X}$,
$\mathcal{X} \in \mathbb{F}_{q^m}^n$ – sent message,
$\mathcal{X} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \end{pmatrix}^T$, $x_i \in \mathbb{F}_{q^m}$
rank$A = n$, $A$ – known transfer matrix over $\mathbb{F}_q$

Overlay network




Every relay node can decode a message from previous one

# Adversary Model

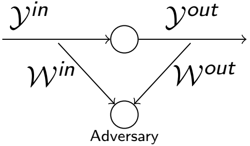
External active adversary

- injects up to $t$ malicious packets: $\mathcal{Y} = A\mathcal{X} + D\mathcal{Z},\ \mathcal{Z} \in \mathbb{F}_{q^m}^t$ – malicious packets, $D$ – transfer matrix of malicious packets
- eavesdrops up to $\mu$ packets: $\mathcal{W} = E\mathcal{Y},\ \text{rank}E = \mu, E$ defines which coordinates of $\mathcal{Y}$ are eavesdropped by an adversary

Active adversary harming = passive adversary harming + erroneous transmission

# Anonymous Scheme Requirements

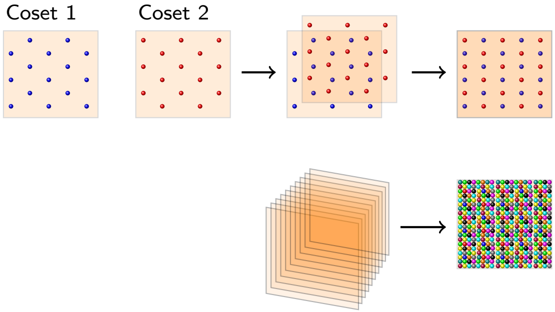
1. Security condition. $\mathcal{S} \in \mathbb{F}_{q^m}^k \to \mathcal{X} \in \mathbb{F}_{q^m}^n : \; I(\mathcal{S}; \mathcal{W}) = 0$, necessary to prevent traceability.
2. Reliability condition. $\mathcal{Y} = A\mathcal{X} + D\mathcal{Z}$ must satisfy $H(\mathcal{S}|\mathcal{Y}) = 0 \; \forall A \; \mathrm{rank} A = n, \; \forall D, \mathcal{Z}$.
3. Anonymous condition.




$I(\mathcal{W}^{in}; \mathcal{W}^{out}) = 0$ which leads to $I(\mathcal{Y}^{in}; \mathcal{Y}^{out}) = 0$

# Coset Coding. Error Free Case

$(n, n-k)$ code $C$
$\sigma : \mathcal{M} \to \{C + v\}$
$\mathbf{x} = \sigma(\mathbf{m})$
$\mathbf{x}$ – concatenation of secret message $\mathbf{s}$ and random bits, $\mathbf{s}$ labeles a coset, random bits decide a random point inside the coset




adversary information $\mathbf{z} = \mu$ coordinates of $\mathbf{x}$

$$H(\mathbf{s}|\mathbf{z}) = \begin{cases} n-\mu, & n-d+1 \le \mu \le n, d - C \text{ minimal distance} \\ k, & 0 \le \mu \le d'-1, d' - C^{\perp} \text{ minimal distance} \end{cases}$$

if $C$ is MDS code, then $k$ bits may be transmitted in secret under $\mu \le n-k$ observations

# Coset Coding. Noisy Coding

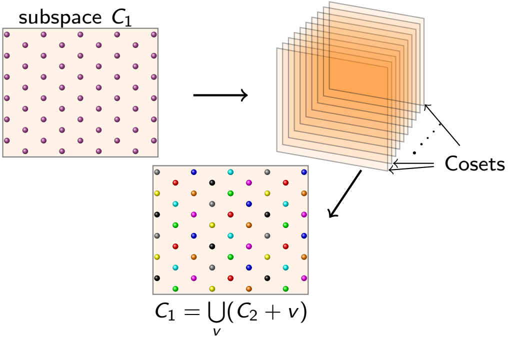
$C_2 \subset C_1$
$\{(n, k_1),\ (n, k_2)\},\ k_1 > k_2$

$\sigma : \mathcal{M} \to \{C_2 + v\}$

$H_2 = \begin{pmatrix} H_1 \\ \Delta H \end{pmatrix}$

$s_1 = H_1 x$
$s_2 = H_2 x$
$\Delta s = \Delta H x$ relative syndrome

$s_2 = \begin{pmatrix} s_1 \\ \Delta s \end{pmatrix}$




if $x \in C_1$ then $s_2 = \begin{pmatrix} 0 \\ \Delta s \end{pmatrix}$ $C_1$ may be filled in $2^{k_1 - k_2}$ cosets of $C_2$
by varying $\Delta s$ given $s_1 \equiv 0$

# Explicit Error Correcting Coset Coding Scheme

## Silva-Kschischang Scheme

$\mathcal{S} \in \mathbb{F}_{q^m}^k$, $\mathcal{V} \in \mathbb{F}_{q^m}^\mu$ is uniform and independent of $\mathcal{S}$

$$\mathcal{U} = \begin{pmatrix} \mathcal{S} \\ \mathcal{V} \end{pmatrix}$$

$$\mathcal{X} = G_1^T \mathcal{U}, \; G_1 - \text{generator matrix of } (n, k+\mu) \; MRD \text{ code}$$

Error Correcting

up to $t$ errors may be corrected if $d_R \geq 2t + 1$

Security

$T \in \mathbb{F}_{q^m}^{n \times n}$, $T$ – invertible matrix, $T^T = \begin{pmatrix} \Delta G \\ G_1 \end{pmatrix}$

$I(\mathcal{S}; \mathcal{W}) = 0$ if $T^T = \begin{pmatrix} \Delta G \\ \Delta G_1 \\ G_2 \end{pmatrix}$, $G_2$ – matrix of $(n, \mu)$ MRD code

$$\mathcal{X} = G_1^T \mathcal{U} = T \begin{pmatrix} 0 \\ \mathcal{U} \end{pmatrix} = T \begin{pmatrix} \mathcal{S}' \\ \mathcal{V} \end{pmatrix} = (\Delta G^T \; \Delta G_1^T \; G_2^T) \begin{pmatrix} \mathcal{S}' \\ \mathcal{V} \end{pmatrix}$$

$$= (\Delta G^T \; \Delta G_1^T) \begin{pmatrix} 0 \\ \mathcal{S} \end{pmatrix} + G_2^T \mathcal{V}$$

# Anonymous Scheme

Consider

$$\mathcal{X}^{out} = \mathcal{X}^{in} + G_2^T\mathcal{V}' = \begin{pmatrix}\Delta G^T & \Delta G_1^T\end{pmatrix}\begin{pmatrix}0\\ \mathcal{S}\end{pmatrix} + G_2^T(\mathcal{V}+\mathcal{V}'),$$

where $\mathcal{V}'$ is uniform over $\mathbb{F}_{q^m}^{\mu}$ and independent of $\mathcal{X}^{in}$.

$\mathcal{X}^{out}$ belongs to the same coset as $\mathcal{X}^{in}$ $\Rightarrow$ transmits the same infromation

## Lemma

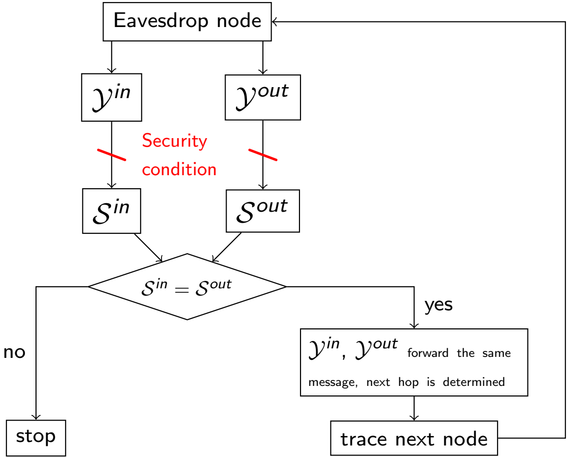
*Let $x$ and $y$ be two independent statistical variables from finite field. If $x$ is uniformly distributed over the field, then $z = x + y$ is uniformly distributed as well and independent of $y$.*

Then $\mathcal{X}^{out}$ is uniform over $\mathbb{F}_{q^m}^{\mu}$ and independent of $\mathcal{X}^{in}$.

$$\begin{aligned}\mathcal{Y}^{in} &= A_{in}\mathcal{X}^{in} + D_{in}\mathcal{Z}^{in}\\ \mathcal{Y}^{out} &= A_{in-out}(A_{in}(\mathcal{X}^{in} + G_2^T\mathcal{V}') + D_{in}\mathcal{Z}^{in} + D_{out}\mathcal{Z}^{out})\\ &= A_{in-out}(\mathcal{Y}^{in} + A_{in}G_2^T\mathcal{V}' + D_{out}\mathcal{Z}^{out})\end{aligned}$$

$$I(\mathcal{Y}^{out};\mathcal{Y}^{in}) = 0$$

# Possible Attack



## Conclusion

The proposed scheme

+ is simple
+ doesn't increase decoding complexity

– has requirement to network topology

Q&A