Secrecy and Robustness for Active Attack in Secure Network Coding

Masahito Hayashi[1,2], Masaki Owari[3], Go Kato[4] and Ning Cai[5]

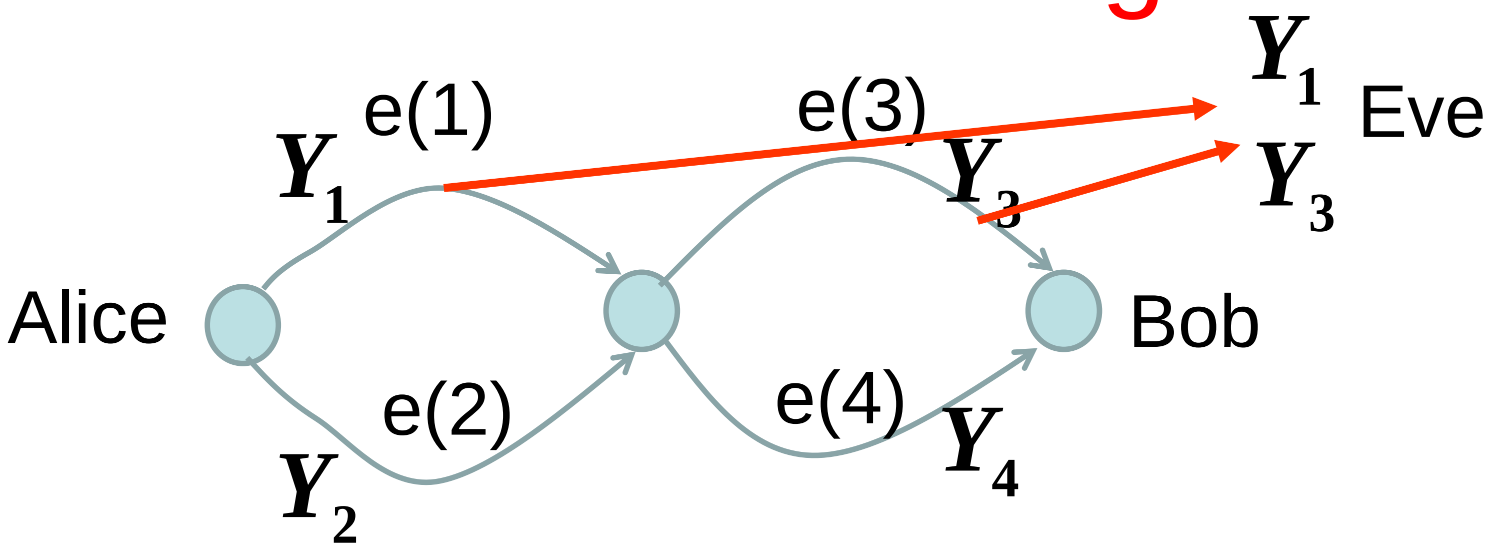
arXiv:1703.00723
Accepted for ISIT2017

1:Graduate School of Mathematics, Nagoya University
2:Centre for Quantum Technologies, National University of Singapore (NUS)
3:Faculty of Informatics, Shizuoka University
4:NTT Communication Science Laboratories, NTT Corporation
5:School of Information Science & Technology, ShanghaiTech University

Contents

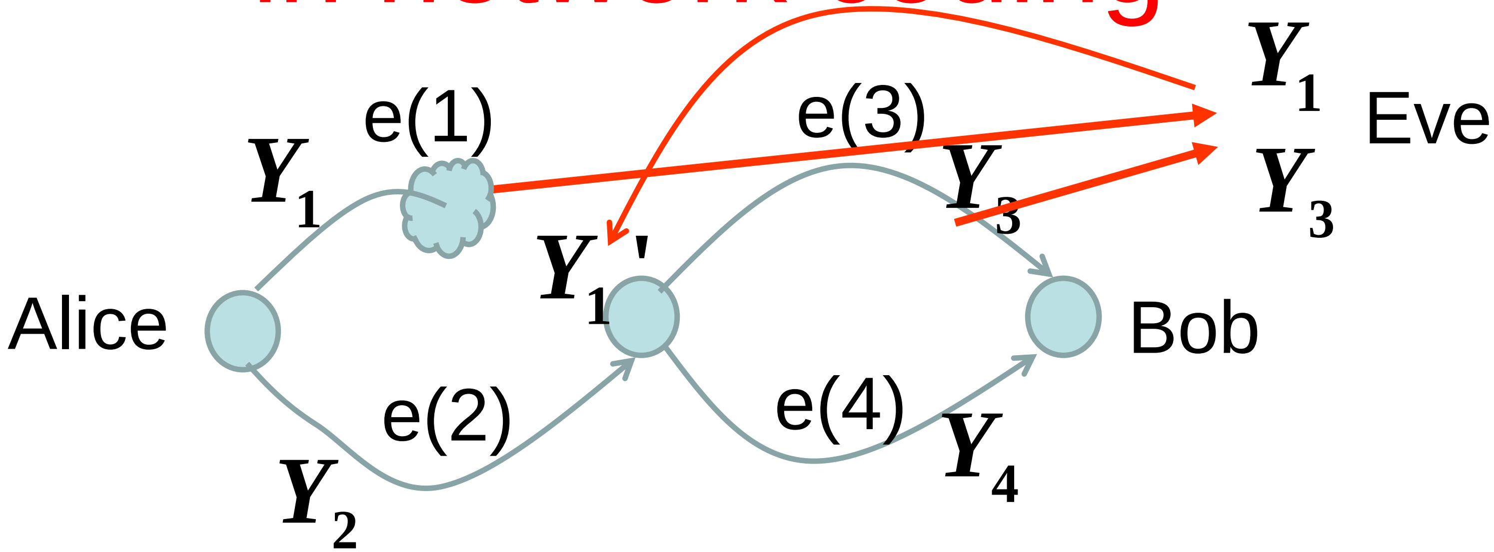
- Conventional secrecy analysis in network coding
- Two types of answers
- Non-linear example (GF(2))
- Linear codes
- Secrecy and Robustness for linear network model
- Asymptotic universal code for robustness
- Asymptotic universal code for secrecy and robustness
- Asymptotic universal code for secrecy

Conventional secrecy analysis in network coding



Eve eavesdrops the information on edges, but does not change it. (Passive attack)

Conventional secrecy analysis in network coding



Eve eavesdrops the information on edges, but does not change it. (Passive attack)

Can Eve obtain more information if Eve changes the information on edges (Active attack)?

⇨ Answer depends on type of codes!

Two types of answers

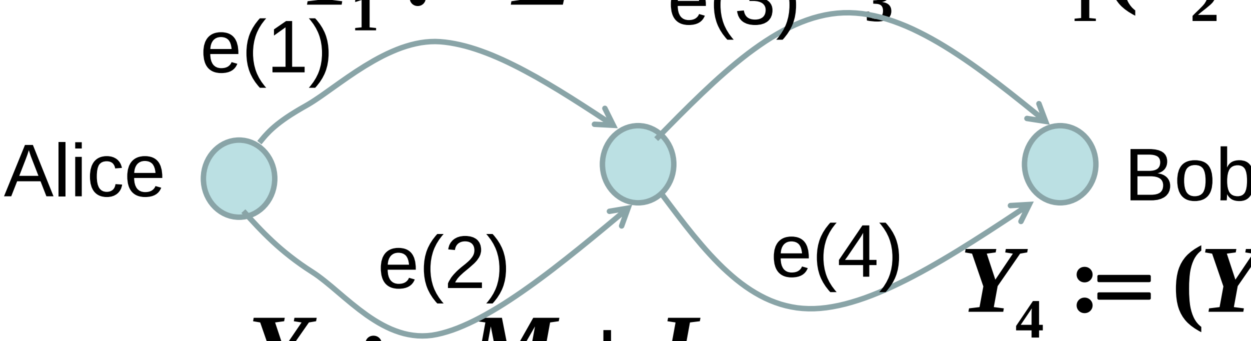
(1)In the linear code case,
Eve cannot improve her performance.

(2) In the non-linear code case,
Eve can improve her performance.

Non-linear example (GF(2))

$$Y_1 := L$$

$$Y_3 := Y_1(Y_2 + Y_1) = ML$$



$$Y_4 := (Y_1 + 1)(Y_2 + Y_1)$$
$$= ML + M$$

$$Y_2 := M + L$$

M : Message

L : Scramble variable

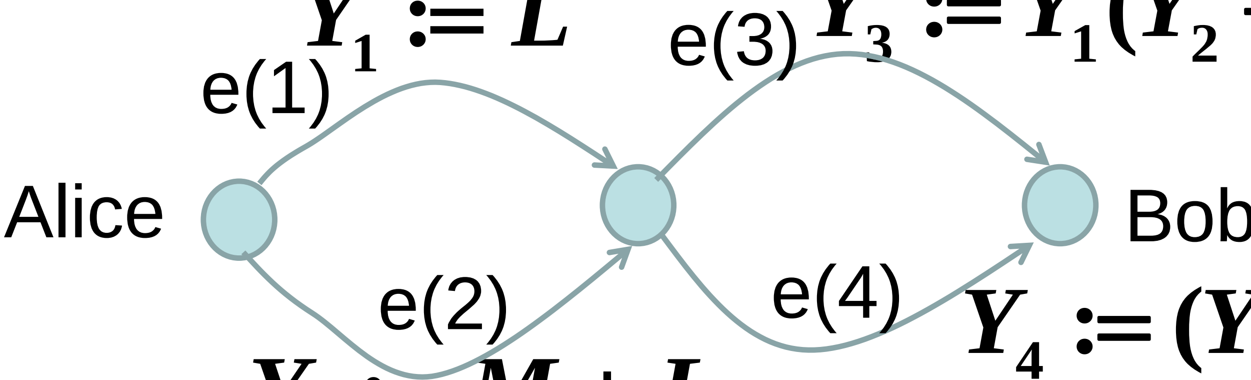
When Eve eavesdrops two edges except for {e(1),e(2)}, {e(3),e(4)} without modification,
Eve cannot recover the message M, *i.e.*,

$$I(M;Y_1,Y_3) = I(M;Y_1,Y_4)$$
$$= I(M;Y_2,Y_3) = I(M;Y_2,Y_4) = 1/2$$

Non-linear example (GF(2))

$Y_1 := L$

$Y_3 := Y_1(Y_2 + Y_1) = ML$



$Y_4 := (Y_1 + 1)(Y_2 + Y_1)$

$Y_2 := M + L$

$= ML + M$

M : Message L : Scramble variable

When Eve eavesdrops {e(1),e(3)}, Eve replace Y_1 by 1.
Eve obtain perfect information for M because

$$Y_3 + Y_1 + 1 = M$$

When Eve eavesdrops {e(1),e(4)}, Eve replace Y_1 by 0.
Eve obtain perfect information for M because

$$Y_3 + Y_1 = M$$

In other case, Eve has no good attack.

Linear codes

When all operations in nodes are linear,
there exist matrices $\boldsymbol{K}_B, \boldsymbol{H}_B, \boldsymbol{K}_E, \boldsymbol{H}_E$ such that

Bob receives $\boldsymbol{Y}_B = \boldsymbol{K}_B \boldsymbol{X} + \boldsymbol{H}_B \boldsymbol{Z}$

Eve receives $\boldsymbol{Y}_E = \boldsymbol{K}_E \boldsymbol{X} + \boldsymbol{H}_E \boldsymbol{Z}$

adding modification

$\boldsymbol{\alpha}$ Eve's strategy (non-linear)

$\boldsymbol{X}$: Alice's input

$\boldsymbol{Z}$: Eve's input

$\boldsymbol{H}_{E;j,i} = \boldsymbol{0}$ for $\boldsymbol{i} > \boldsymbol{j}$

⇒ $\boldsymbol{K}_E \boldsymbol{X}$: Eve's output of passive attack

⇒ Eve can simulate Eve's output with active attack from Eve's output of passive attack.

⇒ Eve obtain no merit with active attack.

Secrecy and Robustness for linear network model

We are allowed to manage encoder and decoder.
Linear operations on intermediate nodes are fixed.

Φ_n : Code (pair of encoder and decoder)

Criteria:

$k[\Phi_n]$: coding length

$P_e[\Phi_n, \mathrm{K}, \mathrm{H}, \alpha]$: decoding error probability

$I[\Phi_n, \mathrm{K}, \mathrm{H}, \alpha]$: Leaked information

$$\mathrm{K} = (K_B, K_E),\ \mathrm{H} = (H_B, H_E)$$

Asymptotic universal code for robustness

Jaggi et al. (2007)

For given m_0, m_1, m_2, there exists a sequence of codes $\{\Phi_n\}_n$ such that

$$\lim_{n\to\infty} k[\Phi_n]/n = m_0 - m_1$$

$$\lim_{n\to\infty} P_e[\Phi_n, \mathrm{K}, \mathrm{H}, \alpha] = 0$$

for $\forall \alpha$

$$\mathbf{rank}\, K_B = m_0,\ \mathbf{rank}\, H_B = m_1,$$

$$\mathbf{rank}\, K_E = m_2 < m_0 - m_1$$

Calculation complexity of Φ_n is $O(n \log n)$.

Asymptotic universal code for secrecy and robustness

For given m_0, m_1, m_2, there exists a sequence of codes $\{\Phi_n\}_n$ such that

$$\lim_{n\to\infty} k[\Phi_n]/n = m_0 - m_1 - m_2$$

$$\lim_{n\to\infty} P_e[\Phi_n,\mathrm{K},\mathrm{H},\alpha]=0$$

$$\lim_{n\to\infty} I[\Phi_n,\mathrm{K},\mathrm{H},\alpha]=0$$

for $\forall \alpha$

$$\mathrm{rank}\, K_B = m_0,\ \mathrm{rank}\, H_B = m_1,\ \mathrm{rank}\, K_E = m_2$$

Calculation complexity of Φ_n is $O(n \log n)$.

Proof

Combining the left over hashing lemma with Jaggi's result, we obtain the secrecy when Eve makes no modification.

Eve has no merit for eavesdropping when she makes modification.
So, we obtain the desired statement.

Asymptotic universal code for secrecy

For given m_0, m_1, m_2, there exists a sequence of codes $\{\Phi_n\}_n$ such that

$$\lim_{n\to\infty} k[\Phi_n]/n = m_0 - m_2$$

$$P_e[\Phi_n, \mathrm{K}, \mathrm{H}, 0] = 0 \qquad \alpha = 0 \text{ (no modification)}$$

$$\lim_{n\to\infty} I[\Phi_n, \mathrm{K}, \mathrm{H}, \alpha] = 0$$

for $\forall \alpha$

$$\mathrm{rank}\, K_B = m_0, \ \mathrm{rank}\, K_E = m_2$$

Calculation complexity of Φ_n is $O(n \log n)$.

Proof

We use the initial m_0 transmission to estimate K_B.

So, $$P_e[\Phi_n, \mathrm{K}, \mathrm{H}, 0] = 0$$

Using the left over hashing lemma,
we obtain the secrecy when
Eve makes no modification.

Eve has no merit for eavesdropping
when she makes modification.
So, we obtain the desired statement.

This protocol is useful to sharing secret random number
when Alice and Bob share small size of secret random number and they can use public channel.

References

- Cai and Yeung, “Secure network coding,” *ISIT 2002*
- Jaggi et al. “Resilient network coding in the presence of byzantine adversaries,” *IEEE INFOCOM 2007*.
- Jaggi et al. “Resilient Network Coding in the Presence of Byzantine Adversaries,” *IEEE IT (2008).*
- Jaggi and Langberg, “Resilient network coding in the presence of eavesdropping byzantine adversaries,” *ISIT 2007.*