情報理論的暗号の最近の発展と未解決問題

IT研究会＠泉慶

November, 2017

渡辺 峻 (東京農工大)

joint work with Himanshu Tyagi (IISc Bangalore)
Secret Key Cryptography

Alice \[ M \] Enc. \[ C \] Dec. \[ M \] Bob

Enc.

Dec.

Eve

\[ K \]

\[ K \]
A secret key crypto system is secure only if

$$H(K) \geq H(M)$$

Key length must be as large as message length…
Wyner’s Wiretap Channel

Wyner’s Wiretap Channel

\[ W(y, z|x) = W_1(y|x)W_2(z|y) \] : Degraded Wiretap Channel [Wyner 75]

General wiretap channel [Csiszár-Körner]
Secret Key Agreement: Model

\[ \text{[Maurer 93, Ahlswede-Csiszár 93]} \]

- Alice
- Bob
- Eve
- \( X \)
- \( Y \)
- \( Z \)
Secret Key Agreement: Protocol

[Maurer 93, Ahlswede-Csiszár 93]

Interactive Public Communication

\[ \Pi = (\Pi_1, \ldots, \Pi_r) \]

\[ \Pi_1 = \Pi_1(X) \]
\[ \Pi_2 = \Pi_2(Y, \Pi_1) \]
\[ \vdots \]
\[ \Pi_r = \Pi_r(Y, \Pi_1, \ldots, \Pi_{r-1}) \]
Secret Key Agreement: Protocol

\[ \Pi = (\Pi_1, \ldots, \Pi_r) \]

\[ K_1 = K_1(X, \Pi) \]

\[ K_2 = K_2(Y, \Pi) \]
Example 1: Maurer’s Satellite Model
Example 2: Fading of Wireless Communication

\[ X = \alpha H + N_1 \]
\[ Y = \alpha H + N_2 \]
\[ Z' = \alpha H' + N_3 \]
\[ Z'' = \alpha H'' + N_4 \]

[Hassan et. al. ’96]
Example 3: Fuzzy Extractor (Biometric Security)

[Dodis et. al. 04]
The generate key is $(\varepsilon, \delta)$-SK ($0 \leq \varepsilon, \delta < 1$) if there exists $K$ such that

**Reliability** \[ \Pr\{K_1 = K_2 = K\} \geq 1 - \varepsilon \]

**Security** \[ d(P_{K^{\Pi Z}}, P_{\text{unif} \times P^{\Pi Z}}) \leq \delta \]

\[
d(P, Q) := \frac{1}{2} \sum_a |P(a) - Q(a)| \quad P^{\Pi Z} : \text{marginal of } P_{K^{\Pi Z}}
\]

\[
P_{\text{unif}}(k) = \frac{1}{|\mathcal{K}|}
\]
Problem Formulation of SK

The generate key is $(\varepsilon, \delta)$-SK \((0 \leq \varepsilon, \delta < 1)\) if there exists \(K\) such that

Reliability \[ \Pr\{K_1 = K_2 = K\} \geq 1 - \varepsilon \]

Security \[ d(P_{K\Pi Z}, P_{\text{unif}} \times P_{\Pi Z}) \leq \delta \]

\[ d(P, Q) := \frac{1}{2} \sum_a |P(a) - Q(a)| \quad \quad P_{\Pi Z} : \text{marginal of } P_{K\Pi Z} \]

\[ P_{\text{unif}}(k) = \frac{1}{|\mathcal{K}|} \]

\[ S_{\varepsilon, \delta}(X, Y | Z) : \text{maximum } \log |\mathcal{K}| \text{ such that a protocol generating } (\varepsilon, \delta)\text{-SK exists} \]
For i.i.d. observations \( \{(X^n, Y^n, Z^n)\}_{n=1}^\infty \),

\[
C(X, Y|Z) := \lim_{\varepsilon, \delta \to 0} \lim inf_{n \to \infty} \frac{1}{n} S_{\varepsilon, \delta}(X^n, Y^n|Z^n)
\]
For i.i.d. observations \( \{(X^n, Y^n, Z^n)\}_{n=1}^{\infty} \),

\[
C(X, Y|Z) := \lim_{\varepsilon, \delta \to 0} \liminf_{n \to \infty} \frac{1}{n} S_{\varepsilon, \delta}(X^n, Y^n|Z^n)
\]

Basic lower (achievability) bound:

\[
C(X, Y|Z) \geq H(X|Z) - H(X|Y)
\]

Basic upper (converse) bound:

\[
C(X, Y|Z) \leq I(X \land Y|Z)
\]
Secret Key Capacity

For i.i.d. observations \( \{(X^n, Y^n, Z^n)\}_{n=1}^\infty \),

\[
C(X, Y|Z) := \lim_{\varepsilon, \delta \to 0} \liminf_{n \to \infty} \frac{1}{n} S_{\varepsilon, \delta}(X^n, Y^n|Z^n)
\]

Basic lower (achievability) bound:

\[
C(X, Y|Z) \geq H(X|Z) - H(X|Y)
\]

Basic upper (converse) bound:

\[
C(X, Y|Z) \leq I(X \land Y|Z)
\]

Theorem [Maurer 93, Ahlswede-Csiszár 93]

When \( X \rightarrow Y \rightarrow Z \) holds,

\[
C(X, Y|Z) = I(X \land Y|Z)
\]

In particular,

\[
C(X, Y) = I(X \land Y)
\]
Idea of achievability

• Information reconciliation
  share a common random variable

• Privacy amplification
  extract a secret key
Use Slepian-Wolf coding:

If \( R > H(X|Y) \), there exists a code such that \( \Pr\{X^n \neq \hat{X}^n\} \rightarrow 0 \)
Alice and Bob shall generate secret key from $X$ when $Z$ is known to Eve.

**Definition** (2-Universal hash family)

A random function $F : \mathcal{X} \rightarrow \{0, 1\}^l$ is called 2-UHF if

$$P(F(x) = F(x')) \leq \frac{1}{2^l}, \quad \forall x \neq x' \in \mathcal{X}$$

eg)

- the set of all functions from $\mathcal{X}$ to $\{0, 1\}^l$
- the set of all linear functions from $\mathcal{X}$ to $\{0, 1\}^l$
Privacy Amplification

**Definition (Conditional min-entropy)**

For $P_{XZ}$ and $Q_Z$, the conditional min-entropy of $P_{XZ}$ given $Q_Z$ is

$$H_{\min}(P_{XZ}|Q_Z) := \min_{x \in \mathcal{X}, z \in \text{supp}(Q_Z)} \log \frac{Q_Z(z)}{P_{XZ}(x, z)}$$

Then, the conditional min-entropy of $P_{XZ}$ given $Z$ is

$$H_{\min}(P_{XZ}|Z) := \max_{Q_Z} H_{\min}(P_{XZ}|Q_Z)$$
**Privacy Amplification**

**Definition (Conditional min-entropy)**

For \( P_{XZ} \) and \( Q_Z \), the conditional min-entropy of \( P_{XZ} \) given \( Q_Z \) is

\[
H_{\min}(P_{XZ}|Q_Z) := \min_{x \in \mathcal{X}, z \in \text{supp}(Q_Z)} \log \frac{Q_Z(z)}{P_{XZ}(x, z)}
\]

Then, the conditional min-entropy of \( P_{XZ} \) given \( Z \) is

\[
H_{\min}(P_{XZ}|Z) := \max_{Q_Z} H_{\min}(P_{XZ}|Q_Z)
\]

The closed form (-log of success guessing probability):

\[
H_{\min}(P_{XZ}|Z) = -\log \sum_z P_Z(z) \max_x P_{X|Z}(x|z)
\]

\[
Q^*_Z(z) \propto P_Z(z) \max_x P_{X|Z}(x|z)
\]
The following bound is useful (cf. [Impagliazzo-Levin-Luby 89, Renner 05]).

**Theorem** (Leftover Hash Lemma)

For 2-UHF $F$, $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\text{unif}} \times P_Z \times P_F) \leq \frac{1}{2} \sqrt{2^l - H_{\text{min}}(P_{XZ}|Z)}$$
Leftover Hash Lemma

The following bound is useful (cf. [Impagliazzo-Levin-Luby 89, Renner 05]).

**Theorem** (Leftover Hash Lemma)

For 2-UHF $F$, $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\text{unif}} \times P_Z \times P_F) \leq \frac{1}{2} \sqrt{2^{l-H_{\text{min}}(P_{XZ}|Z)}}$$

$\delta$-secure secret key of length

$$H_{\text{min}}(P_{XZ}|Z) - 2 \log(1/2\delta)$$

can be generated.
Leftover Hash Lemma

The following bound is useful (cf. [Impagliazzo-Levin-Luby 89, Renner 05]).

**Theorem** (Leftover Hash Lemma)

For 2-UHF $F$, $K = F(X)$ satisfies

$$d(P_{KZF}, P_{unif} \times P_{Z} \times P_{F}) \leq \frac{1}{2} \sqrt{2^{l-H_{\text{min}}(P_{XZ}|Z)}}$$

$\delta$-secure secret key of length

$$H_{\text{min}}(P_{XZ}|Z) - 2 \log(1/2\delta)$$

can be generated.

Typically, this bound is loose…; for i.i.d.,

$$\frac{1}{n} H_{\text{min}}(P_{XZ}^{n}|Z^{n}) = H_{\text{min}}(P_{XZ}|Z) < H(X|Z)$$
Smoothing:

\[ P_{XZ} \rightarrow \tilde{P}_{XZ} \]
under the condition
\[ d(\tilde{P}_{XZ}, P_{XZ}) \leq \delta \]
(allow sub-normalized distribution)

We allow sub-normalized distribution since we typically choose truncated distribution

\[ \tilde{P}_{XZ}(x, z) = P_{XZ}(x, z)1[(x, z) \in \mathcal{T}] \]

for some \( \mathcal{T} \) with

\[ P_{XZ}(\mathcal{T}) \geq 1 - 2\delta \]
Smooth Conditional Min-Entropy

**Definition** (Smooth conditional min-entropy)

For $P_{XZ}$ and $Q_Z$, the smooth conditional min-entropy of $P_{XZ}$ given $Q_Z$ is

$$H^\delta_{\min}(P_{XZ}|Q_Z) := \max_{\tilde{P}_{XZ} \in \mathcal{B}_\delta(P_{XZ})} H_{\min}(\tilde{P}_{XZ}|Q_Z)$$

$$\mathcal{B}_\delta(P_{XZ}) := \{\tilde{P}_{XZ} \in \mathcal{P}_{\text{sub}}(\mathcal{X} \times \mathcal{Z}) : d(\tilde{P}_{XZ}, P_{XZ}) \leq \delta\}$$

Then, the smooth conditional min-entropy of $P_{XZ}$ given $Z$ is

$$H^\delta_{\min}(P_{XZ}|Z) := \max_{Q_Z} H^\delta_{\min}(P_{XZ}|Q_Z)$$
Apply triangular inequality for smoothed distribution...

**Theorem** (Leftover Hash Lemma with smoothing)

For 2-UHF $F$, $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\text{unif}} \times P_Z \times P_F) \leq 2\delta + \frac{1}{2} \sqrt{2^{l-H_{\text{min}}(P_{XZ}|Z)}}$$
Leftover Hash Lemma with Smoothing

Apply triangular inequality for smoothed distribution...

**Theorem** (Leftover Hash Lemma with smoothing)

For 2-UHF $F$, $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\text{unif}} \times P_Z \times P_F) \leq 2\delta + \frac{1}{2} \sqrt{2^{-H_{\min}^{\delta}(P_{XZ}|Z)}}$$

$\delta$-secure secret key of length

$$H_{\min}^{(\delta-\eta)/2}(P_{XZ}|Z) - 2 \log(1/2\eta) - 1$$

can be generated for $0 < \eta \leq \delta$. 
Applying the triangular inequality for smoothed distribution...

**Theorem (Leftover Hash Lemma with smoothing)**

For 2-UHF $F$, $K = F(X)$ satisfies

$$d(P_{KZF}, P_{\text{unif}} \times P_Z \times P_F) \leq 2\delta + \frac{1}{2} \sqrt{2^{l-H_{\min}^\delta(P_{XZ}|Z)}}$$

$\delta$-secure secret key of length

$$H^{(\delta-\eta)/2}(P_{XZ}|Z) - 2\log(1/2\eta) - 1$$

can be generated for $0 < \eta \leq \delta$.

For i.i.d. observation,

$$\lim_{n \to \infty} \frac{1}{n} H^{(\delta-\eta)/2}(P_{XZ}^n|Z^n) = H(X|Z)$$

for $0 < \eta < \delta$. 

Leftover Hash Lemma with Smoothing
The following variant of LHL for $P_{XZV}$ is useful for later application:

**Theorem** (Leftover Hash Lemma with extra message)

For 2-UHF $F$, $K = F(X)$ satisfies

$$d(P_{KVZF}, P_{\text{unif}} \times P_{VZ} \times P_{F}) \leq 2\delta + \frac{1}{2} \sqrt{|\mathcal{V}| 2^{l-H_{\min}^\delta(P_{XZ}|Z)}}$$
The following variant of LHL for $P_{XZV}$ is useful for later application:

**Theorem** (Leftover Hash Lemma with extra message)

For 2-UHF $F$, $K = F(X)$ satisfies

$$d(P_{KVZF}, P_{\text{unif}} \times P_{VZ} \times P_{F}) \leq 2\delta + \frac{1}{2} \sqrt{|V|2^{l-H_{\text{min}}^\delta(P_{XZ}|Z)}}$$

$\delta$-secure secret key of length

$$H_{\text{min}}^{(\delta-\eta)/2}(P_{XZ}|Z) - 2 \log(1/2\delta) - 1 - \log |V|$$

for $0 < \eta \leq \varepsilon$; extra message reduces key length at most $\log |V|$.
Composition of IR and PA

When message of rate $R$ is revealed to Eve in IR

Alice and Bob can generate SK at rate

$$H(X|Z) - R$$

$$\implies H(X|Z) - H(X|Y) \text{ is attainable}$$
When message of rate $R$ is revealed to Eve in IR

Alice and Bob can generate SK at rate

$$H(X|Z) - R$$

$$\implies H(X|Z) - H(X|Y)$$ is attainable

More generally,

(Randomness unknown to Eve initially) $\implies$ (Rate revealed in IR)
Idea of Converse: a property of interactive communication

Interactive communication

Alice

$\Pi_1 = \Pi_1(X)$

Bob

$\Pi_2 = \Pi_2(Y, \Pi_1)$

$\Pi_3 = \Pi_3(X, \Pi_1, \Pi_2)$

:::
Idea of Converse: a property of interactive communication

Interactive communication

Alice

\[ \Pi_1 = \Pi_1(X) \]

Bob

\[ \Pi_2 = \Pi_2(Y, \Pi_1) \]

\[ \Pi_3 = \Pi_3(X, \Pi_1, \Pi_2) \]

\[ \vdots \]

Lemma [Maurer 93, Ahlswede-Csiszár 93]
For any protocol \( \Pi = (\Pi_1, \ldots, \Pi_r) \),

\[ I(X \land Y | Z, \Pi) \leq I(X \land Y | Z) \]

In particular,

\[ P_{XYZ} = P_{X|Z} P_{Y|Z} P_Z \implies P_{XYZ\Pi} = P_{X|Z\Pi} P_{Y|Z\Pi} P_{Z\Pi} \]
A Basic Converse Bound

By the Fano inequality argument,…

**Theorem** [Maurer 93, Ahlswede-Csiszár 93]

For every $0 \leq \varepsilon, \delta < 1$ with $\varepsilon + \delta < 1$,

$$S_{\varepsilon,\delta}(X, Y|Z) \leq \frac{I(X \land Y|Z) + h(\varepsilon) + h(\delta)}{1 - \varepsilon - \delta}$$
By the Fano inequality argument,…

**Theorem** [Maurer 93, Ahlswede-Csiszár 93]

For every $0 \leq \varepsilon, \delta < 1$ with $\varepsilon + \delta < 1$,

$$S_{\varepsilon, \delta}(X, Y|Z) \leq \frac{I(X \land Y|Z) + h(\varepsilon) + h(\delta)}{1 - \varepsilon - \delta}$$

For i.i.d. observations,

$$C(X, Y|Z) = \lim_{\varepsilon, \delta \to 0} \lim_{n \to \infty} \frac{1}{n} S_{\varepsilon, \delta}(X^n, Y^n|Z^n) \leq I(X \land Y|Z)$$

It is tight when $(X, Y, Z)$ form Markov chain (degraded):

$$I(X \land Y|Z) = H(X|Z) - H(X|Y)$$
By relating SK and hypothesis testing,…

**Theorem** [Tyagi-W. 14]
For every $0 \leq \varepsilon, \delta < 1$ and $0 < \eta < 1 - \varepsilon - \delta$, we have

$$S_{\varepsilon, \delta}(X, Y|Z) \leq -\log \beta_{\varepsilon+\delta+\eta}(P_{XYZ}, Q_{XYZ}) + 2 \log(1/\eta)$$

for any $Q_{XYZ} = Q_{X|Z}Q_{Y|Z}Q_Z$. 
Theorem [Tyagi-W. 14]

For every $0 \leq \varepsilon, \delta < 1$ and $0 < \eta < 1 - \varepsilon - \delta$, we have

$$S_{\varepsilon, \delta}(X, Y \mid Z) \leq -\log \beta_{\varepsilon+\delta+\eta}(P_{XYZ}, Q_{XYZ}) + 2 \log(1/\eta)$$

for any $Q_{XYZ} = Q_{X \mid Z}Q_{Y \mid Z}Q_{Z}$.

For i.i.d. observations,

$$C_{\varepsilon, \delta}(X, Y \mid Z) = \liminf_{n \to \infty} \frac{1}{n} S_{\varepsilon, \delta}(X^n, Y^n \mid Z^n) \leq I(X \wedge Y \mid Z)$$

strong converse can be proved.

It is also tight up to the second-order term for degraded case.
Second-Order Rate of Secret Key Agreement
The standard protocol with

- information reconciliation
- privacy amplification

achieves the secrecy capacity: \( H(X|Z) - H(X|Y) = I(X \land Y|Z) \)

The standard protocol is always optimal? Does interaction help in some case?
Second-Order Rate of Secret Key Agreement

The standard protocol with

- information reconciliation
- privacy amplification

achieves the secrecy capacity:

\[ H(X|Z) - H(X|Y) = I(X \land Y | Z) \]

The standard protocol is always optimal? Does interaction help in some case?

**Theorem** [Hayashi-Tyagi-W. 14]

For \( 0 < \varepsilon, \delta < 1 \) with \( \varepsilon + \delta < 1 \),

\[
S_{\varepsilon,\delta}(X^n, Y^n|Z^n) = nI(X \land Y | Z) - \sqrt{nVQ^{-1}(\varepsilon + \delta)} + O(\log n)
\]

where

\[
V := \text{Var} \left[ \log \left( \frac{P_{XY|Z}(X,Y|Z)}{P_X(Z|Z)P_Y(0|Z)} \right) \right]
\]

\[
Q(a) := \int_a^{\infty} \frac{1}{\sqrt{2\pi}} \exp \left( -\frac{t^2}{2} \right) dt
\]
Does Standard Protocol Work?

- information reconciliation

- privacy amplification
Does Standard Protocol Work?

- information reconciliation

\[ nH(X|Y) + \sqrt{nV_{X|Y}Q^{-1}(\varepsilon)} + O(\log n) \]

\[ V_{X|Y} = \text{Var} \left[ \log \frac{1}{P_{X|Y}(X|Y)} \right] \]

- privacy amplification
Does Standard Protocol Work?

- information reconciliation

\[ nH(X|Y) + \sqrt{nV_{X|Y} Q^{-1}(\varepsilon)} + \mathcal{O}(\log n) \]

\[ V_{X|Y} = \text{Var} \left[ \log \frac{1}{P_{X|Y}(X|Y)} \right] \]

- privacy amplification

\[ nH(X|Z) - \sqrt{nV_{X|Z} Q^{-1}(\delta)} + \mathcal{O}(\log n) \]

\[ V_{X|Z} = \text{Var} \left[ \log \frac{1}{P_{X|Z}(X|Z)} \right] \]
Does Standard Protocol Work?

- Information reconciliation

\[ nH(X|Y) + \sqrt{nV_{X|Y}Q^{-1}(\varepsilon)} + \mathcal{O}(\log n) \]

\[ V_{X|Y} = \text{Var} \left[ \log \frac{1}{P_{X|Y}(X|Y)} \right] \]

- Privacy amplification

\[ nH(X|Z) - \sqrt{nV_{X|Z}Q^{-1}(\delta)} + \mathcal{O}(\log n) \]

\[ V_{X|Z} = \text{Var} \left[ \log \frac{1}{P_{X|Z}(X|Z)} \right] \]

\[ nI(X \land Y|Z) - \sqrt{nV_{X|Y}Q^{-1}(\varepsilon)} - \sqrt{nV_{X|Z}Q^{-1}(\delta)} + \mathcal{O}(\log n) \]

The standard protocol does not achieve the optimal second-order rate.
Does Standard Protocol Work?

- information reconciliation

\[ nH(X|Y) + \sqrt{nV_{X|Y}Q^{-1}(\varepsilon)} + \mathcal{O}(\log n) \]

\[ V_{X|Y} = \text{Var} \left[ \log \frac{1}{P_{X|Y}(X|Y)} \right] \]

- privacy amplification

\[ nH(X|Z) - \sqrt{nV_{X|Z}Q^{-1}(\delta)} + \mathcal{O}(\log n) \]

\[ V_{X|Z} = \text{Var} \left[ \log \frac{1}{P_{X|Z}(X|Z)} \right] \]

\[ nI(X \land Y|Z) - \sqrt{nV_{X|Y}Q^{-1}(\varepsilon)} - \sqrt{nV_{X|Z}Q^{-1}(\delta)} + \mathcal{O}(\log n) \]

The standard protocol does not achieve the optimal second-order rate.

The optimal second-order rate is achieved by an interactive protocol.
Achievability Idea

Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])
Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are...

1. Alice should communicate at small rate if $h_{P_{X|Y}}(X|Y) = \log \frac{1}{P_{X|Y}(X|Y)}$ is small;
Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are…

- Alice should communicate at small rate if \( h_{P_{X|Y}}(X|Y) = \log \frac{1}{P_{X|Y}(X|Y)} \) is small;
- But neither party know the realization of \( h_{P_{X|Y}}(X|Y) \);
Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are…

- Alice should communicate at small rate if $h_{P_X|Y}(X|Y) = \log \frac{1}{P_X|Y(X|Y)}$ is small;
- But neither party know the realization of $h_{P_X|Y}(X|Y)$;
- Alice gradually increase rate until Bob is able to decode $X$;
Achievability Idea

Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are...

- Alice should communicate at small rate if $h_{P_{X|Y}}(X|Y) = \log \frac{1}{P_{X|Y}(X|Y)}$ is small;
- But neither party know the realization of $h_{P_{X|Y}}(X|Y)$;
- Alice gradually increase rate until Bob is able to decode $X$;
- Bob return Ack/Nack until it decode $X$. 
Use interactive Slepian-Wolf coding (cf. [Draper 04, Feder-Schulman 02, Yang-He 10])

Basic ideas are...

- Alice should communicate at small rate if \( h_{P_{X|Y}}(X|Y) = \log \frac{1}{P_{X|Y}(X|Y)} \) is small;
- But neither party know the realization of \( h_{P_{X|Y}}(X|Y) \);
- Alice gradually increase rate until Bob is able to decode \( X \);
- Bob return Ack/Nack until it decode \( X \).

The usage of interaction decreases information revealed to Eve...
Multi-Party Secret Key Agreement
Multi-Party Setting

\[ \Pi = (\Pi_1, \ldots, \Pi_r) \]

\[ X_1, \ldots, X_m \]

\[ K_1, \ldots, K_m \]

\[ A \subset \mathcal{M} := \{1, \ldots, M\} \]

\[ X_\mathcal{M} := (X_1, \ldots, X_m) \]

\[ K_\mathcal{M} := (K_1, \ldots, K_m) \]
Problem Formulation of Multi-Party SK

The generate key is \((\varepsilon, \delta)\text{-SK}\) \((0 \leq \varepsilon, \delta < 1)\) if there exists \(K\) such that

**Reliability** \[ \Pr\{K_1 = \cdots = K_m = K\} \geq 1 - \varepsilon \]

**Security** \[ d(P_{K_{\Pi Z}}, P_{\text{unif} \times P_{\Pi Z}}) \leq \delta \]

\[ S_{\varepsilon, \delta}(X_M) \text{: maximum } \log |\mathcal{K}| \text{ such that a protocol generating } (\varepsilon, \delta)\text{-SK exists} \]

\[ C(X_M) := \lim_{\varepsilon, \delta \to 0} \liminf_{n \to \infty} \frac{1}{n} S_{\varepsilon, \delta}(X_M^n) \]
2 Party Revisited

(Randomness unknown to Eve initially) — (Rate revealed in IR)
2 Party Revisited

(Randomness unknown to Eve initially) — (Rate revealed in IR)

\[ C(X_1, X_2) = I(X_1 \land X_2) \]

\[ = H(X_1) - H(X_1|X_2) \]

it is asymmetric…
2 Party Revisited

(Randomness unknown to Eve initially) — (Rate revealed in IR)

\[ C(X_1, X_2) = I(X_1 \land X_2) \]

\[ = H(X_1) - H(X_1|X_2) \]

It is asymmetric…

\[ = H(X_1, X_2) - H(X_1|X_2) - H(X_2|X_1) \]
2 Party Revisited

(Randomness unknown to Eve initially) — (Rate revealed in IR)

\[ C(X_1, X_2) = I(X_1 \land X_2) \]

\[ = H(X_1) - H(X_1|X_2) \]

it is asymmetric…

\[ = H(X_1, X_2) - H(X_1|X_2) - H(X_2|X_1) \]

\[ H(X_M) \] — communication rate needed to agree on \( X_M \)
Omniscience (Data Exchange) Problem

\[ \Pi = (\Pi_1, \ldots, \Pi_r) \]

\[ L_\epsilon(X_M) : \text{minimum sum-rate for omniscience with} \]

\[ P(X_M^{(i)} = X_M, \forall 1 \leq i \leq m) \geq 1 - \epsilon \]
Asymptotic Omniscience Rate

\[
R(P_{X_M}) = \lim_{\epsilon \to 0} \lim_{n \to \infty} \sup \frac{1}{n} L_\epsilon(X^n_M)
\]
Asymptotic Omniscience Rate

\[ R(P_{X_M}) = \lim_{\epsilon \to 0} \lim_{n \to \infty} \sup L_\epsilon \left( X^n_M \right) \]

\[ R(P_{X_M}) = \min \left\{ \sum_{i=1}^{m} R_i : \sum_{i \in B} R_i \geq H(X_B | X_{B^c}), \ \forall B \subseteq M \right\} \]

[Csiszár-Narayan 04]

Achieved by Slepian-Wolf coding; interaction not needed.
Asymptotic Omniscience Rate

\[ R(P_{X_M}) = \lim_{\epsilon \to 0} \limsup_{n \to \infty} \frac{1}{n} L_\epsilon(X^n_M) \]

\[ R(P_{X_M}) = \min \left\{ \sum_{i=1}^{m} R_i : \sum_{i \in B} R_i \geq H(X_B|X_{B^c}), \quad \forall B \subsetneq M \right\} \]

\[ \geq \max_{\sigma \in \Sigma(M)} \mathbb{H}_\sigma(M|P_{X_M}) \]

[Csizsár-Narayan 04]

Achieved by Slepian-Wolf coding; interaction not needed.

\[ \mathbb{H}_\sigma(M|P_{X_M}) := \frac{1}{|\sigma|-1} \sum_{i=1}^{\sigma} H(X_M|X_{\sigma_i}) \quad \sigma : \text{partition of } M \]

[Chan 08]
Asymptotic Omniscience Rate

\[
R(P_{X,M}) = \lim_{\epsilon \to 0} \limsup_{n \to \infty} \frac{1}{n} L_\epsilon(X^n_M)
\]

\[
R(P_{X,M}) = \min \left\{ \sum_{i=1}^m R_i : \sum_{i \in B} R_i \geq H(X_B|X_{B^c}), \quad \forall B \subsetneq M \right\}
\]

\[
\geq \max_{\sigma \in \Sigma(M)} H_{\sigma}(M|P_{X,M})
\]

Achieved by Slepian-Wolf coding; interaction not needed.

\[
H_{\sigma}(M|P_{X,M}) := \frac{1}{|\sigma| - 1} \sum_{i=1}^{|\sigma|} H(X_M|X_{\sigma_i})
\]

\[
m = 2 \quad \Sigma(M) = \{\{1|2\}\}
\]

\[
R(P_{X,M}) = H(X_1|X_2) + H(X_2|X_1)
\]

[Csizsár-Narayan 04]

[Chan 08]
Asymptotic Omniscience Rate

\[ R(P_{X_M}) = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \sup n^{-1} L_\varepsilon(X^n_M) \]

\[ R(P_{X_M}) = \min \left\{ \sum_{i=1}^{m} R_i : \sum_{i \in B} R_i \geq H(X_B|X_{B^c}), \quad \forall B \subsetneq M \right\} \]

\[ \geq \max_{\sigma \in \Sigma(M)} \mathbb{H}_\sigma(M|P_{X_M}) \]

Achieved by Slepian-Wolf coding; interaction not needed.

\[ \mathbb{H}_\sigma(M|P_{X_M}) := \frac{1}{|\sigma| - 1} \sum_{i=1}^{|\sigma|} H(X_M|X_{\sigma_i}) \quad \sigma : \text{partition of } M \]

\[ m = 3 \quad \Sigma(M) = \{\{1|23\}, \{12|3\}, \{23|1\}, \{12|3\}\} \]

\[ R(P_{X_M}) = \max \left\{ H(X_1|X_2, X_3) + H(X_2, X_3|X_1), H(X_3|X_1, X_2) + H(X_1, X_2|X_3), \right. \]

\[ H(X_2|X_1, X_3) + H(X_1, X_3|X_2), \quad \frac{H(X_2, X_3|X_1) + H(X_1, X_3|X_2) + H(X_1, X_2|X_3)}{2} \]
Multi-Party Secrecy Capacity

Theorem [Csiszár-Narayan 04]

\[ C(X_M) = H(X_M) - R(P_{X_M}) \]
Multi-Party Secrecy Capacity

**Theorem** [Csiszár-Narayan 04, Chan 08]

\[
C(X_M) = H(X_M) - R(P_{X_M}) = \min_{\sigma \in \Sigma(M)} \frac{1}{|\sigma| - 1} D \left( P_{X_M} \left\| \prod_{i=1}^{\left| \sigma \right|} P_{X_{\sigma_i}} \right\| \right)
\]
Multi-Party Secrecy Capacity

Theorem [Csiszár-Narayan 04, Chan 08]

\[
C(X_M) = H(X_M) - R(P_{X_M})
\]

\[
= \min_{\sigma \in \Sigma(M)} \frac{1}{|\sigma| - 1} D\left( P_{X_M} \parallel \prod_{i=1}^{|\sigma|} P_{X_{\sigma_i}} \right)
\]

A single-shot converse can be proved via hypothesis testing [Tyagi-W. 14]
Universal Protocol
We shall construct a SK/Data exchange protocol that does not rely on knowledge of $P_{X_M}$.

It suffices to construct a universal data exchange protocol.
We shall construct a SK/Data exchange protocol that does not rely on knowledge of $P_{X,M}$.

It suffices to construct a universal data exchange protocol.

In fact, it works for a given individual sequence…

**Theorem** [Tyagi-W. 16]

There exists a universal data exchange protocol such that, for a given $X_M$, it communicates

$$nR^*(P_{X_M}) + O(\sqrt{n})$$

where $P_{X_M}$ is the joint type.

The universal protocol is called recursive data exchange (RDE) protocol.
Two-step coding for single-terminal source coding:

1. Send the type $\mathcal{O}(\log n)$
2. Send the index among the type class $nH(P_x) + \mathcal{O}(\log n)$
Universal RDE Protocol

Two-step coding for single-terminal source coding:

1. Send the type $\mathcal{O}(\log n)$
2. Send the index among the type class $nH(P_x) + \mathcal{O}(\log n)$

In the data exchange problem, observations are distributed over the parties…
Universal RDE Protocol

Two-step coding for single-terminal source coding:

1. Send the type $\mathcal{O}(\log n)$
2. Send the index among the type class $nH(P_x) + \mathcal{O}(\log n)$

In the data exchange problem, observations are distributed over the parties...

Use interactive Slepian-Wolf coding [Draper 04, Yang-He 10]

- The encoder gradually increment rate until the decoder recovers $x$
- The decoder return Ack/Nack until it recovers $x$
Universal RDE Protocol

Two-step coding for single-terminal source coding:

1) Send the type $O(\log n)$
2) Send the index among the type class $nH(P_x) + O(\log n)$

In the data exchange problem, observations are distributed over the parties...

Use interactive Slepian-Wolf coding [Draper 04, Yang-He 10]

- The encoder gradually increment rate until the decoder recovers $X$
- The decoder return Ack/Nack until it recovers $X$

The decoder looks for joint type $P_{\hat{X}Y}$ s.t. there exists a unique $\hat{X}$ satisfying

1) $P_{\hat{x}y} = P_{XY}$
2) $R_t \geq H(X|Y) + \Delta$
3) Hash values (bin indices) of $\hat{X}$ up to round $t$ are compatible.
Decoding Rule for Local Omniscience

Local omniscience region for $A \subseteq \mathcal{M}$:

$$
\mathcal{R}_{c0}^\Delta (A | X_A) = \left\{ (R_i : i \in A) : \sum_{i \in B} R_i \geq H(\overline{X}_B | \overline{X}_{A \setminus B}) + |B| \Delta, \ \forall B \subseteq A \right\}
$$
Decoding Rule for Local Omniscience

Local omniscience region for \( A \subseteq \mathcal{M} \): 

\[
\mathcal{R}_{c0}^\Delta (A|P_{\overline{X}_A}) = \left\{ (R_i : i \in A) : \sum_{i \in B} R_i \geq H(\overline{X}_B|\overline{X}_{A\setminus B}) + |B|\Delta, \forall B \subseteq A \right\}
\]

\( i \) th party looks for maximal \( i \in A \subseteq \mathcal{M} \) and \( P_{\overline{X}_A} \) s.t. there exists a unique \( \hat{X}_A \) satisfying

1) \( \hat{x}_i = x_i, \ P_{\hat{x}_A} = P_{\overline{X}_A} \)

2) \( (R^{(t)}_i : i \in A) \in \mathcal{R}_{c0}^\Delta (A|P_{\overline{X}_A}) \)

3) Hash values (bin indices) of \( \hat{X}_A \) up to round \( t \) are compatible.
Decoding Rule for Local Omniscience

Local omniscience region for $A \subseteq \mathcal{M}$:

$$
\mathcal{R}^\Delta_{co0}(A|P_{\overline{X}_A}) = \left\{ (R_i : i \in A) : \sum_{i \in B} R_i \geq H(\overline{X}_B|\overline{X}_{A\setminus B}) + |B| \Delta, \forall B \subseteq A \right\}
$$

The $i$th party looks for maximal $i \in A \subseteq \mathcal{M}$ and $P_{\overline{X}_A}$ s.t. there exists a unique $\hat{X}_A$ satisfying

1) $\hat{x}_i = x_i$, $P_{\hat{x}_A} = P_{\overline{X}_A}$

2) $(R^t_i : i \in A) \in \mathcal{R}^\Delta_{co0}(A|P_{\overline{X}_A})$

3) Hash values (bin indices) of $\hat{X}_A$ up to round $t$ are compatible.

Once accumulated rate vector enters a local omniscience region, local omniscience occur automatically. Difficulty is how to increment rates...
Two-party case:

$$H(\overline{X}_2 | \overline{X}_1)$$

$$H(\overline{X}_1 | \overline{X}_2)$$

It is asymmetric…
Rate Increment Rule

Two-party case:

\[ H(X_2|X_1) \]

\[ H(X_1|X_2) \]

\[ H(X_1|\bar{X}_2) - H(\bar{X}_2|X_1) \]
Two-party case:

\[ H(\overline{X}_2|\overline{X}_1) \]

\[ H(\overline{X}_1|\overline{X}_2) \]

\[ H(\overline{X}_1|\overline{X}_2) - H(\overline{X}_2|\overline{X}_1) = H(\overline{X}_1) - H(\overline{X}_2) \]
Two-party case:

\[
H(X_2|X_1) = H(X_1|X_2)
\]

\[
H(X_1|X_2) - H(X_2|X_1) = H(X_1) - H(X_2)
\]

W.L.G., assume \( H(X_1) \geq H(X_2) \)
Two-party case:

\[ H(X_2|X_1) - H(X_2|X_1) = H(X_1) - H(X_2) \]

W.L.G., assume \( H(X_1) \geq H(X_2) \)

Party 1: \( R_1^{(0)} = 0 \); \( R_1^{(t+1)} := R_1^{(t)} + \Delta \)
Two-party case:

\[ H(X_2 | X_1) - H(X_2 | X_1) = H(X_1) - H(X_2) \]

W.L.G., assume \( H(X_1) \geq H(X_2) \)

Party 1: \( R_1^{(0)} = 0; \ R_1^{(t+1)} := R_1^{(t)} + \Delta \)

Party 2: start communication if \( R_1^{(t)} \geq H(X_1) - H(X_2) \) ;
Two-party case:

\[ H(\overline{X}_2 | \overline{X}_1) = H(\overline{X}_1 | \overline{X}_2) \]

\[ H(\overline{X}_1 | \overline{X}_2) - H(\overline{X}_2 | \overline{X}_1) = H(\overline{X}_1) - H(\overline{X}_2) \]

W.L.G., assume \( H(\overline{X}_1) \geq H(\overline{X}_2) \)

Party 1: \( R_1^{(0)} = 0 \); \( R_1^{(t+1)} := R_1^{(t)} + \Delta \)

Party 2: start communication if \( R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_2) \); \( R_2^{(0)} = 0 \); \( R_2^{(t+1)} = R_2^{(t)} + \Delta \)
Multi-party case:

W.L.G., assume \( H(X_1) \geq H(X_2) \geq \cdots \geq H(X_m) \)
Multi-party case:

W.L.G., assume \( H(\overline{X}_1) \geq H(\overline{X}_2) \geq \cdots \geq H(\overline{X}_m) \)

Party 1: \( R_1^{(0)} = 0 \); \( R_1^{(t+1)} := R_1^{(t)} + \Delta \)
Multi-party case:

W.L.G., assume \( H(\overline{X}_1) \geq H(\overline{X}_2) \geq \cdots \geq H(\overline{X}_m) \)

Party 1: \( R_1^{(0)} = 0 ; \; R_1^{(t+1)} := R_1^{(t)} + \Delta \)

Party 2: start communication if \( R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_2) ; \; R_2^{(0)} = 0 ; \; R_2^{(t+1)} = R_2^{(t)} + \Delta \)
Multi-party case:

W.L.G., assume \( H(X_1) \geq H(X_2) \geq \cdots \geq H(X_m) \)

Party 1: \( R_1^{(0)} = 0 \); \( R_1^{(t+1)} := R_1^{(t)} + \Delta \)

Party 2: start communication if \( R_1^{(t)} \geq H(X_1) - H(X_2) \); \( R_2^{(0)} = 0 \); \( R_2^{(t+1)} = R_2^{(t)} + \Delta \)

Party 3: start communication if \( R_1^{(t)} \geq H(X_1) - H(X_3) \); \( R_3^{(0)} = 0 \); \( R_3^{(t+1)} = R_3^{(t)} + \Delta \)

\[ \vdots \]
Rate Increment Rule

Multi-party case:

W.L.G., assume \( H(\overline{X}_1) \geq H(\overline{X}_2) \geq \cdots \geq H(\overline{X}_m) \)

Party 1: \( R_1^{(0)} = 0 ; \ R_1^{(t+1)} := R_1^{(t)} + \Delta \)

Party 2: start communication if \( R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_2) \); \( R_2^{(0)} = 0 \); \( R_2^{(t+1)} = R_2^{(t)} + \Delta \)

Party 3: start communication if \( R_1^{(t)} \geq H(\overline{X}_1) - H(\overline{X}_3) \); \( R_3^{(0)} = 0 \); \( R_3^{(t+1)} = R_3^{(t)} + \Delta \)

\vdots

Rate assignment for the tipping

\[
\sum_{i \in A \setminus \{j\}} R_i^*(A) = H(\overline{X}_A | \overline{X}_j), \ j \in A
\]

Property:

\[
R_i^*(A) - R_j^*(A) = H(\overline{X}_i) - H(\overline{X}_j)
\]
Theorem (rough statement)

At some point, \((R_i^{(t)} : i \in A)\) for some \(A \subseteq \mathcal{M}\) reaches \(\mathcal{R}_{c0}^\Delta(A|P_{\overline{X}_A})\) at

\[ (R_i^*(A) : i \in A) \mod \mathcal{O}(\Delta) \]
Recursive Structure

**Theorem** *(rough statement)*

At some point, \((R_i^t : i \in A)\) for some \(A \subseteq \mathcal{M}\) reaches \( R_{c_0}^A(A|P_{\bar{X}_A}) \) at

\[
(R_i^*(A) : i \in A) \mod \mathcal{O}(\Delta)
\]

Parties in \(A\) attain *local omniscience*.

From that point, the parties in \(A\) behaves as if one large party: increment rule is

\[
R_i^{(t+1)} = R_i^{(t)} + \frac{\Delta}{|A|}, \quad i \in A \quad (R_A^{(t+1)} = R_A^{(t)} + \Delta)
\]
Recursive Structure

**Theorem (rough statement)**

At some point, \((R_i^{(t)} : i \in A)\) for some \(A \subseteq \mathcal{M}\) reaches \(\mathcal{R}^{\Delta}_{c0}(A|P_{X_A})\) at

\[(R_i^*(A) : i \in A) \text { modulo } \mathcal{O}(\Delta)\]

Parties in \(A\) attain **local omniscience**.

From that point, the parties in \(A\) behaves as if one large party: increment rule is

\[R_i^{(t+1)} = R_i^{(t)} + \frac{\Delta}{|A|}, \ i \in A \quad (R_A^{(t+1)} = R_A^{(t)} + \Delta)\]

**Theorem (rough statement)**

The protocol proceed as if \(A\) were one party from the begin with…
Recursive Structure

P1
\[X_1\]

P3
\[X_3\]

P4
\[X_4\]

P2
\[X_2\]

P5
\[X_5\]
Recursive Structure
Recursive Structure

Recursive

P1
X1

P3
X3

P4
X4

P2
X2

P5
X5

recursive
Corollary (rough statement)

The protocol recursively attain omniscience with rate

\[ R(P_{x,M}) + O(\Delta) + O\left(\frac{1}{n\Delta}\right) + O\left(\frac{\log n}{n}\right) \]

slack of rate increment

rate for Ack/Nack
proportional to rounds \( O(1/\Delta) \)
Some Open Problems
(1) Non-degraded case:

- Even the first-order capacity is not known in general.
- When interaction is not allowed, capacity is known but involves auxiliary RVs.
- What is the second-order rate when the capacity is known?
(1) Non-degraded case:

- Even the first-order capacity is not known in general.
- When interaction is not allowed, capacity is known but involves auxiliary RVs.
- What is the second-order rate when the capacity is known?

(2) Necessity of interaction to attain the optimal second-order rate

- Even for the degraded case, the standard protocol does not attain the optimal second-order rate.
- How about other non-interactive protocols? Interaction is necessary?
(1) Non-degraded case:

- Even the first-order capacity is not known in general.
- When interaction is not allowed, capacity is known but involves auxiliary RVs.
- What is the second-order rate when the capacity is known?

(2) Necessity of interaction to attain the optimal second-order rate

- Even for the degraded case, the standard protocol does not attain the optimal second-order rate.
- How about other non-interactive protocols? Interaction is necessary?

(3) Universal protocol for the case with helpers

- When only subset $\mathcal{A} \subset \mathcal{M}$ try to attain omniscience, is there universal protocol?
- Slepian-Wolf coding is known to be optimal, but the rate formula is more involved.
Thank you for listening.