A bound on secret key length via binary hypothesis testing

Himanshu Tyagi
Joint work with Shun Watanabe
Multiparty Secret Key Agreement

Party $i$ computes $K_i(X_i, F) \in \mathcal{K}$; Eavesdropper observes $F, Z$

$K_1, \ldots, K_m$ constitute an $(\epsilon, \delta)$-secret key of length $\log \mathcal{K}$ if

\[ P(K_1 = K_2 = \ldots = K_m) \geq 1 - \epsilon, \quad \text{:Recoverability} \]
\[ \frac{1}{2} \|P_{K_1^1 FZ} - P_{\text{unif}} \times P_{FZ}\|_1 \leq \delta, \quad \text{:Secrecy} \]
Alternative Definition of a Secret Key

$K_1, \ldots, K_m$ constitute an $(\epsilon, \delta)$-secret key of length $\log \mathcal{K}$ if

$$P( K_1 = K_2 = \ldots = K_m) \geq 1 - \epsilon,$$

$$\frac{1}{2} \| P_{K_1FZ} - P_{\text{unif}} \times P_{FZ} \|_1 \leq \delta$$

$K_1, \ldots, K_m$ constitute an $\epsilon$-secret key of length $\log \mathcal{K}$ if

$$\frac{1}{2} \| P_{K_1K_2\ldots K_mFZ} - P_{\text{unif},m} \times P_{FZ} \|_1 \leq \epsilon,$$

where

$$P_{\text{unif},m}(k_1, \ldots, k_m) = \frac{1}{|\mathcal{K}|} \mathbb{1}(k_1 = \ldots k_m).$$
Alternative Definition of a Secret Key

$K_1, ..., K_m$ constitute an $(\epsilon, \delta)$-secret key of length $\log K$ if

\[
P (K_1 = K_2 = ... = K_m) \geq 1 - \epsilon,
\]

\[
\frac{1}{2} \| \mathbb{P}_{K_1FZ} - \mathbb{P}_{\text{unif}} \times \mathbb{P}_{FZ} \|_1 \leq \delta
\]

$K_1, ..., K_m$ constitute an $\epsilon$-secret key of length $\log K$ if

\[
\frac{1}{2} \| \mathbb{P}_{K_1K_2...K_mFZ} - \mathbb{P}_{\text{unif},m} \times \mathbb{P}_{FZ} \|_1 \leq \epsilon,
\]

where

\[
\mathbb{P}_{\text{unif},m}(k_1, ..., k_m) = \frac{1}{|K|} \mathbb{1}(k_1 = ...k_m).
\]

Lemma

$(\epsilon, \delta)$-SK $\Rightarrow$ $(\epsilon + \delta)$-SK, and conversely, $\epsilon$-SK $\Rightarrow$ $(\epsilon, \epsilon)$-SK.
$K_1, ..., K_m$ constitute an $\epsilon$-secret key of length $\log \mathcal{K}$ if

$$\frac{1}{2} \Vert P_{K_1 K_2 ... K_m FZ} - P_{\text{unif},m} \times P_{FZ} \Vert_1 \leq \epsilon.$$ 

**Definition**

$S_\epsilon(X_1, ..., X_m \mid Z) \triangleq$ maximum length of an $\epsilon$-secret key
Upper bound for $S_\varepsilon(X_1, \ldots, X_m \mid Z)$
If $X_1$ and $X_2$ are independent conditioned on $Z$:

$$S_\epsilon(X_1, X_2|Z) \approx 0$$
If $X_1$ and $X_2$ are independent conditioned on $Z$:

$$S_\epsilon(X_1, X_2 | Z) \approx 0$$

If for some partition $\pi = \{\pi_1, \ldots, \pi_k\}$ of $\{1, \ldots, m\}$, $X_{\pi_1}, \ldots, X_{\pi_k}$ are independent conditioned on $Z$:

$$S_\epsilon(X_1, \ldots, X_m | Z) \approx 0$$
If \( X_1 \) and \( X_2 \) are independent conditioned on \( Z \):

\[
S_\epsilon(X_1, X_2|Z) \approx 0
\]

If for some partition \( \pi = \{\pi_1, \ldots, \pi_k\} \) of \( \{1, \ldots, m\} \),

\( X_{\pi_1}, \ldots, X_{\pi_k} \) are independent conditioned on \( Z \):

\[
S_\epsilon(X_1, \ldots, X_m|Z) \approx 0
\]

Bound \( S_\epsilon(X_1, \ldots, X_m|Z) \) in terms of “how far” is \( P_{X_1,\ldots,X_mZ} \)

is from a conditionally independent distribution
Consider the following binary hypothesis testing problem:

\[ H_0 : \quad X \sim P \]

vs.

\[ H_1 : \quad X \sim Q \]

Define

\[ \beta_\epsilon(P, Q) \triangleq \inf \sum_{x \in \mathcal{X}} Q(x)T(0|x), \]

where the \( \inf \) is over all random tests \( T : \mathcal{X} \rightarrow \{0, 1\} \) s.t.

\[ \sum_{x \in \mathcal{X}} P(x)T(1|x) \leq \epsilon. \]
Consider the following binary hypothesis testing problem:

\[ H_0 : \quad X \sim P \]
\[ vs. \]
\[ H_1 : \quad X \sim Q \]

Define

\[ \beta_\epsilon(P, Q) \triangleq \inf \sum_{x \in \mathcal{X}} Q(x)T(0|x), \]

where the \( \inf \) is over all random tests \( T : \mathcal{X} \rightarrow \{0, 1\} \) s.t.

\[ \sum_{x \in \mathcal{X}} P(x)T(1|x) \leq \epsilon. \]

*Data processing.* For every stochastic matrix \( W : \mathcal{X} \rightarrow \mathcal{Y} \)

\[ \beta_\epsilon(P, Q) \leq \beta_\epsilon(PW, QW) \]
Given a partition $\pi = \{\pi_1, \ldots, \pi_k\}$ of $\{1, \ldots, m\}$

- Let $Q(x_1, \ldots, x_m|z) = \prod_{i=1}^{k} Q(x_{\pi_i}|z)$

For the binary hypothesis testing:

$H_0 : X_1, \ldots, X_m, Z \sim P,$

$H_1 : X_1, \ldots, X_m, Z \sim Q,$

consider the degraded observations $K_1, \ldots, K_m, F, Z.$
Given a partition \( \pi = \{\pi_1, \ldots, \pi_k\} \) of \( \{1, \ldots, m\} \)

- Let \( Q(x_1, \ldots, x_m|z) = \prod_{i=1}^{k} Q(x_{\pi_i}|z) \)

For the binary hypothesis testing:

\[
H_0 : \quad X_1, \ldots, X_m, Z \sim P,
\]

\[
H_1 : \quad X_1, \ldots, X_m, Z \sim Q,
\]

consider the degraded observations \( K_1, \ldots, K_m, F, Z \).

Let \( W_{K_1 \ldots K_m F|X_1 \ldots X_m Z} \) represent the protocol.
Consider the degraded binary hypothesis testing:

\[ H_0 : \quad K_1, \ldots, K_m, F, Z \sim P_{K_1 \ldots K_m} \mathbb{F} \mathbb{Z} = P \mathbb{W} \]

\[ H_1 : \quad K_1, \ldots, K_m, F, Z \sim Q_{K_1 \ldots K_m} \mathbb{F} \mathbb{Z} = Q \mathbb{W} \]

Consider a test with the acceptance region \( A \) defined by:

\[
A \triangleq \left\{ \log \frac{P_{\text{unif},m}(K_1, \ldots, K_m)}{Q_{K_1 \ldots K_m|FZ}(K_1 \ldots K_m|F, Z)} \geq \lambda_\pi \right\}
\]

where

\[
\lambda_\pi = (|\pi| - 1) \log |\mathcal{K}| - |\pi| \log(1/\eta)
\]
Reduction Argument

Consider the degraded binary hypothesis testing:

\[ H_0 : \quad K_1, \ldots, K_m, F, Z \sim P_{K_1,\ldots,K_m|FZ} = PW \]
\[ H_1 : \quad K_1, \ldots, K_m, F, Z \sim Q_{K_1,\ldots,K_m|FZ} = QW \]

Consider a test with the acceptance region \( \mathcal{A} \) defined by:

\[
\mathcal{A} \triangleq \left\{ \log \frac{P_{\text{unif},m}(K_1, \ldots, K_m)}{Q_{K_1\ldots K_m|FZ}(K_1\ldots K_m|F, Z)} \geq \lambda_\pi \right\}
\]

where

\[
\lambda_\pi = (|\pi| - 1) \log |\mathcal{K}| - |\pi| \log(1/\eta)
\]

Likelihood ratio test with \( P_{K_1\ldots K_m|FZ} \) replaced by \( P_{\text{unif},m} \)

- recall: \( \frac{1}{2} \| P_{K_1 K_2 \ldots K_m FZ} - P_{\text{unif},m} \times P_{FZ} \|_1 \leq \epsilon \)
Reduction Argument

Missed Detection: \[ Q_{K_1\ldots K_m F_Z}(A) \leq |\mathcal{K}|^{1-|\pi|} \eta^{-|\pi|} \]

False Alarm: \[ P_{K_1\ldots K_m F_Z}(A^c) \leq \epsilon + \eta \]
Reduction Argument

Missed Detection:  \( Q_{K_1...K_m}FZ(A) \leq |K|^{1-|\pi|}\eta-|\pi| \) - easy

False Alarm:  \( P_{K_1...K_m}FZ(A^c) \leq \epsilon + \eta \) - requires work

Key steps:

\( Q_{K_1...K_m}|FZ = \prod_{i=1}^{k} Q_{K_{\pi_i}}|FZ \)

\( \triangleright \) Apply Hölder’s inequality to the product form
Reduction Argument

Missed Detection: \[ Q_{K_1 \ldots K_m} F_Z (A) \leq |K|^{1-|\pi|} \eta^{-|\pi|} \] - easy

False Alarm: \[ P_{K_1 \ldots K_m} F_Z (A^c) \leq \epsilon + \eta \] - requires work

Key steps:
- \[ Q_{K_1 \ldots K_m} F_Z = \prod_{i=1}^{k} Q_{K_{\pi_i}} F_Z \]
- Apply Hölder’s inequality to the product form

Lemma (Reduction)

For every \( 0 \leq \epsilon < 1 \) and \( 0 < \eta < 1 - \epsilon \),

\[ S_\epsilon (X_1, \ldots, X_m | Z) \leq \frac{1}{|\pi| - 1} \left[ - \log \beta_{\epsilon+\eta} (PW, QW) + |\pi| \log (1/\eta) \right] . \]
**Reduction Argument**

**Missed Detection:** \( Q_{K_1 \ldots K_m} F_Z (A) \leq |K|^{1-|\pi|} \eta^{-|\pi|} \) - easy

**False Alarm:** \( P_{K_1 \ldots K_m} F_Z (A^c) \leq \epsilon + \eta \) - requires work

**Key steps:**
- \( Q_{K_1 \ldots K_m} F_Z = \prod_{i=1}^k Q_{K_{\pi_i}} F_Z \)
- Apply Hölder’s inequality to the product form

**Lemma (Reduction)**

For every \( 0 \leq \epsilon < 1 \) and \( 0 < \eta < 1 - \epsilon \),

\[
S_\epsilon(X_1, \ldots, X_m | Z) \leq \frac{1}{|\pi| - 1} \left[ - \log \beta_{\epsilon+\eta}(PW, QW) + |\pi| \log \left( \frac{1}{\eta} \right) \right].
\]

By data processing: \( \beta_{\epsilon+\eta}(PW, QW) \geq \beta_{\epsilon+\eta}(P, Q) \)
Conditional Independence Testing Bound

**Theorem**

For every $0 \leq \epsilon < 1$ and $0 < \eta < 1 - \epsilon$,

$$S_\epsilon(X_1, \ldots, X_m|Z) \leq \frac{1}{|\pi| - 1} \left[-\log \beta_{\epsilon+\eta}(P, Q) + |\pi| \log \frac{1}{\eta}\right],$$

where

$$Q(x_1, \ldots, x_m|z) = \prod_{i=1}^{k} Q(x_{\pi_i}|z).$$

For two parties:

$$S_\epsilon(X_1, X_2|Z) \leq -\log \beta_{\epsilon+\eta}(P_{X_1X_2Z}, P_{X_1|Z}P_{X_2|Z}P_{Z}) + 2 \log \frac{1}{\eta}.$$
### Theorem

For every $0 \leq \epsilon < 1$ and $0 < \eta < 1 - \epsilon$,

$$S_\epsilon(X_1, \ldots, X_m | Z) \leq \frac{1}{|\pi| - 1} \left[ - \log \beta_{\epsilon+\eta} (P, Q) + |\pi| \log \left( \frac{1}{\eta} \right) \right],$$

where

$$Q(x_1, \ldots, x_m | z) = \prod_{i=1}^{k} Q(x_{\pi_i} | z).$$

For two parties:

$$S_\epsilon(X_1, X_2 | Z) \leq - \log \beta_{\epsilon+\eta} \left( P_{X_1 X_2 Z}, P_{X_1 | Z} P_{X_2 | Z} P_Z \right) + 2 \log \left( \frac{1}{\eta} \right)$$

Connections to meta-converse of Polyanskiy, Poor, and Vérdú
Strong Converse for Secret Key Capacity
Consider IID observations $X_1, \ldots, X_m \equiv X_1^n, \ldots, X_m^n, Z = \emptyset$.

Recall: $K_1, \ldots, K_m$ constitute an $(\epsilon, \delta)$-secret key of length $\log K$ if

$$P(K_1 = K_2 = \ldots = K_m) \geq 1 - \epsilon, \quad \text{:Recoverability}$$

$$\frac{1}{2}\|P_{K_1F} - P_{\text{unif}} \times P_F\|_1 \leq \delta, \quad \text{:Secrecy}$$

Secret Key Capacity: $C_{\epsilon, \delta} \equiv \liminf_n \frac{1}{n} S_{\epsilon, \delta}(X_1^n, \ldots, X_m^n)$
Strong Converse for Secret Key Agreement

Consider IID observations $X_1, \ldots, X_m \equiv X_1^n, \ldots, X_m^n$, $Z = \emptyset$

Recall: $K_1, \ldots, K_m$ constitute an $(\epsilon, \delta)$-secret key of length $\log \mathcal{K}$ if

$$P(K_1 = K_2 = \ldots = K_m) \geq 1 - \epsilon,$$

Recoverability

$$\frac{1}{2} \|P_{K_1F} - P_{\text{unif}} \times P_F\|_1 \leq \delta,$$

Secrecy

Secret Key Capacity: $C_{\epsilon,\delta} \equiv \liminf_n \frac{1}{n} S_{\epsilon,\delta}(X_1^n, \ldots, X_m^n)$

[Maurer ‘93] [Ahlswede-Csiszár ‘93] [Csiszar-Narayan ‘04]
By the *conditional independence testing* bound:

For every partition $\pi$ and $\eta < 1 - \epsilon - \delta$, 

$$C_{\epsilon,\delta} \leq \frac{1}{|\pi| - 1} \liminf_{n} \frac{1}{n} \log \beta_{\epsilon + \delta + \eta} \left(P_{X_{1}^{n}\ldots X_{m}^{n}}, \prod_{i=1}^{k} P_{X_{\pi_{i}}^{n}} \right)$$

$$= \frac{1}{|\pi| - 1} D \left(P_{X_{1}\ldots X_{m}} \parallel \prod_{i=1}^{k} P_{X_{\pi_{i}}} \right),$$

where the equality follows from Stein’s Lemma.
Strong Converse for Secret Key Agreement

By the *conditional independence testing* bound:

For every partition \( \pi \) and \( \eta < 1 - \epsilon - \delta \),

\[
C_{\epsilon,\delta} \leq \frac{1}{|\pi| - 1} \liminf_{n \to \infty} \frac{1}{n} \log \beta_{\epsilon+\delta+\eta} \left( \mathbb{P}_{X^n_1 \ldots X^n_m}, \prod_{i=1}^k \mathbb{P}_{X^n_{\pi_i}} \right)
\]

\[
= \frac{1}{|\pi| - 1} D \left( \mathbb{P}_{X_1 \ldots X_m} \left\| \prod_{i=1}^k \mathbb{P}_{X_{\pi_i}} \right\| \right),
\]

where the equality follows from Stein’s Lemma.

**Theorem (Strong Converse)**

*For every* \( \epsilon + \delta < 1 \),

\[
C_{\epsilon,\delta} = \min_{\pi} \frac{1}{|\pi| - 1} D \left( \mathbb{P}_{X_1 \ldots X_m} \left\| \prod_{i=1}^k \mathbb{P}_{X_{\pi_i}} \right\| \right).
\]

Direct part by [Csiszár-Narayan ‘04] and [Chang-Zheng ‘10]
In Closing ... 

We establish an upper bound on the length of secret keys that can be generated by public discussion.

Our conditional independence testing bound relates secret key agreement to binary hypothesis testing.
We establish an upper bound on the length of secret keys that can be generated by public discussion.

Our conditional independence testing bound relates secret key agreement to binary hypothesis testing.

In progress: consequences for cryptographic applications such as oblivious transfer and bit commitment.
We establish an upper bound on the length of secret keys that can be generated by public discussion.

Our conditional independence testing bound relates secret key agreement to binary hypothesis testing.

In progress: consequences for cryptographic applications such as oblivious transfer and bit commitment.

[Tyagi-Watanabe, Eurocrypt ‘14]

[Hayashi-Tyagi-Watanabe, ISIT ‘14]