Secret Key Agreement:
General Capacity and Second-Order Asymptotics

Masahito Hayashi    Himanshu Tyagi    Shun Watanabe
Two party secret key agreement

Maurer 93, Ahlswede-Csiszár 93

A random variable $K$ constitutes an $(\epsilon, \delta)$-SK if:

\[
P(K_x = K_y = K) \geq 1 - \epsilon \quad : \text{recoverability}
\]

\[
\frac{1}{2} \|P_{KF} - P_{\text{unif}}P_F\| \leq \delta \quad : \text{security}
\]
Two party secret key agreement

Maurer 93, Ahlswede-Csiszár 93

A random variable $K$ constitutes an $(\epsilon, \delta)$-SK if:

$$P(K_x = K_y = K) \geq 1 - \epsilon : \text{recoverability}$$

$$\frac{1}{2} \|P_{KF} - P_{\text{unif}}P_F\| \leq \delta : \text{security}$$
A random variable $K$ constitutes an $(\epsilon, \delta)$-SK if:

\[
P(K_x = K_y = K) \geq 1 - \epsilon \quad \text{: recoverability}
\]

\[
\frac{1}{2} \|P_{KF} - P_{unif}P_F\| \leq \delta \quad \text{: security}
\]

What is the maximum length $S(X, Y)$ of a SK that can be generated?
Where do we stand?

Maurer 93, Ahlswede-Csiszár 93
\[ S(X^n, Y^n) = nI(X \land Y) + o(n) \quad \text{(Secret key capacity)} \]

Csiszár-Narayan 04
Secret key capacity for multiple terminals

Renner-Wolf 03, 05
Single-shot bounds on \( S(X, Y) \)
Where do we stand?

**Maurer 93, Ahlswede-Csiszár 93**

\[ S(X^n, Y^n) = nI(X \land Y) + o(n) \quad \text{(Secret key capacity)} \]

**Csiszár-Narayan 04**

Secret key capacity for multiple terminals

**Renner-Wolf 03, 05**

Single-shot bounds on \( S(X, Y) \)

Typical construction: \( X \) sends a compressed version of itself to \( Y \), and the \( K \) is *extracted* from shared \( X \) using a 2-universal hash family
Where do we stand?

Maurer 93, Ahlswede-Csiszár 93
\[ S(X^n, Y^n) = n I(X \land Y) + o(n) \]  (Secret key capacity)

Csiszár-Narayan 04
Secret key capacity for multiple terminals

Renner-Wolf 03, 05
Single-shot bounds on \( S(X, Y) \)

Typical construction: \( X \) sends a compressed version of itself to \( Y \), and the \( K \) is extracted from shared \( X \) using a 2-universal hash family

Converse??
Where do we stand?

Maurer 93, Ahlswede-Csiszár 93 Fano's inequality
\[ S(X^n, Y^n) = nI(X \land Y) + o(n) \] (Secret key capacity)

Csiszár-Narayan 04 Fano’s inequality
Secret key capacity for multiple terminals

Renner-Wolf 03, 05 \sim Potential function method
Single-shot bounds on \( S(X, Y) \)

Typical construction: \( X \) sends a compressed version of itself to \( Y \), and the \( K \) is extracted from shared \( X \) using a 2-universal hash family

Converse??
The source of our rekindled excitement about this problem:

**Theorem (Tyagi-Watanabe 2014)**

Given $\epsilon, \delta \geq 0$ with $\epsilon + \delta < 1$ and $0 < \eta < 1 - \epsilon - \delta$. It holds that

$$S_{\epsilon,\delta}(X, Y) \leq -\log \beta_{\epsilon+\delta+\eta}(P_{XY}, P_X P_Y) + 2 \log(1/\eta)$$
The source of our rekindled excitement about this problem:

**Theorem (Tyagi-Watanabe 2014)**

Given $\epsilon, \delta \geq 0$ with $\epsilon + \delta < 1$ and $0 < \eta < 1 - \epsilon - \delta$. It holds that

$$S_{\epsilon, \delta} (X, Y) \leq - \log \beta_{\epsilon+\delta+\eta}(P_{XY}, P_X P_Y) + 2 \log(1/\eta)$$

where

$$\beta_{\epsilon}(P, Q) \triangleq \inf_{T: P[T] \geq 1-\epsilon} Q[T],$$

and

$$P[T] = \sum_v P(v) T(0|v) \quad \text{and} \quad Q[T] = \sum_v Q(v) T(0|v)$$
The source of our rekindled excitement about this problem:

**Theorem (Tyagi-Watanabe 2014)**

Given \( \epsilon, \delta \geq 0 \) with \( \epsilon + \delta < 1 \) and \( 0 < \eta < 1 - \epsilon - \delta \). It holds that

\[
S_{\epsilon,\delta}(X, Y) \leq - \log \beta_{\epsilon+\delta+\eta}(P_{XY}, P_X P_Y) + 2 \log(1/\eta)
\]

where

\[
\beta_{\epsilon}(P, Q) \triangleq \inf_{T: P[T] \geq 1-\epsilon} Q[T],
\]

where

\[
P[T] = \sum_v P(v) T(0|v) \quad Q[T] = \sum_v Q(v) T(0|v)
\]

In the spirit of *meta-converse* of Polyanskiy, Poor, and Verdu
Recall the two steps of SK agreement:

**Step 1 (aka Information reconciliation).**
Slepian-Wolf code to send $X$ to $Y$

**Step 2 (aka Randomness extraction or privacy amplification).**
“Random function” $K$ to extract uniform random bits from $X$ as $K(X)$

**Example.** For $(X, Y) \equiv (X^n, Y^n)$
Rate of communication in step 1 $= H(X \mid Y) = H(X) - I(X \wedge Y)$
Rate of randomness extraction in step 2 $= H(X)$

The difference is the secret key capacity
Recall the two steps of SK agreement:

**Step 1 (aka Information reconciliation).**
Slepian-Wolf code to send $X$ to $Y$

**Step 2 (aka Randomness extraction or privacy amplification).**
“Random function” $K$ to extract uniform random bits from $X$ as $K(X)$

**Example.** For $(X, Y) \equiv (X^n, Y^n)$
Rate of communication in step 1 $= H(X \mid Y) = H(X) - I(X \land Y)$
Rate of randomness extraction in step 2 $= H(X)$

The difference is the secret key capacity

Are we done?
Recall the two steps of SK agreement:

**Step 1 (aka Information reconciliation).**
Slepian-Wolf code to send $X$ to $Y$

**Step 2 (aka Randomness extraction or privacy amplification).**
“Random function” $K$ to extract uniform random bits from $X$ as $K(X)$

**Example.** For $(X, Y) \equiv (X^n, Y^n)$

Rate of communication in step 1 $= H(X \mid Y) = H(X) - I(X \wedge Y)$

Rate of randomness extraction in step 2 $= H(X)$

The difference is the secret key capacity

Are we done? Not quite. Let’s take a careful look
Lemma (Slepian-Wolf coding)

There exists a code \((e, d)\) of size \(M\) with encoder \(e : \mathcal{X} \rightarrow \{1, \ldots, M\}\), and a decoder \(d : \{1, \ldots, M\} \times \mathcal{Y} \rightarrow \mathcal{X}\), such that

\[
P_{XY} \left( \{(x, y) \mid x \neq d(e(x), y)\} \right)
\leq P_{XY} \left( \{(x, y) \mid -\log P_{X|Y}(x \mid y) \geq \log M - \gamma\} \right) + 2^{-\gamma}.
\]
Lemma (Slepian-Wolf coding)

There exists a code \((e, d)\) of size \(M\) with encoder \(e : \mathcal{X} \rightarrow \{1, \ldots, M\}\), and a decoder \(d : \{1, \ldots, M\} \times \mathcal{Y} \rightarrow \mathcal{X}\), such that

\[
\Pr_{X,Y} \left( \{(x, y) \mid x \neq d(e(x), y)\} \right) \\
\leq \Pr_{X,Y} \left( \{(x, y) \mid -\log \Pr_{X|Y}(x \mid y) \geq \log M - \gamma\} \right) + 2^{-\gamma}.
\]

\[
-\log \Pr_{X|Y} = -\log \Pr_{X} - \log(\Pr_{Y|X}/\Pr_{Y})
\]

Compare with

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

The second term is a proxy for the mutual information
Step 1: Slepian-Wolf theorem

Miyake Kanaya 95, Han 03

Lemma (Slepian-Wolf coding)

There exists a code \((e, d)\) of size \(M\) with encoder \(e : \mathcal{X} \to \{1, \ldots, M\}\), and a decoder \(d : \{1, \ldots, M\} \times \mathcal{Y} \to \mathcal{X}\), such that

\[
\begin{align*}
P_{XY}(\{(x, y) \mid x \neq d(e(x), y)\}) & \\
\leq P_{XY}(\{(x, y) \mid \geq \log M - \gamma\}) + 2^{-\gamma}.
\end{align*}
\]

\[-\log P_{X|Y} = -\log P_X - \log(P_{Y|X}/P_Y)\]

Compare with

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

The second term is a proxy for the mutual information

Communication rate needed is approximately equal to

(large probability upper bound on \(-\log P_X\) - \log(P_{Y|X}/P_Y))
Step 2: Leftover hash lemma

Lesson from the step 1: Communication rate is approximately

\[(\text{large probability upper bound on } - \log P_X) - \log(P_{Y|X}/P_Y)\]

Recall that the \textit{min entropy} of \(X\) is given by

\[H_{\text{min}}(P_X) = -\log \max_x P_X(x)\]

Impagliazzo et. al. 89, Bennett et. al. 95, Renner-Wolf 05

Lemma (Leftover hash)

There exists a function \(K\) of \(X\) taking values in \(\mathcal{K}\) such that

\[
\|P_{KZ} - P_{\text{unif}} Z\| \leq \sqrt{\mathcal{K}|Z| 2^{-H_{\text{min}}(P_X)}}
\]
Step 2: Leftover hash lemma

Lesson from the step 1: Communication rate is approximately

\[(\text{large probability upper bound on } - \log P_X) - \log(P_{Y|X}/P_Y)\]

Recall that the min entropy of $X$ is given by

\[H_{\text{min}}(P_X) = -\log \max_x P_X(x)\]

Impagliazzo et. al. 89, Bennett et. al. 95, Renner-Wolf 05

Lemma (Leftover hash)

There exists a function $K$ of $X$ taking values in $\mathcal{K}$ such that

\[\|P_{KZ} - P_{\text{unif}}P_Z\| \leq \sqrt{\mathcal{K}|Z|2^{-H_{\text{min}}(P_X)}}\]

Randomness can be extracted at a rate approximately equal to

\[(\text{large probability lower bound on } - \log P_X)\]
Step 2: Leftover hash lemma

Lesson from the step 1: Communication rate is approximately

\[(\text{large probability upper bound on } -\log P_X) - \log(P_{Y|X}/P_Y)\]

Recall that the min entropy of \(X\) is given by

\[H_{\min}(P_X) = -\log \max_x P_X(x)\]

Impagliazzo et. al. 89, Bennett et. al. 95, Renner-Wolf 05

Lemma (Leftover hash)

There exists a function \(K\) of \(X\) taking values in \(K\) such that

\[\|P_{KZ} - P_{\text{unif}}P_Z\| \leq \sqrt{|K||Z| - H_{\min}(P_X)}\]

Randomness can be extracted at a rate approximately equal to

\[(\text{large probability lower bound on } -\log P_X)\]
Spectrum slicing

A slice of the spectrum

Slice the spectrum of $X$ into $L$ bins of length $\Delta$ and send the bin number to $Y$.
Single-shot achievability

Theorem

For every $\gamma > 0$ and $0 \leq \lambda \leq \lambda_{\text{min}}$, there exists an $(\epsilon, \delta)$-SK $K$ taking values in $\mathcal{K}$ with

$$\epsilon \leq P \left( \log \frac{P_{XY} (X, Y)}{P_X (X) P_Y (Y)} \leq \lambda + \gamma + \Delta \right)$$

$$+ P \left( -\log P_X (X) \notin (\lambda_{\text{min}}, \lambda_{\text{max}}) \right) + \frac{1}{L}$$

$$\delta \leq \frac{1}{2} \sqrt{|\mathcal{K}| 2^{-(\lambda - 2 \log L)}}$$
Consider a sequence of sources \((X_n, Y_n)\)

The **SK capacity** \(C\) is defined as

\[
C \triangleq \sup_{\epsilon_n, \delta_n} \lim_{n \to \infty} \inf \frac{1}{n} S_{\epsilon_n, \delta_n} (X_n, Y_n)
\]

where the \(\sup\) is over all \(\epsilon_n, \delta_n \geq 0\) such that

\[
\lim_{n \to \infty} \epsilon_n + \delta_n = 0
\]
Secret key capacity for general sources

Consider a sequence of sources \((X_n, Y_n)\)

The **SK capacity** \(C\) is defined as

\[
C \triangleq \sup_{\epsilon_n, \delta_n} \liminf_{n \to \infty} \frac{1}{n} S_{\epsilon_n, \delta_n}(X_n, Y_n)
\]

where the \(\sup\) is over all \(\epsilon_n, \delta_n \geq 0\) such that

\[
\lim_{n \to \infty} \epsilon_n + \delta_n = 0
\]

The **inf-mutual information rate** \(I(X \land Y)\) is defined as

\[
I(X \land Y) \triangleq \sup \left\{ \alpha \mid \lim_{n \to \infty} P(Z_n < \alpha) = 0 \right\}
\]

where

\[
Z_n = \frac{1}{n} \log \frac{P_{X_n Y_n}(X_n, Y_n)}{P_{X_n}(X_n) P_{Y_n}(Y_n)}
\]
General capacity

**Theorem (Secret key capacity)**

The SK capacity $C$ for a sequence of sources $\{X_n, Y_n\}_{n=1}^{\infty}$ is given by

$$C = I(X \land Y)$$
General capacity

**Theorem (Secret key capacity)**

The SK capacity $C$ for a sequence of sources $\{X_n, Y_n\}_{n=1}^{\infty}$ is given by

$$C = I(X \land Y)$$

**Converse.** Follows from our *conditional independence testing bound* with:

**Lemma (Verdú)**

For every $\epsilon_n$ such that

$$\lim_{n \to \infty} \epsilon_n = 0$$

it holds that

$$\liminf_{n} \frac{1}{n} \log \beta_{\epsilon_n} (P_{X_n Y_n}, P_{X_n} P_{Y_n}) \leq I(X \land Y)$$
Theorem (Secret key capacity)

The SK capacity $C$ for a sequence of sources $\{X_n, Y_n\}_{n=1}^{\infty}$ is given by

$$C = I(X \land Y)$$

Achievability. Use the single-shot construction with

$$\lambda_{\text{max}} = n \left( \overline{H}(X) + \Delta \right)$$

$$\lambda_{\text{min}} = n \left( H(X) - \Delta \right)$$

$$\lambda = n \left( I(X \land Y) - \Delta \right)$$
Towards characterizing finite-blocklength performance

We identify the second term in the asymptotic expansion of $S(X^n, Y^n)$:

**Theorem (Second order asymptotics)**

For every $0 < \epsilon < 1$ and IID RVs $X^n, Y^n$, we have

$$S_\epsilon (X^n, Y^n) = nI(X \land Y) - \sqrt{nV}Q^{-1}(\epsilon) + o(\sqrt{n})$$

The quantity $V$ is given by

$$V = \text{Var} \left( \log \frac{P_{XY}(X, Y)}{P_X(X)P_Y(Y)} \right)$$
Towards characterizing finite-blocklength performance

We identify the second term in the asymptotic expansion of $S(X^n, Y^n)$:

**Theorem (Second order asymptotics)**

For every $0 < \epsilon < 1$ and IID RVs $X^n, Y^n$, we have

$$S_{\epsilon} (X^n, Y^n) = nI(X \land Y) - \sqrt{nV}Q^{-1}(\epsilon) + o(\sqrt{n})$$

The quantity $V$ is given by

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

Proof relies on the use of Berry-Esseen theorem as in Polyanskiy-Poor-Verdu 10
Towards characterizing finite-blocklength performance

We identify the second term in the asymptotic expansion of $S(X^n, Y^n)$:

**Theorem (Second order asymptotics)**

For every $0 < \epsilon < 1$ and IID RVs $X^n, Y^n$, we have

$$S_{\epsilon} (X^n, Y^n) = nI(X \land Y) - \sqrt{nVQ}^{-1}(\epsilon) + o(\sqrt{n})$$

The quantity $V$ is given by

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

Proof relies on the use of Berry-Esseen theorem as in Polyanskiy-Poor-Verdu 10

What about $S_{\epsilon, \delta}(X^n, Y^n)$?
What if the eavesdropper has side information $Z$?

Best known converse bound on SK capacity due to Gohari-Ananthram 08

Recently we obtained a one-shot version of this bound


Also, we have a single-shot achievability scheme that is asymptotically tight when $X, Y, Z$ form a Markov chain