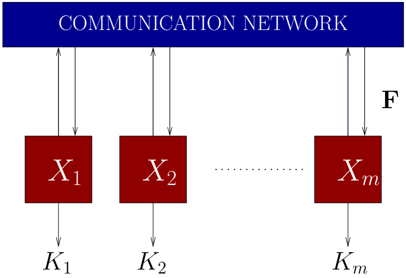
A Bound For Multiparty Secret Key Agreement

And

Implications For A Problem Of Secure Computing

Himanshu Tyagi and Shun Watanabe

Multiparty Secret Key Agreement



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

$K_1, ..., K_m$ constitute an (ϵ, δ)-secret key of length $\log \mathcal{K}$ if

$$\mathrm{P}\left(K_1 = K_2 = ... = K_m\right) \geq 1 - \epsilon, \qquad \text{:Recoverability}$$

$$\frac{1}{2}\|\mathrm{P}_{K_1\mathbf{F}Z} - \mathrm{P}_{\mathtt{unif}} \times \mathrm{P}_{\mathbf{F}Z}\|_1 \leq \delta, \qquad \text{:Secrecy}$$

Alternative Definition of a Secret Key

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

$$\frac{1}{2}\|\mathrm{P}_{K_1K_2...K_m\mathbf{F}Z} - \mathrm{P}_{\mathtt{unif},m} \times \mathrm{P}_{\mathbf{F}Z}\|_1 \le \epsilon,$$

where

$$\mathrm{P}_{\mathtt{unif},m}\left(k_1, ..., k_m\right) = \frac{1}{|\mathcal{K}|}\mathbb{1}(k_1 = ...k_m).$$

Alternative Definition of a Secret Key

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

$$\frac{1}{2}\|\mathrm{P}_{K_1K_2...K_m\mathbf{F}Z} - \mathrm{P}_{\mathtt{unif},m} \times \mathrm{P}_{\mathbf{F}Z}\|_1 \leq \epsilon,$$

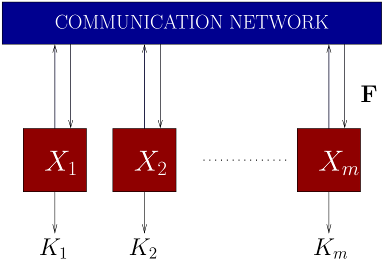
where

$$\mathrm{P}_{\mathtt{unif},m}(k_1, ..., k_m) = \frac{1}{|\mathcal{K}|}\mathbb{1}(k_1 = ...k_m).$$

Lemma

(ϵ, δ)-SK$\Rightarrow$ $(\epsilon + \delta)$-SK, and conversely, ϵ-SK $\Rightarrow$ (ϵ, ϵ)-SK.

Multiparty Secret Key Agreement



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

$$\frac{1}{2} \| \mathrm{P}_{K_1 K_2 \ldots K_m \mathbf{F} Z} - \mathrm{P}_{\mathtt{unif},m} \times \mathrm{P}_{\mathbf{F} Z} \|_1 \leq \epsilon.$$

Definition

$S_\epsilon(X_1, \ldots, X_m \mid Z) \triangleq$ maximum length of an ϵ-secret key

Upper bound for $S_\epsilon(X_1, ..., X_m \mid Z)$

No Correlation No Secret Key

If X_1 and X_2 are independent conditioned on Z:

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

No Correlation No Secret Key

If X_1 and X_2 are independent conditioned on Z:

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

If for some partition $\pi = \{\pi_1, ..., \pi_k\}$ of $\{1, ..., m\}$,

$X_{\pi_1}, ..., X_{\pi_k}$ are independent conditioned on Z:

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

No Correlation No Secret Key

If X_1 and X_2 are independent conditioned on Z:

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

If for some partition $\pi = \{\pi_1, ..., \pi_k\}$ of $\{1, ..., m\}$,

$X_{\pi_1}, ..., X_{\pi_k}$ are independent conditioned on Z:

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

Bound $S_\epsilon(X_1, ..., X_m|Z)$ in terms of "how far" is $\mathrm{P}_{X_1,...,X_mZ}$ is from a conditionally independent distribution

Digression: Binary Hypothesis Testing

Consider the following binary hypothesis testing problem:

$$\begin{aligned} H0: &\quad X \sim P \\ &vs. \\ H1: &\quad X \sim Q \end{aligned}$$

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 $T : \mathcal{X} \to \{0, 1\}$ s.t.

$$\sum_{x \in \mathcal{X}} P(x) T(1|x) \le \epsilon.$$

Digression: Binary Hypothesis Testing

Consider the following binary hypothesis testing problem:

$$H0: \quad X \sim P$$
$$vs.$$
$$H1: \quad X \sim Q$$

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 $T : \mathcal{X} \to \{0,1\}$ s.t.

$$\sum_{x \in \mathcal{X}} P(x) T(1|x) \le \epsilon.$$

Data processing. For every stochastic matrix $W : \mathcal{X} \to \mathcal{Y}$

$$\beta_\epsilon(P,Q) \le \beta_\epsilon(PW, QW)$$

Reduction Argument

Given a partition $\pi = \{\pi_1, ..., \pi_k\}$ of $\{1, ..., m\}$

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

For the binary hypothesis testing:

$$\begin{aligned} H0: &\quad X_1, ..., X_m, Z \sim \mathrm{P}, \\ H1: &\quad X_1, ..., X_m, Z \sim \mathrm{Q}, \end{aligned}$$

consider the degraded observations $K_1, ..., K_m, \mathbf{F}, Z$.

Reduction Argument

Given a partition $\pi = \{\pi_1, ..., \pi_k\}$ of $\{1, ..., m\}$

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

For the binary hypothesis testing:

$$\begin{aligned} H0: &\quad X_1, ..., X_m, Z \sim \mathrm{P}, \\ H1: &\quad X_1, ..., X_m, Z \sim \mathrm{Q}, \end{aligned}$$

consider the degraded observations $K_1, ..., K_m, \mathbf{F}, Z$.

Let $W_{K_1 \dots K_m \mathbf{F}|X_1 \dots X_m Z}$ represent the protocol.

Reduction Argument

Consider the degraded binary hypothesis testing:

$$\begin{aligned} H0: &\quad K_1, ..., K_m, \mathbf{F}, Z \sim \mathrm{P}_{K_1 ..., K_m \mathbf{F} Z} = \mathrm{P}W \\ H1: &\quad K_1, ..., K_m, \mathbf{F}, Z \sim \mathrm{Q}_{K_1 ..., K_m \mathbf{F} Z} = \mathrm{Q}W \end{aligned}$$

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

$$\mathcal{A} \triangleq \left\{ \log \frac{\mathrm{P}_{\mathrm{unif},m}(K_1, ..., K_m)}{\mathrm{Q}_{K_1 ... K_m | \mathbf{F} Z}(K_1 ... K_m | \mathbf{F}, Z)} \geq \lambda_\pi \right\}$$

where

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

Reduction Argument

Consider the degraded binary hypothesis testing:

$$H0: \quad K_1, ..., K_m, \mathbf{F}, Z \sim \mathrm{P}_{K_1 ..., K_m \mathbf{F} Z} = \mathrm{P}W$$
$$H1: \quad K_1, ..., K_m, \mathbf{F}, Z \sim \mathrm{Q}_{K_1 ..., K_m \mathbf{F} Z} = \mathrm{Q}W$$

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

$$\mathcal{A} \triangleq \left\{ \log \frac{\mathrm{P}_{\mathrm{unif},m}(K_1, ..., K_m)}{\mathrm{Q}_{K_1 ... K_m | \mathbf{F} Z}(K_1 ... K_m | \mathbf{F}, Z)} \geq \lambda_\pi \right\}$$

where

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

Likelihood ratio test with $\mathrm{P}_{K_1 ... K_m | \mathbf{F} Z}$ replaced by $\mathrm{P}_{\mathrm{unif},m}$

- recall: $\frac{1}{2} \| \mathrm{P}_{K_1 K_2 ... K_m \mathbf{F} Z} - \mathrm{P}_{\mathtt{unif},m} \times \mathrm{P}_{\mathbf{F} Z} \|_1 \leq \epsilon$

Reduction Argument

Missed Detection: $\mathrm{Q}_{K_1 \dots K_m \mathbf{F} Z}(\mathcal{A}) \leq |\mathcal{K}|^{1-|\pi|} \eta^{-|\pi|}$

False Alarm: $\mathrm{P}_{K_1 \dots K_m \mathbf{F} Z}(\mathcal{A}^c) \leq \epsilon + \eta$

Reduction Argument

Missed Detection: $\mathrm{Q}_{K_1 \ldots K_m \mathbf{F} Z}(\mathcal{A}) \leq |\mathcal{K}|^{1-|\pi|} \eta^{-|\pi|}$ - easy

False Alarm: $\mathrm{P}_{K_1 \ldots K_m \mathbf{F} Z}(\mathcal{A}^c) \leq \epsilon + \eta$ - requires work

Lemma (Reduction)

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

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

Reduction Argument

Missed Detection: $\mathrm{Q}_{K_1 \ldots K_m \mathbf{F} Z}(\mathcal{A}) \leq |\mathcal{K}|^{1-|\pi|} \eta^{-|\pi|}$ - easy

False Alarm: $\mathrm{P}_{K_1 \ldots K_m \mathbf{F} Z}(\mathcal{A}^c) \leq \epsilon + \eta$ - requires work

Lemma (Reduction)

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

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

By data processing: $\beta_{\epsilon+\eta}\left(\mathrm{P}W, \mathrm{Q}W\right) \geq \beta_{\epsilon+\eta}\left(\mathrm{P}, \mathrm{Q}\right)$

Conditional Independence Testing Bound

Theorem

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

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

where

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

For two parties:

$$S_\epsilon(X_1, X_2|Z) \leq - \log \beta_{\epsilon+\eta} \left(\mathrm{P}_{X_1 X_2 Z}, \mathrm{P}_{X_1|Z} \mathrm{P}_{X_2|Z} \mathrm{P}_Z \right) + 2 \log \left(1/\eta \right)$$

Conditional Independence Testing Bound

Theorem

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

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

where

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

For two parties:

$$S_\epsilon(X_1, X_2|Z) \leq -\log \beta_{\epsilon+\eta}\left(\mathrm{P}_{X_1X_2Z}, \mathrm{P}_{X_1|Z}\mathrm{P}_{X_2|Z}\mathrm{P}_Z\right) + 2\log\left(1/\eta\right)$$

Connections to meta-converse of Polyanskiy, Poor, and Vérdu

Implications of the Upper Bound

1. Strong Converse for Secret Key Agreement

[Maurer '93] [Ahlswede-Csiszár '93] [Csiszar-Narayan '04]

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

(ϵ, δ)-Secret Key Capacity: $C_{\epsilon,\delta} := \liminf_n \frac{1}{n} S_{\epsilon,\delta}(X_1^n, ..., X_m^n)$

Secret Key Capacity: $C := \inf_{\epsilon,\delta} C_{\epsilon,\delta}.$

1. Strong Converse for Secret Key Agreement

[Maurer '93] [Ahlswede-Csiszár '93] [Csiszar-Narayan '04]

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

(ϵ, δ)-Secret Key Capacity: $C_{\epsilon,\delta} := \liminf_n \frac{1}{n} S_{\epsilon,\delta}(X_1^n, ..., X_m^n)$

Secret Key Capacity: $C := \inf_{\epsilon,\delta} C_{\epsilon,\delta}.$

Theorem

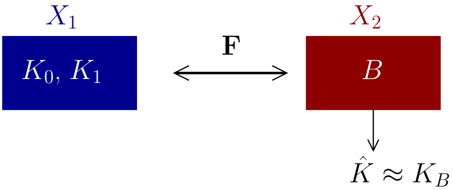
For $0 < \epsilon, \delta$ *with* $\epsilon + \delta < 1$,

$$C_{\epsilon,\delta} = C,$$

and for all $\epsilon + \delta \geq 1$,

$$C_{\epsilon,\delta} = \infty.$$

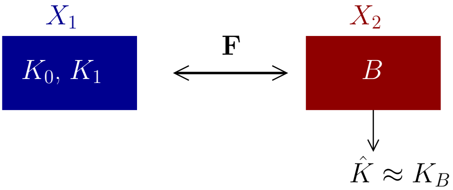
2. Information Theoretically Secure OT



[Even-Goldreich-Lempel 85], ..., [Nascimento-Winters 06]

- Reliability: $\mathrm{P}\left(\hat{K} \neq K_B\right) \leq \epsilon$
- Security 1: $\frac{1}{2}\left\|\mathrm{P}_{BK_0K_1X_1\mathbf{F}} - \mathrm{P}_B \times \mathrm{P}_{K_0K_1X_1\mathbf{F}}\right\|_1 \leq \delta_1$
- Security 2: $\frac{1}{2}\left\|\mathrm{P}_{K_{\overline{B}}BX_2\mathbf{F}} - \mathrm{P}_{K_{\overline{B}}} \times \mathrm{P}_{BX_2\mathbf{F}}\right\|_1 \leq \delta_2$

2. Information Theoretically Secure OT



[Even-Goldreich-Lempel 85], ..., [Nascimento-Winters 06]

- Reliability: $\mathrm{P}\left(\hat{K} \neq K_B\right) \leq \epsilon$
- Security 1: $\frac{1}{2}\left\|\mathrm{P}_{BK_0K_1X_1\mathbf{F}} - \mathrm{P}_B \times \mathrm{P}_{K_0K_1X_1\mathbf{F}}\right\|_1 \leq \delta_1$
- Security 2: $\frac{1}{2}\left\|\mathrm{P}_{K_{\overline{B}}BX_2\mathbf{F}} - \mathrm{P}_{K_{\overline{B}}} \times \mathrm{P}_{BX_2\mathbf{F}}\right\|_1 \leq \delta_2$

How large can the length l of OT be?

Bounds on the Efficiency of OT

Theorem (Reduction of SK Agreement to OT)

For an $(\epsilon, \delta_1, \delta_2)$*-OT of length* l

$$l \lesssim \min\left\{S_{\epsilon+\delta_1+2\delta_2}(X_1, X_2),\ S_{\epsilon+\delta_1+2\delta_2}\left(X_1, (X_1, X_2) \mid X_2\right)\right\}$$

Bounds on the Efficiency of OT

Theorem (Reduction of SK Agreement to OT)

For an $(\epsilon, \delta_1, \delta_2)$-OT of length l

$$l \lesssim \min\{S_{\epsilon+\delta_1+2\delta_2}(X_1, X_2),\ S_{\epsilon+\delta_1+2\delta_2}(X_1, (X_1, X_2) \mid X_2)\}$$

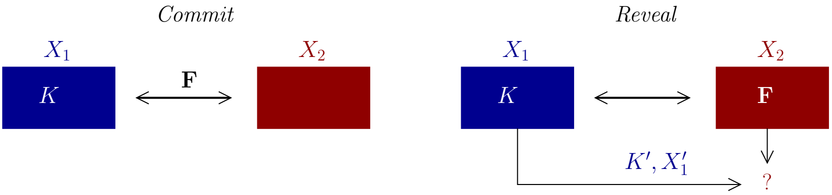
OT Capacity (for IID observations):

Maximum rate (l/n) of OT length (with $\delta_{1n}, \delta_{2n} \to 0$)

$$C_\epsilon(X_1, X_2) \leq \min\{I(X_1 \wedge X_2), H(X_1 \mid X_2)\}$$

"Strong" version of the Ahlswede-Csiszár upper bound

3. Information Theoretic Bit Commitment



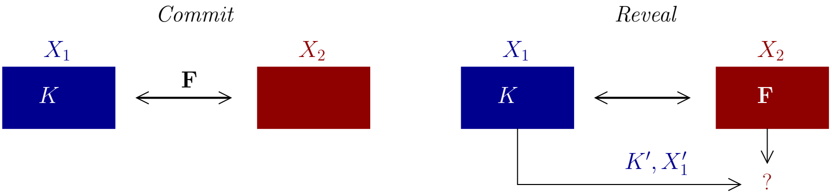
Party 2 constructs a test T for the hypothesis: "Secret is k"

Recovery: $\mathrm{P}\left(T(K, X_1, X_2, \mathbf{F}) = 1\right) \le \epsilon$

Security: $\frac{1}{2}\left\|\mathrm{P}_{KX_2\mathbf{F}} - \mathrm{P}_K \times \mathrm{P}_{X_2\mathbf{F}}\right\|_1 \le \delta_1$

Binding: $\mathrm{P}\left(T(K', X_1', X_2, \mathbf{F}) = 0, K' \neq K\right) \le \delta_2$

3. Information Theoretic Bit Commitment



Party 2 constructs a test T for the hypothesis: "Secret is k"

Recovery: $\mathrm{P}\left(T(K, X_1, X_2, \mathbf{F}) = 1\right) \leq \epsilon$

Security: $\dfrac{1}{2}\left\|\mathrm{P}_{K X_2 \mathbf{F}} - \mathrm{P}_K \times \mathrm{P}_{X_2 \mathbf{F}}\right\|_1 \leq \delta_1$

Binding: $\mathrm{P}\left(T(K', X_1', X_2, \mathbf{F}) = 0, K' \neq K\right) \leq \delta_2$

How large can the length l of BC be?

Bound on the Efficiency of BC

Theorem (Reduction of SK Agreement to BC)

For an $(\epsilon, \delta_1, \delta_2)$-BC of length l,

$$l \lesssim S_{\epsilon+\delta_1+\delta_2}\left(X_1, (X_1, X_2)|X_2\right)$$

Bound on the Efficiency of BC

Theorem (Reduction of SK Agreement to BC)

For an $(\epsilon, \delta_1, \delta_2)$*-BC of length* l*,*

$$l \lesssim S_{\epsilon+\delta_1+\delta_2}\left(X_1, (X_1, X_2)|X_2\right)$$

Efficiency of reduction of BC to OT

Given n-length OT: $X_1 \equiv K_0, K_1 \qquad X_2 \equiv K_B, B$.

The possible length l of BC is bounded as:

$$l \leq n + O(\log(1 - \epsilon - \delta_1 - \delta_2))$$

Bound on the Efficiency of BC

Theorem (Reduction of SK Agreement to BC)

For an $(\epsilon, \delta_1, \delta_2)$-BC of length l,

$$l \lesssim S_{\epsilon+\delta_1+\delta_2}\left(X_1, (X_1, X_2)|X_2\right)$$

Efficiency of reduction of BC to OT

Given n-length OT: $X_1 \equiv K_0, K_1 \qquad X_2 \equiv K_B, B$.

The possible length l of BC is bounded as:

$$l \leq n + O(\log(1 - \epsilon - \delta_1 - \delta_2))$$

Improves a bound of [Ranellucci et. al. 11]

Bound on the Efficiency of BC

Theorem (Reduction of SK Agreement to BC)

For an $(\epsilon, \delta_1, \delta_2)$*-BC of length* l*,*

$$l \lesssim S_{\epsilon+\delta_1+\delta_2}\left(X_1, (X_1, X_2)|X_2\right)$$

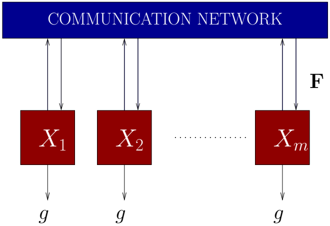
[Nascimento-Winters-Imai 03] BC capacity $C = H(X_1 \mid X_2)$

Strong converse for BC capacity

$$C_{\epsilon,\delta_1,\delta_2}(X_1, X_2) \leq H(X_1 \mid X_2), \quad \epsilon + \delta_1 + \delta_2 < 1$$

4. Secure Computing with Trusted Parties

Parties are trusted, the communication channel is not



Party i computes $G_i(X_i, \mathbf{F})$; Eavesdropper observes $\mathbf{F}, Z$

A function g is (ϵ, δ)-secure computable if

$$\mathrm{P}\left(G_1 = G_2 = \dots = G_m = g(X_1, \dots, X_m)\right) \geq 1 - \epsilon, \qquad \text{:Recoverability}$$

$$\frac{1}{2}\|\mathrm{P}_{G\mathbf{F}Z} - \mathrm{P}_G \times \mathrm{P}_{\mathbf{F}Z}\|_1 \leq \delta, \qquad \text{:Secrecy}$$

Characterization of securely computable functions

[Tyagi-Gupta-Narayan '11] IID case with $Z = \emptyset$

A function g is secure computable (asymptotically) iff

$$H(G) \leq C$$

Characterization of securely computable functions

[Tyagi-Gupta-Narayan '11] IID case with $Z = \emptyset$

A function g is secure computable (asymptotically) iff

$$H(G) \leq C$$

A single-shot necessary condition

Theorem

If a function g is (ϵ, δ)-secure computable, then

$$H_{\min}^{\xi}(\mathrm{P}_G) \lesssim \frac{-1}{|\pi| - 1} \log \beta_{\epsilon+\delta+2\xi}\big(\mathrm{P}_{X_{\mathcal{M}}Z}, \mathrm{Q}_{X_{\mathcal{M}}Z}\big),$$

where

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

In Closing...

We derived converse results for IT cryptography,

which are valid for the single-shot case

In Closing...

We derived converse results for IT cryptography,

which are valid for the single-shot case

Key idea: Reduction of hypothesis testing to crypto primitives

In Closing...

We derived converse results for IT cryptography,

which are valid for the single-shot case

Key idea: Reduction of hypothesis testing to crypto primitives

By observing the outputs of any IT secure crypto primitive

we can measure the correlation in the observations

In Closing...

We derived converse results for IT cryptography,

which are valid for the single-shot case

Key idea: Reduction of hypothesis testing to crypto primitives

By observing the outputs of any IT secure crypto primitive

we can measure the correlation in the observations

H. Tyagi and S. Watanabe, "*Converses for secret key agreement and secure computing,*" arXiv:1404.5715, 2014

In Closing...

We derived converse results for IT cryptography,

which are valid for the single-shot case

Key idea: Reduction of hypothesis testing to crypto primitives

By observing the outputs of any IT secure crypto primitive

we can measure the correlation in the observations

H. Tyagi and S. Watanabe, "*Converses for secret key agreement and secure computing,*" arXiv:1404.5715, 2014

How close do efficient schemes come to these performance bounds??