Converses for Information Theoretic Cryptography

Himanshu Tyagi

Joint work with Shun Watanabe

UC San Diego

Marriage of Cryptography and Computation

Behind every successful secure transmission

there is a (computational) cryptography primitive

Matchmakers of early 80s

Limitations of Computational Cryptography

Computationally expensive

Not feasible to put a cryptographic primitive on every small device

No "formal" proof of security

Proof is in the eating of the pudding (which we ordered online)

Limitations of Computational Cryptography

Computationally expensive

Not feasible to put a cryptographic primitive on every small device

No "formal" proof of security

Proof is in the eating of the pudding (which we ordered online)

> Cryptographers seldom sleep well([M]). Their careers are frequently based on very precise complexity-theoretic assumptions, which could be shattered the next morning. A polynomial time

Kilian 1988, "Founding cryptography on oblivious transfer"

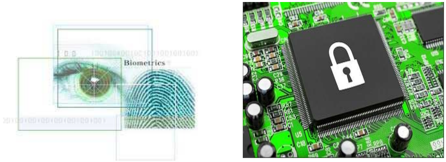
Information Theoretic Cryptography

... is provably secure and efficiently implementable

provided we have some shared correlative randomness:

$e.g.$ noisy channels, correlated randomness, quantum observations

Inherent randomness in the wireless medium



Randomness in physical data

Concerns for Information Theoretic Cryptography

- Engineering problem:

  - How does one make correlated randomness available?

  physically unclonable functions, biometrics,
  secret keys from channel fades, quantum key distribution, ...

  - How can we model eavesdropper's side information?

  timing attack, side channel attack, wormhole attack, ...

- Analysis often relies on simplifying assumptions on statistics:

  - Universal protocols?

  constructions based on hash families and error correcting codes

  - Nonasymptotic performance?

  converses based on reduction arguments

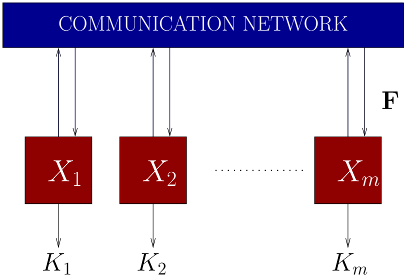
Outline

1. Secret key generation
   - Secret keys from correlated observations
   - Upper bound for secret key length
2. Oblivious transfer
   - Oblivious transfer via erasure channel
   - Converse result for oblivious transfer
3. Bit commitment

Secret Key Agreement

Multiparty Secret Key Agreement

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



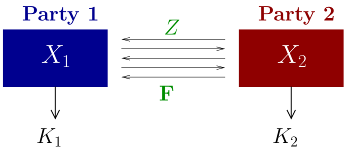
Party i computes $K_i(X_i, \mathbf{F}) \in \mathcal{K}$; Eavesdropper observes $\mathbf{F}, Z$

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

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

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

Two-party Secret Key Agreement



K constitutes a secret key of length $\log \mathcal{K}$ if

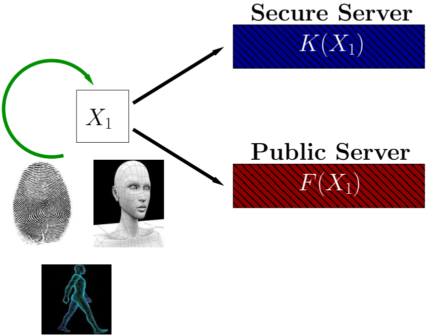
$$\mathrm{P}\left(K = K_1 = K_2\right) \geq 1 - \epsilon, \qquad \text{:Recoverability}$$

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

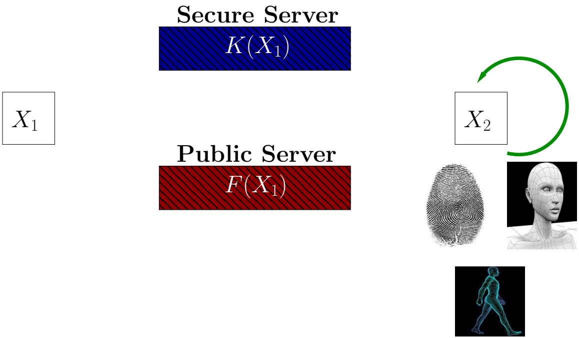
Definition

$S_{\epsilon,\delta}(X_1, X_2 \mid Z) \triangleq$ maximum length of a secret key

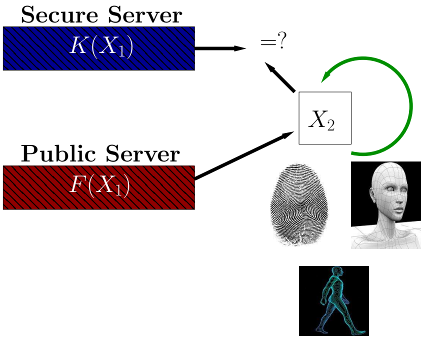
Biometric Security as Secret Key Agreement



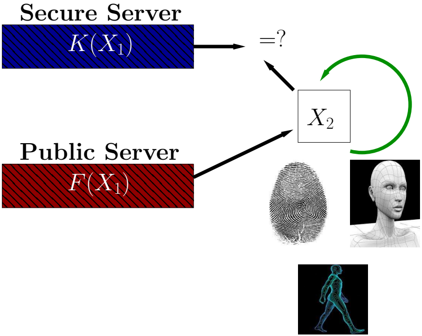
Biometric Security as Secret Key Agreement



Biometric Security as Secret Key Agreement



Biometric Security as Secret Key Agreement



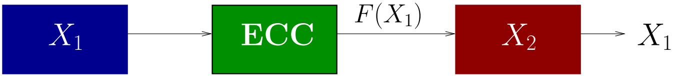
Similar approach can be applied for physically uncloneable functions

Efficient Secret Key Construction

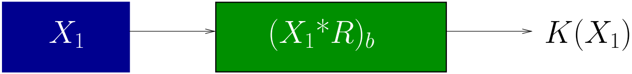
[Dodis-Ostrovsky-Reyzin-Smith 04]

X_1 and X_2 are n-length binary vectors with Hamming distance d

1. Error correcting code with minimum distance $2d + 1$



2. 2-universal hash family: Multiplication over $GF(2^n)$



Alternative Definition of a Secret Key

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

$$\mathrm{P}\left(K_1 = K_2 = ... = K_m\right) \geq 1 - \epsilon,$$
$$\frac{1}{2}\|\mathrm{P}_{K_1 \mathbf{F} Z} - \mathrm{P}_{\mathtt{unif}} \times \mathrm{P}_{\mathbf{F} Z}\|_1 \leq \delta$$

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

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

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, δ)-secret key of length $\log \mathcal{K}$ if

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

$$\frac{1}{2} \| \mathrm{P}_{K_1 \mathbf{F} Z} - \mathrm{P}_{\texttt{unif}} \times \mathrm{P}_{\mathbf{F} Z} \|_1 \leq \delta$$

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

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

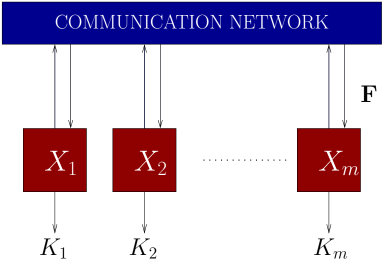
where

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

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 $\mathrm{P}_{X_1,...,X_m Z}$

is from a conditionally independent distribution

Digression: Binary Hypothesis Testing

Consider the following binary hypothesis testing problem:

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

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.

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

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.

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

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

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

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 $W_{K_1 ... K_m \mathbf{F} | X_1 ... X_m Z}$ 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:

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

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

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

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

Key steps:

- $\mathrm{Q}_{K_1 \ldots K_m | \mathbf{F} Z} = \prod_{i=1}^{k} \mathrm{Q}_{K_{\pi_i} | \mathbf{F} Z}$
- Apply Hölder's inequality to the product form

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

Key steps:

- $\mathrm{Q}_{K_1 \ldots K_m | \mathbf{F} Z} = \prod_{i=1}^{k} \mathrm{Q}_{K_{\pi_i} | \mathbf{F} Z}$
- Apply Hölder's inequality to the product form

Lemma

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

Key steps:

- $\mathrm{Q}_{K_1 \ldots K_m | \mathbf{F} Z} = \prod_{i=1}^{k} \mathrm{Q}_{K_{\pi_i} | \mathbf{F} Z}$
- Apply Hölder's inequality to the product form

Lemma

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

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

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:

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

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

Oblivious Transfer

Kilian 88:

Every secure function computation can be accomplished using OT

Rabin 81:

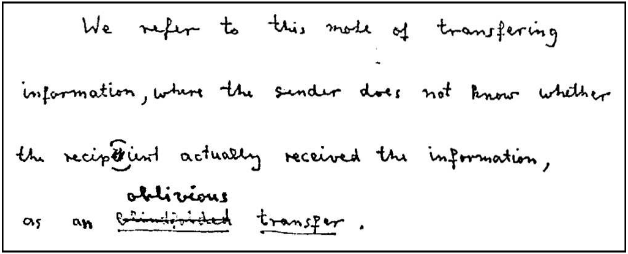
We refer to this mode of transferring information, where the sender does not know whether the recipient actually received the information, as an ~~[illegible]~~ oblivious transfer.

Oblivious Transfer: Basic Building Block of Cryptography

Kilian 88:

Every secure function computation can be accomplished using OT

Rabin 81:

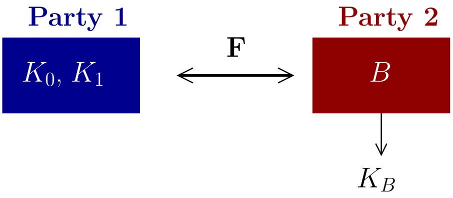


We refer to this mode of transferring information, where the sender does not know whether the recipient actually received the information, as an oblivious ~~[illegible]~~ transfer.

Example: Any noisy communication channel!

One-of-Two Oblivious Transfer

[Even, Goldreich, Lempel 85]



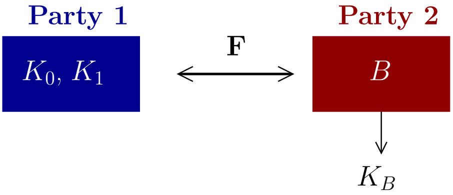
An instance of *Private Information Retrieval*

- K_0, K_1 are binary strings of length l
  B is a bit

B must remain "concealed" from Party 1

$K_{\overline{B}}$ must remain "concealed" from Party 2

Information Theoretically Secure OT

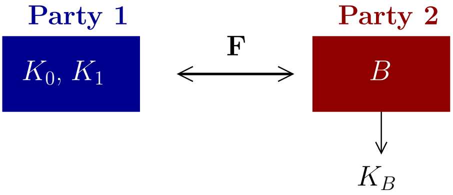


- K_0, K_1 are *random* binary strings of length l
  B is a random bit

Observations of party 1 are almost independent of B

Observations of party 2 are almost independent of $K_{\overline{B}}$

Information Theoretically Secure OT



- K_0, K_1 are *random* binary strings of length l
  B is a random bit

Observations of party 1 are almost independent of B

Observations of party 2 are almost independent of $K_{\overline{B}}$

Cannot be done without additional resources!

Making IT Secure OT Possible

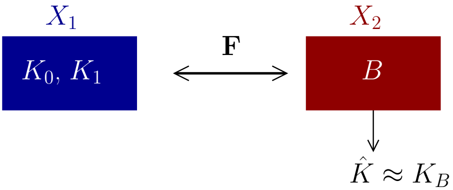
Additional Resources:

1. Noisy channels: [Crépeau-Kilian 88], [Crépeau 97], ...

DMC W used n times

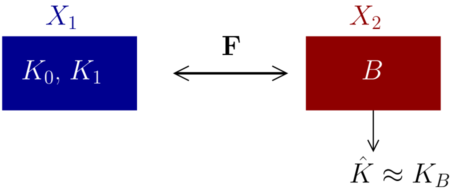
2. Correlated randomness: ..., [Nascimento-Winter 08]

n independent samples from $\mathrm{P}_{X_1 X_2}$



- Reliability: $\mathrm{P}\left(\hat{K} \neq K_B\right) \leq \epsilon$
- Security 1: $\frac{1}{2} \left\| \mathrm{P}_{B K_0 K_1 X_1 \mathbf{F}} - \mathrm{P}_B \times \mathrm{P}_{K_0 K_1 X_1 \mathbf{F}} \right\|_1 \leq \delta_1$
- Security 2: $\frac{1}{2} \left\| \mathrm{P}_{K_{\overline{B}} B X_2 \mathbf{F}} - \mathrm{P}_{K_{\overline{B}}} \times \mathrm{P}_{B X_2 \mathbf{F}} \right\|_1 \leq \delta_2$

Information Theoretically Secure OT



- 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: $\frac{1}{2}\left\|\mathrm{P}_{K_{\overline{B}}BX_2\mathbf{F}} - \mathrm{P}_{K_{\overline{B}}} \times \mathrm{P}_{BX_2\mathbf{F}}\right\|_1 \leq \delta_2$

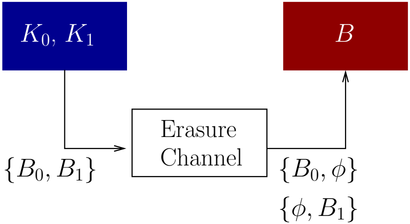
How large can the length l of OT be?

Oblivious Transfer Using Erasure Channel

[Crépeau 97, Nascimento-Winter 08]

Combinatorial erasure channel:

Erases half of the transmitted bits randomly



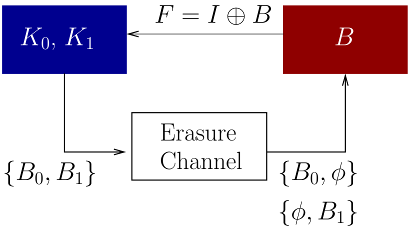
One-bit Oblivious Transfer

Oblivious Transfer Using Erasure Channel

[Crépeau 97, Nascimento-Winter 08]

Combinatorial erasure channel:

Erases half of the transmitted bits randomly



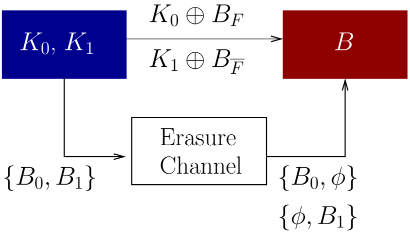
One-bit Oblivious Transfer

Oblivious Transfer Using Erasure Channel

[Crépeau 97, Nascimento-Winter 08]

Combinatorial erasure channel:

Erases half of the transmitted bits randomly



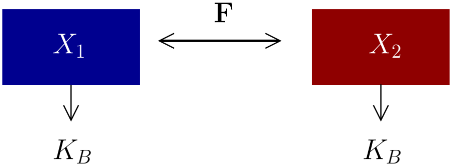
One-bit Oblivious Transfer

Converse for oblivious transfer

Reduction of SK Agreement to OT

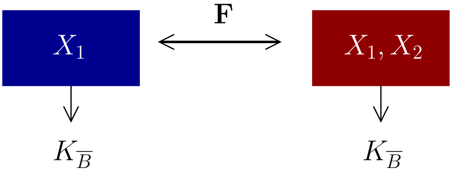
We bound the length of OT by reducing it to SK

Reduction 1:

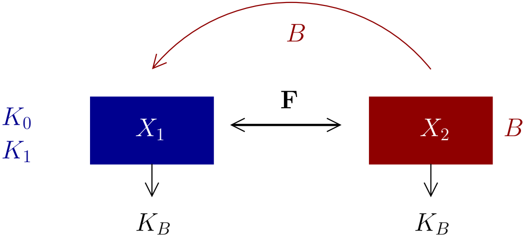


Reduction 2:

Eavesdropper observes X_2



Reduction 1 of SK Agreement to OT

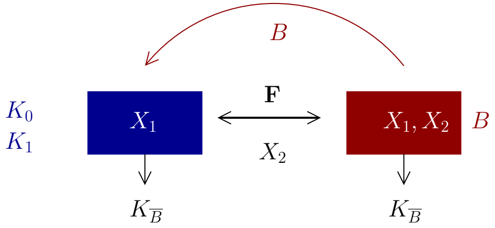


$(\epsilon, \delta_1, \delta_2)$-OT of length l yields $(\epsilon + \delta_1 + 2\delta_2)$-OT of length l

Using the conditional independence testing bound:

$$l \leq S_{\epsilon+\delta_1+2\delta_2}(X_1, X_2) \lesssim -\log \beta_{\epsilon+\delta_1+2\delta_2}\left(\mathrm{P}_{X_1X_2}, \mathrm{P}_{X_1}\mathrm{P}_{X_2}\right)$$

Reduction 2 of SK Agreement to OT



1. Party 2 simulates $\tilde{X}_2$ pretending that it observed $\overline{B}$
2. It estimates $\hat{K}$ from $(\tilde{X}_2, \overline{B})$ instead of (X_2, B)

$(\epsilon, \delta_1, \delta_2)$-OT of length l yields $(\epsilon + \delta_1 + 4\delta_2)$-OT of length l

$$
\begin{aligned}
l &\leq S_{\epsilon+\delta_1+4\delta_2}(X_1, (X_1, X_2)|X_2) \\
&\lesssim -\log \beta_{\epsilon+\delta_1+4\delta_2}\left(\mathrm{P}_{X_1 X_1 X_2}, \mathrm{P}_{X_1|X_2}\mathrm{P}_{X_1|X_2}\mathrm{P}_{X_2}\right)
\end{aligned}
$$

Bounds on the Efficiency of OT

Theorem

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

$$l \lesssim -\log \beta_{\epsilon+\delta_1+2\delta_2} \left(\mathrm{P}_{X_1X_2}, \mathrm{P}_{X_1}\mathrm{P}_{X_2}\right)$$

$$l \lesssim -\log \beta_{\epsilon+\delta_1+4\delta_2} \left(\mathrm{P}_{X_1X_1X_2}, \mathrm{P}_{X_1|X_2}\mathrm{P}_{X_1|X_2}\mathrm{P}_{X_2}\right)$$

OT Capacity (for IID observations):

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

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

"Strong" version of the Ahlswede-Csiszár upper bound

Bit Commitment

Chess Players' Dilemma

[Blum 82], ..., [Nascimento-Winters-Imai 03]

If I make the last move, you will get the whole night to think!

Chess Players' Dilemma

[Blum 82], ..., [Nascimento-Winters-Imai 03]

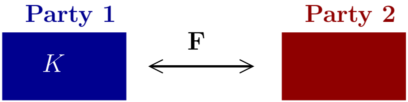
If I make the last move, you will get the whole night to think!

Zero-knowledge proofs, authentication, verifiable secret sharing, ...

Bit Commitment

[Blum 82], ..., [Nascimento-Winters-Imai 03]

Commit Phase



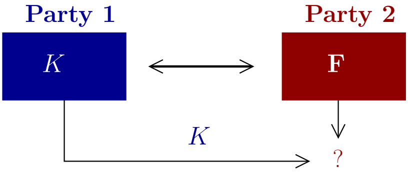
Party 1 has an l-bit message K

K must remain concealed fom party 2

Bit Commitment

[Blum 82], ..., [Nascimento-Winters-Imai 03]

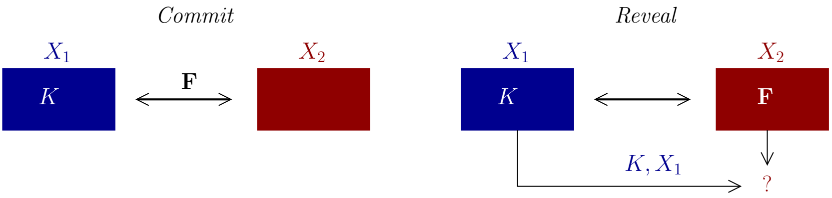
Reveal Phase



K must be reliably recoverable

Party 1 should not be able to cheat

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

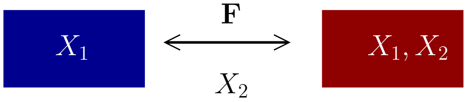
Binding: $\mathrm{P}\left(T(K', X_1', X_2, \mathbf{F}) = 0, K' \neq K\right) \leq \delta_2$

Converse for bit commitment

Bound on the Efficiency of BC

[Imai-Morozov-Nascimento-Winter 06]

Reduction of SK generation to OT



Theorem

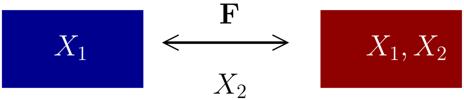
For an $(\epsilon, \delta_1, \delta_2)$-BC of length l,

$$l \lesssim -\log \beta_{\epsilon+\delta_1+\delta_2}\left(\mathrm{P}_{X_1 X_1 X_2}, \mathrm{P}_{X_1|X_2}\mathrm{P}_{X_1|X_2}\mathrm{P}_{X_2}\right)$$

Bound on the Efficiency of BC

[Imai-Morozov-Nascimento-Winter 06]

Reduction of SK generation to OT



Theorem

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

$$l \lesssim -\log \beta_{\epsilon+\delta_1+\delta_2}\left(\mathrm{P}_{X_1 X_1 X_2}, \mathrm{P}_{X_1|X_2}\mathrm{P}_{X_1|X_2}\mathrm{P}_{X_2}\right)$$

Example: Constructing BC from n-length OT

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

In Closing ...

Our converse results give us a tool to evaluating the performance of various information theoretic cryptography primitives

For other implications:

H. Tyagi and S. Watanabe, "A bound for multiparty secret key agreement and implications for a problem of secure computing," EUROCRYPT, 2014

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

How close to optimal can we get with efficient schemes?