One-Way Secret-Key Agreement and Applications to Circuit Polarization and Immunization of Public-Key Encryption

Thomas Holenstein and Renato Renner

Department of Computer Science
Swiss Federal Institute of Technology (ETH)
Zürich, Switzerland

August 18, 2005

Focus of this Talk

- Information theoretically secure one-way secret-key agreement.
- A special class of random variables.
- Circuit polarization.

Setting

Alice $\qquad\qquad\qquad\qquad$ Bob

$X_1, \ldots, X_n \quad \longrightarrow \quad Y_1, \ldots, Y_n$

Eve

$Z_1, \ldots, Z_n$

Setting

Alice

$X_1, \ldots, X_n$

S_A

M $\longrightarrow$

Bob

$Y_1, \ldots, Y_n$

S_B

Eve

$Z_1, \ldots, Z_n$

Setting

Alice

$X_1, \ldots, X_n$

S_A

$\xrightarrow{\quad M \quad}$

Bob

$Y_1, \ldots, Y_n$

S_B

Eve

$Z_1, \ldots, Z_n$

$\Pr[S_A = S_B] \geq 1 - 2^{-k}$

Given $M, Z_1, \ldots, Z_n$:
$\Delta(S_A, U) \leq 2^{-k}$

Example

Alice $\qquad\qquad\qquad\qquad$ Bob

$0\,1\,0\,1\,1\,1\,0 \longrightarrow 0\,1 \star 1 \star 1\,0$

Eve

$\star 1\,0 \star 1 \star \star \star$

Example

Alice

0 1 0 1 1 1 0

$C \leftarrow_R$ Code

$\xrightarrow{(0\,1\,0\,1\,1\,1\,0) \oplus C}$

Bob

$0\,1 \star 1 \star 1\,0$

Eve

$\star 1\,0 \star 1 \star \star \star$

Example

Alice		Bob
0 1 0 1 1 1 0	$\xrightarrow{(0\,1\,0\,1\,1\,1\,0) \oplus C}$	$0\,1 \star 1 \star 1\,0$
$C \leftarrow_R$ Code		

Eve

$\star 1\,0 \star 1 \star \star \star$

Bob can find C, Eve still has some uncertainity about C.

Example

Alice

0 1 0 1 1 1 0

$C \leftarrow_R$ Code

S_A

$\xrightarrow{(0\,1\,0\,1\,1\,1\,0) \oplus C,\ \text{Seed}}$

Bob

$0\,1 \star 1 \star 1\,0$

S_B

Eve

$\star 1\,0 \star 1 \star \star \star$

Bob can find C, Eve still has some uncertainity about C.

Alice and Bob apply a strong extractor to C to get the key.

One-Way Key Rate

If $H(X|Z) > H(X|Y)$, then one-way key agreement is possible:

One-Way Key Rate

If $H(X|Z) > H(X|Y)$, then one-way key agreement is possible:

Information Reconciliation
: Use enough instances of the random variables and an appropriate error correcting code with rate close to the capacity. This gives Alice and Bob a common string with some privacy.

One-Way Key Rate

If $H(X|Z) > H(X|Y)$, then one-way key agreement is possible:

Information Reconciliation
: Use enough instances of the random variables and an appropriate error correcting code with rate close to the capacity. This gives Alice and Bob a common string with some privacy.

Privacy Amplification
: Use an extractor to extract the key.

One-Way Key Rate

If $H(X|Z) > H(X|Y)$, then one-way key agreement is possible:

Information Reconciliation
: Use enough instances of the random variables and an appropriate error correcting code with rate close to the capacity. This gives Alice and Bob a common string with some privacy.

Privacy Amplification
: Use an extractor to extract the key.

Rate achieved with this protocol: $H(X|Z) - H(X|Y)$.

Preprocessing Helps

$H(X|Z) > H(X|Y)$ is *not* a necessary condition:

X	Y	Z
00	0	0
01	0	1
10	1	0
11	1	1

$$H(X|Z) = H(X|Y) = 1.$$

Preprocessing Helps

$H(X|Z) > H(X|Y)$ is *not* a necessary condition:

X	Y	Z
00	0	0
01	0	1
10	1	0
11	1	1

$$H(X|Z) = H(X|Y) = 1.$$

Forgetting helps: Alice forgets the second bit, gets U:

$$H(U|Z) = 1, \quad H(U|Y) = 0.$$

Preprocessing Helps

$H(X|Z) > H(X|Y)$ is *not* a necessary condition:

X	Y	Z
00	0	0
01	0	1
10	1	0
11	1	1

$$H(X|Z) = H(X|Y) = 1.$$

Forgetting helps: Alice forgets the second bit, gets U:

$$H(U|Z) = 1, \quad H(U|Y) = 0.$$

Sending helps: Alice sends the second bit (V) to Bob:

$$H(X|ZV) = 1, \quad H(X|YV) = 0.$$

Preprocessing Helps

Forgetting and sending is sufficient:

Theorem (Ahlswede, Csiszár, 1993)

The key rate for one-way communication is

$$S_{\rightarrow}(X;Y|Z) = \max_{(U,V)\leftrightarrow X \leftrightarrow YZ} H(U|ZV) - H(U|YV).$$

Preprocessing Helps

Forgetting and sending is sufficient:

Theorem (Ahlswede, Csiszár, 1993)

The key rate for one-way communication is

$$S_{\rightarrow}(X;Y|Z) = \max_{(U,V)\leftrightarrow X \leftrightarrow YZ} H(U|ZV) - H(U|YV).$$

A proof of optimality can be found in [AC93] and is sketched in the paper.

Preprocessing Helps

Forgetting and sending is sufficient:

Theorem (Ahlswede, Csiszár, 1993)

The key rate for one-way communication is

$$S_{\rightarrow}(X;Y|Z) = \max_{(U,V)\leftrightarrow X\leftrightarrow YZ} H(U|ZV) - H(U|YV).$$

A proof of optimality can be found in [AC93] and is sketched in the paper.

(Remark: In the paper it is also shown how this rate can be achieved with poly-time Alice and Bob.)

A Class of Random Variables: $\mathcal{D}(\alpha, \beta)$

- Alice and Bob have bits X and Y with correlation α:

$$\Pr[X = Y] \geq \frac{1+\alpha}{2}.$$

A Class of Random Variables: $\mathcal{D}(\alpha, \beta)$

- Alice and Bob have bits X and Y with correlation α:

$$\Pr[X = Y] \geq \frac{1+\alpha}{2}\,.$$

- With probability β, Information about X is leaked to Eve. Otherwise, Eve *stays ignorant*.

A Class of Random Variables: $\mathcal{D}(\alpha, \beta)$

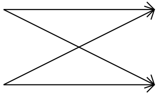
- Alice and Bob have bits X and Y with correlation α:

$$\Pr[X = Y] \geq \frac{1+\alpha}{2} .$$

- With probability β, Information about X is leaked to Eve. Otherwise, Eve *stays ignorant*.

Standard Example:

$X \in_R \{0,1\}$



$Y \in \{0,1\}$

$$p_{\text{flip}} = \frac{1-\alpha}{2}$$

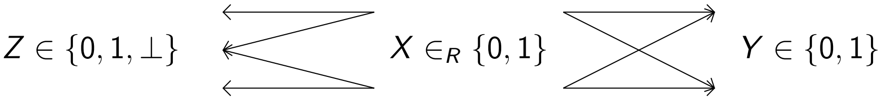
A Class of Random Variables: $\mathcal{D}(\alpha, \beta)$

- Alice and Bob have bits X and Y with correlation α:

$$\Pr[X = Y] \geq \frac{1+\alpha}{2} .$$

- With probability β, Information about X is leaked to Eve. Otherwise, Eve *stays ignorant*.

Standard Example:



$p_{\text{erasure}} = 1 - \beta$ $\qquad$ $p_{\text{flip}} = \frac{1-\alpha}{2}$

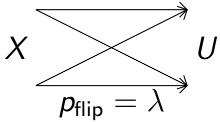
Key-Rate for the Class $\mathcal{D}(\alpha, \beta)$

Let $P_{XYZ} \in \mathcal{D}(\alpha, \beta)$ be α-correleated, leakage β. Can "forgetting" increase $H(U|ZV) - H(U|YV)$?

Key-Rate for the Class $\mathcal{D}(\alpha, \beta)$

Let $P_{XYZ} \in \mathcal{D}(\alpha, \beta)$ be α-correleated, leakage β. Can "forgetting" increase $H(U|ZV) - H(U|YV)$?

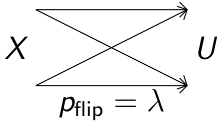
Yes:



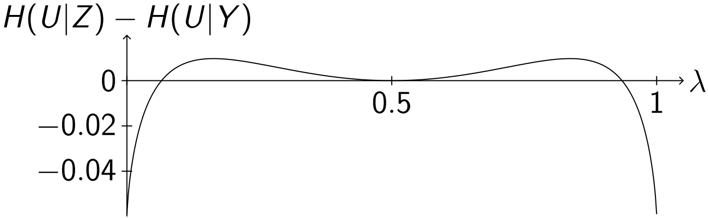
Key-Rate for the Class $\mathcal{D}(\alpha, \beta)$

Let $P_{XYZ} \in \mathcal{D}(\alpha, \beta)$ be α-correleated, leakage β. Can "forgetting" increase $H(U|ZV) - H(U|YV)$?

Yes:



Example: $(\alpha = 0.8,\ \beta = 0.59)$



Key-Rate for the Class $\mathcal{D}(\alpha, \beta)$

If Alice gets a random bit, Bob a "binary symmetric" noisy version, Eve an "erasure channel" noisy version, then adding noise hurts Eve more than Bob, i.e., increases $H(U|ZV) - H(U|YV)$.

Key-Rate for the Class $\mathcal{D}(\alpha, \beta)$

If Alice gets a random bit, Bob a "binary symmetric" noisy version, Eve an "erasure channel" noisy version, then adding noise hurts Eve more than Bob, i.e., increases $H(U|ZV) - H(U|YV)$.

Question: Can we do better than this?

Key-Rate for the Class $\mathcal{D}(\alpha, \beta)$

If Alice gets a random bit, Bob a "binary symmetric" noisy version, Eve an "erasure channel" noisy version, then adding noise hurts Eve more than Bob, i.e., increases $H(U|ZV) - H(U|YV)$.

Question: Can we do better than this?

Answer: No. Use

$$H(U|ZV) - H(U|YV) = \\ H(Z|UV) - H(Y|UV) - (H(Z|V) - H(Y|V)),$$

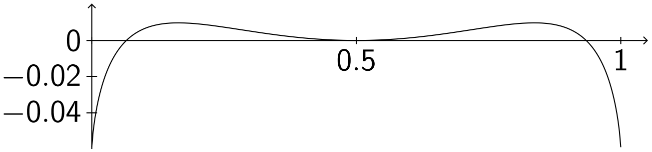
to prove optimality (see paper for details).

Key-Rate for the Class $\mathcal{D}(\alpha, \beta)$

Theorem

For α-correlated random variables which leak information with probability β the key rate is:

$$S_{\rightarrow}(X; Y|Z) = \begin{cases} \max_{\lambda} g_{\alpha,\beta}(\lambda) \geq \frac{(\alpha^2-\beta)^2}{7} & \alpha^2 > \beta \\ 0 & \textit{otherwise.} \end{cases}$$



$g_{\alpha,\beta}(\lambda) \qquad \alpha = 0.8, \beta = 0.59$

Honest Verifier Statistical Zero Knowledge

Zero Knowledge Proof of Graph-Nonisomorphism

G_0 G_1

Honest Verifier Statistical Zero Knowledge

Zero Knowledge Proof of Graph-Nonisomorphism

Verifier — **Prover**

Choose π, b

$\pi(G_b)$ →

Find b

← b

Check answer

HVSZK: Circuits

Consider the following circuits:

C_0 :	Input: Randomness.	Output: A permutation of G_0
C_1 :	Input: Randomness.	Output: A permutation of G_1

HVSZK: Circuits

Consider the following circuits:

C_0 : Input: Randomness. Output: A permutation of G_0

C_1 : Input: Randomness. Output: A permutation of G_1

$$G_0 \ncong G_1 \quad \Rightarrow \quad \Delta(C_0, C_1) = 1$$

$$G_0 \cong G_1 \quad \Rightarrow \quad \Delta(C_0, C_1) = 0$$

HVSZK: Circuits

Theorem (Sahai, Vadhan)

Any promise problem in HVSZK can be mapped to a pair of circuits (C_0, C_1) *such that:*

- *For yes-instances:* $\Delta(C_0, C_1) \geq 1 - 2^{-k}$.
- *For no-instances:* $\Delta(C_0, C_1) \leq 2^{-k}$.

HVSZK: Circuits

Theorem (Sahai, Vadhan)

Any promise problem in HVSZK can be mapped to a pair of circuits (C_0, C_1) *such that:*

- *For yes-instances:* $\Delta(C_0, C_1) \geq 1 - 2^{-k}$.
- *For no-instances:* $\Delta(C_0, C_1) \leq 2^{-k}$.

The proof first constructs circuits with

- Yes-instances: $\Delta(C_0, C_1) \geq \alpha$.
- No-instances: $\Delta(C_0, C_1) \leq \beta$.

and then *polarizes* these circuits.

A HVSZK-Protocol for $\Delta(C_0, C_1) \geq \alpha$

Given: pair (C_0, C_1) such that

- $\Delta(C_0, C_1) \geq \alpha$ or
- $\Delta(C_0, C_1) \leq \beta$,

where $\alpha^2 > \beta$.

A HVSZK-Protocol for $\Delta(C_0, C_1) \geq \alpha$

Given: pair (C_0, C_1) such that

- $\Delta(C_0, C_1) \geq \alpha$ or
- $\Delta(C_0, C_1) \leq \beta$,

where $\alpha^2 > \beta$.

Verifier		**Prover**
Choose $X_1, \ldots, X_n$	$C_{X_1}, \ldots C_{X_n}$ $\longrightarrow$	Find $Y_1, \ldots, Y_n$
	$\text{OWSKA}(X_1, \ldots, X_n)$ $\longrightarrow$	Find S_B
Check if $S_A = S_B$	$\longleftarrow$ S_B	

Circuit Polarization and OWSKA

Theorem

Oblivious circuit polarization and OWSKA for $\mathcal{D}(\alpha, \beta)$ is equivalent.

Circuit Polarization and OWSKA

Theorem

Oblivious circuit polarization and OWSKA for $\mathcal{D}(\alpha, \beta)$ is equivalent.

Proof:

- OWSKA implies (oblivious) circuit polarization (as above).
- Oblivious circuit polarization implies OWSKA (similar).

Circuit Polarization and OWSKA

Theorem

Oblivious circuit polarization and OWSKA for $\mathcal{D}(\alpha, \beta)$ is equivalent.

Proof:

- OWSKA implies (oblivious) circuit polarization (as above).
- Oblivious circuit polarization implies OWSKA (similar).

Corollary

Oblivious circuit polarization is possible if and only if $\alpha^2 > \beta$.

Circuit Polarization and OWSKA

Theorem

Oblivious circuit polarization and OWSKA for $\mathcal{D}(\alpha, \beta)$ is equivalent.

Proof:

- OWSKA implies (oblivious) circuit polarization (as above).
- Oblivious circuit polarization implies OWSKA (similar).

Corollary

Oblivious circuit polarization is possible if and only if $\alpha^2 > \beta$.

Notes:

- Conjectured in Vadhan's PhD thesis.
- Does not hold for *non-oblivious* polarization.

Conclusions

- One-way secret-key agreement for α-correlated random variables with leakage β is possible if and only if $\alpha^2 > \beta$.

Conclusions

- One-way secret-key agreement for α-correlated random variables with leakage β is possible if and only if $\alpha^2 > \beta$.
- Oblivious circuit polarization *is the same* as one-way secret-key agreement for α-correlated random variables with leakage β.

Conclusions

- One-way secret-key agreement for α-correlated random variables with leakage β is possible if and only if $\alpha^2 > \beta$.
- Oblivious circuit polarization *is the same* as one-way secret-key agreement for α-correlated random variables with leakage β.
- Also in the paper: immunization of public-key bit encryption schemes (cf. [Dwork, Naor, Reingold, EC 04] – this paper is also the origin of OWSKA/Polarization-equivalence).

Conclusions

- One-way secret-key agreement for α-correlated random variables with leakage β is possible if and only if $\alpha^2 > \beta$.
- Oblivious circuit polarization *is the same* as one-way secret-key agreement for α-correlated random variables with leakage β.
- Also in the paper: immunization of public-key bit encryption schemes (cf. [Dwork, Naor, Reingold, EC 04] – this paper is also the origin of OWSKA/Polarization-equivalence).
- Security proof of the OWSKA protocol in the paper uses smooth Rényi-entropy [cf. Renner, Wolf, AC 05].