Efficient One-Way Secret-Key Agreement and Private Channel Coding via Polarization

Joseph M. Renes, Renato Renner, David Sutter

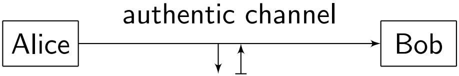
Institute for Theoretical Physics

ASIACRYPT 2013, Bangalore

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

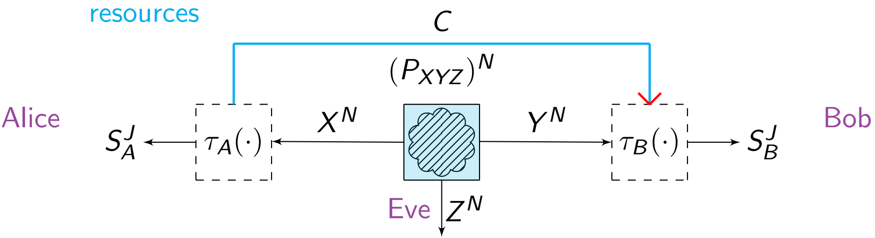
Information Theoretic Cryptography

Goal: information-theoretically secure private communication



- impossible [Shannon'48]
- possible when assuming correlated randomness [Maurer'93]
  - one-way secret key agreement
  - private channel coding over a wiretap channel

One-Way Secret-Key Agreement (SKA)

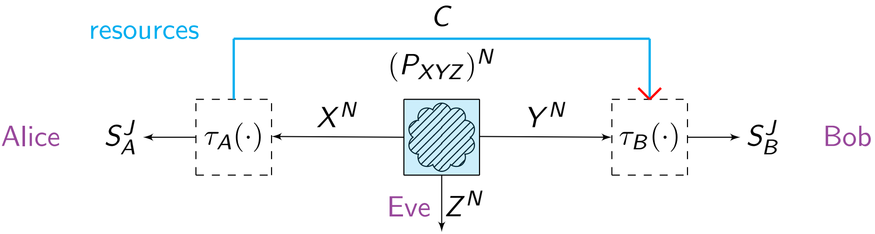


- reliability $\lim_{J\to\infty} \Pr\left[S_A^J \neq S_B^J\right] = 0$

uniformly distributed

- (strong) secrecy $\lim_{N\to\infty} \| P_{S_A^J, Z^N, C} - \boxed{\overline{P}_{S_A^J}} \times P_{Z^N, C} \|_1 = 0$

One-Way Secret-Key Agreement (SKA)



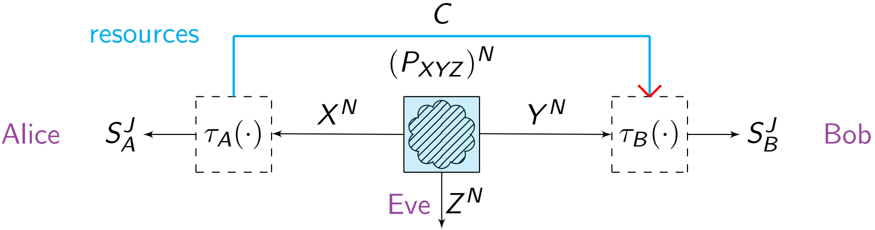
- reliability $\lim_{J\to\infty} \Pr\left[S_A^J \neq S_B^J\right] = 0$
- (strong) secrecy $\lim_{N\to\infty} \| P_{S_A^J, Z^N, C} - \boxed{\overline{P}_{S_A^J}} \times P_{Z^N, C} \|_1 = 0$ uniformly distributed

Historically

- (weak) secrecy $\lim_{N\to\infty} \frac{1}{N} I\left(S_A^J; Z^N, C\right) = 0$ insufficient [Maurer&Wolf'00]
- (strong) secrecy $\lim_{N\to\infty} I\left(S_A^J; Z^N, C\right) = 0$

$$\lim_{N\to\infty} \delta\left(P_{S_A^J}, \overline{P}_{S_A^J}\right) = 0$$

One-Way Secret-Key Agreement (SKA)



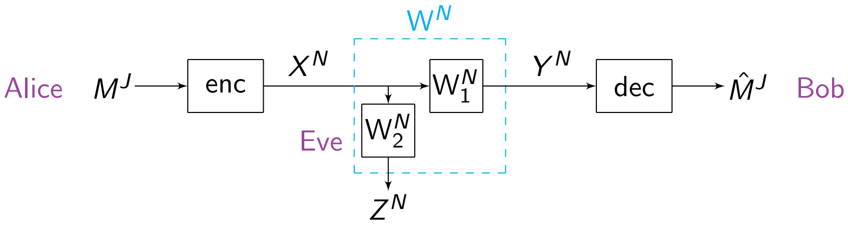
- reliability $\lim_{J\to\infty} \Pr\left[S_A^J \neq S_B^J\right] = 0$
- (strong) secrecy $\lim_{N\to\infty} \| P_{S_A^J, Z^N, C} - \boxed{\overline{P}_{S_A^J}} \times P_{Z^N, C} \|_1 = 0$

uniformly distributed

Thm[Csiszár&Körner'78]**:** One-way secret-key rate

$$S_\rightarrow(X;Y|Z) = \begin{cases} \max\limits_{P_{U,V}} & H(U|Z,V) - H(U|Y,V) \\ \text{s.t.} & V \multimap U \multimap X \multimap (Y,Z), \\ & |\mathcal{V}| \leqslant |\mathcal{X}|,\ |\mathcal{U}| \leqslant |\mathcal{X}|^2. \end{cases}$$

Private Channel Coding (PCC)



- reliability $\lim_{J\to\infty} \Pr\left[M^J \neq \hat{M}^J\right] = 0$
- (strong) secrecy $\lim_{N\to\infty} \|P_{M^J,Z^N,C} - P_{M^J} \times P_{Z^N,C}\|_1 = 0$

Thm[Csiszár&Körner'78]**:** Secrecy capacity

$$C_s = \begin{cases} \max\limits_{P_{V,X}} & H(V|Z) - H(V|Y) \\ \text{s.t.} & V \multimap X \multimap (Y,Z), \\ & |\mathcal{V}| \leqslant |\mathcal{X}|. \end{cases}$$

Efficient, Optimal Protocols

essentially linear complexity

- efficient $\neq$ practically efficient
- optimal $=$ achieve the highest possible rate
- (practically) efficient one-way secret-key agreement
  - only weak secrecy, degradability assumptions [Abbe'12]
  - shared key, degradability assumptions [Chou *et al.*'13]
- (practically) efficient private channel coding
  - only weak secrecy, degradability assumptions [Mahdavifar&Vardy'11]
  - binary symmetric wiretap channels (degradablity?!) [Bellare *et al.*'12]
  - degraded wiretap channels [Sasoglu&Vardy'13]

Efficient, Optimal Protocols

essentially linear complexity

- efficient $\neq$ practically efficient
- optimal = achieve the highest possible rate
- (practically) efficient one-way secret-key agreement
  - only weak secrecy, degradability assumptions [Abbe'12]
  - shared key, degradability assumptions [Chou *et al.*'13]
- (practically) efficient private channel coding
  - only weak secrecy, degradability assumptions [Mahdavifar&Vardy'11]
  - binary symmetric wiretap channels (degradablity?!) [Bellare *et al.*'12]
  - degraded wiretap channels [Sasoglu&Vardy'13]

getting rid of these assumptions

Polarization Phenomenon - Polar Codes

polar transform

- let $(X^N, Y^N) \sim (P_{X,Y})^N$
  let $U^N = G_N X^N$, where $\boxed{G_N} := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\otimes \log N}$
- For $\epsilon \in (0,1)$, define a high- and a low-entropy set

$$\mathcal{R}_\epsilon^N(X|Y) := \left\{ i \in [N] : H\left(U_i \middle| U^{i-1}, Y^N\right) \geqslant 1 - \epsilon \right\}$$
$$\mathcal{D}_\epsilon^N(X|Y) := \left\{ i \in [N] : H\left(U_i \middle| U^{i-1}, Y^N\right) \leqslant \epsilon \right\}$$

Polarization Phenomenon - Polar Codes

- let $(X^N, Y^N) \sim (P_{X,Y})^N$ polar transform
  let $U^N = G_N X^N$, where $G_N := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\otimes \log N}$
- For $\epsilon \in (0,1)$, define a high- and a low-entropy set

$$\mathcal{R}_\epsilon^N(X|Y) := \left\{ i \in [N] : H\left(U_i \middle| U^{i-1}, Y^N\right) \geqslant 1 - \epsilon \right\}$$
$$\mathcal{D}_\epsilon^N(X|Y) := \left\{ i \in [N] : H\left(U_i \middle| U^{i-1}, Y^N\right) \leqslant \epsilon \right\}$$

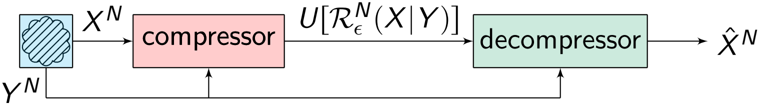
Thm[Arıkan'09]**:** Polarization Phenomenon: For any $\epsilon \in (0,1)$

$$\lim_{N\to\infty} \frac{|\mathcal{R}_\epsilon^N(X|Y)|}{N} = H(X|Y) \text{ and } \lim_{N\to\infty} \frac{|\mathcal{D}_\epsilon^N(X|Y)|}{N} = 1 - H(X|Y)$$

- Heart of polar codes (for source and channel coding)

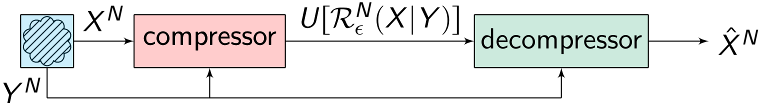
Optimal Lossless Source Coding Using Polar Codes

Task: compress X^N w.r.t. side information Y^N



Optimal Lossless Source Coding Using Polar Codes

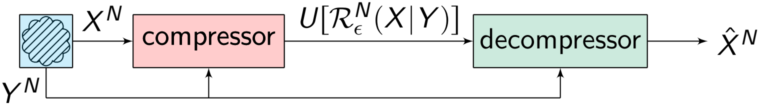
Task: compress X^N w.r.t. side information Y^N



- compression
  - $U^N = G_N X^N$
  - take only $U[\mathcal{R}_\epsilon^N(X|Y)]$
- decompression
  - Likelihood estimation using side information Y^N

Optimal Lossless Source Coding Using Polar Codes

Task: compress X^N w.r.t. side information Y^N



- compression
  - $U^N = G_N X^N$
  - take only $U[\mathcal{R}_\epsilon^N(X|Y)]$

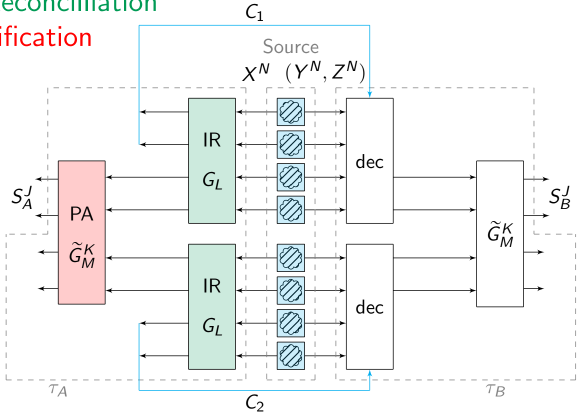
$O(N \log N)$

- decompression
  - Likelihood estimation using side information Y^N
- reliable[Arıkan'10] $\Pr\left[X^N \neq \hat{X}^N\right] = O(2^{-N^\beta})$ for $\beta < \frac{1}{2}$
- optimal [Slepian&Wolf'73], $H(X|Y) = \lim_{N\to\infty} \frac{1}{N}|\mathcal{R}_\epsilon^N(X|Y)|$

One-Way Secret-Key Agreement Protocol (M=2, L=4)

Information Reconcilliation

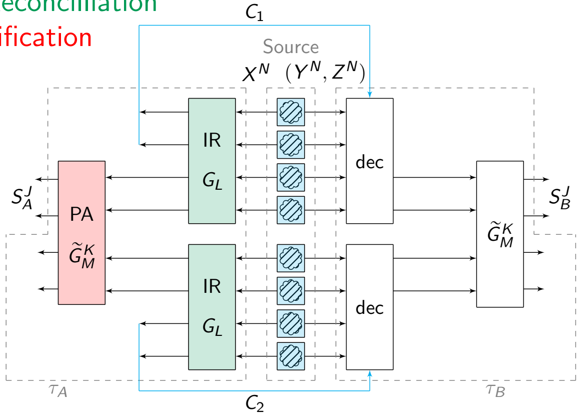
Privacy Amplification



One-Way Secret-Key Agreement Protocol (M=2, L=4)

Information Reconcilliation

Privacy Amplification



- no degradability assumptions
- no shared key needed

One-Way Secret-Key Agreement Characteristics

For any $\beta < \frac{1}{2}$

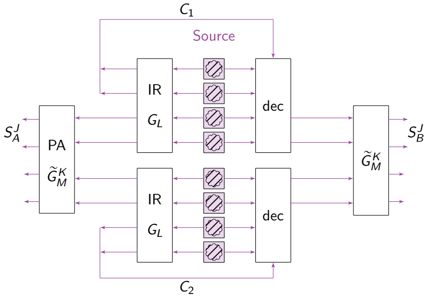
- Reliability: $\Pr\left[S_A^J \neq S_B^J\right] = O\left(M 2^{-L^{\beta}}\right)$
- Secrecy: $\left\| P_{S_A^J, Z^N, C} - \overline{P}_{S_A^J} \times P_{Z^N, C} \right\|_1 = O\left(\sqrt{N} 2^{-\frac{N^{\beta}}{2}}\right)$
- Rate: $R := \frac{J}{N} \geqslant \max\left\{0, H(X|Z) - H(X|Y) - \frac{o(N)}{N}\right\}$
- Complexity: $O(N \log N)$

M = # inner blocks

L = # inputs per inner block

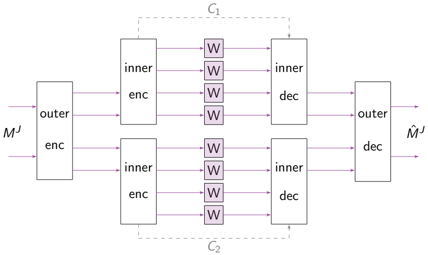
N = ML (blocklength)

Private Channel Coding (L = 4, M = 2)



Source

Secret-key agreement

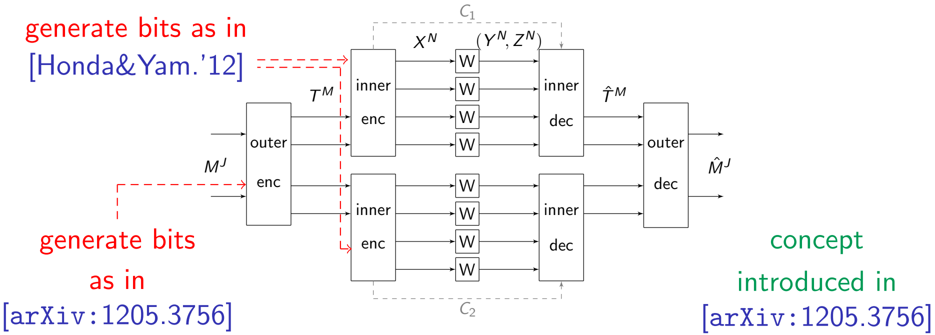


s

Private channel coding

Wiretap channel

Private Channel Coding ($L = 4$, $M = 2$)



- Run secret-key agreement scheme in reverse
- Mimic redundant bits
- Approx. of the secret-key agreement scenario (*shaping*) → same decoder can be used

Private Channel Coding: Characteristics

For any $\beta < \frac{1}{2}$

- Reliability: $\Pr\left[M^J \neq \hat{M}^J\right] = O\left(M2^{-L^\beta}\right)$
- Secrecy: $\|P_{M^J,Z^N,C} - \bar{P}_{M^J} \times P_{Z^N,C}\|_1 = O\left(\sqrt{N}2^{-\frac{N^\beta}{2}}\right)$
- Rate: $R \geqslant \max\left\{0, H(X|Z) - H(X|Y) - \frac{o(N)}{N}\right\}$
- Complexity: $O(N \log N)$

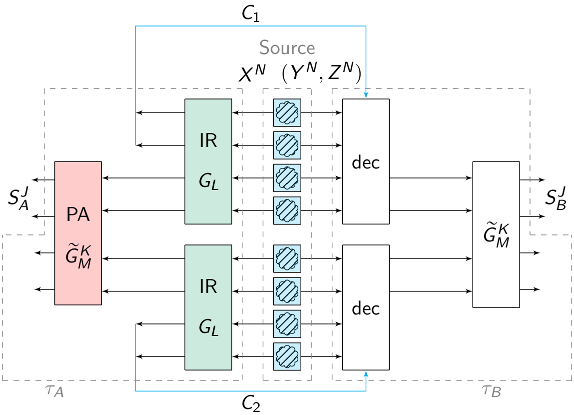
M = # inner blocks
L = # inputs per inner block
N = ML (blocklength)

Summary

One-way secret-key agreement and private channel coding

- at the optimal rate
- strong secrecy
- $O(N \log N)$ computational complexity
- no degradability assumptions
- no preshared key

Code Construction



Find index set at IR and PA layer

- IR: can be done in linear time [Tal&Vardy'11]
- PA: not fully solved yet