

Rate-Adaptive Reconciliation

Grupo de Investigación en
Información y Computación Cuántica

<http://gcc.ls.fi.upm.es/>

Facultad de Informática
Universidad Politécnica de Madrid

QUITEMAD Workshop

Outline

- 1 Secret Key Agreement
- 2 Information Reconciliation
- 3 Rate Adaptive Protocol for Information Reconciliation

Information Theoretic Secret Key Agreement

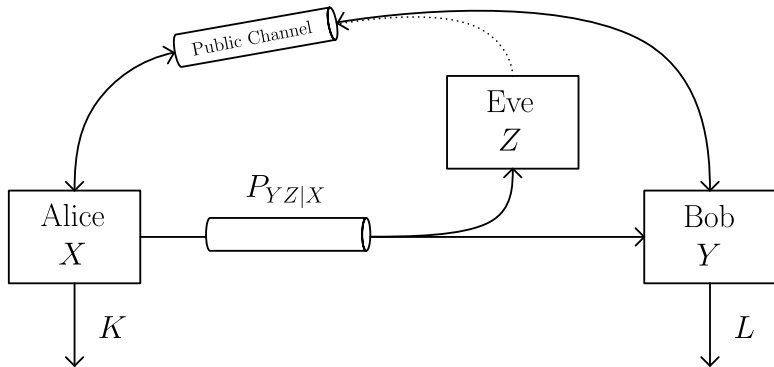


Figure: Channel type model with wiretapper (Ahlswede and Csiszar 1993)

Secret Key Agreement: A two step approach

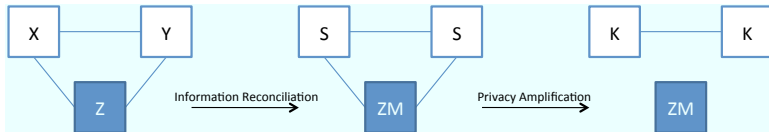


Figure: Variable relations in each step of the key distillation process (Van Assche 2004)

Information Reconciliation as Source Coding with Side Information

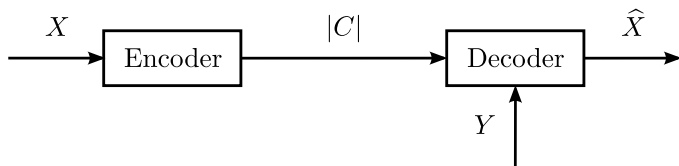


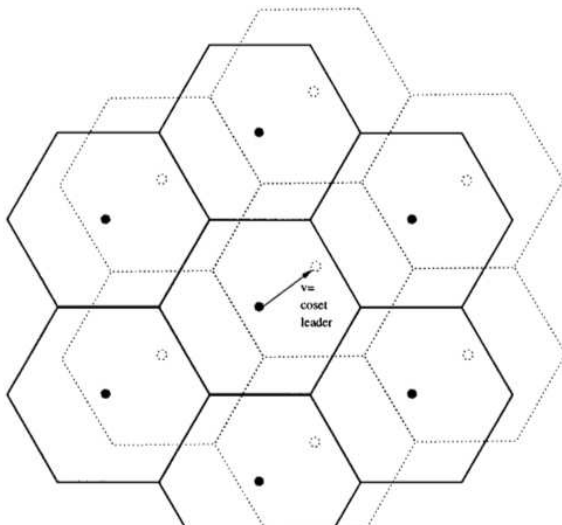
Figure: Source coding with side information.

Definition

Information Reconciliation Efficiency

$$f = \frac{|C|}{H(X|Y)} \geq 1$$

Syndrome Coding



Constraints: no interactivity

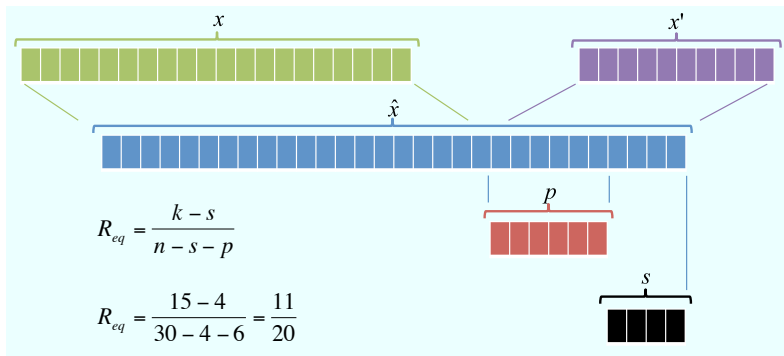
Acts on packets of the same length

Rate-adaptive with maximum granularity

Uses one LDPC code

No interactivity

Solution



Protocol

Alice and Bob have a code of size $|\hat{x}|$ and an accurate estimate of p_{err} .

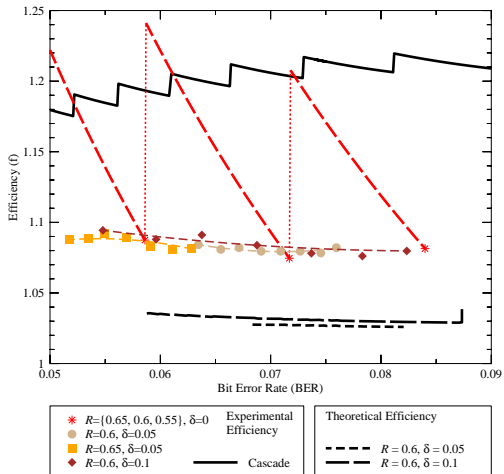
Alice:

- 1 Creates the extended string $\hat{x} = x|s|p_A$
- 2 Transmits $s(\hat{x})|s$




Bob:

- 3 Creates the extended string $\hat{y} = y|s|p_B$
- 4 Tries to decode \hat{x}

Simulation Results



Bibliography

-  D. Elkouss, J. Martínez, D. Lancho and V. Martín.
Rate Compatible Protocol for Information Reconciliation:
An application to QKD.
IEEE Information Theory Workshop, pp. 145-149, 2010.
-  D. Elkouss, J. Martínez, D. Lancho and V. Martín.
Método de reconciliación de información para QKD
mediante el uso de códigos LDPC adaptando la tasa de
información
Patent P201030099.
-  D. Elkouss, J. Martínez and V. Martín.
Efficient Reconciliation with Rate Adaptive Codes in
Quantum Key Distribution
Quantum Information and Computation, pp. 226-238, 2011.

Constraints: interactivity

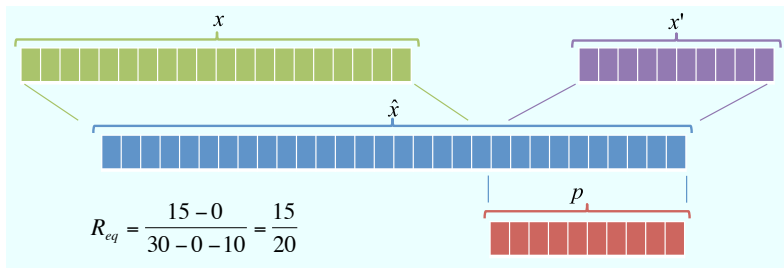
Acts on packets of the same length

Rate-adaptive with maximum granularity

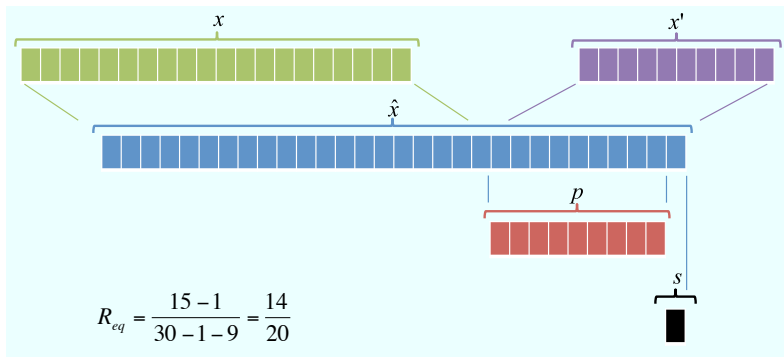
Uses one LDPC code

Some interactivity allowed

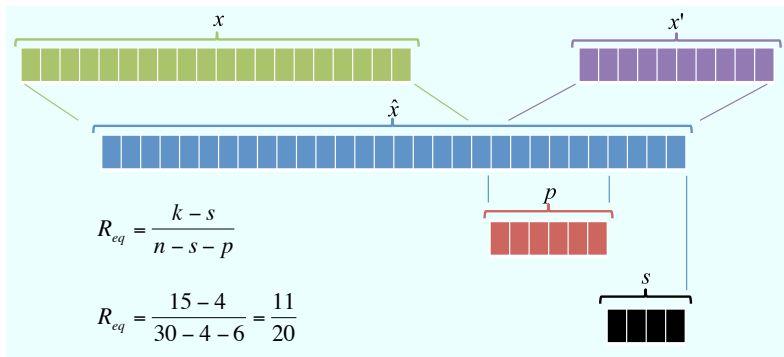
Solution



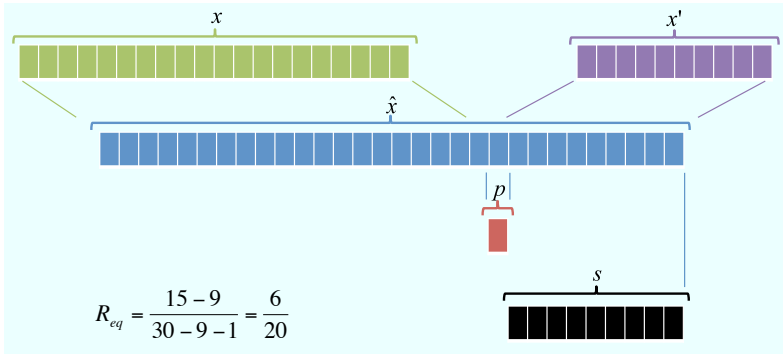
Solution



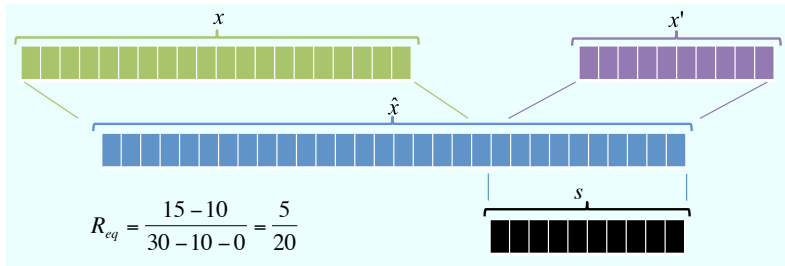
Solution



Solution



Solution



Protocol

Bob:

- 3 Creates the extended string $\hat{y} = y|s|p_B$
- 4 Tries to decode \hat{x}
- 5 Transmits the result to Alice

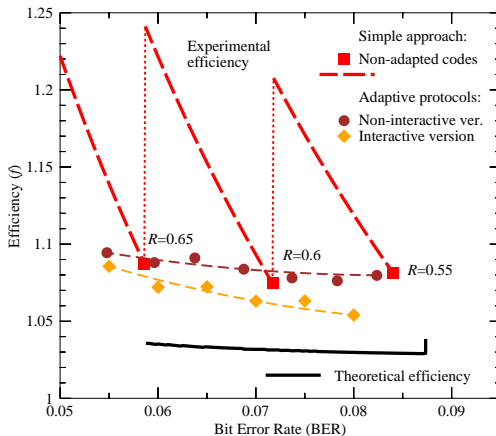
Alice:

- 6 If successful decoding \Rightarrow end
- 7 Transmits s'

Bob:

- 3 Creates the extended string $\hat{y} = y|s|p_B$
- 4 ...

Simulation Results



Bibliography



J. Martínez, D. Elkouss and V. Martín.

Interactive Reconciliation with Low-Density Parity-Check Codes.

6th Int. Symposium on Turbo Codes & Iterative Information Processing, pp. 280-284, 2010.

Summary

The efficiency of Information Reconciliation has a strong impact on the size of the final secret key

Error correcting codes are a good solution to the problem

We propose a rate compatible solution with the same efficiency as adapted codes