

Quantum Cryptography with Finite Resources

Valerio Scarani

Centre for Quantum Technologies, National University of Singapore

Renato Renner

Institute for Theoretical Physics, ETH Zurich

Introduction

The issue at stake

Secret key rate:

$$r = S(A | E) - H(A | B)$$

$$= I(A : B) - I_{Eve}$$

“Eve’s uncertainty minus Bob’s uncertainty on Alice’s string”

“Capacity of the A-B channel minus Eve’s knowledge”

- Example: BB84 qubits: $r = 1 - 2h(Q)$

This expression is **asymptotic**, i.e. correct only in the limit of infinitely long keys.

How does the bound scale with the number N of exchanged quantum signals?

Abstract QKD



Asymptotic

$$r(\infty) = S(A | E) - H(A | B)$$

Finite key

$$r(n, m) = \frac{n}{N} \left[S_{\xi(m)}(A | E) - \Delta(n) - \text{leak}_{EC} \right]$$

Only a fraction of the signals can be devoted to the key

Perfect EC is computationally hard. Typical: $\text{leak} \approx 1.2 H(A|B)$

Correction to PA when performed on blocks of size $n < \infty$

Statistics performed on a sample $m < \infty$ are subject to fluctuations

Criterion for Security

For Finite-Key analysis, it is crucial to quantify security using a **composable definition** with **operational meaning**.

Reason: for finite samples, the probability of failure cannot be 0 \Rightarrow need to:

$$\left. \begin{array}{l} \text{Failure}(\text{Key}) \leq \varepsilon \\ \text{Failure}(\text{Task}) \leq \varepsilon' \end{array} \right\} \text{Failure} \leq \varepsilon + \varepsilon'$$

← Know what this number means
 ← Control how it propagates

Security definition: **trace distance from a perfect key**

$$\left\| \rho_{SE} - \rho_U \otimes \rho_E \right\| \leq \varepsilon \quad \text{with } \rho_U = \text{completely mixed state}$$

ε = **maximum failure probability**

i.e. maximum probability that the key is not uniform and independent of Eve

Overview of finite key studies

- Inamori, Lütkenhaus, Mayers 2001
 - BB84, weak coherent pulses
 - ε = accessible info: non-composable
- Meyer et al. PRA 2006
 - Six-state qubits
 - ε = composable, but restricted class of attacks
- Hayashi PRA 2006-2007
 - BB84, weak pulses, also decoy
 - ε = composable in PRA 2007

Experiment!

This work

- General formalism; application to BB84, six-states and Ekert implemented with qubits
- ε = composable

General Formalism & Case Study

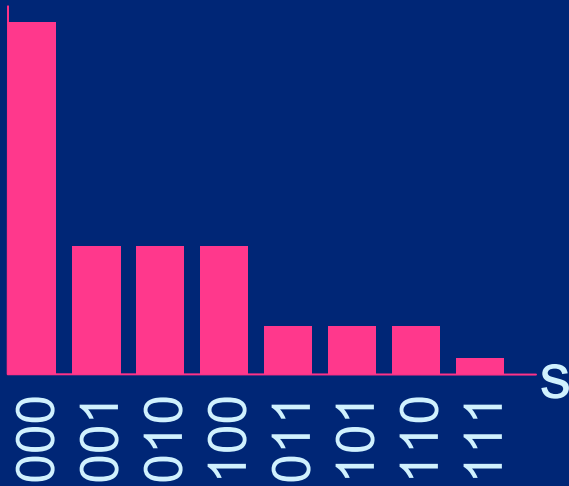
Tools: Smooth Renyi Entropies

R. Renner, Ph.D. Thesis, quant-ph/0512258

$$H_{\max} \text{ or } H_0: H_0(P) = \log|\{s \mid P(s) > 0\}|$$

$$H_{\min} \text{ or } H_\infty: H_\infty(P) = -\log[\max_s P(s)]$$

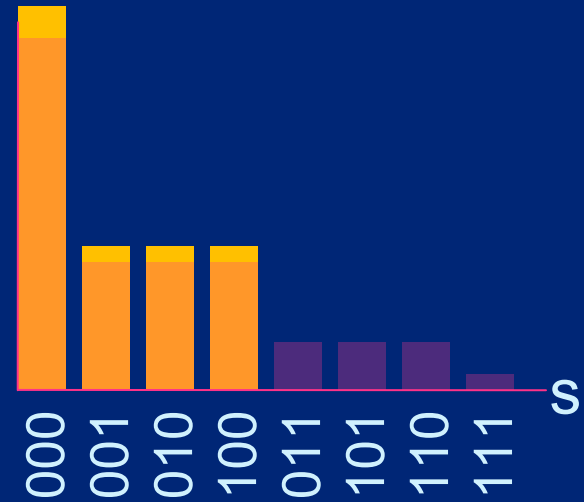
$P = \text{Bernoulli}(3/4, 1/4)$



$P(s) > 0$ for all s
 $\rightarrow H_0 = \log 8 = 3$

But how large a deviation can one tolerate?

P' ϵ -close to P



$P(s) > 0$ for 4 s
 $\rightarrow H_0^\epsilon = \log 4 = 2$

Result

$$r = \frac{n}{N} \left[S_{\mu}(A | E) - \Delta(n) - leak_{EC} \right]$$

$$\mu = \sqrt{\frac{2 \ln(1/\varepsilon'') + d \ln(m+1)}{m}}$$

$$\Delta(n) = 2 \log \frac{1}{2(\varepsilon - \varepsilon' - \varepsilon_{EC})} + 7 \sqrt{n \log \frac{2}{\varepsilon' - \varepsilon''}} \quad (+DF)$$

Given parameters:

- ε desired security
- N exchanged signals
- d outcomes of measurement
- $leak_{EC}, \varepsilon_{EC}$ describe EC

Other parameters:

- (n, m) such that $n+m < N$
- ε' controls PA
- ε'' smoothing of H_{∞}
- DF if De Finetti needed

Case study: BB84 Protocol

- Asymmetric: key from ZZ, param's from XX
- One-way classical post-processing
- Pre-processing neglected

Exchange of N q-signals and sifting

$ZZ \rightarrow Np_z^2 = n$: raw key

$XX \rightarrow Np_x^2 = m$: parameter estimation

$ZX \rightarrow Np_zp_x$ discarded

$XZ \rightarrow Np_zp_x$ discarded

Gottesman and Lo 2003; Kraus, Gisin and Renner 2005:
Symmetries of the protocols \Rightarrow can compute with collective attacks
without having to invoke the exponential De Finetti theorem.

Computing $S_\mu(A|E)$

$$r = \frac{n}{N} \left[S_\mu(A|E) - \Delta(n) - leak_{EC} \right]$$

For BB84 with single qubits:

Parameter
estimation:

$$P_{XX}(+,+) = P_{XX}(-,-) = (1 - e_p) / 2$$

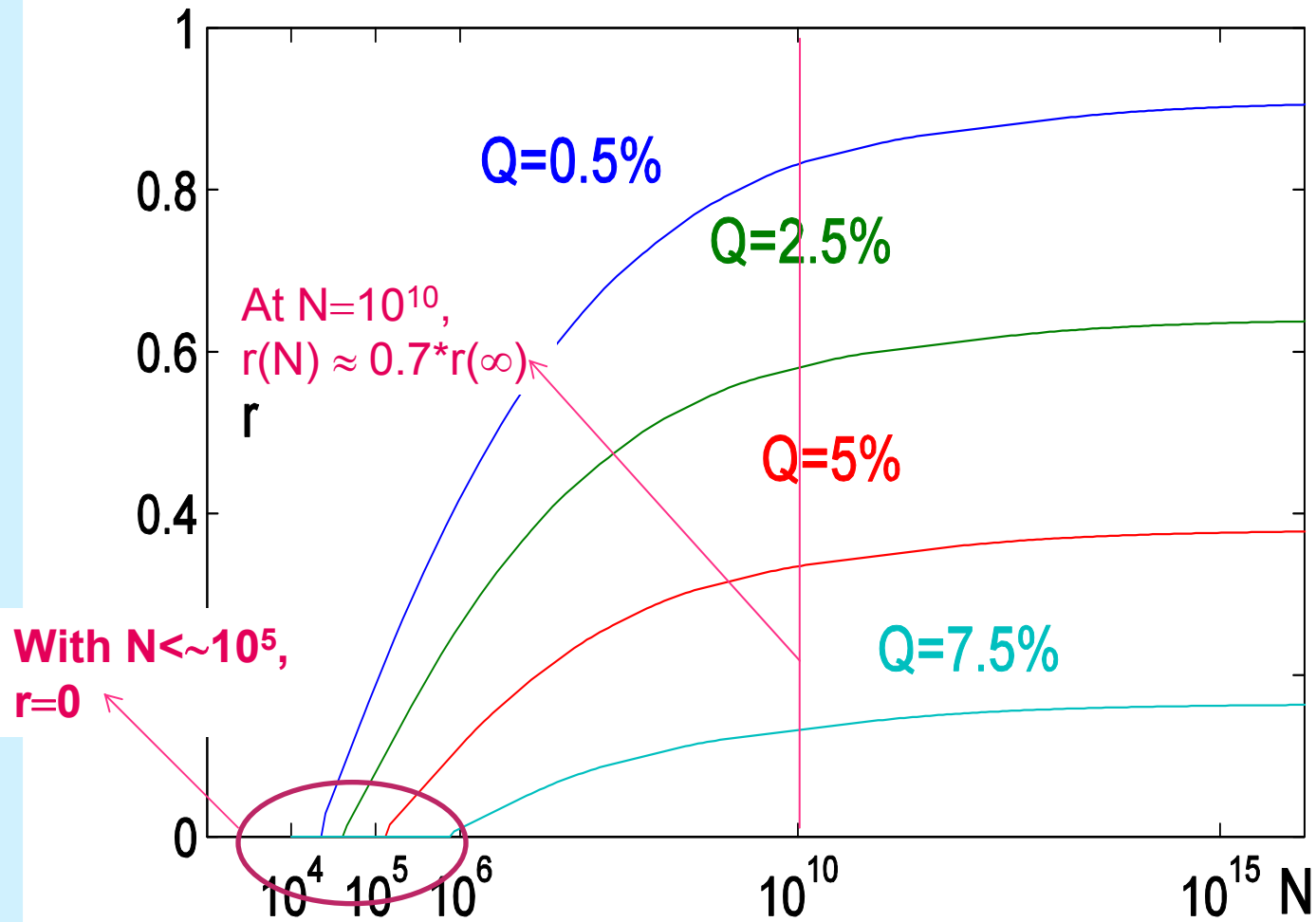
$$P_{XX}(+,-) = P_{XX}(-,+) = e_p / 2$$

→ asymptotically: $S_{\mu=0}(A|E) = 1 - h(e_p)$



$$S_\mu(A|E) = 1 - h(e_p + \mu)$$

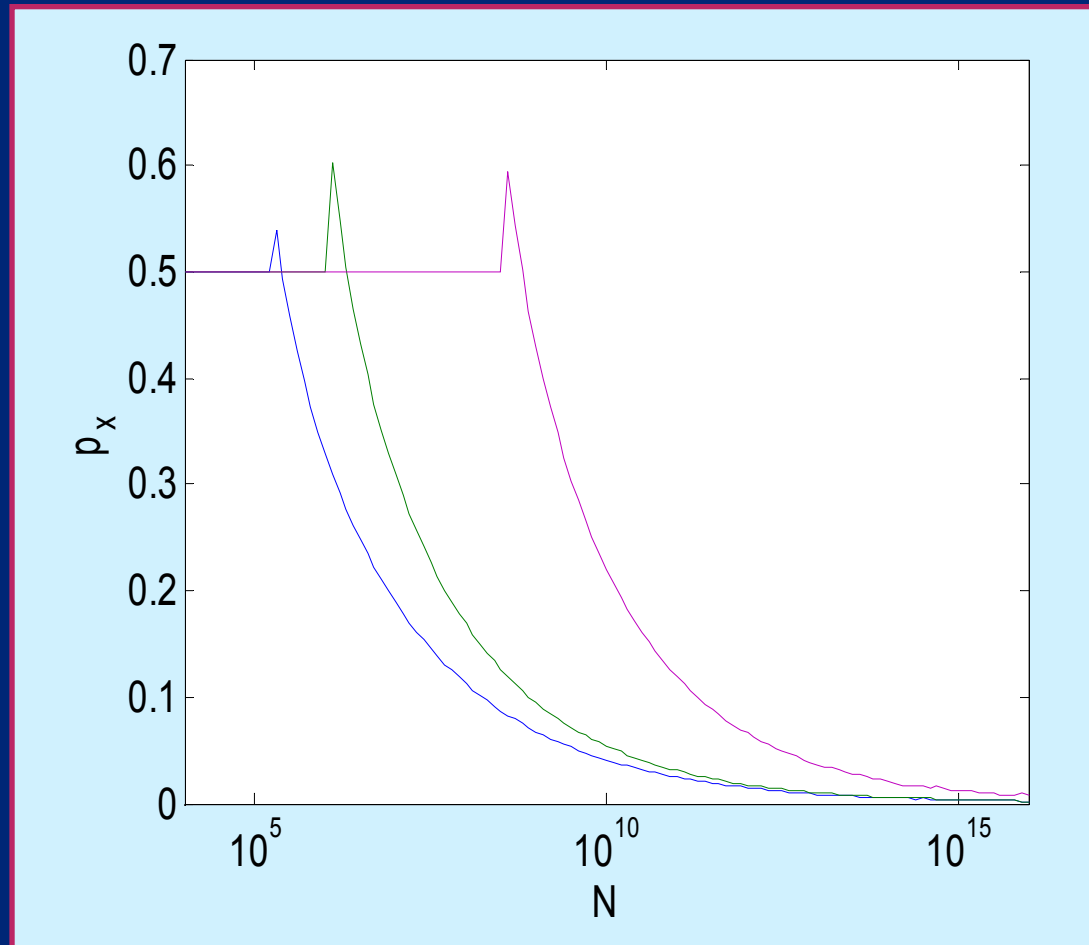
BB84, single qubits



Questions that can be answered

“How frequently should one measure in the X basis?”
Before: “Well... enough to do some statistics...”

Finite-key
studies:



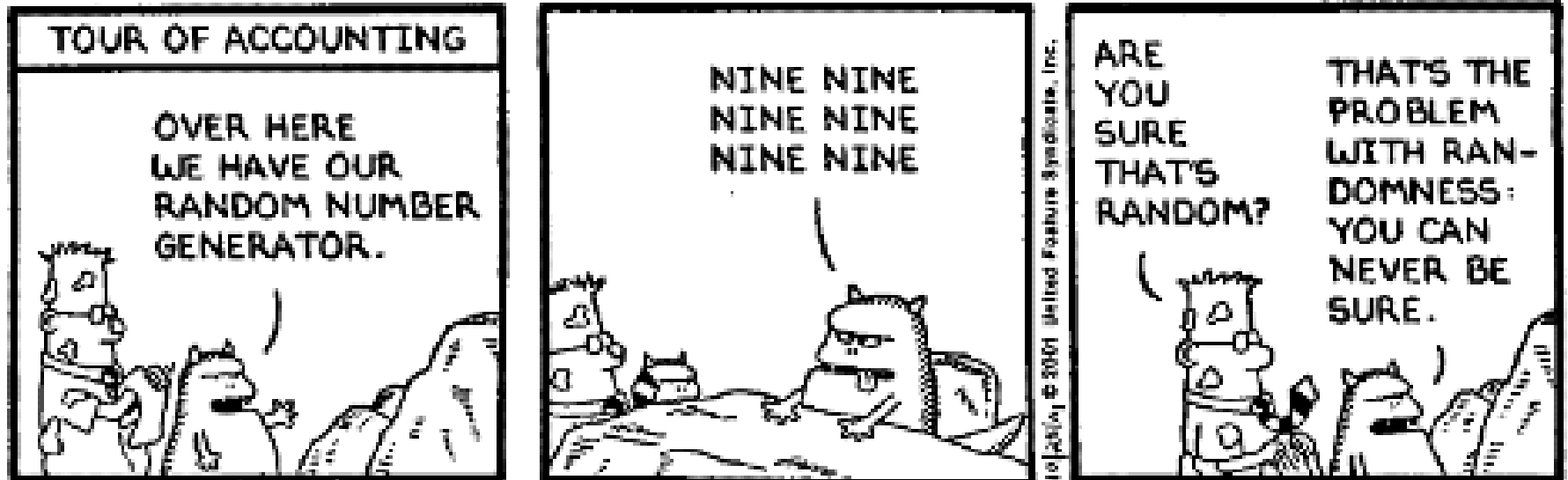
Various remarks

- The same analysis has been done for the six-state protocol and the Ekert protocol.
- Application to weak coherent pulses: work in progress, compare with Hayashi PRA 2006-7.
- The bounds for BB84 and six-states (any implementation) are tight for 1-way communication, no pre-processing.
- The formalism is general. But if one has to introduce the De Finetti theorem, the bounds are no longer tight (and are very bad).

Summary

- Finite-key analysis: essential in practice
- General formalism with the right definition of security
 - Composable
 - Operational meaning
- Case study: BB84, qubits, one-way
 - No secret key with less than 10^5 signals
 - At 10^{10} , 0.7 of the asymptotic value
 - Asymptotic value reached for 10^{15}

Thank You



Reference: VS&RR, arXiv:0708.0709