Imperial College London

20/06/19

Quantum Technologies for Cryptography

Mario Berta

University of Warwick — Computer Science Colloquium

Quantum Information Science

- Understanding quantum systems (e.g., single atoms or electrons) is hard

Richard Feynman

The Nobel Foundation

Understanding physics with computers 81

"trying to find a computer simulation of physics seems to me to be an excellent program to follow out (...) nature is not classical, dammit, and if you want to make a simulation of nature, you would better make it quantum mechanical, and by golly it is a wonderful problem, because it does not look so easy"

- Information processing based on quantum physics:
  Quantum Information Science

Quantum Technologies

Main motivation is

that we believe quantum technologies will enable us to do things that we do not know how to do using only (future) classical technology

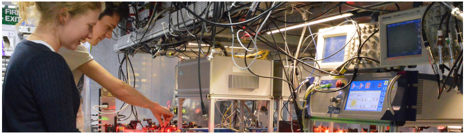
- Academic interest: EU quantum manifesto + UK national network of quantum technology hubs (UKNQT) + US/China etc.

UK NATIONAL
QUANTUM
TECHNOLOGIES
PROGRAMME

- Central intelligence agencies NSA + GCHQ: "we must act now against the quantum computing threat in cryptography"
- Big IT players investing in quantum technologies: Alibaba, Google, IBM, Intel, Microsoft, Nokia Bell Labs, NTT Laboratories, etc.

Quantum Technologies: Hardware

- Build well-controlled quantum systems: approaches range from cavity quantum electrodynamics, optical lattices, ion traps, superconductors, quantum dots, linear optics, nuclear magnetic resonance, etc.



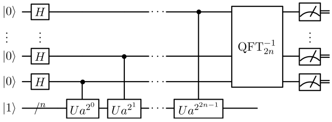
Imperial Centre for Quantum Engineering, Science and Technology (QuEST)

Hardware based (direct) applications

Quantum sensing, quantum clocks, quantum annealing, analogue quantum simulations, etc.

Overview of Quantum Technologies

1. Quantum simulation: evolution of quantum systems (digital) for computational quantum chemistry
2. Quantum computation: up to super-polynomial speed-ups over best-known classical algorithms, e.g.,



Shor's algorithm 94

Quantum algorithm

for prime factorization breaks RSA public key cryptosystem — virtually any encryption scheme in use today

3. Quantum cryptography: quantum-safe cryptography + quantum-based cryptography
4. Quantum communication: quantum repeaters, quantum internet

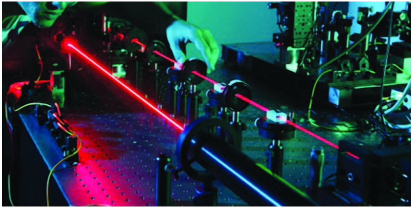
This Talk: Quantum Cryptography

Quantum-safe (post-quantum) cryptography:

- academic interest (e.g.,CRYPTO)
- ongoing NIST "Post-Quantum Cryptography Standardization"
- computational / quantum memory attacks

Quantum-based cryptography:

- quantum key distribution
- secure multi-party computation
- delegated computation
- randomness generation

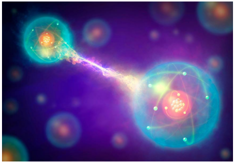


Imperial College London

Cryptography from Uncertainty versus Entanglement

- Heisenberg's uncertainty principle

- Strong quantum correlations — entanglement

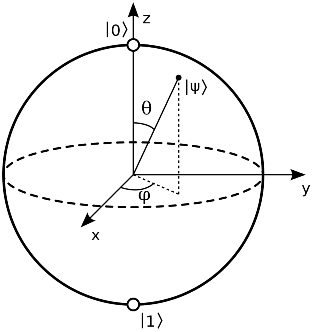


- Basic idea: principles fight each other $\Rightarrow$ quantum cryptography but also quantum adversaries

Overview

Qubits

- Classical information unit: bits take values 0 or 1 with certain probabilities
- Quantum information unit: qubits take values $|\psi\rangle$ on the Bloch sphere $S^2 \subset \mathbb{R}^3$



Uncertainty Principle

- Quantum mechanics: impossible to measure in what exact state $|\psi\rangle$ the qubit is, rather measure along axis, e.g., X or Z
  $\Rightarrow$ measurement collapses $|\psi\rangle$ to probability distributions $\{p_x\}$ or $\{q_z\}$
- Heisenberg's uncertainty principle

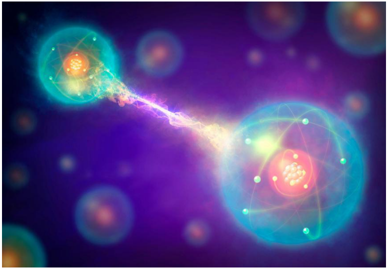
Information-theoretic uncertainty relation [Maassen-Uffink 88]

$$\underbrace{H(X)}_{\text{uncertainty about } X} + \underbrace{H(Z)}_{\text{uncertainty about } Z} \geq 1 \quad \text{with } H(X) = -\sum_x p_x \log p_x \text{ Shannon entropy}$$

Imperial College London

Entanglement

- Quantum correlations between qubits can become much stronger than classical correlations — entanglement



- Implications for the concept of uncertainty [Einstein *et al.* 35]: measurement results on A available when having access to B

Imperial College London

Uncertainty versus Bipartite Entanglement

- Entanglement changes uncertainty relation (quantum adversary B)

$$H(X) + H(Z) \geq 1 \quad \Rightarrow \quad \underbrace{H(X|B)}_{\substack{\text{uncertainty about} \\ X \text{ given } B}} + \underbrace{H(Z|B)}_{\substack{\text{uncertainty about} \\ Z \text{ given } B}} = 0 \ngeq 1$$

with $H(X|B) = H(XB) - H(B)$ the conditional von Neumann entropy

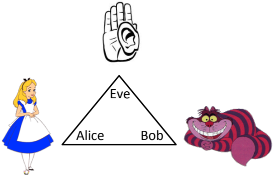
Uncertainty — entanglement [Coles *et al.* (B.) Rev. Mod. Phys. 17]

$$\underbrace{H(X|B)}_{\substack{\text{uncertainty about} \\ X \text{ given } B}} + \underbrace{H(Z|B)}_{\substack{\text{uncertainty about} \\ Z \text{ given } B}} \geq 1 + \underbrace{H(A|B)}_{\substack{\text{entanglement} \\ \text{between } A \text{ and } B}}$$

- What happens if we add a second observer E?

Uncertainty versus Tripartite Entanglement

- Entanglement is monogamous — it cannot be shared freely



Tripartite uncertainty [Coles *et al.* (B.) Rev. Mod. Phys. 17]

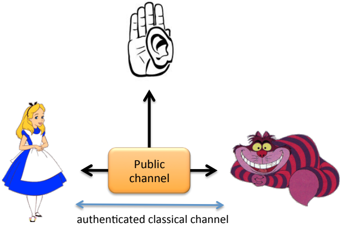
$$\underbrace{H(Z|E)}_{\substack{\text{Eve's uncertainty} \\ \text{about Alice's } Z}} + \underbrace{H(X|B)}_{\substack{\text{Bob's uncertainty} \\ \text{about Alice's } X}} \geq 1$$

- Interplay between uncertainty and entanglement leads to cryptography

Imperial College London

Quantum Key Distribution: Setup

- Fully insecure public quantum channel together with authenticated classical channel and local randomness allow for information-theoretically secure key distribution [Wiesner 70] [Bennett & Brassard 84] [Mayers 06]

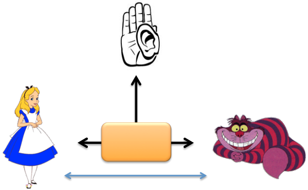


- Key allows for secure communication (message size = key size) [Vernam 26] [Shannon 49]
- Monogamy of entanglement and uncertainty principle for security

Quantum Key Distribution: Protocol & Security

- Toy protocol [Ekert 91]

  1. **Preparation**: share two-qubit state, using the public channel
  2. **Measurement**: along X or Z axis, coordinate using authenticated channel
  3. **Repeat**: steps 1 and 2 many times
  4. **Parameter estimation**: including privacy amplification and error correction

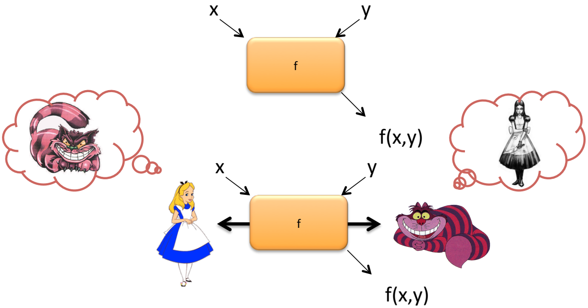


QKD security proof idea

$$\underbrace{H(Z|E)}_{\text{Eve's uncertainty about key } Z} \geq 1 - H(X|B) \geq 1 - \underbrace{H(X|X')}_{\text{with Alice \& Bob}}$$

Two-Party Cryptography: Task

- Two mutually distrustful parties want to achieve a task, example: secure function evaluation (others are secure identification, bit commitment, oblivious transfer, coin tossing, etc.)



- Quantum advantage but no information-theoretic security possible [Lo 97]

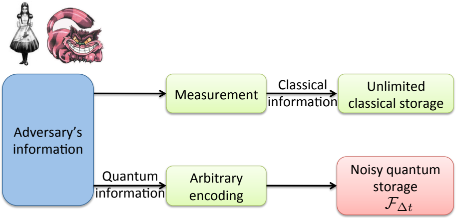
Imperial College London

Two-Party Cryptography: Model & Security

- Security analysis: need bound for entanglement $H(A|B)$ in

$$H(X|B) + H(Z|B) \geq 1 + H(A|B)$$

- Bounded (noisy) storage model: adversary computationally all powerful, actions are instantaneous, unlimited classical storage, but limited quantum memory [Damgard *et al.* 05]



- Quantum: no quantum memory needed for implementation vs. $n - O(\log^2 n)$ qubits to break scheme [Pirandola *et al.* (B.) arXiv 19]

Quantum Adversaries I

- Cryptographic sub-routines like privacy amplification for post-processing [Bennett & Brassard 88]

Main challenge

Do these protocols work when taking quantum adversaries into account?
Yes [Renner 05] + No [Gavinsky *et al.* 07]

- Routines as bilinear optimization problems [B. *et al.* SIAM J. Optim. 16]

$$\begin{aligned} p(A,g,k) = \underset{(z_\alpha, y_\beta)}{\text{maximize}} \quad & \sum_{\alpha,\beta} A_{\alpha,\beta} z_\alpha y_\beta \\ \text{subject to} \quad & g(z_1,\ldots,z_N) \geq 0 \\ & k(y_1,\ldots,y_M) \geq 0 \end{aligned}$$

  with sets of affine constraints $\{g(z_1,\ldots,z_N)\}$ and $\{k(y_1,\ldots,y_M)\}$
- General theory of pseudo-randomness [Vadhan 07]

Imperial College London

Quantum Adversaries II

$$
\begin{aligned}
p(A,g,k) = \underset{(z_\alpha, y_\beta)}{\text{maximize}} \quad & \sum_{\alpha,\beta} A_{\alpha,\beta} z_\alpha y_\beta \\
\text{subject to} \quad & g(z_1,\ldots,z_N) \geq 0 \\
& k(y_1,\ldots,y_M) \geq 0
\end{aligned}
$$

- The performance $p^*(A,g,k)$ against quantum adversaries is measured by quantum bilinear optimization [B. *et al.* SIAM J Optim. 16]

$$
\begin{aligned}
p^*(A,g,k) = \underset{\left(|\psi\rangle \in \mathbb{C}^{2^n}, E_\alpha, D_\beta\right)}{\text{maximize}} \quad & \sum_{\alpha,\beta} A_{\alpha,\beta} \langle\psi| E_\alpha D_\beta |\psi\rangle \\
\text{subject to} \quad & E_\alpha D_\beta - D_\beta E_\alpha = 0 \\
& g(E_1,\ldots,E_N) \succeq 0 \\
& k(D_1,\ldots,D_M) \succeq 0
\end{aligned}
$$

  where $g(E_1,\ldots,E_N) \succeq 0$ and $k(D_1,\ldots,D_M) \succeq 0$ positive semidefinite
- Characterization via operator spaces = non-commutative Banach spaces [B. *et al.* IEEE Trans. Inf. Theory 16]

Quantum Adversaries III

- Can we find outer approximations $p(A, g, k) \leq p^*(A, g, k) \leq \cdots$?

Semidefinite hierarchies [B. *et al.* SIAM J. Optim. 16 / arXiv 19]

$$p(A, g, k) \leq p^*(A, g, k) = \mathrm{SDP}_\infty(A, g, k) \leq \cdots \leq \mathrm{SDP}_1(A, g, k)$$

- Semidefinite program (SDP): optimization of linear objective function over intersection of the cone of positive semidefinite matrices with affine space
- Can certify security against quantum adversaries if for example

$$p(A, g, k) \leq p^*(A, g, k) \leq \mathrm{SDP}_1(A, g, k) \overset{?}{\leq} C \cdot p(A, g, k)$$

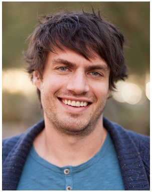
- Flexible proof tool for upper bounding the power of quantum adversaries for a variety of cryptographic protocols

Conclusion & Outlook

- Quantum technologies for cryptography, challenges from quantum adversaries:
  1. Relation between uncertainty and entanglement for simple and tight security proofs
  2. Efficiently computable semidefinite programming upper bounds on the power of quantum adversaries
- Security of mathematical model versus security of experimental implementation — goal is to close this gap
- Security in laboratory versus secure for everyday use — quantum technologies are adding non-trivially to this equation
- Device-independent cryptography? Yes, but not practical yet...

Imperial College
London

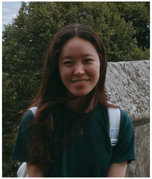
Quantum Information at Imperial



Mario Berta

Carlo Sparaciari

Francesco Borderi



Hyejung Jee

Navneeth Ramakrishnan

Samson Wang

Imperial College London

Further Reading

- **Quantum computational supremacy**, Aram Harrow & Ashley Montanaro, Nature 549, 203 (2017)
- **Quantum computing in the NISQ era and beyond**, John Preskill, Quantum 2, 79 (2018)
- **Entropic uncertainty relations and their applications**, Patrick J. Coles *et al.* (Mario Berta), Reviews of Modern Physics 89, 015002 (2017)
- **Advances in quantum cryptography**, Stefano Pirandola *et al.* (Mario Berta), arXiv:1906.01645 (2019)