Quantum Cryptography

Dylan Evans, Alec Landow, Aaron Ross, Stefan Salanski

Department of Physics, University of Virginia

May 2nd, 2011

UVA QCP

What is Cryptography?

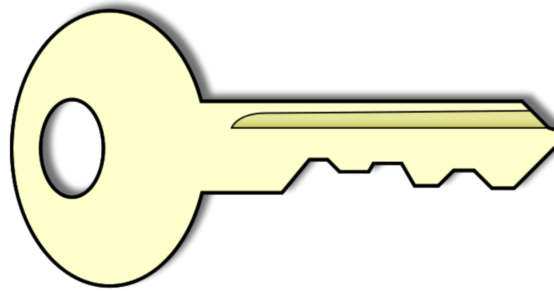
- Cryptography: the practice of keeping data

SECRET

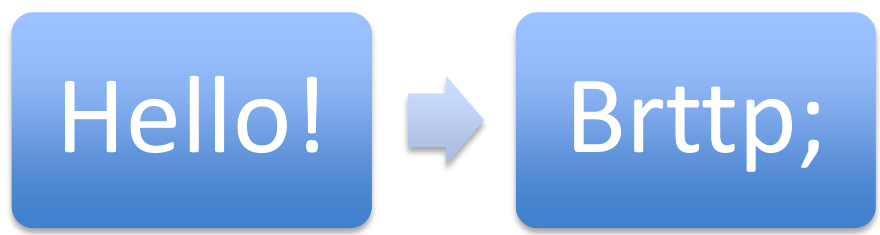
by some encoding procedure

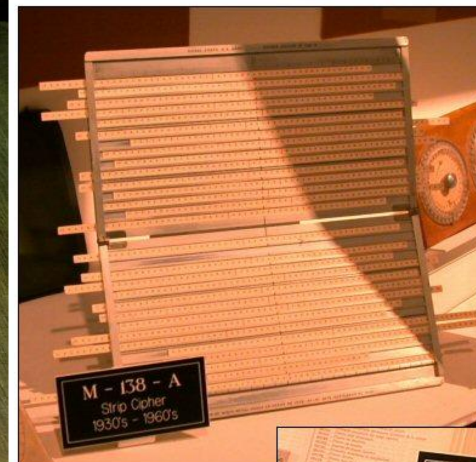
Classical Cryptography

- Physical keys

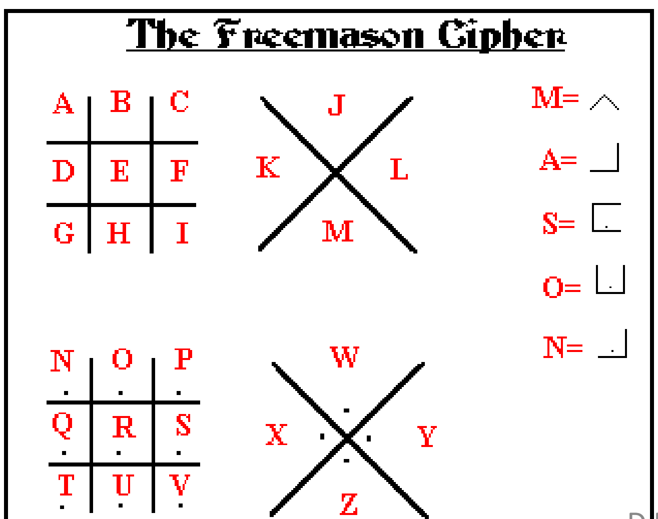


- Mechanical systems
- Replacement Rules:



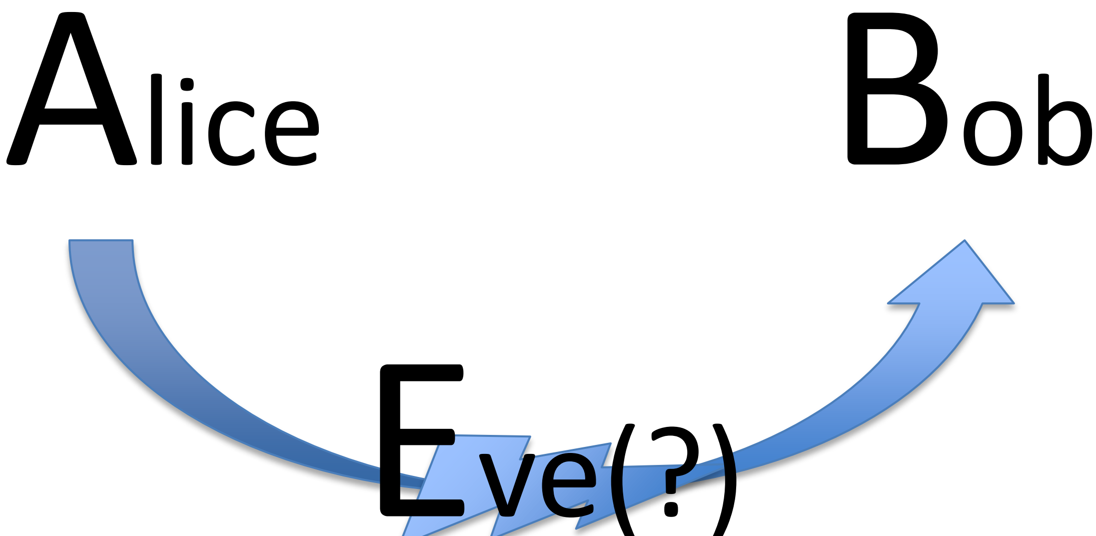


SIMPLE CIPHER DEVICES
(GVG / PD)



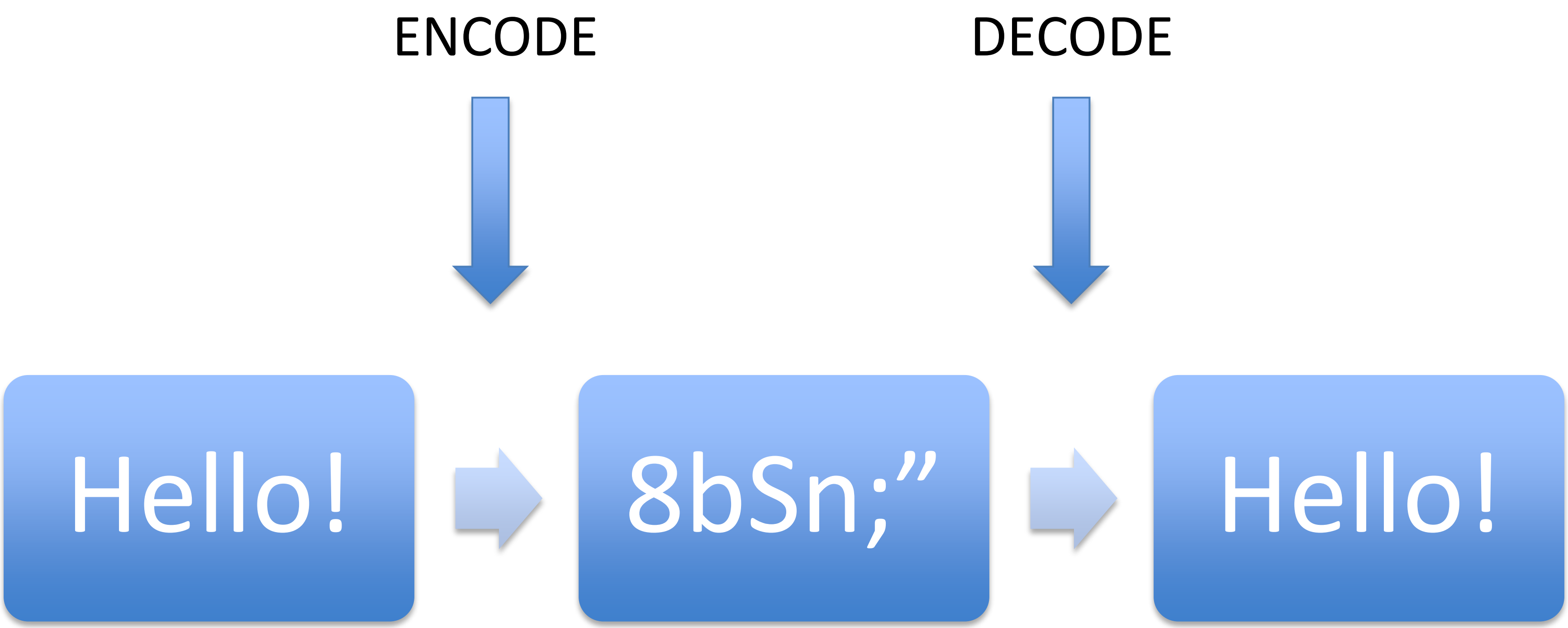
Meet Alice, Bob, and Eve

- Alice wants to tell something to Bob.
- Eve wants to eavesdrop.



Modern Cryptography

- Involves mathematical and information theoretic techniques to ensure security
- RSA protocol (MIT, 1978)



Sent message
(Alice)

Encoded message
(Eve might be
watching!)

Received message
(Bob)

Symmetric Key Distribution

- Alice and Bob use SAME key
- Bitwise addition modulo 2:

$$c_i = p_i \oplus k_i$$

$$p_i = c_i \oplus k_i = p_i \oplus k_i \oplus k_i = p_i$$

D Evans, A Landow, A Ross, S Salanski UVa
Dept. of Phys.

Asymmetric Key Distribution

- Alice and Bob use DIFFERENT keys
- Hinges on difficulty of factorization of integers (exponential time complexity)
  - 2048 bits ≈ 617 decimal digits => LONG TIME

Quantum Mechanical Background

- Every measurement perturbs the system
- No-cloning theorem (Wooters, Zurek, Dieks 1982):

  An outside observer CANNOT faithfully replicate an unknown quantum state!

No-Cloning Theorem

$$U\left|\chi_1 \otimes \phi\right\rangle = \left|\chi_1 \otimes \chi_1\right\rangle$$

$$X \;=\; \langle \chi_1 \otimes \phi | U^\dagger U | \chi_2 \otimes \phi \rangle$$

$$X = \langle \chi_1 \otimes \phi | \chi_2 \otimes \phi \rangle = \langle \chi_1 | \chi_2 \rangle$$

$$X = \langle \chi_1 \otimes \chi_1 | \chi_2 \otimes \chi_2 \rangle = \langle \chi_1 | \chi_2 \rangle^2$$

Motivation Behind QC

- Classical cryptosystems typically use AKD
- Shor (1994): factorization of integers by quantum computer in POLYNOMIAL time complexity
- Need secure and easy way to utilize SKD

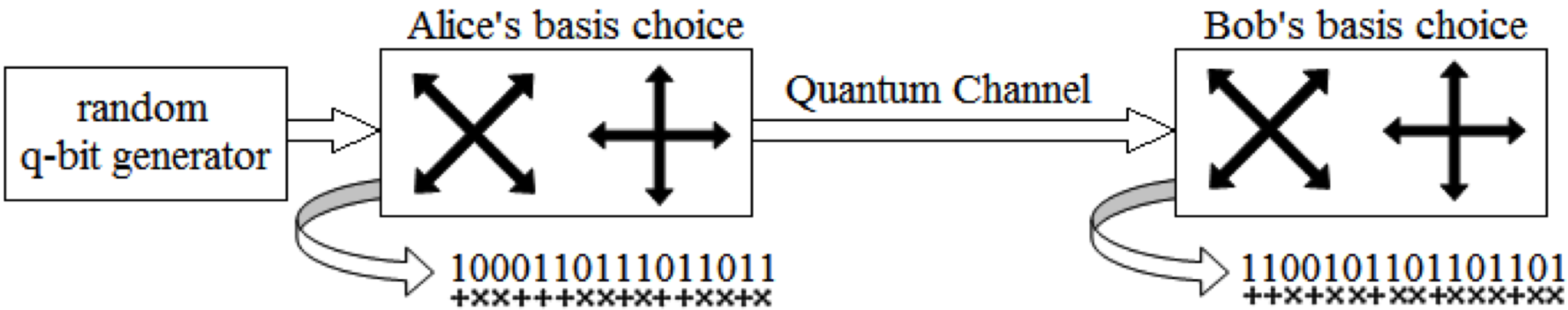
Protocols of Quantum Key Distribution

- BB84 (SKD)
  - Bennett and Brassard (1984)

- EPR (SKD)
  - Artur Ekert (1991)
  - Very similar to BB84

BB84 Protocol

- 2 bases of photon polarization:
  - Vertical/horizontal, |1/0>, and ±45°, |±>
  - 0 : |0> and |->
  - 1 : |1> and |+>
  - (!) THE TWO BASES ARE NOT ORTHOGONAL (!)
- 2 channels:
  - 1 classical, 1 quantum


random
q-bit generator
Alice's basis choice
Quantum Channel
Bob's basis choice
1000110111011011
+××+++××+×++××+×
1100101101101101
++×+××+××+×××+××


A +××+++××+×++××+×
B ++×+××+××+×××+××
1 00 1 1 1
Sifted Key:
100111

Quantum Bit Error Rate (QBER)

- QBER: Probability that Bob measures the wrong polarization when Alice's basis is known

$$q_0 = p_f + \frac{p_d n q \Sigma f_r t_l \mu}{2}$$

D Evans, A Landow, A Ross, S Salanski UVa
Dept. of Phys.

Information Reconciliation

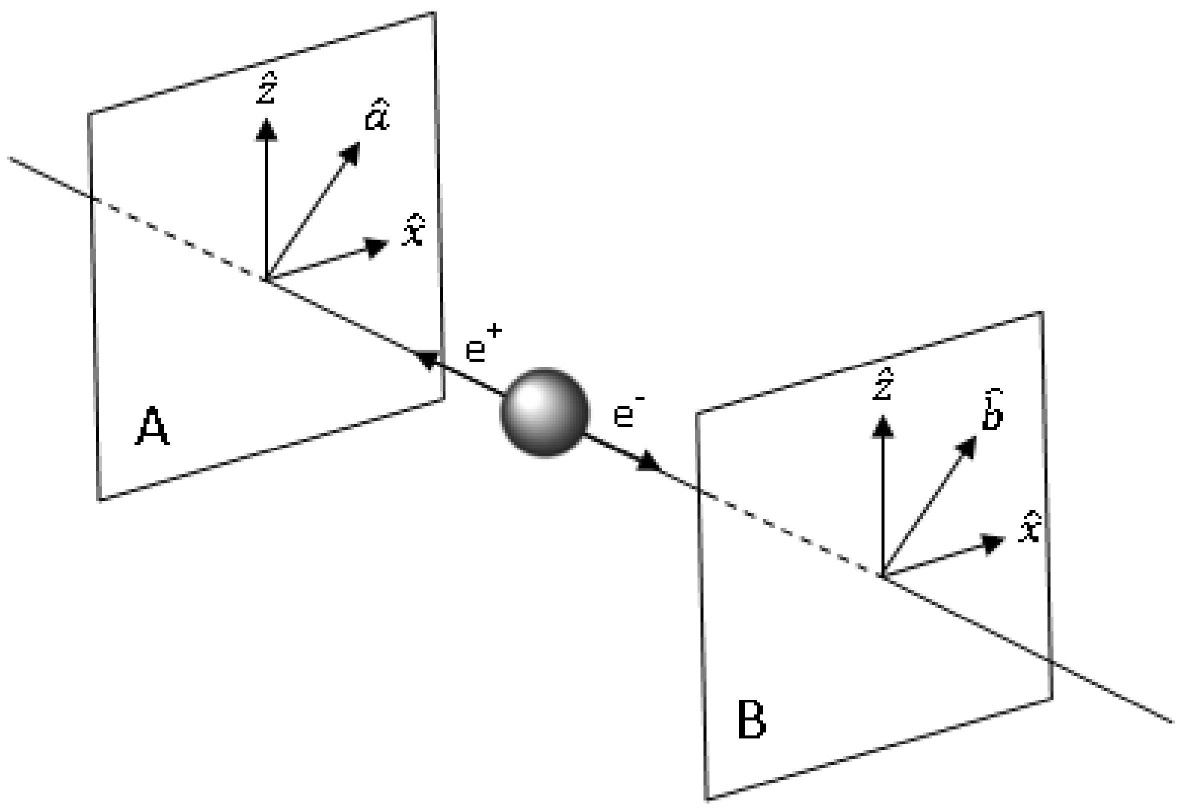
- $R > q_0$? THROW OUT ENTIRE KEY
- $R < q_0$?

- Information Reconciliation
  - Divide string, calculate parity, compare
  - Different? Divide that part more! Find the bad bit
  - Discard final bit at end of check

Privacy Amplification

- Choose m = n – k – s bits at random from sifted key
- Compute parity
- Rinse and repeat
- String of parities becomes NEW sifted key

Ekert's EPR Protocol

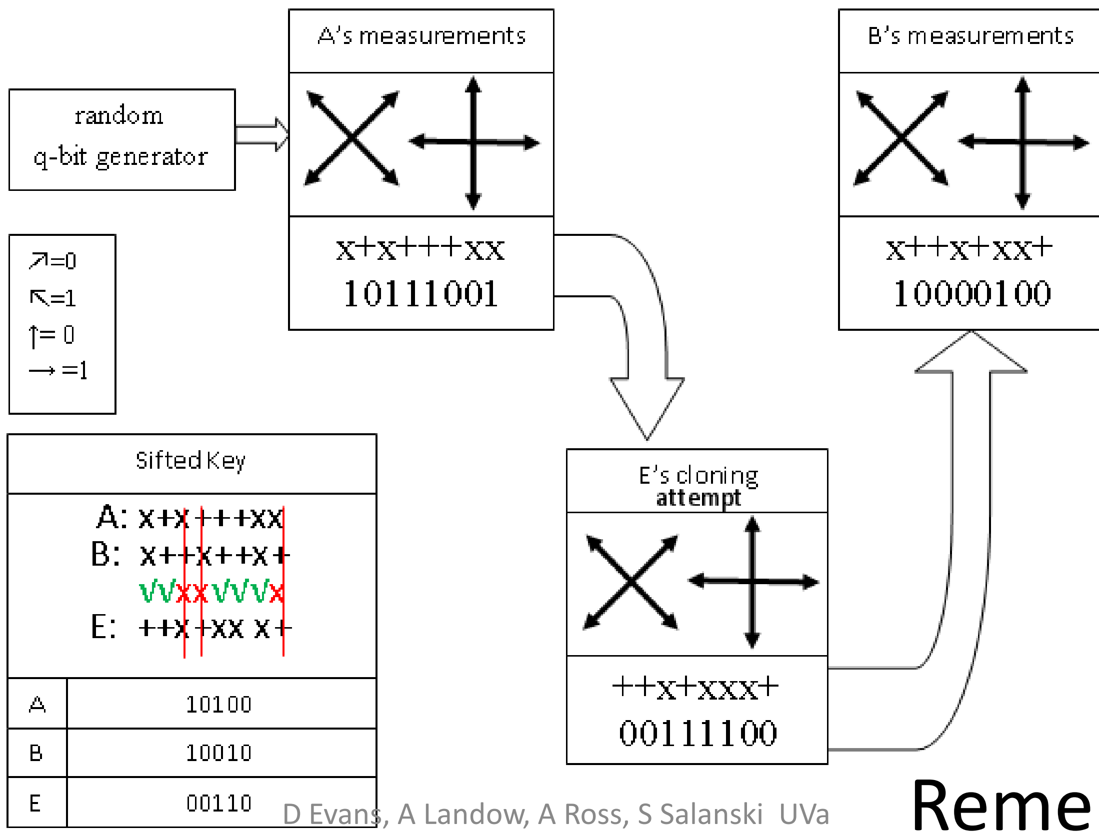


What About Error?

- Bell's Inequalities : EPR :: QBER : BB84
- Ensure states are entangled
  - "Violation" of Bell's inequalities is a good thing!

Eavesdropping on BB84

- Intercept-resend strategy



Remember QBER!

Eavesdropping on EPR

- Send out 2 qubits that are not entangled
- Send out 2 of 3 correlated particles, hold on to third

Technology

- Quantum channel = free space or optical fiber
- Free space limitations?
  - Weather dependence
  - Necessity of direct line of sight
- Optical fiber limitations?
  - Kinks or bends in fiber are problematic

Outlook

- Quantum key distribution is UNBREAKABLE… if performed perfectly.
- It is the QM that gives rise to the nature of QC
- Single photon lasers don't exist yet!
- Neither do single photon detectors (might not ever due to dark noise)
- Other protocols on the rise, i.e., quantum teleportation

References

[1] G. Benenti, G. Casati and G. Strini, *Principles of Quantum Computation and Information, Volume I: Basic Concepts*, World Scientific, New Jersey, 1st Edition, 2004.

[2] D. Brußand G. Leuchs, *Lectures on Quantum Information*, Wiley-Vch, Weinheim, 1st Edition, 2007.

[3] M. Bellac, *Quantum Information and Quantum Computation*, Cambridge University Press, New York, 1st Edition, 2006.

[4] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *submitted to Rev. Mod. Phys.*, Group of Applied Physics, University of Geneva, February 1st, 2008.

[5] R. Gelles, *Security of Quantum Key Distribution Against Collective Attacks*, Technion IIT, September 8th, 2005.

[6] Ekert. A, Phys. Rev. Lett. 67, 661-663 (1991).

[7] R. Hughes, J. Nordholt, D. Derkacs and C. Peterson, *Practical free-space quantum key distribution over 10 km in daylight and at night*, Los Alamos Physics Division.

[8] M. Dusek, O. Haderka and M. Hendrych, *Generalized beam-splitting attack in quantum cryptography with dim coherent states*, Optics Comm., October 1999.

[9] Kurtsiefer, C. Phys. Rev. Lett. 85, 290293 (2000).

[10] BB84 and Ekert91 Protocols, *http : //www.quantiki.org/wiki/BB84 _and_Ekert91_protocols*, Quantiki.

[11] E. Biham, M. Boyer, P. Boykin, T. Mor, V. Roychowdhury, J. Cryptology (2006) 19: 381439.