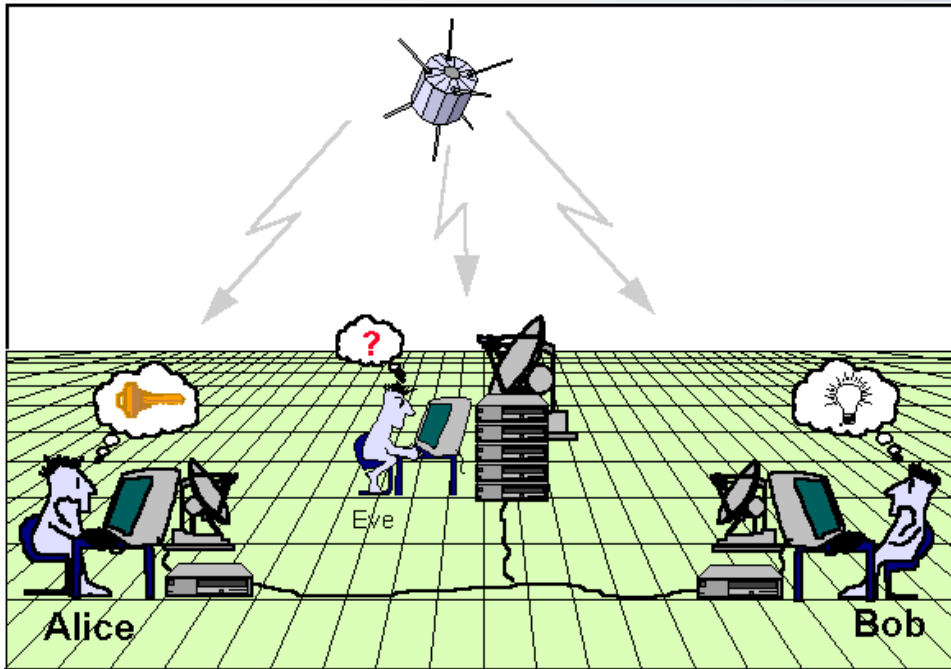


# Information Security in the Quantum Age

Anderson C A Nascimento, Ph.D.  
Universidade de Brasília



# Introduction



- One of the main goals of cryptography: to provide a way for two legal parties (Alice and Bob) to communicate securely in the presence of eavesdroppers.

# Crypto also deals with more general tasks!



- Secure Two-Party Computations

# The Millionaires Problem



Two millionaires want to know who is the richest one between them. However, they are not willing to reveal the amount of their wealth.

# Secure Two Party Computations

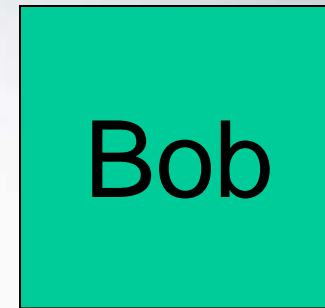


X



Alice

Y



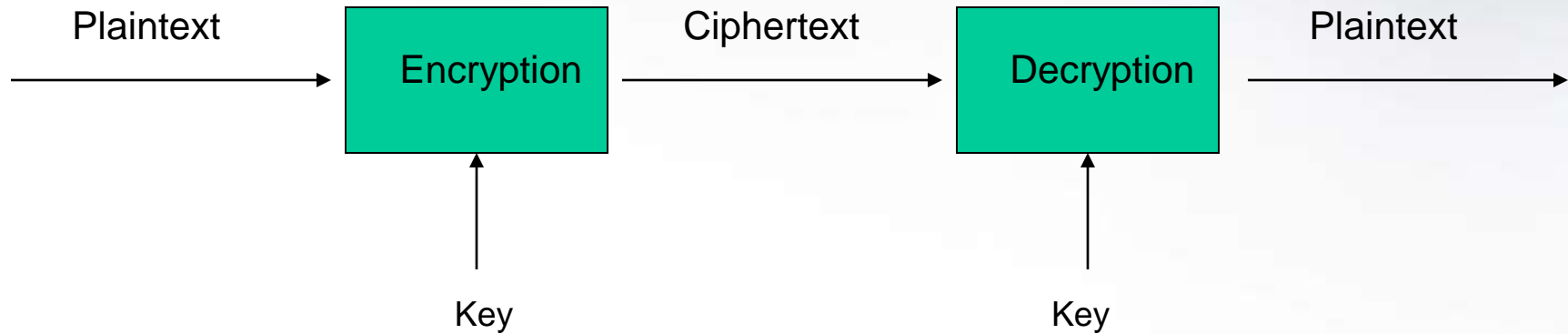
$F(X, Y)$

Alice should know nothing about  $F(X, Y)$  besides what can be computed from  $X$ .

Bob should know nothing about  $X$  besides what can be computed from  $F(X, Y)$

If both players are honest Bob should receive  $F(X, Y)$

# Secret Message Transmission

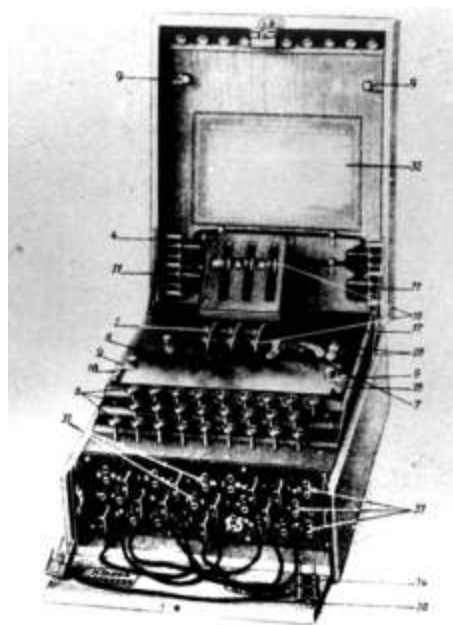


$$E_k(M)=C$$

$$D_k(C)=M$$

**The Security of the scheme must rely only on the secrecy of the key!**

# How can we know if a given cryptographic system is secure?



# Perfect and Proven Secrecy



- One-Time Pad

$$C = M + K \pmod{2}$$

M = 0 0 1 1 1 0 0 1 0 1

K = 1 0 1 1 0 1 0 1 0 1

---

C = 1 0 0 0 1 1 0 0 0 0

**The Key must be random and used only once!**

**The key must have the same length of the message!**



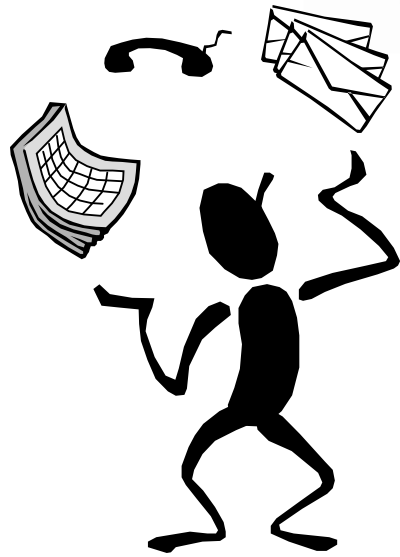
Claude E. Shannon, "**Communication Theory of Secrecy Systems**", Bell System Technical Journal, vol.28-4, page 656--715, 1949

# Computationally Secure Systems

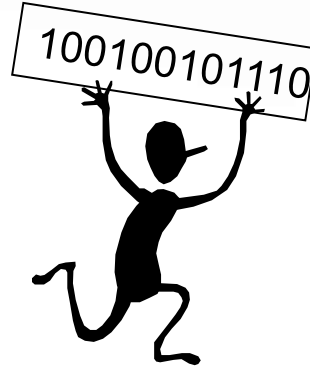


- Instead of aiming at unconditional security, we assume that our adversaries are computationally bounded.
- That means the system can be broken in principle. However, in order to do so an adversary would have to efficiently solve seemingly hard computational problems.
- 
- Then, it is possible to design good symmetric ciphers:
  - Short and reusable keys
  - Efficient

# Key Distribution Problem



Alice



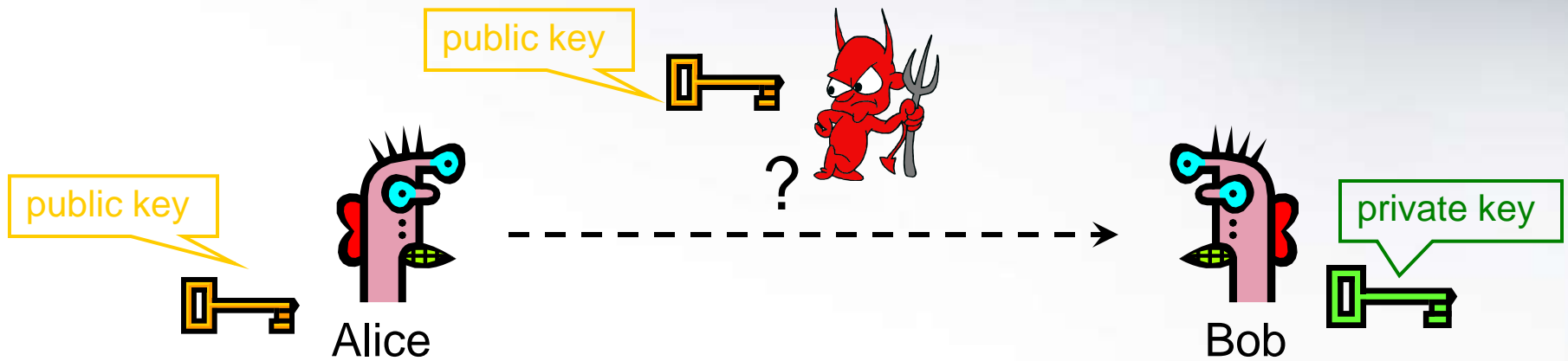
Bob

One has to rely on a secure channel!

# Solution

## Diffie-Hellman Key Exchange

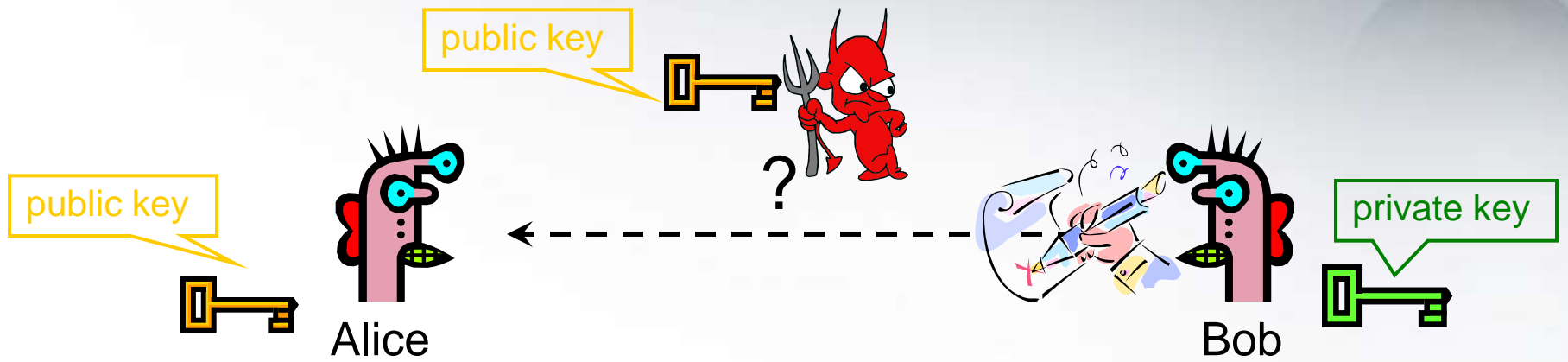
## Public Key Cryptography



Given: Everybody knows Bob's **public key**  
- How is this achieved in practice?  
Only Bob knows the corresponding **private key**

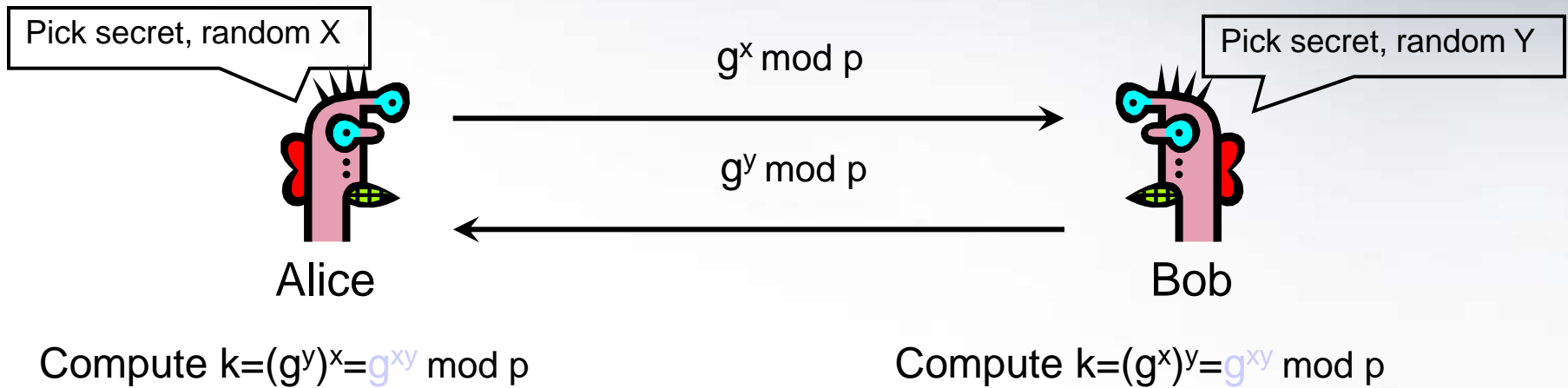
Diffie, W. Hellman, M. ,**New Direction in Cryptography**, Information Theory, IEEE Transactions on, Nov 1976 Volume: 22, Issue: 6, On page(s): 644-654

# Bonus: Digital Signatures!



By using his private Key, Bob can produce a “signature” of a given message which can be verified by anyone who knows his public key.

# DH Key Exchange



slide 13

Having never met before, Alice and Bob can agree on a random and secret key.

Secure against passive adversaries.

**Computing the discrete logarithm seems to be difficult.**

# RSA

[Rivest, Shamir, Adleman 1977]



- Key generation:
  - Generate large primes  $p, q$ 
    - Say, 1024 bits each (need primality testing, too)
  - Compute  $n=pq$  and  $\varphi(n)=(p-1)(q-1)$
  - Choose small  $e$ , relatively prime to  $\varphi(n)$ 
    - Typically,  $e=3$  (may be vulnerable) or  $e=2^{16}+1=65537$
  - Compute unique  $d$  such that  $ed = 1 \pmod{\varphi(n)}$
  - Public key =  $(e,n)$ ; private key =  $d$
- Encryption of  $m$ :  $c = m^e \pmod n$ 
  - Modular exponentiation by repeated squaring
- Decryption of  $c$ :  $c^d \pmod n = (m^e)^d \pmod n = m$

# RSA



- RSA can be broken if the integer factoring problem (IFP) can be solved efficiently.
- No polynomial algorithms are known to solve this problem.

# Other PKCs



- ElGamal PKC – Security related to the discrete logarithm problems
- DSS – Digital Signature Standard
- The discrete logarithm problem can be defined for other Galois Fields such as points of elliptical curves.
- In the case of elliptical curves, the problem seems to become even harder!
  - ONE CAN USE SHORTER KEYS!
  - ECC – Elliptical Curves Cryptography (Koblitz)

# IPSec



- IKE – Internet Key Exchange – Based on the DH Key Exchange
- Once a secret and symmetric key is shared, it is used to provide confidentiality, authenticity and integrity.

# TLS/SSL



- Uses public key cryptography to share a symmetric key in a handshake protocol.
- Uses the shared symmetric key to authenticate (MACs) and to provide confidentiality.

# Secure Two Party Computations



X



Alice

Y



**SOLVED**



$F(X, Y)$

Alice should know nothing about  $F(X, Y)$  besides what can be computed from  $X$ .

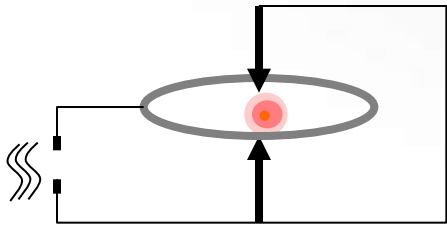
Bob should know nothing about  $X$  besides what can be computed from  $F(X, Y)$

If both players are honest Bob should receive  $F(X, Y)$

# Peter Shor (1994)



## The Relevance of Quantum Computing for Future Cryptography:



Schematic view of a Paul ion trap used for manipulation of quantum information

- Quantum Algorithms for factoring and discrete logarithm are efficient
- Simple quantum logic gates have already been realized

All the public key cryptosystems currently used in practice would be broken if we had quantum computers capable of computing with some hundreds of qubits.

Shor's algorithm exploits some weird properties of quantum systems (parallelism, entanglement and so on)

# Shor's Result



- Integer Factorization – IFP: RSA.
- Discrete Logarithm and Diffie-Hellman – DLP, CDHP, DDHP, BDHP, ...: (EC)DSA, (EC)DH, pairing-based cryptosystems.
- These intractability assumptions (and several others) reduce to that of the *Hidden Subgroup Problem* – HSP.
  - **Shor's algorithm is a threat to:**
    - IKE – IPsec
    - TLS/SSL
    - **Public Key Infra-Structure**

# Quantum Computers



- All the current implementations are mostly based on MRI
- There is a theoretical limit on the number of qubits this kind of implementation can deal with (no more than 20)
- Other possible implementations:
  - Ion Traps
  - Quantum Dots

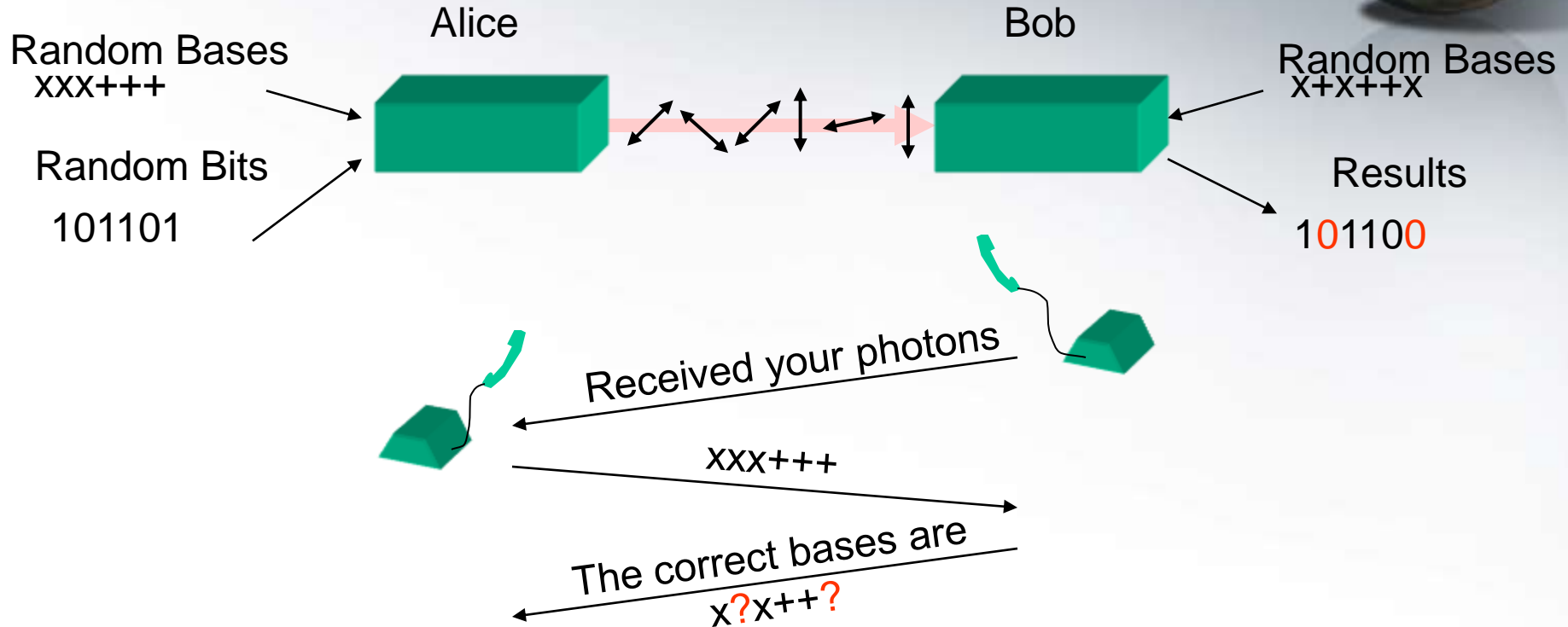
**Most of the Scientists agree that implementing a quantum computer is basically an engineering problem!**

# What can we do about it?



- Symmetric Key cryptography seems to withhold quantum attacks.
- Thus, we would like to have:
  - **Key Exchange**
  - **Digital Signatures**

# Quantum Key Distribution



Every eavesdropper has to decide on a measurement **before** he knows the bases. This disturbs the quantum state and the eavesdropper can be detected before the key is used. Alice and Bob will compare part of the key before using it.

Quantum mechanics allows a key agreement with perfect security

# Quantum Key Distribution



- Problems:
  - Highly inefficient (transmission rate)
  - Expensive
  - Requires an authenticated channel
  - Limited to short transmission distances (there are no quantum repeaters with current technology).

# Quantum Cryptography



- Secure Quantum Two-Party and Multi-Party Computations are impossible without further assumptions.
- No Digital Signatures.

# Post-Quantum Cryptosystems



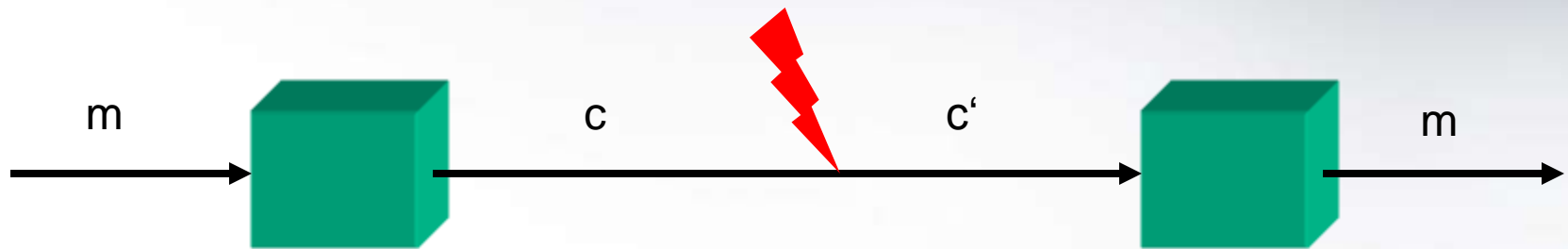
- These are CLASSICAL systems which are believed to resist attacks performed by an adversary holding a quantum computer.
- There are theoretical analysis which point out that quantum computers might not be able to efficiently tackle NP hard problems.
- Thus, we may obtain public key cryptosystems which are “quantum secure” by carefully modifying NP hard problems into crypto assumptions.

**Plug in replacements for RSA/ECC.**

# McEliece



Error Correcting Codes

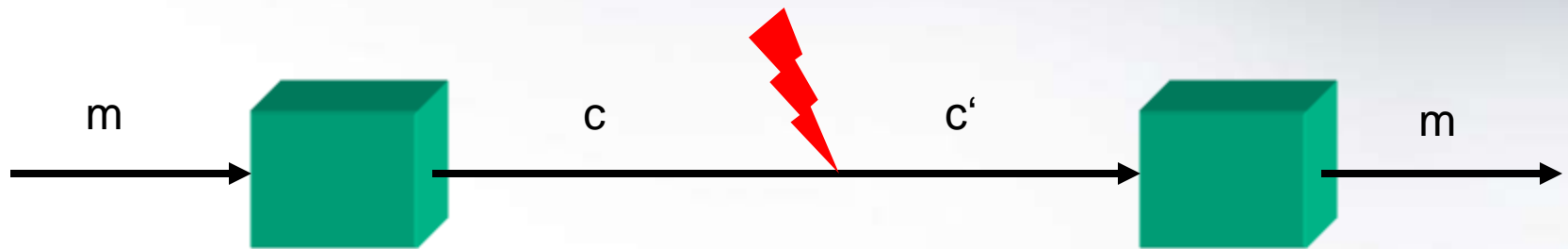


Random linear codes are good, but difficult to decode.

# McEliece



Error Correcting Codes



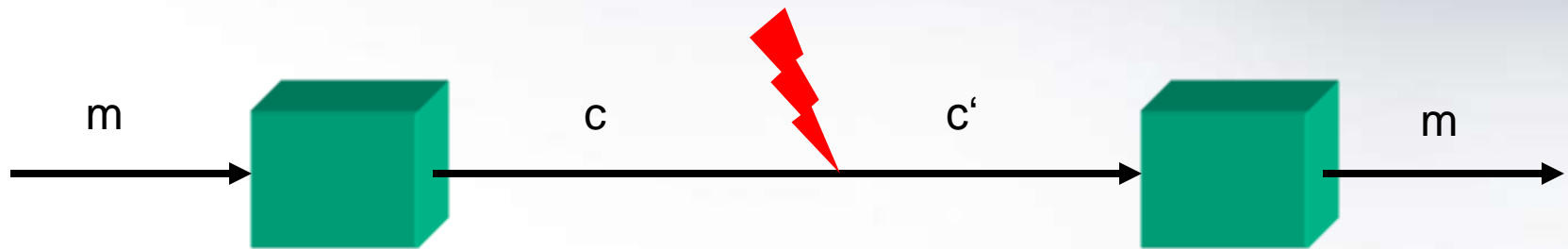
Random linear codes are good, but difficult to decode.

NP complete

# McEliece



Error Correcting Codes



Random linear codes are good, but difficult to decode.

McEliece turned this into a public key scheme

# Goppa Codes



Goppa codes are algebraic geometry codes with good error correction properties.

# Scrambled Goppa Codes



$$P \cdot G \cdot S = G'$$

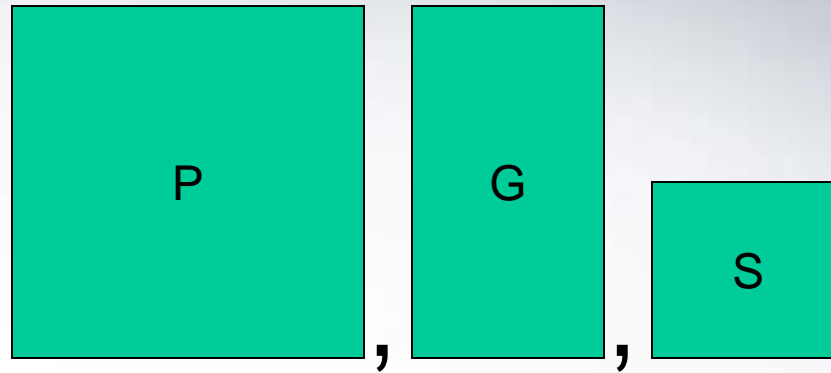
The diagram illustrates the scrambling process of a Goppa code. It consists of four teal-colored rectangular boxes with black outlines. From left to right: a large square box labeled 'P', a tall vertical rectangular box labeled 'G', a smaller square box labeled 'S', an equals sign, and another tall vertical rectangular box labeled 'G'.

$G'$  looks like a generator matrix of a random code

# The McEliece Cryptosystem



Secret key:



Public key:



# The McEliece Cryptosystem



Encrypt:

$$G' \cdot m + e = c$$

Decrypt:

$$c \cdot P^{-1} \xrightarrow{\text{error correction procedure}} S^{-1} = m$$

random error vector  
with  $t$  errors

# The McEliece Assumptions



- A scrambled Goppa code matrix is indistinguishable from a random matrix
- Decoding a random linear code is hard on average

# The McEliece Assumptions



- PKE
- Digital Signatures
- Secure Computations (Two-Party and Multi-Party)

# Problems



- Large Key Size

**Table 1: A Comparison of Public Key Cryptographic Algorithms at the 80 Bit Security Level**

	Estimated Time (PC)			Limited Lifetime?	Public Key Size (kbits)	Private Key Size (kbits)	Message Size (kbits)
	Setup (ms)	Public Key Operation (ms)	Private Key Operation (ms)				
Lamport Signature	1	1	1	1 signature	~10	~10	~10
Lamport w/Merkle	1	1	1	$2^{40}$ signatures	0.08	~250	~50
McEliece Encryption	0.1	0.01	0.1	no	500	1000	1
McEliece Signature	0.1	0.01	20,000	no	4000	4000	0.16
NTRUENCRYPT	0.1	0.1	0.1	no	2	2	2
NTRUSIGN	0.1	0.1	0.1	$2^{30}$ signatures	2	2	4
RSA	2000	0.1	5	no	1	1	1
DSA	2	2	2	no	2	0.16	0.32
Diffie-Hellman	2	2	2	no	2	0.16	1
ECC	2	2	2	no	0.32	0.16	0.32

# Problems



- No scheme based on McEliece is CCA2 secure in the standard model.

# Brazil



- Interestingly, these last two questions have been recently attacked by Brazilian researchers.

## Compact McEliece Keys from Goppa Codes

Rafael Misoczki<sup>1</sup> and Paulo S. L. M. Barreto<sup>1\*</sup>

Departamento de Engenharia de Computação e Sistemas Digitais (PCS),  
Escola Politécnica, Universidade de São Paulo, Brazil.  
{rmisoczki, pbarreto}@larc.usp.br

SAC 2009

CT-RSA 2009

## A CCA2 Secure Public Key Encryption Scheme Based on the McEliece Assumptions in the Standard Model

Rafael Dowsley<sup>1</sup>, Jörn Müller-Quade<sup>2</sup>, Anderson C. A. Nascimento<sup>1</sup>

<sup>1</sup> Department of Electrical Engineering, University of Brasilia,  
Campus Universitário Darcy Ribeiro, Brasília, CEP: 70910-900, Brazil,  
Email: rafaeldowsley@redes.unb.br, andclay@ene.unb.br

<sup>2</sup> Universität Karlsruhe, Institut für Algorithmen und Kognitive Systeme,  
Am Fasanengarten 5, 76128 Karlsruhe, Germany.  
E-mail: muellerq@ira.uka.de

# Conclusions



- A lot of work to be done
  - Practical Side:
    - More efficient implementations
    - Standards
    - Implementations in practical protocols
  - Theoretical Side:
    - What is possible?

# InfoSec@UnB



- Prof. Anderson C A Nascimento (Crypto)
- Prof. Rafael de Sousa (InfoSec, Computational Trust)
- Prof. Ricardo Puttini (ID Management, Intrusion Detection)