Post Scryptum

Spring School
Village les Ramayes
19-23 mars 2018

Organizers :
Vanessa Vitse
Antoine Joux

Supported by ERC-669891 Almacrypt

Welcome !

Historical Cryptography

Main problem

B C

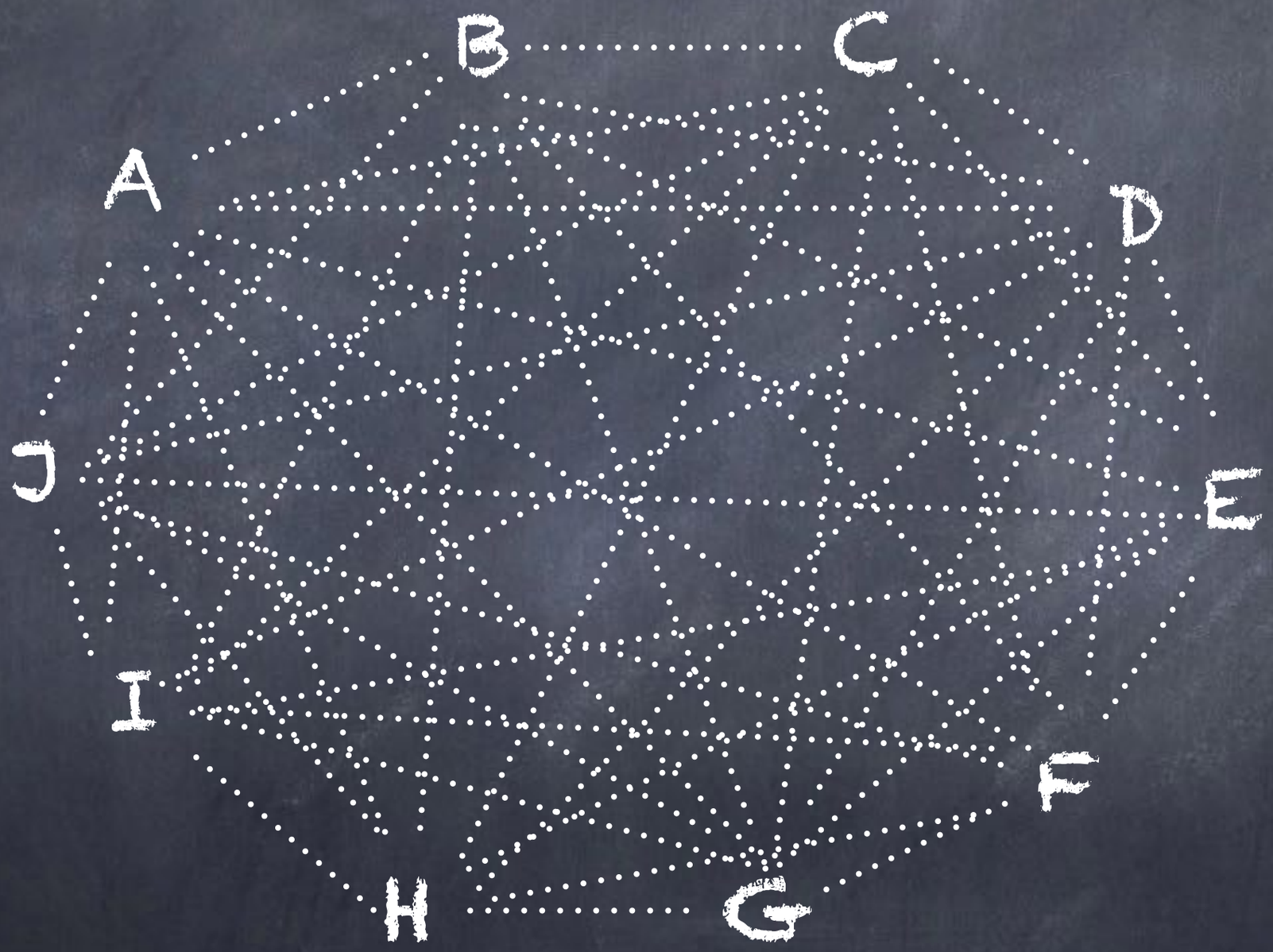
A D

J E

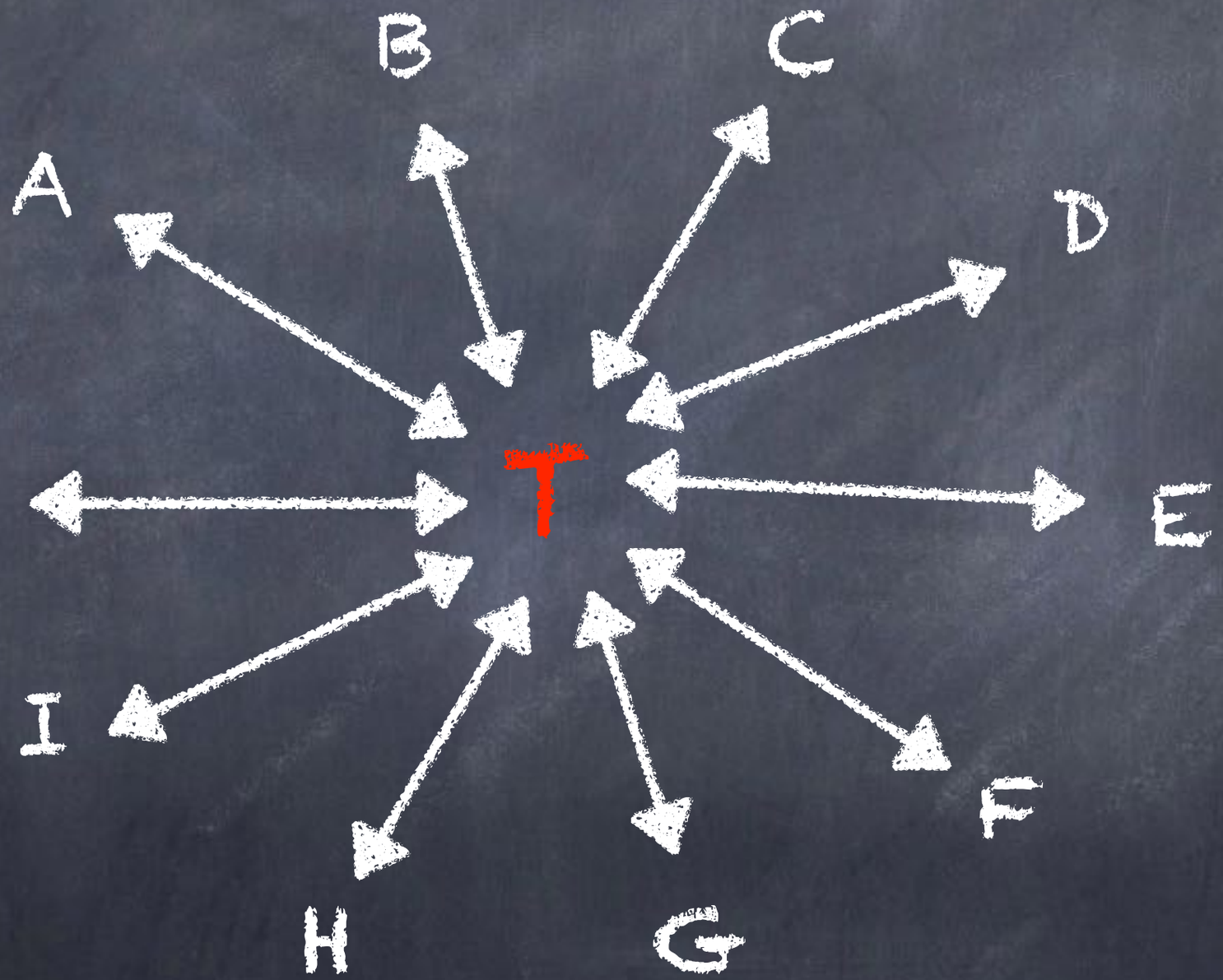
I F

H G

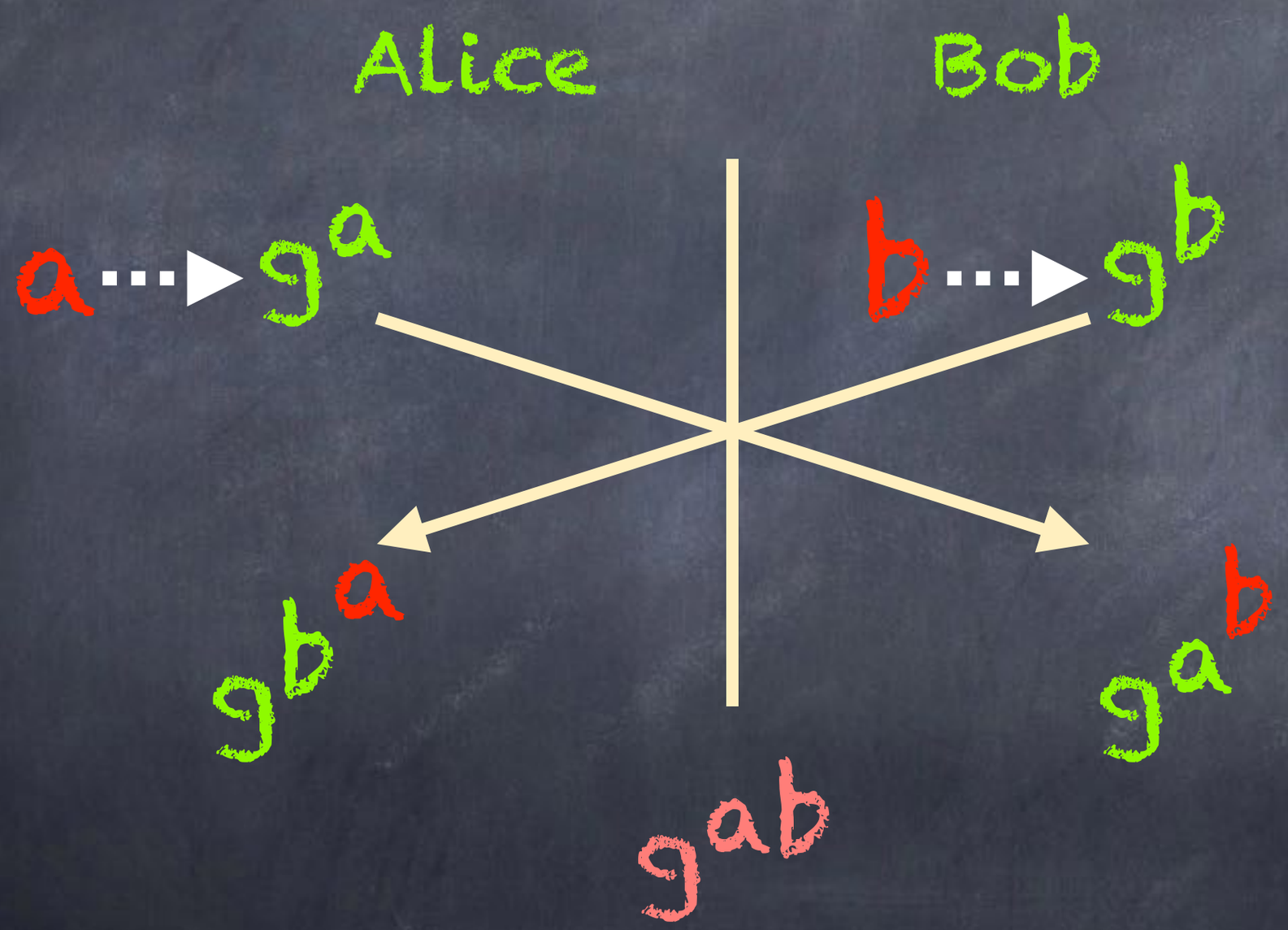
Main problem



Main problem



Public key crypto (Diffie-Hellman 1976)



g generator of a (large) cyclic group

Today

Public-key crypto

Applications

Discrete Log

Factoring

Hard problems (Hopefully)

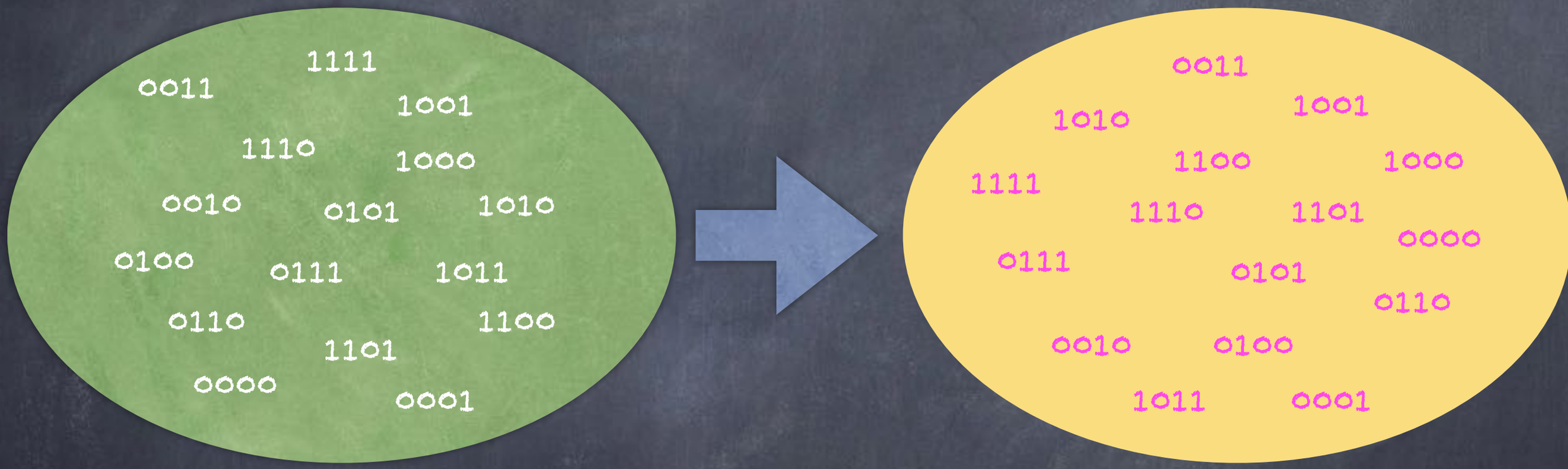
The threat of Quantum Computers

Quantum physics ?

State superposition of a physical object

+

Quantum computer (compute phase)



Quantum computer (measurement phase)

1001

1001

Exhaustive Search

How to go back

For a « perfect » function : time N

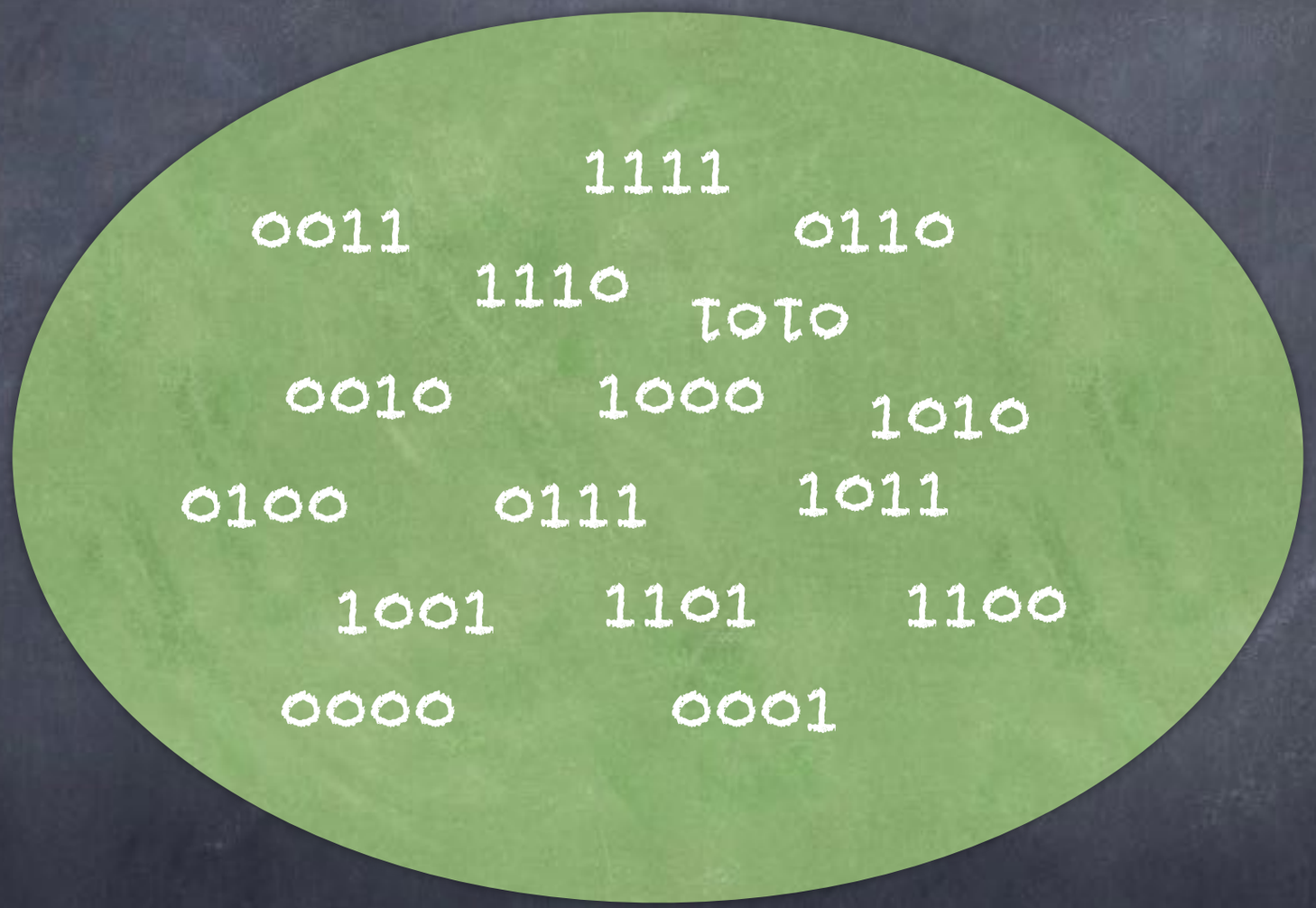
Post-quantum Era

A fast quantum mechanical algorithm for database search

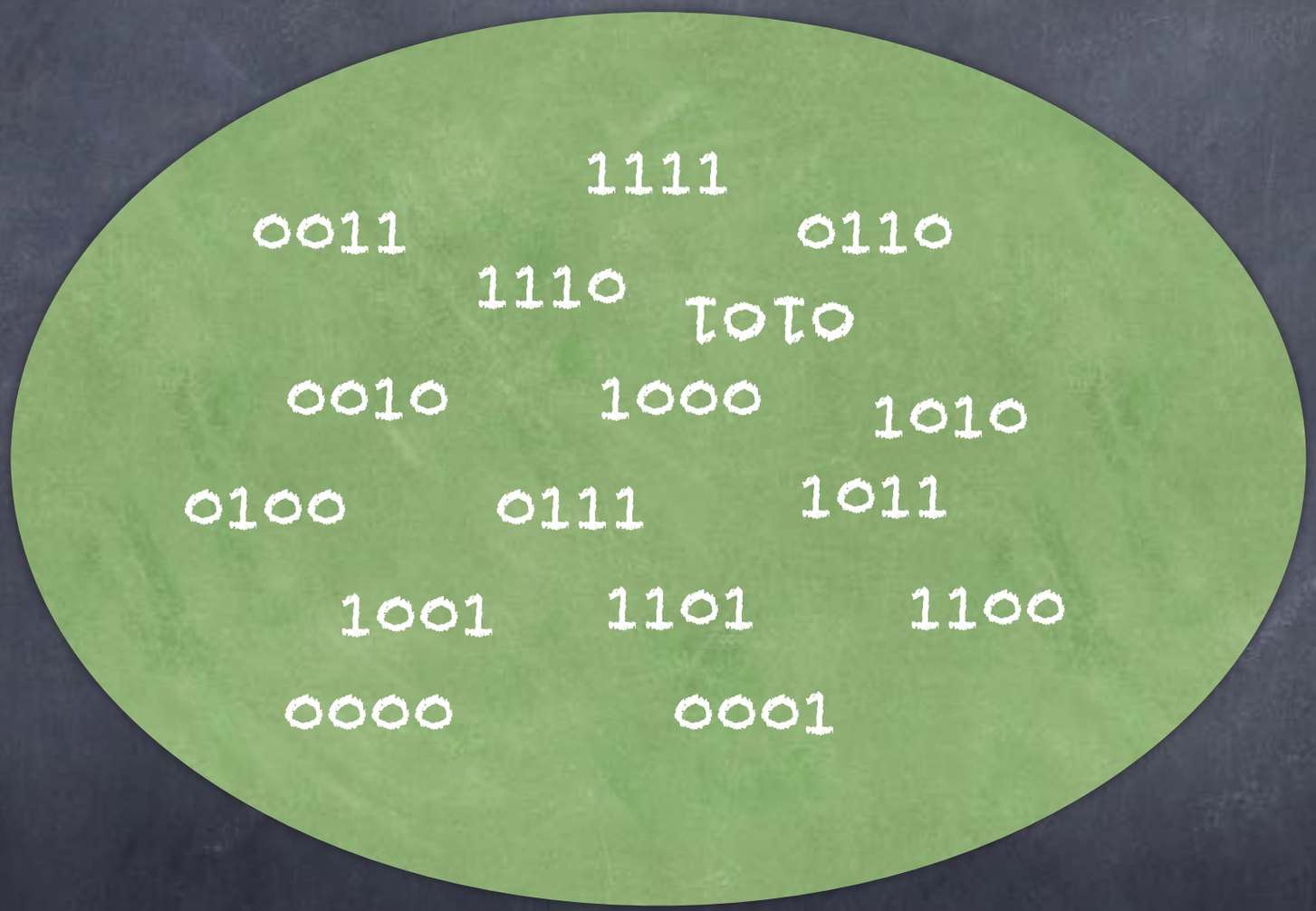
Lov K. Grover
3C-404A, Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkgrover@bell-labs.com

Search within N elts in time Sqrt(N)
(even for a « perfect » function)

Grover


1111
0011
0110
1110
1010
0010
1000
1010
0100
0111
1011
1001
1101
1100
0000
0001

Grover



Running

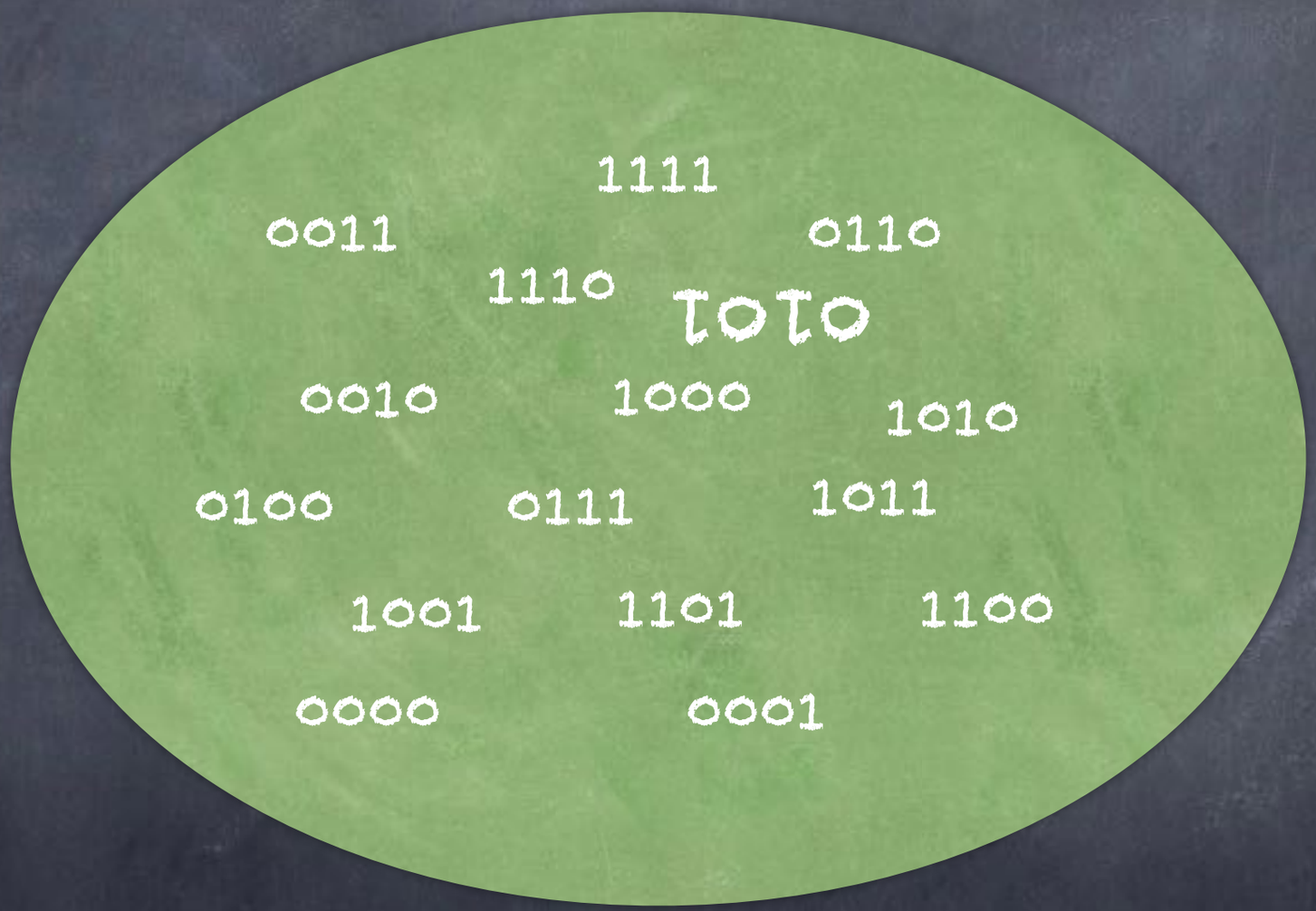
Grover

Running

Grover

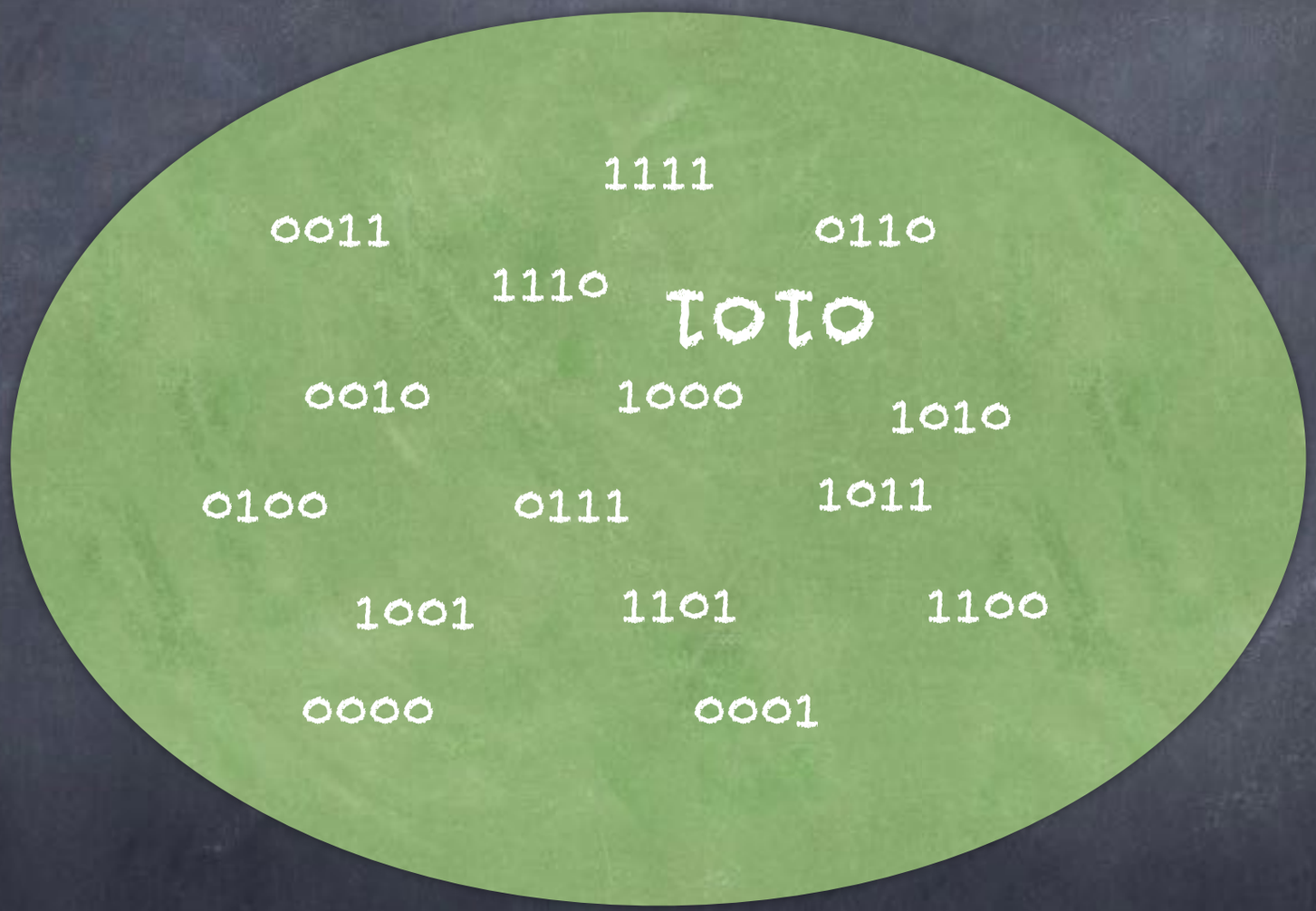
Running .

Grover



Running ..

Grover



Running ...

Grover

toto

Consequences in crypto

Doubling the size of symmetric key !

Post-quantum Era

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

arXiv:quant-ph/9508027v2 25 Jan 1996

Quantum Fourier transform

Consequences

Consequences

The community reacts

Codes MQ Isog. Lattices Mersenne

A post-quantum primer

Mersenne cryptosystem

Mersenne (single bit version)

$p = 2^n - 1$

$H = f/g$ (f and g containing few 1s)

Encryption

a et b with few 1s

$C = \pm(a\ H + b)$

Decryption

$gC = \pm[a\ f + b\ g]$

nb 1 => ±

Mersenne (single bit version)

$p = 2^{31} - 1 = 2147483647 = 0x7FFFFFFF$

$H = f/g = 0x80020000/0x20000008$

$= 0x42E8BE0F$

Encryption

$a = 0x808800$

$b = 0x40000080$

$C = \pm(a\ H + b)$

$= 0x766CAB3A$

Decryption

$gC = 0x1100884A6$

nb 1 = 8 (< 15) => +

$p = 2^n - 1$

Enjoy the school !