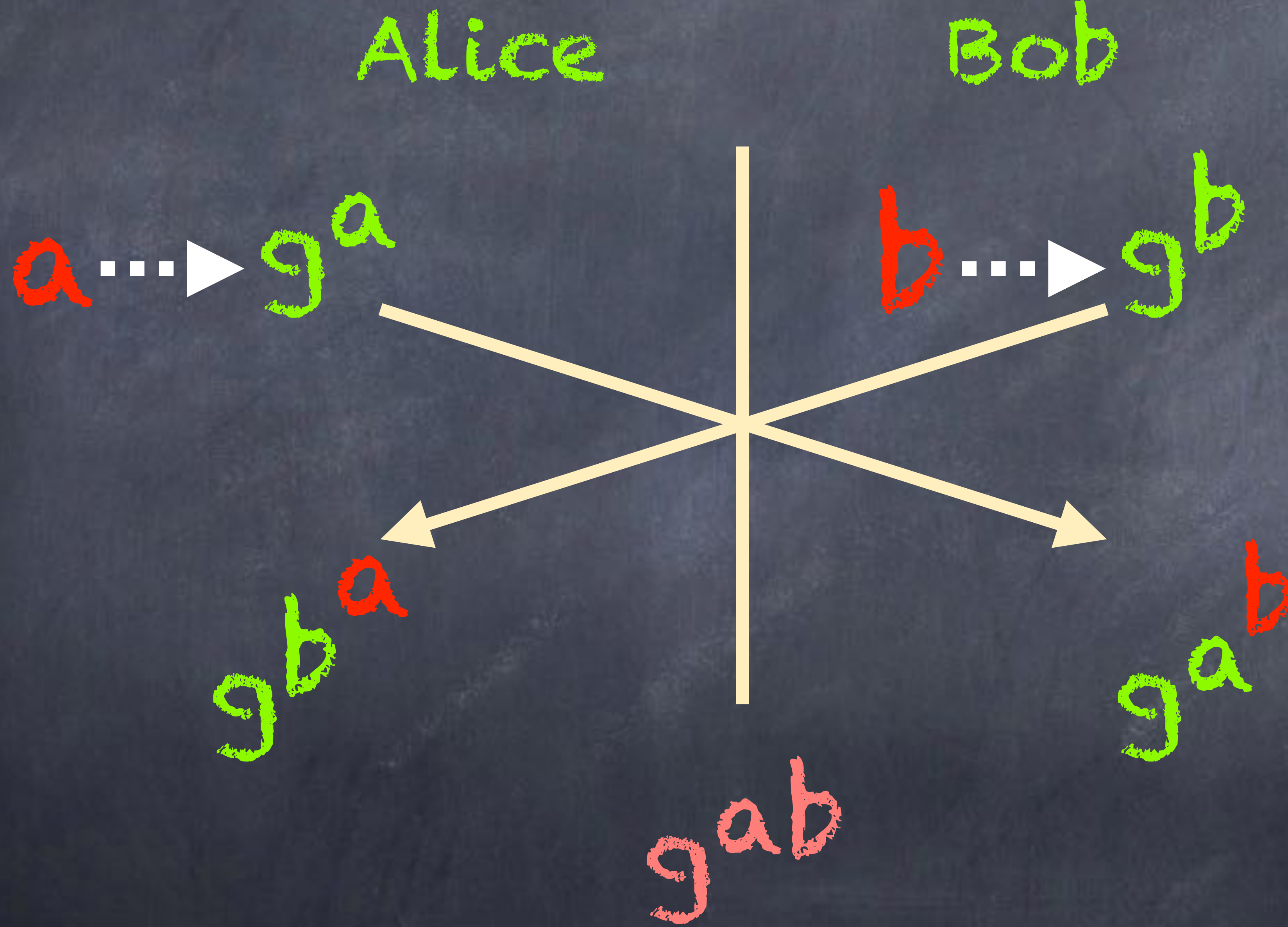
The Mersenne cryptosystem

Latca@Bertinoro
May 21st, 2018

Antoine Joux
joint work with Divesh Aggarwal,
Anupam Prakash and Miklos Santha

Public key crypto
(Diffie-Hellman 1976)



g generator of a (large) cyclic group

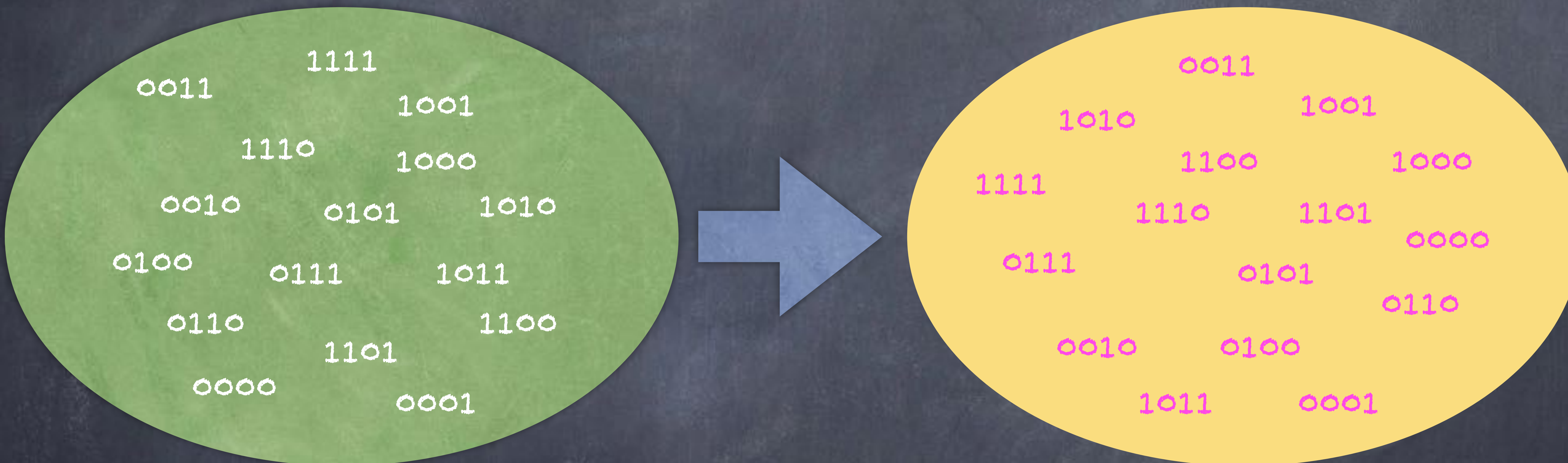
The threat of Quantum Computers

Quantum physics ?

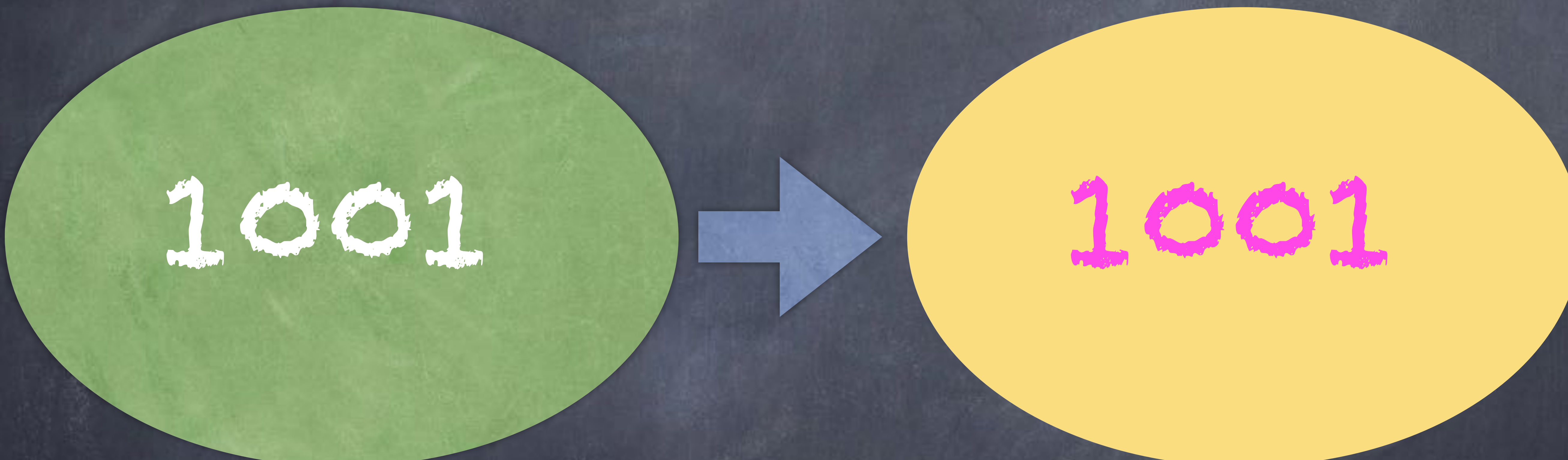
State superposition of a physical object

+

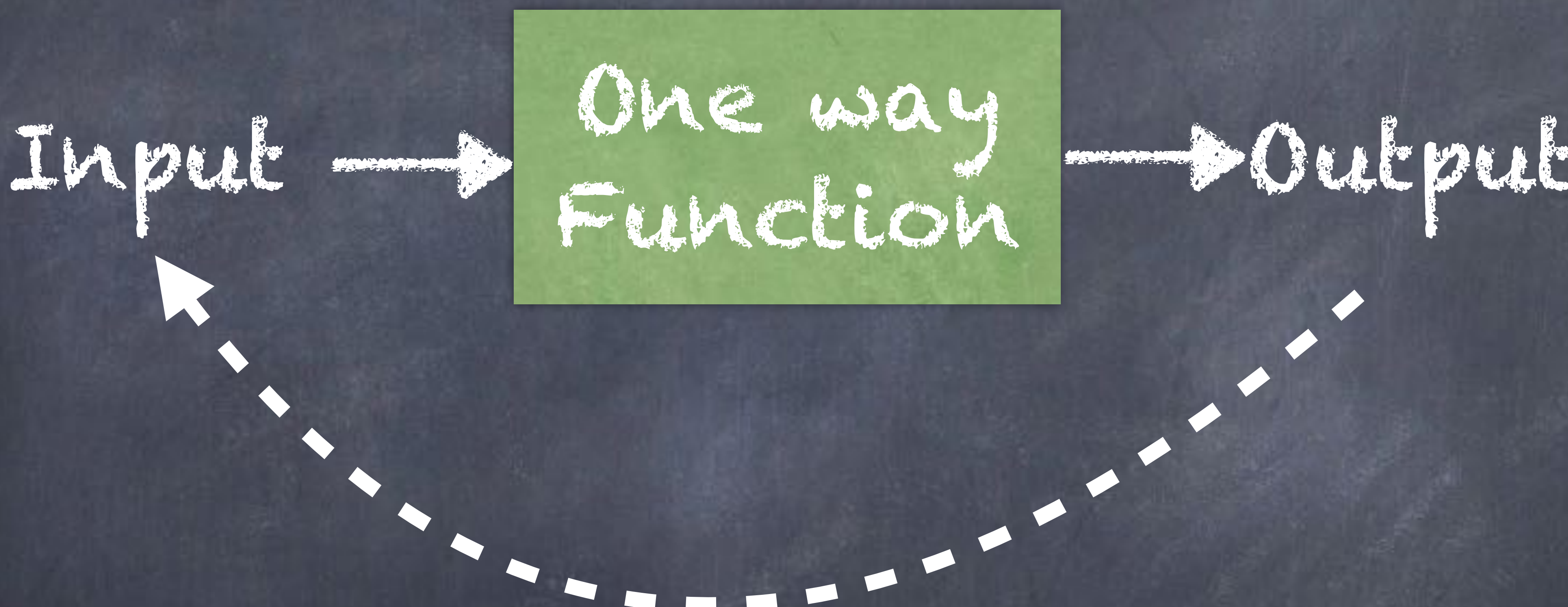
Quantum computer (compute phase)



Quantum computer (measurement phase)



Exhaustive Search



How to go back

For a « perfect » function : time N

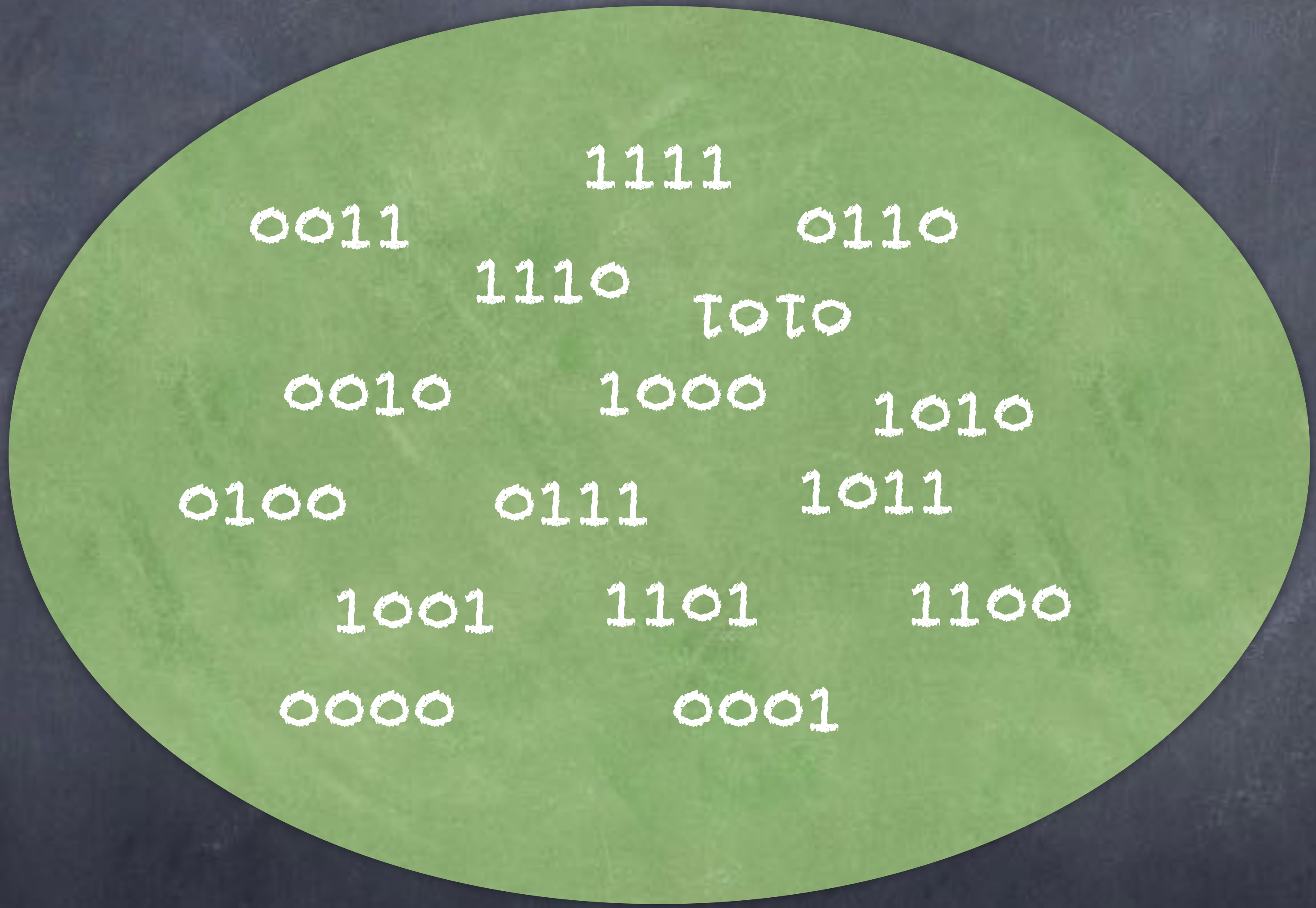
Post-quantum Era

A fast quantum mechanical algorithm for database search

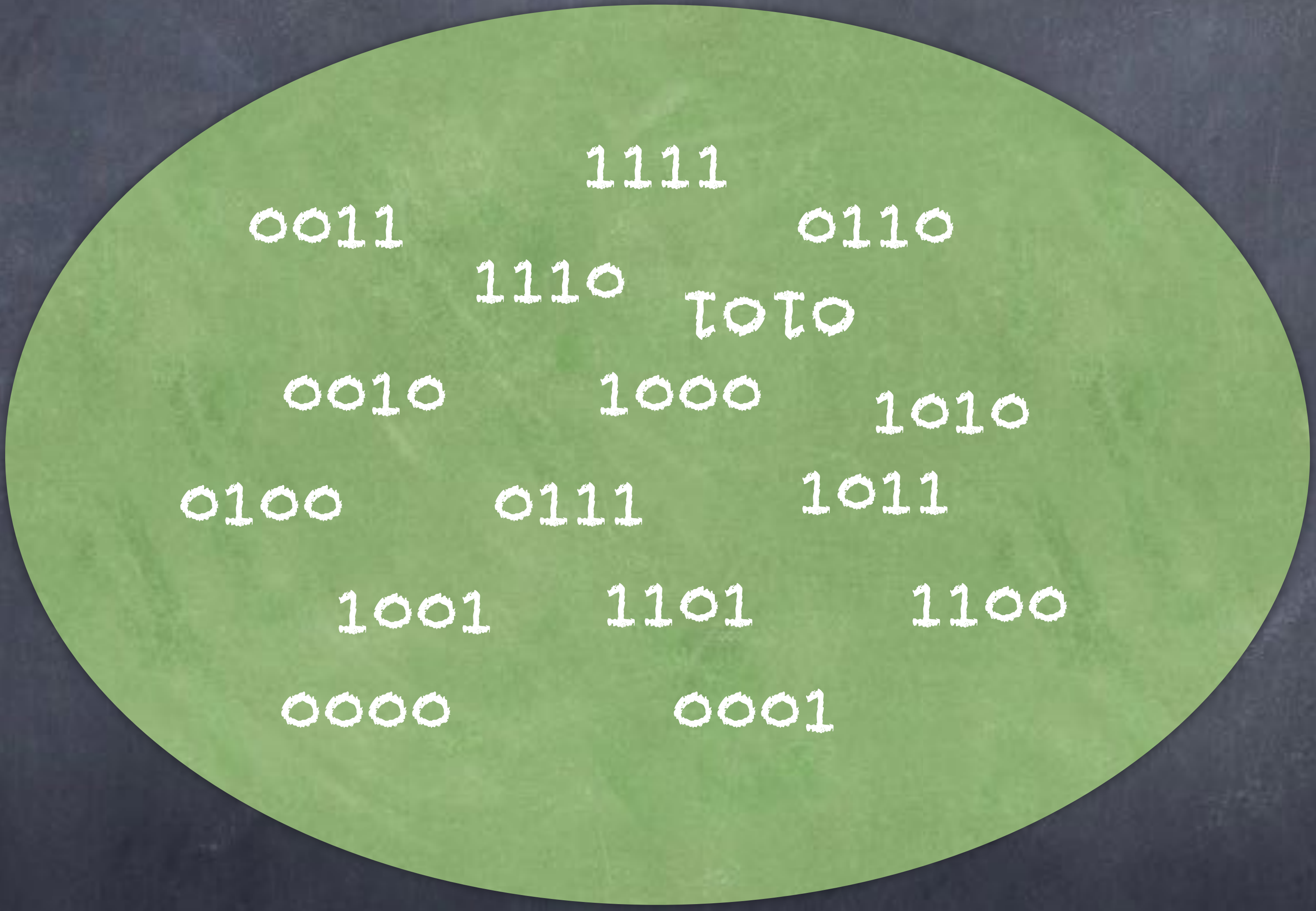
Lov K. Grover
3C-404A, Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkgrover@bell-labs.com

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

Grover

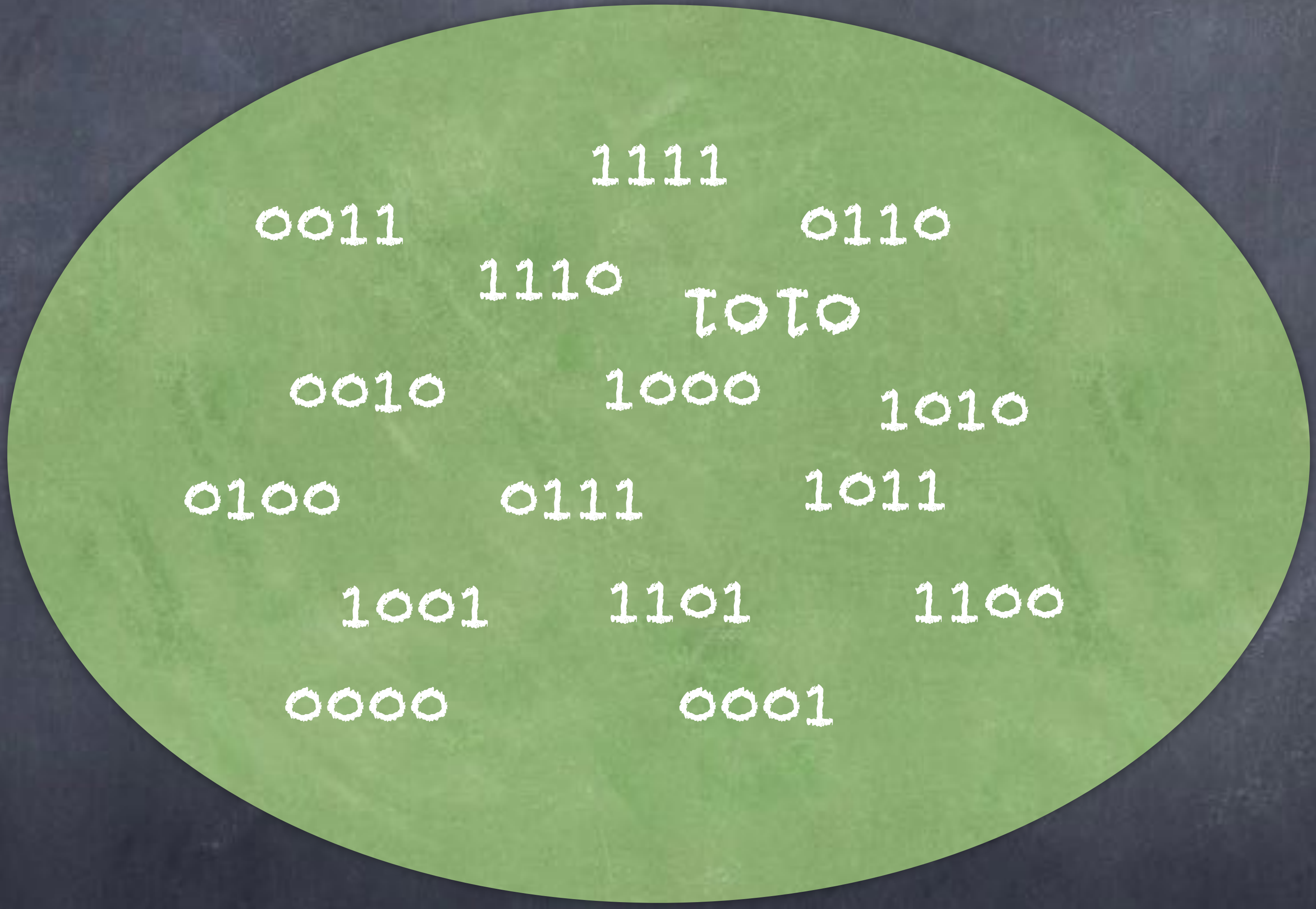

1111
0011
0110
1110
0101
0010
1000
1010
0100
0111
1011
1001
1101
1100
0000
0001

Grover



Running

Grover



Running

Grover

1111

0011 0110

1110 TOTO

0010 1000 1010

0100 0111 1011

1001 1101 1100

0000 0001

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

- Diffie - Hellman
- RSA

No longer secure

Mersenne system

- Inside Ring and Noise family with
  - NTRU
  - Codes
  - Ideal Lattices, RLWE

- With a different Ring
  - Z/pZ (p Mersenne prime)

Mersenne ring and distance

- Ring Z/pZ
  - p a Mersenne prime, i.e., 2^n-1

Let :

- Rp(X)=rep of X in [0,p-1]

- HW(X)=num of 1 in binary of X

Some easy properties of arithmetic mod p

0) $X \equiv (X \bmod 2^n) + (X \operatorname{div} 2^n)$ [mod p]

1) $HW(X+Y) \leq HW(X) + HW(Y)$

2) $HW(XY) \leq HW(X) \times HW(Y)$

3) $HW(Rp(X)) \leq HW(X)$

4) $Rp(X) \neq 0 \Rightarrow HW(Rp(-X)) = n - HW(Rp(X))$

Warm Up

Single bit version

Mersenne basics (single bit version)

H=f/g [mod p]
(f and g containing few 1s, i.e. ≤h)

Encryption

a et b with few 1s

C=±(a H + b)

Decryption

gC=±[a f + b g]
nb 1 => ±

Mersenne basics (single bit version)

$p = 2^{31} - 1 = 2147483647 = 0x7FFFFFFF$
$H = f/g = 0x8002000/0x20000008$
$= 0x42E8BE0F$

Encryption

a=0x80800
b=0x40000080
C=±(a H + b)
=0x766CAB3A

Decryption

gC=0x110084A6
nb 1 = 8 (< 15) => +

Mersenne basics (single bit version)

Analysis of decryption

$$g(aH+b) \equiv af+bg \; [\text{mod } p]$$

$$\begin{aligned} HW(Rp(af+bg)) &\leq HW(a)HW(f)+HW(b)HW(g) \\ &\leq 2\,h^2 \leq n/2 \end{aligned}$$

$$\begin{aligned} HW(Rp(-(af+bg))) &= n - HW(Rp(af+bg)) \\ &\geq n/2 \end{aligned}$$

Multi-bit Mersenne

underlying encryption

Mersenne basics
Change key for more bits

$H = f/g \iff f(-1/H) + g = 0$ [mod p]

I.e. $f R + g = 0$

$T = f R + g$ [mod p]
(R fully random)

Mersenne
(basic multi-bit encrypt)

$T = fR + g$ [mod p] (R fully random)

Encryption

$C1 = a\ R + b1$

$C2 = a\ T + b2$

$E(m) = (C1, C2 \oplus Enc(m))$

Decryption of $(C1, Z)$

$C2' = f\ C1$

$m = Dec(C2' \oplus Z)$

Enc and Dec : Encoding / Decoding

Mersenne
(basic multi-bit encrypt)

Analysis of decryption

$C2 = afR + (ag+b2)$
$C2' = afR + b1\,f$

$\text{Hdist}(C2, C2') \leq \text{Hdist}(C2, afR) + \text{Hdist}(C2', afR)$

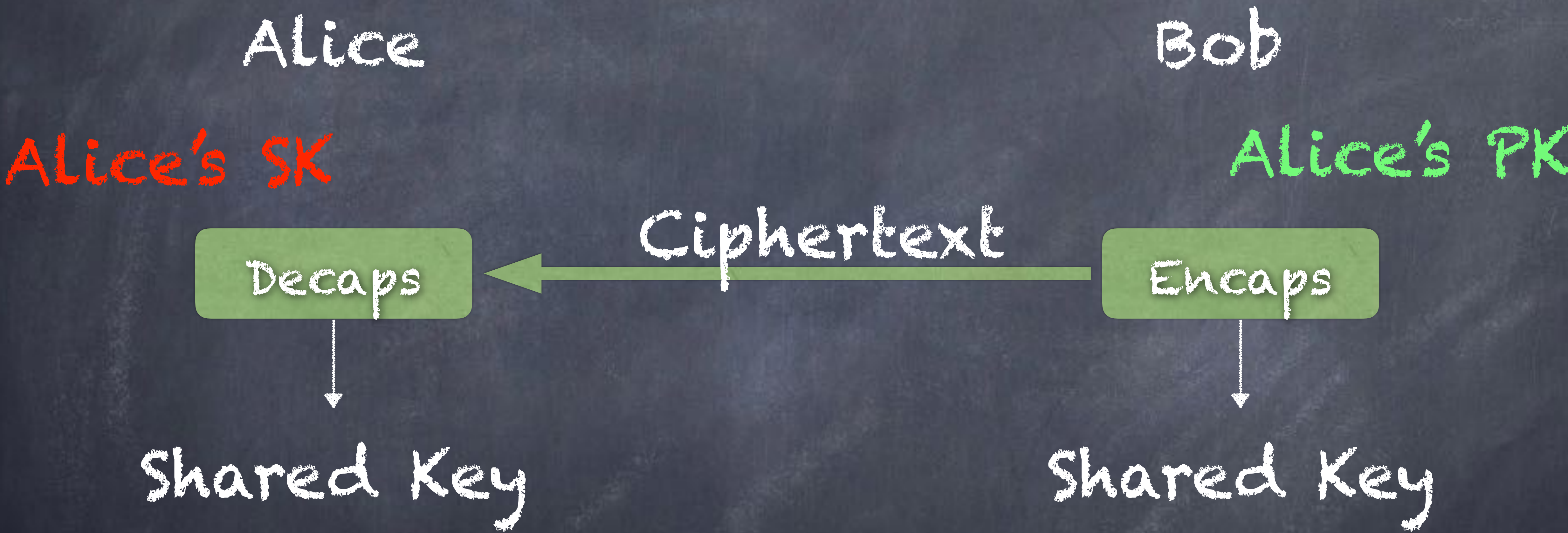
Thus Dec(Enc(m) + small error) = m

Heuristic : Error is well distributed
Allows to use simple repetition code

Multi-bit Mersenne

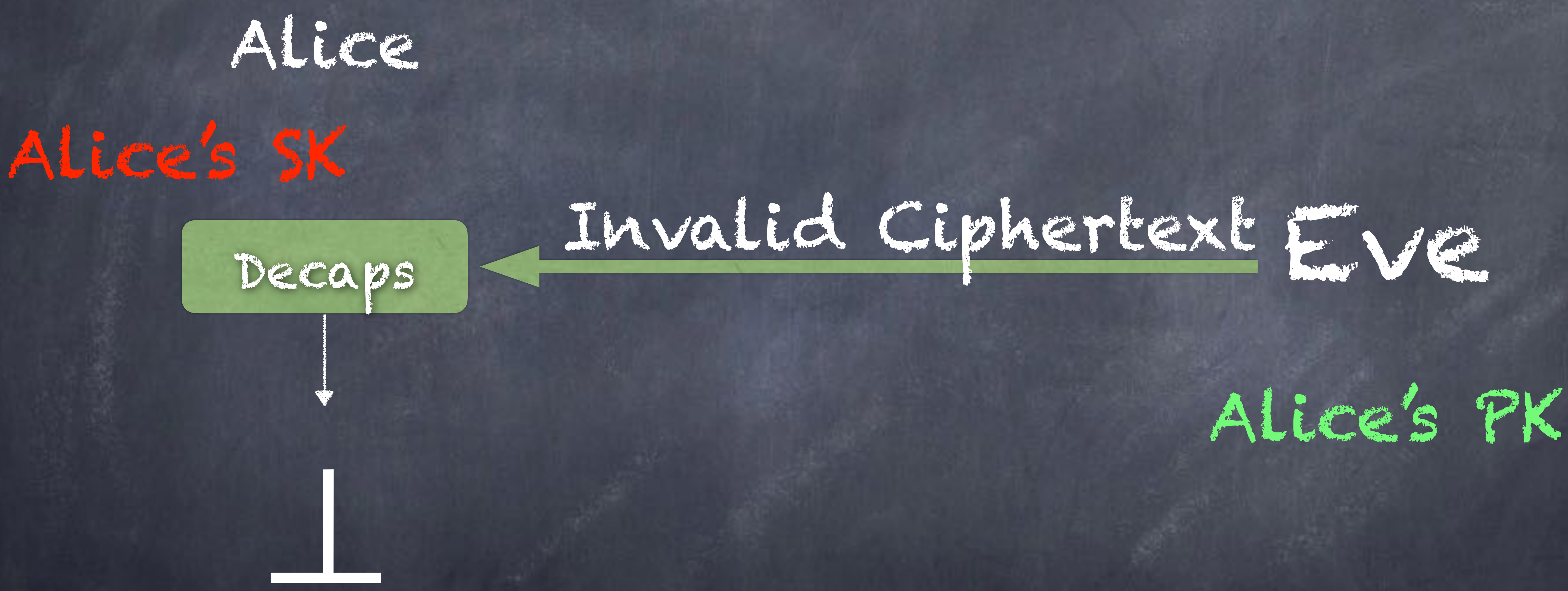
CCA-KEM

CCA-KEM



Alice
Bob
Alice's SK
Alice's PK
Ciphertext
Decaps
Encaps
Shared Key
Shared Key

CCA-KEM under active attack



Mersenne KEM encaps (with CCA security)

S = Random seed

1) Initialize PRNG/XOF from s
2) Produce pseudo random shared secret
3) Run basic encryption of s
   (getting a, b1, b2 from PRNG)
4) Output (C1, Z)

Mersenne KEM decaps (with CCA security)

1) Run basic decryption on (C1, Z)
2) Re-encapsulate from s
3) Compare and Output
    a) Shared secret
    b) or ⊥

Mersenne parameters

$n = 756839$

Low HW parameter $h=256$

Encode 256 bits:
with 2048-repetition coding

Repetition Code and Heuristic

- Window decrypts if < 1024 errors

- Only have a global bound
- Heuristic: it's well distributed

- Alternative solution:
  (Pseudo-)Randomly permute bits

Hard Problem

Distinguish

Hidden low weight

(R1, R2,
a R1+b1, a R2+b2)

a, b1, b2 with low HW

Random tuple

(R1, R2, R3, R4)

=> Semantic Security

Best Known attacks (for proposed params)

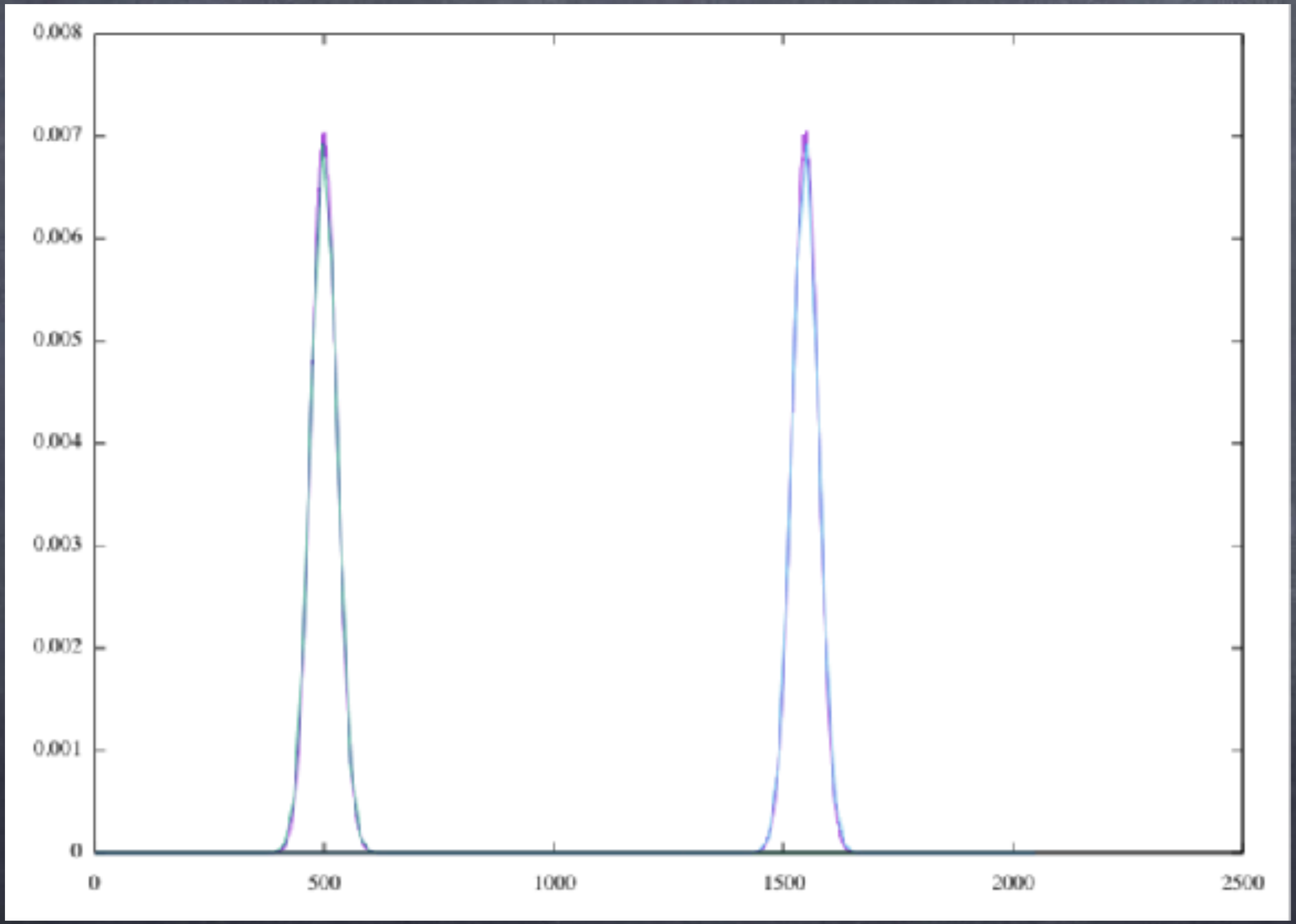
Classical : Worse than $2^{2h} \ll \binom{n-1}{h-1}^{1/2}$

Quantum : Worse than $2^{h} \ll \binom{n-1}{h-1}^{1/3}$

- (Generalized) weak key attacks
- (Noisy) birthday paradox technique

Conclusion

Heuristics


0.008
0.007
0.006
0.005
0.004
0.003
0.002
0.001
0
0
500
1000
1500
2000
2500