The Mersenne-756839 cryptosystem

Antoine Joux

joint work with Divesh Aggarwal, Anupam Prakash and Miklos Santha

Mersenne system

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

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

Mersenne system Advantages

Main advantage: Simplicity

Required familiarity argument:

They are named after Marin Mersenne, a French Minim friar, who studied them in the early 17th century. (Wikipedia)

Mersenne ring and distance

- Ring $\mathbb{Z}/p\mathbb{Z}$
  - 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) $X \equiv (X \bmod 2^n) + (X \operatorname{div} 2^n) \pmod p$
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)

$H = f/g \pmod p$
(f and g containing few 1s, i.e. $\leq h$)

Encryption

a et b with few 1s

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

Decryption

$gC = \pm[a\,f + b\,g]$
nb 1 => ±

Mersenne basics (single bit version)

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

$H = f/g = 0x80002000/0x20000008$

$= 0x42E8BE0F$

Encryption

$a = 0x80800$

$b = 0x40000080$

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

$= 0x766CAB3A$

Decryption

$gC = 0x1100844A6$

$wb\ 1 = 8\ (< 15) \Rightarrow +$

Mersenne basics (single bit version)

Analysis of decryption

$$g(aH+b) \equiv af+bg \pmod{p}$$

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

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

Multi-bit Mersenne

underlying encryption

Mersenne basics
Change key for more bits

$$H = f/g \pmod p \quad \Leftrightarrow \quad f(-1/H) + g = 0 \pmod p$$

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

$T = f R + g \pmod p$ (R fully random)

Mersenne
(basic multi-bit encrypt)

$T = fR + g \pmod p$ (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

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

$Hdist(C2,C2') \leq Hdist(C2,afR) + Hdist(C2',afR)$

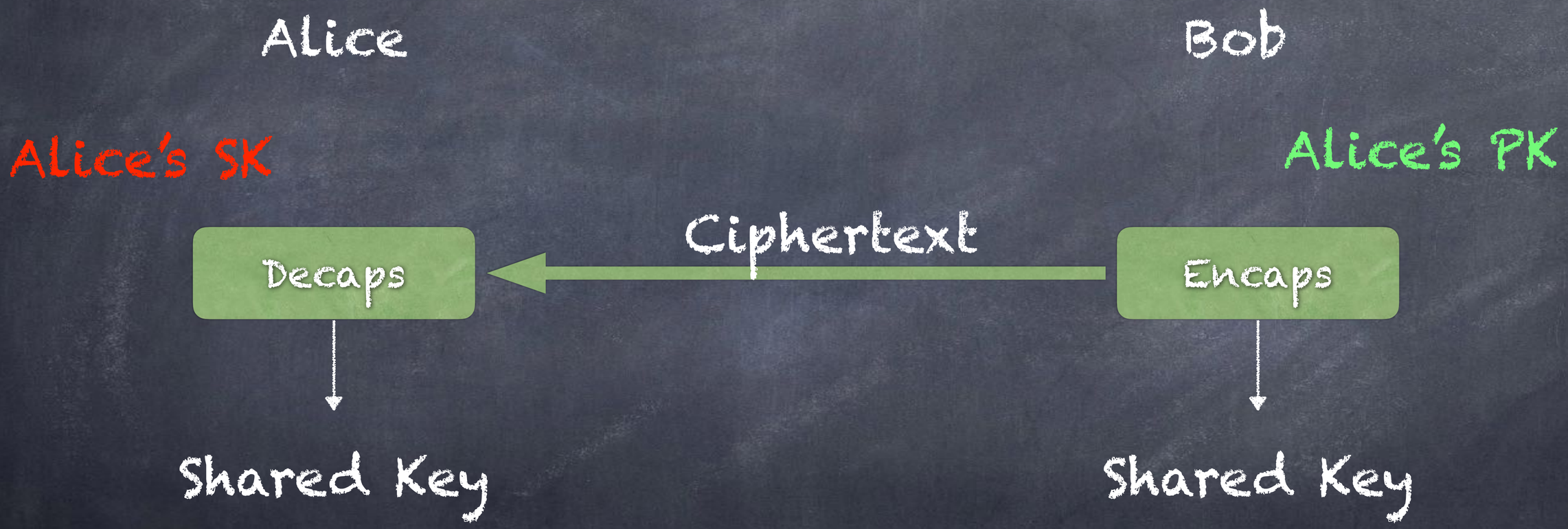
Thus $Dec(Enc(m) + \text{small error}) = m$

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

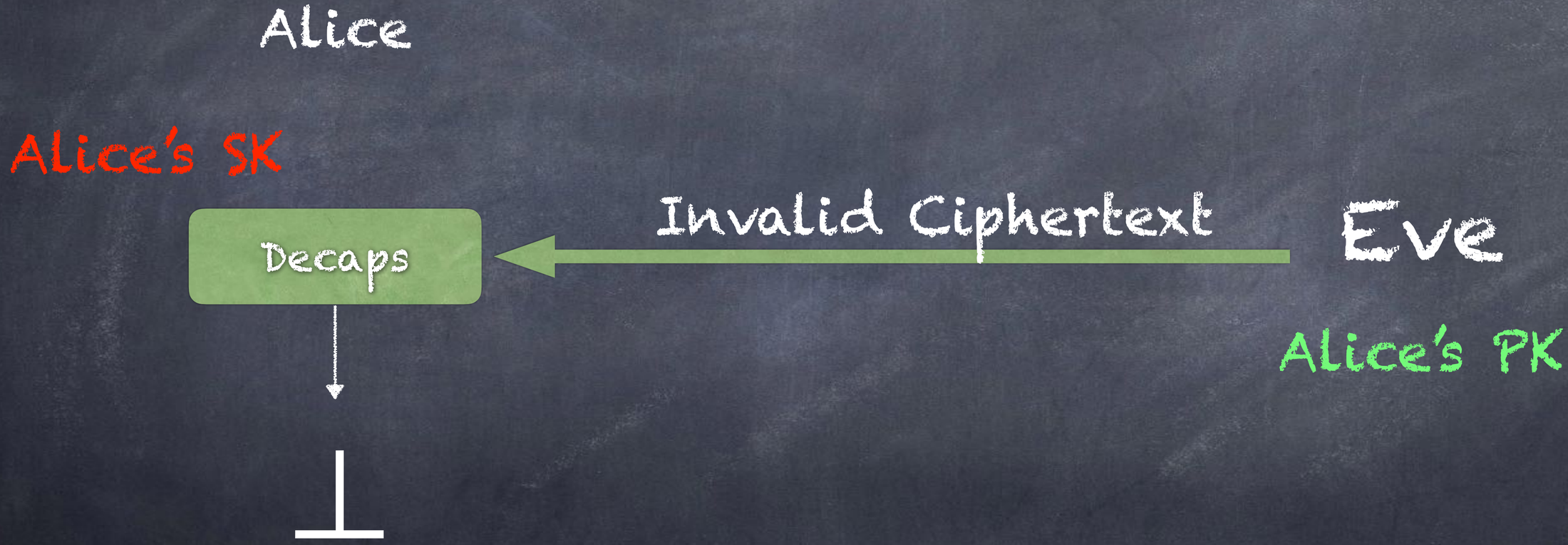
Multi-bit Mersenne

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)

We used the XOF provided by NIST – Easy to change

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 $\perp$

Mersenne SK compression

SK = Short private key

1) Initialize PRNG/XOF from SK
2) Produce pseudo random R, f, g
3) Public key is (R,T)
4) Long private key is f

Also prevents generation of weak keys

Mersenne parameters

$n = 756839$

Low HW parameter $h=256$

Encode 256 bits:
with 2048-repetition coding

Mersenne KEM data

Timings on Intel Core i7-4980HQ @2.8GHz

KeyGen: 5.3 ms
Encapsulate: 7.2 ms
Decapsulate: 16.2 ms (Opt 10.5 ms)

Sizes: PK 184.8 KB ; SK 32 B; KEM 156.4 KB
Decryption failure Pr: $< 2^{-239}$

Code size: 367 (resp. 381) lines of C

No Patents (that we know of)

Optimization TBD

- Make sparse/dense multiplication faster
- Reuse RSA hardware multiplier for speed-up
- Use faster XOF

Hard Problem

Distinguish

Hidden low weight

$(R_1, R_2, a R_1+b_1, a R_2+b_2)$

a, b_1, b_2 with low HW

Random tuple

(R_1, R_2, R_3, R_4)

Best Known attacks (for proposed params)

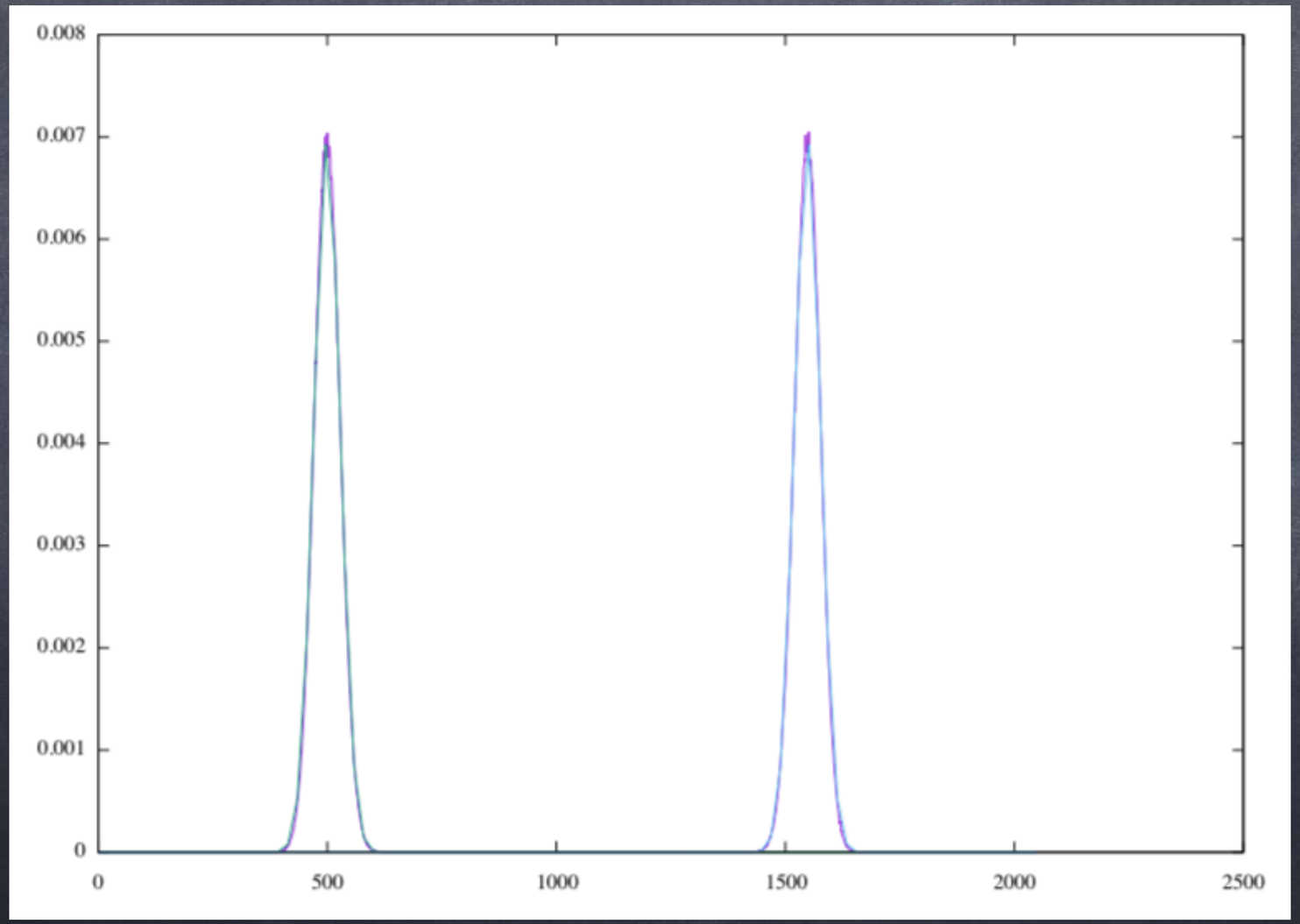
Classical : Worse than $2^{2h} << \binom{n-1}{h-1}^{1/2}$

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

Consistent with targeted level 5

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