A new public-key crypto system via Mersenne numbers

Divesh Aggarwal

joint work with Antoine Joux, Anupam Prakash and Miklos Santha

Public-key cryptography

-Introduced by Diffie and Hellman in [DH76]

-Many candidates over the years

-The quest in the recent years has shifted to advanced primitives

-In this work, we propose an arguably simpler PKC scheme.

-We also believe it is secure against quantum attacks.

Mersenne cryptosystem

- Belongs to the Ring and Noise family with
  - NTRU
  - Code-based crypto
  - Ring LWE based crypto

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

- a different Noise: Hamming weight mod p.

Mersenne cryptosystem

Mersenne primes: They are primes of the form $p=2^n-1$, where n is a prime, and is named after Marin Mersenne, a French mathematician, who studied them in the early 17th century. (Wikipedia)

Main advantage of the cryptosystem: Simplicity

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 rep of X mod p

Some properties of arithmetic mod p

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

```
 11010100111001
+00000000001000
_______________
=11010101000001
```

2) For all i, $HW(X\,2^i) = HW(X)$

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

Induction

4) $HW(-X) = n - HW(X)$

Warm Up

Single bit version

Hard problem

p = 2^n - 1, h << n

f, g are numbers mod p with few (< h) 1s in binary rep.

H=f/g [mod p]

Assumption: Given H, obtain f, g.

Single bit version

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

Encryption

a and b with few 1s

$C0 = Enc(0) = (a\ H + b)$
$C1 = Enc(1) = -(a\ H + b)$

Decryption

$gC = \pm [a\ f + b\ g]$
Compute HW(gC)
Small => 0
Large => 1

Toy Example

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

$H=f/g=0x8002000/0x20000008$

$=0x42E8BE0F$

Encryption

a=0x80800

b=0x40000080

$C = Enc(0) = (a\ H + b)$

$=0x766CAB3A$

Decryption

$gC = 0x110084A6$

$HW(gC) = 8\ (< 15) \Rightarrow 0$

Correctness of decryption

For correctness, we need $n > 4h^2$

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

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

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

Multi-bit version

underlying encryption

Change public/private key

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

$C1 = a\ R + b1$

$C2 = a\ T + b2$

$Z = C2 \oplus E(m)$

$\mathrm{Enc}(m) = (C1,\ Z)$

Decryption of (C1,Z)

$C2' = f\ C1$

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

E and D : Error correction code

Multi-bit encryption

Analysis of decryption

$$C2 = a\,T + b2 = afR + (ag+b2)$$
$$C2' = f\,C1 = f\,(a\,R + b1) = afR + b1\,f$$

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

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

Heuristic : Error is well distributed

Allows to use simple repetition code

Analysis of decryption

LEMMA: Let U be a random n-bit string and let x be an n-bit string of Hamming weight h. Then

$$\Pr[\mathrm{Hdist}(U, U + x) > 2h(1 + c)] < \text{negligible}$$

EXAMPLE:

11001010101011110101110101000111110100101

+00001000000010001000000001000010000100010

11010010101101111101110101101001111000111

Choice of error-correcting code

-Thus, the total number of errors we expect is at most $e = 2\ (2\ h^2 + h)$

-We need an ECC correcting e out of n errors

-Can use Reed Muller codes, and $n = O(h^2)$

-The number e is clearly an overestimate of the no. of errors in practice

-Also, we expect the errors to be distributed randomly

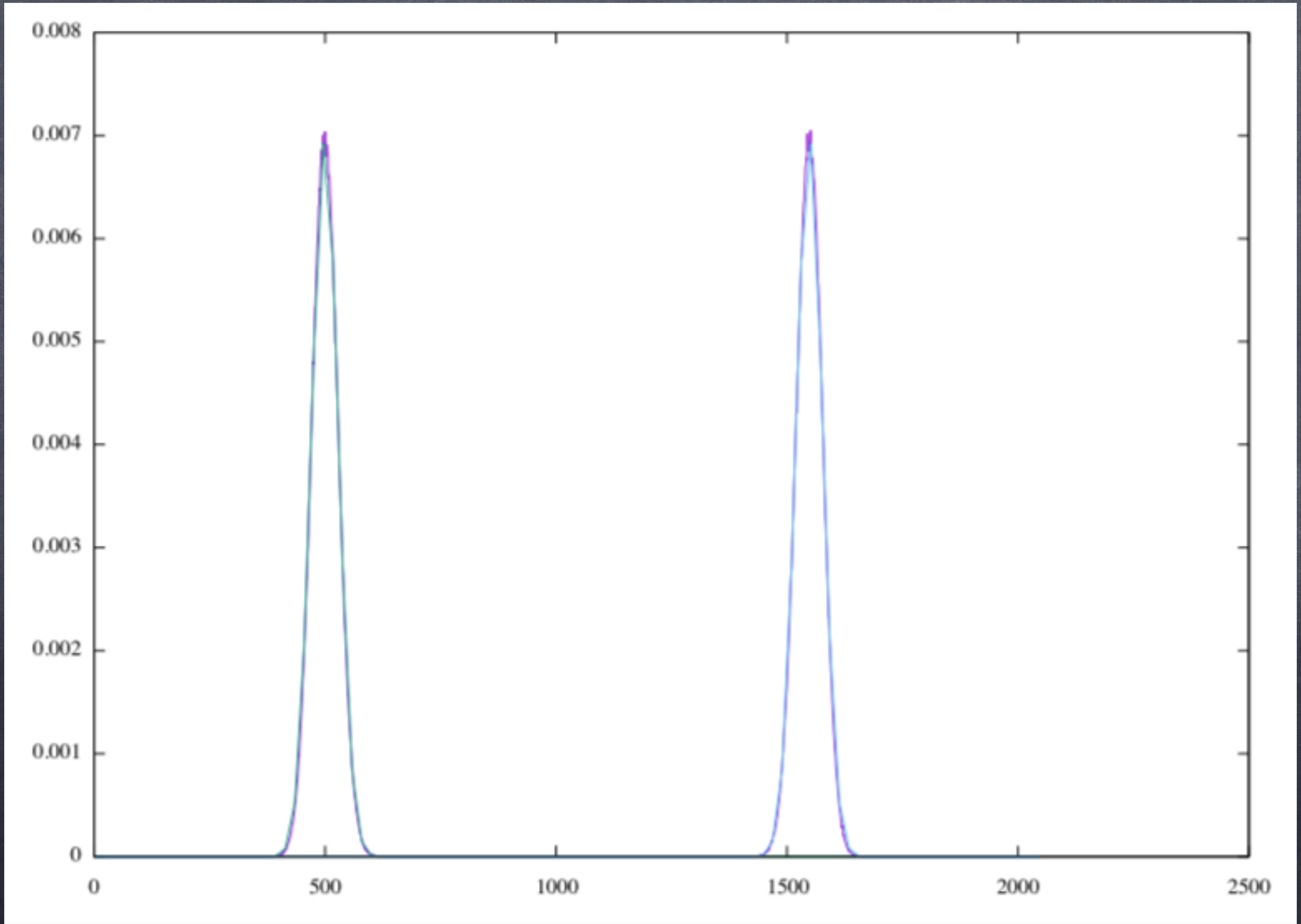
Recommended parameters

n = 756839

Low HW parameter h=256

Encode 256 bits:
with 2048-repetition coding

Heuristics


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

Hard Problem

Distinguish

Hidden low weight

(R1, R2, aR1+b1, a R2+b2)

a, b1, b2 with low HW

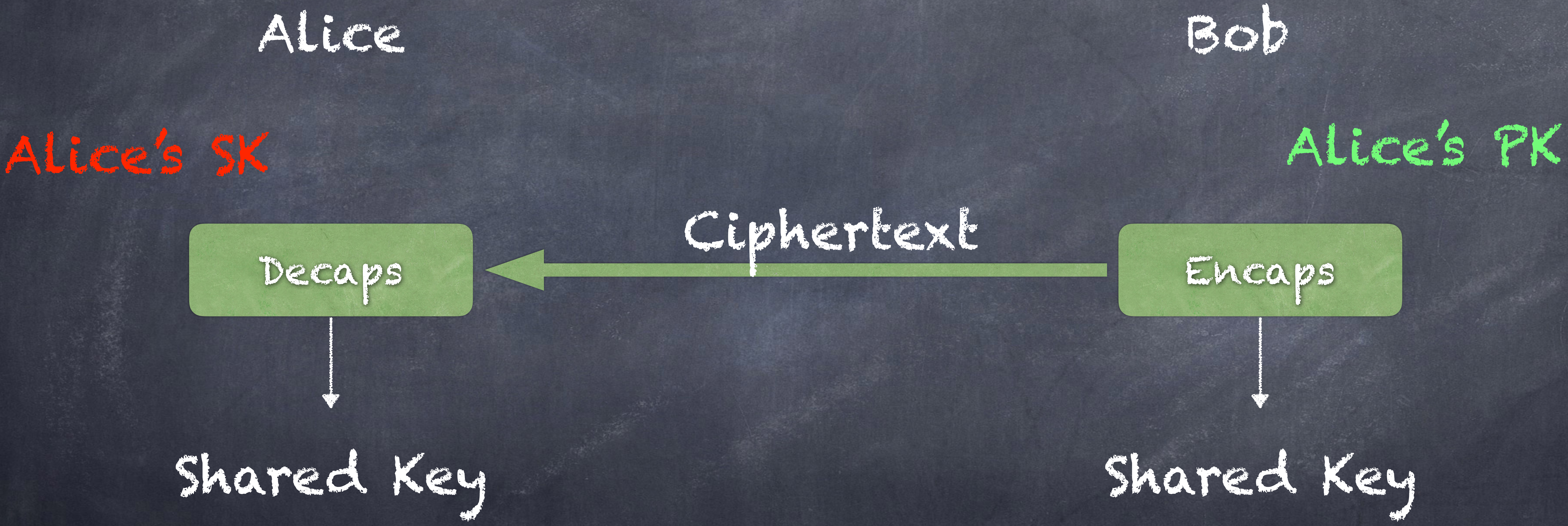
Random tuple

(R1, R2, R3, R4)

Multi-bit Mersenne

CCA-KEM

CCA-KEM



Alice

Bob

Alice's SK

Alice's PK

Decaps

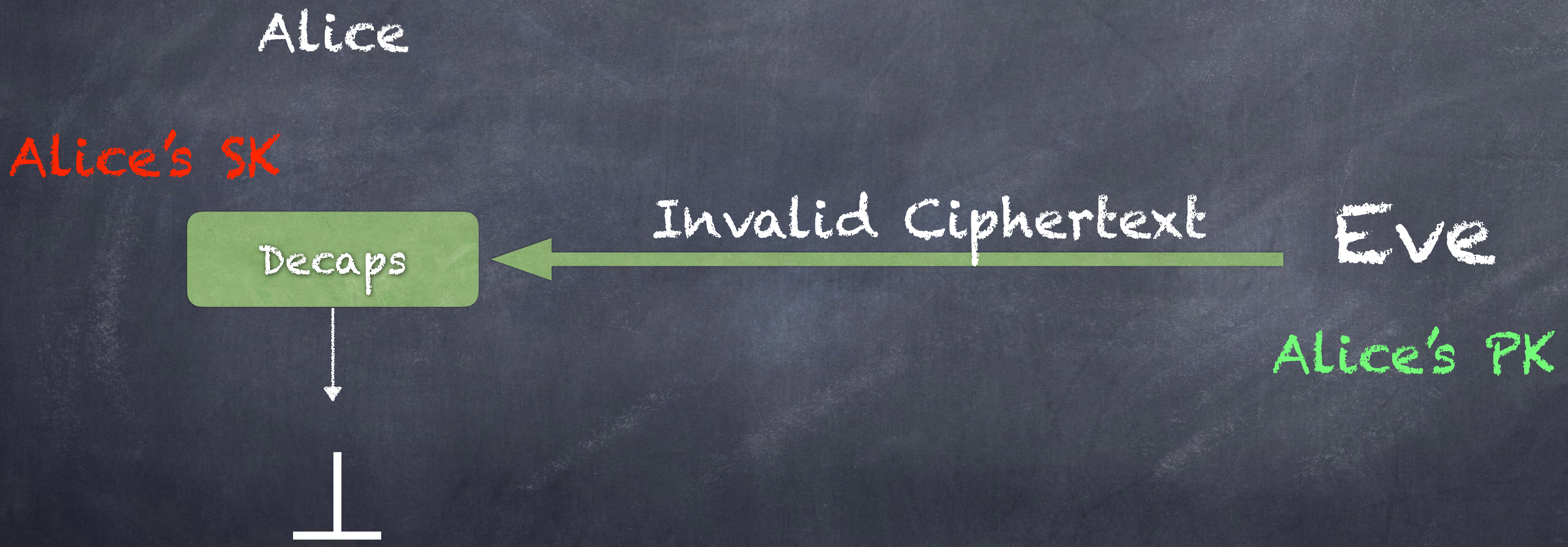
Ciphertext

Encaps

Shared Key

Shared Key

CCA-KEM under active attack



Alice

Alice's SK

Decaps

$\perp$

Invalid Ciphertext

Eve

Alice's PK

Mersenne KEM encaps (with CCA security)

S = Random seed

1) Initialize PRG from s
2) Produce pseudo random shared secret
3) Run basic encryption of s
   (getting a, b1, b2 from PRG)
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 $\perp$

Best Known attacks [BCGN17, BDJW18] (for proposed params)

Trivial : $\binom{n}{h}$

Best Classical : At least 2^{2h}

Best Quantum : At least 2^{h}

Future Work

-Cryptanalysis

-Improve efficiency without compromising security

Thank You