Postquantum Crypto Project
Round 3 Updates: SIKE, FrodoKEM

November 13, 2020

Carl A. Miller

NIST Computer Security Division

Internal talk - not for public distribution

SIKE

(Supersingular isogeny key exchange)

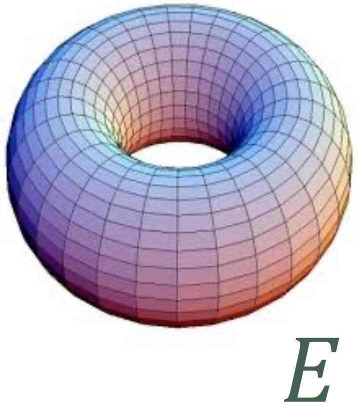
Review of SIKE

SIKE is based on elliptic curves.

Smooth algebraic curves of the form

$$y^2 = f(x),$$

where deg f = 3.



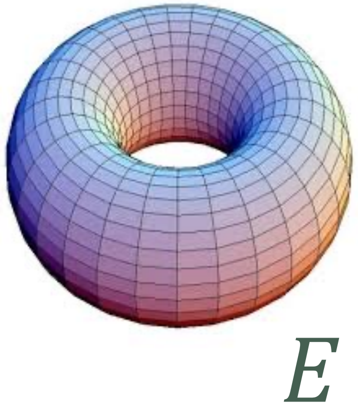
Review of SIKE

SIKE is based on elliptic curves.

For any prime power q, the points $\mathrm{E}(\mathbb{F}_q)$ form a finite abelian group.

SIKE uses elliptic curves for which

$$\left|E\left(\mathbb{F}_q\right)\right| = 2^{\mathrm{c}}3^{\mathrm{d}}.$$



Review of SIKE

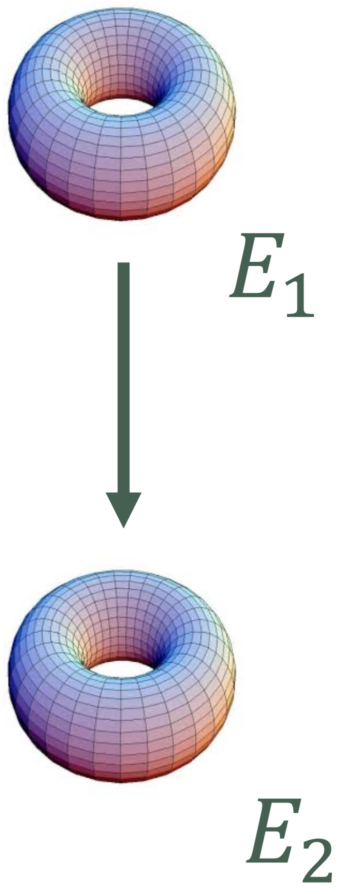
SIKE is based on elliptic curves.

For any prime power q, the points $\mathrm{E}(\mathbb{F}_q)$ form a finite abelian group.

SIKE uses elliptic curves for which

$$|E(\mathbb{F}_q)| = 2^{\mathrm{c}}3^{\mathrm{d}}.$$

An **isogeny** is an algebraic map that is also a group homomorphism.



Review of SIKE

SIKE is Diffie-Hellman style key encapsulation based on isogenies.

E = public curve

Random subgroup $S \subseteq E(\mathbb{F}_q)$

$\Longrightarrow$ isogeny f: $E \to E'$ with kernel S.

Broadcast

Random subgroup $\mathrm{T} \subseteq E(\mathbb{F}_q)$

$\Longrightarrow$ isogeny g: $E \to E''$ with kernel T.

Alice and Bob compute the curve $E''/f(T) \cong E'/g(S)$ and compute their shared key from it.

Key Compression

In the uncompressed version of SIKE, an isogeny f is stored by computing the x-coordinates of the points $\{f(P), f(Q), f(R)\}$ for three fixed points P, Q, R.

In the compressed version, the points $\{f(P), f(Q), f(R)\}$ are expressed as linear combinations of chosen points on the new elliptic curve E'. This "requires roughly half as many bits."

Pohlig-Hellman algorithm

To do this, we need to solve the discrete log problem.

This is done iteratively, exploiting the fact that $\left|E\left(\mathbb{F}_q\right)\right| = 2^{\mathrm{c}}3^{\mathrm{d}}$.

Round 3 Changes

Optimizations for the compression procedure.

Appendix F

Changes made in the 3rd round

The main differences between the second round and third round SIKE submissions are as follows.

- Optimized ARMv8 implementations are now available for all parameter sets.
- Optimized Cortex M4 and VHDL implementations are now available for all uncompressed parameter sets.
- New (space and time) optimizations for compressed SIKE have been added; see Appendix C.
- New pre-computation tables for discrete logarithms have been added, reducing static library sizes for compressed SIKE by 80-90%; see Appendix D.
- Appendix C and Appendix D in the previous version have been swapped.

FrodoKEM

Review of Frodo

Basic LWE assumption: Suppose that A is a random m x n matrix, S is a random n x p matrix, and

$$B = AS + E,$$

where E is Gaussian. Then, given A, the matrix B is indistinguishable from random.

Review of Frodo

Basic LWE assumption: Suppose that A is a random m x n matrix, S is a ~~random~~ n x p matrix, and

Gaussian

B = AS + E,

where E is Gaussian. Then, given A, the matrix B is indistinguishable from random.

This is “normal form” LWE.

Review of Frodo

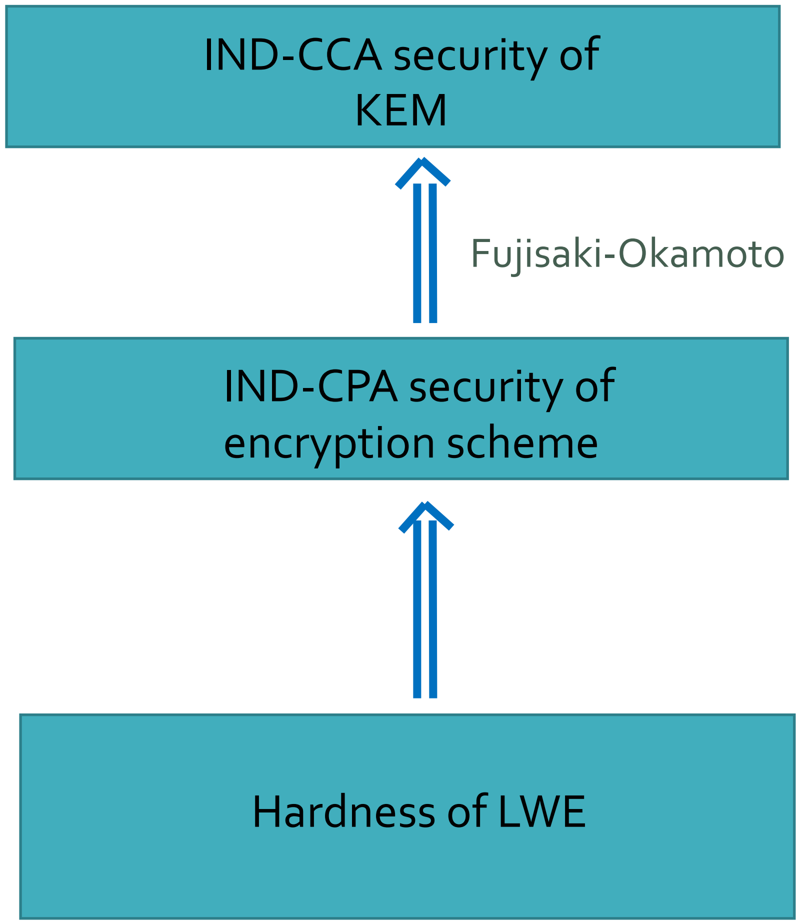
Suppose that Bob has a message μ.
He encodes it into the **most significant bits** of the entries of a matrix M.
He generates two new LWE samples (one from A, one from B) and adds M to the 2^{nd} one.

A, B, S

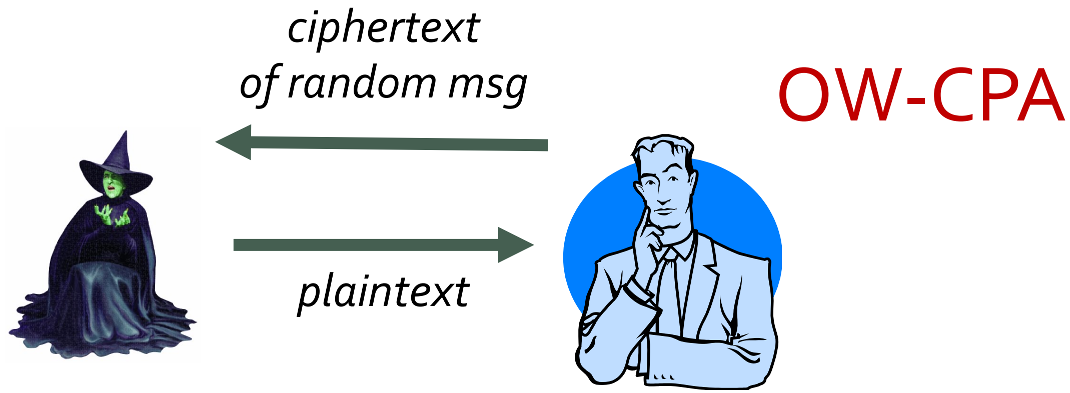
S'A + E'
S'B + E'' + M

A and B (:= AS + E),

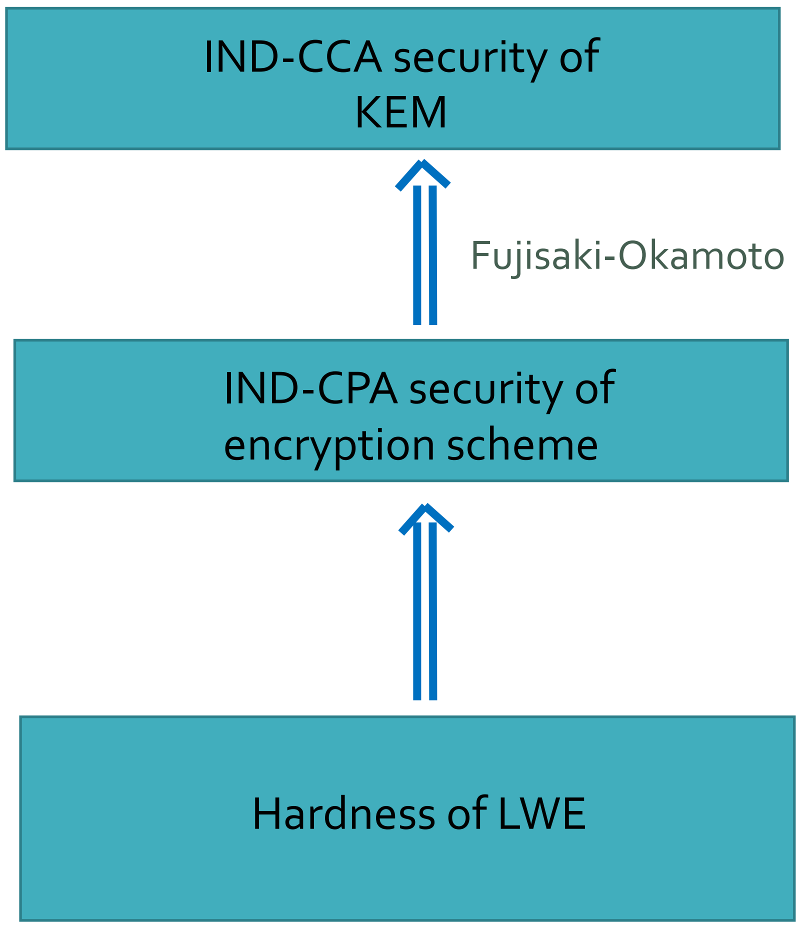
Classical Security Analysis



Round 2:
The authors claimed that since their encryption scheme is OW-CPA, its Fujisaki-Okamoto transform is IND-CCA.



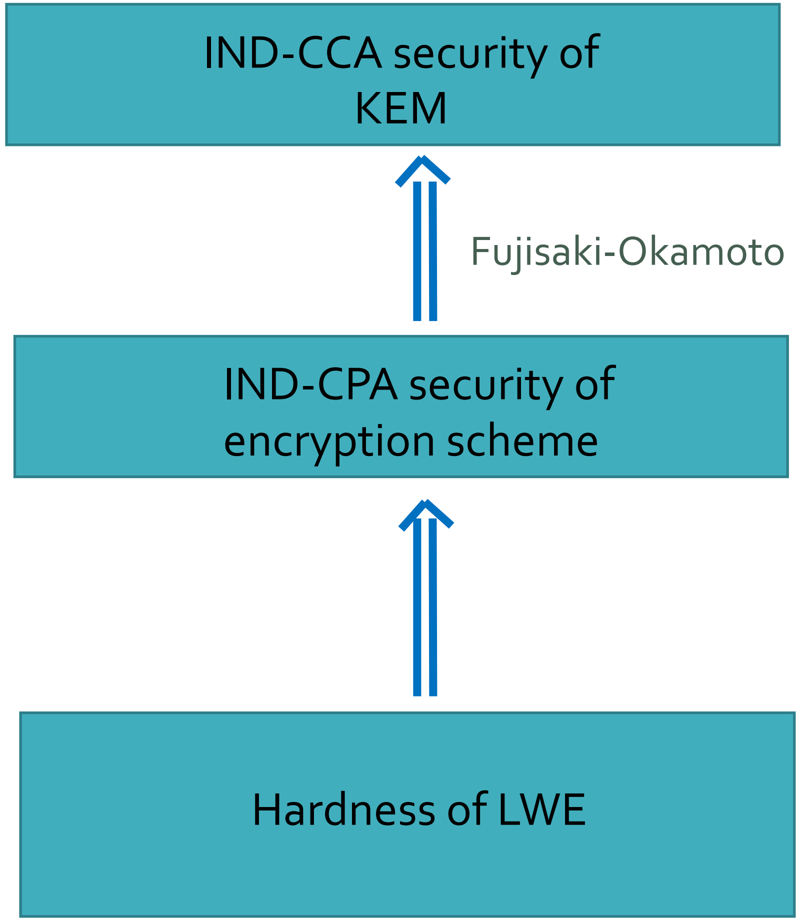
Classical Security Analysis



Round 2:
The authors claimed that since their encryption scheme is OW-CPA, its Fujisaki-Okamoto transform is IND-CCA.

D. Bernstein said he couldn't find that fact in the cited paper.

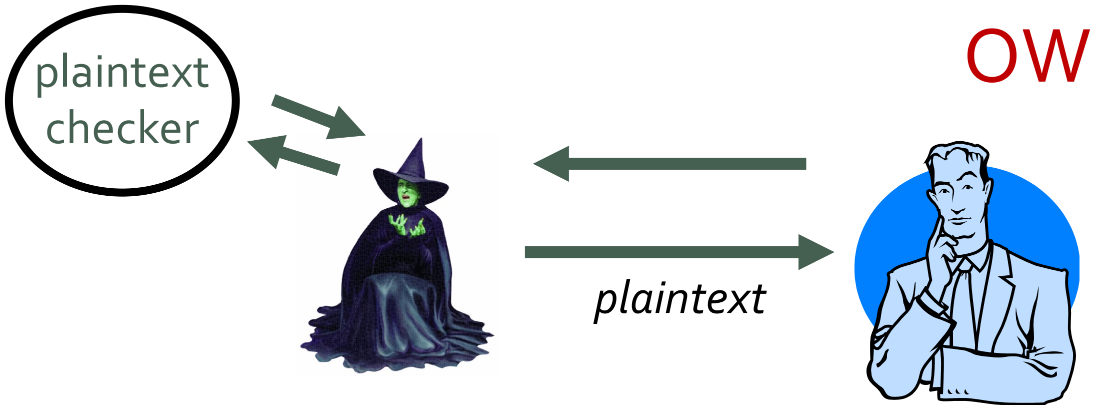
Classical Security Analysis



Round 3:
The authors give a new and more detailed analysis:

IND-CPA encryption
$\Longrightarrow$ OW-PCA deterministic encryption
$\Longrightarrow$ IND-CCA key encapsulation

OW-PCA



Other Changes in Round 3

- Guo et al. (2020) claimed a general timing attack on all Fujisaki-Okamoto schemes.
  The authors added comments to point out that their IND-CCA decapsulation steps must be done in constant time.

- The authors added a section, "Beyond Core-SVP Hardness," about how recent research affects claimed security strength. (They did not change their parameter sets.)

- Lots of minor changes are also listed.