Supersingular Isogeny Key Encapsulation

Presented by David Jao

University of Waterloo and evolutionQ, Inc.

Full list of submitters:

Reza Azarderakhsh, FAU
Matt Campagna, Amazon
Craig Costello, MSR
Luca De Feo, UVSQ
Basil Hess, ISG
Amir Jalali, LinkedIn
David Jao, UW
Brian Koziel, TI
Brian LaMacchia, MSR
Patrick Longa, MSR
Michael Naehrig, MSR
Geovandro Pereira, UW
Joost Renes, Radboud
Vladimir Soukharev, ISG
David Urbanik, UofT

`https://sike.org`

August 23, 2019

SIKE

Supersingular **I**sogeny **K**ey **E**ncapsulation (SIKE)

- IND-CCA2 KEM
- Based on **S**upersingular **I**sogeny **D**iffie-**H**ellman (SIDH)
- Uses Hofheinz et al. transformation (TCC 2017) on SIDH to achieve CCA security

The SIKE protocol specifies:

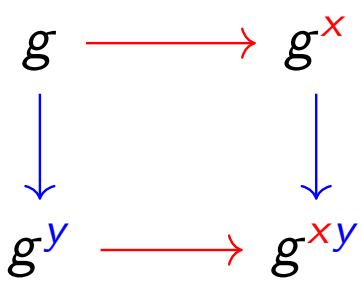
- Parameter sets
- Key/ciphertext formats
- Encapsulation/decapsulation mechanisms
- Choice of symmetric primitives (hash functions, etc.)

Overview of SIDH

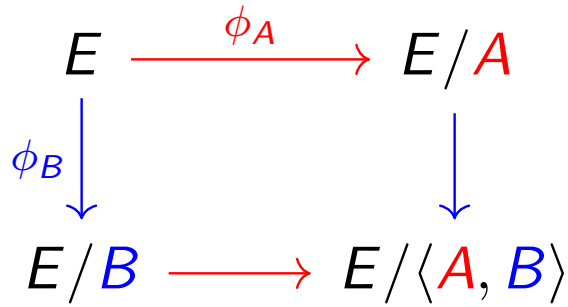
1. Public parameters: Supersingular elliptic curve E over $\mathbb{F}_{p^2}$.
2. Alice chooses a kernel $A \subset E(\mathbb{F}_{p^2})$ and sends E/A to Bob.
3. Bob chooses a kernel $B \subset E(\mathbb{F}_{p^2})$ and sends E/B to Alice.
4. The shared secret is

$$E/\langle A, B\rangle = (E/A)/\phi_A(B) = (E/B)/\phi_B(A).$$

Diffie-Hellman (DH)



SIDH



Changes for SIKE in second round

- New parameter sets: SIKEp434, SIKEp503, SIKEp610, SIKEp751, ~~SIKEp964~~
- New starting curve $E : y^2 = x^3 + 6x^2 + x$
- Key compression: $\approx 40\%$ smaller public keys and ciphertexts
- Updated security analysis

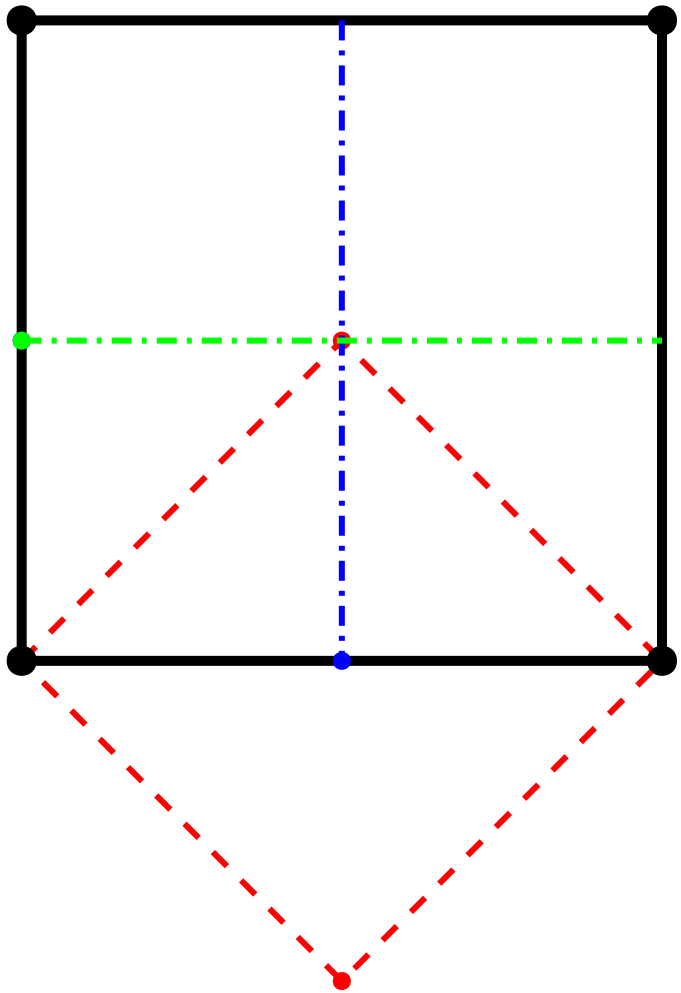
Parameter sets

Scheme	prime p	$\log_2 p$	Security level
SIKEp434	$2^{216}3^{137} - 1$	433.14	NIST 1
SIKEp503	$2^{250}3^{159} - 1$	502.01	NIST 2
SIKEp610	$2^{305}3^{192} - 1$	609.31	NIST 3
SIKEp751	$2^{372}3^{239} - 1$	750.81	NIST 5

New starting curve

The previous starting curve $y^2 = x^3 + x$ has complex multiplication symmetries, reducing key entropy.

- Red kernel point yields curve isomorphic to starting curve.
- Blue and green kernel points yield curves isomorphic to each other.



Key compression

Scheme	Public key	Decaps (x86_64)
SIKEp434	330 bytes	11.3 $\times 10^6$ cc
SIKEp434_compressed	196 bytes	18.9 $\times 10^6$ cc
SIKEp503	378 bytes	15.6 $\times 10^6$ cc
SIKEp503_compressed	224 bytes	25.5 $\times 10^6$ cc
SIKEp610	462 bytes	28.6 $\times 10^6$ cc
SIKEp610_compressed	273 bytes	45.5 $\times 10^6$ cc
SIKEp751	564 bytes	45.4 $\times 10^6$ cc
SIKEp751_compressed	331 bytes	72.8 $\times 10^6$ cc

Security analysis

Attack cost	SIKEp434			SIKEp610		
	G	D	W	G	D	W
Grover [1]	126	116	10	171	160	10
Tani (optimal $\#G$) [2]	124	114	25	169	159	25
Tani (optimal $D \times W$) [2]	131	122	10	177	166	10
Van Oorschot-Wiener [2]	132	14	128	177	14	173

1. *A framework for reducing the overhead of the quantum oracle for use with Grover's algorithm with applications to cryptanalysis of SIKE*, Benjamin I. Pring and Jean-François Biasse, MathCrypt 2019
2. *Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE*, Sam Jaques and John Schanck, CRYPTO 2019

Recent implementations

Decapsulation times, cc $\times 10^6$	SIKEp503	SIKEp751
ARM64 (NIST 2nd round)	47.4	159.5
ARM64 [1]	39.7	138.4
Cortex M4 [2]	183	491

1. *ARMv8 SIKE: Optimized Supersingular Isogeny Key Encapsulation on ARMv8 Processors*, Amir Jalali, Reza Azarderakhsh, Mehran Mozaffari Kermani, Matthew Campagna, and David Jao, IEEE TCAS, `10.1109/TCSI.2019.2920869`. Code available at `https://github.com/amirjalali65/armv8-sike`
2. *SIKE Round 2 Speed Record on ARM Cortex-M4*, Hwajeong Seo, Amir Jalali, and Reza Azarderakhsh, 2019/535.

Summary

SIKE advantages:

- Smallest public key size
- Straightforward parameter selection
- No decryption error, Gaussians, rejection sampling, etc.
- Generic attacks are well understood
- Only KEM proposal not based on lattices / codes / LW[ER]

SIKE disadvantages:

- Slow
- Future analysis may uncover non-generic attacks against SIKE (though none are known so far)

Future work:

- Cryptanalysis and side-channel attacks