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, FAU
- David Jao, UW
- Brian Koziel, TI
- Brian LaMacchia, MSR
- Patrick Longa, MSR
- Michael Naehrig, MSR
- Joost Renes, Radboud
- Vladimir Soukharev, ISG
- David Urbanik, UW

http://sike.org

April 11, 2018
Supersingular Isogeny Key Encapsulation (SIKE)

- IND-CCA2 KEM
- Based on Supersingular Isogeny Diffie-Hellman (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.)
A brief history of SIDH

  ▶ First explicit mention of isogenies in cryptography
  ▶ Unpublished until 2006

Galbraith, *Constructing isogenies between elliptic curves over finite fields* (1999)
  ▶ First published cryptanalysis of isogeny problem

  ▶ First (only?) patent on isogeny-based cryptography
  ▶ Does not apply to SIDH
  ▶ SIDH/SIKE is, to our knowledge, patent-free

Charles et al., *Cryptographic hash functions from expander graphs* (2009)
  ▶ First use of supersingular isogenies in cryptography
A brief history of SIDH

Stolbunov, *Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves* (2010)
- First published isogeny-based public-key cryptosystem
- Essentially identical to Couveignes’ unpublished 1996 work
- Partially broken by Childs, Jao, and Soukharev (2014)

Jao and De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies* (2011)
- Invention of SIDH
- First supersingular isogeny-based public-key cryptosystem

- Active attack against SIDH with static key re-use
- Necessitates use of Hofheinz et al. transform for CCA security
Overview of SIDH

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

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

\[
\begin{array}{c}
E \xrightarrow{\phi_A} E/A \\
\phi_B \downarrow \quad \downarrow \\
E/B \quad \quad \rightarrow \quad \quad \quad E/\langle A, B \rangle
\end{array}
\]
Detailed description of SIDH

Public parameters:
- Prime \( p = 2^{e_2}3^{e_3} - 1 \)
- Supersingular elliptic curve \( E/F_p^2 \) of order \((p + 1)^2\)
- \( \mathbb{Z} \)-basis \( \{P_2, Q_2\} \) of \( E[2^{e_2}] \) and \( \{P_3, Q_3\} \) of \( E[3^{e_3}] \)

Alice:
- Choose \( sk_2 \in \mathbb{Z} \) and compute \( S_2 = P_2 + sk_2 Q_2 \) of order \( 2^{e_2} \)
- Compute \( \phi_2 : E \rightarrow E/\langle S_2 \rangle \)
- Send \( E/\langle S_2 \rangle, \phi_2(P_3), \phi_2(Q_3) \) to Bob

Bob:
- Same as Alice, swapping 2 with 3

The shared secret is derived from

\[
E/\langle S_2, S_3 \rangle = (E/\langle S_2 \rangle)/\langle \phi_2(P_3) + sk_3 \phi_2(Q_3) \rangle = (E/\langle S_3 \rangle)/\langle \phi_3(P_2) + sk_2 \phi_3(Q_2) \rangle
\]
SIKE parameter sets

SIKEp503:
▶ \( p = 2^{250}3^{159} - 1 \) (note, the value of this prime is listed incorrectly in the spec)
▶ \( P_2 = 3^{159} \cdot E(i + 4), \ Q_2 = 3^{159} \cdot E(14) \)
▶ \( P_3 = 2^{250} \cdot E(i + 7), \ Q_3 = 2^{250} \cdot E(6) \)

SIKEp751:
▶ \( p = 2^{372}3^{239} - 1 \)
▶ \( P_2 = 3^{239} \cdot E(i + 5), \ Q_2 = 3^{239} \cdot E(11) \)
▶ \( P_3 = 2^{372} \cdot E(i + 2), \ Q_3 = 2^{372} \cdot E(6) \)

SIKEp964:
▶ \( p = 2^{486}3^{301} - 1 \)
▶ \( P_2 = 3^{301} \cdot E(i + 23), \ Q_2 = 3^{301} \cdot E(11) \)
▶ \( P_3 = 2^{486} \cdot E(i + 1), \ Q_3 = 2^{486} \cdot E(5) \)

N.b.: \( i = \sqrt{-1} \in \mathbb{F}_{p^2}, \ E: y^2 = x^3 + x \) and \( E(x) = (x, \sqrt{x^3 + x}) \).
Attack complexity

Hardness problem: Given $E$ and $E/A$ with a guarantee of the existence of $\phi: E \to E/A$, find $A$.

Fastest known (passive) attack is a generic collision search or claw search on a space of size $\deg(\phi)$:
In principle, a non-generic attack against SIKE could conceivably exist; however, none is currently known. For generic attacks:

<table>
<thead>
<tr>
<th>Parameter Set</th>
<th>Security</th>
<th>NIST Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIKEp503</td>
<td>SHA256</td>
<td>2</td>
</tr>
<tr>
<td>SIKEp751</td>
<td>SHA384</td>
<td>4</td>
</tr>
<tr>
<td>SIKEp964</td>
<td>AES256/SHA512</td>
<td>5</td>
</tr>
</tbody>
</table>

Recent developments pertaining to SIDH/SIKE security:

- Petit (Asiacrypt 2017): non-generic attacks against “unbalanced” versions of SIDH (not used in SIKE)
- Petit and Lauter, ePrint 2017/962: reductions from the isogeny problem to finding supersingular endomorphism rings
- Urbanik and Jao, AsiaPKC 2018: random self-reducibility
- Adj et al., ePrint:2018/313: proposes smaller parameters for 128-bit security, based on more detailed analysis of attacks
Implementation

(credit: pqbench by Markku-Juhani O. Saarinen)

Key sizes:
- SIKEp503 — 378 bytes
- SIKEp751 — 564 bytes
- SIKEp964 — 726 bytes

- Performance with platform-specific Intel64 assembly optimizations (AVX2) is $\sim 9x$ faster
- Key compression (Zanon et al., PQCrypto 2018):
  - $\sim 40\%$ smaller keys
  - $\sim 2x$ slower performance
  - Not included in SIKE specification, for the sake of simplicity
Summary

SIKE advantages:
- Very small key sizes
- No possibility for decryption error
- No complicated error distributions, rejection sampling, etc.
- Simple, conservative security analysis when assuming only generic attacks

SIKE disadvantages:
- Relatively slow
- Future analysis may uncover non-generic attacks against SIKE (though none are known so far)