Post-Quantum Signal Key Agreement from SIDH

Samuel Dobson Steven D. Galbraith

The University of Auckland

September 28, 2022

Attacks on SIDH

Since submission of this paper, new attacks on SIDH have been announced, using the SIDH public key torsion points to recover the secret in polynomial time:

1. Castryck and Decru [CD22]
2. Maino and Martindale [MM22]
3. Robert [Rob22]

Attacks on SIDH

Since submission of this paper, new attacks on SIDH have been announced, using the SIDH public key torsion points to recover the secret in polynomial time:

1. Castryck and Decru [CD22]
2. Maino and Martindale [MM22]
3. Robert [Rob22]

Countermeasures have already been proposed, and our protocol can be adapted to use them:

1. Masking the torsion point images [Fou22]
2. Masking the degree of the isogenies [Mor22]

Attacks on SIDH

Since submission of this paper, new attacks on SIDH have been announced, using the SIDH public key torsion points to recover the secret in polynomial time:

1. Castryck and Decru [CD22]
2. Maino and Martindale [MM22]
3. Robert [Rob22]

Countermeasures have already been proposed, and our protocol can be adapted to use them:

1. Masking the torsion point images [Fou22]
2. Masking the degree of the isogenies [Mor22]

The paper also includes results about the Signal security model that we hope will be of independent interest.

Overview

1. Overview of Signal X3DH
2. Construction of SI-X3DH
3. Sketch of security proof and reduction techniques
4. Conclusions

Signal X3DH

Signal has two main components:

1. Initial key agreement (X3DH)
2. Double Ratchet protocol.

Signal X3DH

Signal has two main components:

1. Initial key agreement (X3DH)
2. Double Ratchet protocol.

Extended Triple Diffie–Hellman (X3DH) protocol uses two keys from the sender, and two or three keys from the recipient, to derive a shared secret.

The Double Ratchet is used after initial shared secret establishment to regularly update the shared key, for forward and backward secrecy.

Security properties

Important properties of the Signal initial key agreement:

1. Correctness.
2. Secrecy (a.k.a. key-indistinguishability).
3. (Implicit) authentication.
4. Perfect forward secrecy (PFS).
5. Asynchronicity (a.k.a. receiver obliviousness).
6. (Offline) deniability.

Making Signal Post-Quantum

There are known ways to make the double ratchet post-quantum secure with KEMs.The initial key agreement is more complicated.

[BFG+20] is a theoretical work, with no known-secure instantiations.

Two concrete KEM-based schemes:

1. SPQR [BFG+22], requires expensive post-quantum ring signatures for deniability.
2. SC-AKE [HKKP21], requires expensive post-quantum ring signatures for deniability; only uses long term and ephemeral keys (no semi-static keys), introducing the possibility of ephemeral key exhaustion Denial-of-Service.

Making Signal Post-Quantum

SIDH resembles Diffie–Hellman, but is vulnerable to adaptive attacks (at least, in its original form), e.g. GPST attack [GPST16].

SI-X3DH is designed around ensuring that adaptive attacks are prevented.

Making Signal Post-Quantum

SIDH resembles Diffie–Hellman, but is vulnerable to adaptive attacks (at least, in its original form), e.g. GPST attack [GPST16].

SI-X3DH is designed around ensuring that adaptive attacks are prevented.

The GPST attack involves crafting malicious torsion points and learning bits of the secret based on whether the exchange succeeds or fails. It can be defeated by checks that the protocol message is correctly formed:

1. Ephemeral keys can be revealed after-the-fact (Fujisaki–Okamoto transform).
2. Correctness of long-term keys can be proven (e.g. with [DDGZ21]).

Signal X3DH $\rightarrow$ SI-X3DH

IK_B

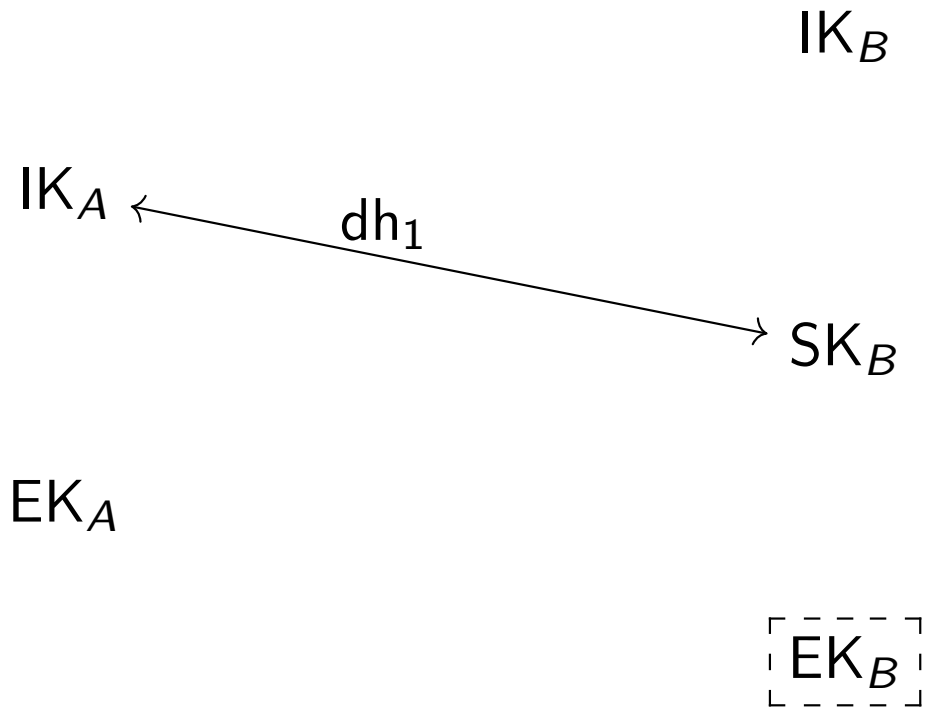
IK_A

SK_B

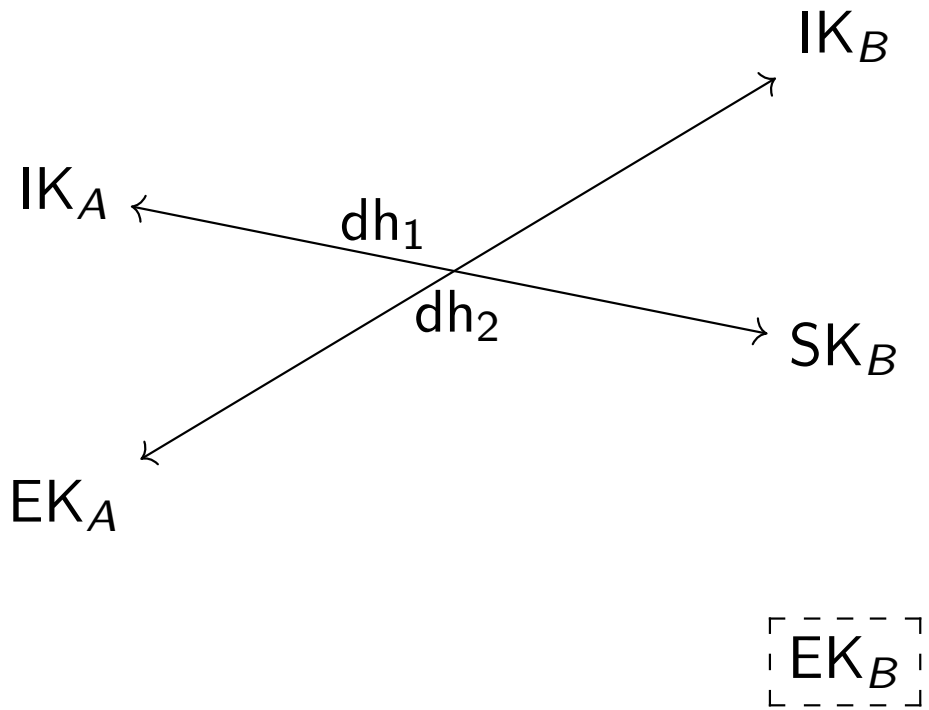
EK_A

EK_B

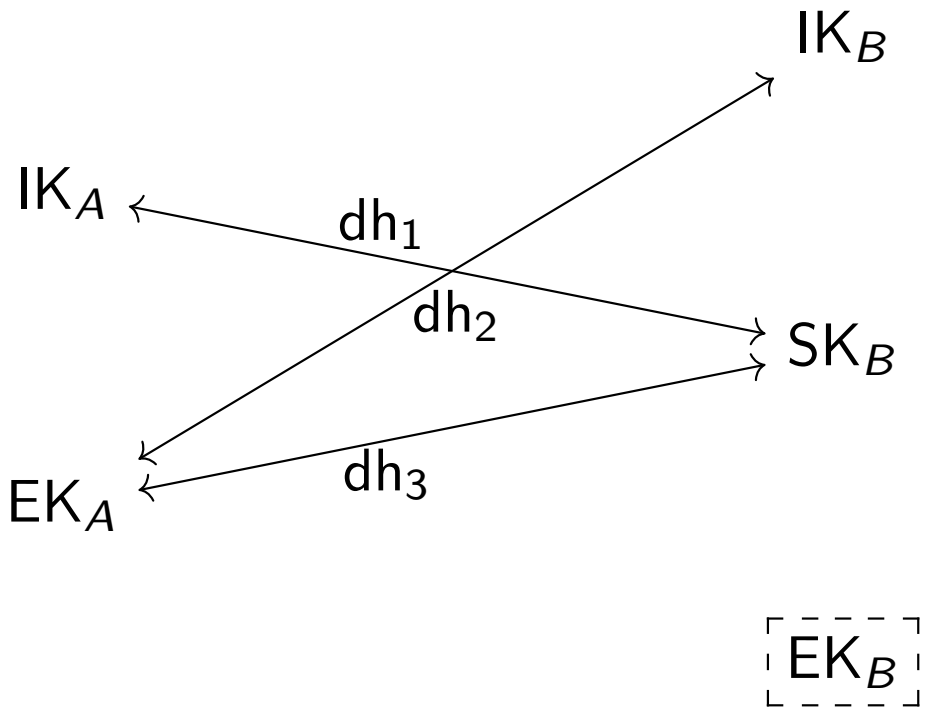
Signal X3DH $\rightarrow$ SI-X3DH



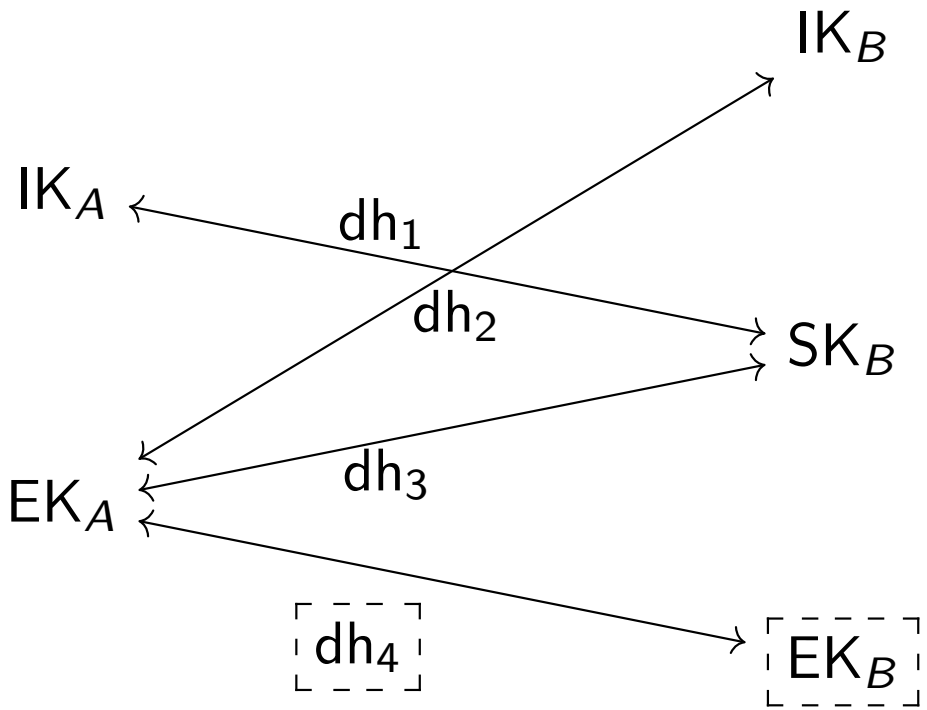
Signal X3DH $\rightarrow$ SI-X3DH



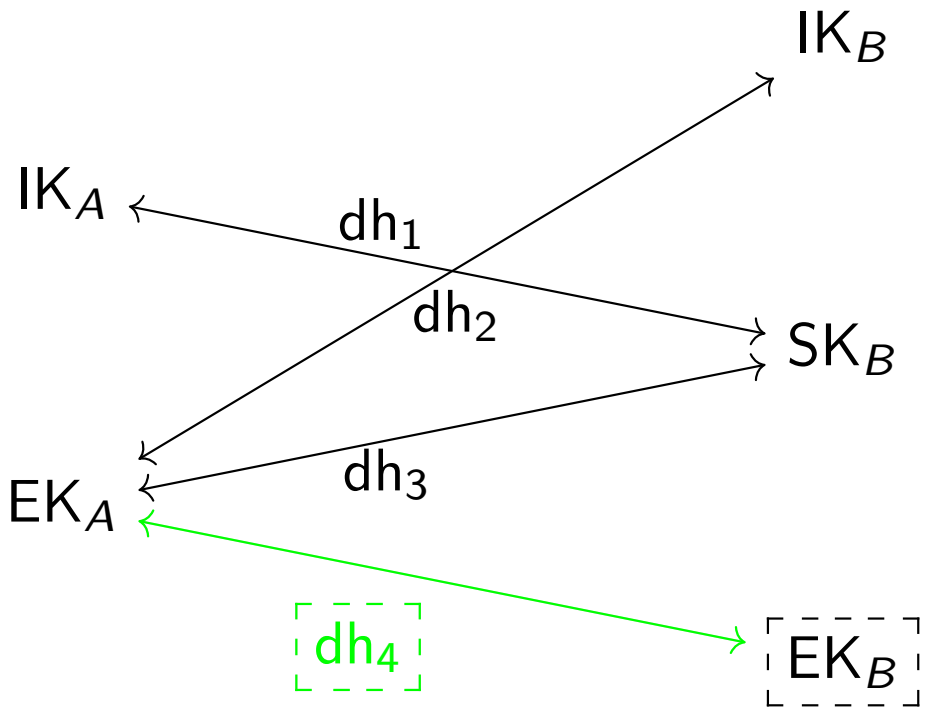
Signal X3DH $\rightarrow$ SI-X3DH



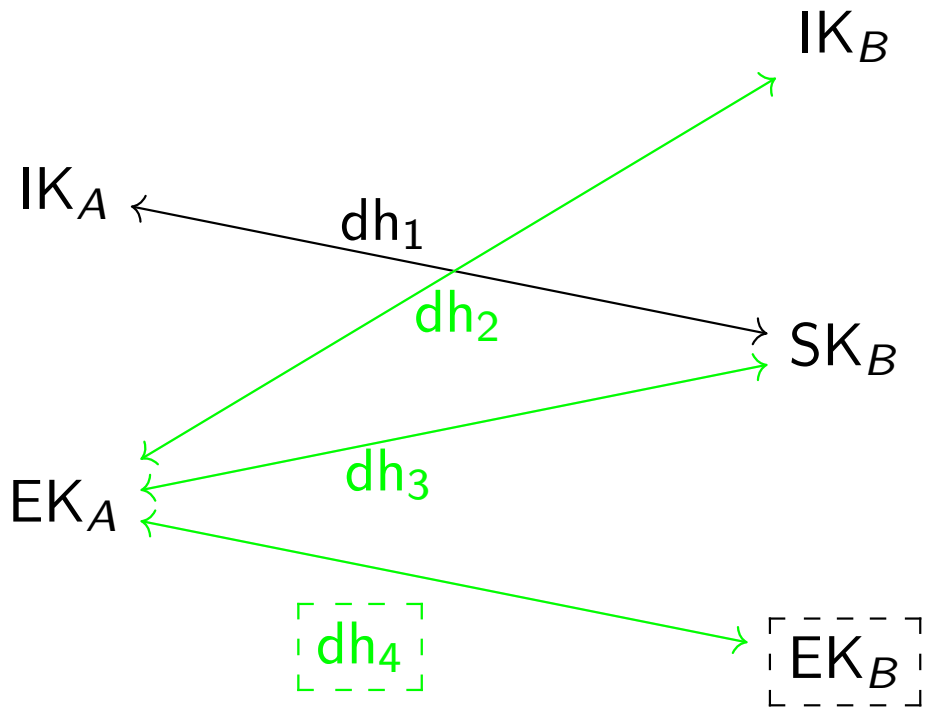
Signal X3DH $\rightarrow$ SI-X3DH



Signal X3DH $\rightarrow$ SI-X3DH



Signal X3DH → SI-X3DH

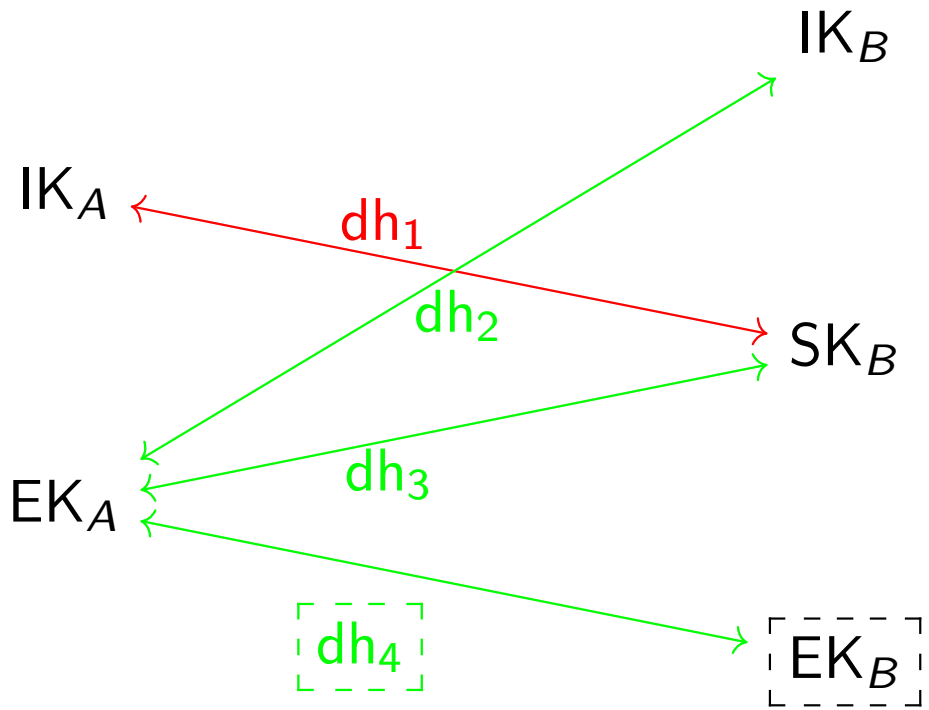


$$s \leftarrow \{0,1\}^n$$

$$EK_A = \text{PubkeyFromSecret}(H_1(s))$$

$$\pi = s \oplus H_2(dh_1) \oplus H_2(dh_2) \oplus H_2(dh_3) \oplus H_2(dh_4)$$

Signal X3DH → SI-X3DH

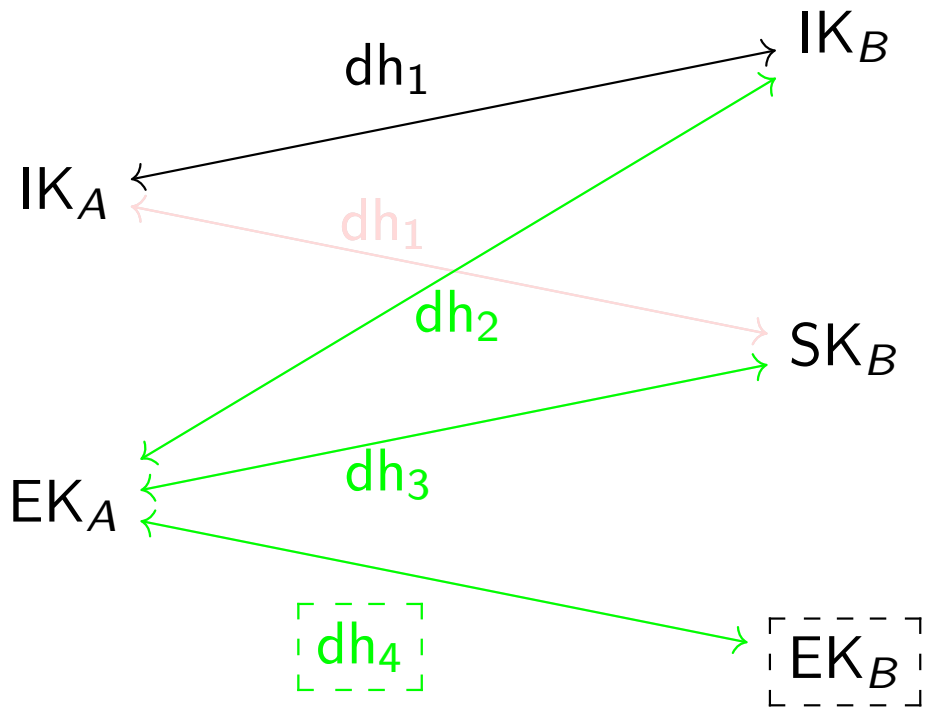


$$s \leftarrow \{0,1\}^n$$

$$\mathsf{EK}_A = \mathsf{PubkeyFromSecret}(H_1(s))$$

$$\pi = s \oplus H_2(\mathsf{dh}_1) \oplus H_2(\mathsf{dh}_2) \oplus H_2(\mathsf{dh}_3) \oplus H_2(\mathsf{dh}_4)$$

Signal X3DH → SI-X3DH



$$s \leftarrow \{0,1\}^n$$

$$\mathsf{EK}_A = \mathsf{PubkeyFromSecret}(H_1(s))$$

$$\pi = s \oplus H_2(\mathsf{dh}_1) \oplus H_2(\mathsf{dh}_2) \oplus H_2(\mathsf{dh}_3) \oplus H_2(\mathsf{dh}_4)$$

Security model

Satisfied:

Event	Matching session exists	$\mathrm{IK}_{\mathcal{I}}$	$\mathrm{EK}_{\mathcal{I}}$	$\mathrm{IK}_{\mathcal{R}}$	$\mathrm{SK}_{\mathcal{R}}$	$\mathrm{EK}_{\mathcal{R}}$	Attack
E_1	No	✓	x	x	✓	-	KCI
E_2	No	x	✓	x	x	-	MEX
E_3	No	x	-	x	x	✓	MEX
E_5	Yes	✓	x	✓	x	x	wPFS
E_6	Yes	x	✓	x	x	✓	MEX
E_7	Yes	✓	x	x	✓	✓	KCI

Unsatisfied:

Event	Matching session exists	$\mathrm{IK}_{\mathcal{I}}$	$\mathrm{EK}_{\mathcal{I}}$	$\mathrm{IK}_{\mathcal{R}}$	$\mathrm{SK}_{\mathcal{R}}$	$\mathrm{EK}_{\mathcal{R}}$	Attack
E_4	No	x	-	✓	✓	x	KCI
E_8	Yes	x	✓	✓	✓	x	KCI

Security model (previous work)

Previous work [HKKP21] uses a strong CK-type model that includes all these cases (without semi-static keys). Signal X3DH does not satisfy this model.

[BFG+22] uses a custom key-indistinguishability model following the one by [CGCD+20]. This makes it difficult to compare with models using more standard CK-type notation—e.g. w.r.t PFS, KCI, and MEX properties.

Reduction techniques

Security proof of Signal X3DH given in [CGCD$^+$20] relies on Gap-DH assumption.

There is no Gap-DH equivalent in the isogeny setting—(perfectly) deciding whether an isogeny of a certain degree exists allows computation of the isogeny by testing elliptic curve neighbors.

We introduce new problems that reduce from the computational problem. A similar technique may be useful in other proofs (e.g. Signal X3DH with a FO transform can be proven secure from computational DH in the ROM).

Reduction techniques

Definition (Verifiable SI-CDH (VCDH) problem)

Let pp be SIDH public parameters, and K_1 and K_2 be two SIDH public keys (whose secret isogenies have coprime degrees specified by pp). Let $\mathcal{O}_{K_1,K_2}$ be an oracle defined as

$$\mathcal{O}_{K_1,K_2}(j') = \begin{cases} 1 & \text{if } j' = \mathrm{SIDH}_{\mathrm{pp}}(K_2, K_1), \\ 0 & \text{otherwise.} \end{cases}$$

Note that K_1, K_2 are *fixed* in the definition of $\mathcal{O}$.
The Verifiable SI-CDH problem is to compute the j-invariant $j = \mathrm{SIDH}_{\mathrm{pp}}(K_2, K_1)$, given pp, K_1, K_2, and $\mathcal{O}_{K_1,K_2}$.

Reduction techniques

Definition (Honest SI-CDH (HCDH) problem)

Let pp be SIDH public parameters, and $s \leftarrow \{0,1\}^\kappa$ be a random seed, where κ is the security parameter. Then, let $K_2 = \text{PubkeyFromSecret}(H_1(s))$ be a public key derived from s, where $H_1(s)$ is an isogeny of degree $\ell_2^{e_2}$. Let K_1 be a second public key (corresponding to an isogeny of degree $\ell_1^{e_1}$). Finally, let π be an FO-proof of the form

$$\pi = s \oplus H_2(\text{SIDH}_{\text{pp}}(K_2, K_1)),$$

where $H_2 : \{0,1\}^* \to \{0,1\}^\kappa$ is a PRG.
The Verifiable SI-CDH problem is, given pp, K_1, K_2, and π, to compute the j-invariant $j = \text{SIDH}_{\text{pp}}(K_2, K_1)$.

Closing remarks

The biggest drawback of this scheme comes from the inefficiency of the SIDH PoK required for the long-term keys. More efficient Proofs of Knowledge for (secure variants of) SIDH is an interesting direction of work.

The "online" exchange is compact—SIDH's short key sizes and a small FO proof.

We hope that the phrasing of Signal's security in the context of standard eCK/CK+ type models is useful for comparison with other protocols.

We also hope that a secure variant of SIDH exists, please go and cryptanalyse the new masked-degree and masked-point proposals!

Thanks for your attention!


Jacqueline Brendel, Marc Fischlin, Felix Günther, Christian Janson, and Douglas Stebila.
Towards post-quantum security for Signal's X3DH handshake.
In *SAC 2020*, volume 12804 of *Lecture Notes in Computer Science*, pages 404–430, 2020.


Jacqueline Brendel, Rune Fiedler, Felix Günther, Christian Janson, and Douglas Stebila.
Post-quantum asynchronous deniable key exchange and the Signal handshake.
In *PKC 2022*, volume 13178 of *Lecture Notes in Computer Science*, pages 3–34. Springer, 2022.


Wouter Castryck and Thomas Decru.
An efficient key recovery attack on SIDH (preliminary version).
Cryptology ePrint Archive, Paper 2022/975, 2022.
https://ia.cr/2022/975.


Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila.

A formal security analysis of the Signal messaging protocol.
Journal of Cryptology, 33(4):1914–1983, 2020.


Luca De Feo, Samuel Dobson, Steven D. Galbraith, and Lukas Zobernig.
SIDH proof of knowledge.
Cryptology ePrint Archive, Paper 2021/1023, 2021.
https://ia.cr/2021/1023.


Tako Boris Fouotsa.
Sidh with masked torsion point images.
Cryptology ePrint Archive, Paper 2022/1054, 2022.
https://eprint.iacr.org/2022/1054.


Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti.
On the security of supersingular isogeny cryptosystems.
In *ASIACRYPT 2016*, pages 63–91. Springer, 2016.


Keitaro Hashimoto, Shuichi Katsumata, Kris Kwiatkowski, and Thomas Prest.

An efficient and generic construction for Signal's handshake (X3DH): Post-quantum, state leakage secure, and deniable.
In *PKC 2021*, pages 410–440. Springer, 2021.


Luciano Maino and Chloe Martindale.
An attack on SIDH with arbitrary starting curve.
Cryptology ePrint Archive, Paper 2022/1026, 2022.
https://ia.cr/2022/1026.


Tomoki Moriya.
Masked-degree sidh.
Cryptology ePrint Archive, Paper 2022/1019, 2022.
https://eprint.iacr.org/2022/1019.


Damien Robert.
Breaking SIDH in polynomial time.
Cryptology ePrint Archive, Paper 2022/1038, 2022.
https://ia.cr/2022/1038.