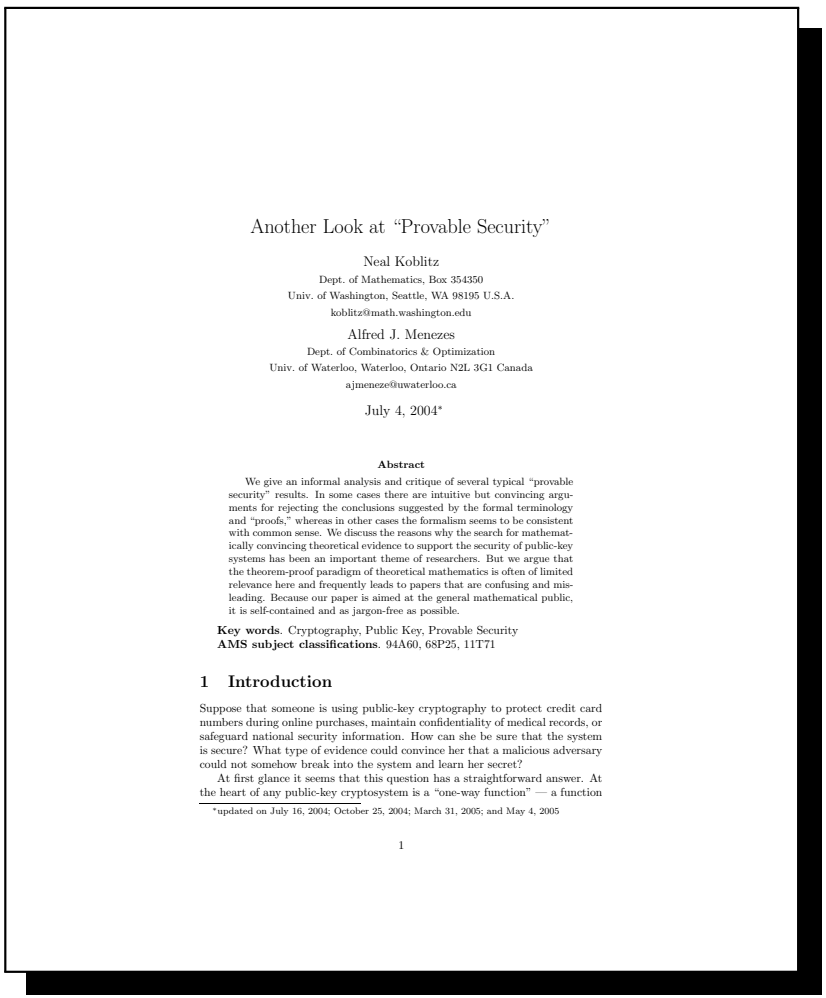
Another Look At Some Isogeny Hardness Assumptions

Simon-Phillipp Merz, Romy Minko, Christophe Petit

ECC 2019

3 December

Motivation



Another Look at "Provable Security"

Neal Koblitz
Dept. of Mathematics, Box 354350
Univ. of Washington, Seattle, WA 98195 U.S.A.
koblitz@math.washington.edu
Alfred J. Menezes
Dept. of Combinatorics & Optimization
Univ. of Waterloo, Waterloo, Ontario N2L 3G1 Canada
ajmeneze@uwaterloo.ca

July 4, 2004*

Abstract

We give an informal analysis and critique of several typical "provable security" results. In some cases there are intuitive but convincing arguments for rejecting the conclusions suggested by the formal terminology and "proofs," whereas in other cases the formalism seems to be consistent with common sense. We discuss the reasons why the search for mathematically convincing theoretical evidence to support the security of public-key systems has been an important theme of researchers. But we argue that the theorem-proof paradigm of theoretical mathematics is often of limited relevance here and frequently leads to papers that are confusing and misleading. Because our paper is aimed at the general mathematical public, it is self-contained and as jargon-free as possible.

Key words. Cryptography, Public Key, Provable Security
AMS subject classifications. 94A60, 68P25, 11T71

1 Introduction

Suppose that someone is using public-key cryptography to protect credit card numbers during online purchases, maintain confidentiality of medical records, or safeguard national security information. How can she be sure that the system is secure? What type of evidence could convince her that a malicious adversary could not somehow break into the system and learn her secret?

At first glance it seems that this question has a straightforward answer. At the heart of any public-key cryptosystem is a "one-way function" — a function

*updated on July 16, 2004; October 25, 2004; March 31, 2005; and May 4, 2005

1

- Isogeny based cryptography is becoming more popular.
- More protocols are developed, and sometimes their security does not reduce to existing problems.
- New 'hard' problems are therefore proposed.

Outline

- (Very Brief) Introduction
- Reviewing Some Isogeny Problems
- Undeniable Signature Schemes
  - Jao-Soukharev (2014)
  - Srinath-Chandrasekaran (2018)
- Attack on the Computational Hardness Assumption
- Attack on the Signature Scheme

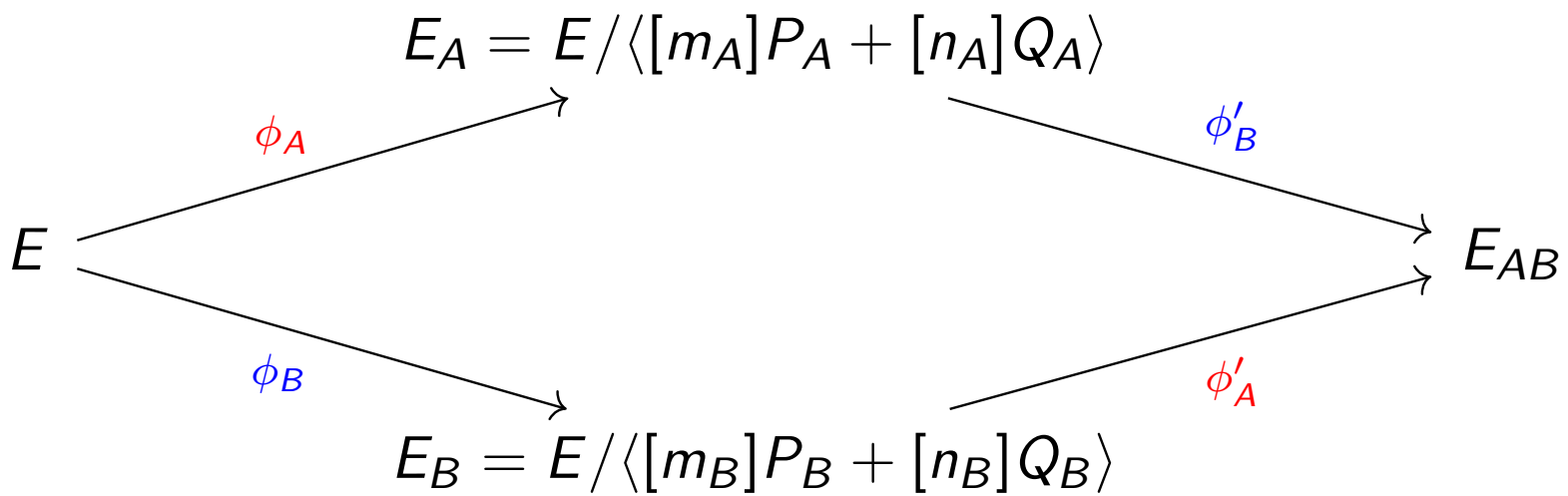
SIDH Protocol
Parameters

- ℓ_A, ℓ_B small distinct primes
- e_A, e_B positive integers
- $p = \ell_A^{e_A} \ell_B^{e_B} f \pm 1$, p prime

Fix a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and bases $\{P_A, Q_A\}, \{P_B, Q_B\}$ of the $\ell_A^{e_A}$ and $\ell_B^{e_B}$ torsions of E, respectively. Alice chooses $0 < m_A, n_A < \ell_A^{e_A}$. Bob chooses $0 < m_B, n_B < \ell_B^{e_B}$.

SIDH Protocol

Alice publishes $E_A, \phi_A(P_B), \phi_A(Q_B)$.
Bob publishes $E_B, \phi_B(P_A), \phi_B(Q_A)$.



Outline

- (Very Brief) Introduction
- Reviewing Some Isogeny Problems
- Undeniable Signature Schemes
  - Jao-Soukharev (2014)
  - Srinath-Chandrasekaran (2018)
- Attack on the Computational Hardness Assumption
- Attack on the Signature Scheme

Problem (SSCDH)

Given the curves E, E_A, E_B and the points $\phi_A(P_B)$, $\phi_A(Q_B)$, $\phi_B(P_A)$ and $\phi_B(Q_A)$, find the j-invariant of

$$E_{AB} = E/\langle [m_A]P_A + [n_A]Q_A,\ [m_B]P_B + [n_B]Q_B \rangle.$$

Problem (Modified SSCDH)

Given E, E_A, E_B *and* $\ker(\phi_B)$, *determine* E_{AB} *up to isomorphism, i.e. find* $j(E_{AB})$.

Signing Oracle

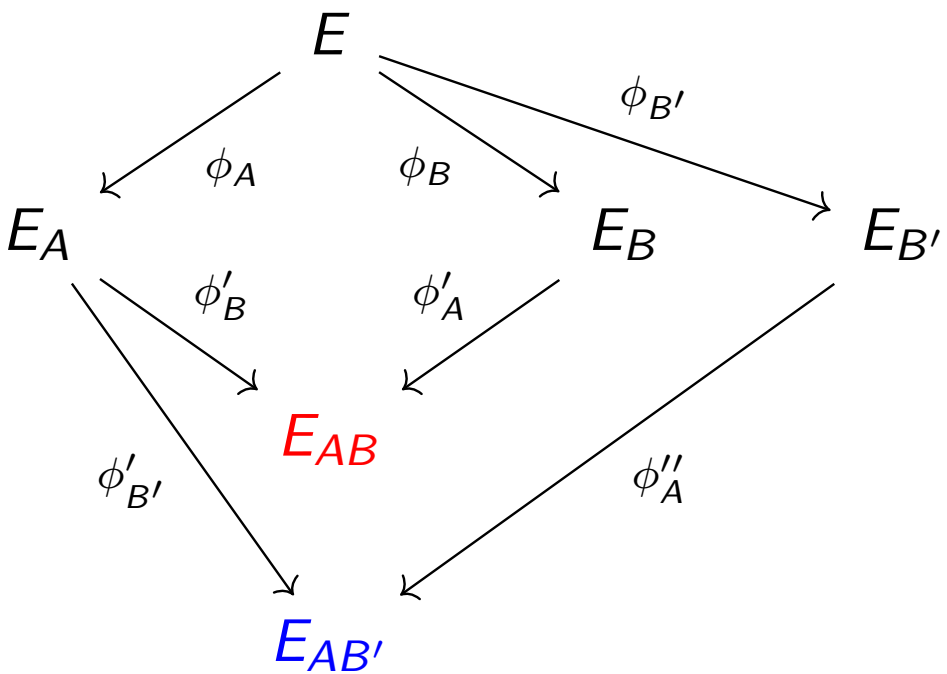
For fixed curves E, E_A, E_B, let $\mathcal{O}_B$ be an oracle that solves MSSCDH for E_A, $E_{B'}$, $\ker(\phi_{B'})$ such that $E_{B'}$ is

- not isomorphic to E_B, and
- $\ell_B^{e_B}$-isogenous to E.

Problem (One-Sided MSSCDH)

For fixed E, E_A, E_B, given $\mathcal{O}_B$, solve MSSCDH for E_A, E_B and $\ker(\phi_B)$.

One-Sided Modified SSCDH



Target Curve

Oracle Output

Signing Oracle

For fixed curves E, E_A let $\mathcal{O}_{\mathcal{A}}$ be an oracle that solves MSSCDH for E_A, E_{B_i}, $\ker(\phi_{B_i})$ upon input of E_{B_i}, $\ell_B^{e_B}$-isogenous to E.

Problem (One-More MSSCDH)

After making q queries to $\mathcal{O}_{\mathcal{A}}$ produce at least $q+1$ distinct pairs of curves (E_{B_i}, E_{AB_i}), where E_{AB_i} is the solution to MSSCDH for E_A, E_{B_i} and $\ker(\phi_{B_i})$, and E_{B_i} are $\ell_B^{e_B}$-isogenous to E for $1 \leq i \leq q+1$.

Outline

- (Very Brief) Introduction
- Reviewing Some Isogeny Problems
- Undeniable Signature Schemes
  - Jao-Soukharev (2014)
  - Srinath-Chandrasekaran (2018)
- Attack on the Computational Hardness Assumption
- Attack on the Signature Scheme

Undeniable Signature Schemes

- $\Sigma = \{\texttt{KeyGen}, \texttt{Sign}, \texttt{Check}, \texttt{Sim}, \pi_{con}, \pi_{dis}\}$.
  - $\texttt{KeyGen}$ generates (v_k, s_k), a verification and signing key-pair.
  - $\texttt{Sign}(s_k, m) = \sigma_m$.
  - $\texttt{Check}((v_k, m, \sigma), s_k)$ determines if σ is valid.
  - $\texttt{Sim}(v_k, m)$ simulates a signature for m.
  - π_{con}, π_{dis} are zero-knowledge interactive protocols.

Jao-Soukharev (2014)

- Let p be a prime of the form $\ell_A^{e_A}\ell_B^{e_B}\ell_C^{e_C} \cdot f \pm 1$.
- Fix a supersingular curve E over $\mathbb{F}_{p^2}$,
- Fix bases $\{P_i, Q_i\}$ of the $\ell_i^{e_i}$ torsion of E for $i \in \{A, B, C\}$.
- Let $H : \{0,1\}^* \to \mathbb{Z}$ be a cryptographic hash function.

Jao-Soukharev (2014)

- **Public Parameters:** $p, E, H, \{P_i, Q_i\}_{i \in \{A,B,C\}}$.
- **Signer's Secret Key:** $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$
  (or $\phi_A : E \to E_A = E/\langle [m_A]P_A + [n_A]Q_A \rangle$).
- **Public Key:** $E_A, \phi_A(P_C), \phi_A(Q_C)$

For message M:

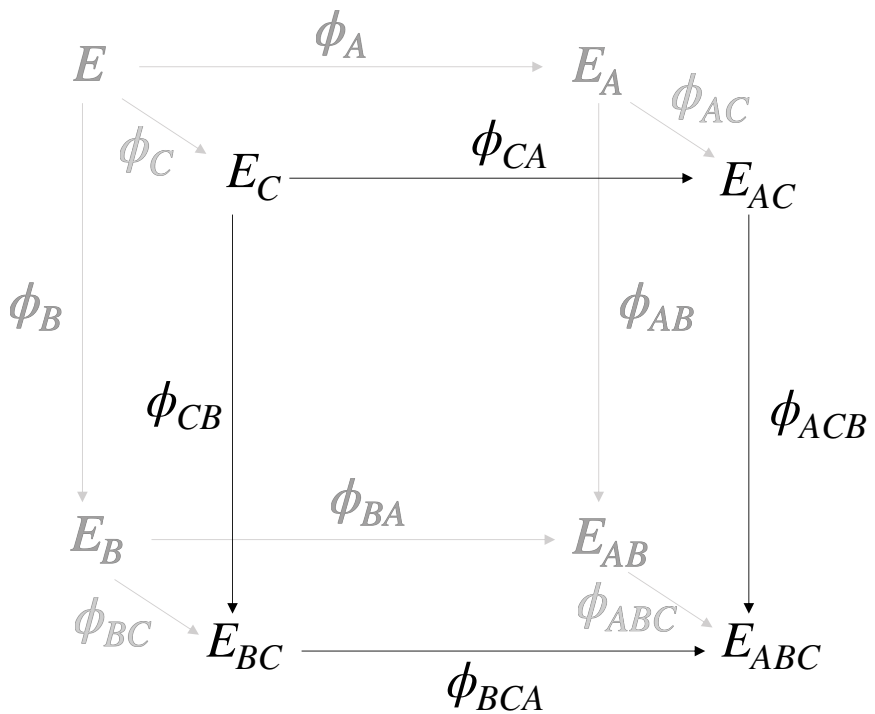
- Compute $E_B = E/\langle P_B + [H(M)]Q_B \rangle$.

$$\begin{array}{ccc} E & \xrightarrow{\phi_A} & E_A \\ \downarrow{\scriptstyle \phi_B} & & \downarrow{\scriptstyle \phi_{AB}} \\ E_B & \xrightarrow{\phi_{BA}} & E_{AB} \end{array}$$

- Output $\sigma = (E_{AB}, \phi_{BA}(\phi_B(P_C)), \phi_{BA}(\phi_B(Q_C)))$.

Jao-Soukharev (2014)
Confirmation/Disavowal

- The signer secretly chooses $m_C, n_C \in \mathbb{Z}/\ell_C\mathbb{Z}$ and computes $S_C = [m_C]P_C + [n_C]Q_C$.



$$E_C = E/\langle S_C \rangle, E_{BC} = E_B/\langle \phi_B(S_C) \rangle$$
$$E_{AC} = E_A/\langle \phi_A(S_C) \rangle, E_{ABC} = E_{BC}/\langle \phi_{CB}([m_A]P_A + [n_A]Q_A) \rangle$$

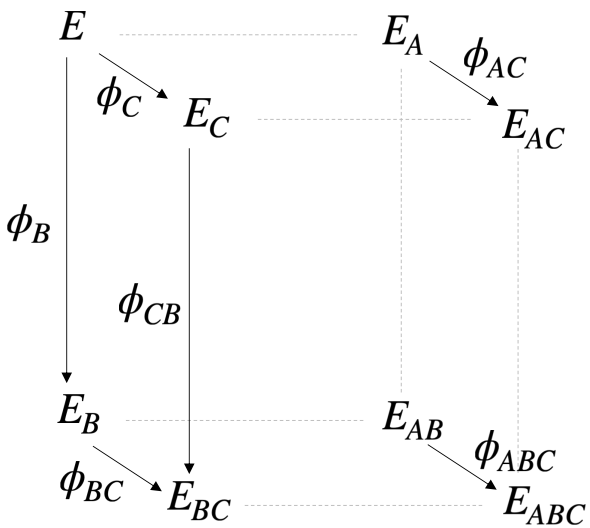
Jao-Soukharev (2014)
Confirmation/Disavowal

- Given $\sigma = \{E_\sigma, P_\sigma, Q_\sigma\}$, $E_{\sigma C} = E_\sigma / \langle [m_c]P_\sigma + [n_C]Q_\sigma \rangle$

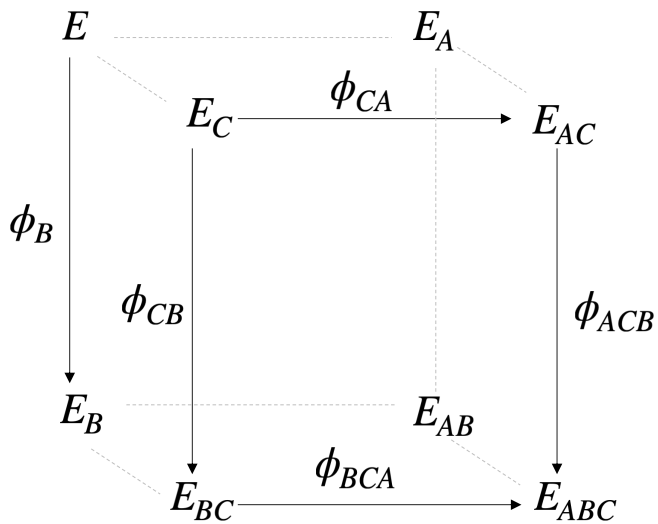
Signer		**Verifier**
Commit: $com = E_C, E_{BC}, E_{AC}, E_{ABC}, \ker(\phi_{CB})$		
	$\xrightarrow{com}$	
		$b \leftarrow\$ \{0,1\}$
	$\xleftarrow{b}$	
if $b = 0, X = \ker(\phi_C)$.		
if $b = 1, X = \ker(\phi_{CA})$.		
	$\xrightarrow{X}$	
		Check $E_{\sigma C} = E_{ABC}$.

Jao-Soukharev (2014)
Confirmation/Disavowal

- Given $\sigma = \{E_\sigma, P_\sigma, Q_\sigma\}$, $E_{\sigma C} = E_\sigma / \langle [m_c]P_\sigma + [n_C]Q_\sigma \rangle$



$b = 0$



$b = 1$

Srinath-Chandrasekaran (2018)
Undeniable Blind Signatures

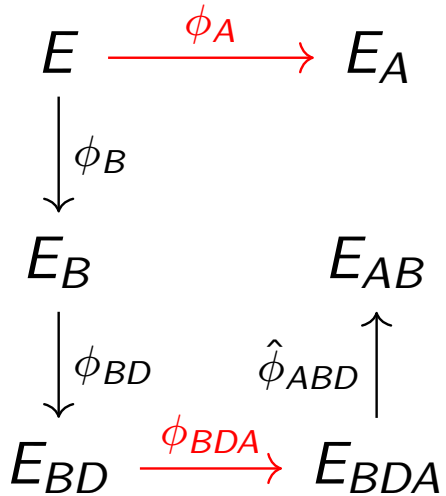


Figure: Signing (with blindness)

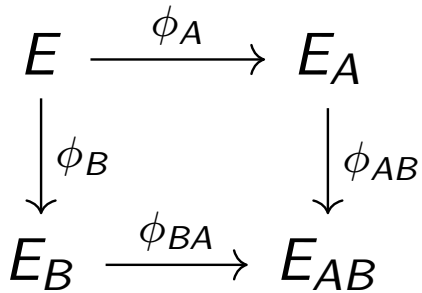


Figure: Verification requires that the signature curve is in the isomorphism class of E_{AB}.

Undeniable Signature Schemes

- Security Properties:
  - Undeniability
  - Unforgeability
  - Invisibility

Unforgeability

- The attacker has access to a signing oracle $\mathcal{O}$.
- They can query the oracle polynomially many times with arbitrarily chosen messages m_i.
- They must output valid (m, σ), where $m \neq m_i$.

Invisibility

- The attacker has access to a signing oracle $\mathcal{O}$.
- They can query the oracle polynomially many times with arbitrarily chosen messages m_i.
- They then send $m_j \neq m_i$ to a challenger.
- The challenger returns σ_c, either a simulated signature or a valid signature for m_j.
- The attacker must decide if σ_c is valid.

Proof of Unforgeability and Invisibility [1]

Given zero-knowledge confirmation and disavowal protocols, forging signatures is equivalent to OMSSCDH.

Invisibility requires that after a polynomial number of queries to the signing oracle, an adversary cannot determine the validity of a signature. This problem is equivalent to OMSSCDH.

[1] David Jao and Vladimir Soukharev. *Isogeny-based quantum-resistant undeniablesignatures.* InInternational Workshop on Post-Quantum Cryptography, pages 160–179. Springer, 2014.

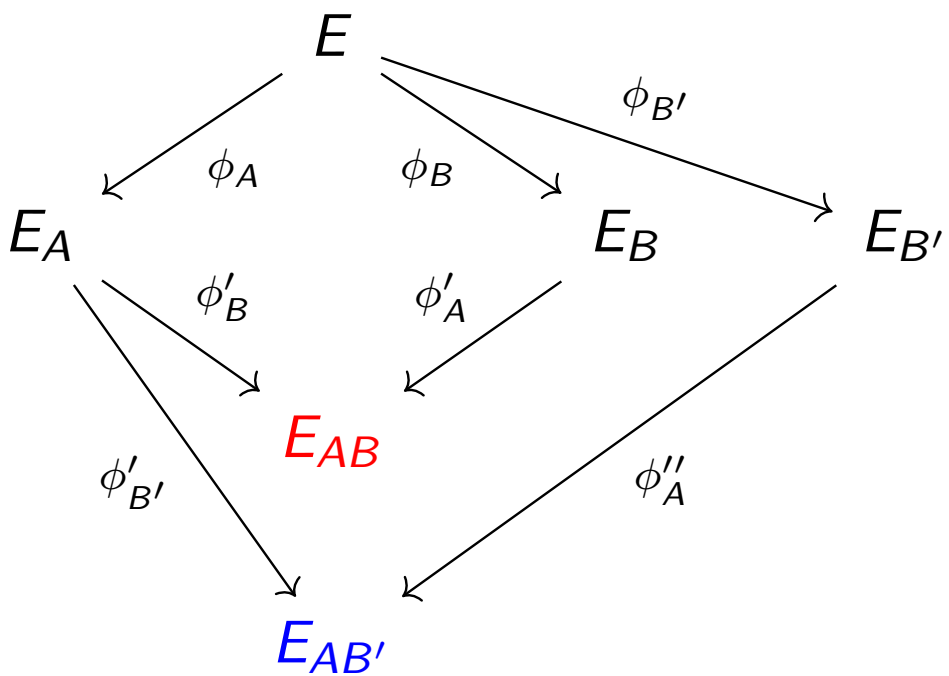
Outline

- (Very Brief) Introduction
- Reviewing Some Isogeny Problems
- Undeniable Signature Schemes
  - Jao-Soukharev (2014)
  - Srinath-Chandrasekaran (2018)
- Attack on the Computational Hardness Assumption
- Attack on the Signature Scheme

An attack against OMSSCDH

Problem (OMSSCDH)

For fixed E, E_A, E_B, given an oracle, $\mathcal{O}$, to solve MSSCDH for E_A, $E_{B'}$, $\ker(\phi_{B'})$ with $E_{B'}$ not isomorphic to E_B and $\ell_B^{e_B}$-isogenous to E, solve MSSCDH for E_A, E_B and $\ker(\phi_B)$.



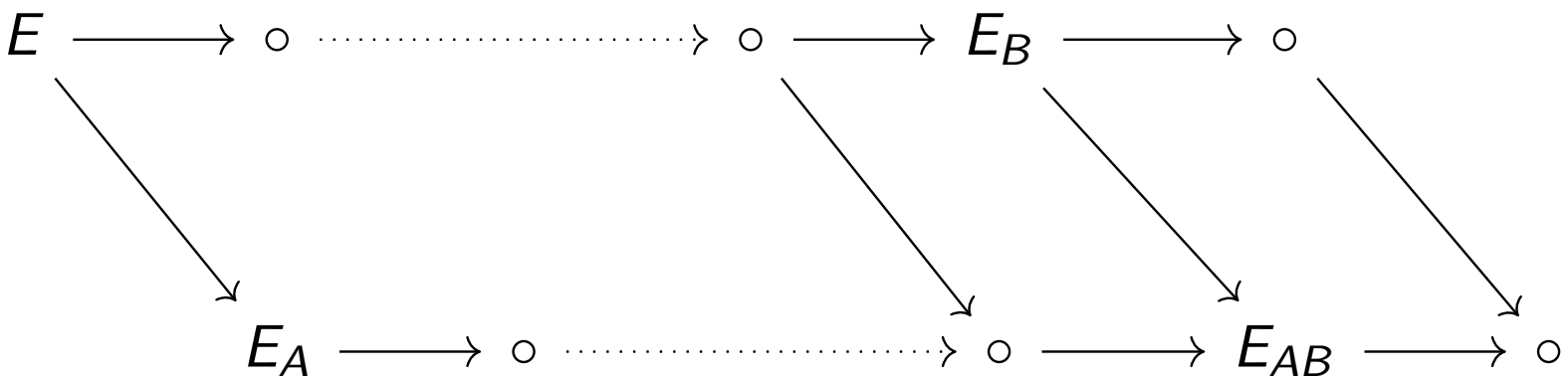
An attack against OMSSCDH

Theorem

A solution to the OMSSCDH problem can be guessed with probability $\frac{1}{(\ell_B+1)\ell_B}$ *after a single query to the signing oracle.*

An attack against OMSSCDH

Suppose we want to solve OMSSCDH given E, E_A, E_B and $\ker(\phi_B)$.



An attack against OMSSCDH

Suppose we want to solve OMSSCDH given E, E_A, E_B and $\ker(\phi_B)$.

- Take E_{B_1}, E_{B_2}, ℓ_B-isogenous to E_B.

An attack against OMSSCDH

Suppose we want to solve OMSSCDH given E, E_A, E_B and $\ker(\phi_B)$.

- Take E_{B_1}, E_{B_2}, ℓ_B-isogenous to E_B.
- Query $\mathcal{O}$ with E_{B_1} and E_{B_2}, to get E_{AB_1} and E_{AB_2}.

An attack against OMSSCDH

Suppose we want to solve OMSSCDH given E, E_A, E_B and $\ker(\phi_B)$.

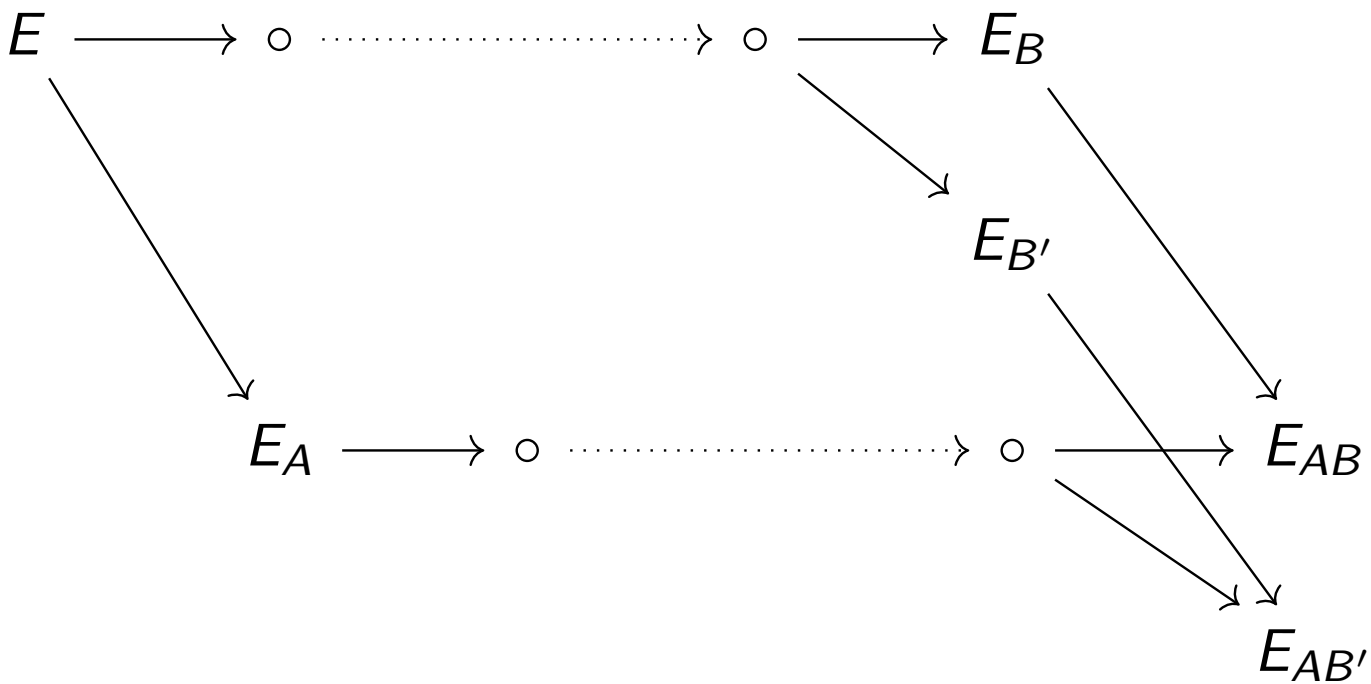
- Take E_{B_1}, E_{B_2}, ℓ_B-isogenous to E_B.
- Query $\mathcal{O}$ with E_{B_1} and E_{B_2}, to get E_{AB_1} and E_{AB_2}.
- List the $\ell_B + 1$ isomorphism classes of E_{AB_1} and E_{AB_2}, ℓ_B-isogenous to E_{AB}.

An attack against OMSSCDH

Suppose we want to solve OMSSCDH given E, E_A, E_B and $\ker(\phi_B)$.

- Take E_{B_1}, E_{B_2}, ℓ_B-isogenous to E_B.
- Query $\mathcal{O}$ with E_{B_1} and E_{B_2}, to get E_{AB_1} and E_{AB_2}.
- List the $\ell_B + 1$ isomorphism classes of E_{AB_1} and E_{AB_2}, ℓ_B-isogenous to E_{AB}.
- The intersection of these lists is the isomorphism class of E_{AB}.

An attack against OMSSCDH



Querying $\mathcal{O}$ with $E_{B'}$ close to E_B yields a curve close to E_{AB}, the target.

An attack against OMSSCDH

We can do better.

- Use $\ker(\phi_B)$ to find $E_{B'}$, ℓ_B^2-isogenous to E_B and $\ell_B^{e_B}$-isogenous to E.

An attack against OMSSCDH

We can do better.

- Use $\ker(\phi_B)$ to find $E_{B'}$, ℓ_B^2-isogenous to E_B and $\ell_B^{e_B}$-isogenous to E.
- Submit $E_{B'}$ to $\mathcal{O}$ to receive $E_{AB'}$.

An attack against OMSSCDH

We can do better.

- Use $\ker(\phi_B)$ to find $E_{B'}$, ℓ_B^2-isogenous to E_B and $\ell_B^{e_B}$-isogenous to E.
- Submit $E_{B'}$ to $\mathcal{O}$ to receive $E_{AB'}$.
- Guess the isomorphism class of E_{AB} with success probability of $\frac{1}{(\ell_B+1)\ell_B}$.

An attack against OMSSCDH

We can do better.

- Use $\ker(\phi_B)$ to find $E_{B'}$, ℓ_B^2-isogenous to E_B and $\ell_B^{e_B}$-isogenous to E.
- Submit $E_{B'}$ to $\mathcal{O}$ to receive $E_{AB'}$.
- Guess the isomorphism class of E_{AB} with success probability of $\frac{1}{(\ell_B+1)\ell_B}$.

This only uses one query to the oracle.

An attack against 1MSSCDH

Problem (One-More MSSCDH)

After making q queries to $\mathcal{O}$ produce at least $q+1$ distinct pairs of curves (E_{B_i}, E_{AB_i}), where E_{AB_i} is the solution to MSSCDH for E_A, E_{B_i} and $\ker(\phi_{B_i})$, E_{B_i} are $\ell_B^{e_B}$-isogenous to E and E_{AB_i} is isomorphic to E_{AB} for $1 \leq i \leq q+1$.

An attack against 1MSSCDH

Theorem

A solution to the 1MSSCDH problem can be guessed with probability $\frac{1}{(\ell_B+1)\ell_B}$ *after a single query to the signing oracle.*

Outline

- (Very Brief) Introduction
- Reviewing Some Isogeny Problems
- Undeniable Signature Schemes
  - Jao-Soukharev (2014)
  - Srinath-Chandrasekaran (2018)
- Attack on the Computational Hardness Assumption
- Attack on the Signature Scheme

Proof of Unforgeability and Invisibility [1]

Given zero-knowledge confirmation and disavowal protocols, forging signatures is equivalent to OMSSCDH.

Invisibility requires that after a polynomial number of queries to the signing oracle, an adversary cannot determine the validity of a signature. This problem is equivalent to OMSSCDH.

[1] David Jao and Vladimir Soukharev. *Isogeny-based quantum-resistant undeniablesignatures.* InInternational Workshop on Post-Quantum Cryptography, pages 160–179. Springer, 2014.

But...

- Messages curves are computed via the hash function H.
- The adversary can only query the oracle with messages.

But...

- Messages curves are computed via the hash function H.
- The adversary can only query the oracle with messages.
- Forging messages seems therefore harder than solving OMSSCDH.

Attack on the Signature Scheme

Let M be the message for which we wish to forge a signature.

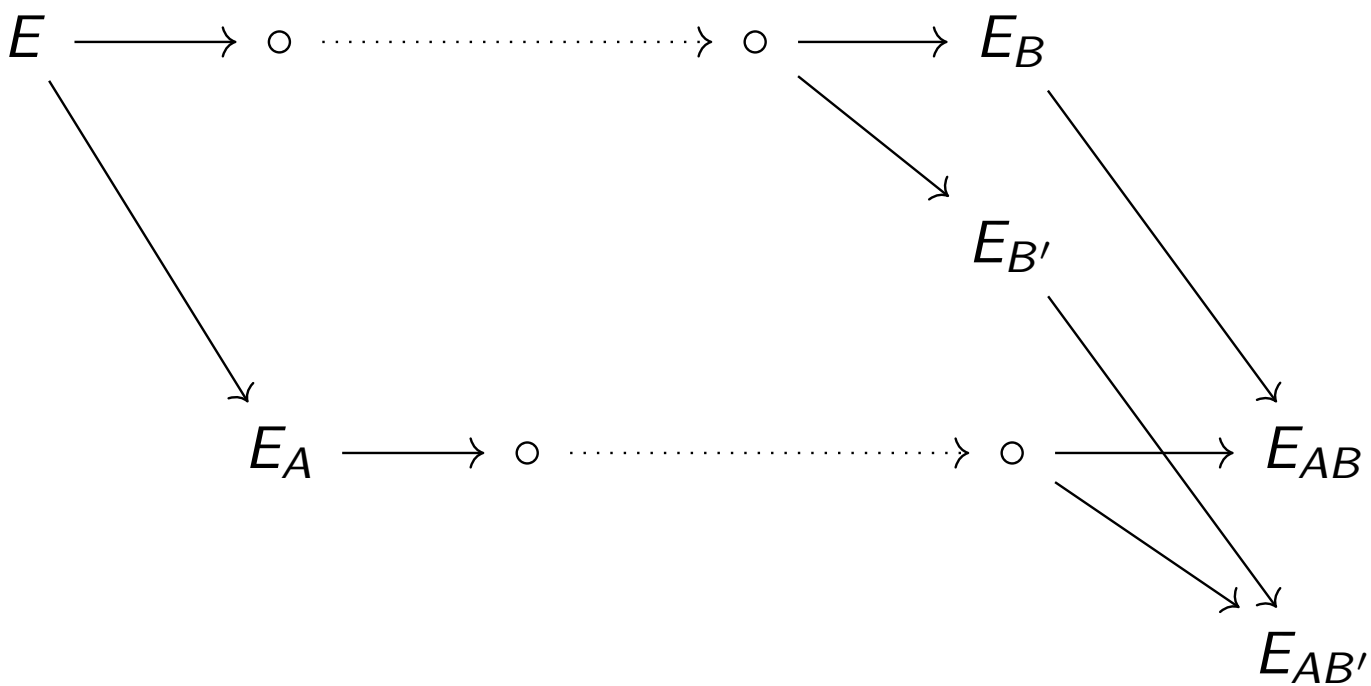
Attack on the Signature Scheme

Let M be the message for which we wish to forge a signature.

Lemma

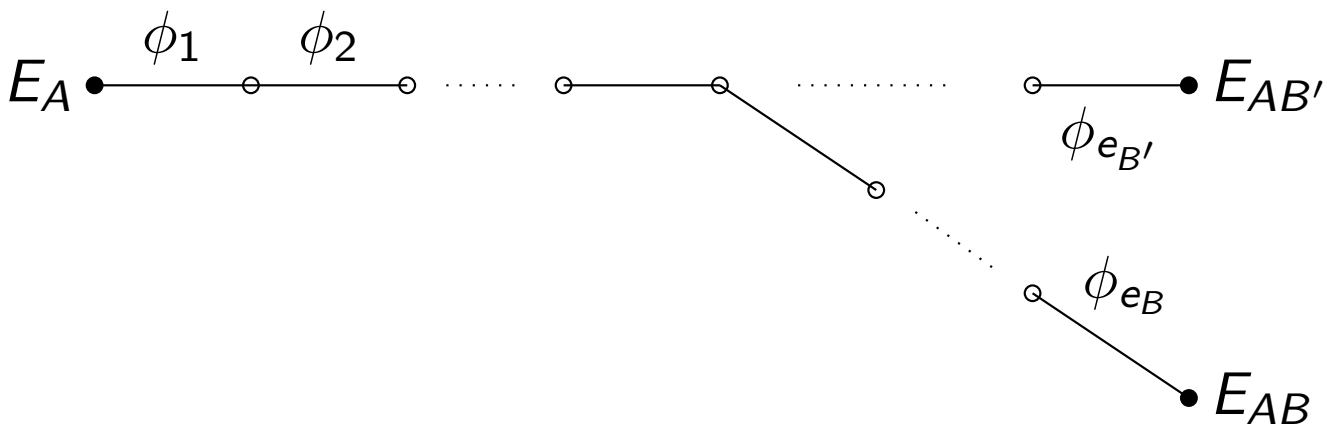
Let E be a supersingular elliptic curve, let ℓ be a prime, let e be an integer, and let $\{P, Q\}$ be a basis for $E[\ell^e]$. Let $\alpha, \beta < \ell^e$ be positive integers congruent modulo ℓ^k for some integer $k < e$. Then the ℓ-isogeny paths from E to $E_\alpha = E/\langle P + [\alpha]Q\rangle$ and $E_\beta = E/\langle P + [\beta]Q\rangle$ are equal up to the k-th step.

An attack against OMSSCDH

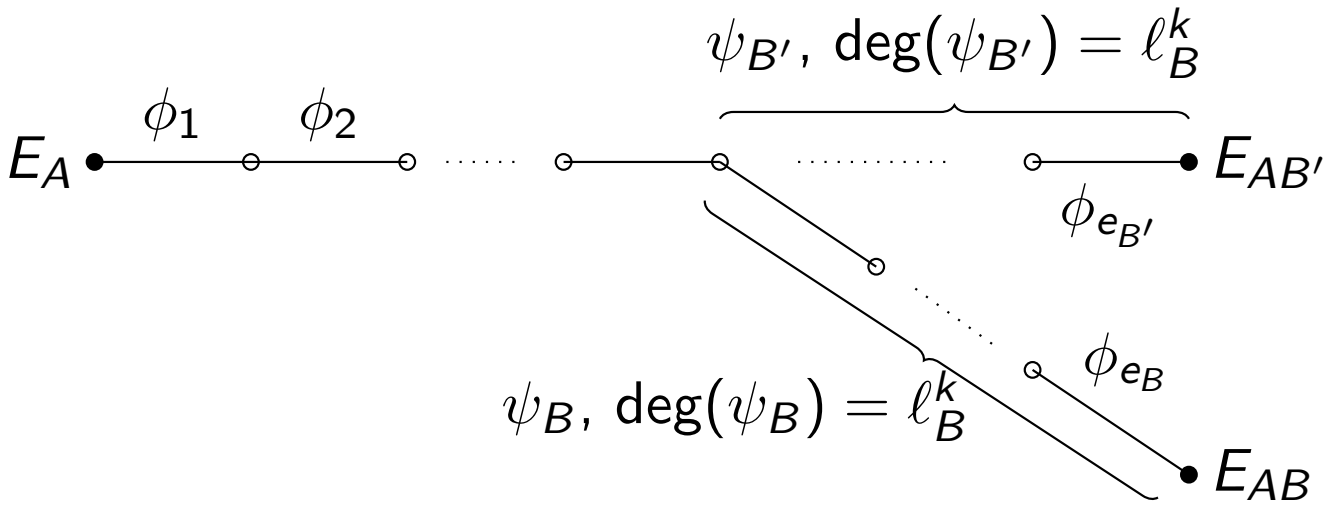


Aim: use the lemma to extend this idea to $E_{B'}$ further from E_B.

Attack on the Signature Scheme



Attack on the Signature Scheme
Finding ψ



- $\psi = \psi_B \circ \hat{\psi}_{B'}$.
- The probability of correctly identifying ψ with a single guess is $\frac{1}{(\ell_B+1)\ell_B^{2k-1}}$.

Attack on the Signature Scheme
Validity of σ

Assume: ψ (and hence, E_{AB}) has been guessed correctly.
Let honest $\sigma = (E_{AB}, P, Q)$, forgery $\sigma_F = (E_{AB}, P_F, Q_F)$.
Oracle: $\sigma' = (E_{AB'}, P' = \phi_{B'A}(\phi_{B'}(P_C)), Q' = \phi_{B'A}(\phi_{B'}(Q_C)))$.

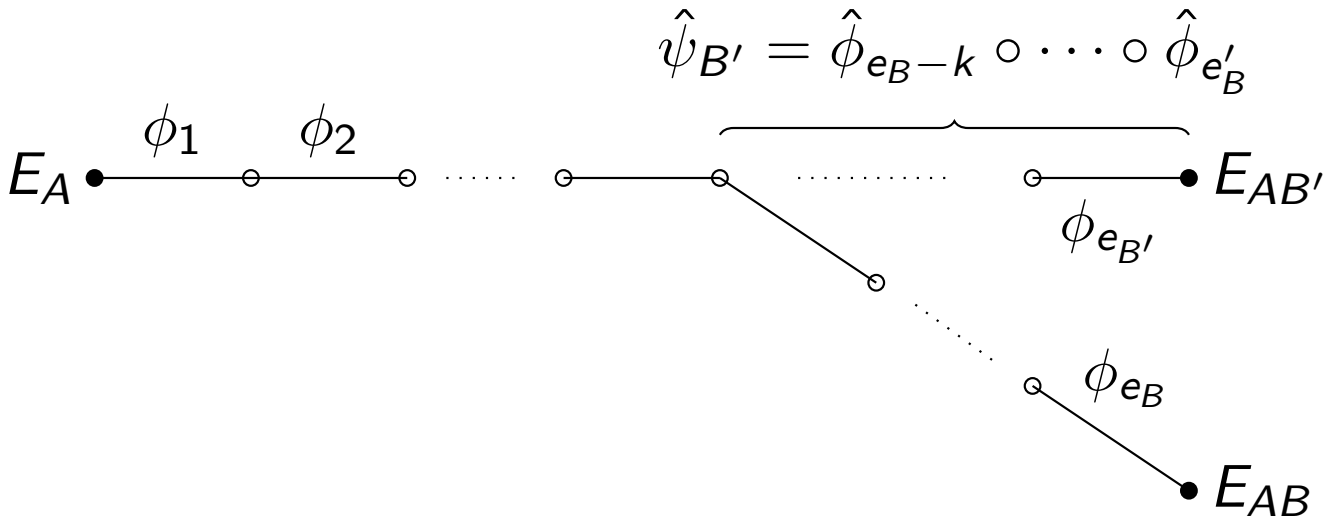
- For confirmation/disavowal:
  - $E_{\sigma C} = E/\langle [m_c]P_F + [n_c]Q_F \rangle$
  - $E_{ABC} = \langle [m_c]P + [n_c]Q \rangle$

Attack on the Signature Scheme
Validity of σ

Assume: ψ (and hence, E_{AB}) has been guessed correctly.
Let honest $\sigma = (E_{AB}, P, Q)$, forgery $\sigma_F = (E_{AB}, P_F, Q_F)$.
Oracle: $\sigma' = (E_{AB'}, P' = \phi_{B'A}(\phi_{B'}(P_C)), Q' = \phi_{B'A}(\phi_{B'}(Q_C)))$.

- ψ takes a point on $E_{AB'}$ to a point on E_{AB}.
- $\psi(P') = \psi(\phi_{B'A}(\phi_{B'}(P_C))) = \psi(\phi_{AB'}(\phi_A(P_C))) \in E_{AB}[\ell_C^{e_C}]$.

Attack on the Signature Scheme
Validity of σ



- $\phi_{AB'} : E_A \to E_{AB'}$.
- $\hat{\psi}_{B'} \circ \phi_{AB'} = [\ell_B^k]\phi_{e_B-k-1} \circ \cdots \circ \phi_1$.

Attack on the Signature Scheme

- Find M' such that $H(M)$ and $H(M')$ differ by a large power of ℓ_B.
- Submit M' to the signing oracle, to receive $\sigma' = (E_{AB'}, P', Q')$.
- Guess the ℓ_B^{2k}-isogeny $\psi : E_{AB'} \to E_{AB}$ where E_{AB} is the unknown curve corresponding to M.
- Find s such that $s\ell_B^k \equiv 1 \mod \ell_C^{e_C}$.
- Compute $\{[s] \cdot \psi(P'), [s] \cdot \psi(Q')\}$.
- Output $\sigma_F = (E_{AB}, [s] \cdot \psi(P'), [s] \cdot \psi(Q'))$.

Theorem (Validity of σ)

Let M, M', s, ψ, P' and Q' are defined as in the attack. Let $\sigma_F = (E_{AB}, [s] \cdot \psi(P'), [s] \cdot \psi(Q'))$ be the output of our attack. Assuming E_{AB} is guess correctly, σ_F is a valid signature for M.

Let λ be our security parameter.
Classical security: Take $2^L = 2^{2\lambda}$.
Quantum security: Take $2^L = 2^{3\lambda}$.

Previous Expected Cost: 2^λ.

Classical Cost

Near collision of L_1 bits:

$$2^{L_1/2}$$

Pr[E_{AB} guessed correctly]:

$$2^{-2(L-L_1)}$$

Take $L_1 = \frac{4L}{5}$. Then, total cost:

$$2^{2L/5}$$

Classical Cost

Near collision of L_1 bits:

$$2^{L_1/2}$$

Pr[E_{AB} guessed correctly]:

$$2^{-2(L-L_1)}$$

Take $L_1 = \frac{4L}{5}$. Then, total cost:

$$2^{2L/5}$$

Quantum Cost

Near collision of L_1 bits:

$$2^{L_1/3}$$

Pr[E_{AB} guessed correctly]:

$$2^{-2(L-L_1)}$$

Take $L_1 = \frac{6L}{7}$. Then, total cost:

$$2^{2L/7}$$

Attack on the Signature Scheme
Attack Cost

- Unforgeability is broken.

Attack on the Signature Scheme
Attack Cost

- Unforgeability is broken.
- For the same level of security, must increase parameters by 25% for classical security (17% for quantum security).

Attack on the Signature Scheme
Attack Cost

- Unforgeability is broken.
- For the same level of security, must increase parameters by 25% for classical security (17% for quantum security).
- The attack implies invisibility is broken.

Conclusion

The OMSSCDH Problem and the 1MSSCDH Problem are solvable in polynomial time (with a single query!).

We have an attack to break the unforgeability and invisibility properties of two undeniable signature schemes:

1. Jao-Soukharev, 2014 [1]
2. Srinath-Chandrasekaran, 2018 [2]

[1] D Jao and V Soukharev. *Isogeny-based quantum-resistant Undeniable Signatures.* In International Workshop on Post-Quantum Cryptography, pages 160–179. Springer, 2014.
[2] M Seshadri Srinath and V Chandrasekaran. *Isogeny-based Quantum-resistant Undeniable Blind Signature Scheme.* International Journal of Network Security,20(1):9–18, 2018

Thank you for listening!

You can read more at: https://eprint.iacr.org/2019/950