RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **CRYP-R09**

Another Look at Some Isogeny Hardness Assumptions

Simon-Philipp Merz[1], Romy Minko[2], Christophe Petit[3]

[1]Royal Holloway, University of London

[2]University of Oxford

[3]University of Birmingham

#RSAC

Isogeny-based Cryptography

- post-quantum (PQ) secure key exchange [JF11]
- based on hardness of finding large-degree isogenies
- small keys, but relatively slow compared to other PQ proposals

Isogeny-based Cryptography

- post-quantum (PQ) secure key exchange [JF11]
- based on hardness of finding large-degree isogenies
- small keys, but relatively slow compared to other PQ proposals

This talk

- cryptanalysis of an isogeny-based hardness assumption
- attack on Jao-Soukharev undeniable signatures

Contents

Elliptic Curves

- solutions (x, y) over some field to the equation

$$E : y^2 = x^3 + Ax + B$$

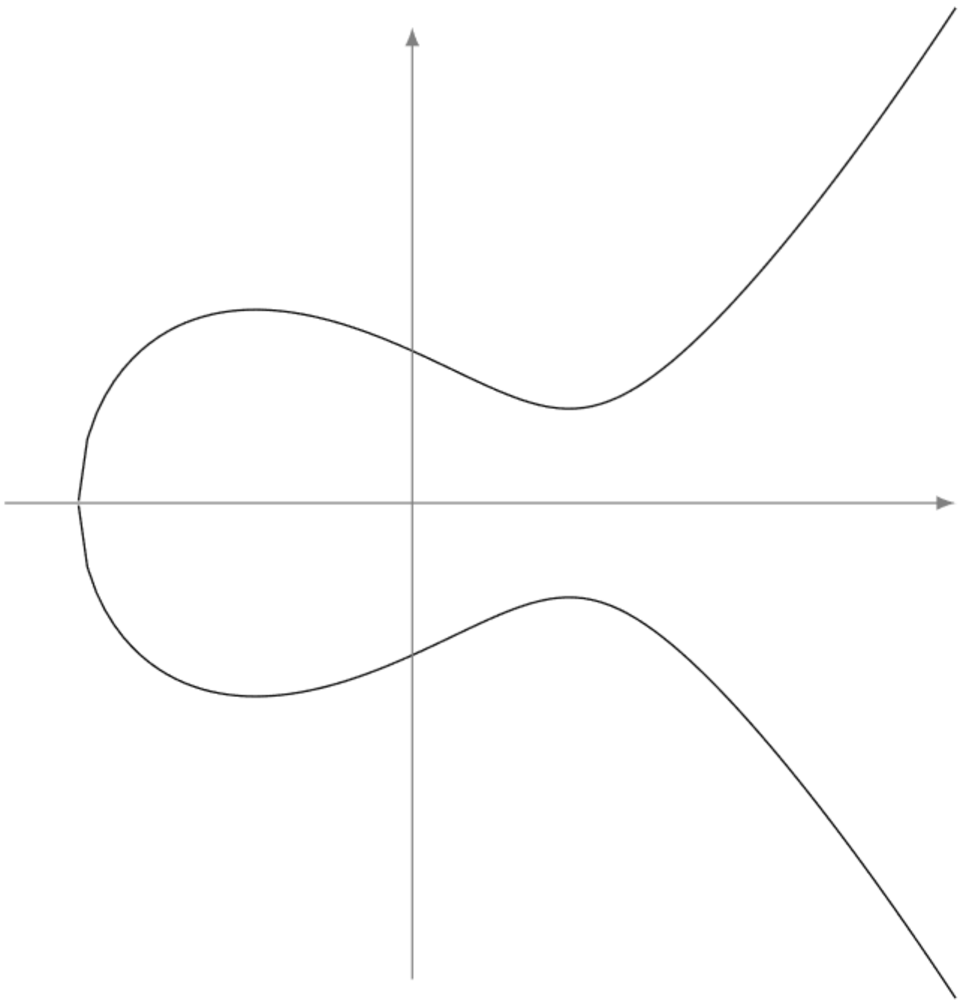
for fixed A, B and $\mathcal{O}_E$ at infinity

Elliptic Curves

- solutions (x, y) over some field to the equation

$$E : y^2 = x^3 + Ax + B$$

for fixed A, B and $\mathcal{O}_E$ at infinity



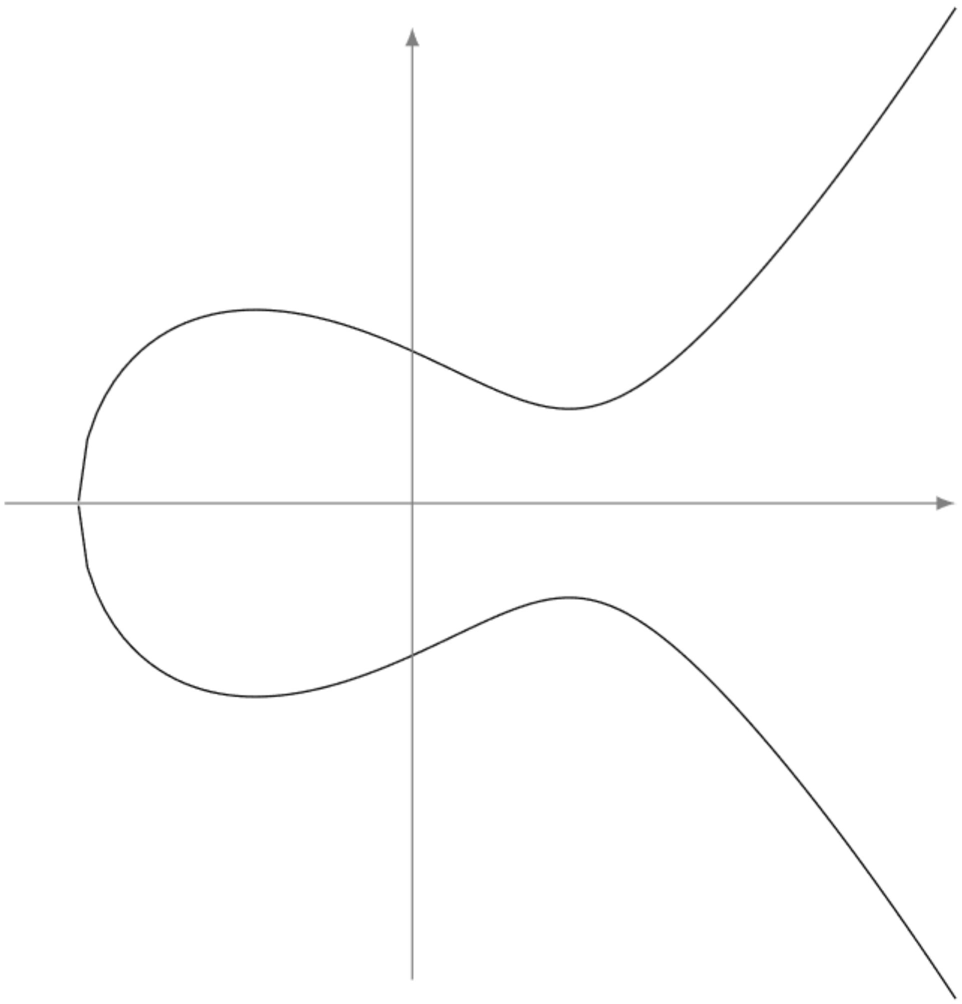
Elliptic Curves

- solutions (x, y) over some field to the equation

$$E : y^2 = x^3 + Ax + B$$

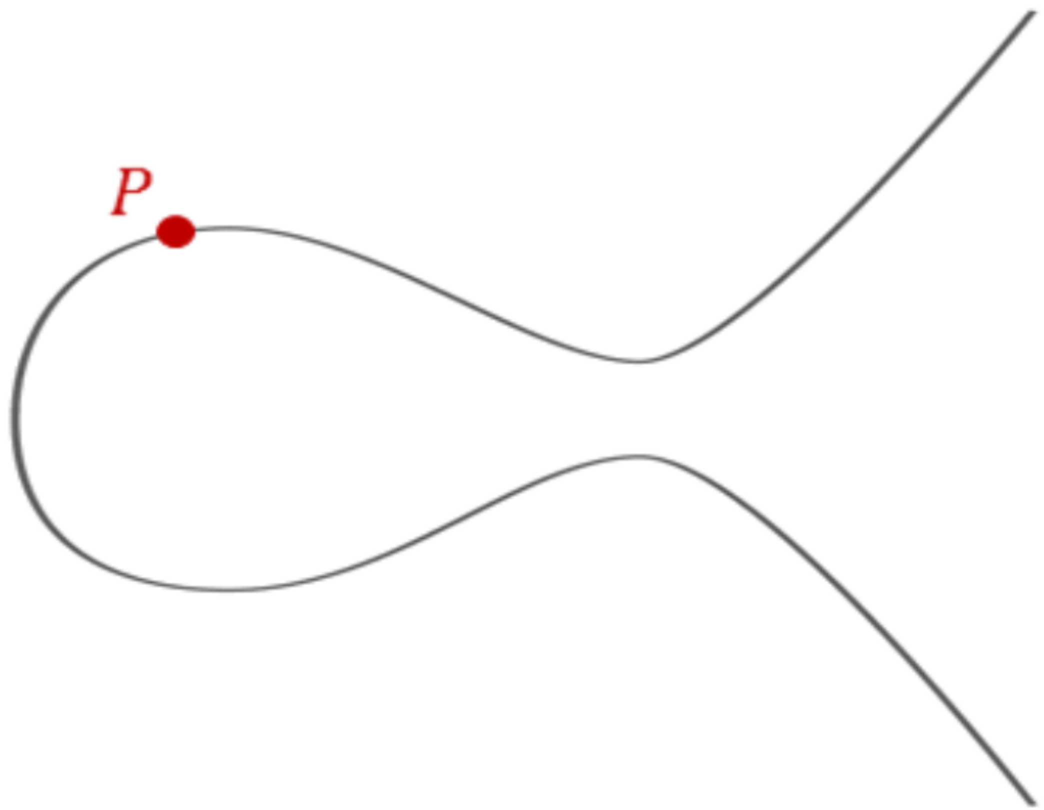
for fixed A, B and $\mathcal{O}_E$ at infinity

- advantage in Cryptography: small keys



ROYAL HOLLOWAY UNIVERSITY OF LONDON

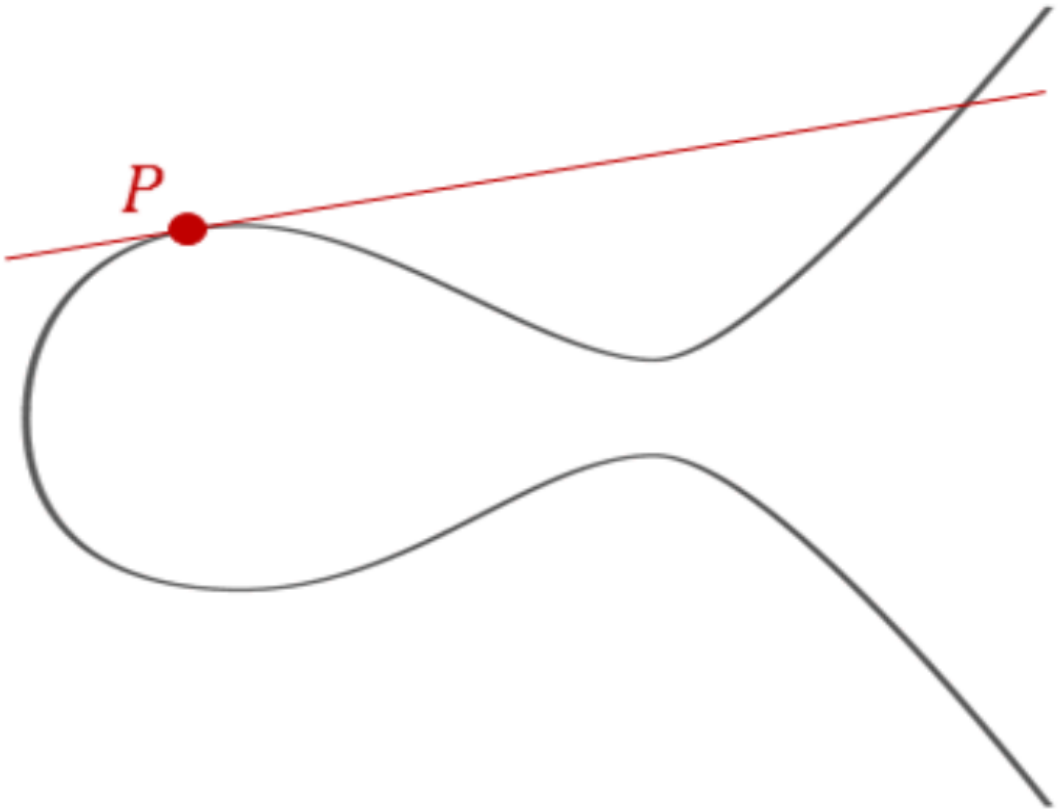
Elliptic Curve Discrete Logarithm Problem



Additive group structure on elliptic curves

ECDLP: Given P and [k]P, compute k.

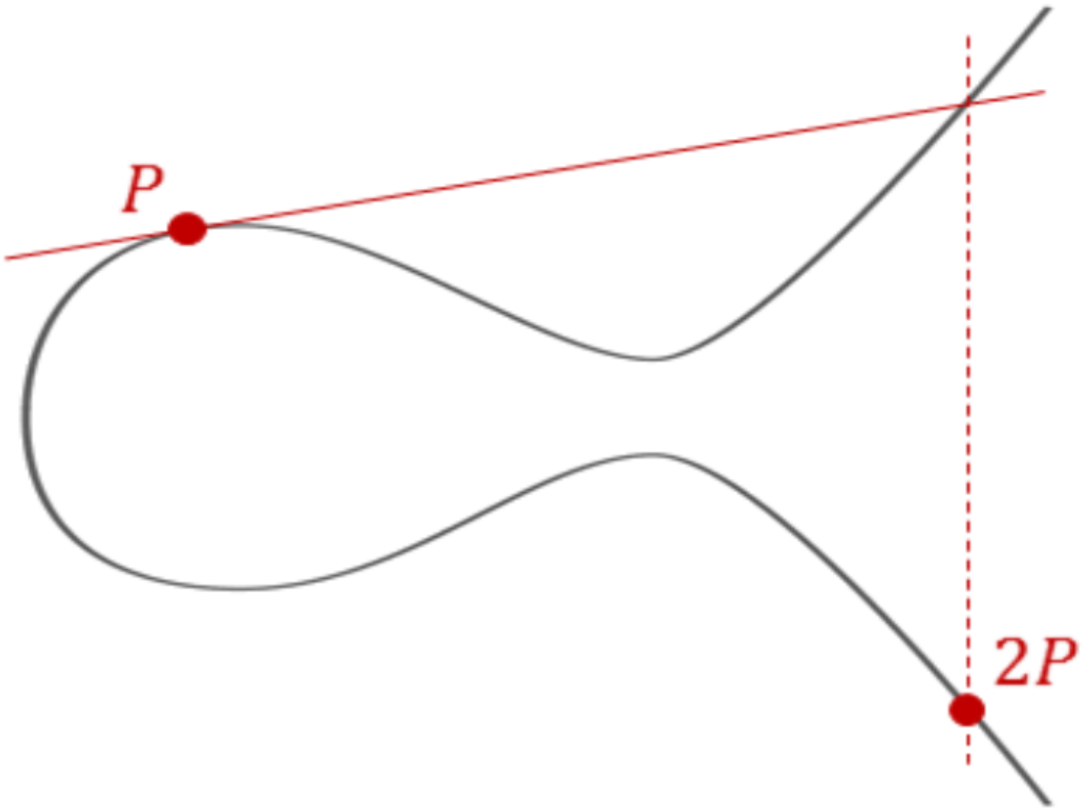
Elliptic Curve Discrete Logarithm Problem



Additive group structure on elliptic curves

ECDLP: Given P and [k]P, compute k.

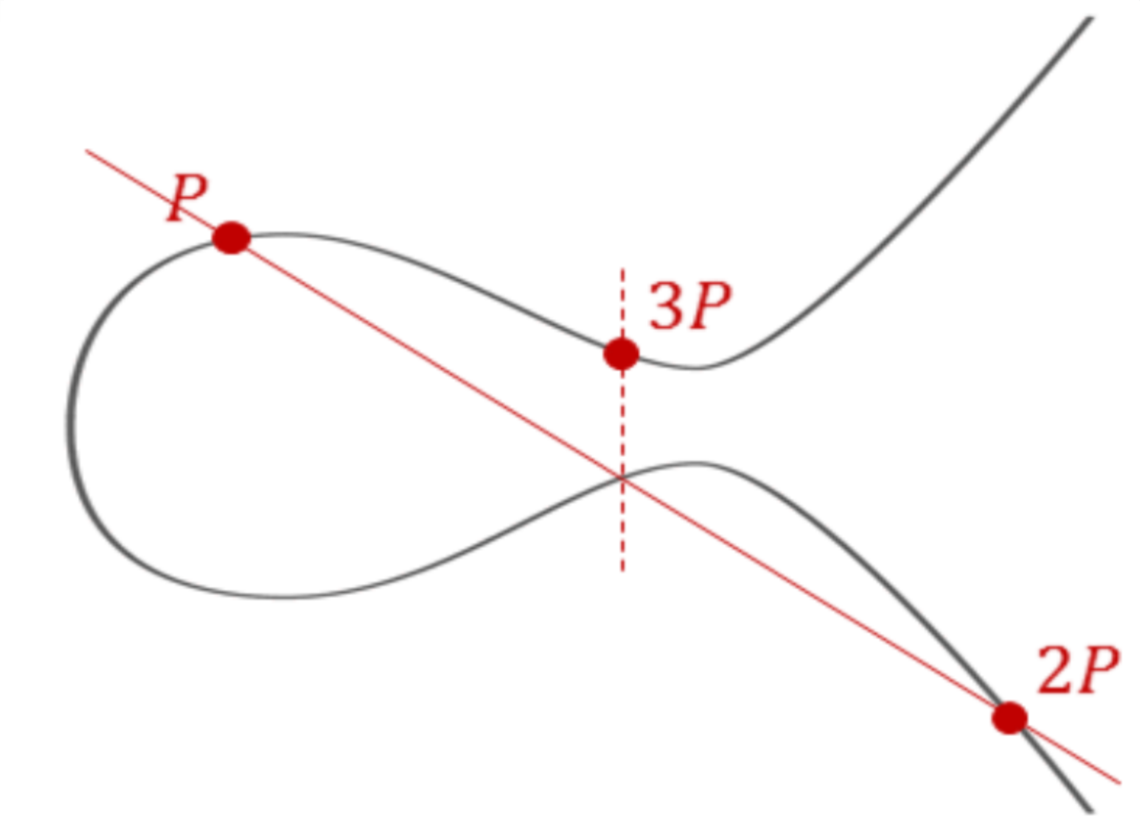
Elliptic Curve Discrete Logarithm Problem



Additive group structure on elliptic curves

ECDLP: Given P and [k]P, compute k.

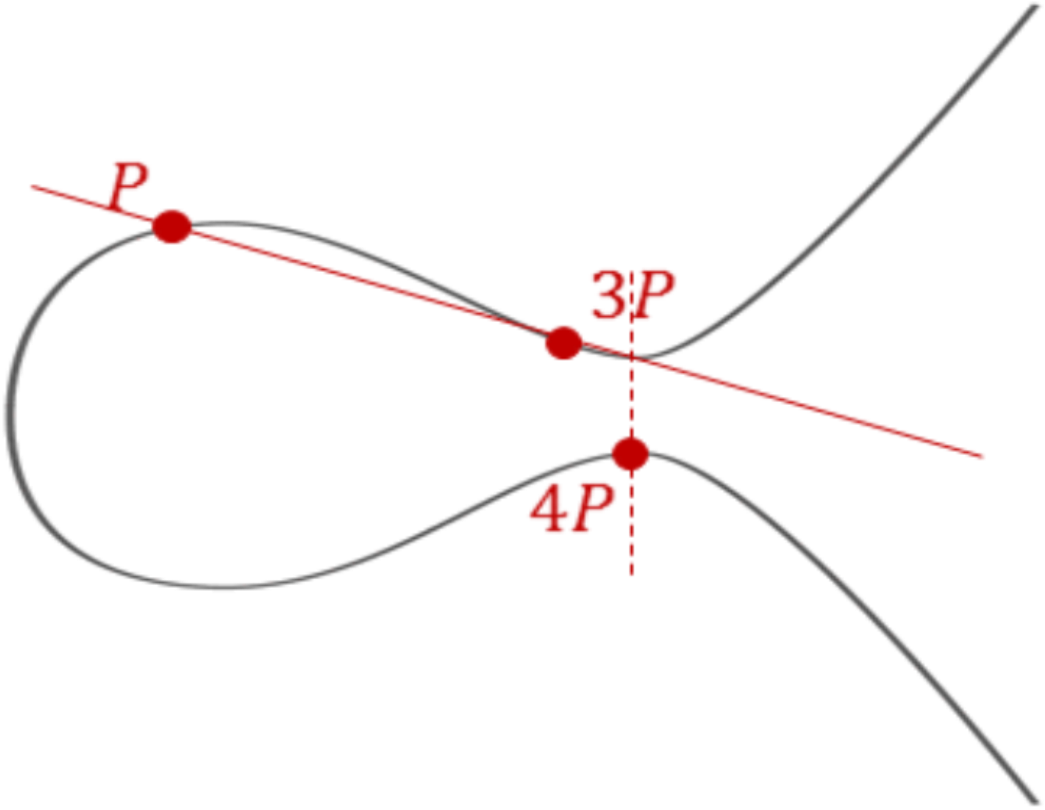
Elliptic Curve Discrete Logarithm Problem



Additive group structure on elliptic curves

ECDLP: Given P and [k]P, compute k.

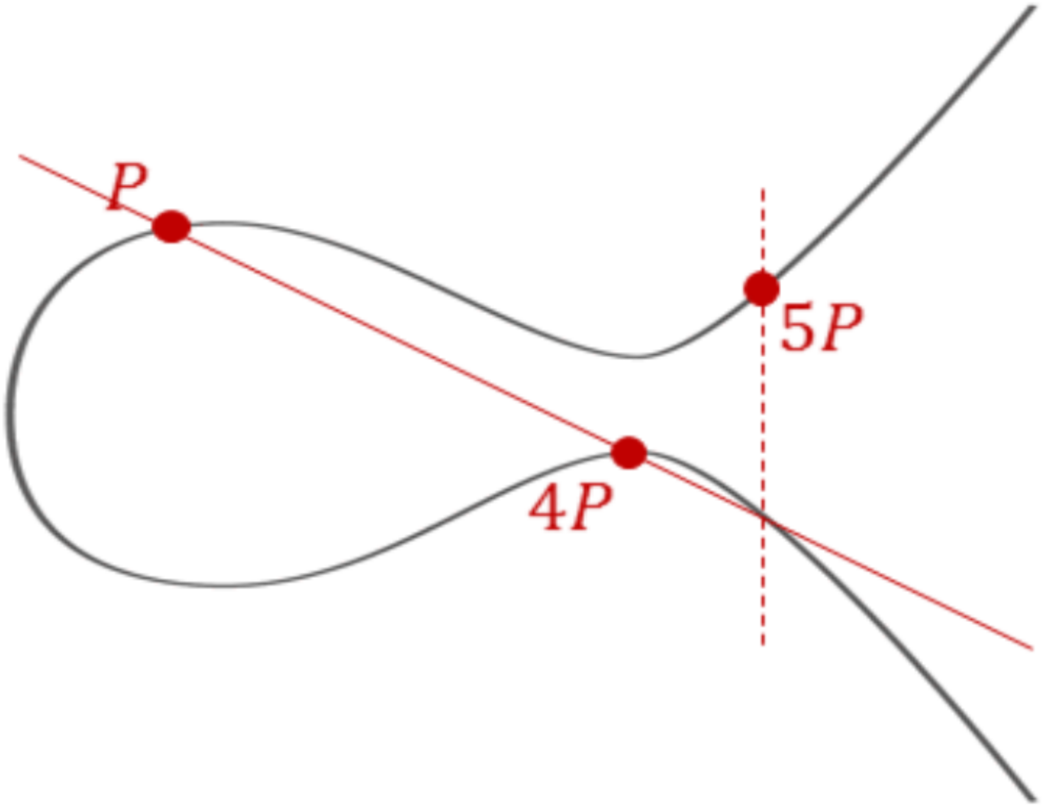
Elliptic Curve Discrete Logarithm Problem



Additive group structure on elliptic curves

ECDLP: Given P and [k]P, compute k.

Elliptic Curve Discrete Logarithm Problem



Additive group structure on elliptic curves

ECDLP: Given P and [k]P, compute k.

Elliptic Curve Discrete Logarithm Problem

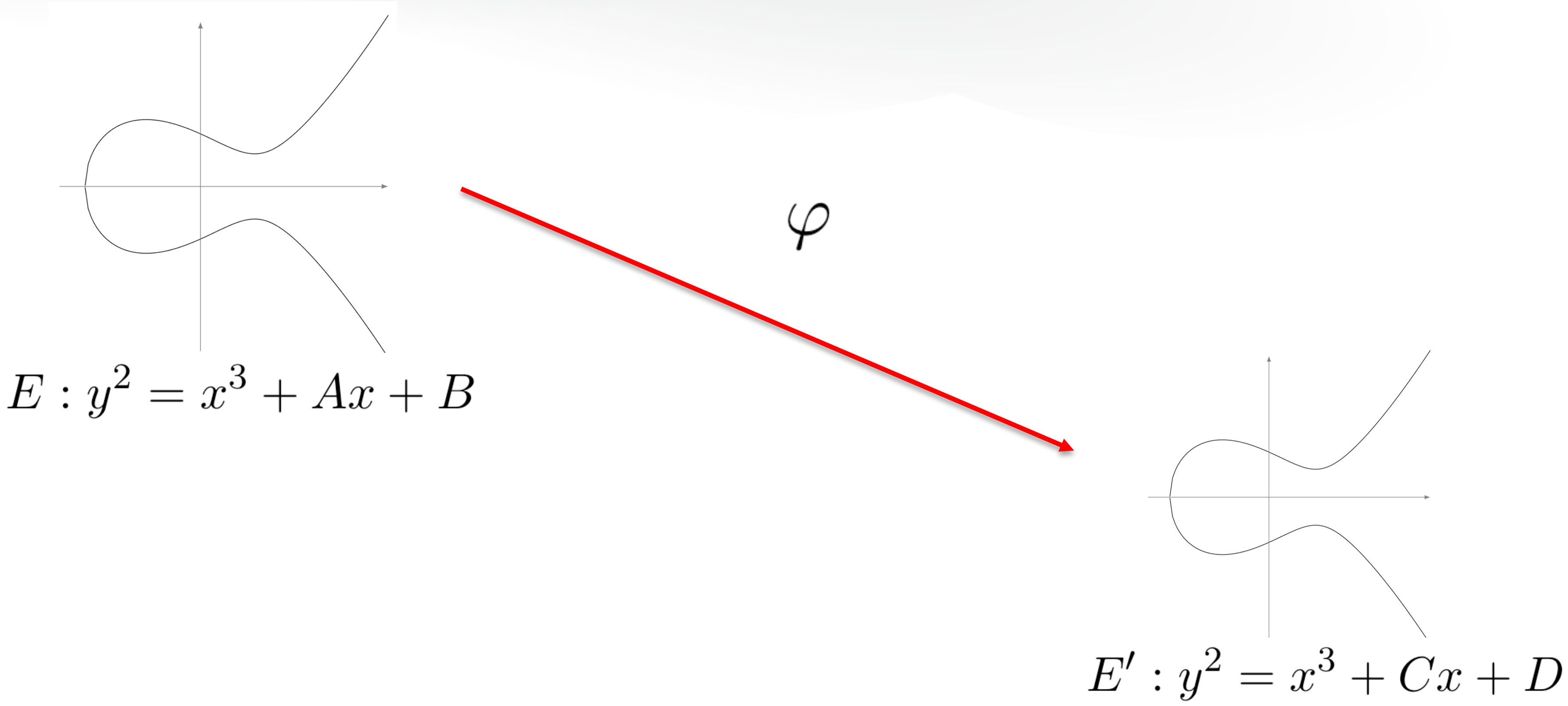
Not quantum-resistant

ECDLP: Given P and [k]P, compute k.

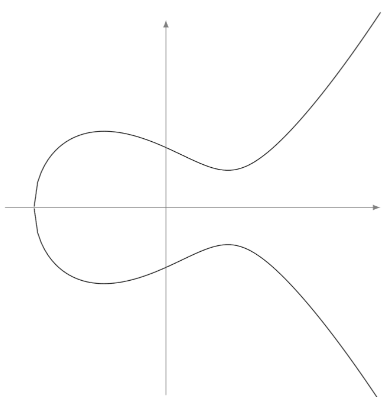
Isogenies

φ

Isogenies

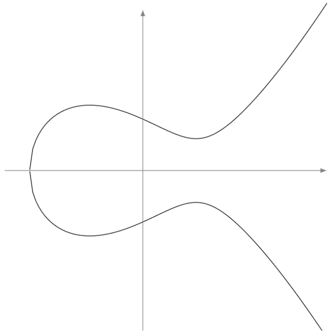


Isogenies



$E : y^2 = x^3 + Ax + B$

φ



$E' : y^2 = x^3 + Cx + D$

- a group morphism $\varphi : E \to E'$
- with kernel any finite subgroup $H \subset E$
- given by rational map of degree $\#H$,

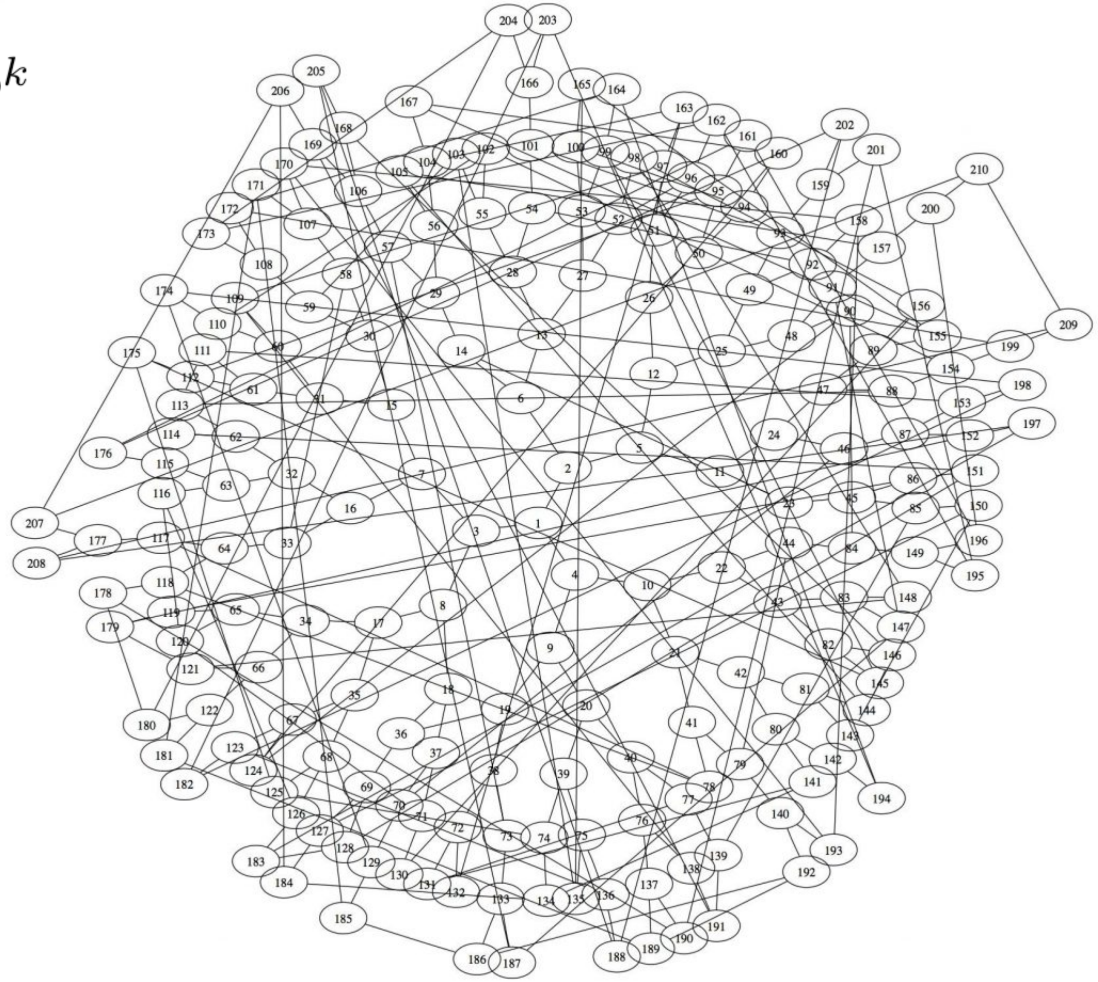
  i.e. $x \mapsto f(x)/g(x), y \mapsto y\big(f(x)/g(x)\big)'$

Isogeny Graphs of a Supersingular Curves

- an elliptic curve E defined over $\mathbb{F}_{p^k}$ is called *supersingular*, if

$$\#E(\mathbb{F}_{p^k}) \equiv 1 \pmod{p}$$

- about $\frac{p}{12}$ supersingular elliptic curves, up to isomorphism



SIDH key exchange [JF11]

E

- fix prime p such that $p = \ell_A^n \ell_B^m - 1$
- supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$
- bases $\langle P_A, Q_A \rangle = E[\ell_A^n]$
  $\langle P_B, Q_B \rangle = E[\ell_B^m]$

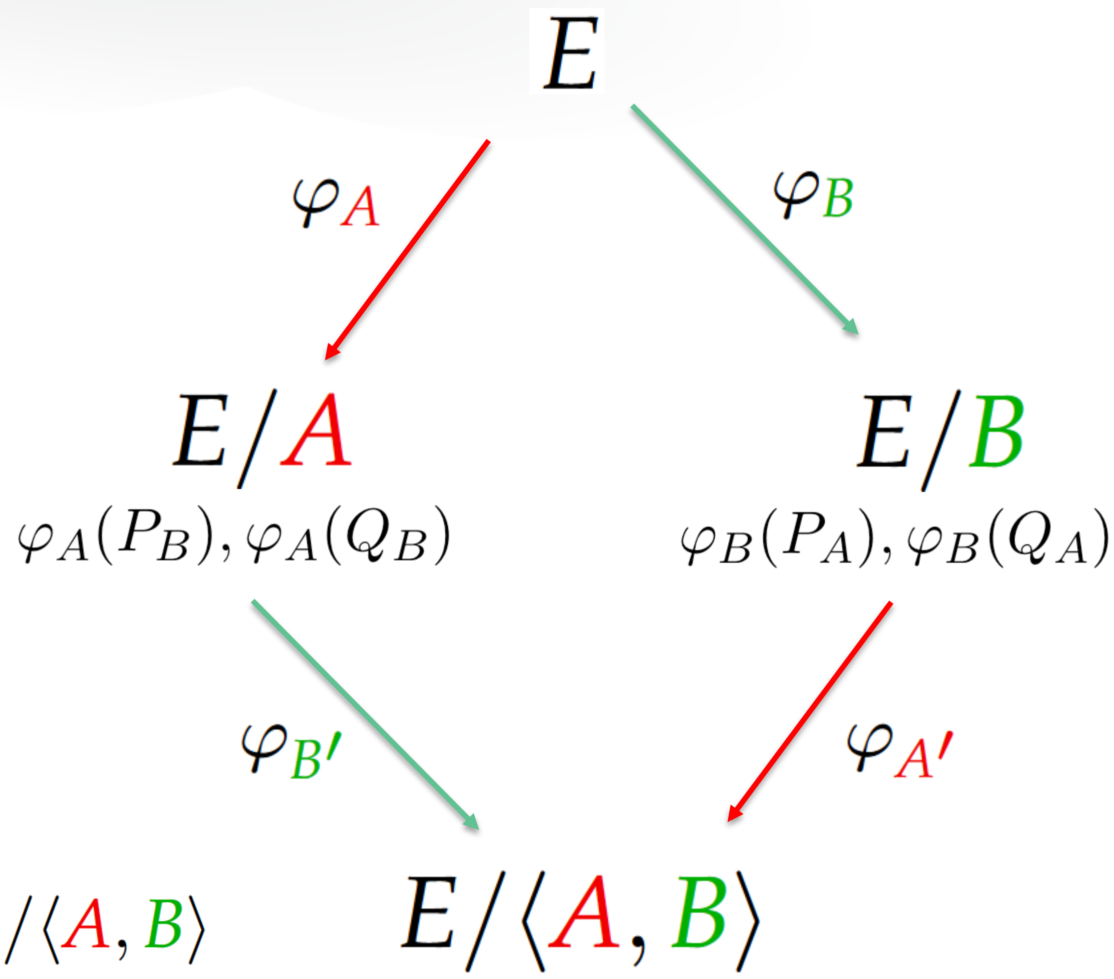
SIDH key exchange [JF11]

- fix prime p such that $p = \ell_A^n \ell_B^m - 1$
- supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$
- bases $\langle P_A, Q_A \rangle = E[\ell_A^n]$
  $\langle P_B, Q_B \rangle = E[\ell_B^m]$
- Alice's secret $A = \langle P_A + [\mathsf{sk}_A] Q_A \rangle$
- Bob's secret $B = \langle P_B + [\mathsf{sk}_B] Q_B \rangle$

$$\begin{array}{ccc} & E & \\ \swarrow^{\varphi_A} & & \searrow^{\varphi_B} \\ E/A & & E/B \\ \varphi_A(P_B), \varphi_A(Q_B) & & \varphi_B(P_A), \varphi_B(Q_A) \end{array}$$

SIDH key exchange [JF11]

- fix prime p such that $p = \ell_A^n \ell_B^m - 1$
- supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$
- bases $\langle P_A, Q_A \rangle = E[\ell_A^n]$
  $\langle P_B, Q_B \rangle = E[\ell_B^m]$
- Alice's secret $A = \langle P_A + [\mathsf{sk}_A] Q_A \rangle$
- Bob's secret $B = \langle P_B + [\mathsf{sk}_B] Q_B \rangle$
- shared secret is isomorphism class of $E/\langle A, B \rangle$



Modified SSCDH

Problem

Given $E, E/A, E/B$ and φ_B .

Compute $E/\langle A, B\rangle$, up to isomorphism.

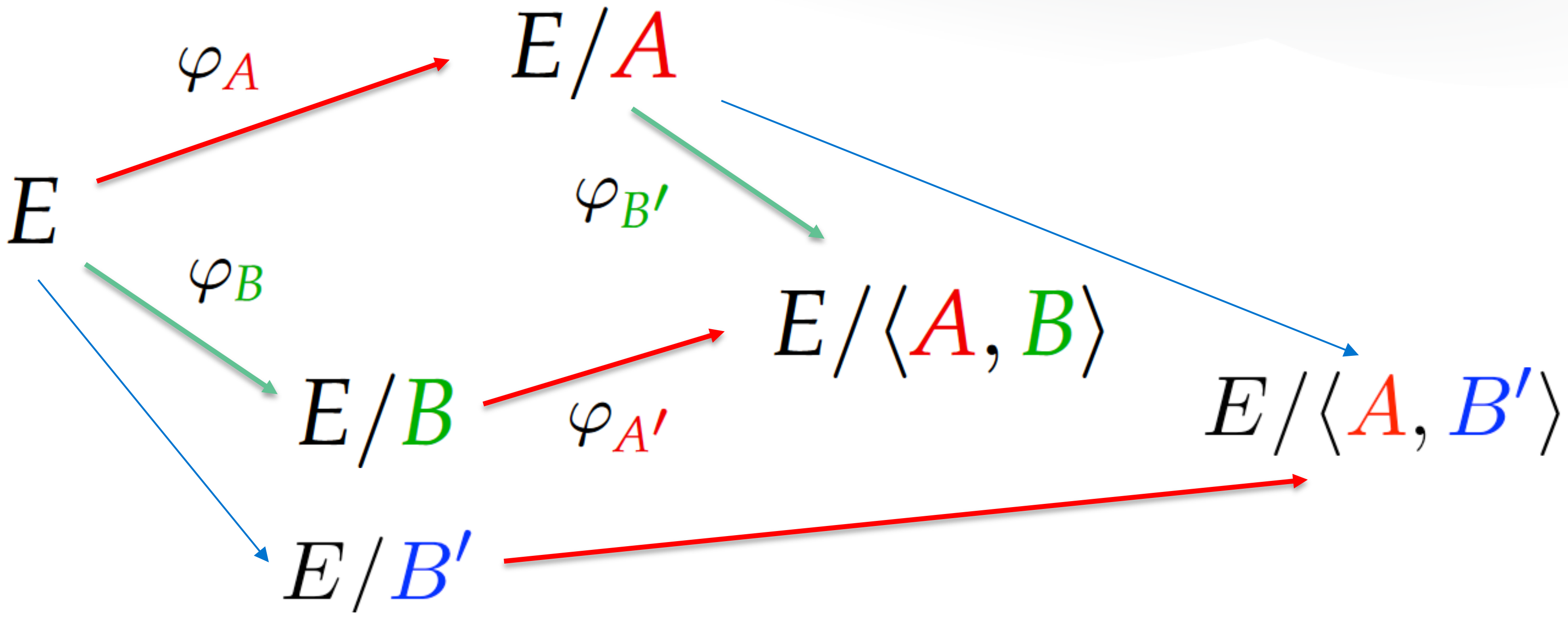
$$\begin{tikzcd}
 & E \arrow[dl, "\varphi_A"'] \arrow[dr, "\varphi_B"] & \\
E/A \arrow[dr, "\varphi_{B'}"'] & & E/B \arrow[dl, "\varphi_{A'}"] \\
 & E/\langle A, B\rangle &
\end{tikzcd}$$

One-Sided Modified SSCDH (OMSSCDH)

$$
\begin{tikzcd}
 & E/A \arrow[dr, "\varphi_{B'}"] & \\
E \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] & & E/\langle A, B\rangle \\
 & E/B \arrow[ur, "\varphi_{A'}"'] &
\end{tikzcd}
$$

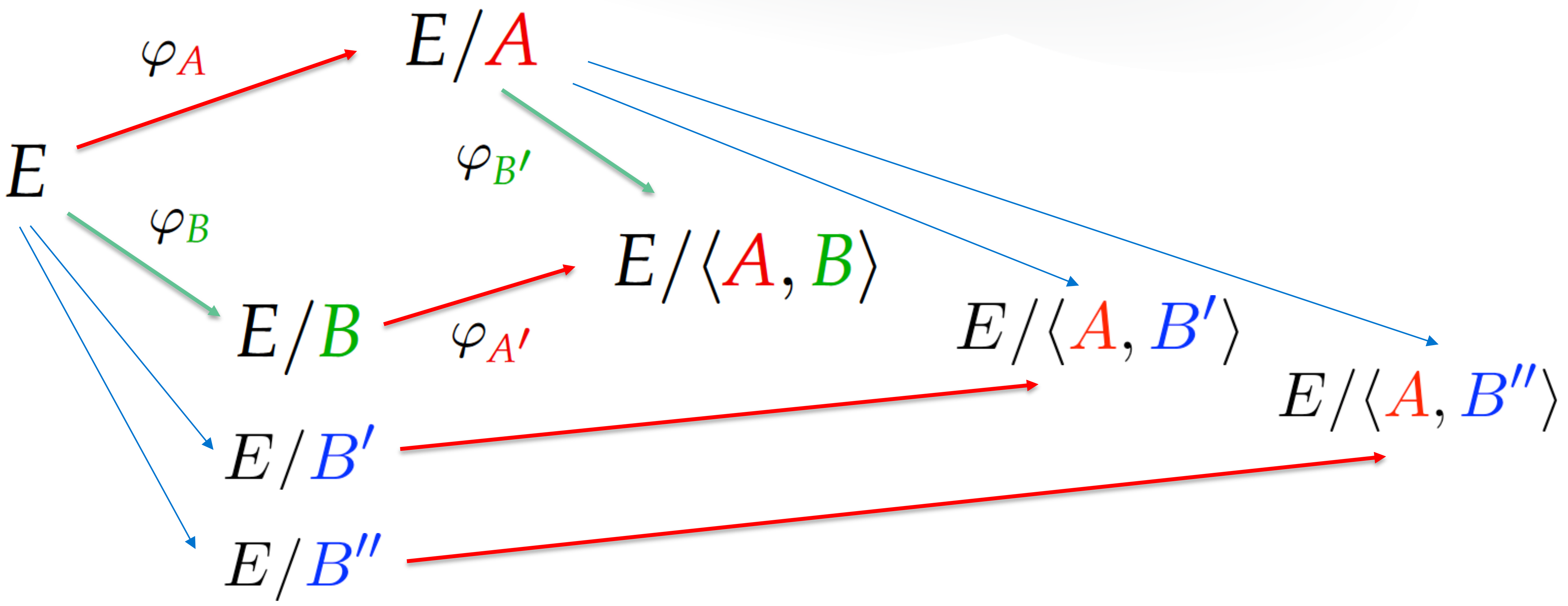
Oracle: Submit a subgroup B' of correct size, to obtain the isomorphism class of $E/\langle A, B'\rangle$

One-Sided Modified SSCDH (OMSSCDH)



Oracle: Submit a subgroup B' of correct size, to obtain the isomorphism class of $E/\langle A, B'\rangle$

One-Sided Modified SSCDH (OMSSCDH)



Oracle: Submit a subgroup B' of correct size, to obtain the isomorphism class of $E/\langle A, B'\rangle$

Application: Jao-Soukharev's Undeniable Signatures

$$\begin{tikzcd}
 & E/A \arrow[dr, "\varphi_{B'}"] \arrow[drr] \arrow[dddrrr] & & & \\
E \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] \arrow[ddr] \arrow[dddr] & & E/\langle A, B\rangle & & \\
 & E/B \arrow[ur, "\varphi_{A'}"'] & & E/\langle A, B'\rangle & \\
 & E/B' \arrow[urr] & & & E/\langle A, B''\rangle \\
 & E/B'' \arrow[urrr] & & &
\end{tikzcd}$$

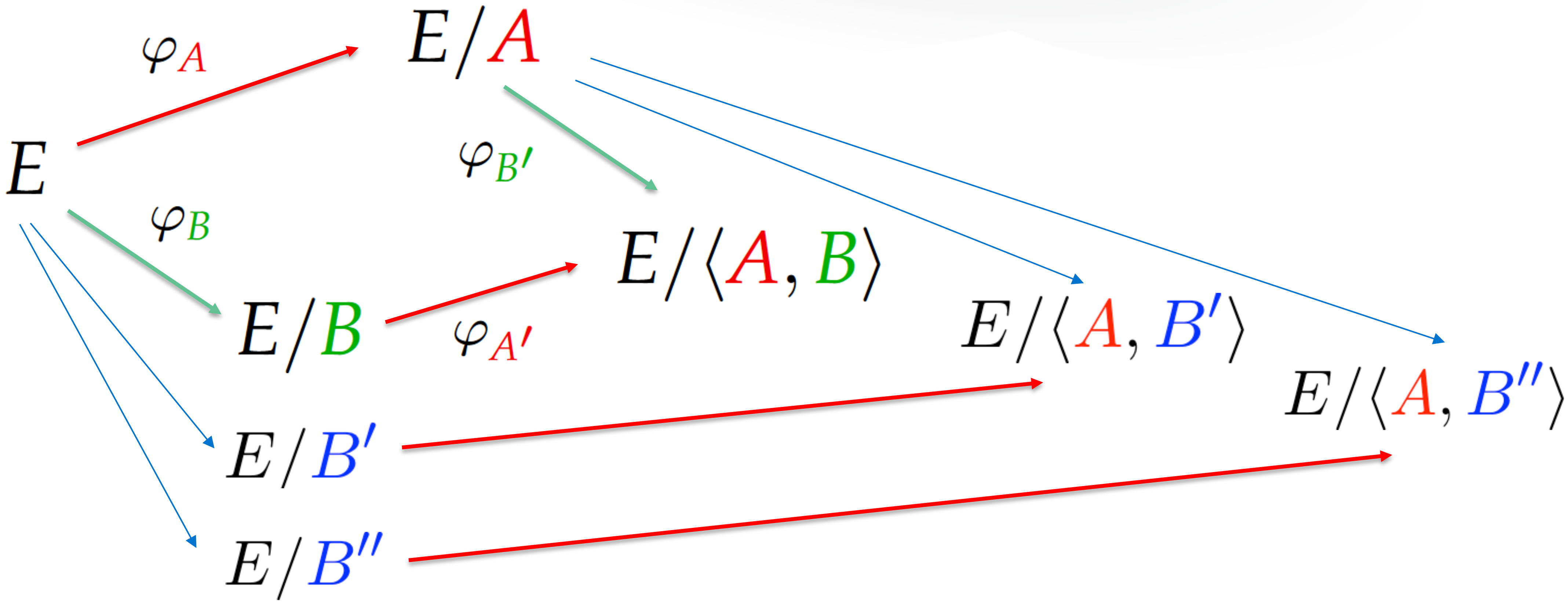
$$B = \langle P_B + H[m]Q_B \rangle$$

$$B' = \langle P_B + H[m']Q_B \rangle$$

$$B'' = \langle P_B + H[m'']Q_B \rangle$$

This problem arises naturally in the security proof of Jao-Soukharev's undeniable signature scheme.

One-Sided Modified SSCDH (OMSSCDH)



Oracle: Submit a subgroup B' of correct size, to obtain the isomorphism class of $E/\langle A, B' \rangle$

Attacking One-Sided Modified SSCDH

$$
\begin{tikzcd}
E \arrow[r] \arrow[dr] & \circ \arrow[r, dotted] & \circ \arrow[r] \arrow[dr] & E_B \arrow[r] \arrow[dr] & \circ \arrow[dr] & \\
& E_A \arrow[r] & \circ \arrow[r, dotted] & \circ \arrow[r] & \boxed{E_{AB}} \arrow[r] & \circ
\end{tikzcd}
$$

Attacking One-Sided Modified SSCDH

$$
\begin{tikzcd}
E \arrow[r] \arrow[dr] & \circ \arrow[r, dotted] & \circ \arrow[r] \arrow[dr] & E_B \arrow[r] \arrow[dr] & \circ \arrow[dr] & \\
& E_A \arrow[r] & \circ \arrow[r, dotted] & \circ \arrow[r] & \boxed{E_{AB}} \arrow[r] & \circ
\end{tikzcd}
$$

Attacking One-Sided Modified SSCDH

$$\begin{tikzcd}
E \arrow[r] \arrow[dr] & \circ \arrow[r, dotted] & \circ \arrow[r] \arrow[dr] & E_B \arrow[r] \arrow[dr] & \circ \arrow[dr] & \\
& E_A \arrow[r] & \circ \arrow[r, dotted] & \circ \arrow[r] & \boxed{E_{AB}} \arrow[r] & \circ
\end{tikzcd}$$

Attacking One-Sided Modified SSCDH

$$
\begin{tikzcd}
E \arrow[r] \arrow[dr] & \circ \arrow[r, dotted] & \circ \arrow[r] \arrow[dr] & E_B \arrow[r] \arrow[dr] & \circ \arrow[dr] & \\
& E_A \arrow[r] & \circ \arrow[r, dotted] & \circ \arrow[r] & \boxed{E_{AB}} \arrow[r] & \circ
\end{tikzcd}
$$

Attacking One-Sided Modified SSCDH

$$
\begin{tikzcd}
E \arrow[r] \arrow[dr] & \circ \arrow[r, dotted] & \circ \arrow[r] \arrow[dr] & E_B \arrow[r] \arrow[dr] & \circ \arrow[dr] & \\
& E_A \arrow[r] & \circ \arrow[r, dotted] & \circ \arrow[r] & \boxed{E_{AB}} \arrow[r] & \circ
\end{tikzcd}
$$

Attacking One-Sided Modified SSCDH

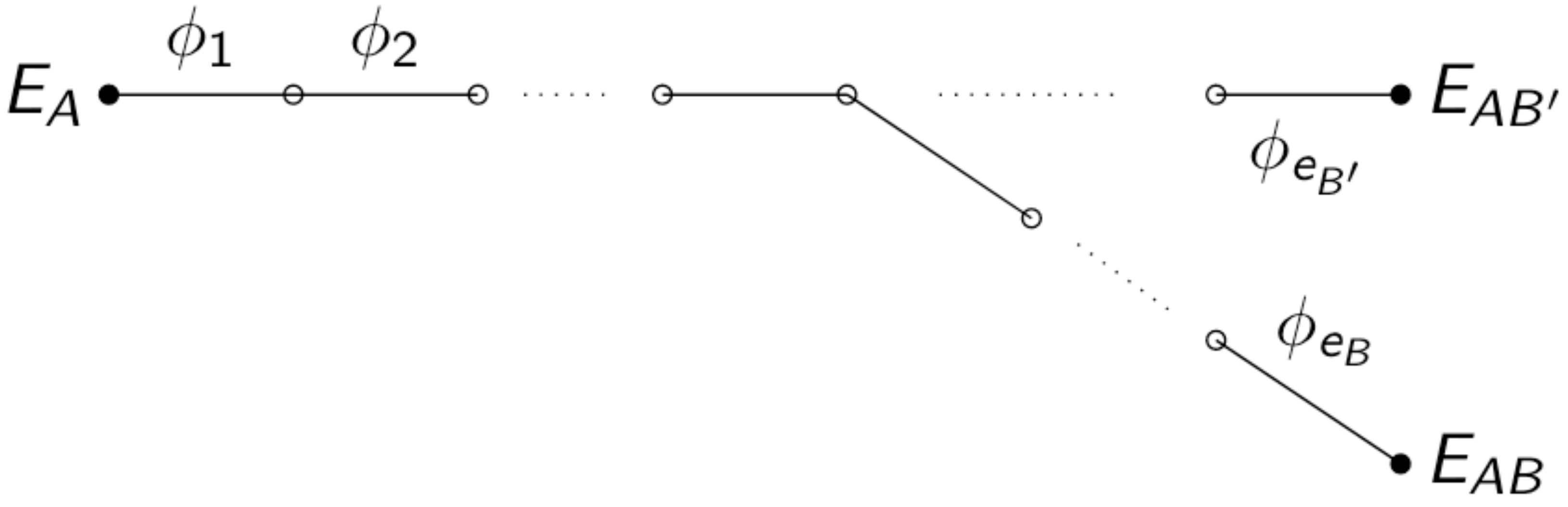
$$
\begin{tikzcd}
E \arrow[r] \arrow[ddr] & \circ \arrow[r, dotted] & \circ \arrow[r] \arrow[dr] & E_B \arrow[ddr] & \\
& & & E_{B'} \arrow[ddr] & \\
& E_A \arrow[r] & \circ \arrow[r, dotted] & \circ \arrow[r] \arrow[dr] & E_{AB} \\
& & & & E_{AB'}
\end{tikzcd}
$$

Theorem: We can guess isomorphism class of E_{AB} with probability $\frac{1}{(\ell_B+1)\ell_B}$ after a single query to the oracle.

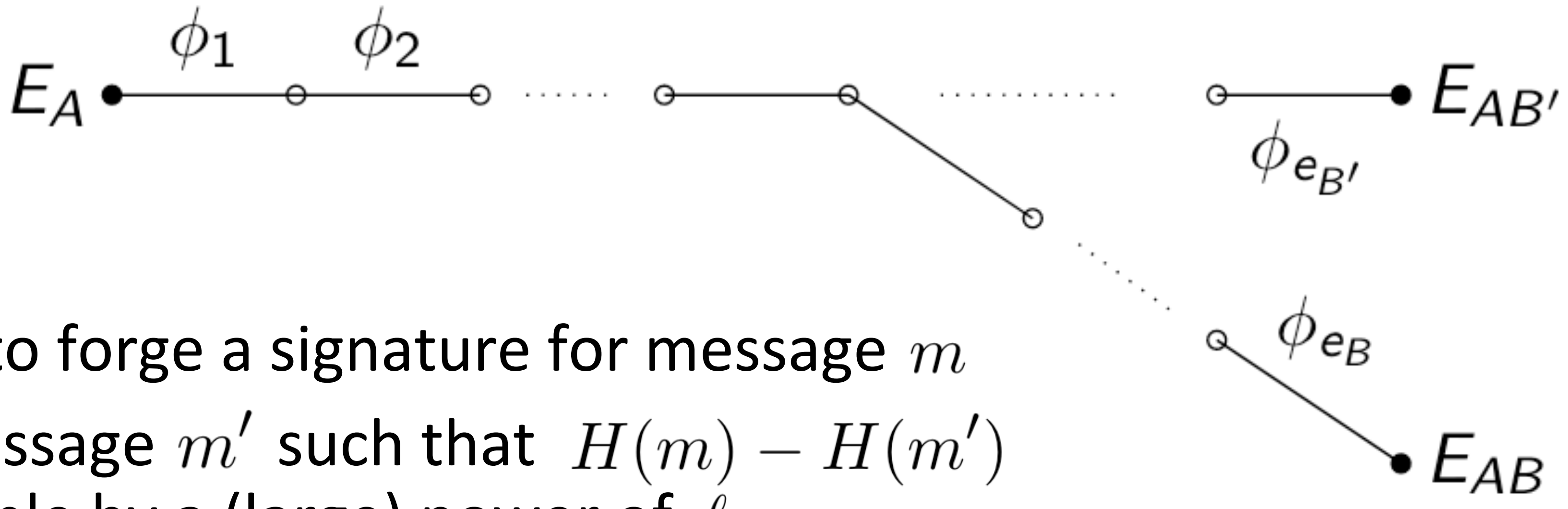
Attacking Jao-Soukharev Undeniable Signatures

Lemma:

Let the notation be as before. If $\alpha, \beta < \ell^e$ are positive integers modulo ℓ^k for some $k \in \mathbb{Z}$, then the ℓ-isogeny paths from E_A to $E_{AB} := E_A/\langle P_B + [\alpha]Q_B \rangle$ and to $E_{AB'} := E_A/\langle P_B + [\beta]Q_B \rangle$ are equal up to the k-th step.



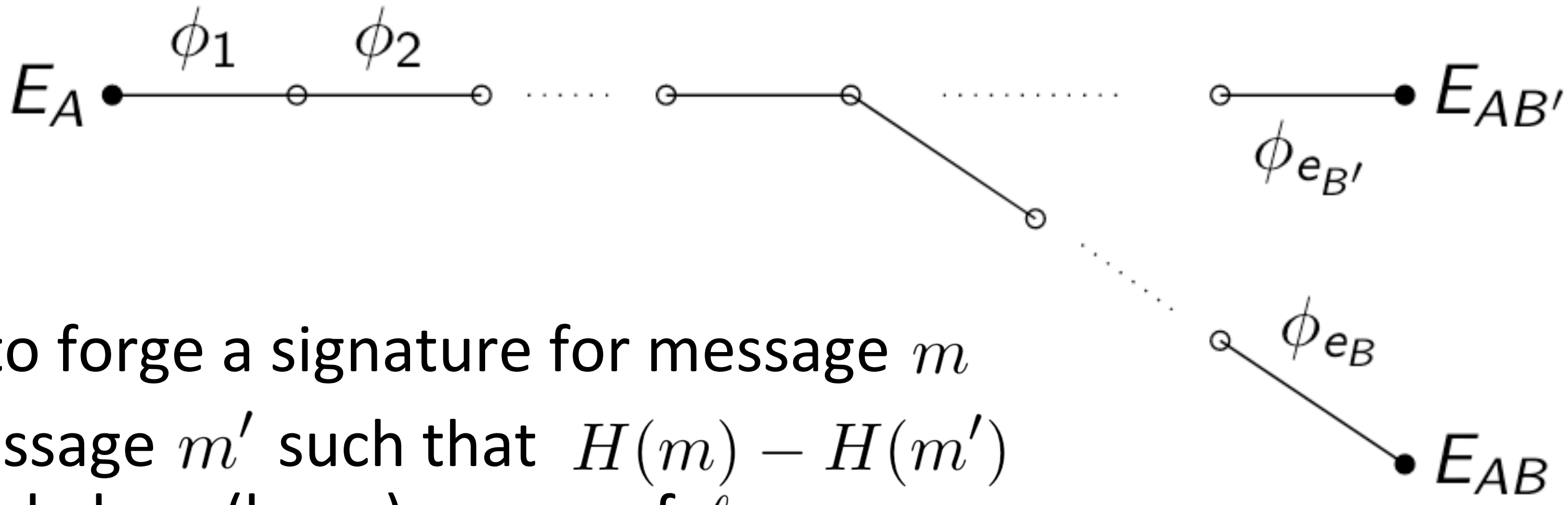
Attacking Jao-Soukharev Undeniable Signatures



Strategy to forge a signature for message m

– find message m' such that $H(m) - H(m')$ is divisible by a (large) power of ℓ_B

Attacking Jao-Soukharev Undeniable Signatures



Strategy to forge a signature for message m

- find message m' such that $H(m) - H(m')$ is divisible by a (large) power of ℓ_B
- use signing oracle to obtain $E_{AB'}$ in signature of m'
- brute-force isogeny $E_{AB'} \to E_{AB}$
- trade-off between the steps

Attacking Jao-Soukharev Undeniable Signatures

Classical Cost

- $2^{\frac{4\lambda}{5}}$ instead of 2^{λ} for security parameter λ

- need to increase parameters by 25%

Quantum Cost

Attacking Jao-Soukharev Undeniable Signatures

Classical Cost

– $2^{\frac{4\lambda}{5}}$ instead of 2^{λ} for security parameter λ

– need to increase parameters by 25%

Quantum Cost

– $2^{\frac{6\lambda}{7}}$ instead of 2^{λ} for security parameter λ

– need to increase parameters by 17%

Conclusion and Takeaway

- raise parameters for Jao-Soukharev undeniable signatures
- the OMSSCDH hardness assumption is broken
- verification of security proofs is important
- try to reduce to standard hardness assumptions

Conclusion and Takeaway

- raise parameters for Jao-Soukharev undeniable signatures
- the OMSSCDH hardness assumption is broken
- verification of security proofs is important
- try to reduce to standard hardness assumptions