Side-Channel Attacks on Quantum-Resistant Supersingular Isogeny Diffie-Hellman

Presenter: Reza Azarderakhsh

CEECS Department and I-Sense, Florida Atlantic University
razarderakhsh@fau.edu

Paper by: Brian Koziel (Texas Instruments) [corresponding author, kozielbrian@gmail.com], Reza Azarderakhsh (Florida Atlantic University), and David Jao (University of Waterloo)

SAC 2017
Ottawa, Ontario, Canada

Outline

1. Introduction
2. SIDH Protocol
3. Refined Power Analysis on SIDH
4. Partial-Zero Attack on Three-point Ladder
5. Zero-Point Attack on Three-Point Ladder
6. RPA on Isogeny Computation
7. Takeaways

Introduction

- Supersingular isogeny Diffie-Hellman (SIDH) as a strong quantum-resistant cryptographic primitive for NIST's PQC standardization
  - Originally presented by Jao and De Feo at PQCrypto 2011
  - Provides small keys, forward secrecy and a Diffie-Hellman key exchange
  - Based on difficulty of computing supersingular isogenies between two curves
- This work proposes three different side-channel attacks on SIDH that target the representation of zero in an implementation

Contributions

- We investigate zero-value attacks in the application of the supersingular isogeny Diffie-Hellman
- We propose three novel zero-value attacks:
  - Two zero-value attacks on the three-point Montgomery ladder commonly used in SIDH implementations
  - A zero-value attack on the large-degree isogeny computation

Isogeny-Based Cryptography

- Proposed by David Jao and Luca De Feo in 2011[1]
- An isogeny is defined as a non-constant rational map $\phi : E_1 \rightarrow E_2$ such that the null point is preserved
- Isogeny-based cryptography centers on the difficulty to compute isogenies between elliptic curves
  - Supersingular elliptic curves feature a non-commutative endomorphism ring for which there is no known classical or quantum subexponential solution
- Supersingular isogeny problem $\rightarrow$ For the supersingular case, it is simple to compute the isogeny $\phi : E \rightarrow E'$ to find E' with ϕ and E, but it is extremely difficult to find ϕ with just E and E'.
- Large-degree isogenies can be efficiently computed by iteratively performing base degree isogenies with Vélu's formulas[2]

[1] Jao, D., De Feo, L.: *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*. PQCrypto 2011: 19-34. (2011).
[2] Vélu, J.: *Isogénies Entre Courbes Elliptiques.* Comptes Rendus de l'Académie des Sciences Paris Séries A-B 273, A238-A241 (1971).

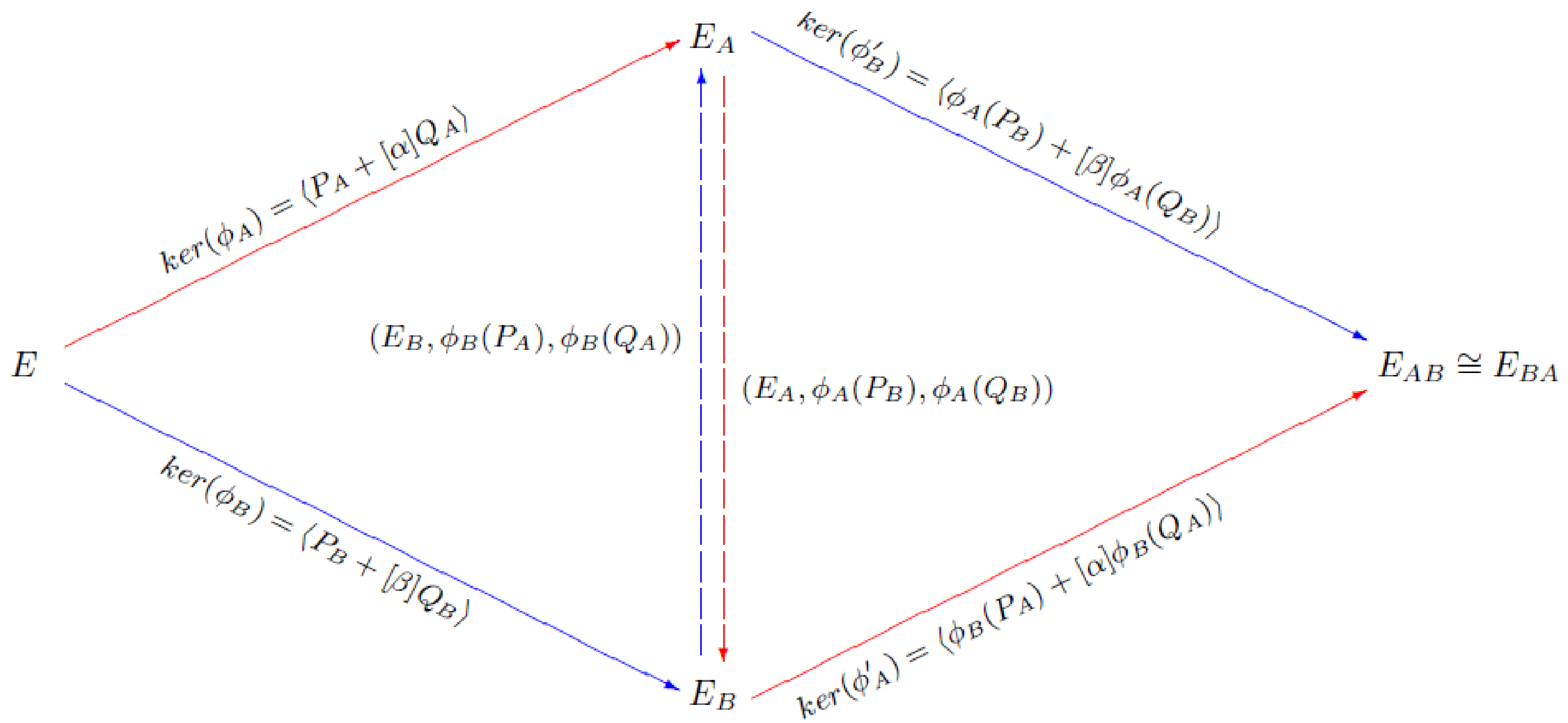
SIDH Overview

- Public Parameters:
  - Smooth Isogeny Prime - $p = \ell_A^{e_A} \ell_B^{e_B} f \pm 1$, where ℓ_A and ℓ_B are small primes, e_A and e_B are positive integers, and f is a small cofactor to make the number prime
  - Starting Supersingular Elliptic Curve, $E_0/\mathbb{F}_{p^2}$
  - Torsion bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ over $E_0[\ell_A^{e_A}]$ and $E_0[\ell_B^{e_B}]$, respectively

SIDH Overview

- Each round is broken into computing a double point multiplication, $R = mP + nQ$, where m and n are secret scalars, and using R as a secret kernel for an isogeny, $\phi : E \to E/\langle R \rangle$.
  - $\phi_A : E \to E/\langle m_A P_A + n_A Q_A \rangle = E_A$ for Alice and $\phi_B : E \to E/\langle m_B P_B + n_B Q_B \rangle = E_B$ for Bob
- After the first round, Alice sends $\{E_A, \phi_A(P_B), \phi_A(Q_B)\}$ and Bob sends $\{E_B, \phi_B(P_A), \phi_B(Q_A)\}$
- After the second round, Alice and Bob have isomorphic curves, so the j-invariant can be used as a shared secret key.
  - $\phi'_A : E_B \to E_B/\langle m_A \phi_B(P_A) + n_A \phi_B(Q_A) \rangle = E_{AB}$ for Alice and $\phi'_B : E_A \to E_A/\langle m_B \phi_A(P_B) + n_B \phi_A(Q_B) \rangle = E_{BA}$ for Bob
  - $j(E_{AB}) = j(E_{BA})$

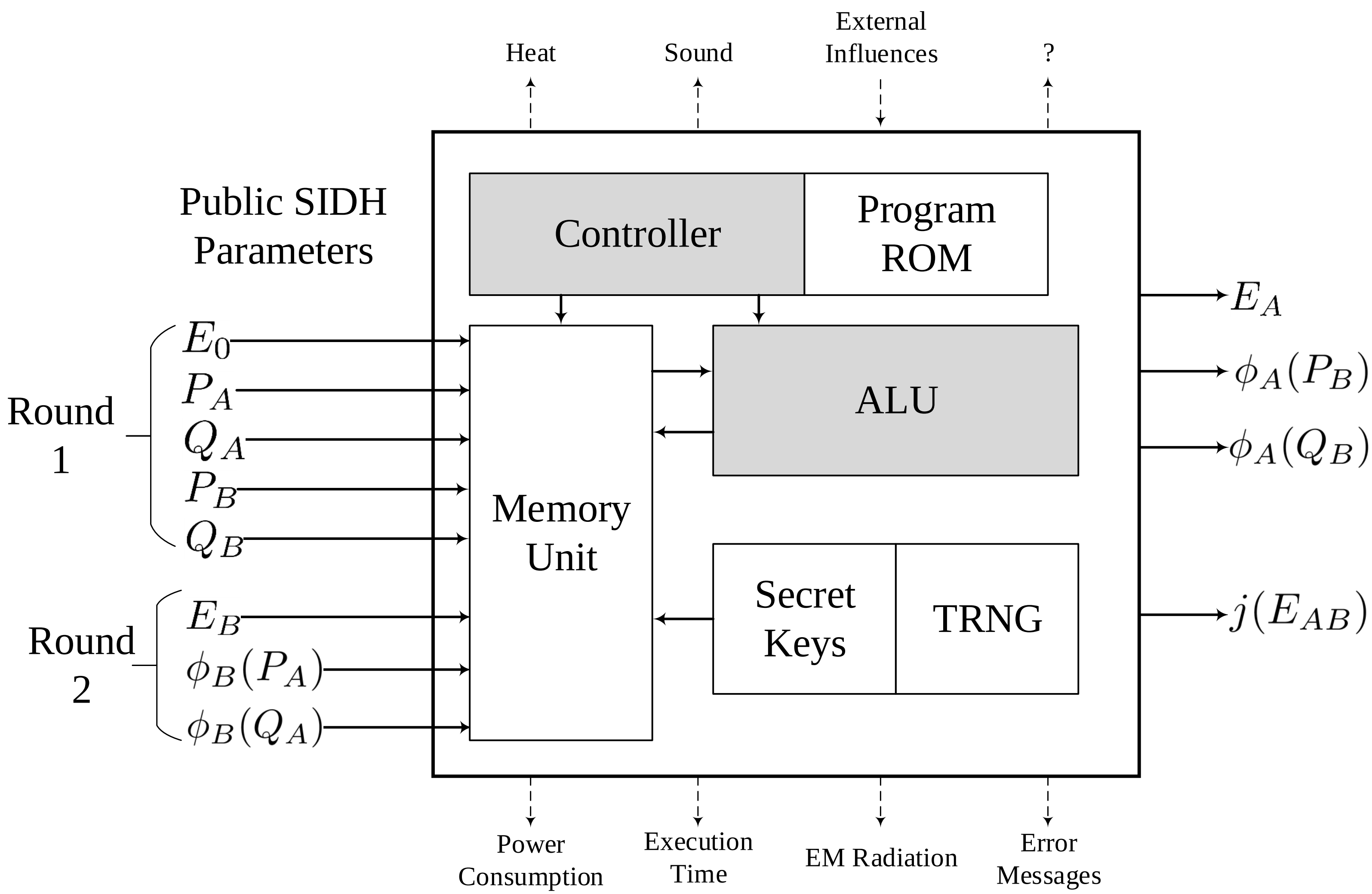
SIDH Protocol



Side-Channel Analysis

- Real-world implementations of cryptosystems must consider the impact of side-channels
- Side-Channel Analysis $\rightarrow$Analyze emissions from an implementation of a cryptosystem
  - Power, Time, Heat
  - Faults, Error Messages
- Implementation-specific

SIDH Cryptosystem with Side-Channels



Side-Channel Analysis Approaches to SIDH

- SIDH can be broken down into kernel point generation and large-degree isogeny computation
- Kernel point generation
  - In SIDH, consists of a double-point multiplication that involves the secret key as a scalar
  - Side-channel analysis can reveal bits of the key or expose the secret kernel
- Large-degree isogeny
  - In SIDH, consists of iteratively computing isogenies of a base degree to perform a isogeny graph walk based on the secret kernel
  - Side-channel analysis can reveal each isogeny path decision

Refined Power Analysis

- Refined Power Analysis (RPA) →Analyzing power emissions with an emphasis on computations involving zero
  - Multiplier and adder circuits involve many digital gates
  - RPA targets unique power signatures produced from a zero operand
- Zero-point attack bypasses several ECC differential power analysis attacks to reveal secret keyst[1]
  - The representation of zero remains constant, even after simple ECC transformations
- Zero-value attack forces zero conditions in ECC computations to reveal secret keys[2]

[1] Goubin, L.: *A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems*. PKC 2003. 199-211 (2002)
[2] Akishita, T., Takagi, T.: *Zero-Value Point Attacks on Elliptic Curve Cryptosystem*. ISC 2003. 218-233 (2003)

RPA on Quadratic Fields

- Since supersingular elliptic curves can be defined over $\mathbb{F}_q = \mathbb{F}_p$ or $\mathbb{F}_q = \mathbb{F}_{p^2}$, we primarily use arithmetic over $\mathbb{F}_{p^2}$
- Let $A, B \in \mathbb{F}_{p^2}$ such that $A = a_1x + a_0, B = b_1x + b_0$ and $a_1, a_0, b_1, b_0 \in \mathbb{F}_p$. We define an irreducible polynomial over this finite field of the form $x^2 + \alpha x + \beta$.
- Addition $\rightarrow A + B = (a_1 + b_1)x + (a_0 + a_1)$
- Multiplication $\rightarrow A \times B = (a_0b_1 + a_1b_0 - \alpha a_1b_1)x + (a_0b_0 - \beta a_1b_1)$
- For RPA, we define A to be
  - Full-zero if $a_0 = 0,\ a_1 = 0$
  - Partial-zero if $a_0 \neq 0,\ a_1 = 0$ or $a_0 = 0,\ a_1 \neq 0$
  - Non-zero if $a_0 \neq 0,\ a_1 \neq 0$

Double-Point Multiplication Optimizations

- Problem: How to efficiently perform the double-point multiplication?
- Solution: Any secret kernel generator will do, so compute $R = P + mQ$[1]
- Problem: Efficient Montgomery coordinate differential arithmetic cannot immediately be used with the above.
- Solution: Utilize three-point differential ladder[1]
  - Each step produces $[t]Q$, $[t+1]Q$, $P+[t]Q$

[1] De Feo, L., Jao, D., Plût, J.: *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*. Journal of Mathematical Cryptology 8(3), 209-247 (Sep. 2014)

Three-Point Differential Ladder for Montgomery Coordinates

- Three-point differential ladder to compute $P+[t]Q$. "dadd$(P,Q,(P-Q).x)$" represents a differential point addition of P and Q, where the x-coordinate of $P-Q$ is known.[1]

Input: Points P and Q on an elliptic curve E, scalar d which is k bits
1: Set $A=0, B=Q, C=P$
2: Compute $Q-P$
3: **for** i decreasing **from** $|d|$ **downto** 1 **do**
4: Let d_i be the i-th bit of d
5: **if** $d_i=0$ **then**
6: $B=$dadd(A,B,Q), $C=$dadd(A,C,P), $A=2A$
7: **else**
8: $A=$dadd(A,B,Q), $C=$dadd$(B,C,Q-P)$, $B=2B$
9: **end if**
10: **end for**
Ensure: $C=P+[t]Q$

[1] Jao, D., De Feo, L., Plût: *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*. Journal of Mathematical Cryptology 8(3), 209-247 (Sep. 2014).

Three-Point Differential Ladder for Montgomery Coordinates

- Three-point differential ladder to compute $P+[t]Q$. "dadd$(P, Q, (P-Q).x)$" represents a differential point addition of P and Q, where the x-coordinate of $P-Q$ is known.[1]

Input: Points P and Q on an elliptic curve E, scalar d which is k bits
1: Set $A=0, B=Q, C=P$
2: Compute $Q-P$
3: **for** i decreasing **from** $|d|$ **downto** 1 **do**
4: Let d_i be the i-th bit of d
5: **if** $d_i=0$ **then**
6: $B=$dadd(A,B,Q), $C=$dadd(A,C,P), $A=2A$
7: **else**
8: $A=$dadd(A,B,Q), $C=$dadd$(B,C,Q-P)$, $B=2B$
9: **end if**
10: **end for**
Ensure: $C=P+[t]Q$

[1] Jao, D., De Feo, L., Plût: *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*. Journal of Mathematical Cryptology 8(3), 209-247 (Sep. 2014).

Partial-Zero Attack on Three-Point Ladder

- For each step of the ladder,
- if $d_i = 0$
  - $C = \mathrm{dadd}(A, C, P)$
- if $d_i = 1$
  - $C = \mathrm{dadd}(B, C, Q - P)$

Partial-Zero Attack on Three-Point Ladder

- For each step of the ladder,
- if $d_i = 0$
  - $C = \text{dadd}(A, C, P)$
- else if $d_i = 1$
  - $C = \text{dadd}(B, C, Q - P)$
- Proposal: Target point differentials P and $Q - P$
  - Choose E,P, $Q - P$ such that $Q - P$ is partial-zero and P is non-zero
  - Results in a power difference for $d_i = 0$ and $d_i = 1$
  - Used as an oracle for each bit of the private key
  - Could be mounted against a dynamic key user if there is enough power contrast

Partial-Zero Attack Countermeasures

- Reject a partial-zero P or a partial-zero $Q - P$
- Randomize representation of P and $Q - P$ to non-zero elements
  - Random projectivization of differential points
    - Reduces efficiency of Montgomery ladder by 2 multiplications per step
  - Random isomorphism of curve and points

Zero-Point Attack on Three-Point Ladder

- Each step of the three-point ladder produces $[t]Q,\ [t+1]Q,\ P+[t]Q$
- Goal of zero-point attack is to predict each bit of the key as a ’0’ or ’1’ and then validate that assumption with a forced zero point.
  - A full-zero point will be used in future computations and identified
- Valid attack on a static key SIDH user
  - Iteratively reveals the bits of the secret key
- Especially dangerous in the context of SIDH, as a malicious party can choose *any* supersingular elliptic curve and points to send as a public key

Zero-Point Attack on Three-Point Ladder

- At the end if the ith step of the three-point ladder, the following points are computed for a secret key d
  - $[x]Q = (\sum_{j=i+1}^{n-1} d_j 2^{j-i} + d_i).Q$
  - $[x+1]Q = (\sum_{j=i+1}^{n-1} d_j 2^{j-i} + d_i + 1).Q$
  - $P + [x]Q = P + (\sum_{j=i+1}^{n-1} d_j 2^{j-i} + d_i).Q$
- Based on our guess d_i, we target a point that will be produced in the $(i+1)$ step
  - if $d_i = 0$, then we will always produce $(\sum_{j=i+1}^{n-1} d_j 2^{j-i} + 1).Q$
  - if $d_i = 1$, then we will always produce $(\sum_{j=i+1}^{n-1} d_j 2^{j-i} + 3).Q$

Zero-Point Attack on Three-Point Ladder

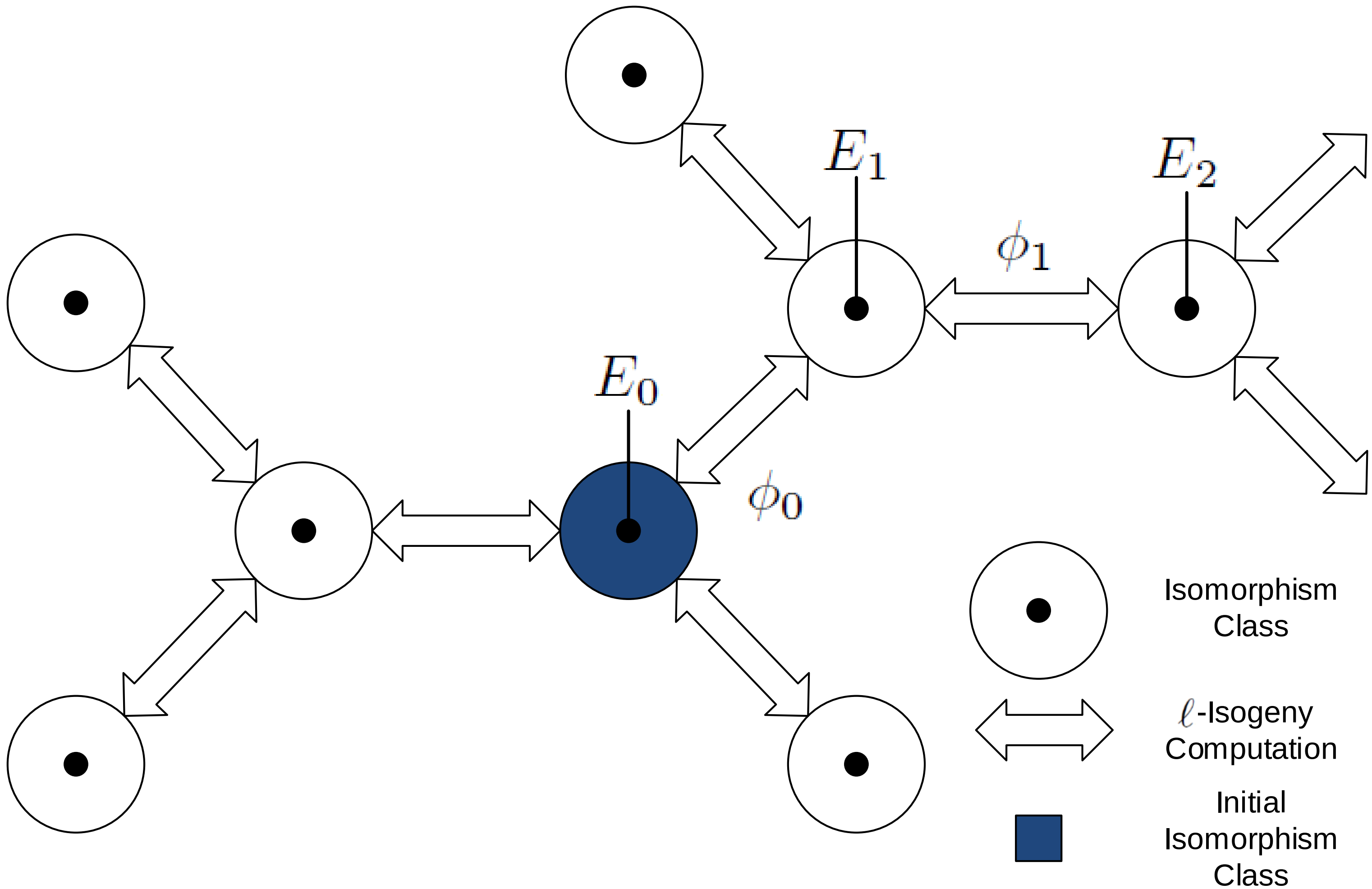
- This attack abuses a point P_0 that has either the x or y-coordinate of 0
  - For Montgomery curves, only point $P_0 = (0, 0)$
- An attacker can force the zero-point condition by solving $P_0 = (\sum_{j=i+1}^{n-1} d_j 2^{j-i} + 1).P_1$ for $d_i = 0$ or $P_0 = (\sum_{j=i+1}^{n-1} d_j 2^{j-i} + 3).P_1$ for $d_i = 1$
- Countermeasures are similar to zero-point countermeasures for ECC[1]:
  - Dynamic keys
  - Initial random isogeny (degree that is not ℓ_A or ℓ_B)
  - Private key representation randomization
  - Point blinding

[1] Smart, N.P.: An Analysis of Goubin's Refinned Power Analysis Attack. CHES 2003. 281-290 (2003)

Isogeny Computation

- Consider the iterative isogenies that are performed based on the secret kernel
  - $\phi_0 \rightarrow \phi_1 \rightarrow \phi_2 \rightarrow \cdots \rightarrow \phi_{e-1}$
- If these isogeny decisions are continuously discovered, then the supersingular isogeny problem becomes *easier*
- Under a specified finite field $\mathbb{F}_q = \mathbb{F}_{p^2}$, there are approximately $p/12$ supersingular curves up to isomorphism
- We can visualize a graph of all isomorphism classes of a specified degree, ℓ, as a complete graph where each node represents a unique isomorphism class and the edges represent an ℓ-isogeny
  - Each node is connected with $\ell + 1$ neighbors

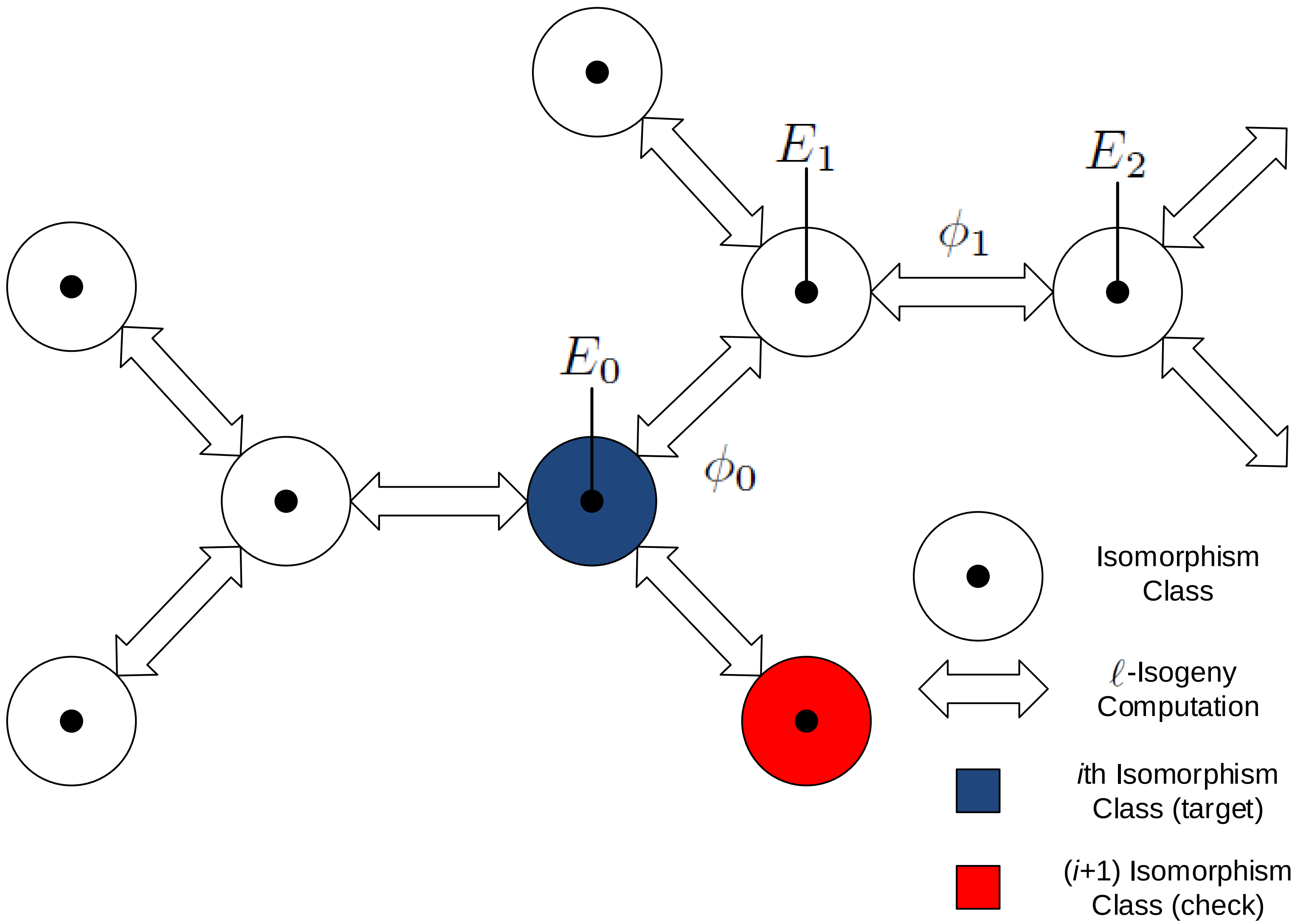
Supersingular Isogeny Graph



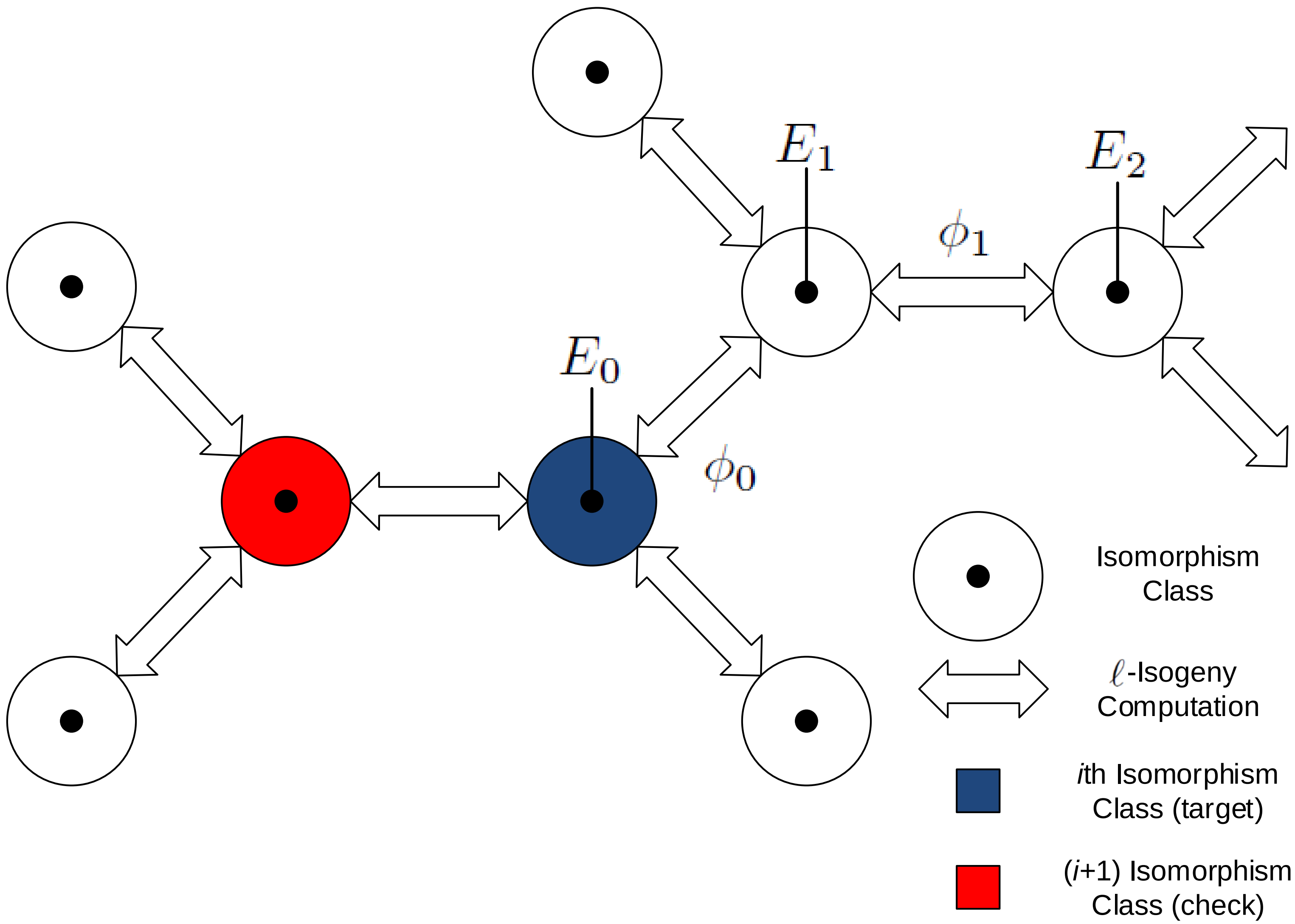
Attacking Isogeny Computation with RPA

- Attack targets a static SIDH user
- Similar to the zero-point attack, we can guess which node will be traversed and verify with a forced zero value
  - Vélu's formulas are deterministic, so an attacker will know which curve will be obtained with each isogeny computation
- We target isogeny decision i and the calculation of the $(i+1)$ isogeny will confirm or deny.
  - Start out at isogeny decision 0 and iteratively build the path up to isogeny decision $e-2$, for a large-degree isogeny of degree ℓ^e
  - Isogeny decision $e-1$ will not be used, but can easily be brute-forced (ℓ possibilities)

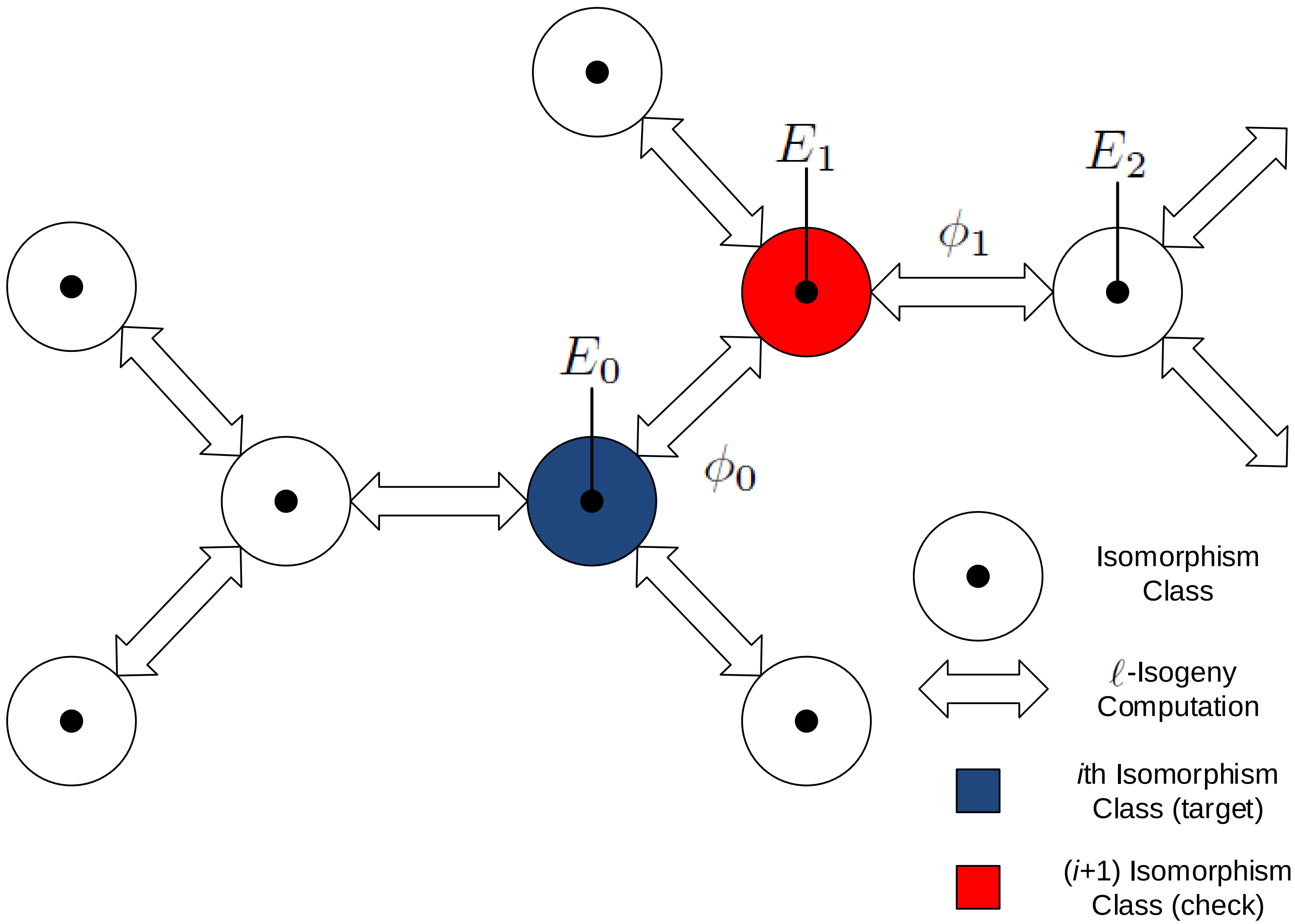
Attacking Iterative Isogeny Walks



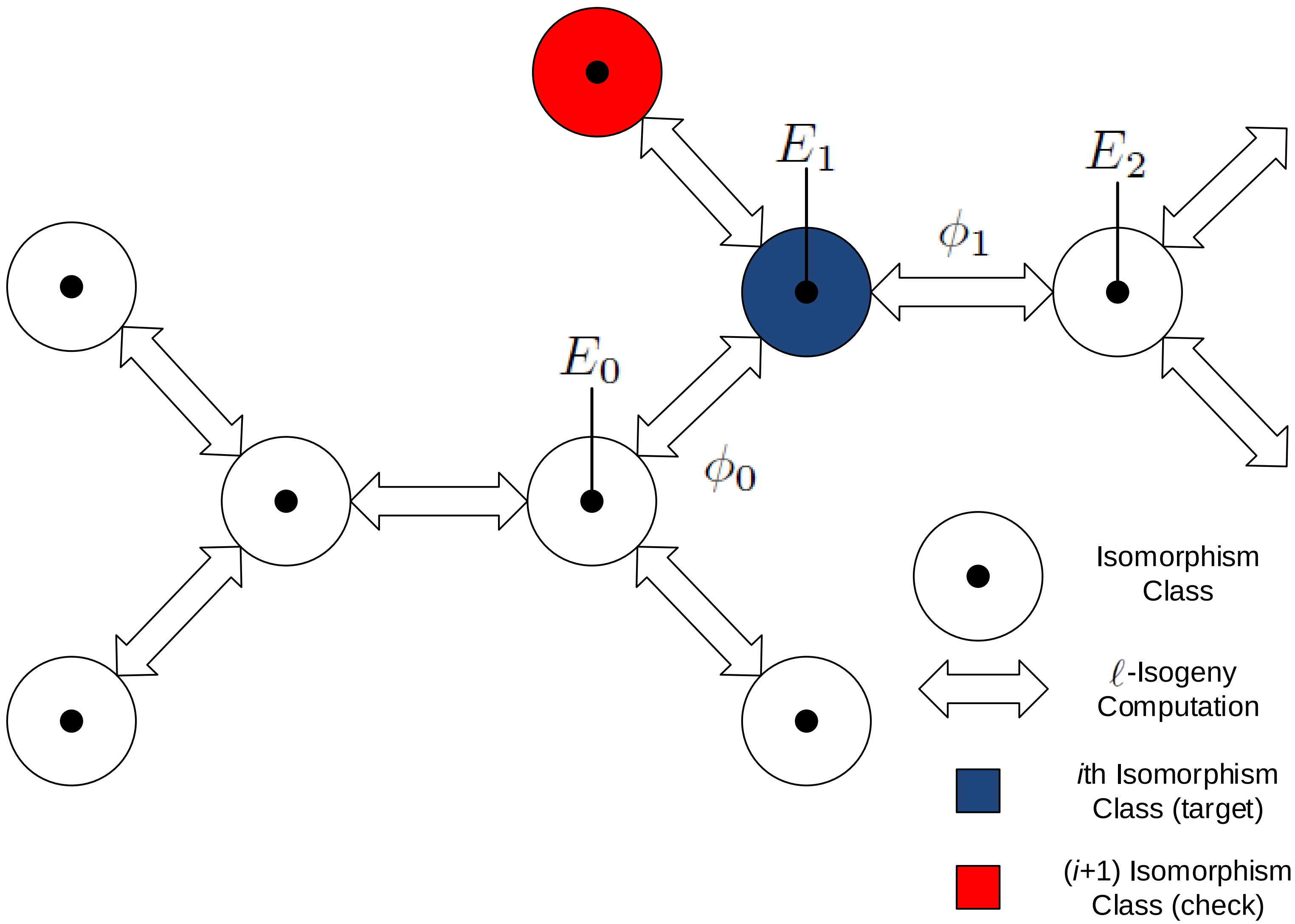
Attacking Iterative Isogeny Walks



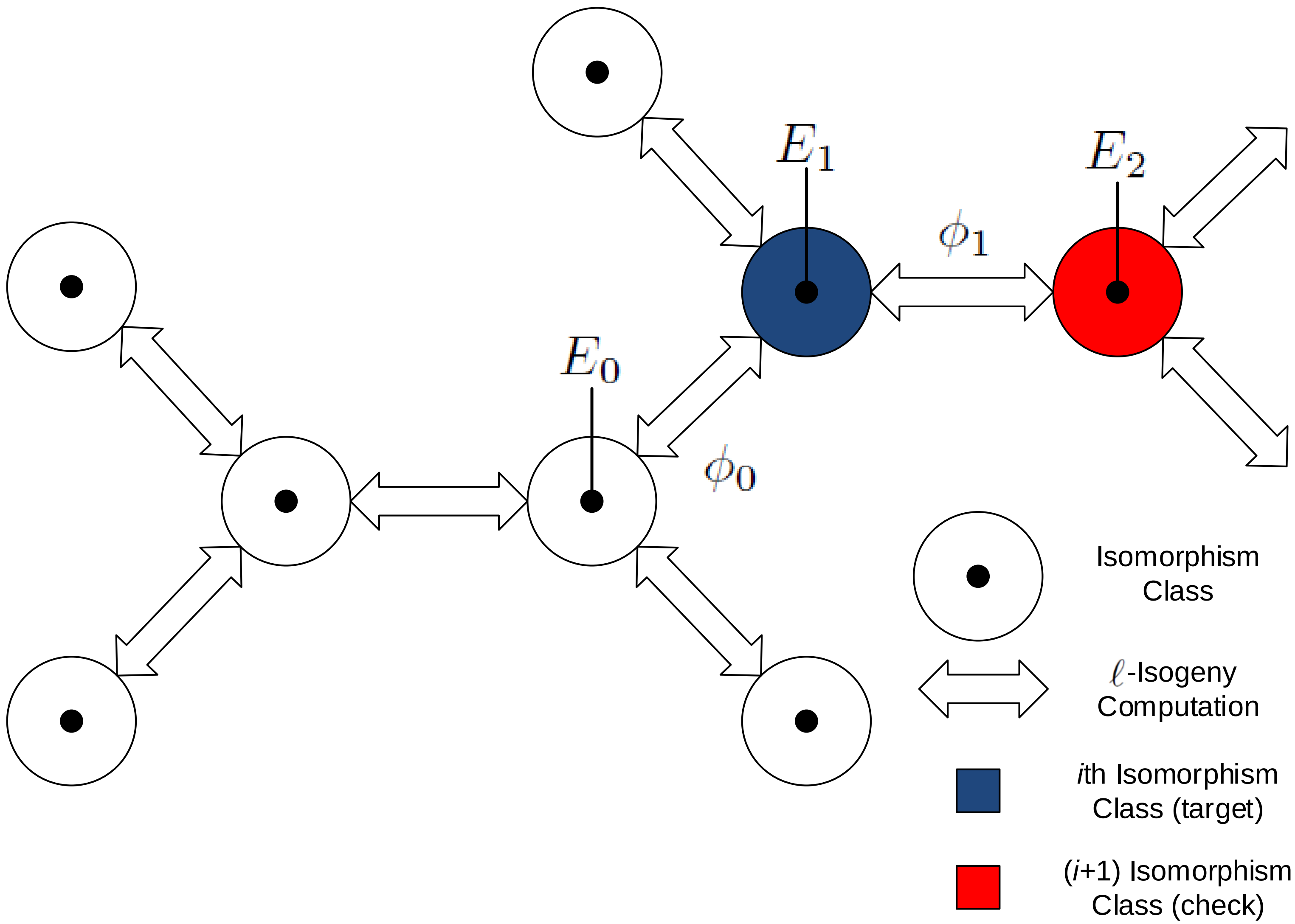
Attacking Iterative Isogeny Walks



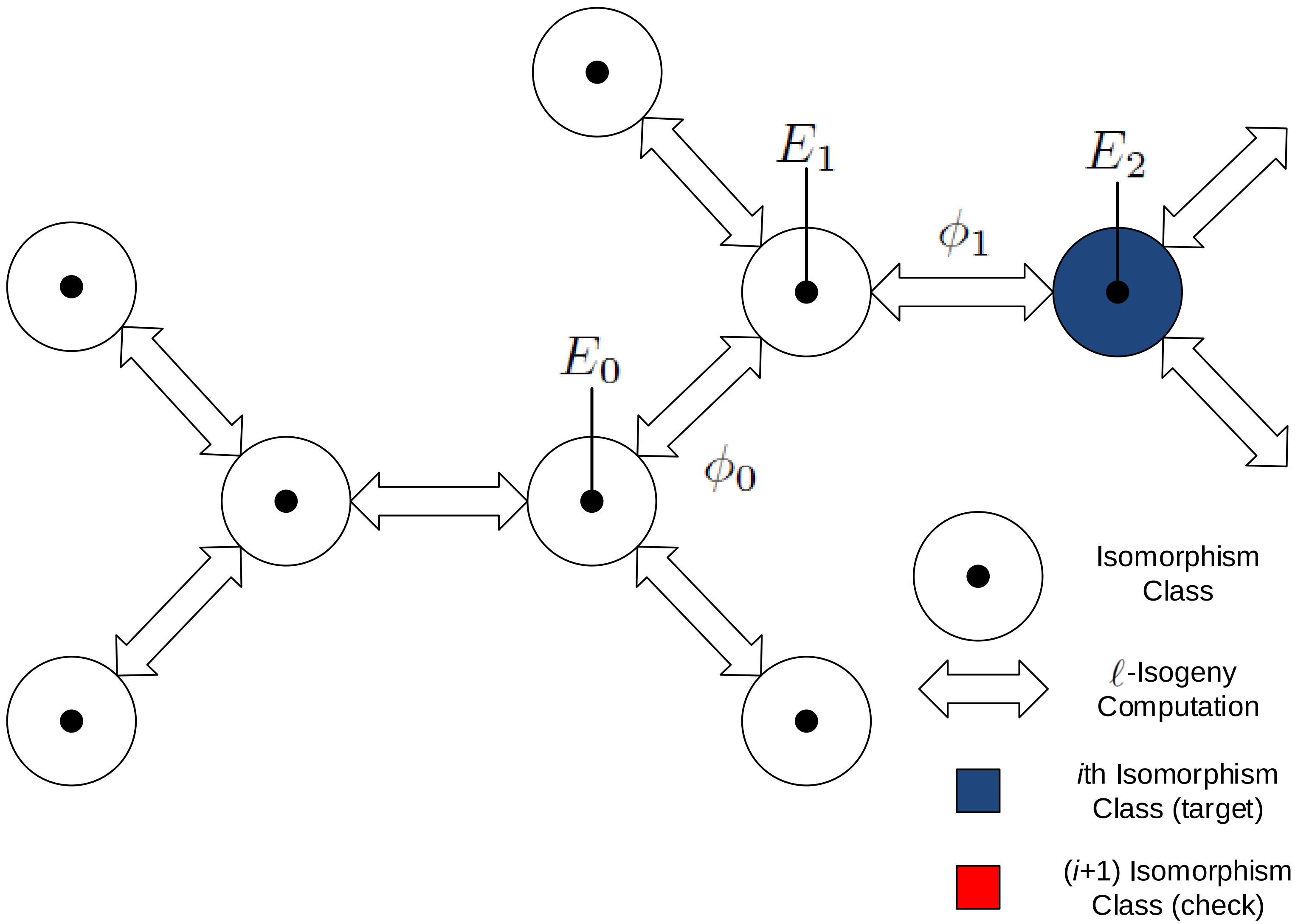
Attacking Iterative Isogeny Walks



Attacking Iterative Isogeny Walks



Attacking Iterative Isogeny Walks



Using RPA on Isogeny Walks

- Two types of RPA attacks on isogeny computations: zero-value coefficient or point attacks
- Zero-value isogeny coefficient attack
  - Force an isogeny to compute a curve with a full-zero coefficient ($A = 0$ or $B = 0$ for an elliptic curve)
  - Can be mounted against the second round of static-key SIDH
- Zero-value isogeny point attack
  - Force an isogeny to compute on a point with a zero-value ($x = 0$ or $y = 0$)
  - Can target torsion basis points in first round of SIDH or intermediate kernel point in either round
  - For SIDH, it is unlikely that a static-key user will accept any public parameters, but this may be possible for other isogeny-based cryptography schemes

RPA on SIDH Countermeasures

- Zero-value attack on large-degree isogeny requires knowledge of the nearby isogenous curves
- Countermeasure $\rightarrow$ Randomize the resulting isogenous curve
  - Dynamic keys
  - Random curve isomorphism
  - Initial isogeny of degree $\ell_r \neq \ell_A, \ell_B$

Conclusions

- Illustrated approaches to using zero-values on SIDH
- Proposed three RPA attacks on SIDH
  - Partial-zero attack on three-point differential ladder
  - Zero point attack on three-point differential ladder
  - Zero-value isogeny coefficient/point attack on large-degree isogeny computation
- These illustrate additional concerns for SIDH implementations, particularly ones using static keys
- Further analysis and demonstrations of such attacks are underway

Thank You!