# What is...Supersingular Elliptic Curve Cryptography?

A look at the evolving role of supersingular elliptic curves in cryptography

Sarah Arpin, University of Colorado Boulder

sarah.arpin@colorado.edu

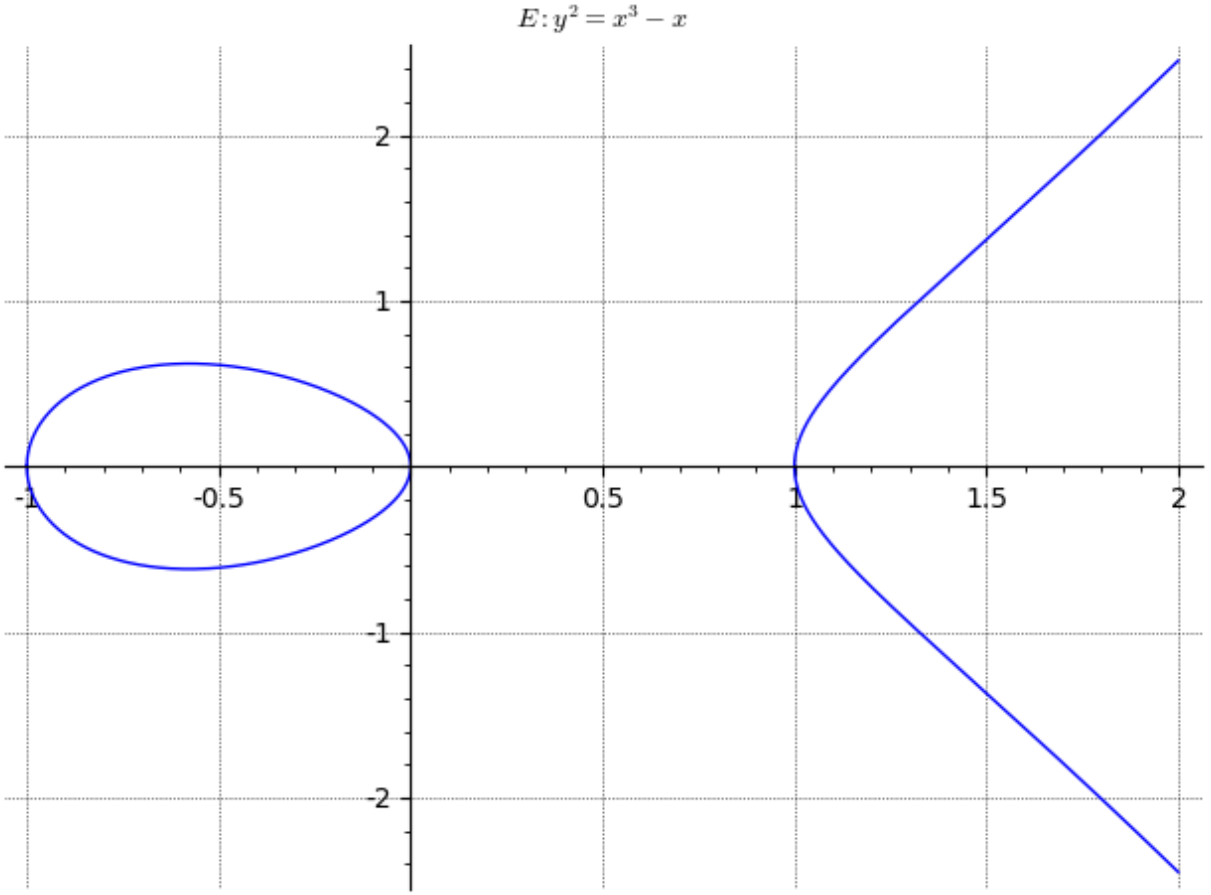
**What is... A Seminar?**

October 21st, 2021

# Table of Contents

# Elliptic Curves

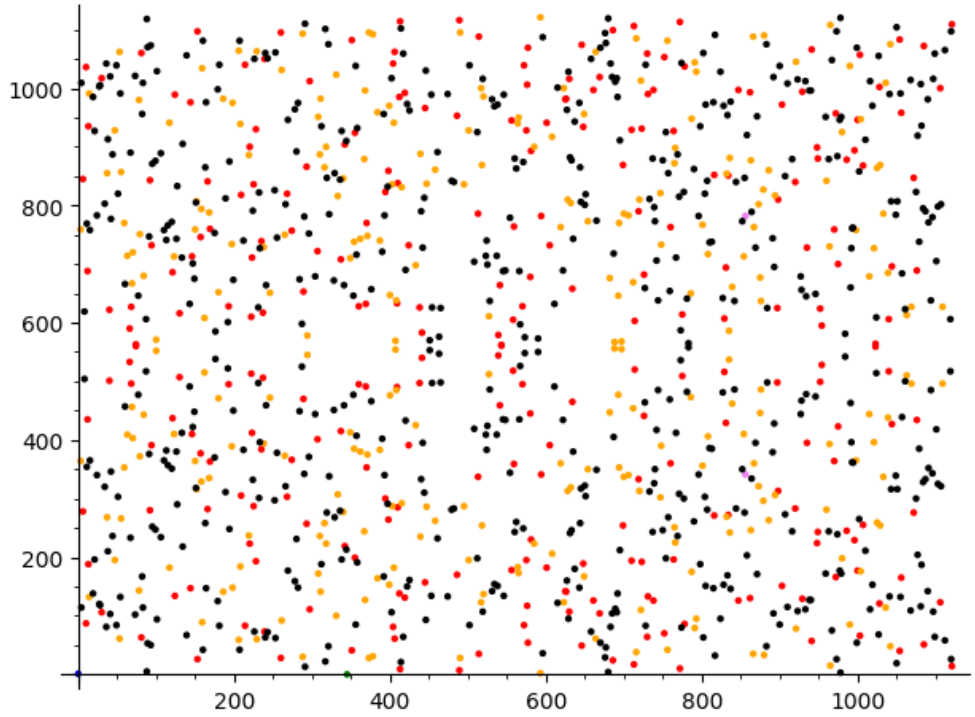
Every elliptic curve has an (affine) equation: $E : y^2 = x^3 + Ax + B$ (char $\neq 2, 3$). Isomorphism classes uniquely identified by $j = 1728\frac{4A^3}{4A^3+27B^2}$.




Points form a group under addition.

# Torsion Subgroups

The points of an elliptic curve form a group under addition.
Pictured below, the points of a supersingular elliptic curve over $\mathbb{F}_{1123}$:




Color specifies the order of the point in the group $E(\mathbb{F}_{1123})$:
Blue = 1, green = 2, violet = 4, red = 281, orange = 562, black = 1124.
$E(K)[N] :=$ points of $E$ defined over $K$ of order $N$
$E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

# Supersingular Elliptic Curves

**Definition (Chapter V[Sil09])**

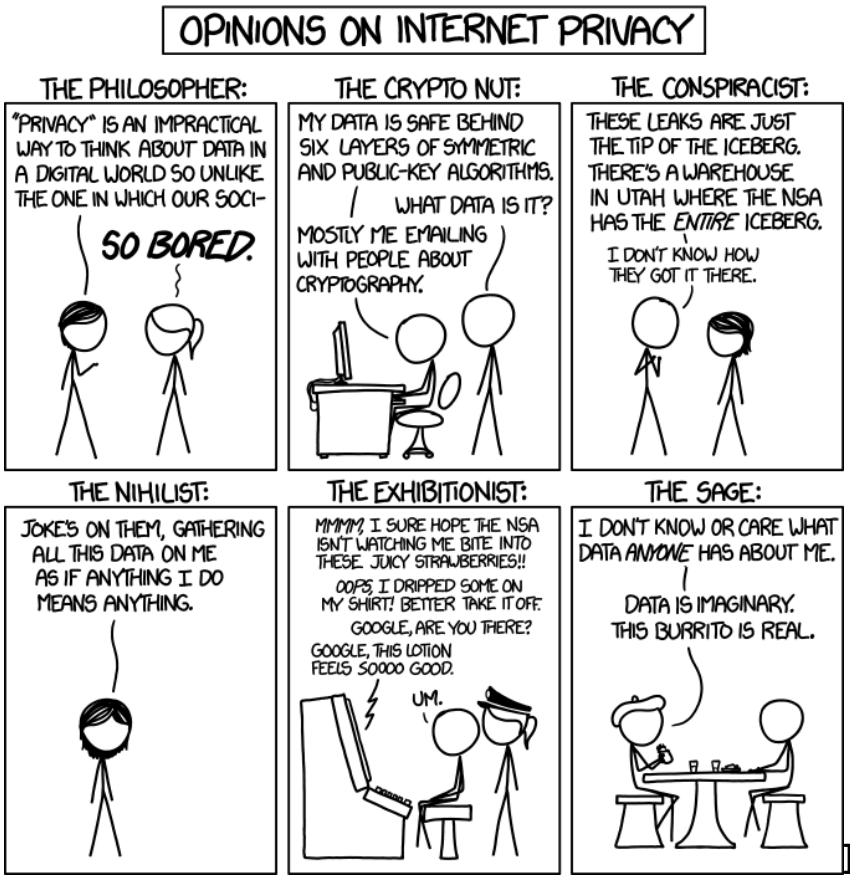
$E$: an elliptic curve defined over a field $K$ of characteristic $p \neq \infty$.
$E$ is **supersingular** iff $E(\overline{\mathbb{F}}_p)[p^r] = \mathcal{O}_E$ for all $r \geq 1$.

If $E/K$ with char(K)$= p \neq \infty$ is not supersingular, $E$ is **ordinary**.

For a given $p$, there are finitely many isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$.

# Axioms of Crypto for a Mathematician

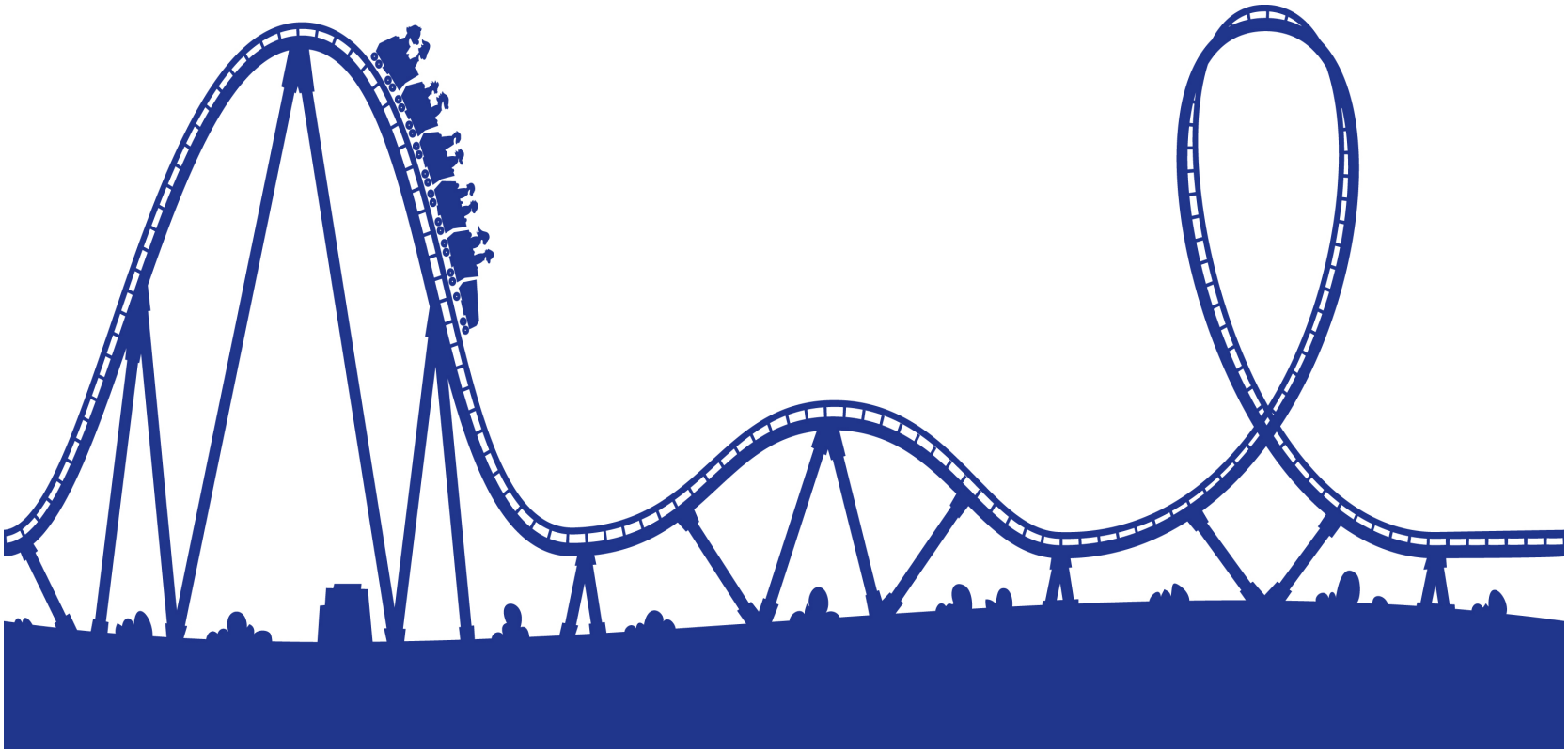
1. The goal is for two parties to obtain a shared secret through public communication.
2. The shared secret establishes a secure line of communication.
3. We are (I am) interested in algorithms for achieving (1).




https://xkcd.com/1269/

# The Trajectory of Supersingular Curves in Crypto

1. Discrete log problem for elliptic curves
2. Pairing-based cryptography (not covered here)
3. Isogeny-based cryptography



# Discrete Log Problem: Generally

$G$ : any group, with generator $g$.

**DLP: General**

Given $g^a$, $g^b$, determine $g^{ab}$.

Difficulty depends on the underlying group.

**Example: $G = (\mathbb{Z}/11\mathbb{Z})^\times$**

$G = \langle 2 \rangle$. Say $2^a = 3$, and $2^b = 4$. What is $2^{ab}$?

# Discrete Log Problem: Generally

$G$ : any group, with generator $g$.

**DLP: General**

Given $g^a$, $g^b$, determine $g^{ab}$.

Difficulty depends on the underlying group.

**Example: $G = (\mathbb{Z}/11\mathbb{Z})^\times$**

$G = \langle 2 \rangle$. Say $2^a = 3$, and $2^b = 4$. What is $2^{ab}$? $2^{ab} = 9$; $a = 8, b = 2$.

If $a$ and $b$ are computationally hard to find, the DLP is hard.

**DLP: Rephrased.**

Given $x \in G = \langle g \rangle$, find $a$ such that $g^a = x$.

# DLP on Elliptic Curves

Recall: The points of an elliptic curve form a group.
Let $[2]P := P + P$, $[3]P := P + P + P$, etc.
In the context of DLP, take $G = E(\mathbb{F}_q)$, $P \in E(\mathbb{F}_q)$ and ask:

**DLP: Hard Problem for Elliptic Curves**

Given $P$, $[a]P$, and $[b]P \in E(\mathbb{F}_q)$, compute $[ab]P$.

The best general classical attack is time exponential in $\log q$, so for large enough $q$ this is computationally hard...

# DLP on Elliptic Curves

Recall: The points of an elliptic curve form a group.
Let $[2]P := P + P$, $[3]P := P + P + P$, etc.
In the context of DLP, take $G = E(\mathbb{F}_q)$, $P \in E(\mathbb{F}_q)$ and ask:

**DLP: Hard Problem for Elliptic Curves**

Given $P$, $[a]P$, and $[b]P \in E(\mathbb{F}_q)$, compute $[ab]P$.

The best general classical attack is time exponential in $\log q$, so for large enough $q$ this is computationally hard...
...except for certain classes of supersingular elliptic curves.

# MOV Algorithm

[MOV93] The MOV Algorithm translates the Elliptic Curve DLP to a DLP in a related finite field.

## General curves:

*Algorithm 2:*

*Input:* An element $P \in E(F_q)$ of order $n$, and $R \in \langle P \rangle$.
*Output:* An integer $l$ such that $R = lP$.

1) Determine the smallest integer $k$ such that $E[n] \subseteq E(F_{q^k})$.
2) Find $Q \in E[n]$ such that $\alpha = e_n(P, Q)$ has order $n$.
3) Compute $\beta = e_n(R, Q)$.
4) Compute $l$, the discrete logarithm of $\beta$ to the base $\alpha$ in $F_{q^k}$.

In Table I, *k* is at most 6!

## Supersingular:

*Algorithm 3:*

*Input:* An element $P$ of order $n$ on a supersingular curve $E(F_q)$, and $R \in \langle P \rangle$.
*Output:* An integer $l$ such that $R = lP$.

1) Determine $k$ and $c$ from Table I.
2) Pick a random point $Q' \in E(F_{q^k})$ and SET $Q = (cn_1/n)Q'$.
3) Compute $\alpha = e_n(P, Q)$ and $\beta = e_n(R, Q)$.
4) Compute the discrete logarithm $l'$ of $\beta$ to the base $\alpha$ in $F_{q^k}$.
5) Check whether $l'P = R$. IF this is so, THEN $l = l'$ and we are done. Otherwise, the order of $\alpha$ must be less than $n$, so GO TO 2).

# Post-Quantum Cryptography

## Post-Quantum Cryptography

- NIST: 2015 call for proposals of post-quantum safe cryptography protocols. Now in Round 3.
- Supersingular Isogeny Graph Cryptography: $\sim$ 15 years old: original hash function by Charles-Goren-Lauter [**CGL06**]; SIKE key exchange [**SIKE**]
- CSIDH, OSIDH, SqiSign: more recent supersingular isogeny-based crypto protocols

## Hard Problems

- Path-finding in supersingular $\ell$-isogeny graph
- Path-finding with additional torsion point information

# Isogenies

**Definition**

An **isogeny** $\phi : E_1 \to E_2$ is a morphism between elliptic curves such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. It has a dual $\widehat{\phi} : E_2 \to E_1$.

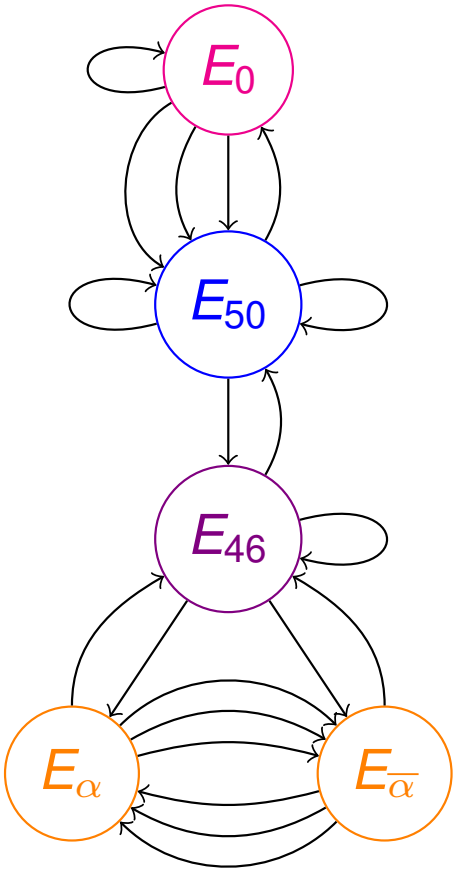
**Theorem (Corollary III.4.9 and Proposition III.4.12 [Sil09])**

*The kernel of a nonzero isogeny is a finite group. A given finite subgroup of points uniquely determines a separable isogeny.*

Supersingular elliptic curves over $\overline{\mathbb{F}}_p$ are all $\ell$-power isogenous.

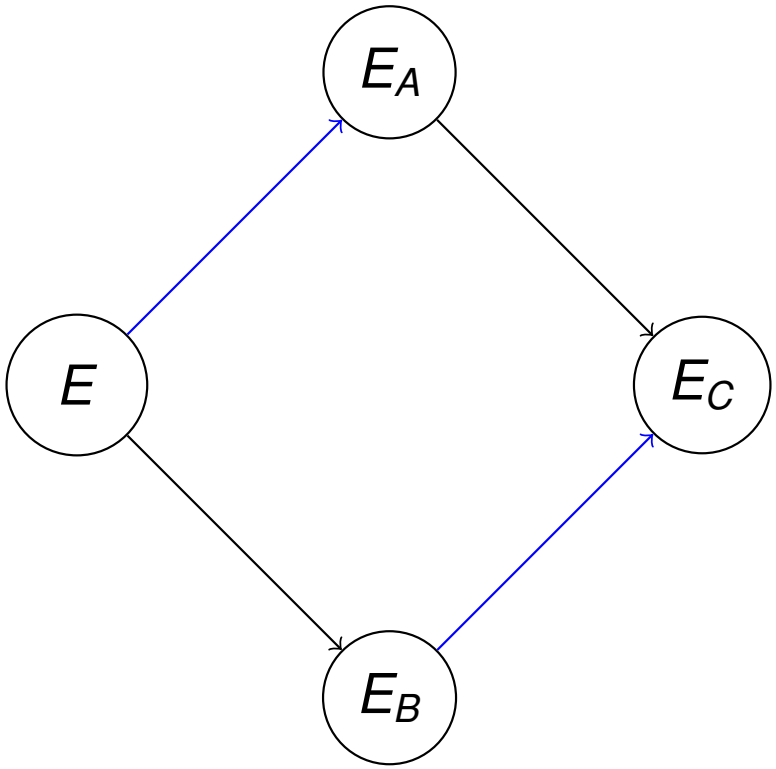
# Supersingular $\ell$-isogeny graph

$p = 53, \ell = 3$

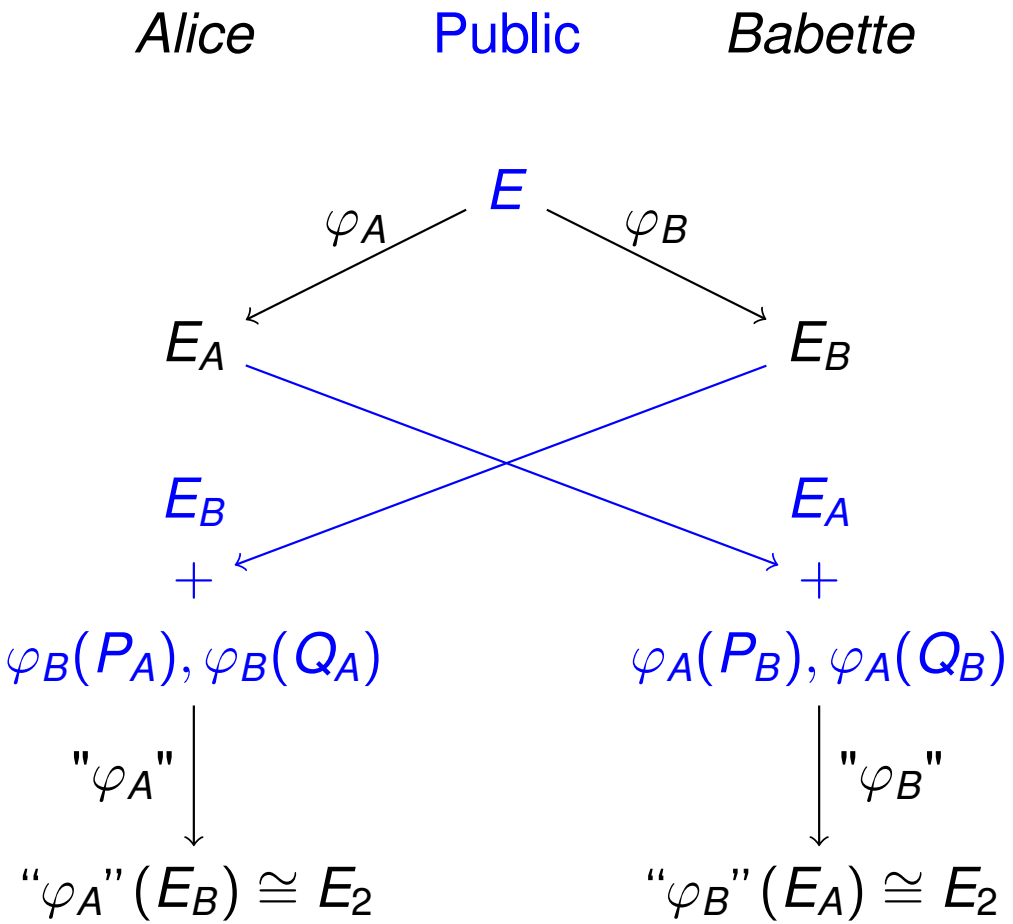



- With the right conditions on $p$, can be taken to be *undirected* by identifying isogenies with their duals
- Connected
- Out-degree $\ell + 1$
- $\sim \lfloor \frac{p}{12} \rfloor$ nodes
- $p$ is cryptographic size

# Diamonds



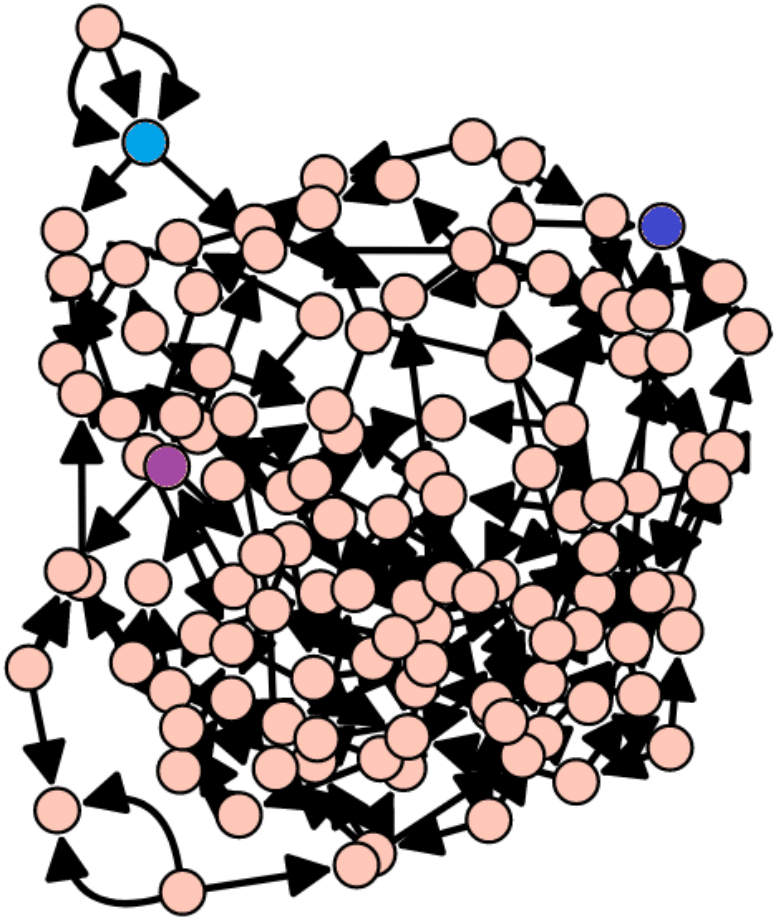
# Supersingular Isogeny Diffie-Hellman (SIKE)




$\varphi_A$ is degree $\ell_A^{e_A}$ and $\varphi_B$ is degree $\ell_B^{e_B}$
$E[\ell_A^{e_A}] = \langle P_A, Q_A \rangle$ and $E[\ell_B^{e_B}] = \langle P_B, Q_B \rangle$

# Hard Problems

1. Given $E_1$, $E_2$, find an $\ell^n$-isogeny between them.
2. Given $E$, $\varphi_A(E)$, and $\varphi_B(E)$, $\varphi_A(P_B)$, $\varphi_A(Q_B)$, $\varphi_B(P_A)$, and $\varphi_B(Q_A)$, find $\varphi_A(\varphi_B(E)) \cong \varphi_B(\varphi_A(E))$.



# How to study security?

Deuring Correspondence

- The supersingular $\ell$-isogeny graph has a relationship with the graph of maximal orders in a quaternion algebra.
- Relationships between underlying hard problems [Eis+18]. The path-finding problem is equivalent to computing the Deuring correspondence.
- The path-finding problem for quaternion algebras has been solved [Koh+14].

Graph Structure

- It is easier to path-find between $\mathbb{F}_p$ points of $\mathcal{G}_{p,\ell}$ [DG16]
- The structure of the subgraph of $\mathbb{F}_p$-points of $\mathcal{G}_{p,\ell}$ is known [Arp+19]
- Public torsion point information could be a weakness [Pet17] [Que+21]. More investigation is needed.

# Summary

- Supersingular curves have seen many ups and downs in cryptography.
- Continued research on these curves is needed and encouraged.
- For more references, see these slides by Steven Galbraith from the Conference on open questions in cryptography and number theory, UC Irvine, September 18,2018:
  `https://www.math.auckland.ac.nz/~sgal018/Silverberg.pdf`

# Thank You !

# Reference I


[Arp+19] Sarah Arpin et al. **Adventures in Supersingularland**. 2019. arXiv: 1909.07779 [math.NT].

[DG16] Christina Delfs and Steven D. Galbraith. "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$". In: **Des. Codes Cryptogr.** 78.2 (2016), pp. 425–440. ISSN: 0925-1022. DOI: 10.1007/s10623-014-0010-1.

[Eis+18] Kirsten Eisenträger et al. "Supersingular isogeny graphs and endomorphism rings: reductions and solutions". In: **Advances in cryptology—EUROCRYPT 2018. Part III**. Vol. 10822. Lecture Notes in Comput. Sci. Springer, Cham, 2018, pp. 329–368.

[Koh+14] David Kohel et al. "On the quaternion $\ell$-isogeny path problem". In: **LMS J. Comput. Math.** 17.suppl. A (2014), pp. 418–432. DOI: 10.1112/S1461157014000151.

# Reference II

[MOV93] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. “Reducing elliptic curve logarithms to logarithms in a finite field”. In: **IEEE Trans. Inform. Theory** 39.5 (1993), pp. 1639–1646. ISSN: 0018-9448. DOI: 10.1109/18.259647.

[Pet17] Christophe Petit. “Faster algorithms for isogeny problems using torsion point images”. In: **Advances in cryptology—ASIACRYPT 2017. Part II**. Vol. 10625. Lecture Notes in Comput. Sci. Springer, Cham, 2017, pp. 330–353. DOI: 10.1007/978-3-319-70697-9_12.

[Que+21] Victoria de Quehen et al. **Improved torsion point attacks on SIDH variants**. 2021. arXiv: 2005.14681 [math.NT].

[Sil09] Joseph H. Silverman. **The arithmetic of elliptic curves**. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.