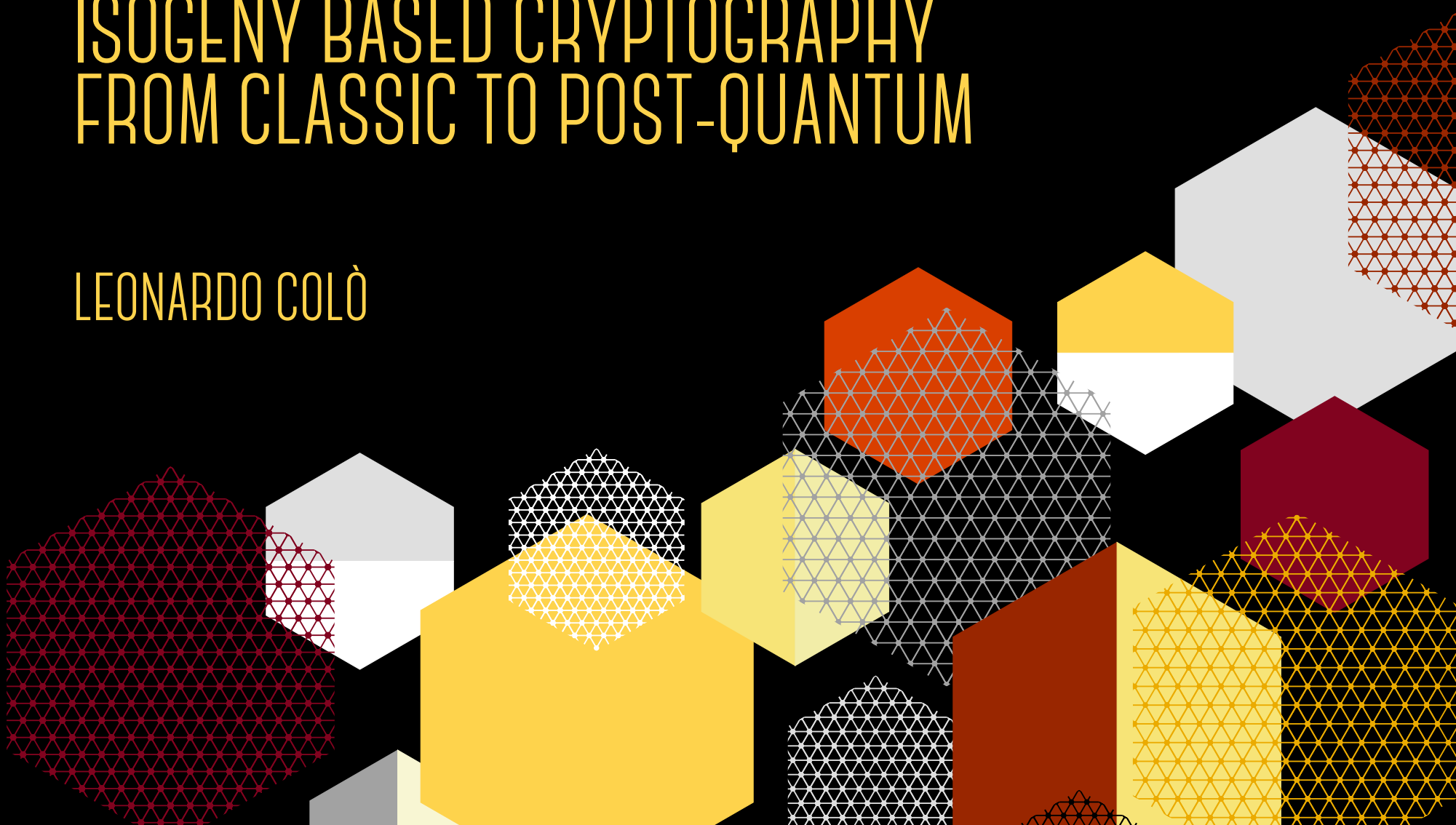
Toronto- 22 July, 2026

FIELDS INSTITUTE

UNIVERSITY OF WATERLOO

ISOGENY BASED CRYPTOGRAPHY FROM CLASSIC TO POST-QUANTUM

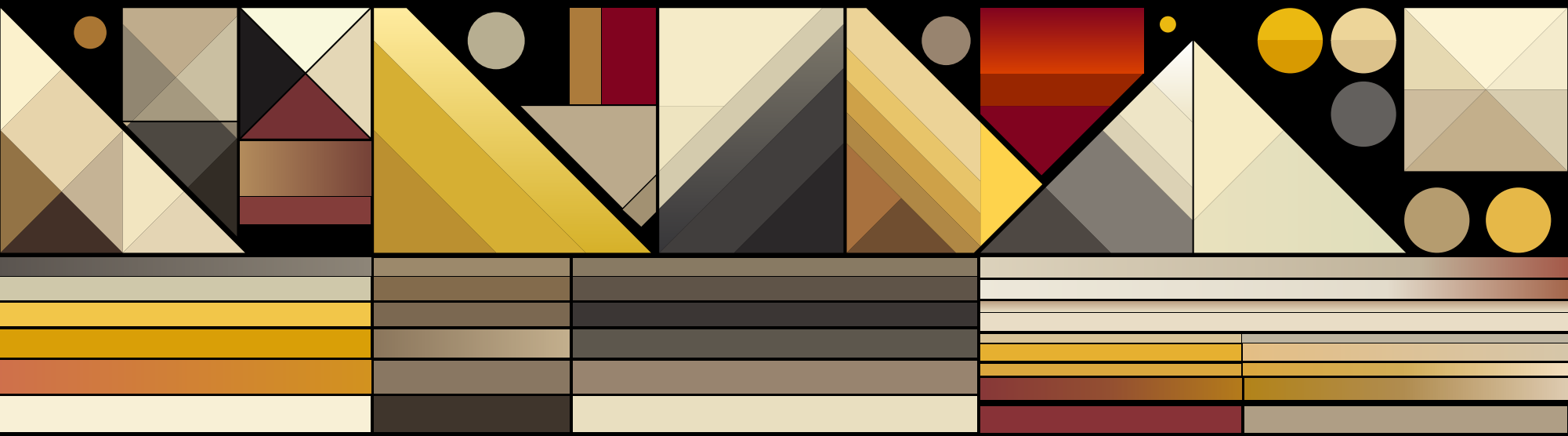
LEONARDO COLÒ



CONTENTS

- Isogenies and Isogeny Graphs
- Cryptographic Hard Problems
- From CGL to CSIDH
- Signatures
- Kani Constructions and PEGASIS

ELLIPTIC CURVES & ISOGENY GRAPHS

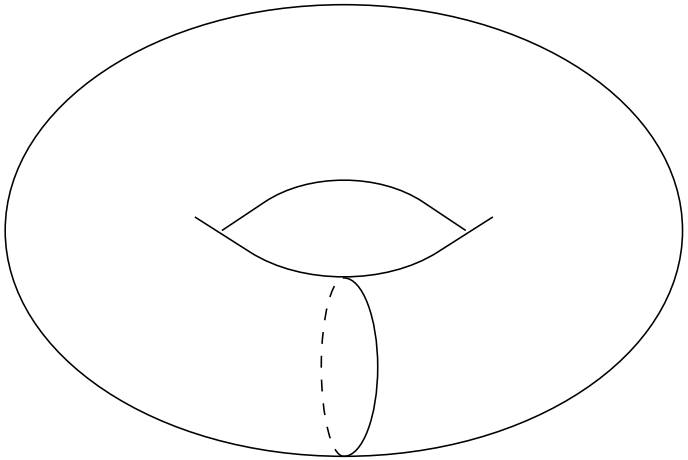


Definition

Let k be a field of characteristic $\neq 2, 3$. An elliptic curve E defined over k is a smooth projective curve of genus 1 defined by a Weierstrass equation

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $a, b \in k$ are such that $4a^3 + 27b^2 \neq 0$.



In general we work with the affine equation of E, i.e., $E : y^2 = x^3 + ax + b$ together with the distinguished point $O = (0 : 1 : 0)$ (said to be the *point at infinity*).

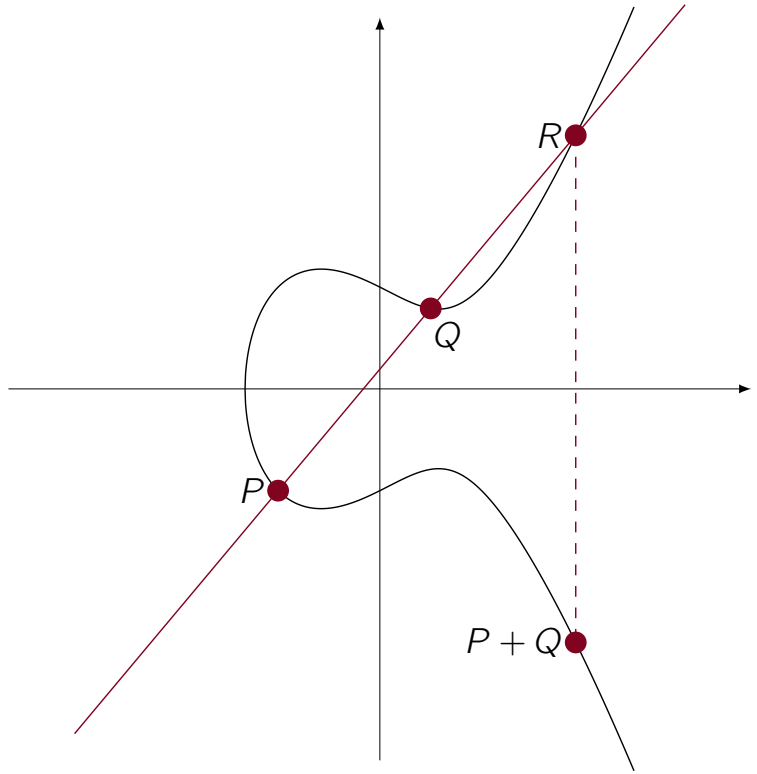
ELLIPTIC CURVES - GROUP LAW

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a group law such that any three colinear points add up to zero.

- The law is algebraic (it has formulas);
- The law is commutative;
- $O = (0 : 1 : 0)$ is the group identity;
- Opposite points have the same x -value.



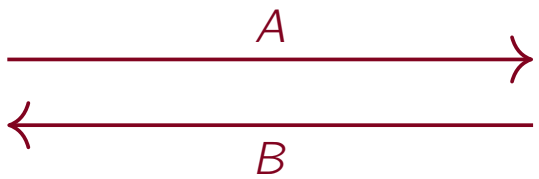
ELLIPTIC CURVES - WHY DO WE CARE?

L.COLÒ UWAT

Goal: Alice and Bob have never met before. They communicate over a public channel and want to agree on a shared secret.

Setup: They agree on an elliptic curve $E/\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$ of large prime order n.

Alice	**Bob**
Pick a random $a \in \mathbb{Z}/n\mathbb{Z}$	Pick a random $b \in \mathbb{Z}/n\mathbb{Z}$
compute $A = [a]P$	compute $B = [b]P$



Shared secret is $[ab]P$

BRIEF HISTORY OF DH KEY EXCHANGE

L.COLÒ UWAT

1976 Diffie and Hellman publish *New Directions in Cryptography*, and suggest using $G = \mathbb{F}_p^*$.

1978 Pollard publishes his discrete logarithm algorithm, with complexity $O\left(\sqrt{\#G}\right)$.

1985 Miller and Koblitz independently suggest using elliptic curves, $G = E(\mathbb{F}_p)$.

1994 Shor publishes his quantum polynomial-time discrete logarithm and factoring algorithm.

2005 The NSA standardizes elliptic-curve key agreement (ECDH) and elliptic-curve signatures (ECDSA).

2017 Approximately 70% of web traffic is secured by ECDH and/or ECDSA.

2017 NIST launches its post-quantum cryptography standardization process and advises against beginning a new migration to elliptic-curve cryptography.

Isomorphisms

The only invertible algebraic maps between elliptic curves are of the form

$$(x, y) \longmapsto \left(u^2 x, u^3 y\right),$$

for some $u \in \overline{k}^*$.
They are group isomorphisms.

j-invariant

Let $E : y^2 = x^3 + ax + b$. The *j-invariant* of E is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Two elliptic curves E and E' are isomorphic over $\overline{k}$ if and only if $j(E) = j(E')$.

Torsion structure

Let E be defined over an algebraically closed field $\overline{k}$ of characteristic p.
If $p \nmid m$, then

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

For powers of the characteristic,

$$E[p^e] \simeq \begin{cases} \mathbb{Z}/p^e\mathbb{Z}, & \text{if } E \text{ is ordinary,} \\ \{O\}, & \text{if } E \text{ is supersingular.} \end{cases}$$

Finite fields: Hasse's theorem

Let E be defined over a finite field $\mathbb{F}_q$. Then

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

ELLIPTIC CURVES - WHAT IS AN ISOGENY?

L.COLÒ UWAT

$$\begin{aligned} \phi : E &\longrightarrow E' \\ P &\longmapsto \phi(P). \end{aligned}$$

An *isogeny* is a map between elliptic curves that is

- a morphism of algebraic curves;
- a group homomorphism;
- nonconstant;
- surjective over the algebraic closure;
- given by rational functions.

Kernel and degree

The kernel of an isogeny is finite. If ϕ is separable, then

$$\deg(\phi) = \#\ker(\phi).$$

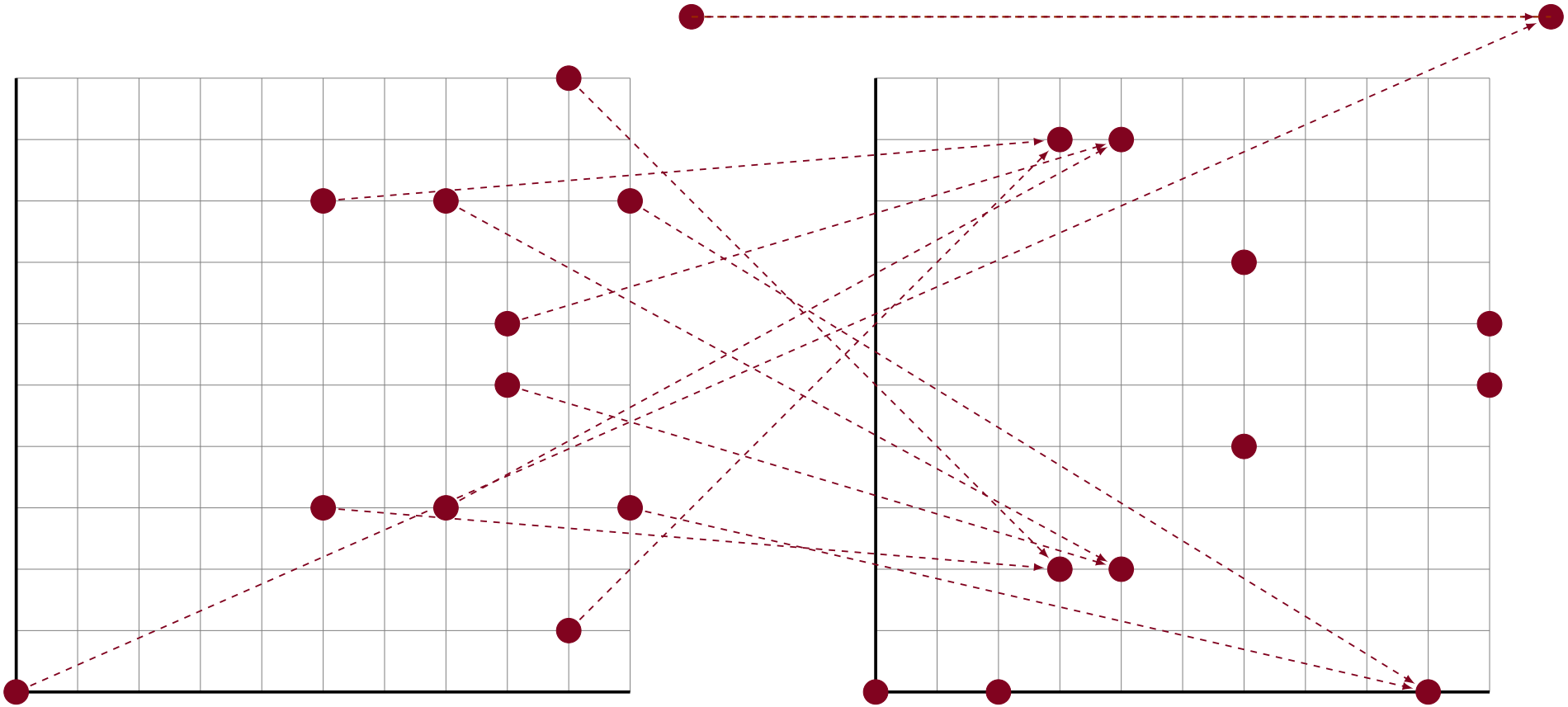
Conversely, every finite subgroup $H \subseteq E(\overline{k})$ determines, up to isomorphism, a separable isogeny $\phi : E \longrightarrow E/H$ with kernel H.

ISOGENIES - AN EXAMPLE

Over $\mathbb{F}_{11}$, we consider the isogeny

$$\psi : E : y^2 = x^3 + x \longrightarrow F : y^2 = x^3 - 4x$$

$$(x, y) \longmapsto \left(\frac{x^2 + 1}{x}, y \frac{x^2 - 1}{x^2} \right)$$



ISOGENIES - PROPERTIES

Let $\phi : E \longrightarrow E'$ be an isogeny defined over a field k of characteristic p.

- $k(E)$ is the field of rational functions on E defined over k;
- $\phi^* k(E')$ is the subfield of $k(E)$ defined by

$$\phi^* k(E') = \{f \circ \phi \mid f \in k(E')\}.$$

Degree and separability

- The degree of ϕ is $\deg(\phi) = [k(E) : \phi^* k(E')]$. It is always finite.
- The isogeny ϕ is called *separable*, *inseparable*, or *purely inseparable* according to whether the corresponding extension of function fields has that property.
- If ϕ is separable, then $\deg(\phi) = \#\ker(\phi)$.
- Every isogeny $\phi : E \to E'$ has a unique dual isogeny $\widehat{\phi} : E' \to E$ satisfying

$$\widehat{\phi} \circ \phi = [\deg(\phi)]_E, \qquad \phi \circ \widehat{\phi} = [\deg(\phi)]_{E'}.$$

ISOGENY GRAPHS

L.COLÒ UWAT

Definition

Given an elliptic curve E over k, and a finite set of primes S, we can associate an isogeny graph $G_S(E)$

- whose vertices are elliptic curves isogenous to E over $\bar{k}$, and
- whose edges are isogenies of degree $\ell \in S$.

If $S = \{\ell\}$, then we write $G_\ell(E)$, the ℓ-isogeny graph.

The vertices are defined up to $\bar{k}$-isomorphism and the edges from a given vertex are defined up to a $\bar{k}$-isomorphism of the codomain.

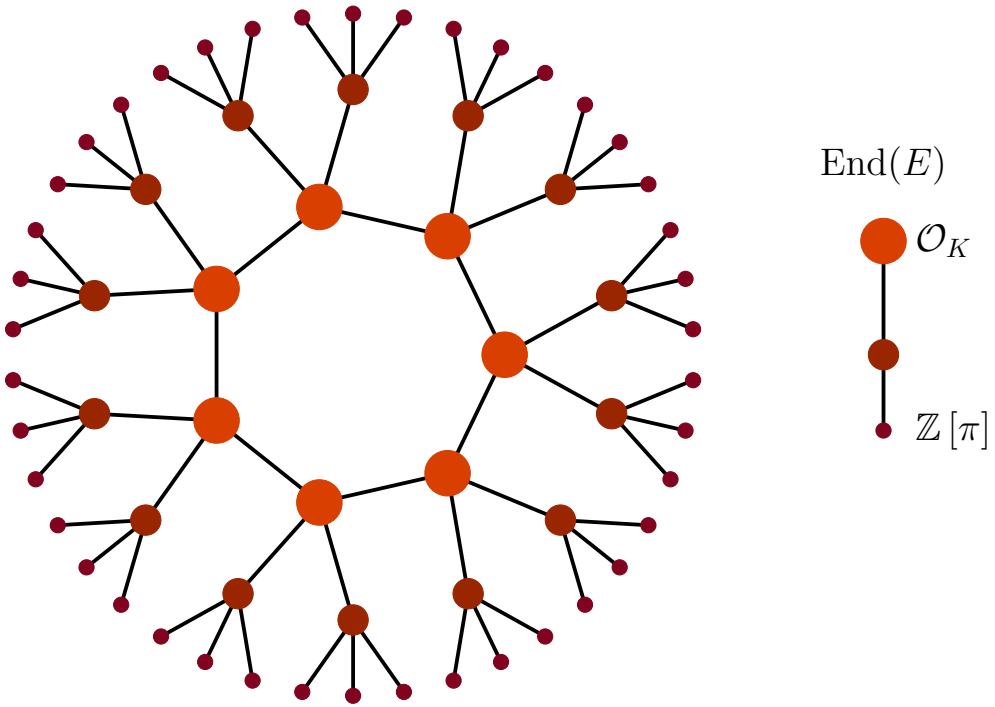
The ℓ-isogeny graph of E is $(\ell + 1)$-regular (as a directed multigraph).

ORDINARY ISOGENY GRAPHS: VOLCANOES

Let $\mathrm{End}(E) = \mathcal{O} \subseteq K$, an imaginary quadratic field. The class group $\mathrm{Cl}(\mathcal{O})$ acts faithfully and transitively on the set of elliptic curves with endomorphism ring $\mathcal{O}$:

$$E \longrightarrow E/E[\mathfrak{a}] \qquad E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \ \forall \alpha \in \mathfrak{a}\}$$

Thus, the CM isogeny graphs can be modelled by an equivalent category of fractional ideals of K.

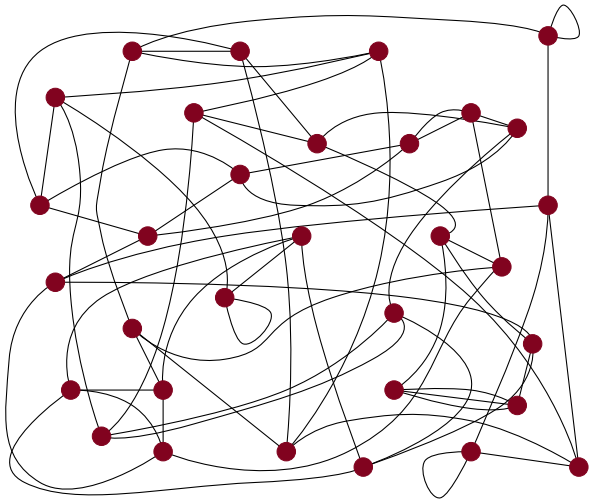


SUPERSINGULAR ISOGENY GRAPHS

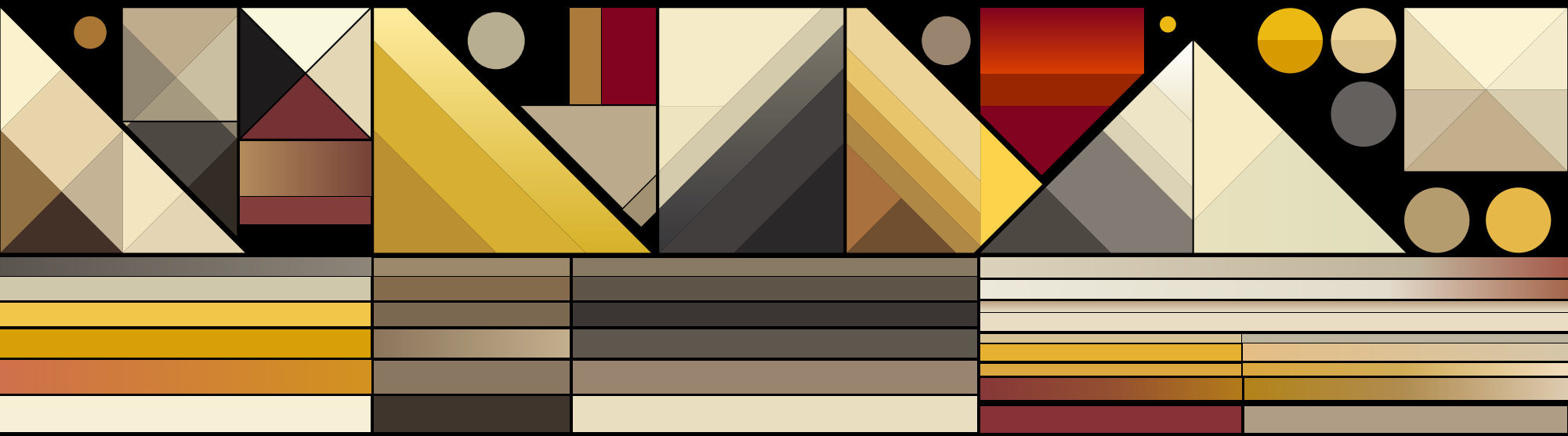
The supersingular isogeny graphs are remarkable because the vertex sets are finite : there are $(p+1)/12+\epsilon_p$ curves. Moreover

- every supersingular elliptic curve can be defined over $\mathbb{F}_{p^2}$;
- all ℓ-isogenies are defined over $\mathbb{F}_{p^2}$;
- every endomorphism of E is defined over $\mathbb{F}_{p^2}$.

The lack of a commutative group acting on the set of supersingular elliptic curves/$\mathbb{F}_{p^2}$ makes the isogeny graph more complicated.



HARD PROBLEMS



Supersingular Isogeny Problem

Given two supersingular elliptic curves $E, E'/\mathbb{F}_{p^2}$ known to be isogenous, compute an isogeny $\phi : E \longrightarrow E'$.

Equivalently, given two vertices in a supersingular isogeny graph, find a path connecting them.

$$E = E_0 \xrightarrow{\ell} E_1 \xrightarrow{\ell} \cdots \xrightarrow{\ell} E_r = E'.$$

- Computing the endpoint of a known path is efficient;
- recovering a path from its endpoints appears difficult;
- different protocols reveal different auxiliary information, leading to different versions of the problem.

HARD PROBLEMS - COLLISION AND PATH FINDING

L.COLÒ UWAT

Fix a small prime ℓ and consider the supersingular ℓ-isogeny graph.

Path-finding problem

Given supersingular elliptic curves E and E', find a chain of ℓ-isogenies connecting them.

Collision problem

Given a starting curve E_0, find two distinct paths

$$\phi_1, \phi_2 : E_0 \longrightarrow E'$$

that end at isomorphic curves.

These problems underlie the intuition behind isogeny-based hash functions:

- Preimage resistance corresponds to recovering a path;
- collision resistance corresponds to finding two walks with the same endpoint.

Endomorphism Ring Problem

Given a supersingular elliptic curve E, compute a basis for

$$\mathsf{End}(E).$$

One-Endomorphism Problem

Given E, compute a non-scalar endomorphism

$$\alpha \in \mathsf{End}(E) \setminus \mathbb{Z}.$$

These problems are closely related to supersingular isogeny path finding:

$$\text{isogenies} \quad \longleftrightarrow \quad \text{quaternion ideals}.$$

DEURING CORRESPONDENCE

- Fix a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$.
- Let $\mathcal{O}_0 := \mathsf{End}(E_0)$ and identify $B_{p,\infty} = \mathcal{O}_0 \otimes_{\mathbb{Z}} \mathbb{Q}$.

Theorem

The contravariant functor

$$E \longmapsto \mathsf{Hom}(E, E_0)$$

defines an equivalence of categories between

- supersingular elliptic curves with isogenies;
- invertible left $\mathcal{O}_0$-modules with nonzero left $\mathcal{O}_0$-module homomorphisms.

Deuring correspondence

Isomorphism classes of supersingular elliptic curves are in bijection with the left ideal class set $\mathsf{Cl}_L(\mathcal{O}_0)$.

QUATERNION ALGEBRAS - IDEALS AND ISOGENIES

L.COLÒ UWAT

A fundamental consequence of the Deuring correspondence is that

Isogenies from E_0 correspond to left ideals of $\mathcal{O}_0$.

- Given an isogeny $\psi : E_0 \longrightarrow E$, the associated left $\mathcal{O}_0$-ideal is

$$I_\psi = \mathsf{Hom}(E, E_0)\psi = \{\alpha \circ \psi \mid \alpha \in \mathsf{Hom}(E, E_0)\}.$$

- Conversely, a left $\mathcal{O}_0$-ideal I determines an isogeny $\phi_I : E_0 \longrightarrow E_I$ whose kernel is

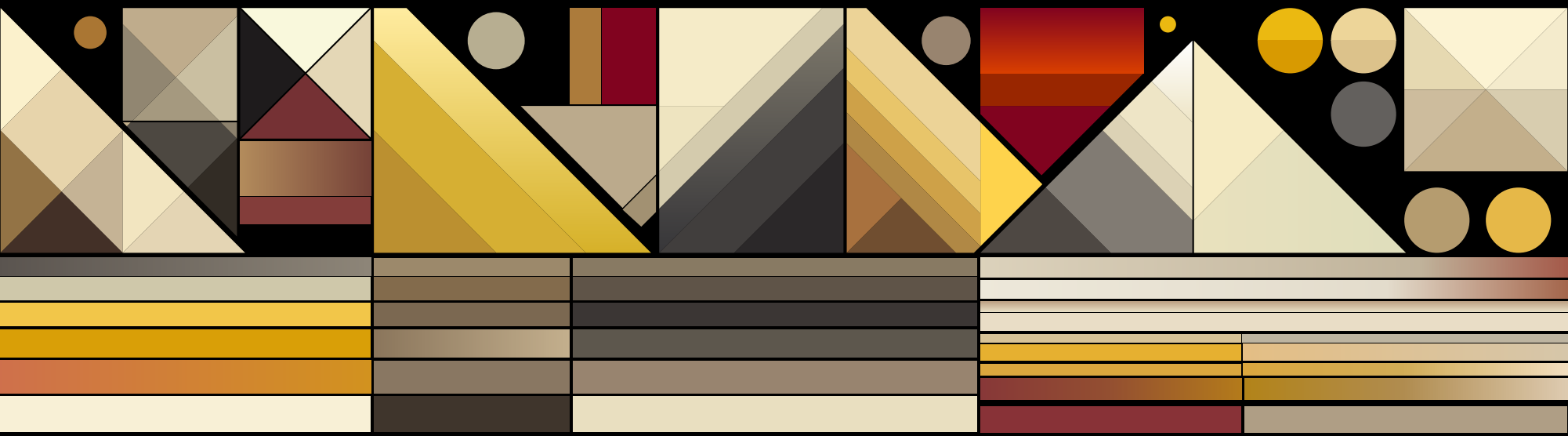
$$E_0[I] := \bigcap_{\alpha \in I} \ker(\alpha).$$

The right order

The endomorphism ring of the codomain is identified with the right order of I:

$$\mathsf{End}(E_I) \simeq \mathcal{O}_R(I) := \{\alpha \in B_{p,\infty} \mid I\alpha \subseteq I\}.$$

HASH FUNCTIONS & KEY EXCHANGES

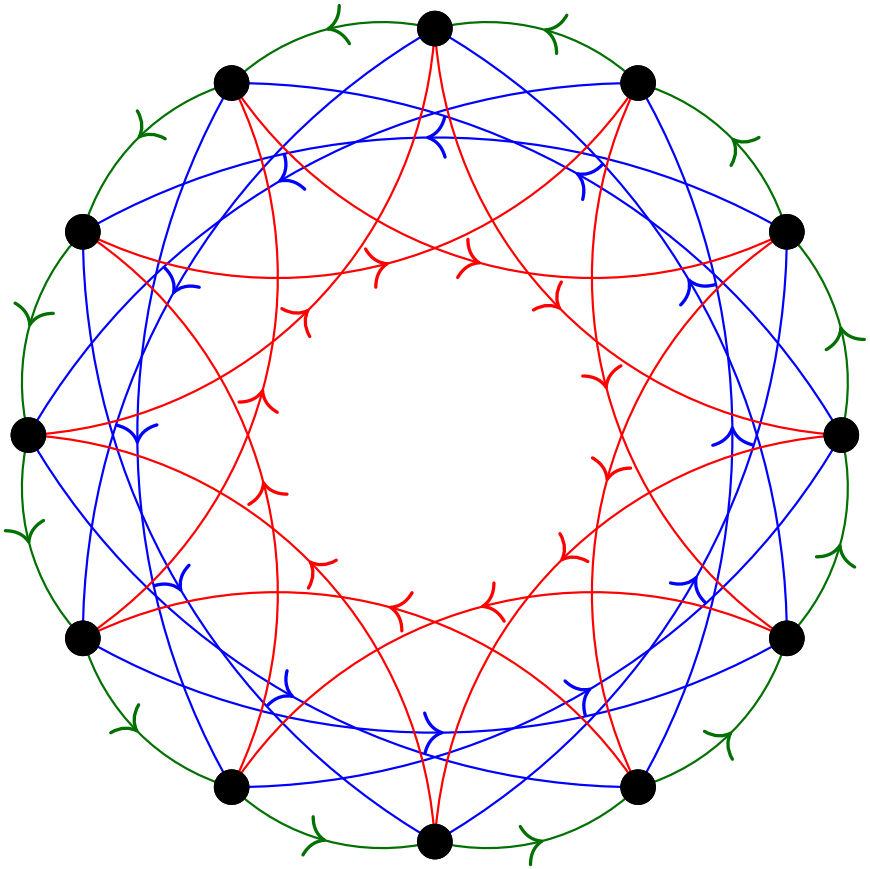


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$

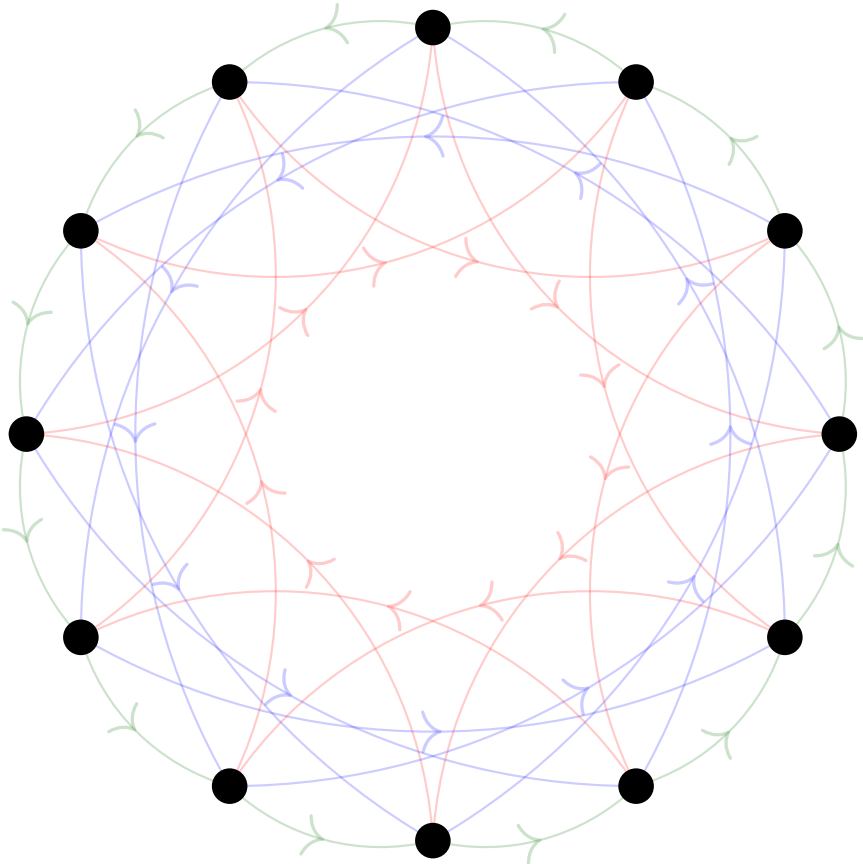


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$

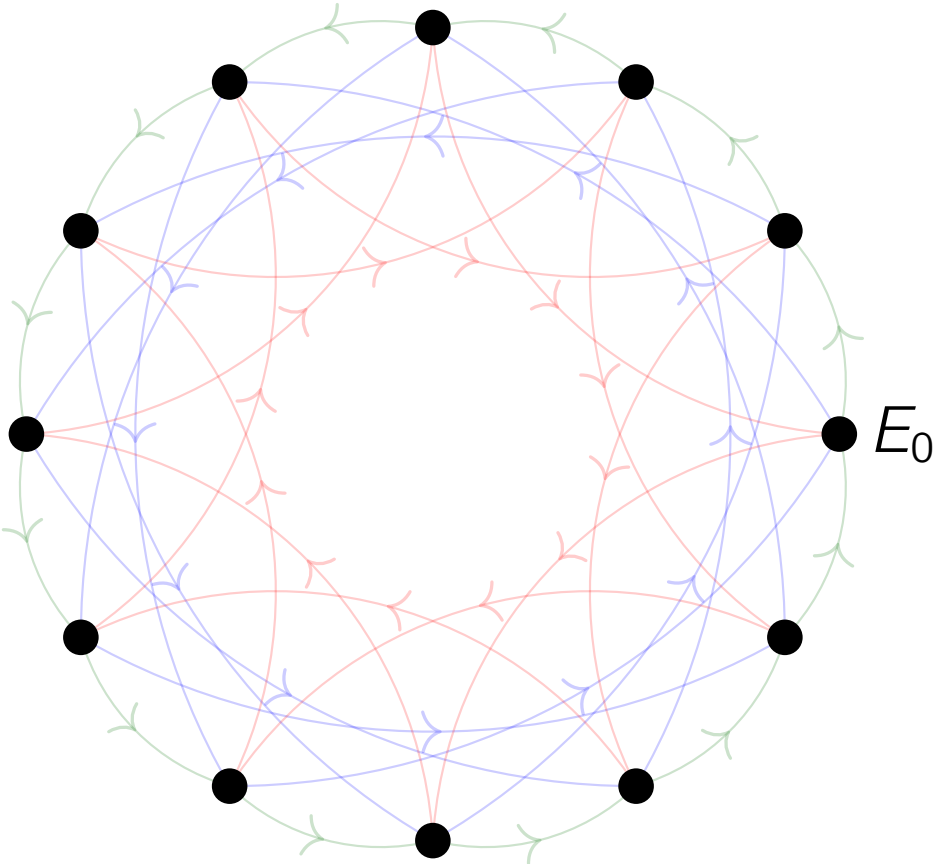


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

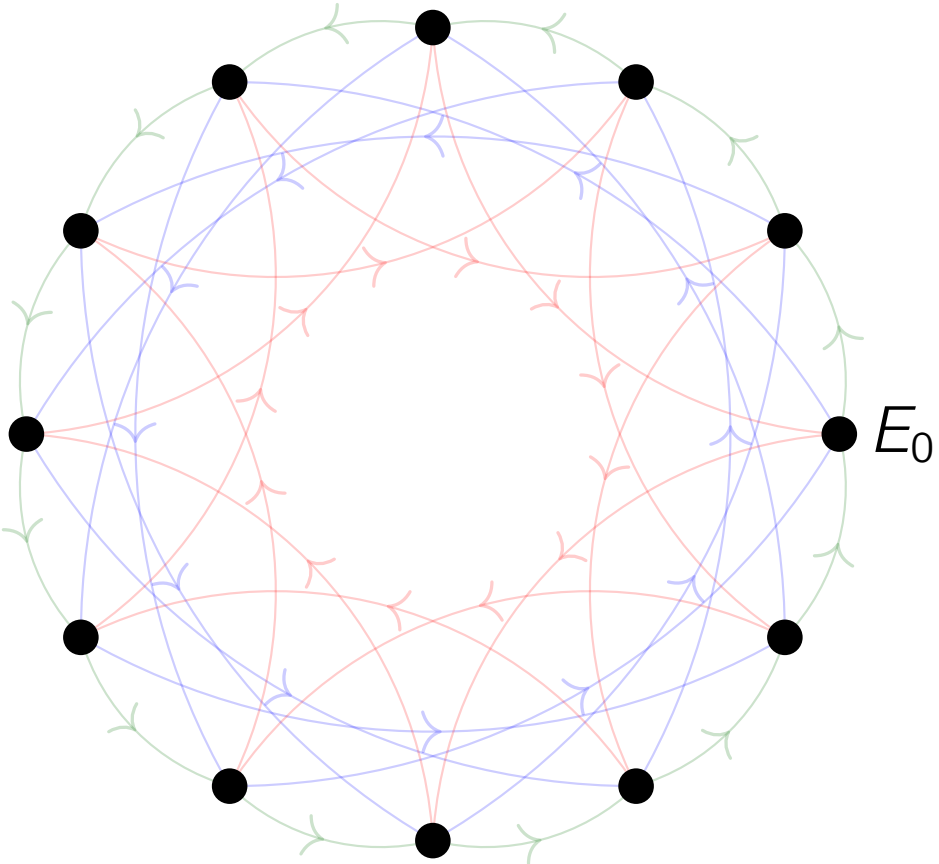
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

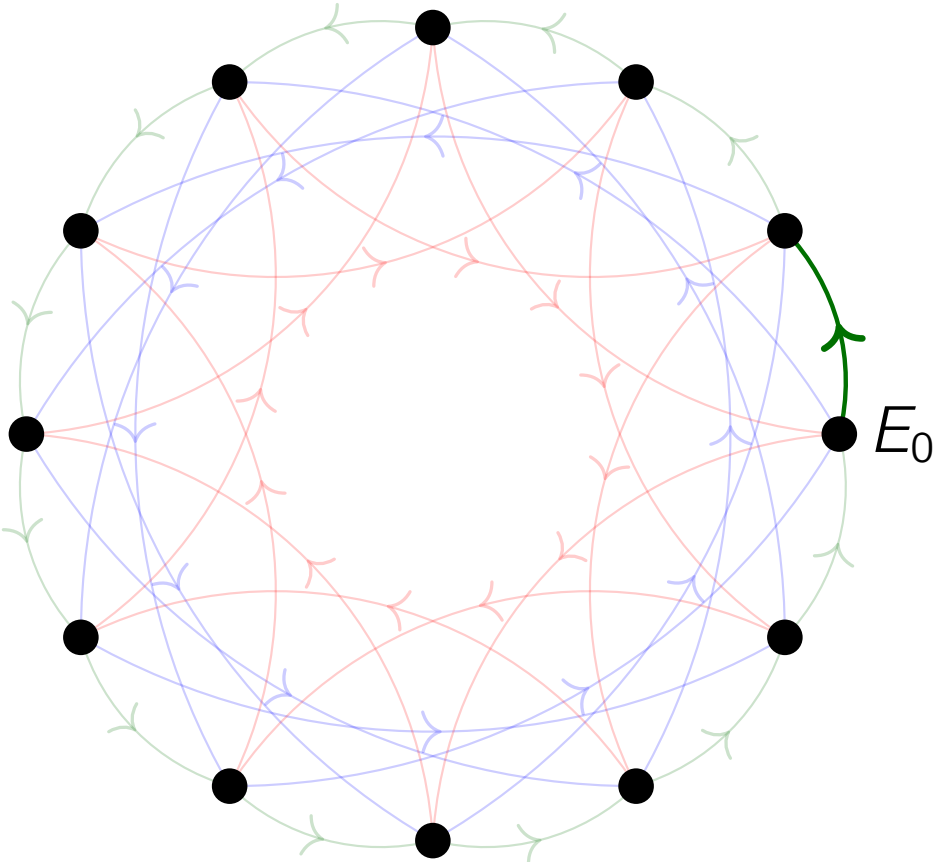
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

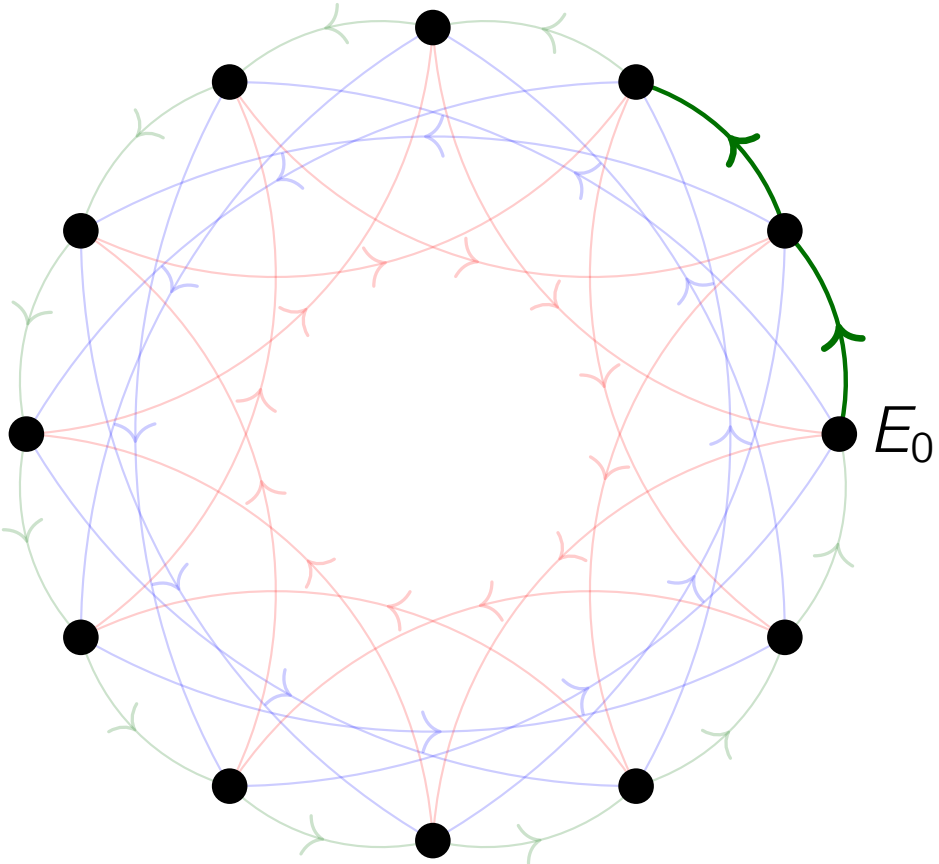
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

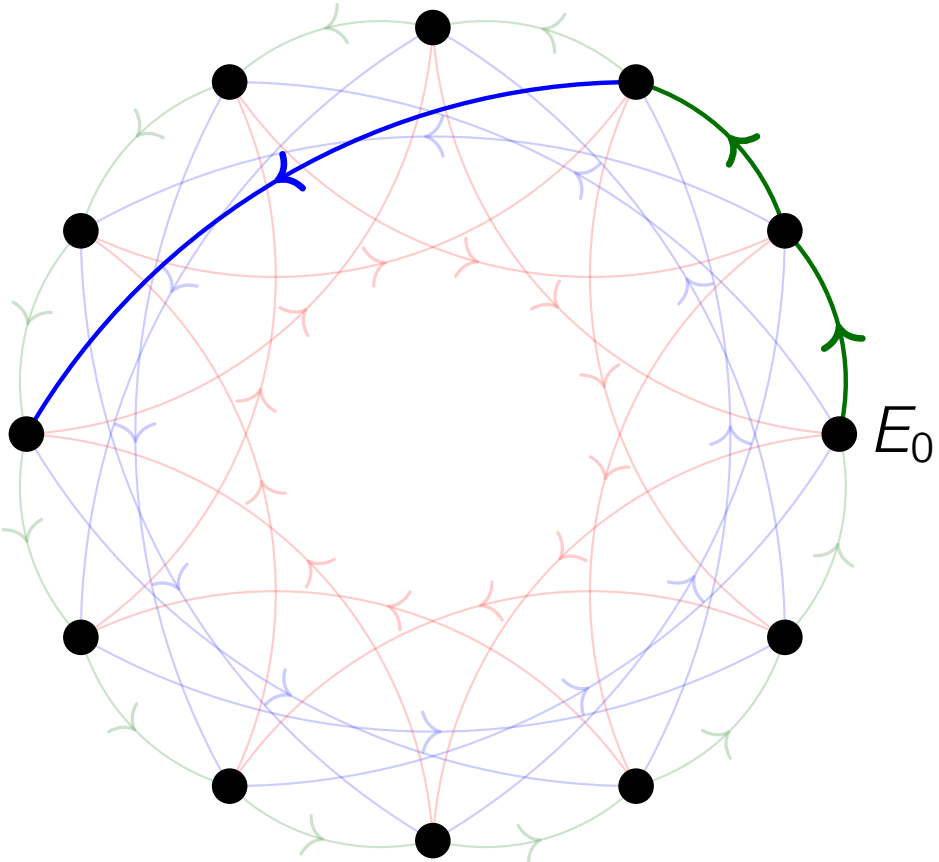
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

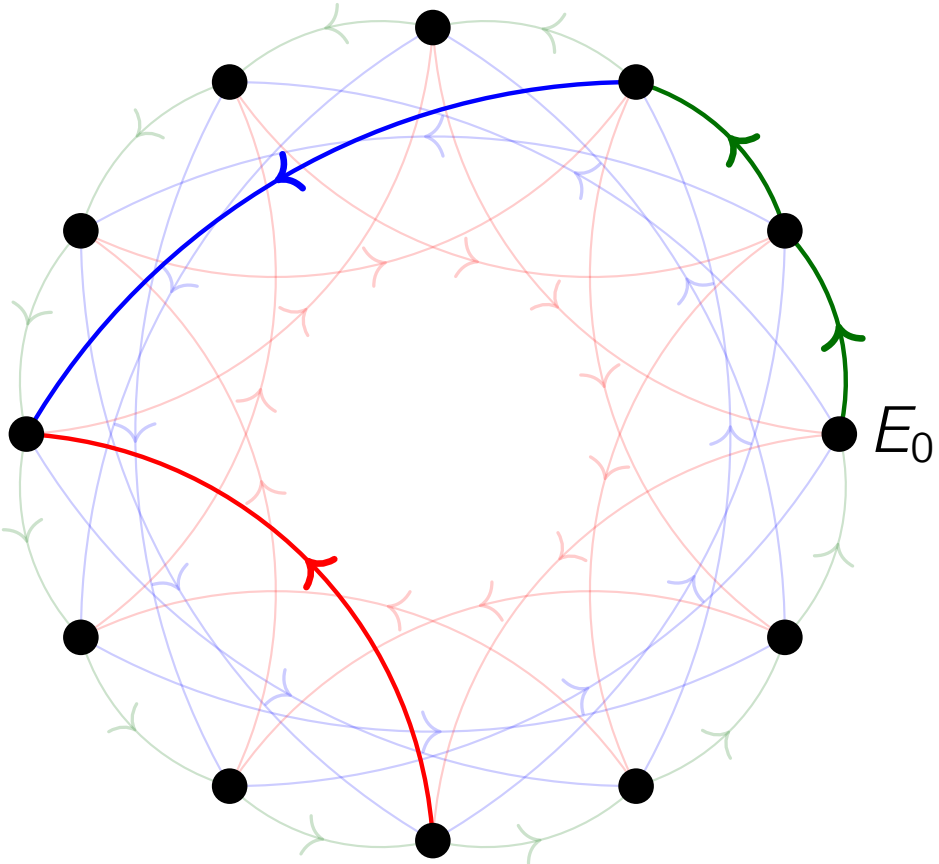
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

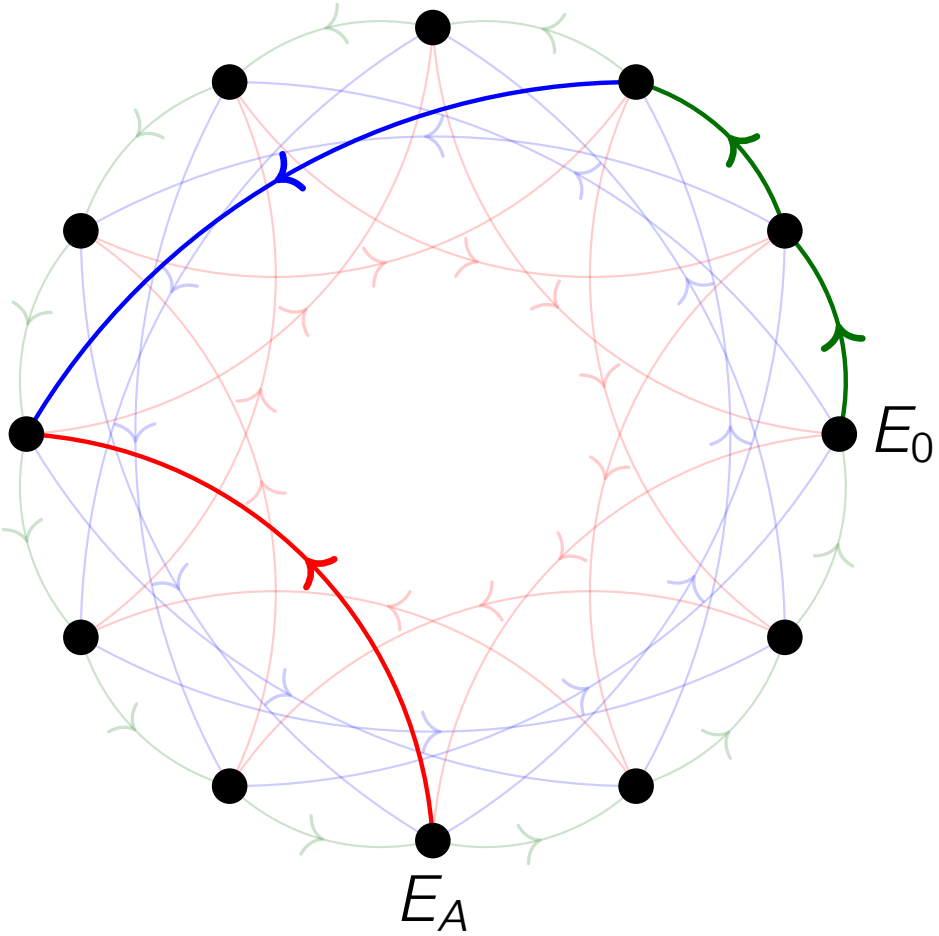
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

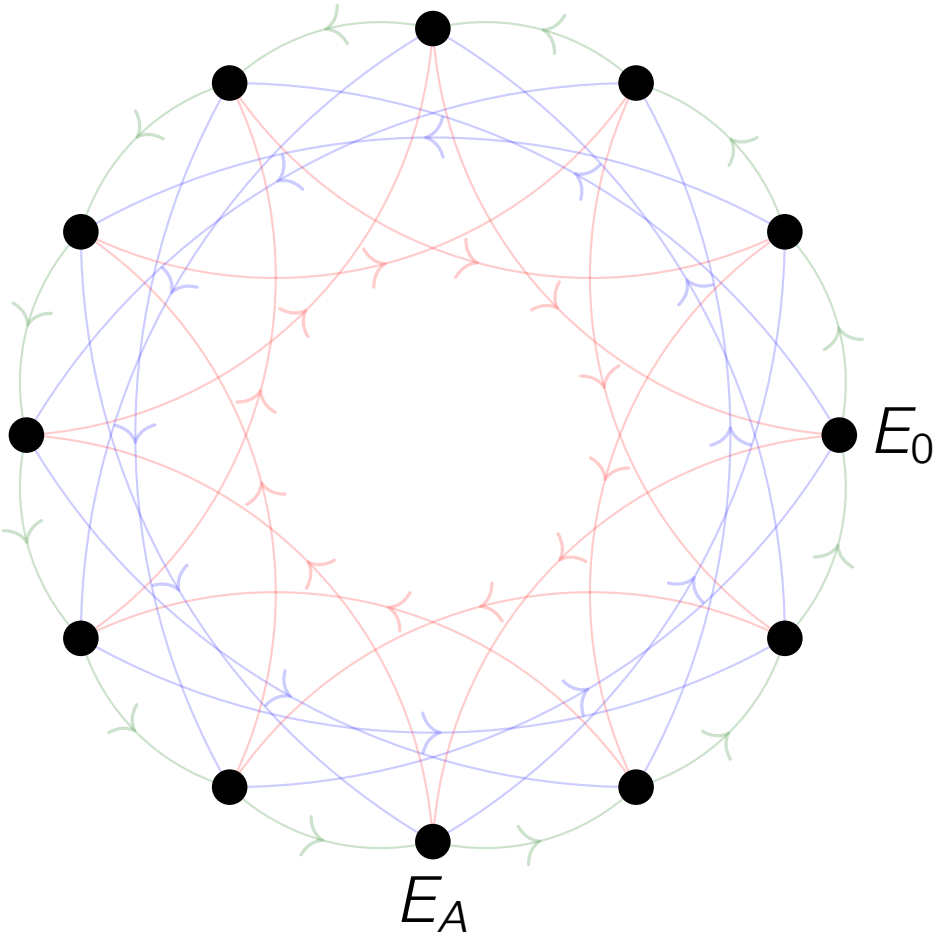


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

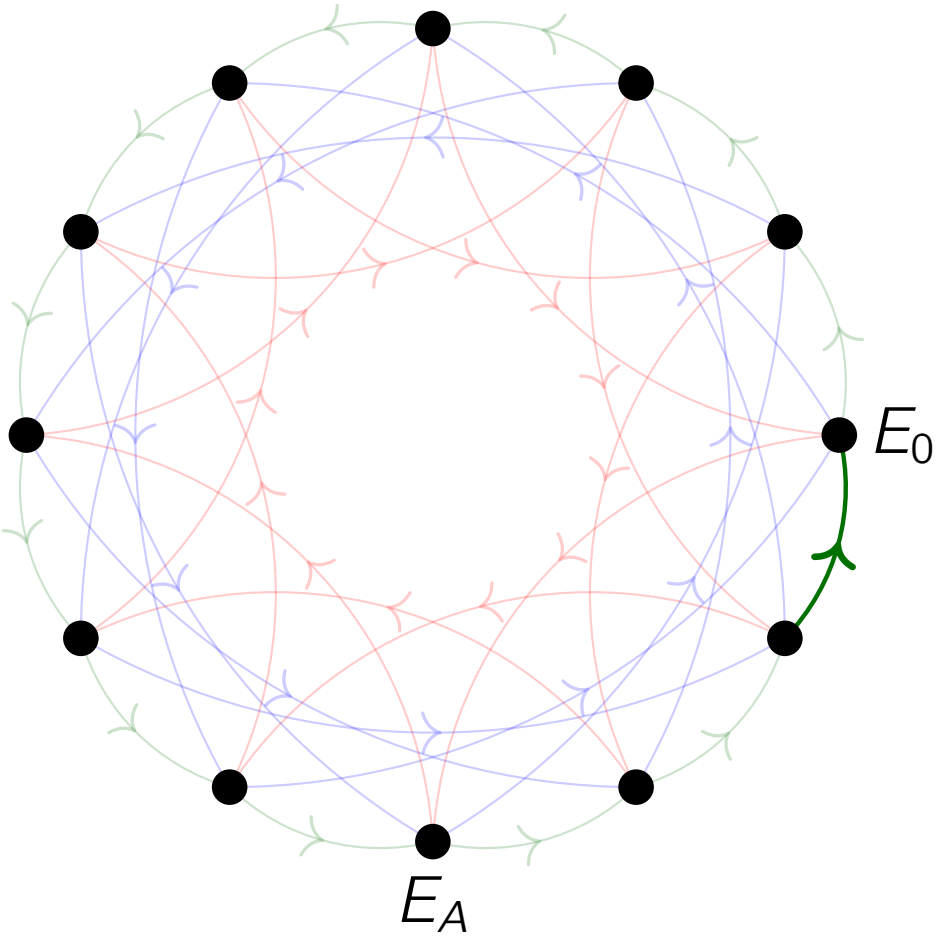
$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

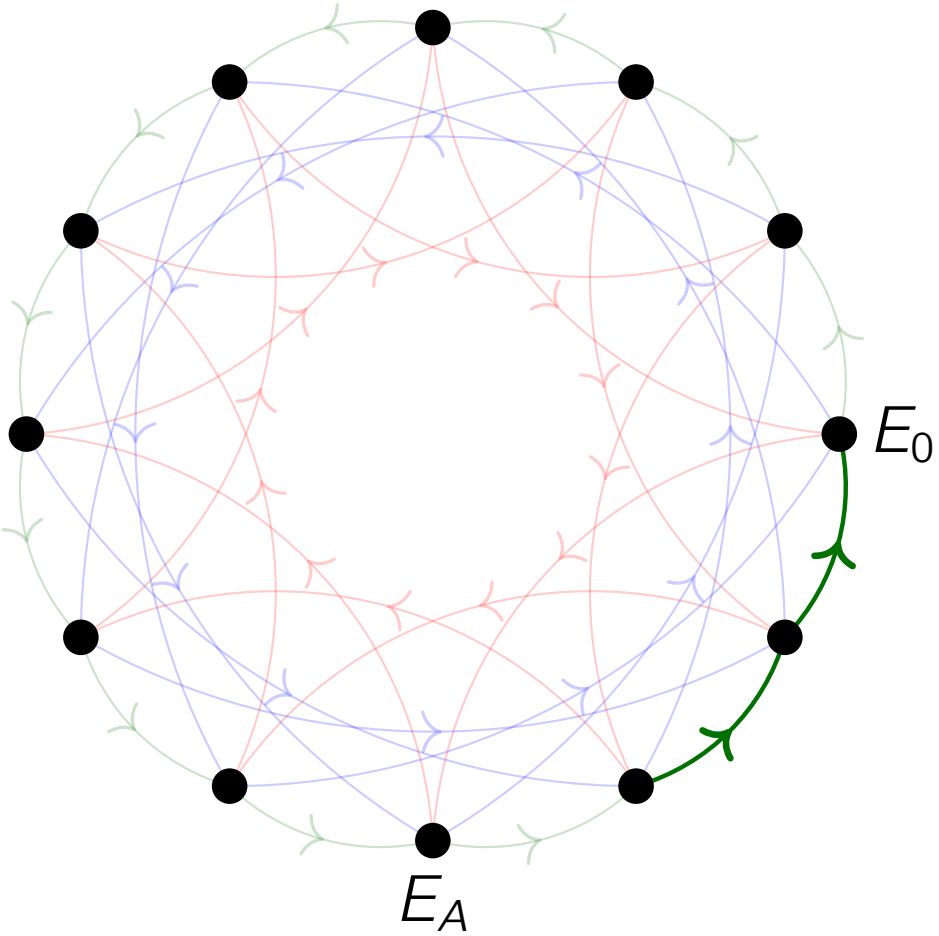
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

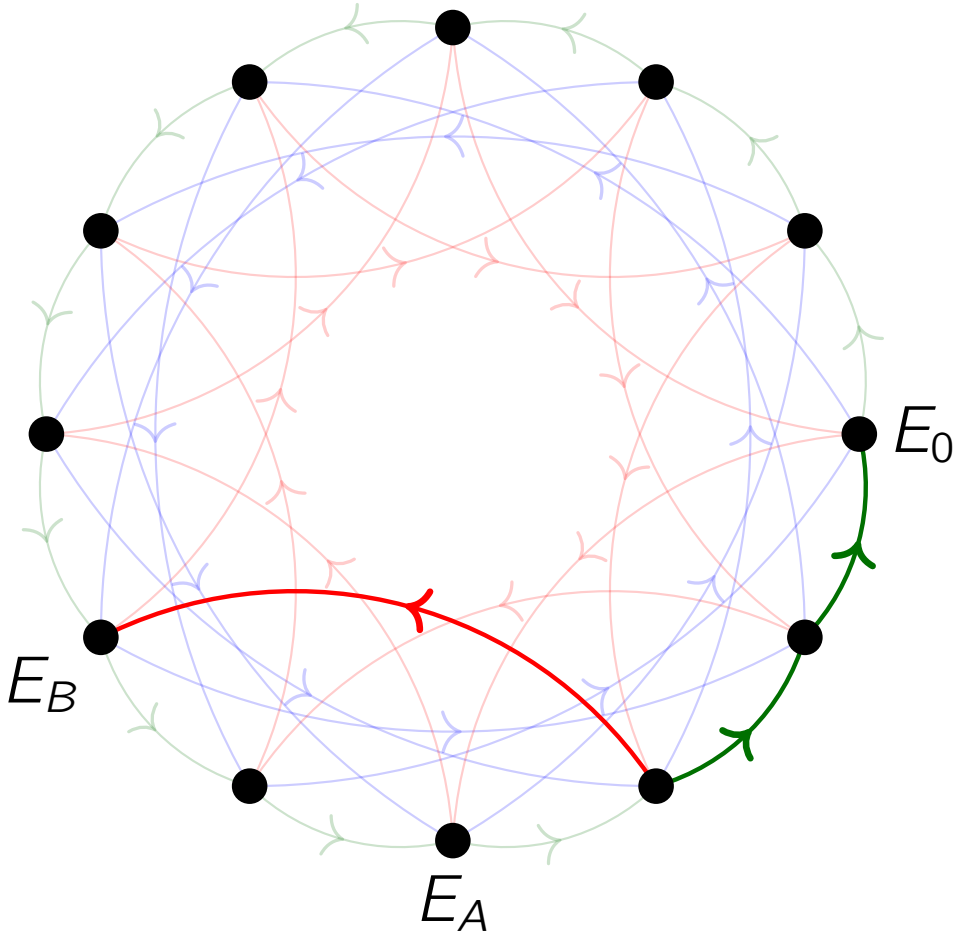
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

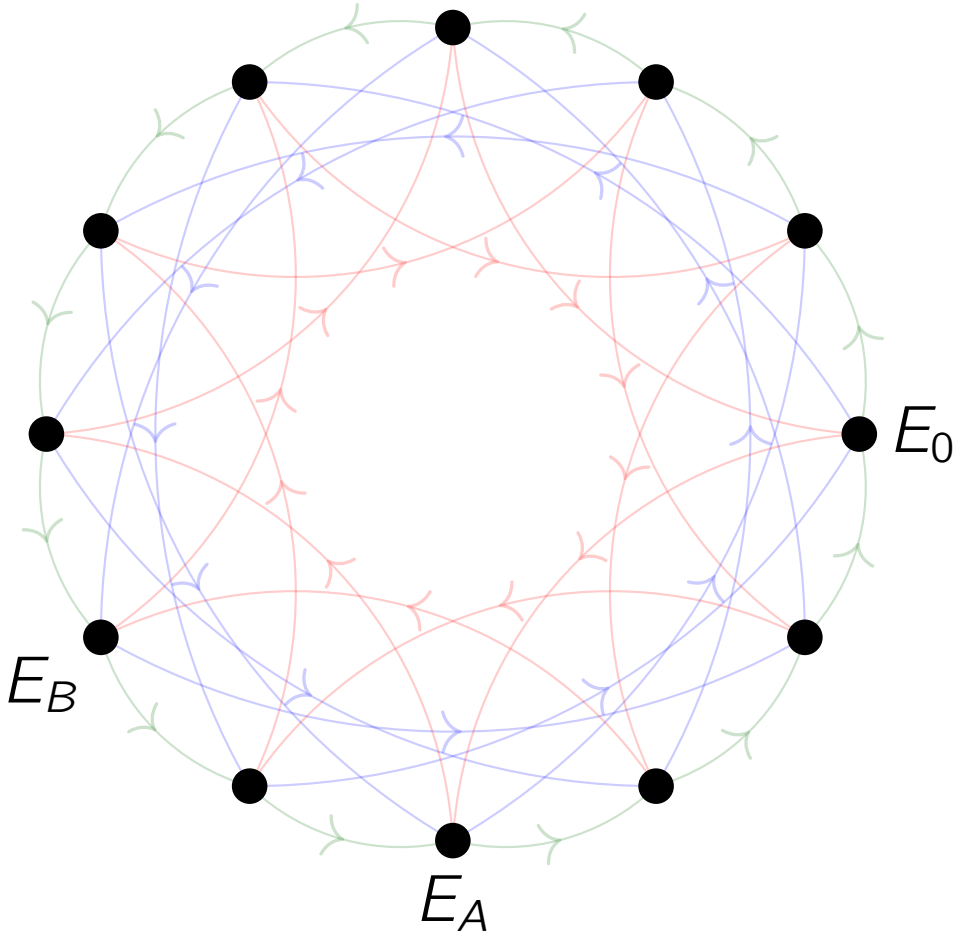
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

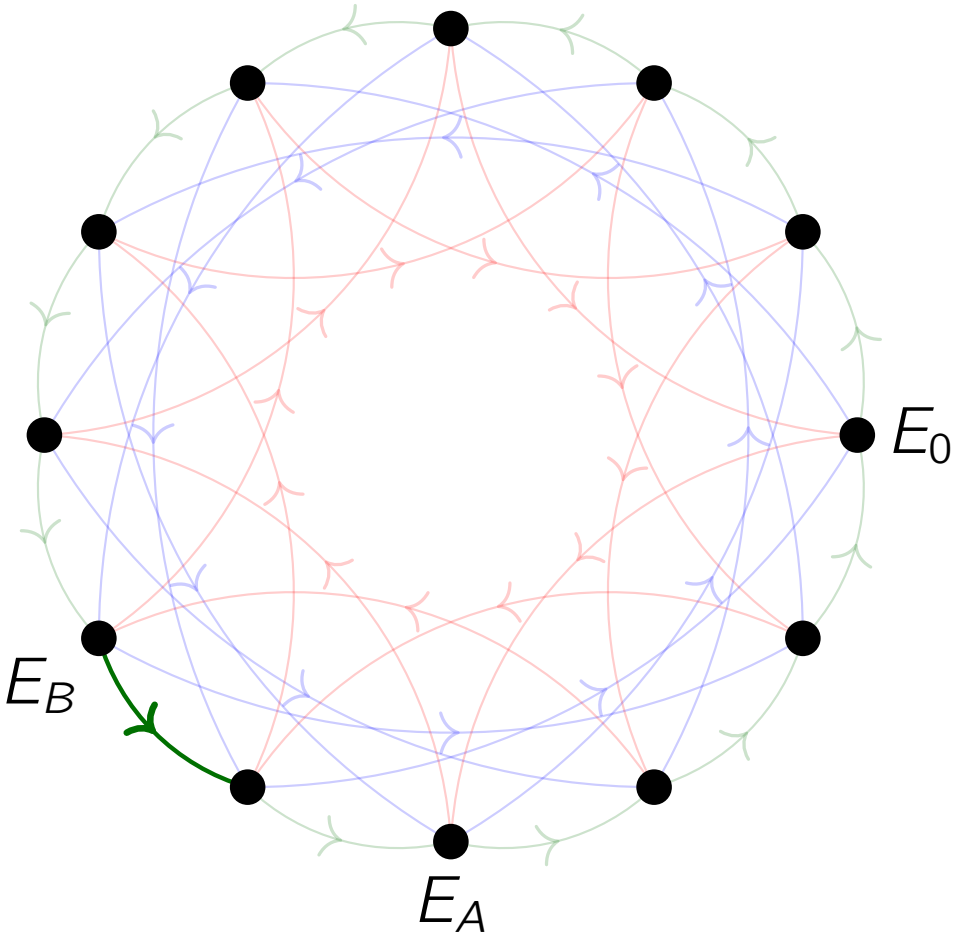
$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2\mathfrak{l}_2^1\mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2}\mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

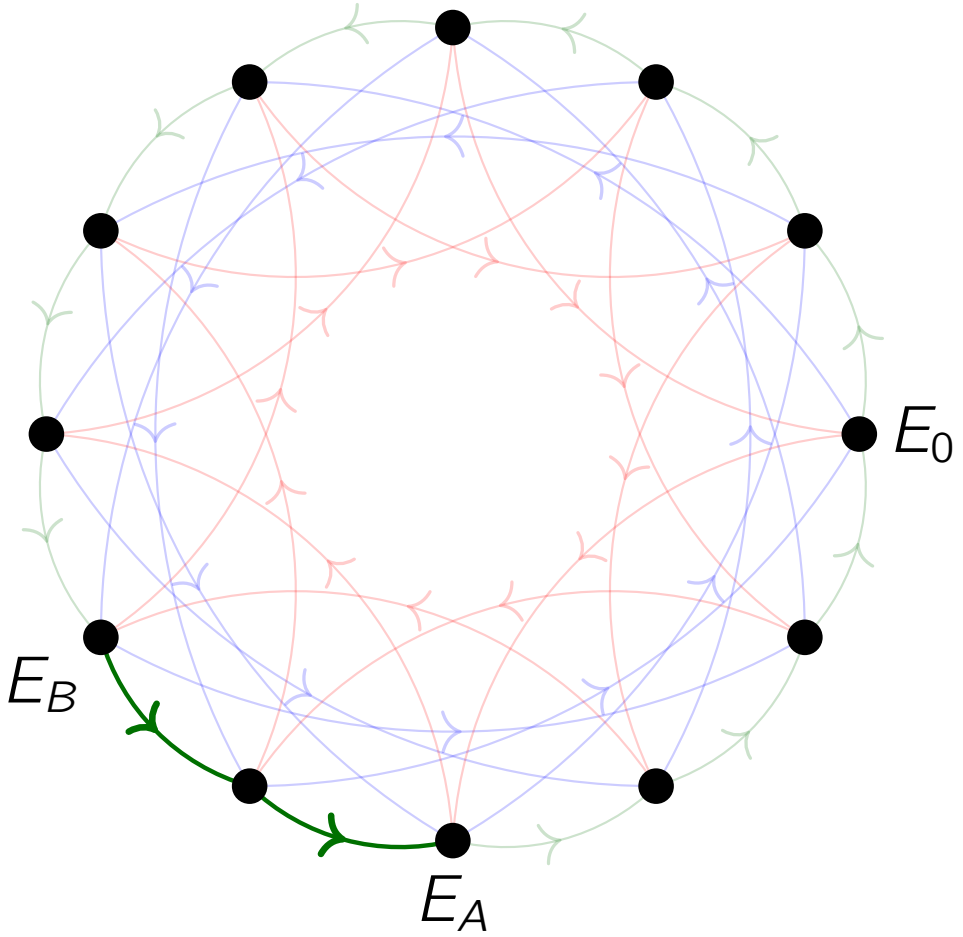
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

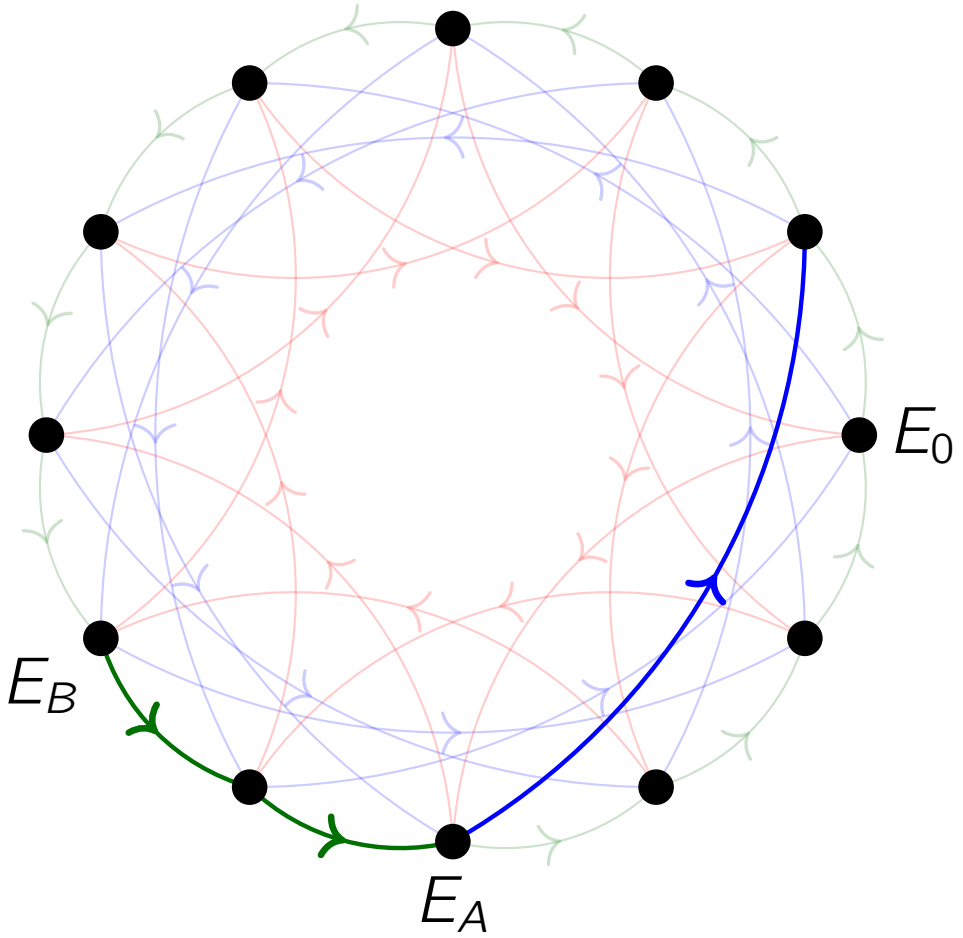
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

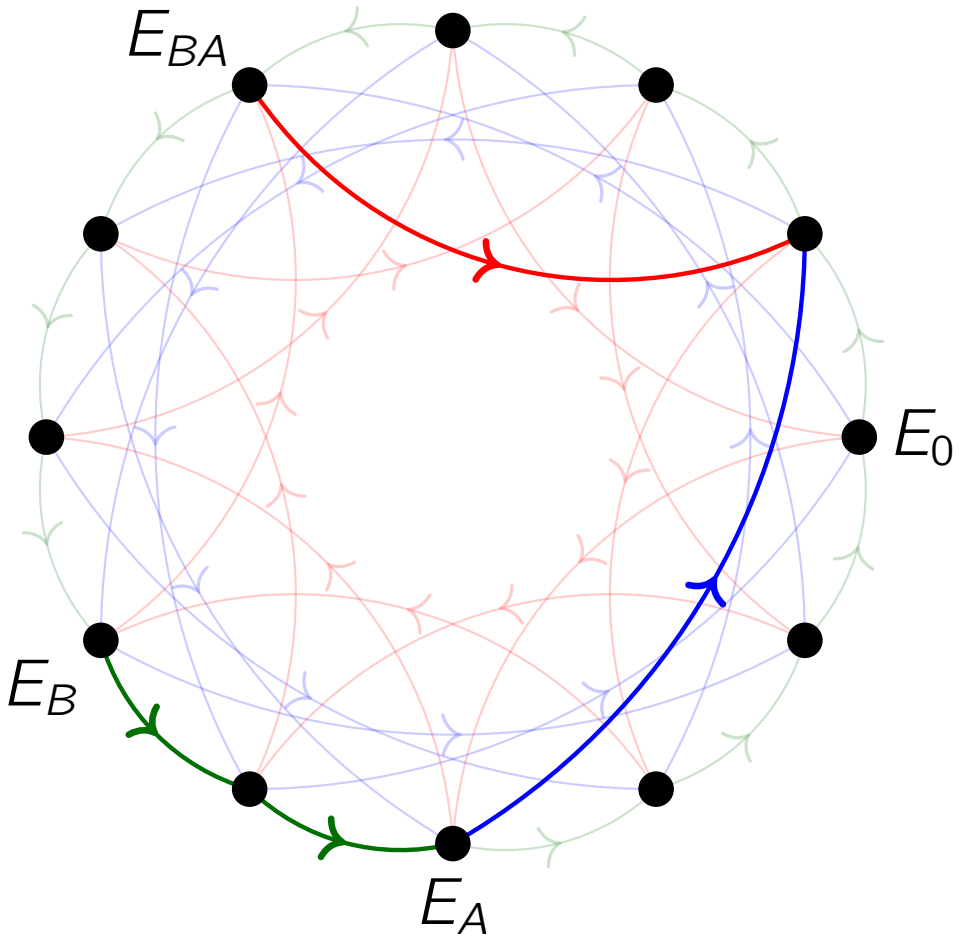
$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \ell_1^2 \ell_2^1 \ell_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

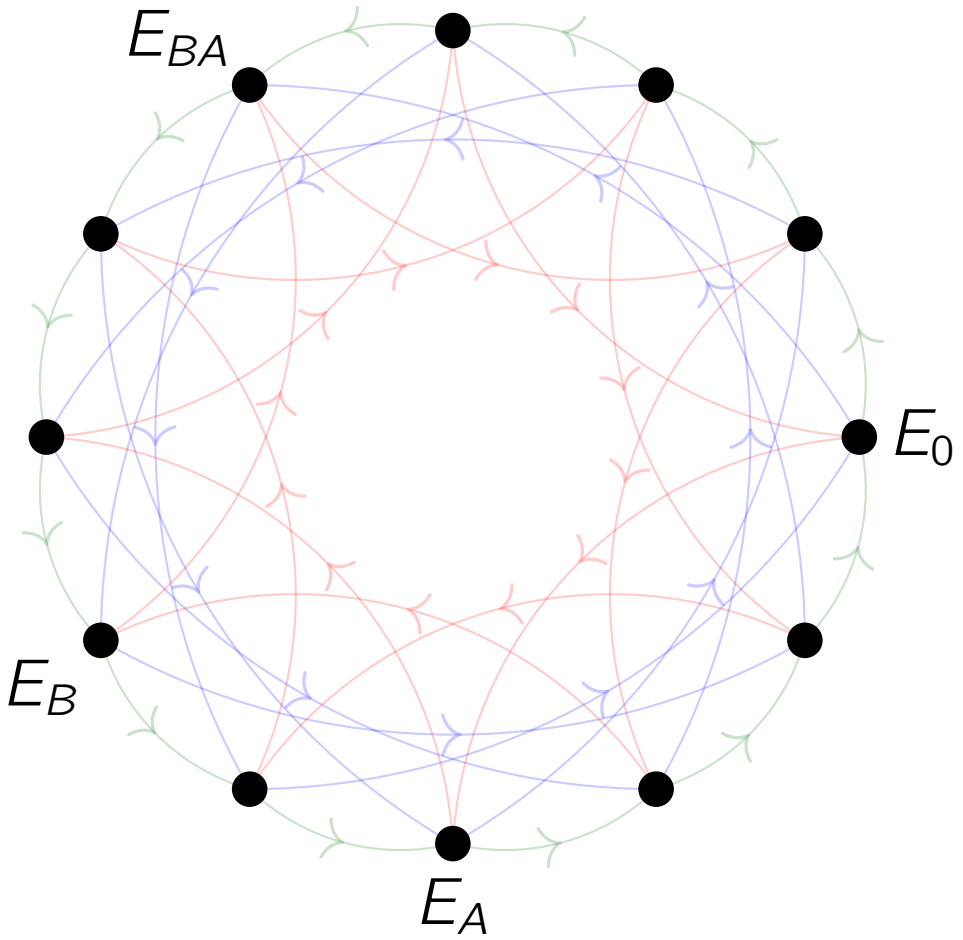
$\mathfrak{a} = \ell_1^{-2} \ell_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \ell_1^2 \ell_2^1 \ell_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \ell_1^{-2} \ell_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

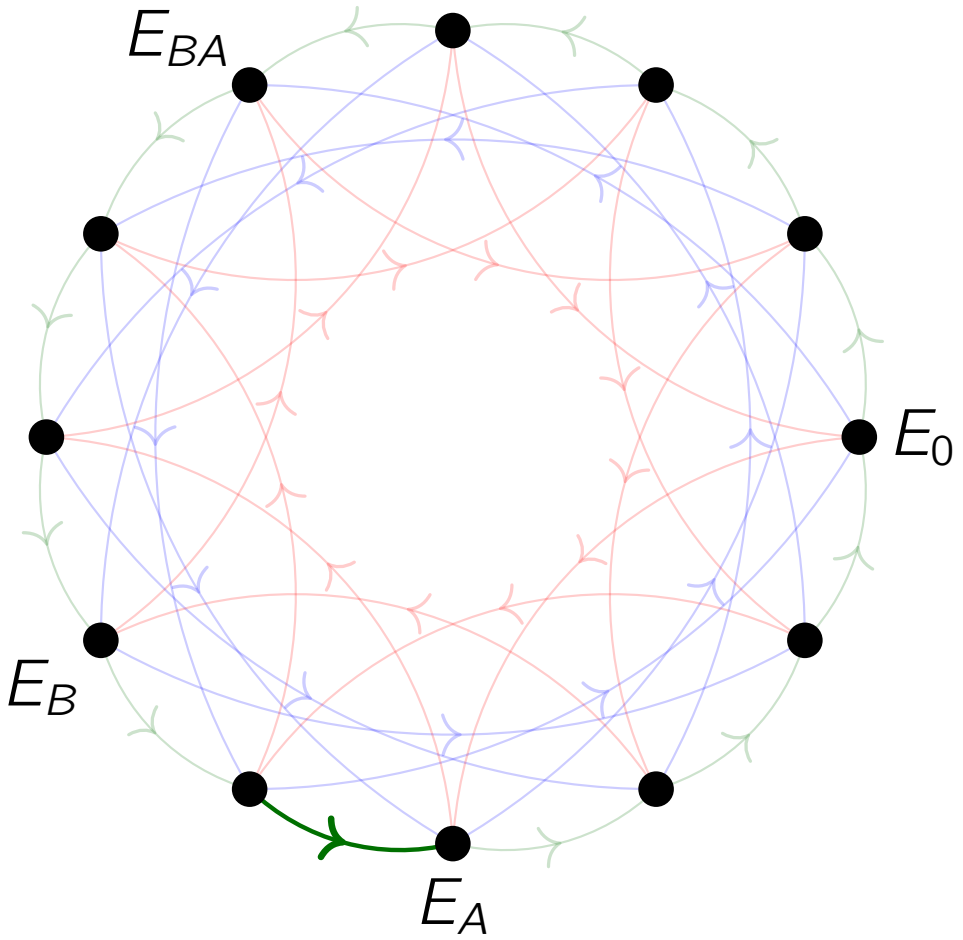
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

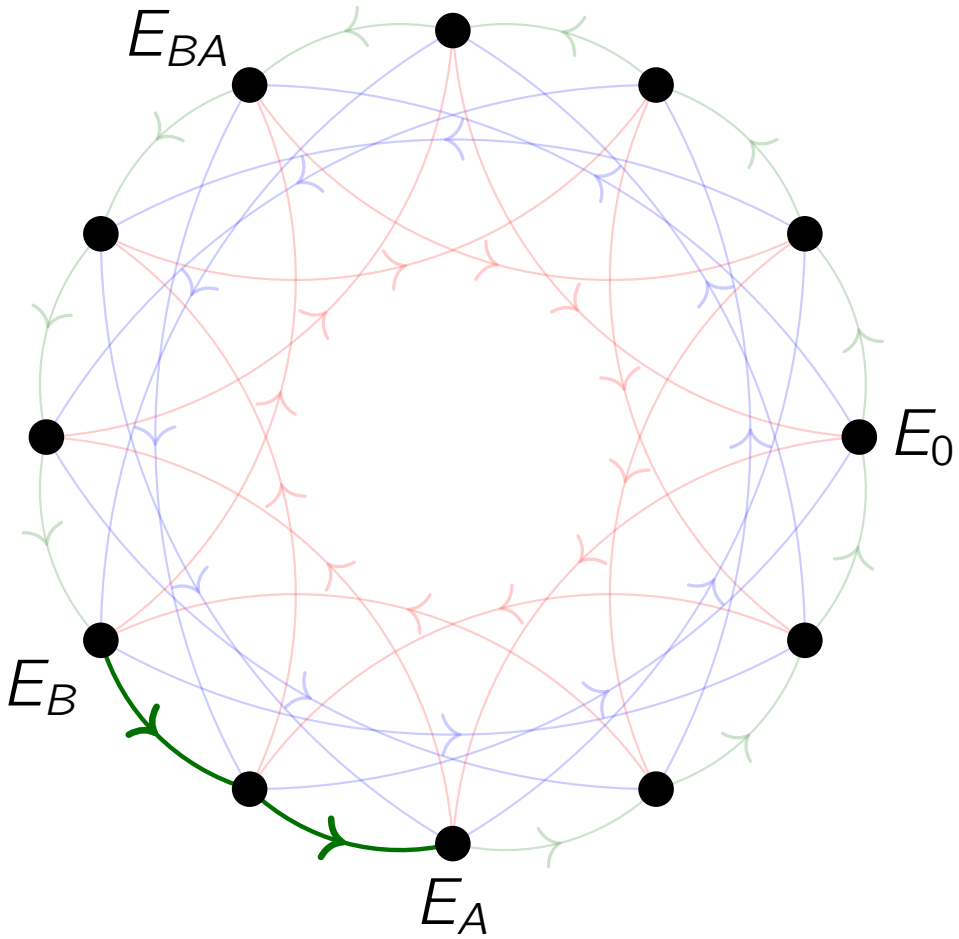
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

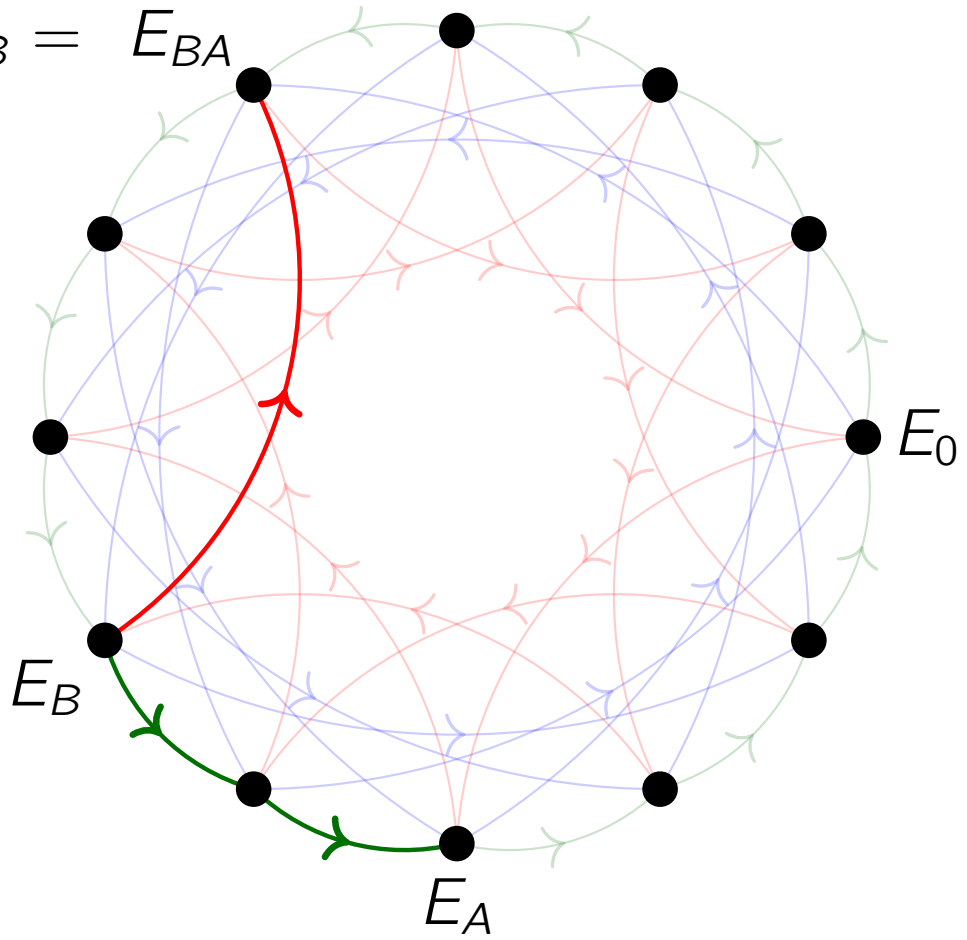
ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$E_{AB} = E_{BA}$

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

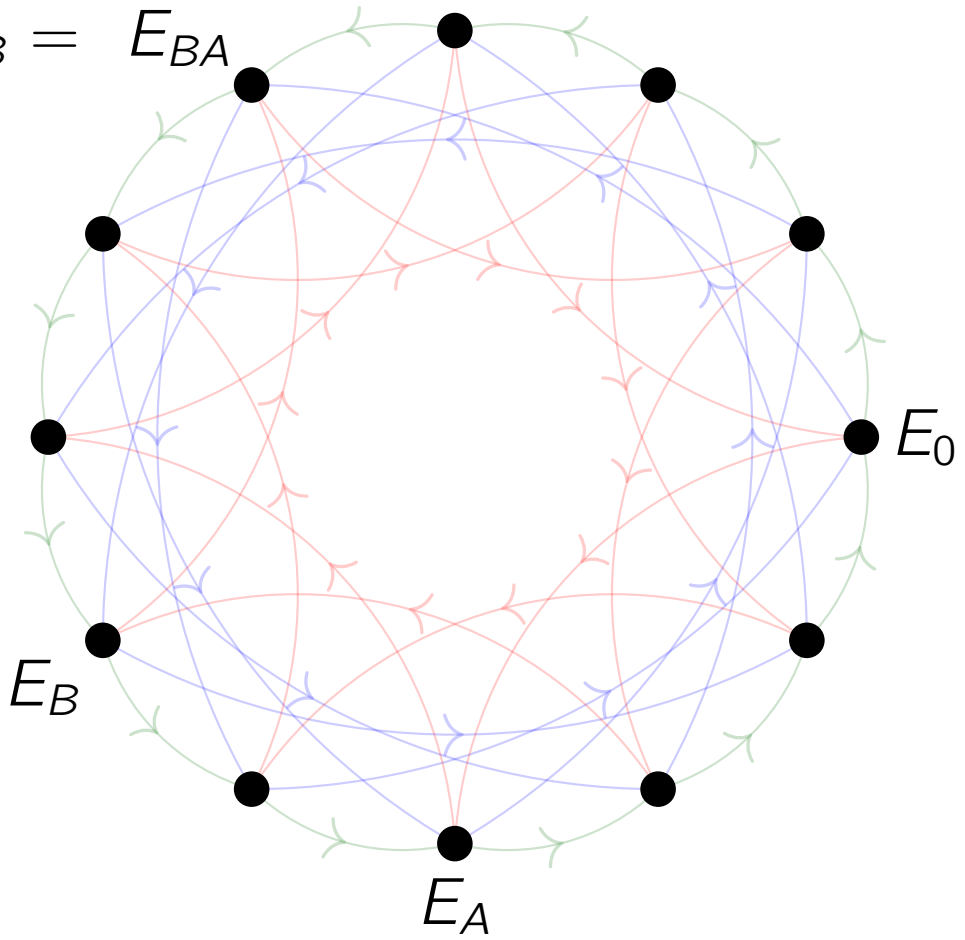
ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$E_{AB} = E_{BA}$

$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \ell_1^2 \ell_2^1 \ell_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \ell_1^{-2} \ell_3^1$

ORDINARY PROTOCOL - DH AND CVS

Goal: Alice and Bob have never met before. They communicate over a public channel and want to agree on a shared secret.

Setup: They agree on an elliptic curve $E/\mathbb{F}_q$ and a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$.

Alice	**Bob**
Pick a random ideal class $[\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O})$	Pick a random ideal class $[\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O})$
compute $E_A = [\mathfrak{a}] * E_0$	compute $E_B = [\mathfrak{b}] * E_0$
$\xrightarrow{E_A}$	
$\xleftarrow{E_B}$	
compute $[\mathfrak{a}] * E_B$	compute $[\mathfrak{b}] * E_A$

Shared secret is $[\mathfrak{a}] * E_B = [\mathfrak{ab}] * E_0 = [\mathfrak{b}] * E_A$

Abelian hidden-shift problem

Let A be a finite abelian group, let S be a finite set, and let $f, g : A \longrightarrow S$ be injective functions.
Assume that there exists an unknown element $b \in A$ such that

$$f(x) = g(xb)$$

for every $x \in A$.
Problem: Recover the hidden shift b.

Recovering the element taking E to E' is an instance of the abelian hidden-shift problem.

KUPERBERGS ALGORITHM

Theorem — Kuperberg, 2003

Let A be a finite abelian group of order N. The abelian hidden-shift problem can be solved on a quantum computer in

$$\exp\left(O\left(\sqrt{\log N}\right)\right) = L_N\left(\frac{1}{2}, O(1)\right)$$

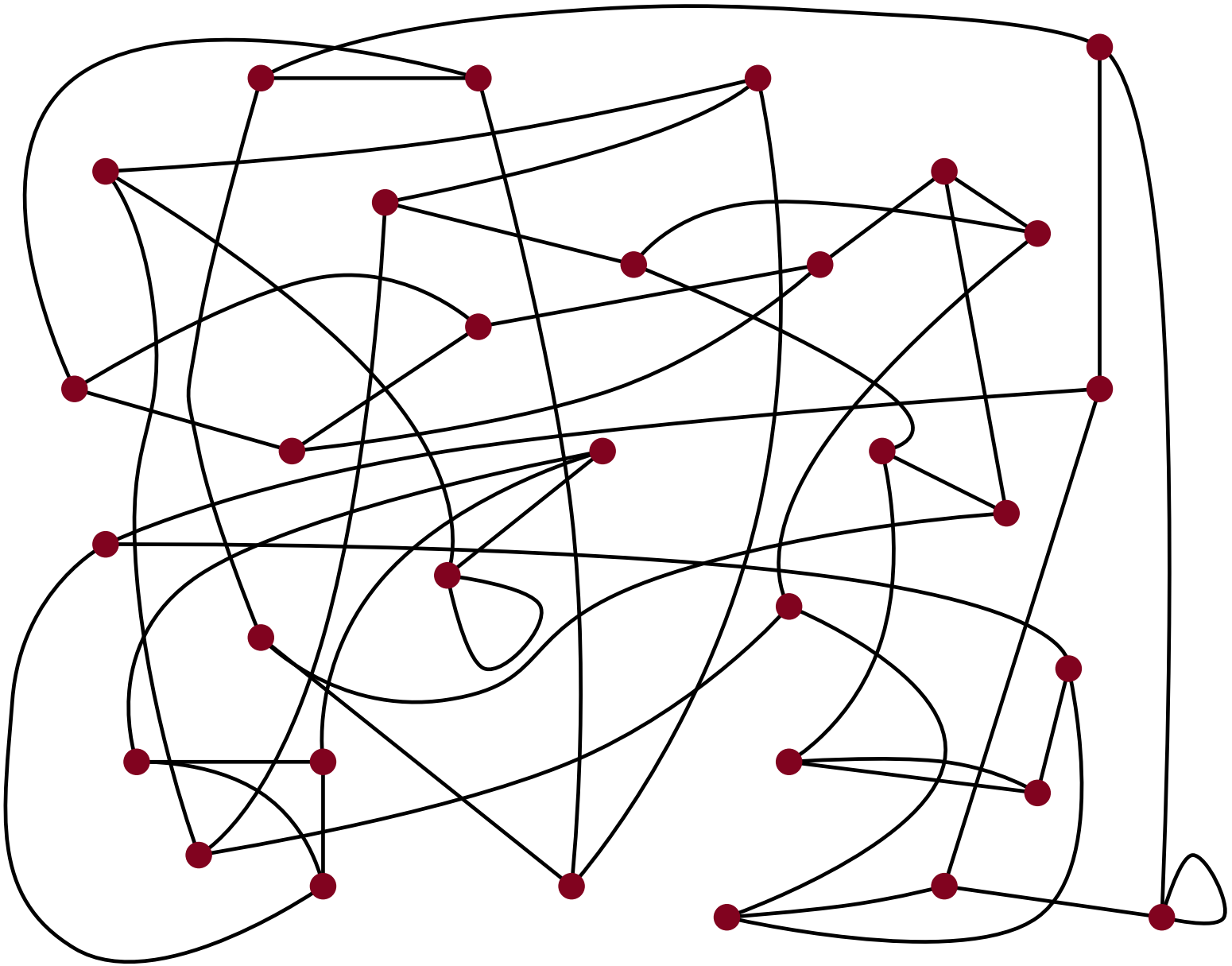
time, space, and oracle queries.

- Kuperberg's algorithm requires many quantum evaluations of the functions f and g.
- In the isogeny setting, these evaluations are group-action computations:

$$f(a) = a * E, \qquad g(a) = a * E'.$$

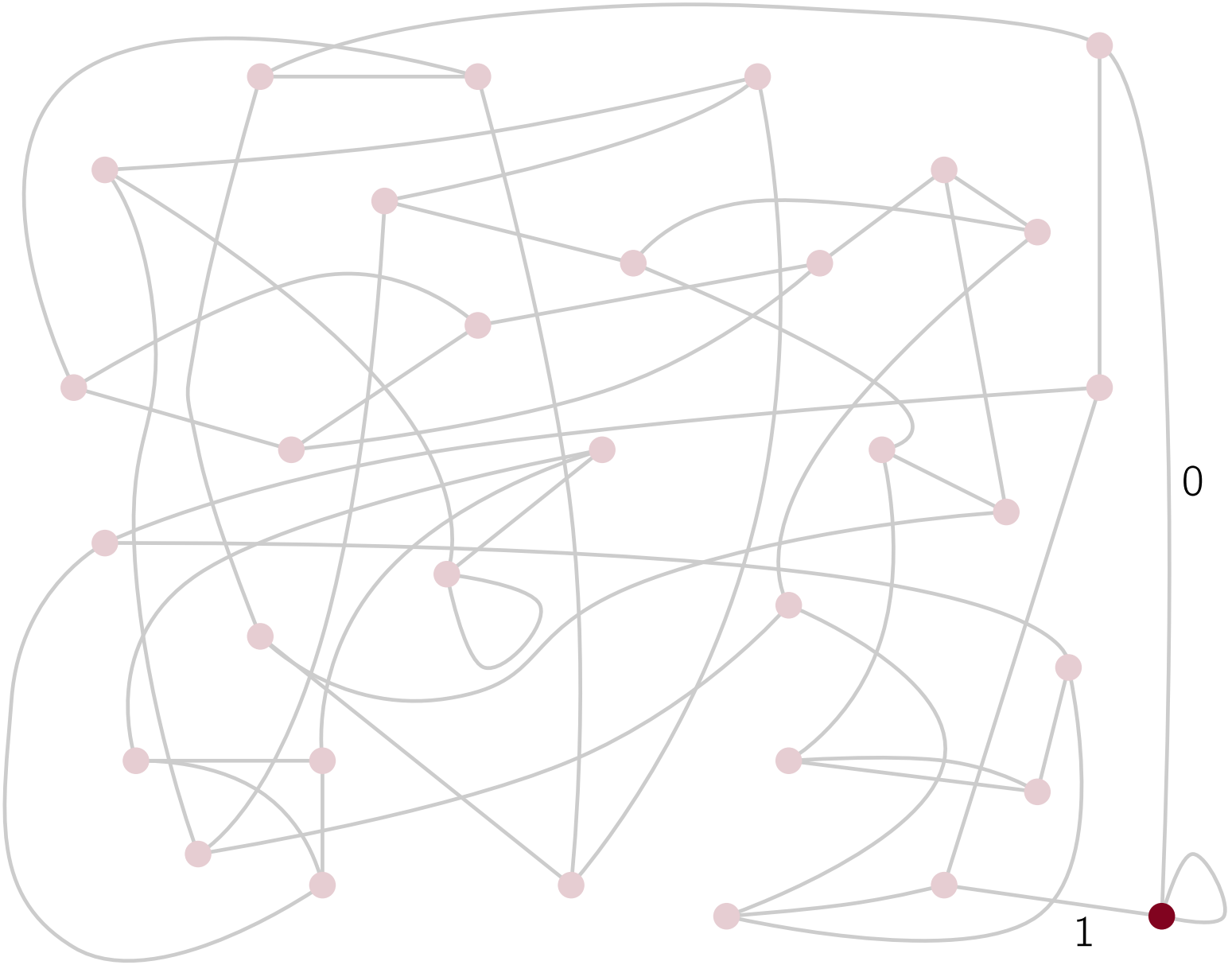
- The quantum cost depends not only on the number of oracle queries, but also on the cost of evaluating the class-group action.
- This gives a subexponential quantum attack against vectorization in commutative group-action systems such as CRS

HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006

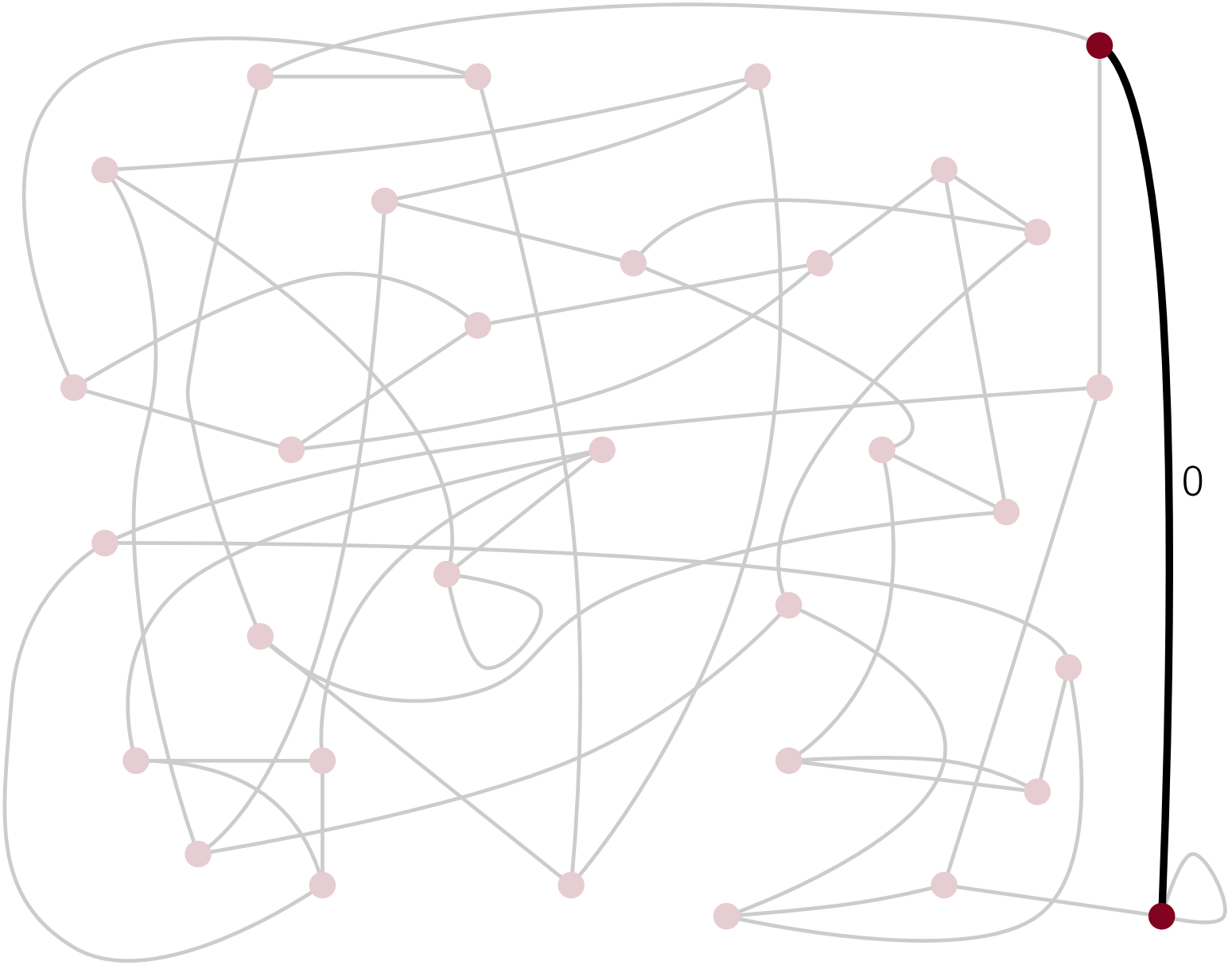


HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006

HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006

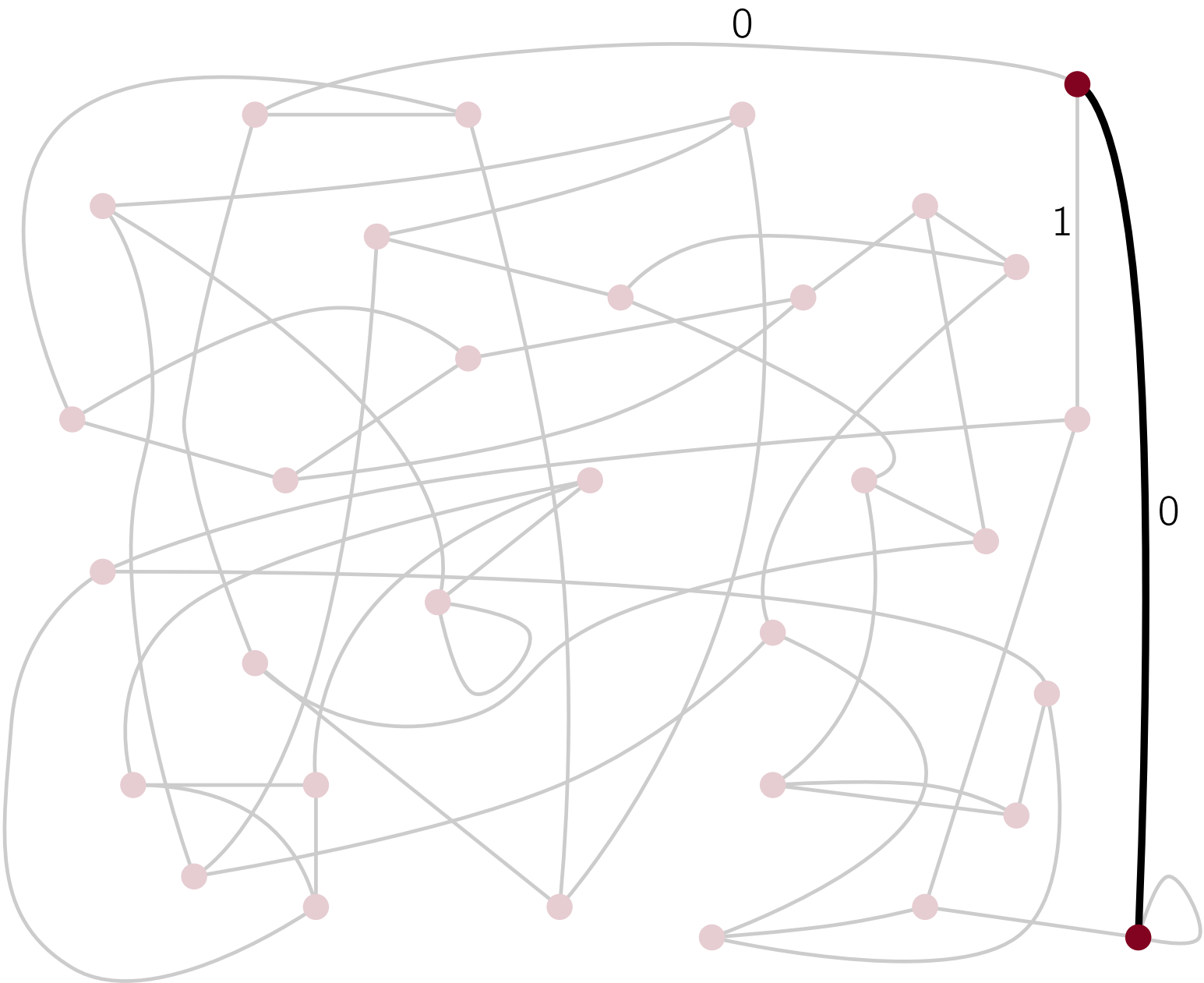


HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006

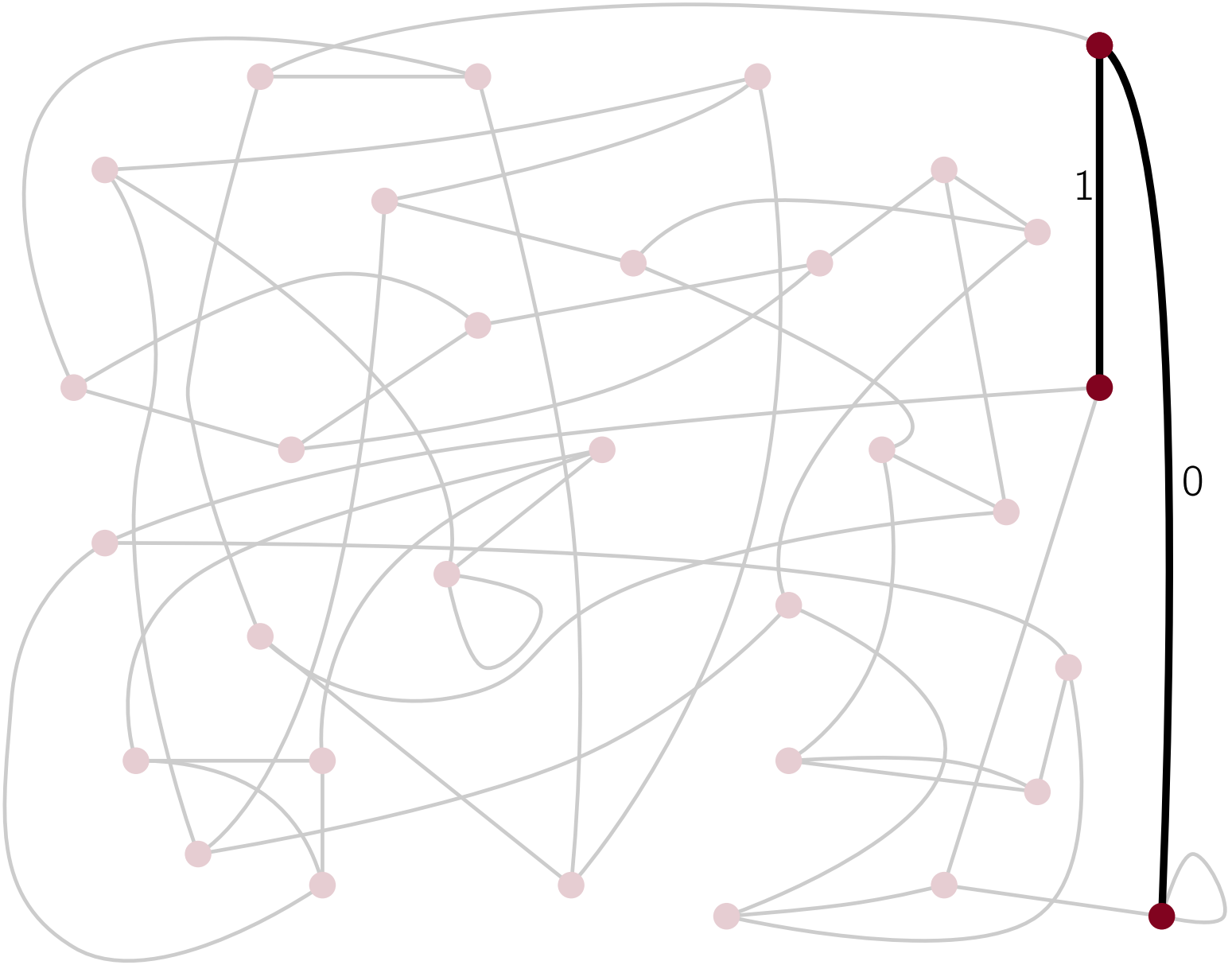


HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006

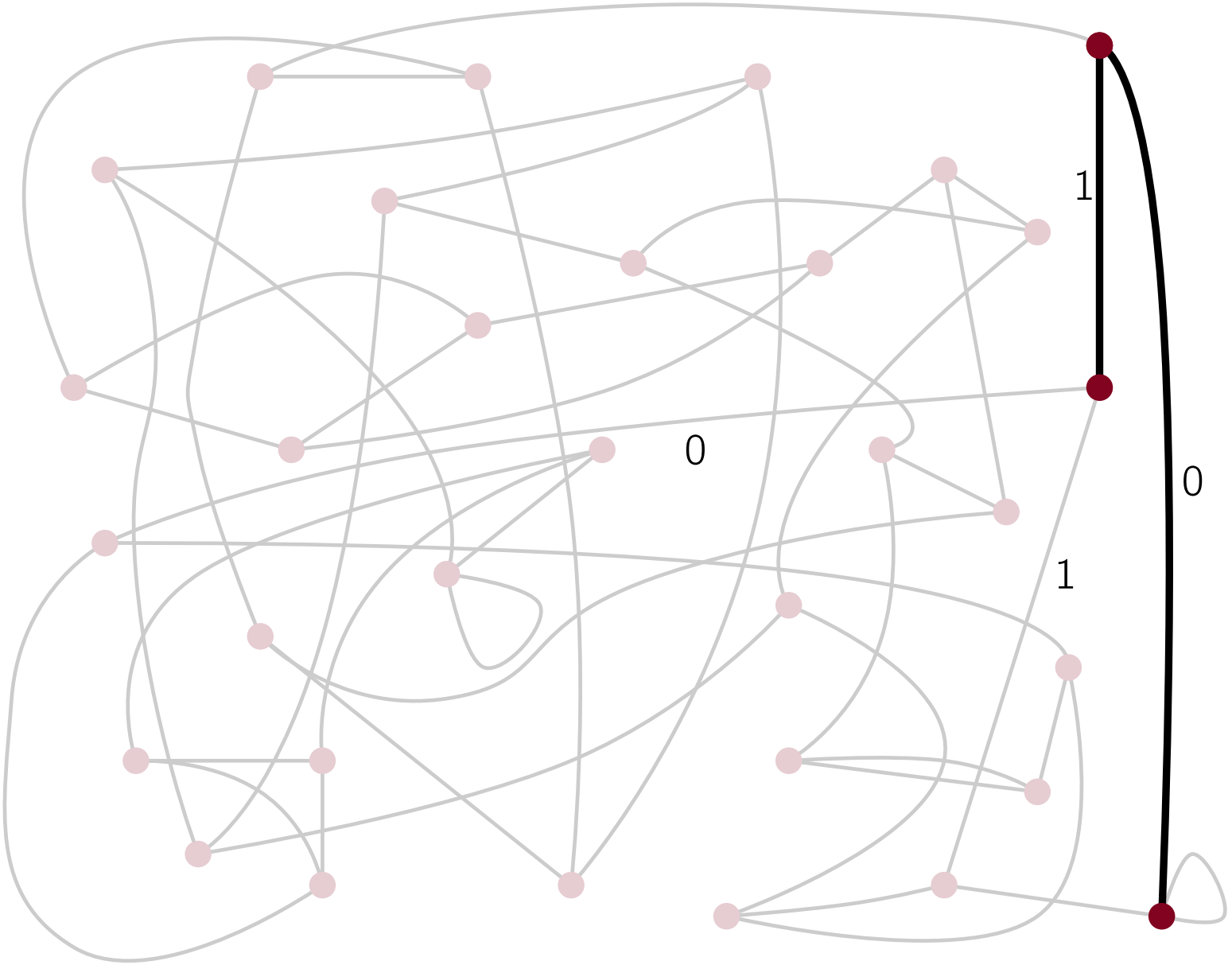
L.COLÒ UWAT



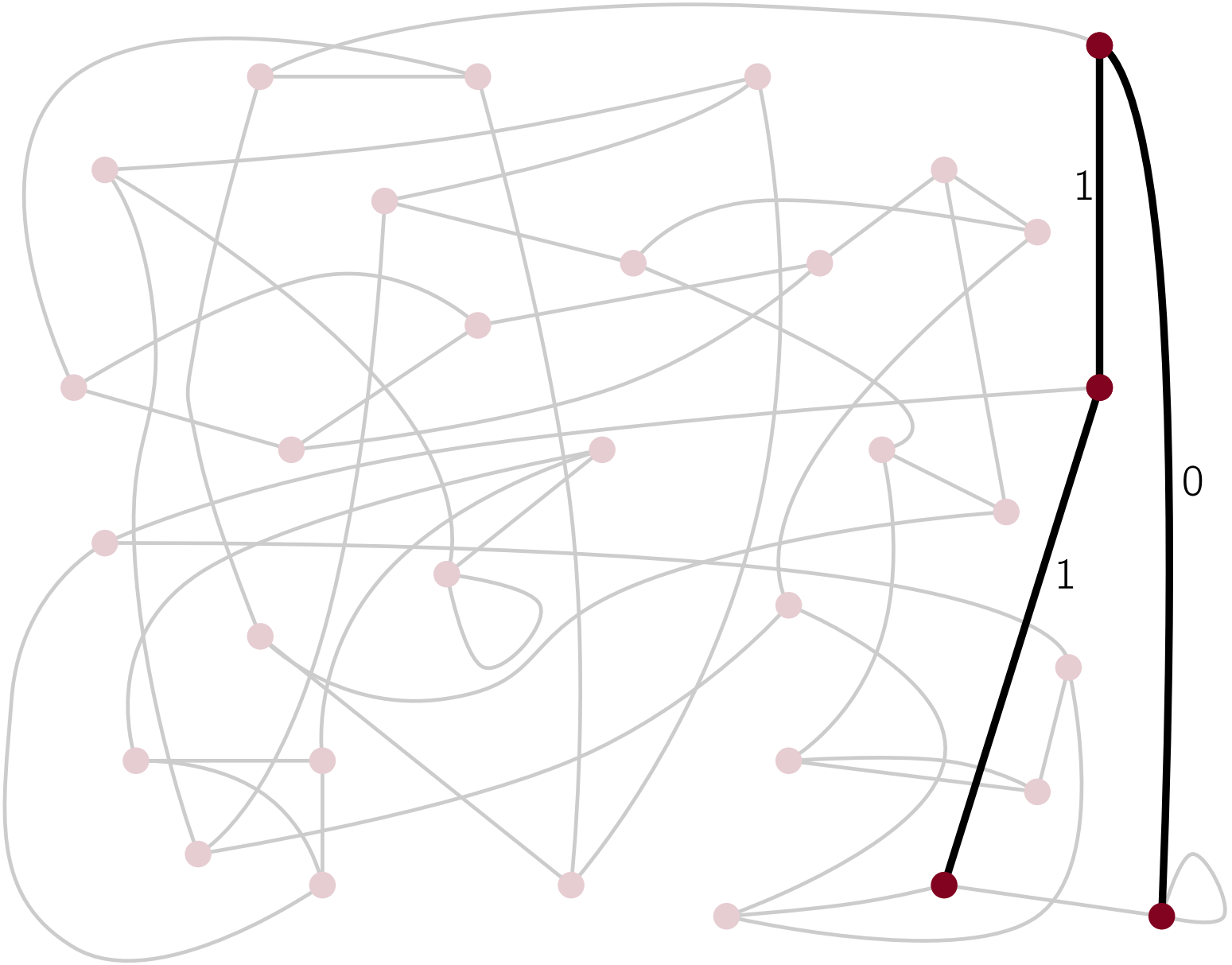
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



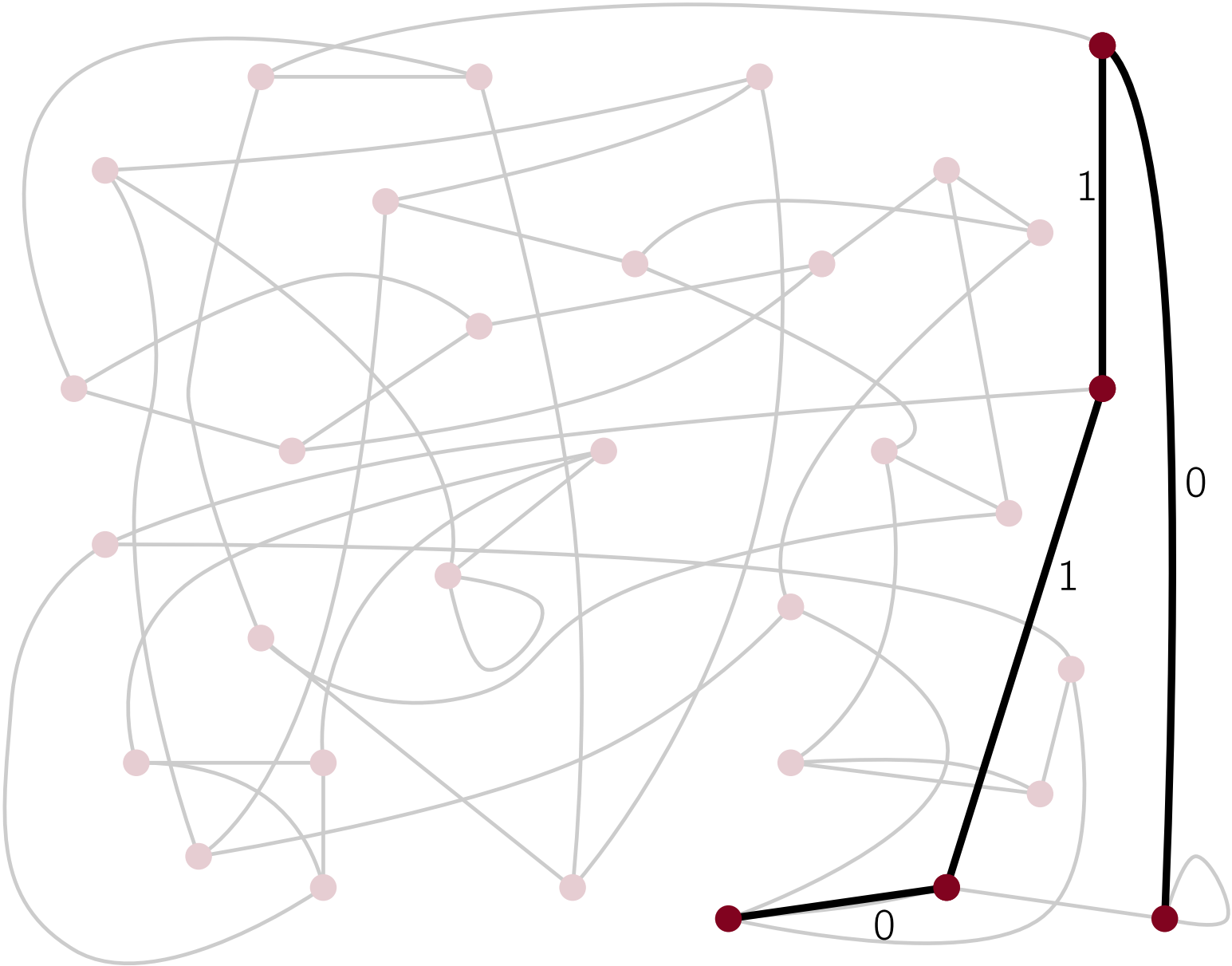
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



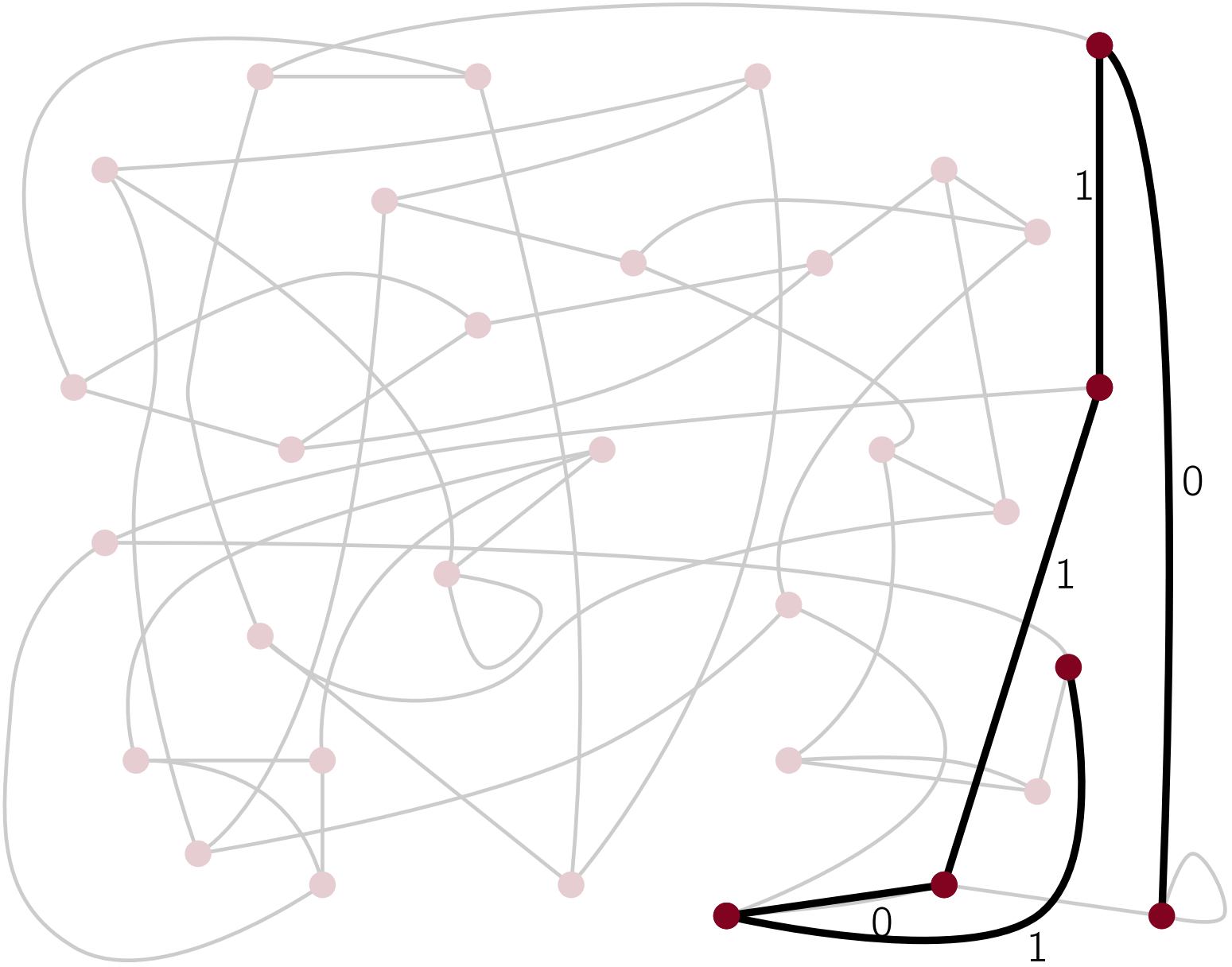
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



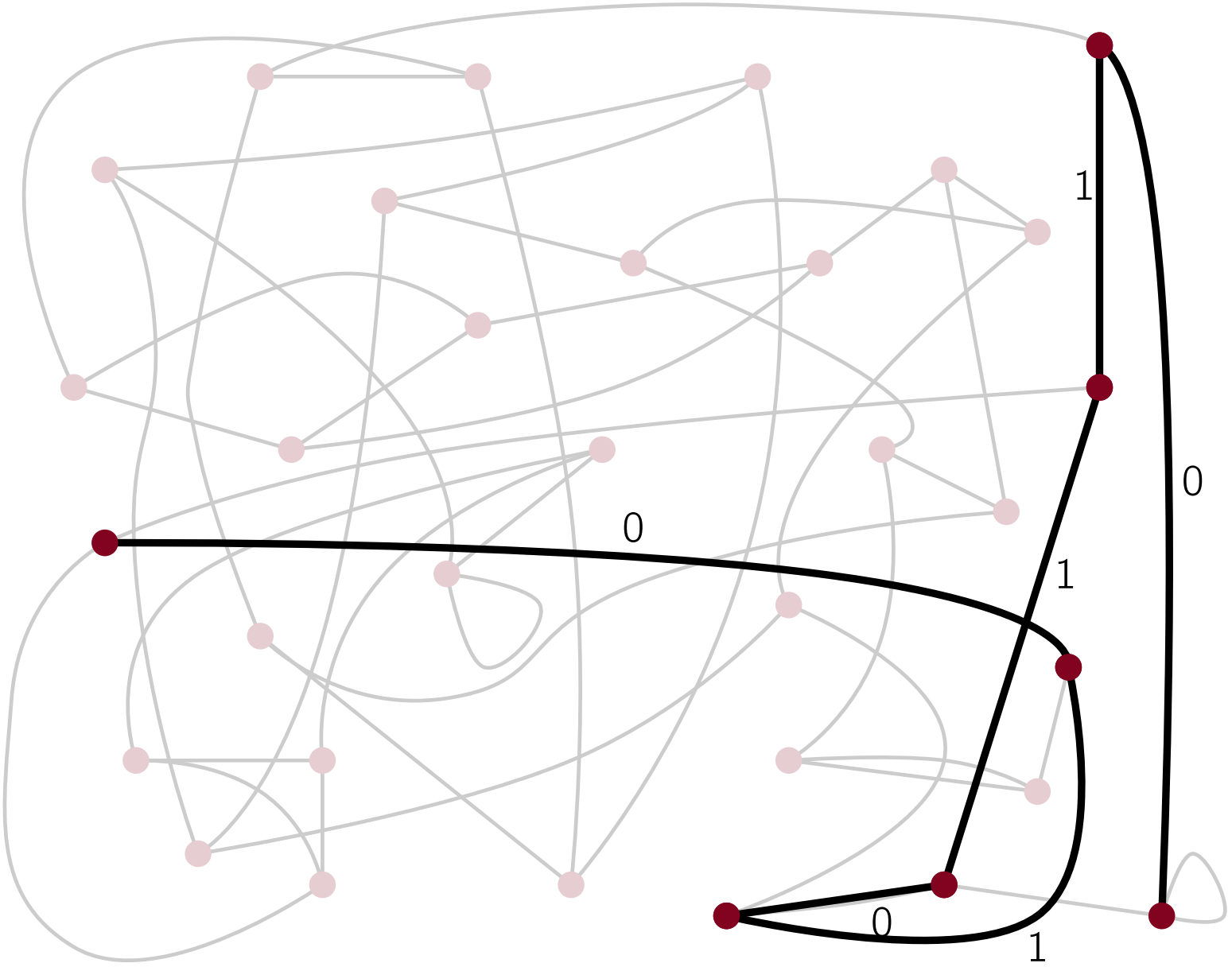
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



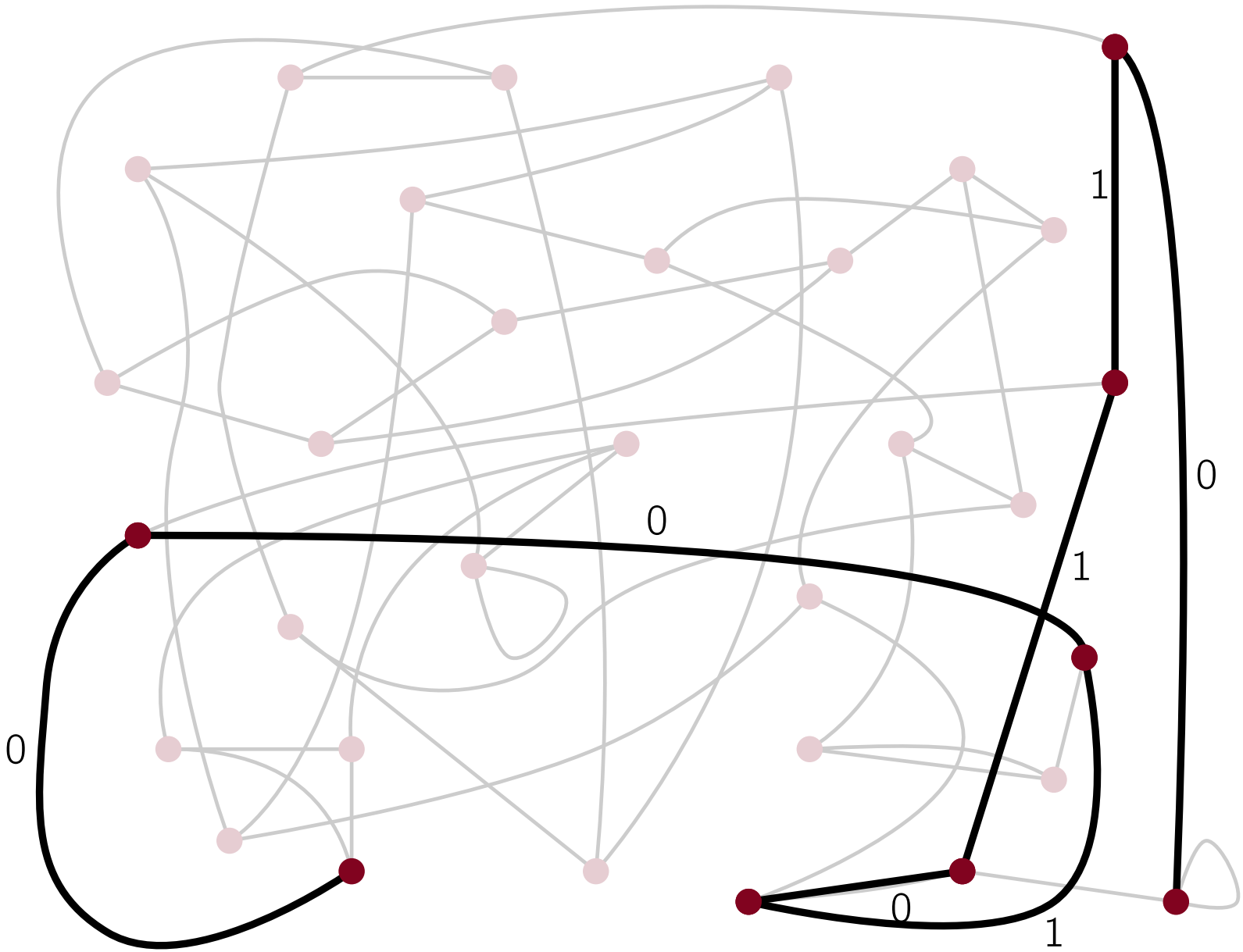
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



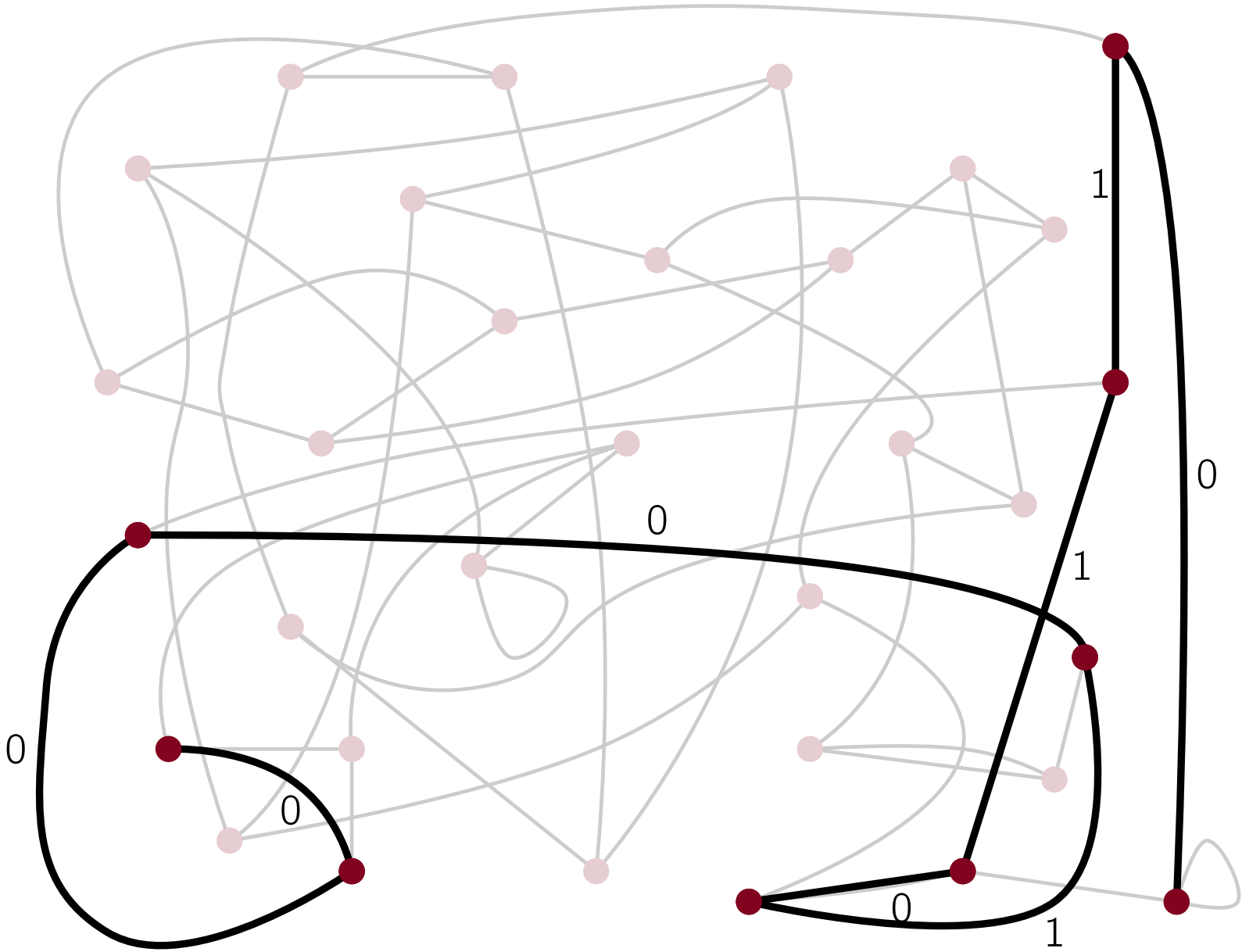
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



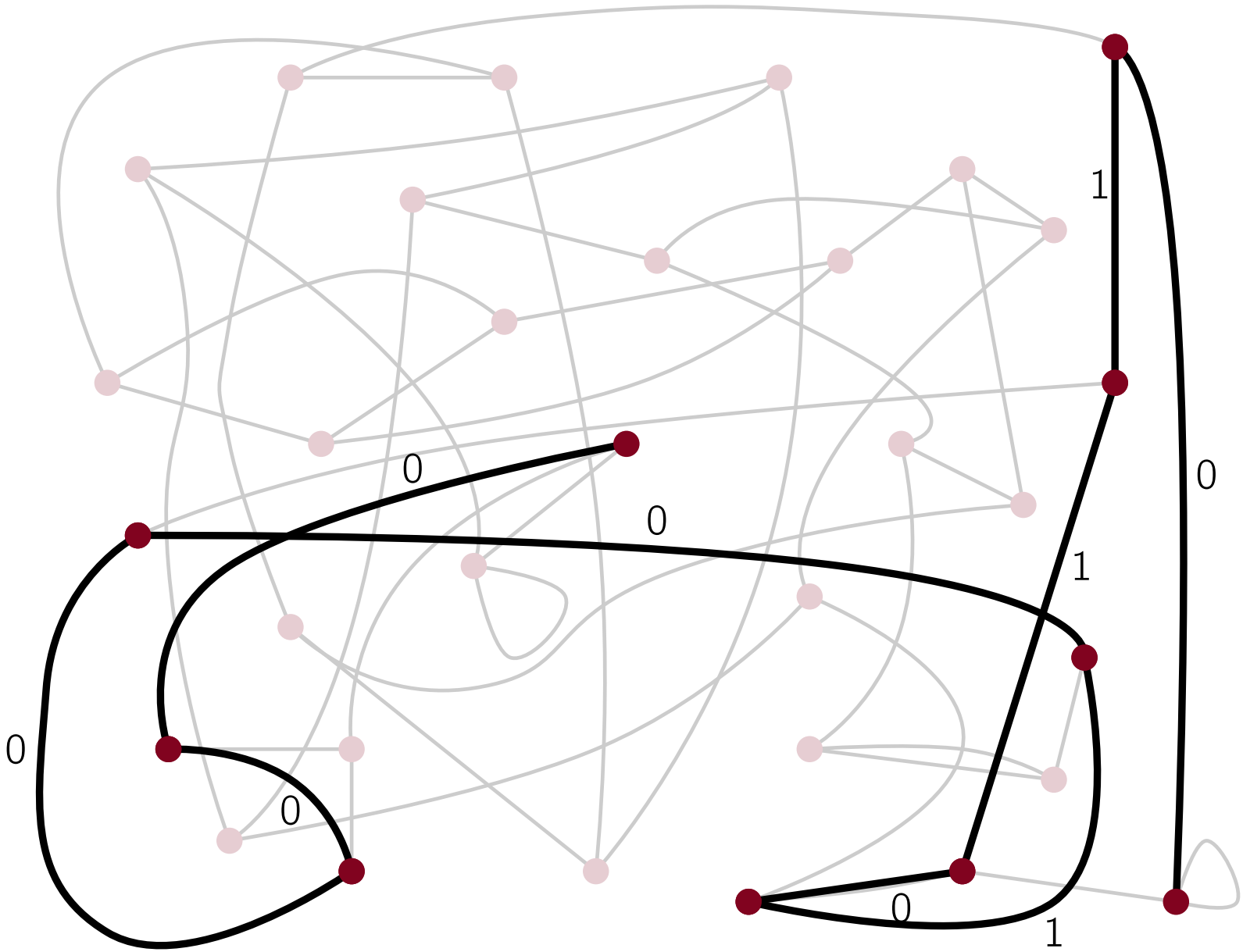
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



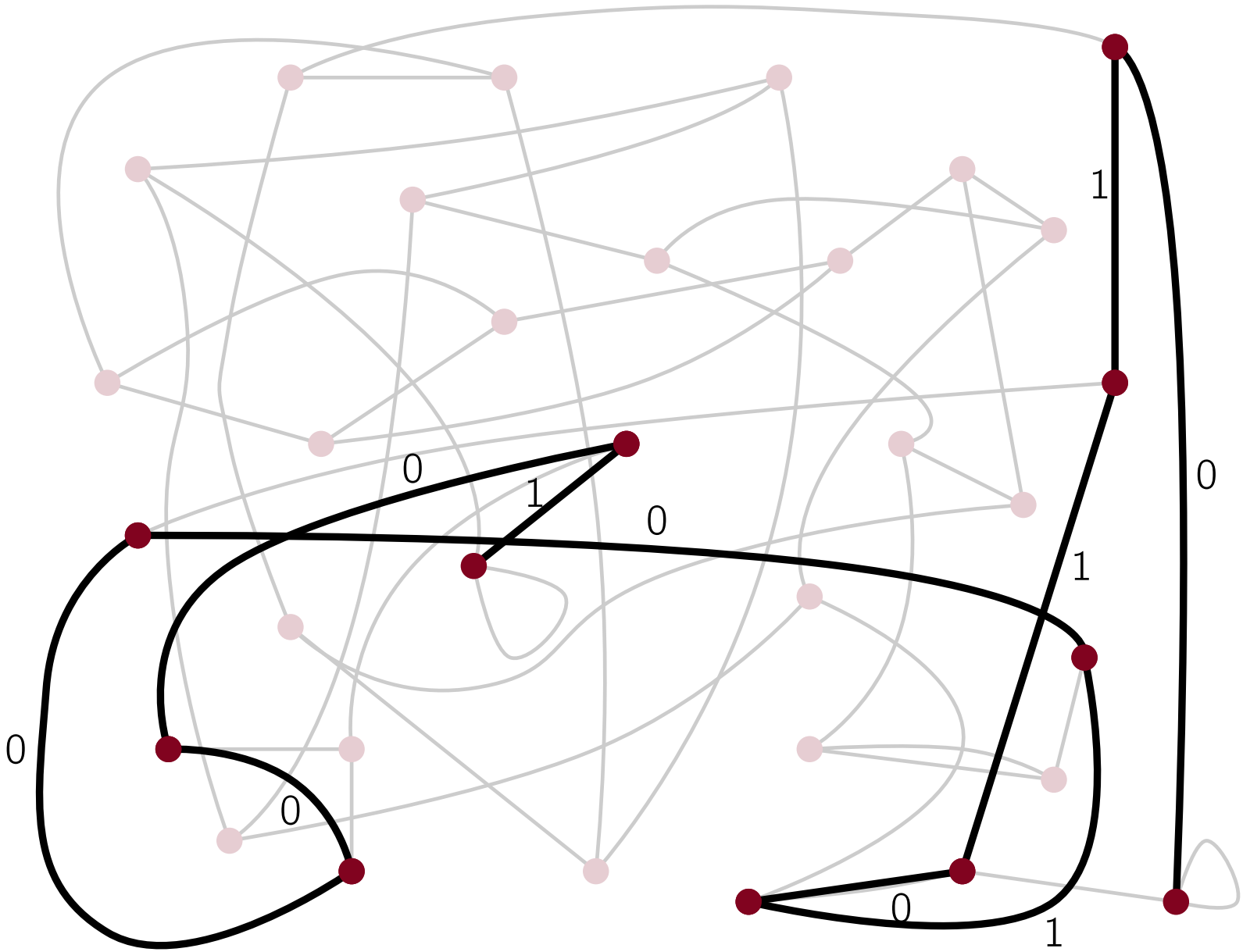
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



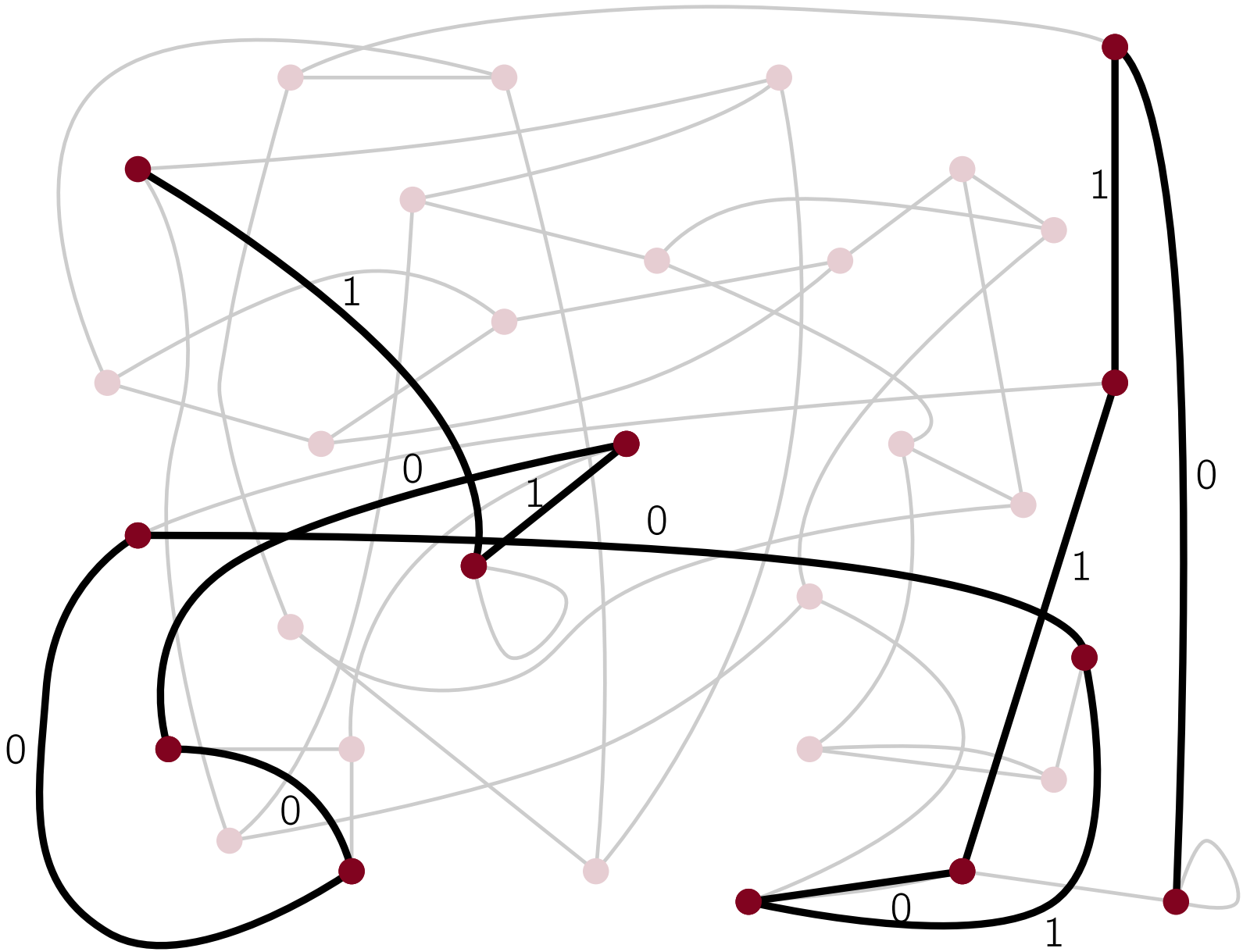
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



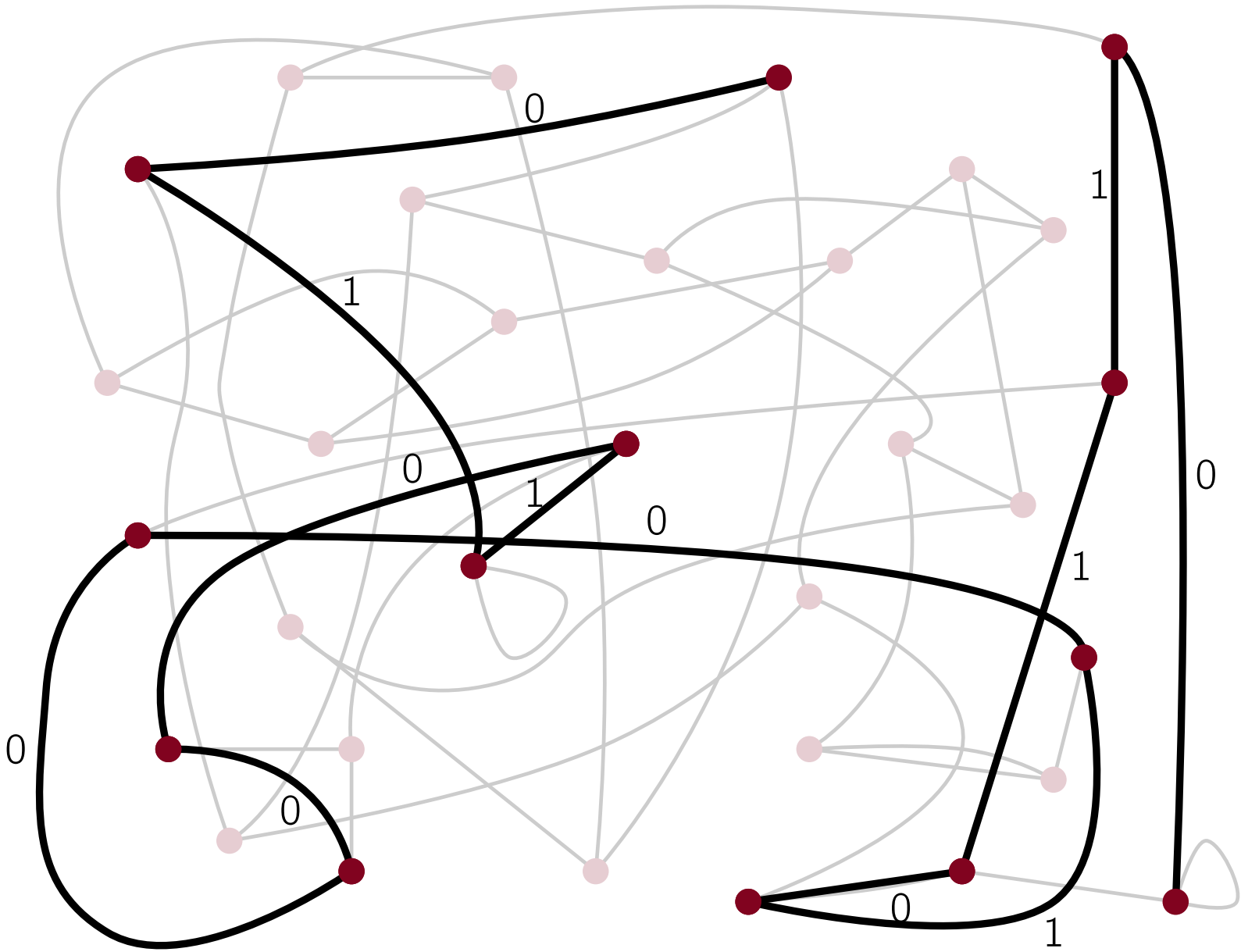
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



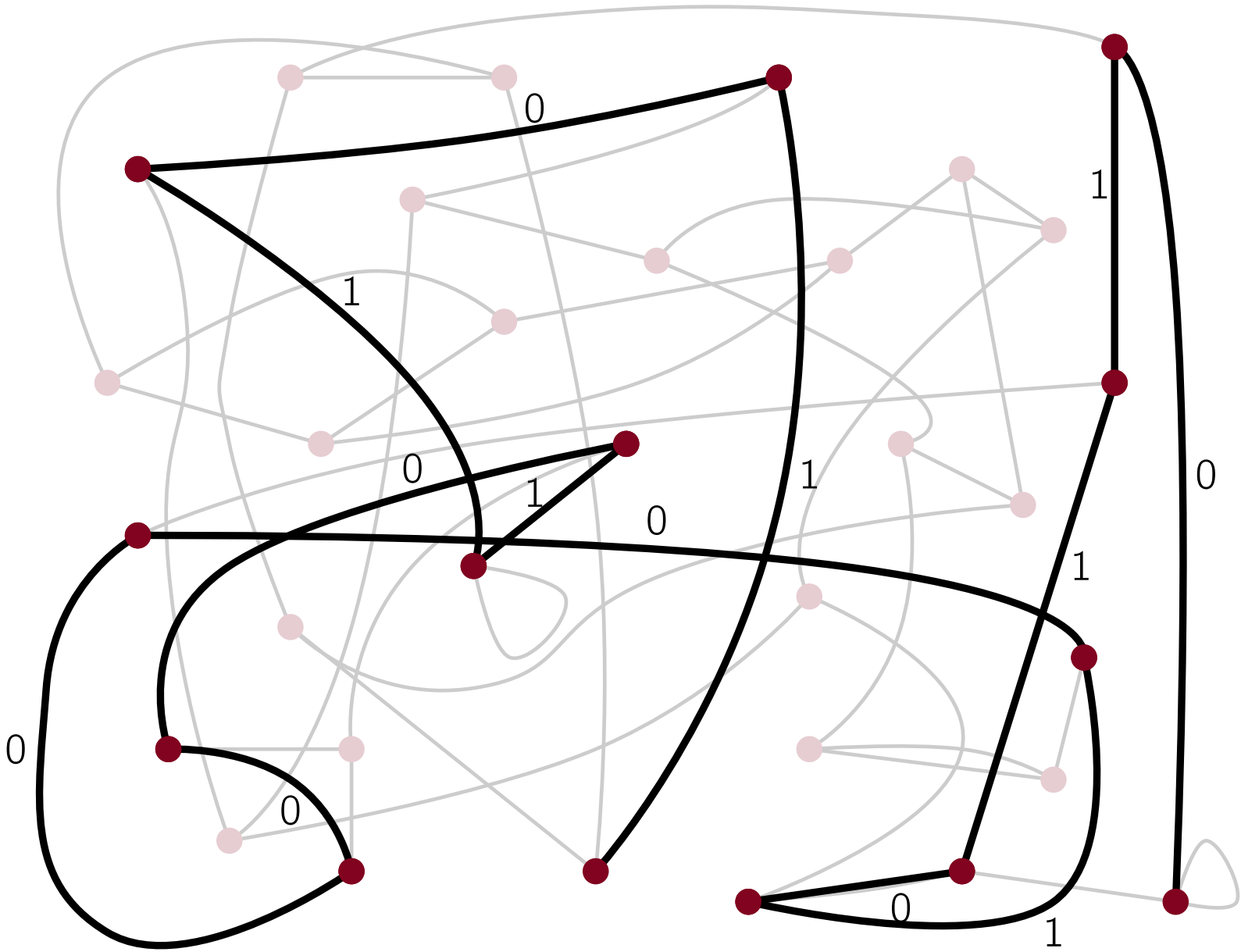
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



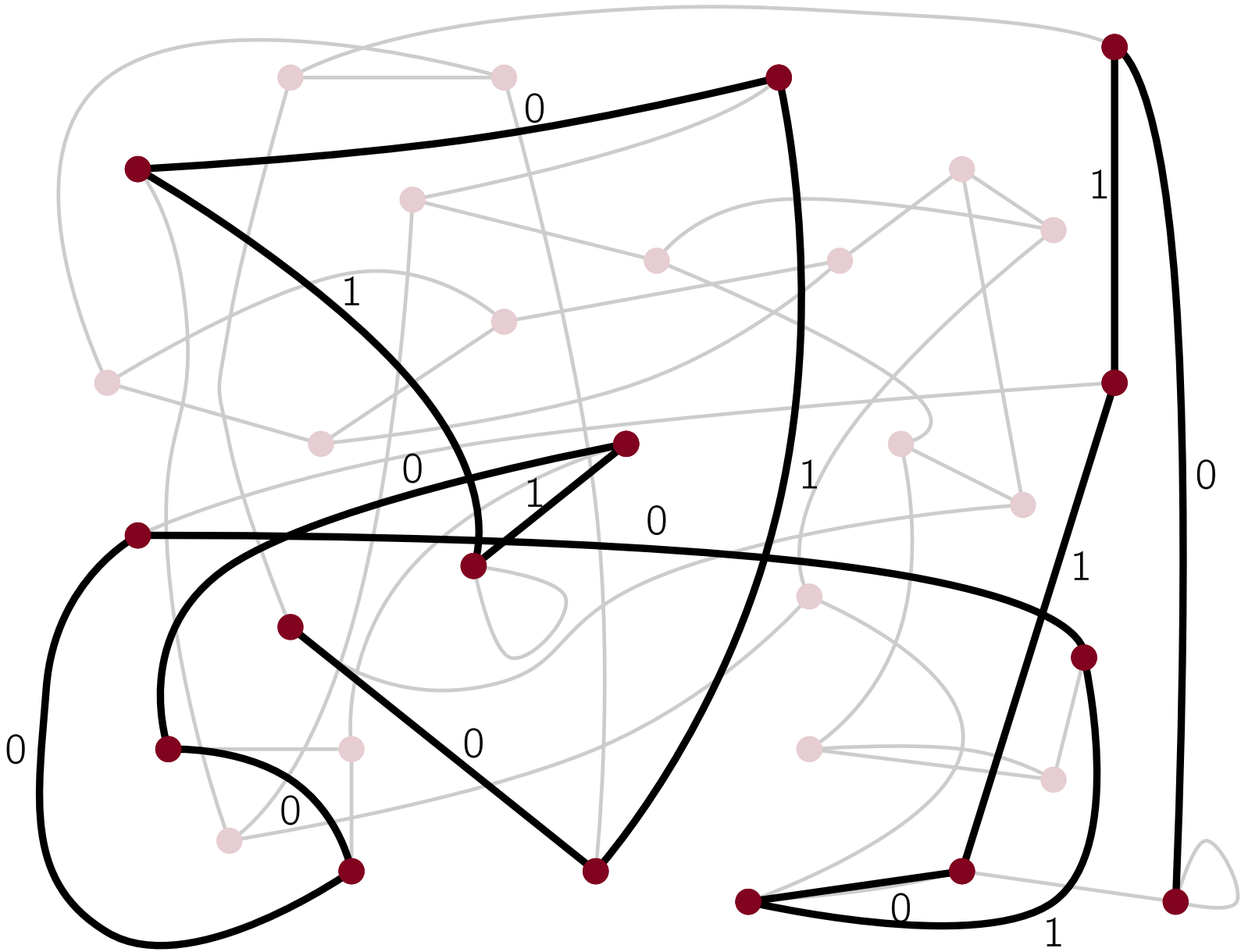
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



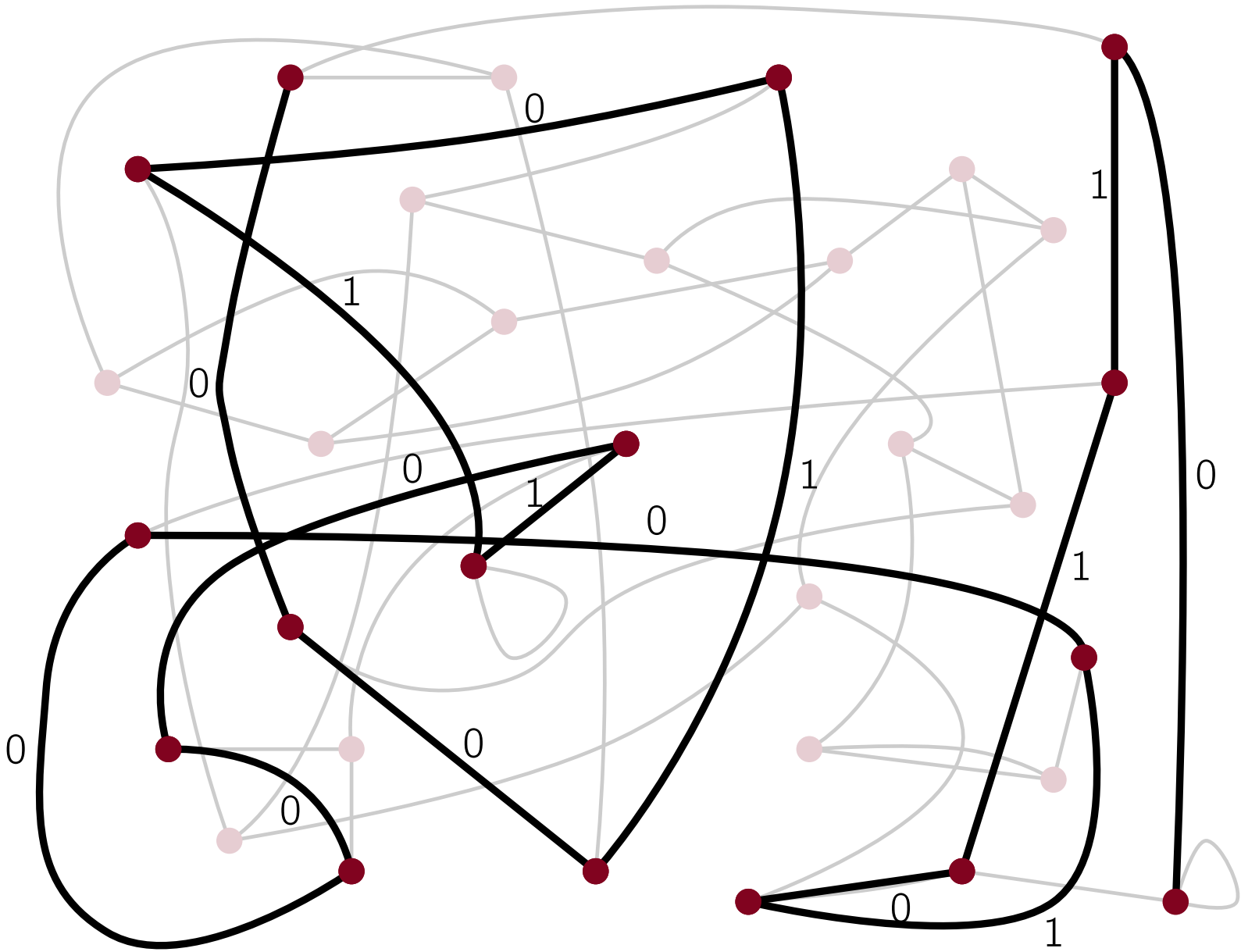
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



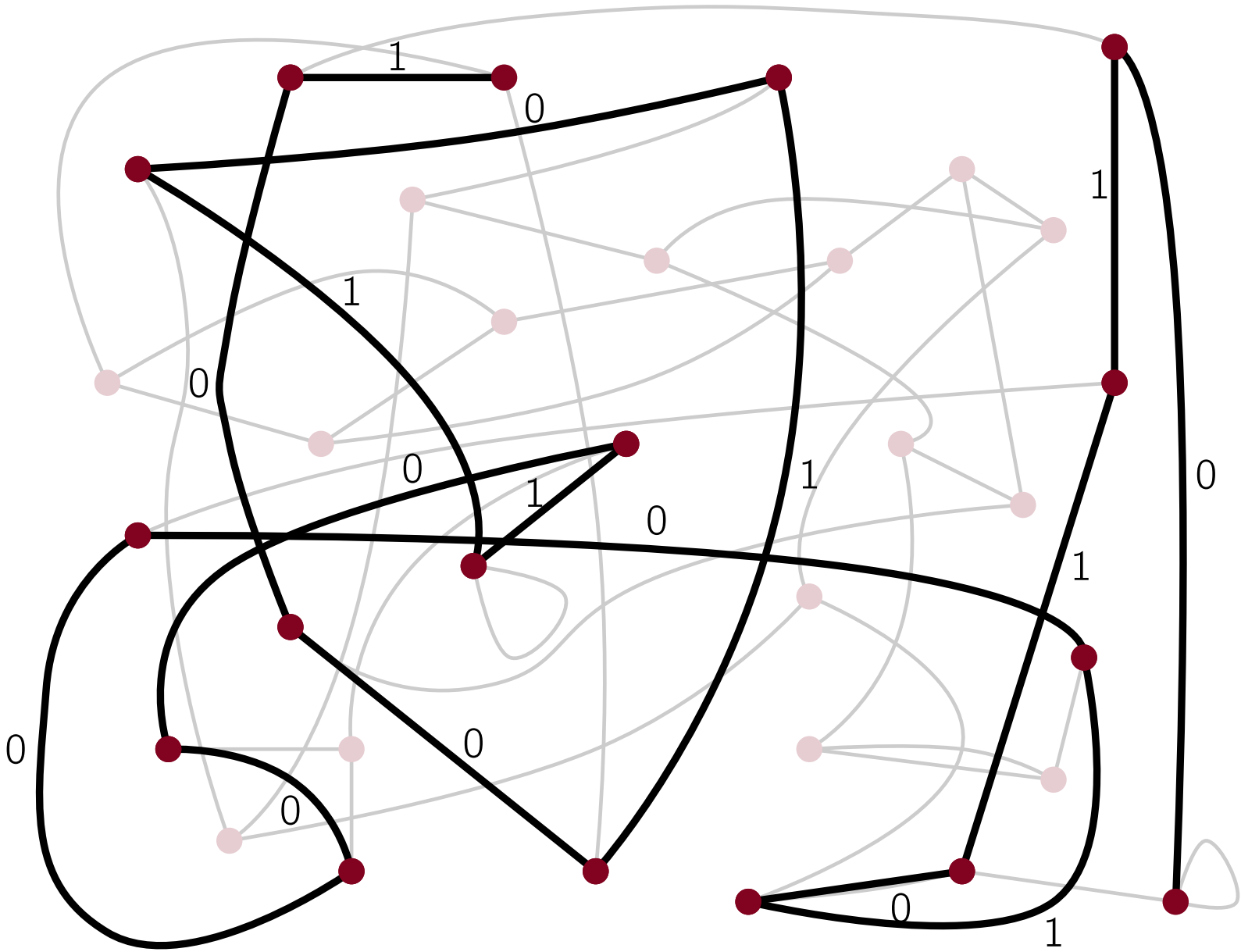
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



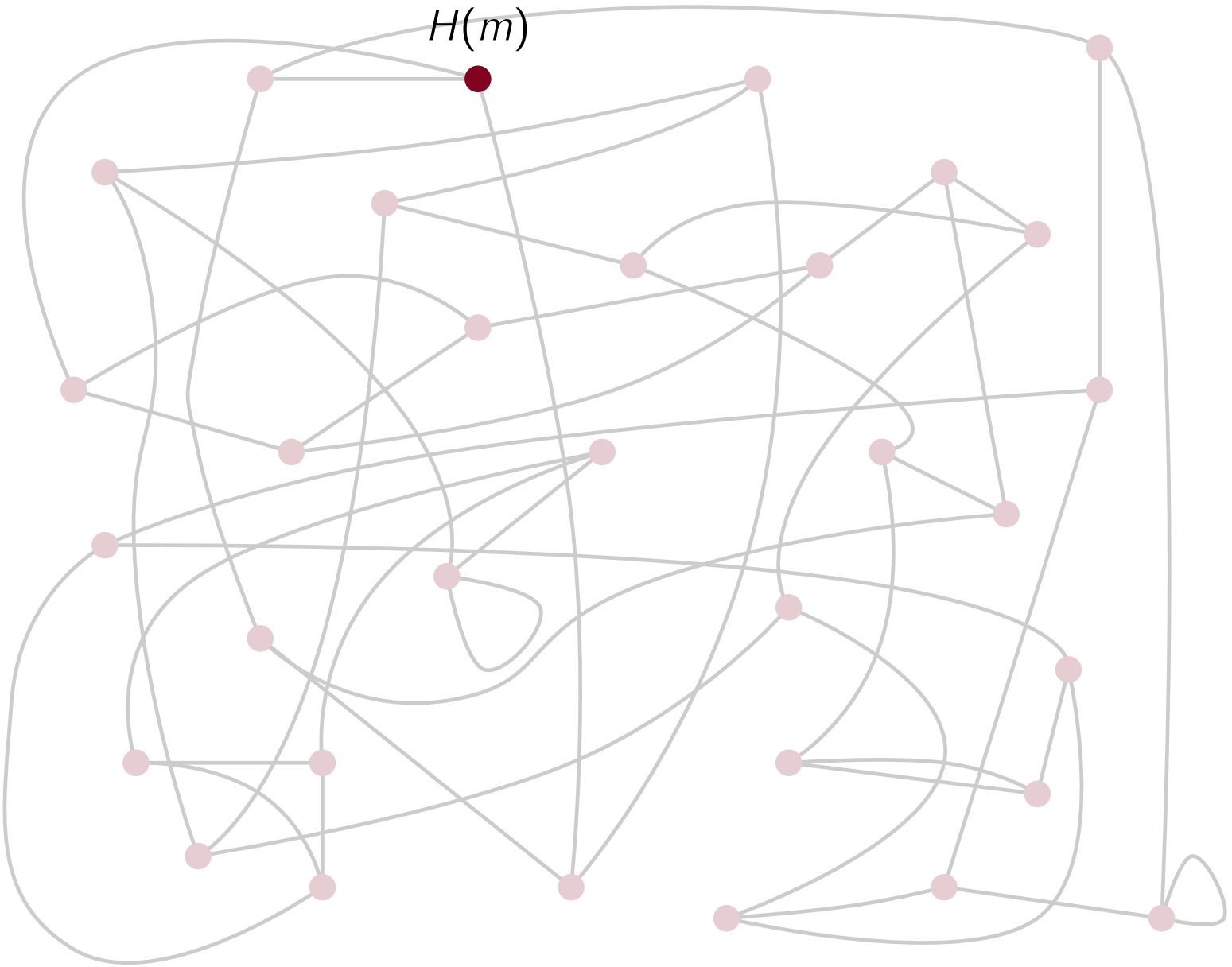
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006

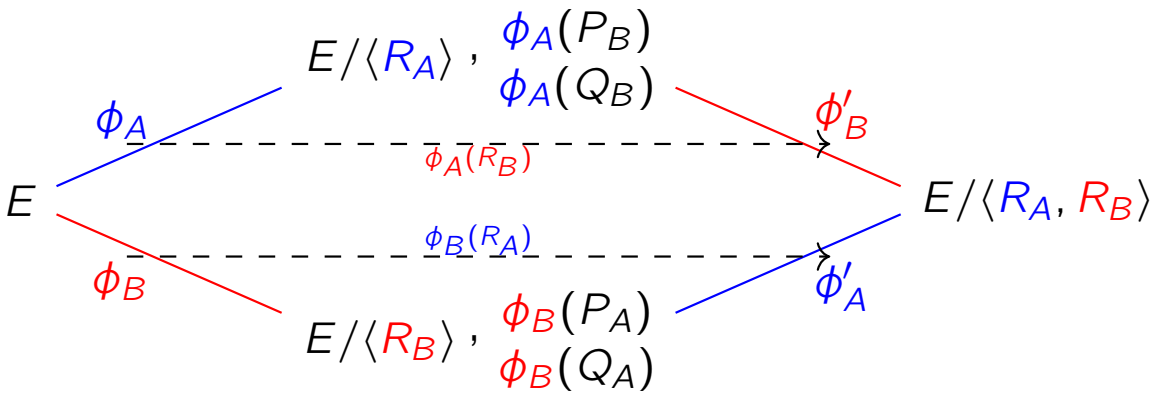


HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



Supersingular isogeny Diffie-Hellman

- Fix two small primes ℓ_A and ℓ_B;
- Choose a prime p such that $p+1 = \ell_A^a \ell_B^b f$ for a small correction term f;
- Pick a supersingular elliptic curve $E/\mathbb{F}_{p^2}$: $E\left(\mathbb{F}_{p^2}\right) \simeq \left(\frac{\mathbb{Z}}{(p+1)\mathbb{Z}}\right)^2$
- Alice consider $E\left[\ell_A^a\right] = \langle P_A, Q_A \rangle$ while Bob takes $E\left[\ell_B^b\right] = \langle P_B, Q_B \rangle$.
- **Secret Data:** $R_A = m_A P_A + n_A Q_A$ and $R_B = m_B P_B + n_B Q_B$.
- **Private Key:** isogenies $\phi_A : E \to E/\langle R_A \rangle$ and $\phi_B : E \to E/\langle R_B \rangle$.
- **Shared Data:** $E_A, \phi_A(P_B), \phi_A(Q_B)$ and $E_B, \phi_B(P_A), \phi_B(Q_A)$.
- **Shared Key:** $E/\langle R_A, R_B \rangle = E_B/\langle \phi_B(R_A) \rangle = E_A/\langle \phi_A(R_B) \rangle$.



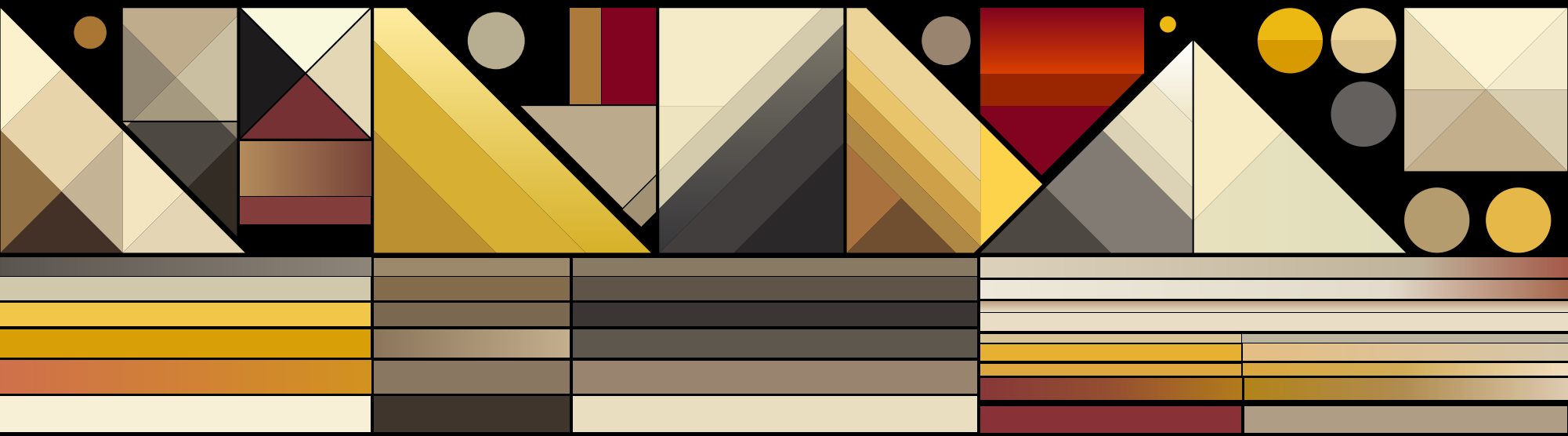
CSIDH - CASTRYCK, LANGE, MARTINDALE, PANNY & RENES, 2018

It is an adaptation of the Couveignes–Rostovtsev–Stolbunov scheme to supersingular elliptic curves.

Commutative Supersingular isogeny Diffie-Hellman

- Fix a prime $p = 4 \cdot \ell_1 \cdot \ldots \cdot \ell_t - 1$ for small distinct odd primes ℓ_i.
- The elliptic curve $E_0 : y^2 = x^3 + x/\mathbb{F}_p$ is supersingular and its endomorphism ring over $\mathbb{F}_p$ is $\mathcal{O} = \mathbb{Z}[\pi]$ (commutative).
- A supersingular Montgomery curve $E_A : y^2 = x^3 + Ax^2 + x/\mathbb{F}_p$ appear in the $\mathcal{Cl}(\mathcal{O})$-orbit of E_0.
- **Private Key:** it is an n-tuple of integers $(e_1, \ldots, e_t)$ sampled in a range $\{-m, \ldots, m\}$ representing an ideal class $[\mathfrak{a}] = [\mathfrak{l}_1^{e_1} \cdot \ldots \cdot \mathfrak{l}_t^{e_t}] \in \mathcal{Cl}(\mathcal{O})$ where $\mathfrak{l}_i = (\ell_i, \pi - 1)$.
- **Public Key:** The Montgomery coefficients A of the elliptic curve $E_A = [\mathfrak{a}] \cdot E_0 : y^2 = x^3 + Ax^2 + x$.
- **Shared Key:** If Alice and Bob have private key $(\mathfrak{a}, A)$ and $(\mathfrak{b}, B)$ then they can compute the shared key $E_{AB} = [\mathfrak{a}][\mathfrak{b}] \cdot E_0 = [\mathfrak{b}][\mathfrak{a}] \cdot E_0$.

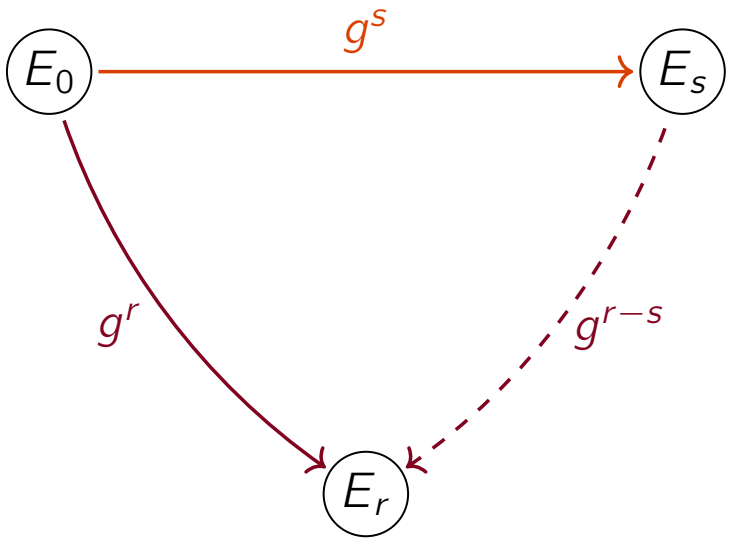
SIGNATURES



SEASIGN

SeaSign is built from the same commutative group-action framework used by CSIDH.

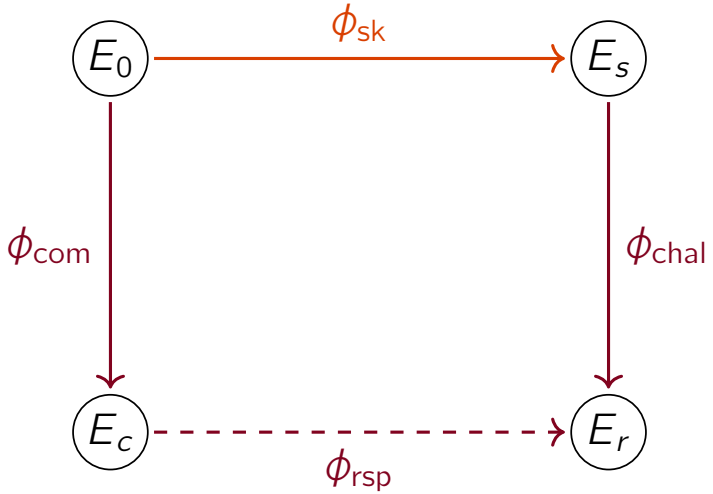
- A key pair (s, g^s).
- Commit to a random element g^r
- Challenge with bit $b \in \{0, 1\}$.
- Respond with $c = r - b \cdot s \bmod \#G$; Verify that $g^c(g^s)^b = g^r$.
- Does not leak because c is uniformly distributed and independent from s.
- Soundness error $1/2 \implies \lambda$ iterations



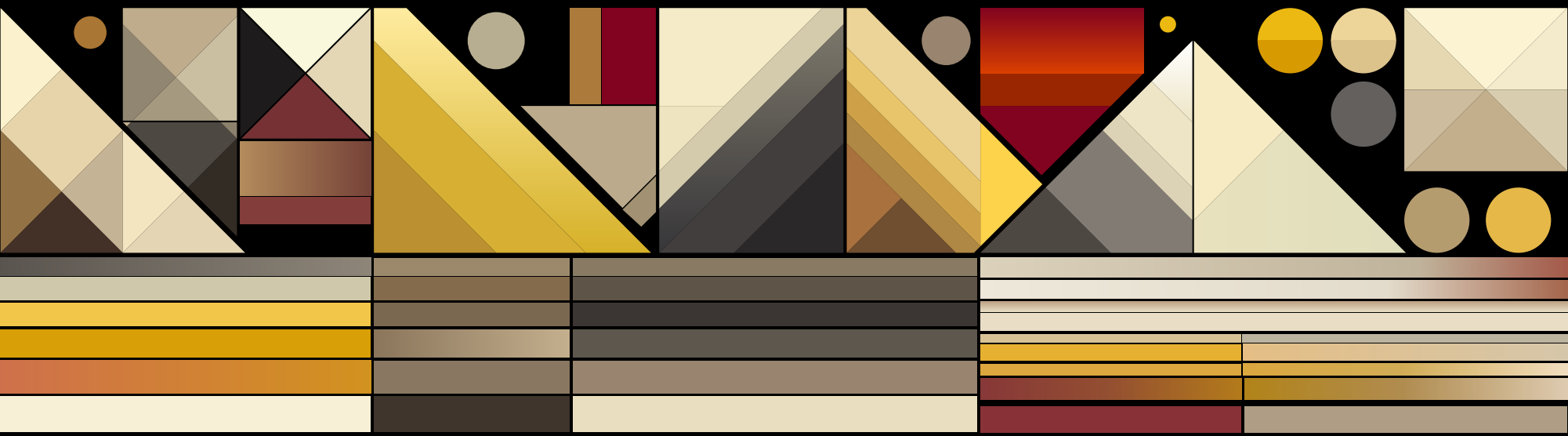
Conceptually it is very close to Schnorr signatures, but it is built from a commutative group action.

The idea is to translate everything into quaternion language.

- A large prime p.
- Special starting curve E_0.
- Sample $\phi_{\mathrm{sk}} : E_0 \to E_s$. pk is E_s.
- Commit to random ϕ_{com}.
- Challenge is a has and corresponds to ϕ_{chal}.
- On the quarternionic side use KLPT to generate ϕ_{rsp}
- Check on curves that it's all correct



HIGHER DIMENSION



KANIS THEOREM

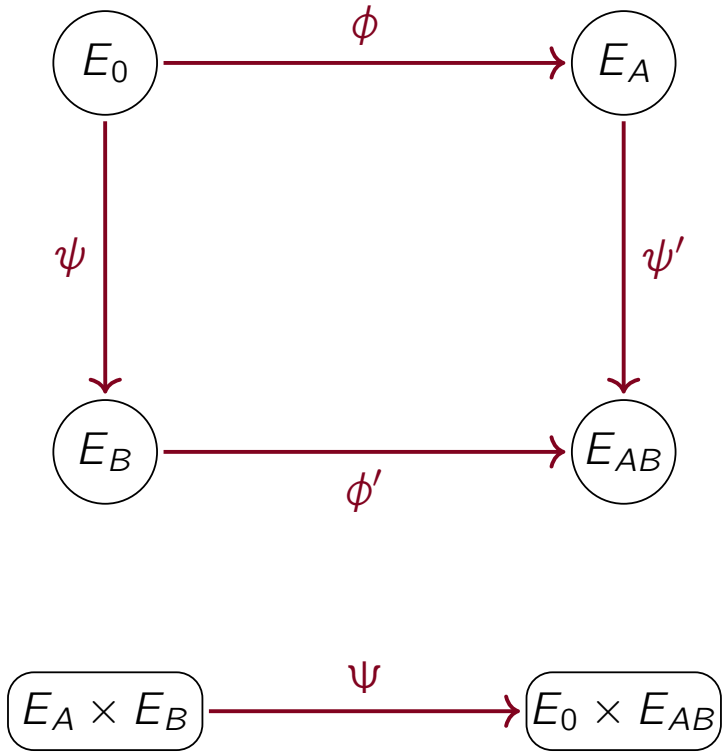
Given an isogeny diamond, there is an isogeny $\Psi : E_A \times E_B \to E_0 \times E_{AB}$ defined by

$$\Psi = \begin{pmatrix} \widetilde{\phi} & \widetilde{\psi'} \\ -\psi & \phi' \end{pmatrix}$$

Moreover, we have

$$\ker \Psi = \langle (\phi(P), \psi(P)) \mid P \in E_0[A+B] \rangle$$

.



- Kani's theorem turns compatible torsion information into a higher-dimensional isogeny;
- Breaks SIDH in polynomial time.

PEGASIS

Let $\mathcal{O}$ be an imaginary quadratic order. PEGASIS computes the class-group action

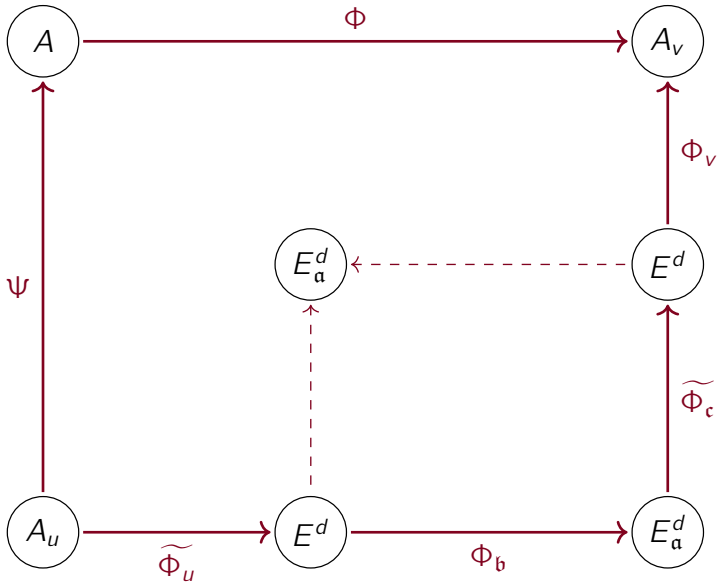
$$\mathrm{Cl}(\mathcal{O}) \times X \longrightarrow X, \qquad ([\mathfrak{a}], (E, \iota)) \longmapsto [\mathfrak{a}] * (E, \iota),$$

where X is a set of supersingular elliptic curves primitively oriented by $\mathcal{O}$.

- Find ideals in the same class: $[\mathfrak{b}] = [\mathfrak{c}] = [\mathfrak{a}]$.
- Find u, v such that $u\,N(\mathfrak{b}_k) + v\,N(\mathfrak{c}_k) = 2^e$ turning the computation into a smooth 2-power isogeny problem.
- Using Kani's construction, combine the two branches obtaining a 2^e-isogeny

$$A_u \times A_v \longrightarrow E_{\mathfrak{a}}^2 \times A$$

- Extract the resulting curve



OTHER CONSTRUCTIONS FROM KANI

Kani's construction provides a way to glue elliptic curves into higher-dimensional abelian varieties:

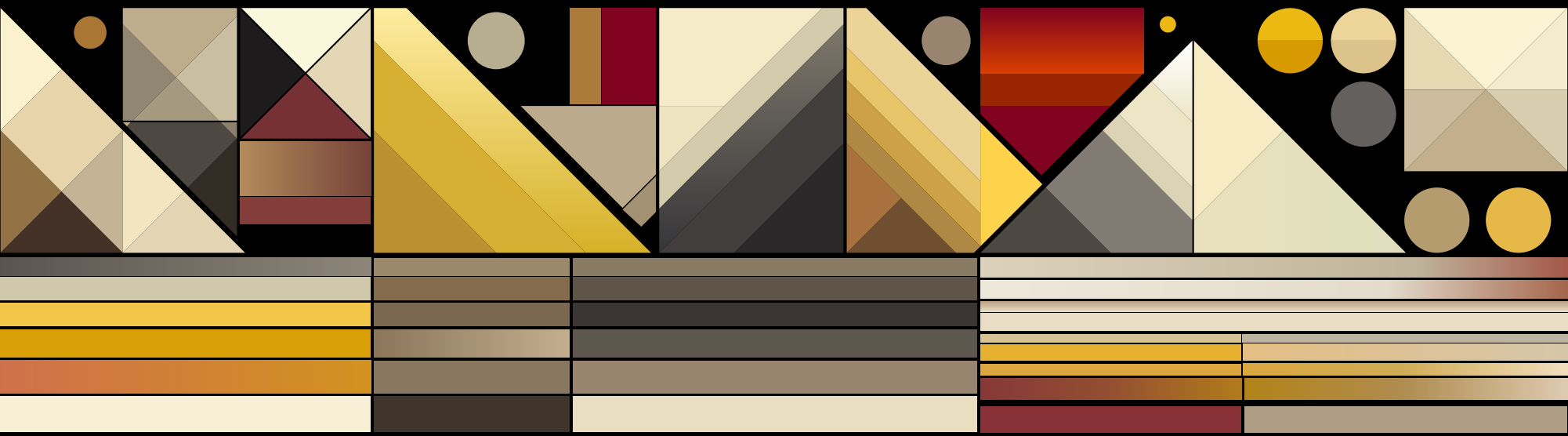
$$E_1 \times E_2 \longrightarrow A$$

and to construct explicit isogenies between products of elliptic curves.

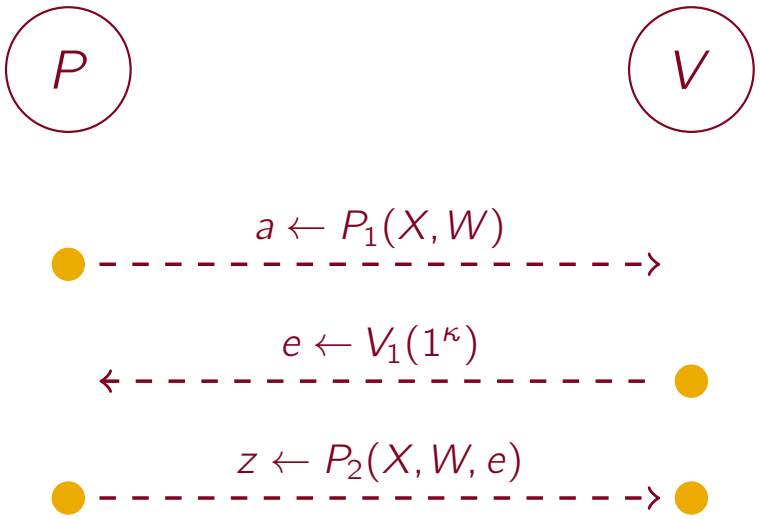
- **SQIsignHD:** Higher-dimensional generalization of SQIsign using isogenies between abelian varieties.
- **FESTA:** A post-quantum signature scheme.
- **POKE**
  Proofs Of Knowledge of Endomorphisms: zero-knowledge proofs using higher-dimensional isogeny diagrams.

Kani's theorem turns relations between elliptic curves into explicit higher-dimensional isogeny constructions.

ZERO KNOWLEDGE

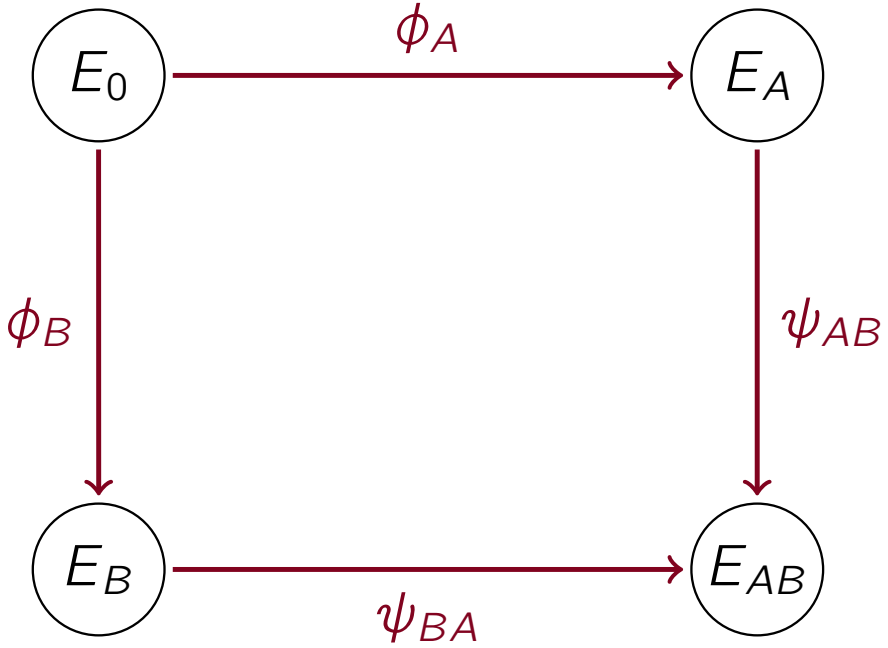


SIGMA-PROTOCOLS



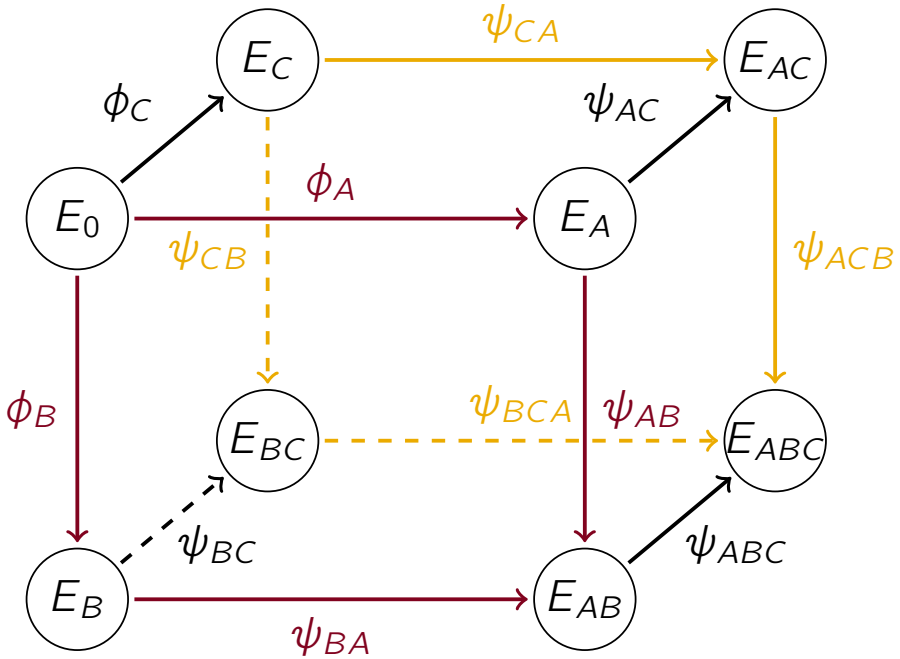
- **Correctness:** An honest prover with a valid witness always produces an accepting transcript.
- **Soundness:** A prover able to answer sufficiently many distinct challenges must encode a real witness.
- **ZK:** Each single opened view hides the witness because it can be simulated.

STATEMENT



- **Public curves:** E_0, E_A, E_B, E_{AB}
- **Public data:** Pairwise coprime A, B, C.
- **Witness:**
  a cyclic A-isogeny ϕ_A
  a cyclic B-isogeny ϕ_B
- **Idea**
  Hide the diamond behind a fresh random C-isogeny (translate it through ϕ_C)

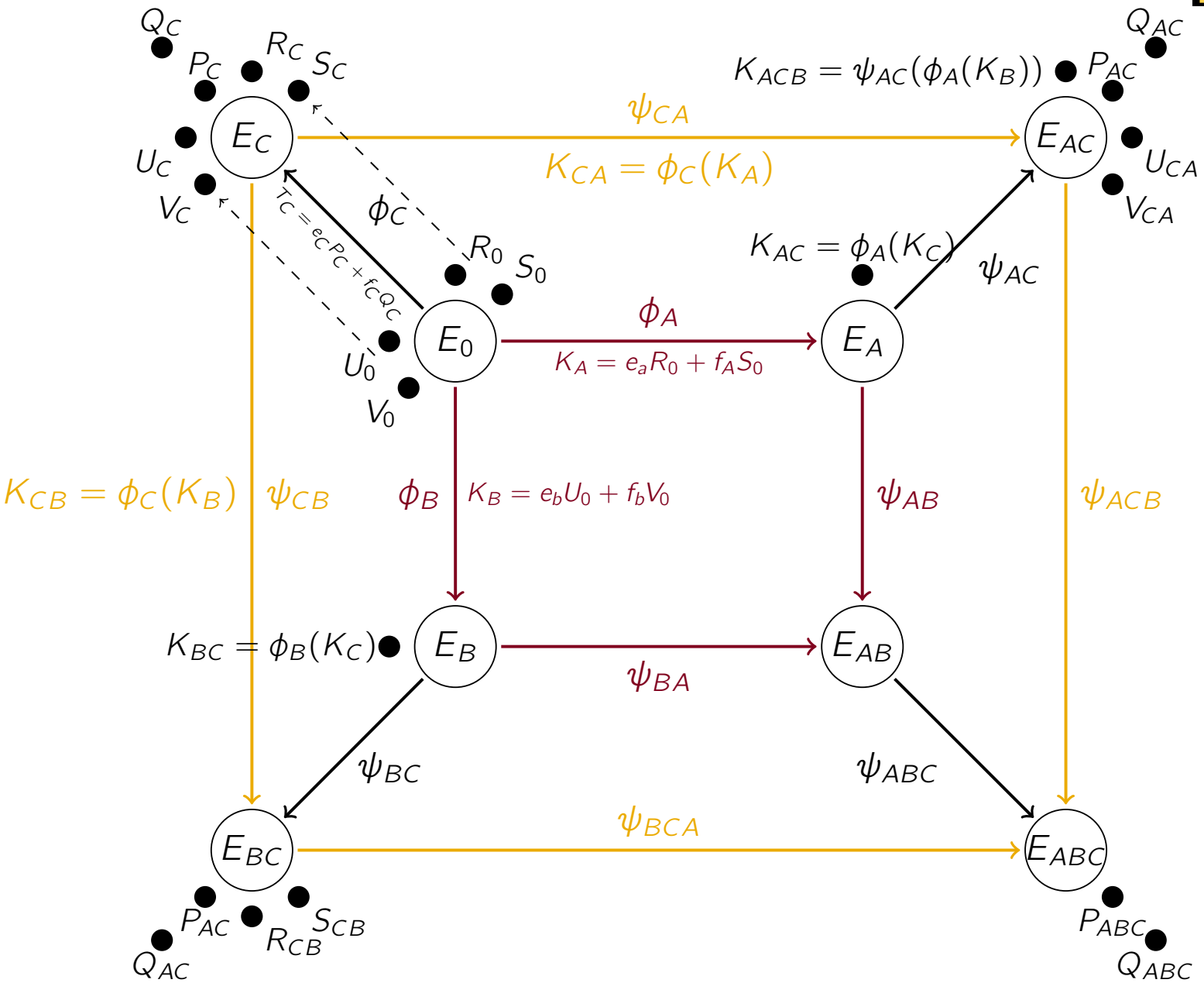
PUSHING THE DIAMOND



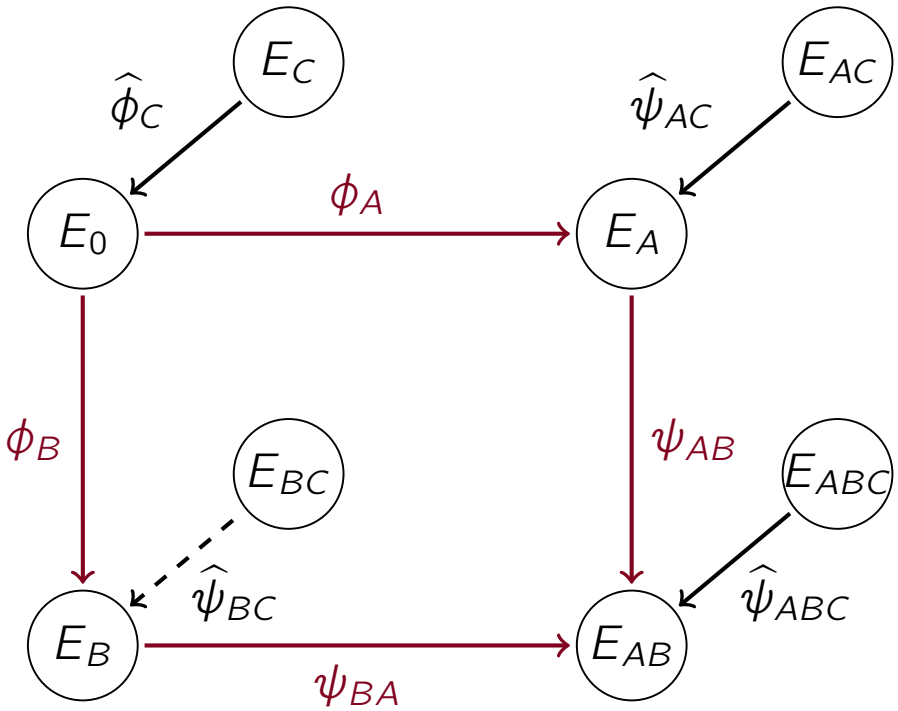
- Sample random cyclic C-isogeny ϕ_C and dual-kernel coordinates $\ker \widehat{\phi_C} = \langle T_C \rangle$
- Transport the A-kernel and B-kernel to E_C to form ψ_{CA} and ψ_{CB}.
- Transport the C-kernel through ϕ_A and ϕ_B to form ψ_{AC} and ψ_{BC}.
- Complete the back square by pushforward to E_{ABC}.

Front face = secret diamond Back face = randomized diamond

COMMITTMENT



CHALLENGES I - CASE 0,1,2,3



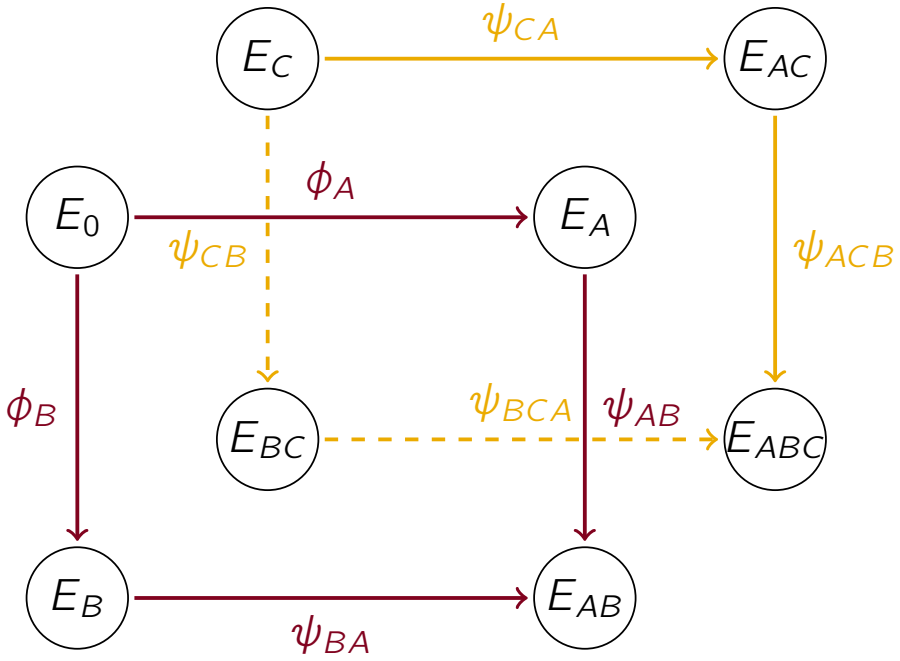
Prover reveals the data describing one of the dual isogenies $\widehat{\phi_C}, \widehat{\phi_{AC}}, \widehat{\phi_{BC}}$ or $\widehat{\phi_{ABC}}$.

- reveals E_{*C}, the basis $E_{*C}[C] = \langle P_*, Q_* \rangle$, the integers e_c, f_C.

Verifiers

- checks committed hashes.
- reconstructs the C-kernel from the committed coordinates.
- check codomain.

CHALLENGES II - CASE 4,5,6,7



Prover reveals the data describing one of the sogenies $\psi_{CA}, \psi_{CB}, \psi_{ACB}$ or ψ_{BCA}.

- opens domain and codomain.
- opens basis for some of the A, B and C torsion for both.

Verifiers

- checks kernel coordinates.
- checks torsion images.

SECURITY PICTURE

L.COLÒ UWAT

Proposition 1

Cube-ZKP is correct.

Proposition 2

Given that the hash function used is computationally binding, Cube-ZKP is 8-sound.

- Soundness is equivalent to "the cube glues together": the opened edges force one front diamond.

Proposition 3

Given a statistically hiding hash function, Cube-ZKP is computationally zero-knowledge assuming DSSP is secure for $d = C$ and $N = \max\{A, B\}$

THANK YOU FOR THE ATTENTION

