Isogeny-based cryptography

A biased introduction

Benjamin Wesolowski, CNRS and ENS de Lyon

29 April 2024, CAIPI Symposium, Rennes, France

Isogenies

Elliptic curves, isogenies, isogeny graphs

Elliptic curves

Elliptic curve over $\mathbb{F}_q$: solutions (x,y) in $\mathbb{F}_q$ of

$$y^2 = x^3 + ax + b$$

$E(\mathbb{F}_q)$ is an additive group

Isogeny: a map

$$\varphi : E_1 \to E_2$$

which preserves certain structures...

- Group **homomorphism** with **finite kernel**

Degree: $\deg(\varphi) = \#\ker(\varphi)$ (for "separable" isogenies)

- $\deg(\varphi \circ \psi) = \deg(\varphi) \cdot \deg(\psi)$

The isogeny problem

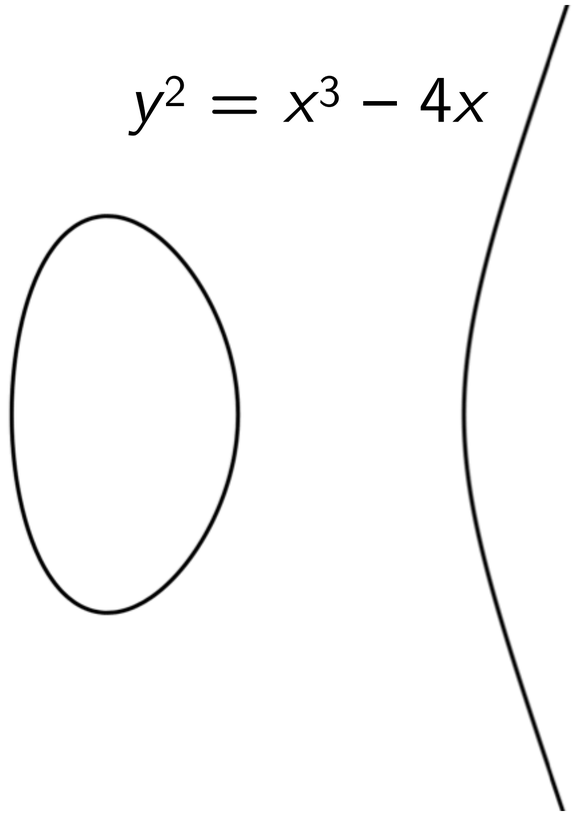
Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

$y^2 = x^3 + x$

elliptic curves:

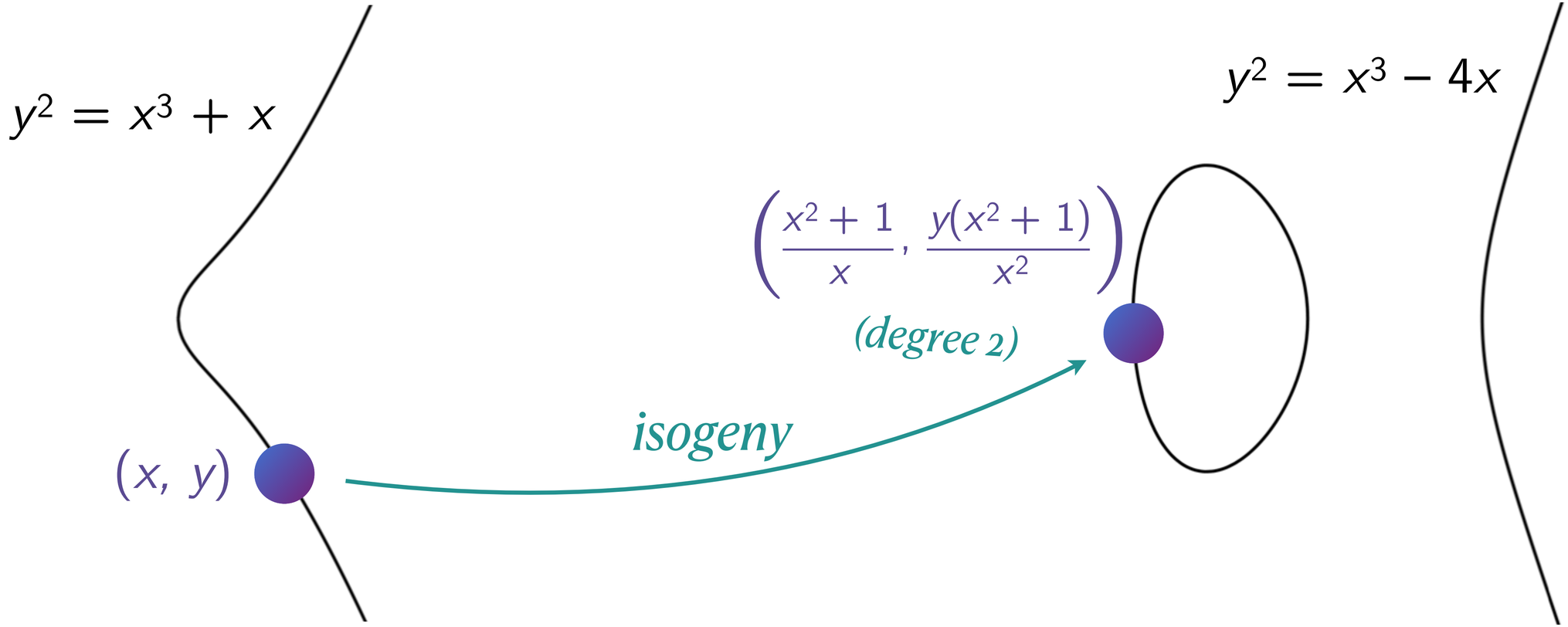
$y^2 = x^3 + ax + b$

$y^2 = x^3 - 4x$



The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$



The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

- Cryptosystems "based on" the isogeny problem?

Expectations: cryptosystems as secure as isogeny problem is hard

The isogeny problem = **Security of cryptosystems**

Hard even for quantum algorithms

Post-quantum cryptography

The isogeny problem

Isogeny problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?

Efficient isogenies

- Explicit polynomial formula, or Vélu's formulae... polynomial time in deg(φ)
  - ✓ Isogenies of *small* degree $\ell = 2$, or 3... "ℓ-isogenies"

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

(degree 2)

Efficient isogenies

- Explicit polynomial formula, or Vélu's formulae… polynomial time in deg(φ)

  ✓ Isogenies of *small* degree $\ell = 2$, or 3… "ℓ-isogenies"

- Given random E_1 and E_2, smallest $\varphi : E_1 \to E_2$ has degree poly(p)

  ✗ Typically in crypto, $p > 2^{256}$

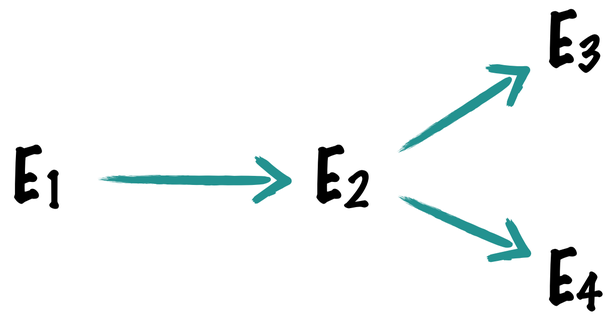
- Compose small isogenies to build bigger ones!

  ✓ Isogenies with **smooth degree** (small prime factors):

  $\varphi_n \circ \ldots \circ \varphi_2 \circ \varphi_1$ represented by ('compose', φ_1, φ_2,… , φ_n), with deg(φ_i) small

Isogeny graph

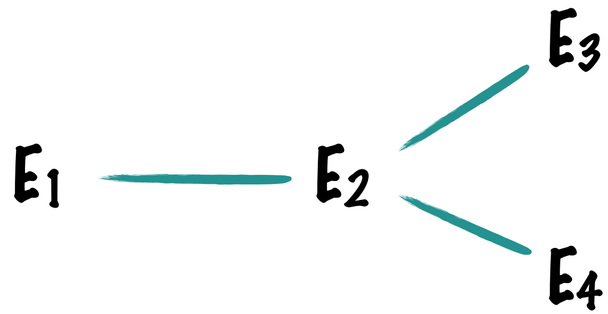
- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies



an isogeny of degree ℓ = an edge in a graph

Isogeny graph

- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies

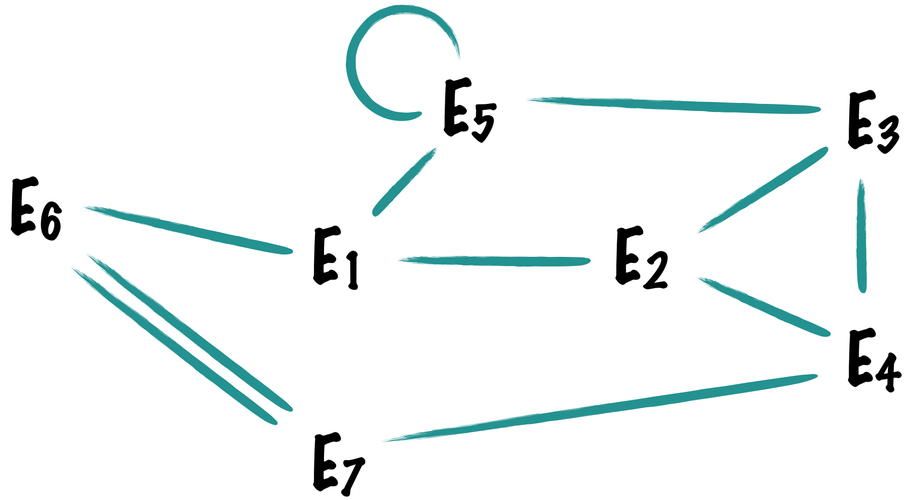


an isogeny of degree ℓ = an edge in a graph

$\exists$ ℓ-isogeny $E_1 \to E_2 \Rightarrow \exists$ ℓ-isogeny $E_2 \to E_1$

Isogeny graph

- Fix small ℓ (say, $\ell = 2$). Can easily compute ℓ-isogenies
- **The ℓ-isogeny graph** (supersingular...)



- (ℓ + 1)-regular, **connected** (for supersingular curves)

The ℓ-isogeny path problem

ℓ-IsogenyPath: Given E_1 and E_2, find an ℓ-isogeny path from E_1 to E_2

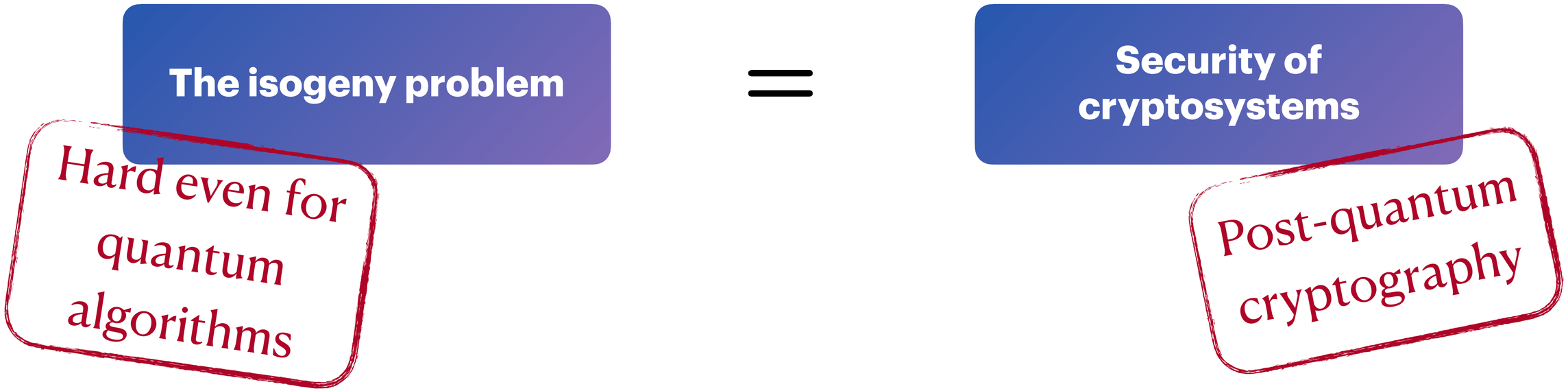
- Path finding in a graph
- Hard for supersingular curves! Best known algorithm = generic graph algorithm
- Typical meaning of ***"the isogeny problem"***

Isogeny-based cryptography

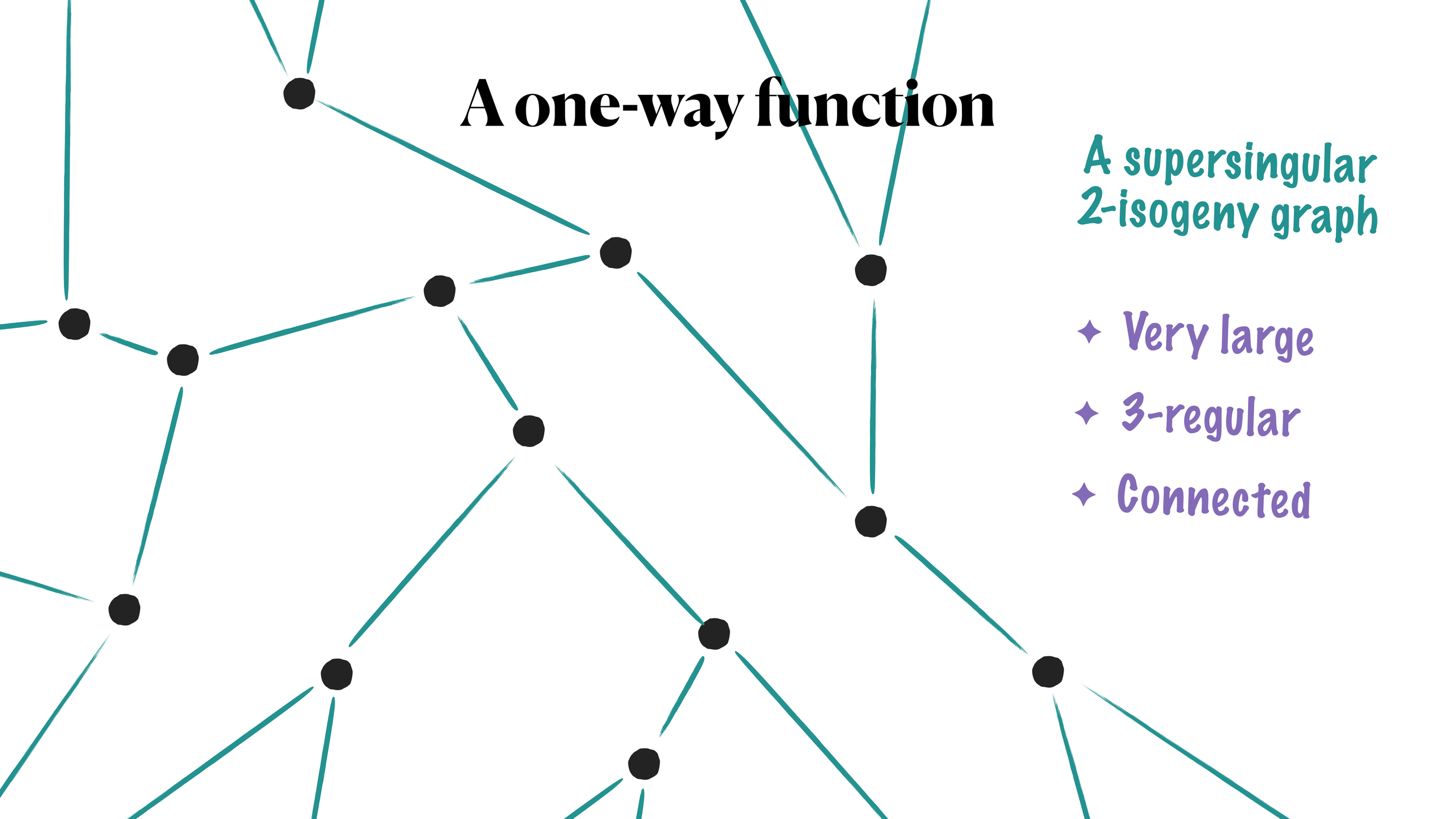
Computational problems and cryptosystems

Isogeny-based cryptography

Expectations: cryptosystems as secure as isogeny problem is hard



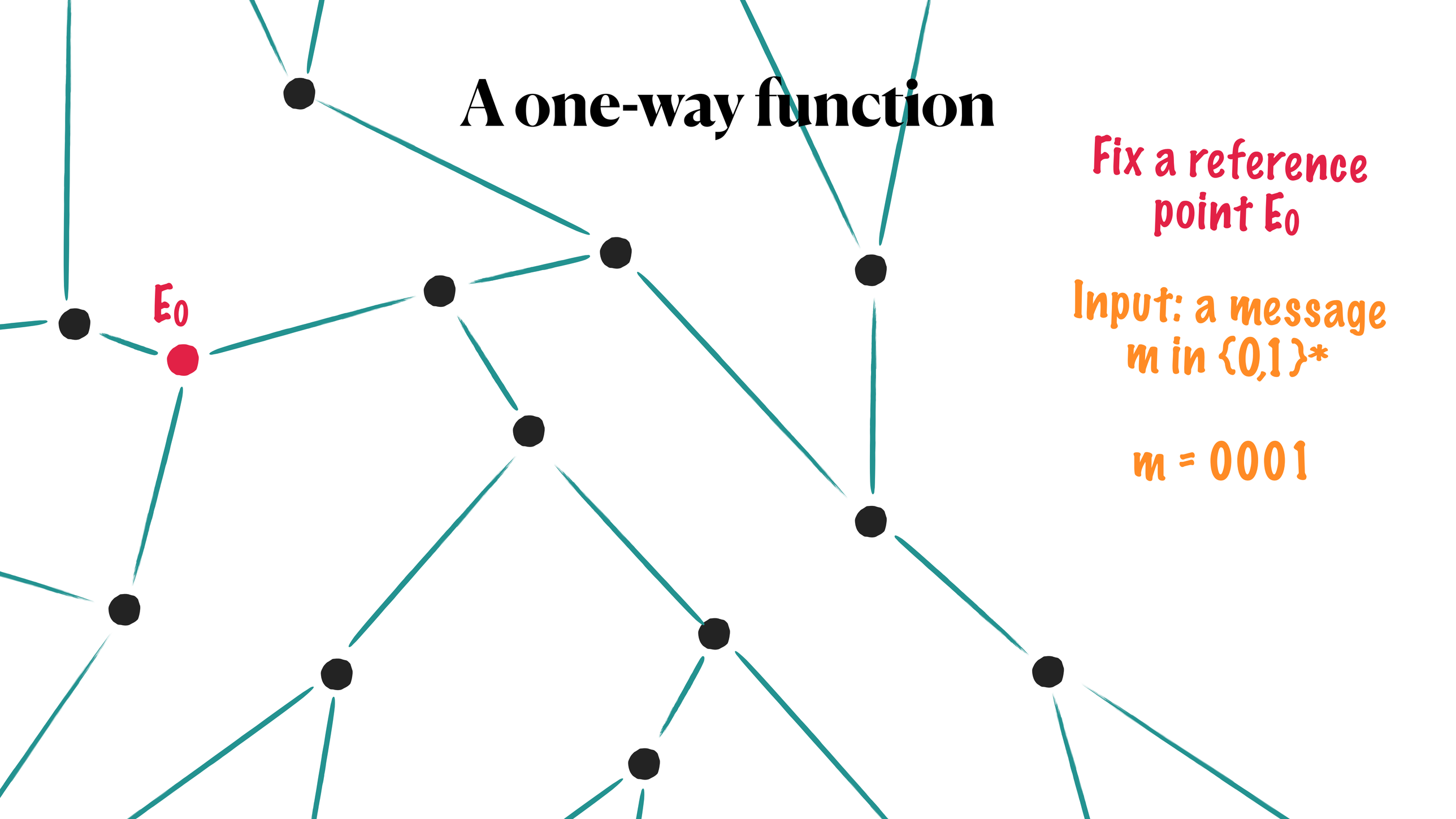
A one-way function



A supersingular 2-isogeny graph

- Very large
- 3-regular
- Connected

A one-way function

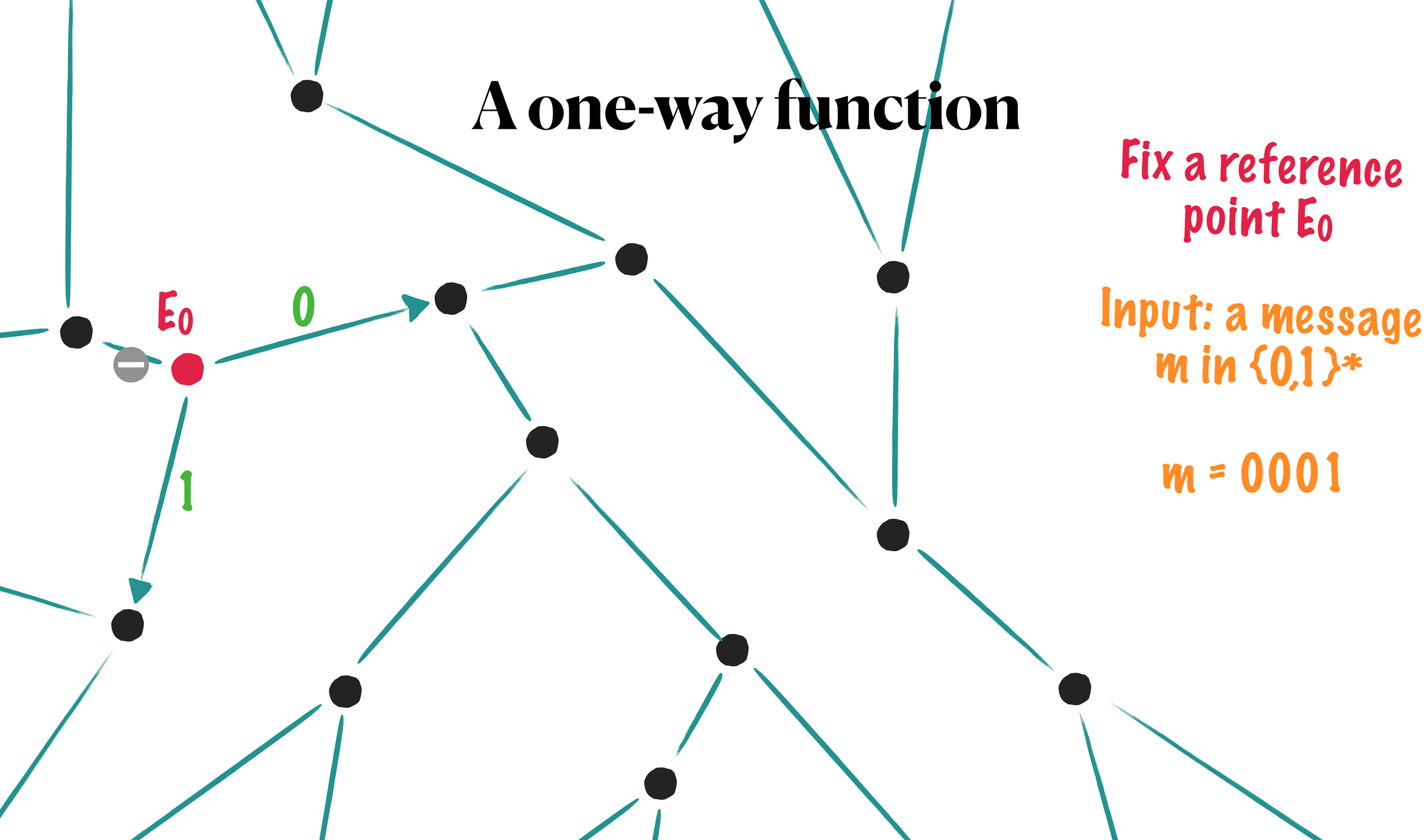


Fix a reference point E_0

Input: a message m in $\{0,1\}^*$

m = 0001

A one-way function

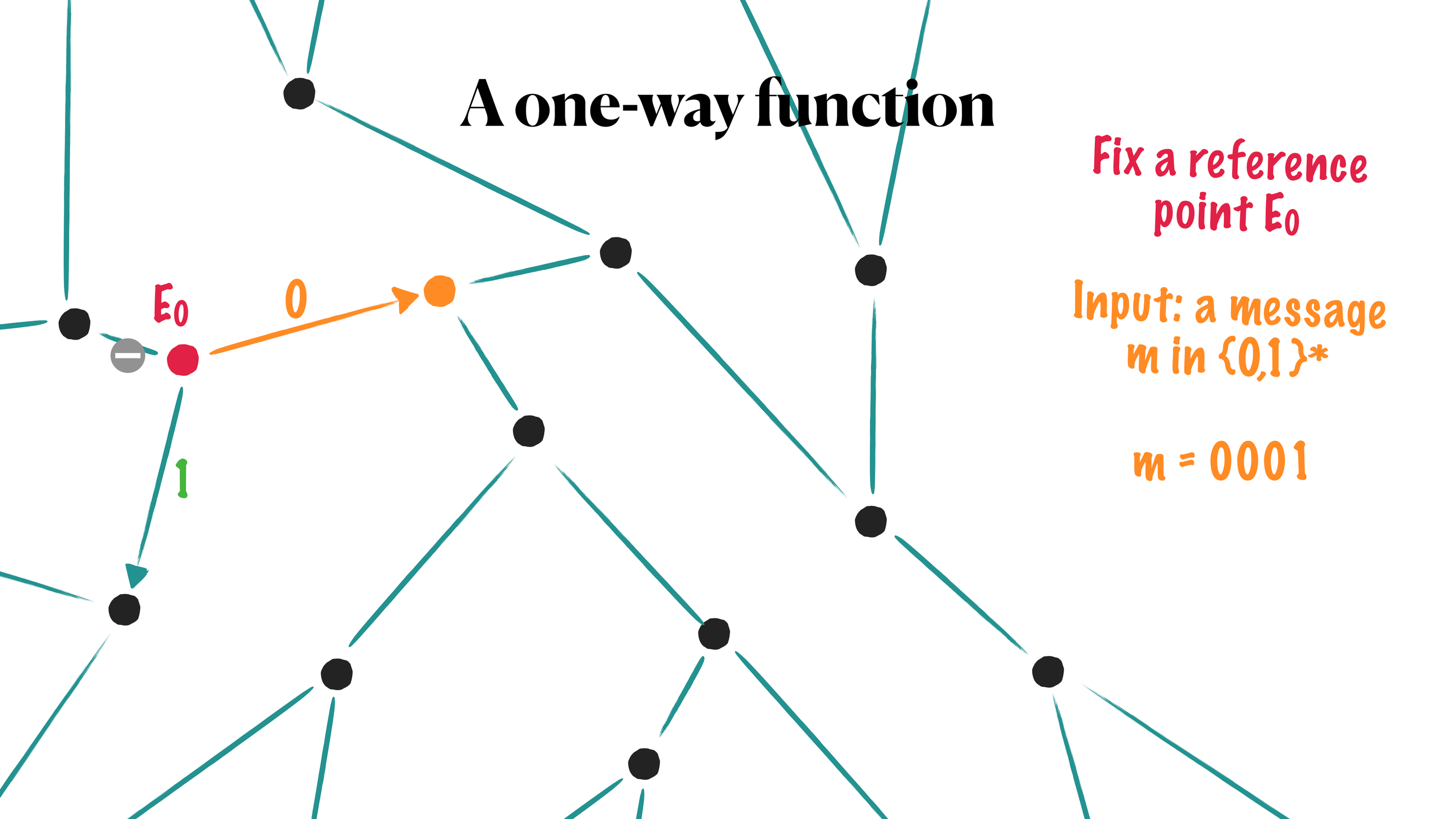


Fix a reference point E_0

Input: a message m in $\{0,1\}^*$

m = 0001

A one-way function

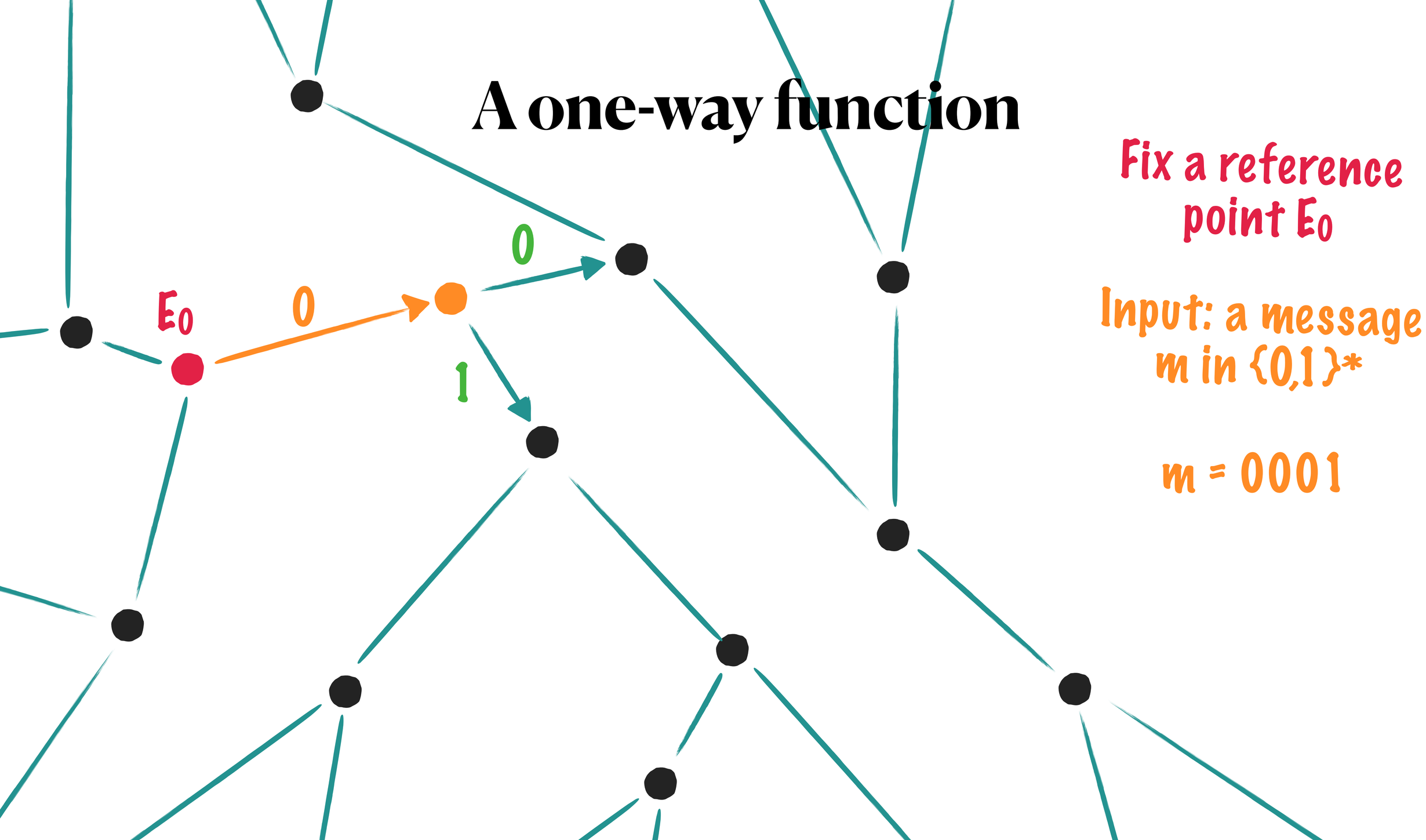


Fix a reference point E_0

Input: a message m in {0,1}*

m = 0001

A one-way function

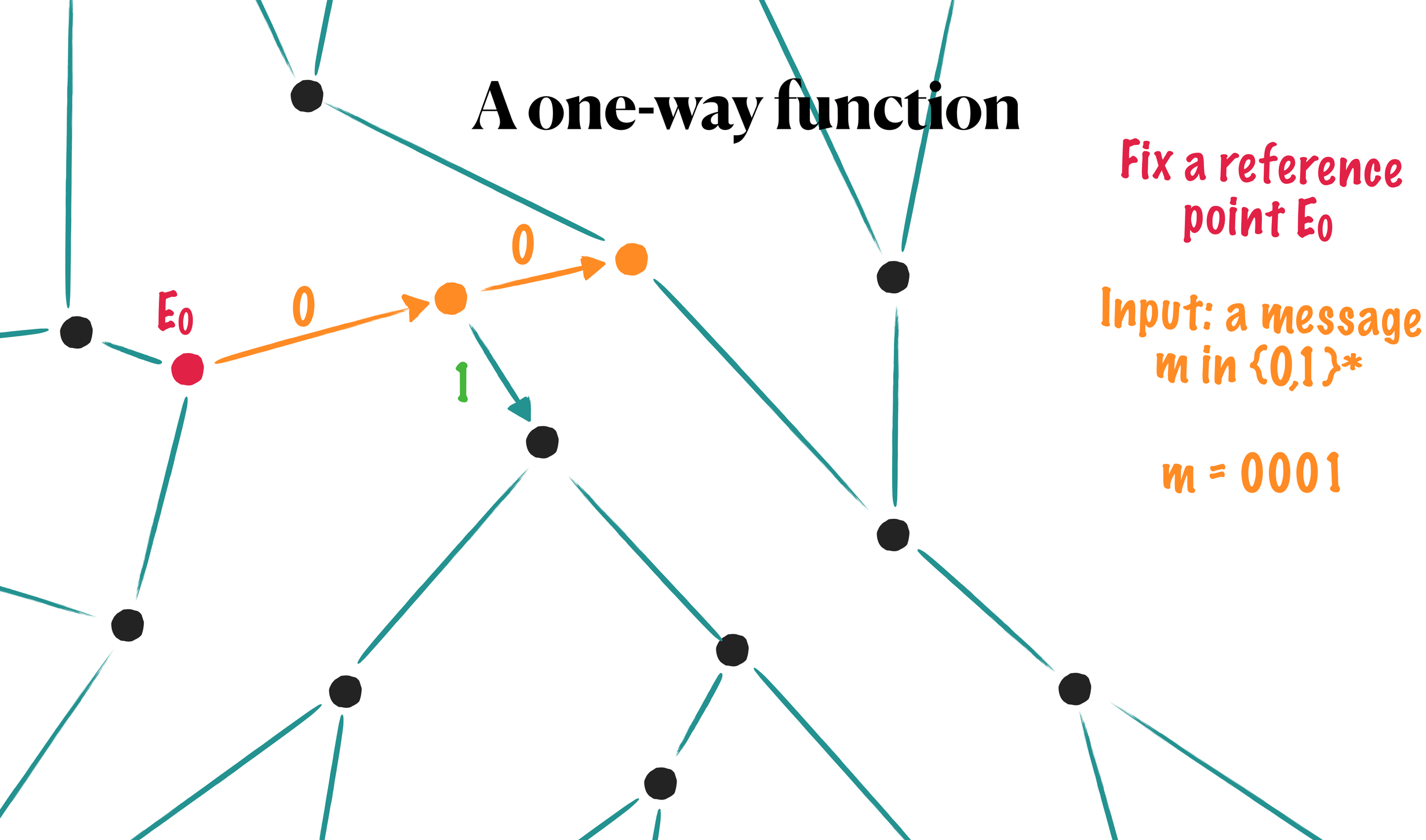


Fix a reference point E_0

Input: a message m in {0,1}*

m = 0001

A one-way function

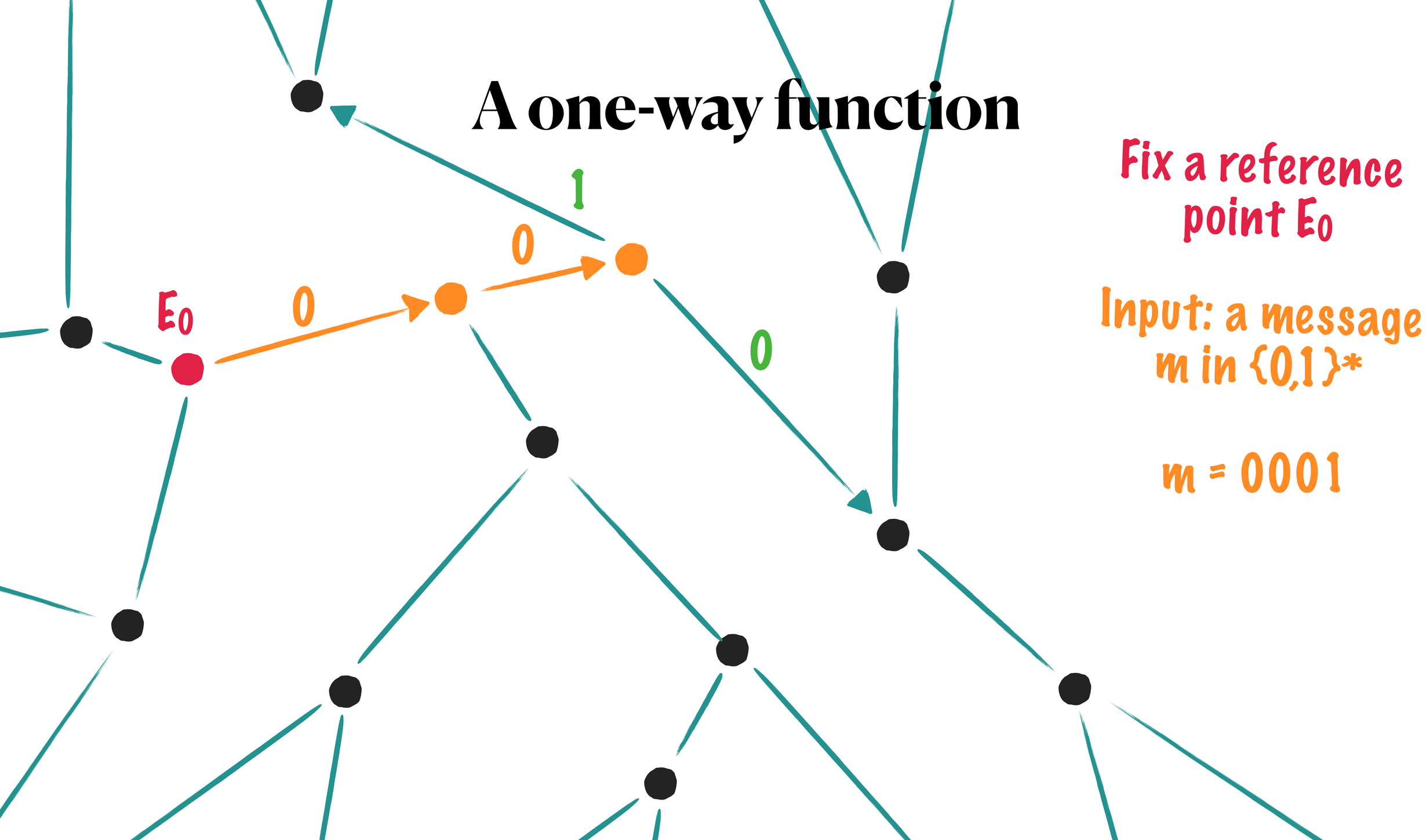


Fix a reference point E_0

Input: a message m in {0,1}*

m = 0001

A one-way function

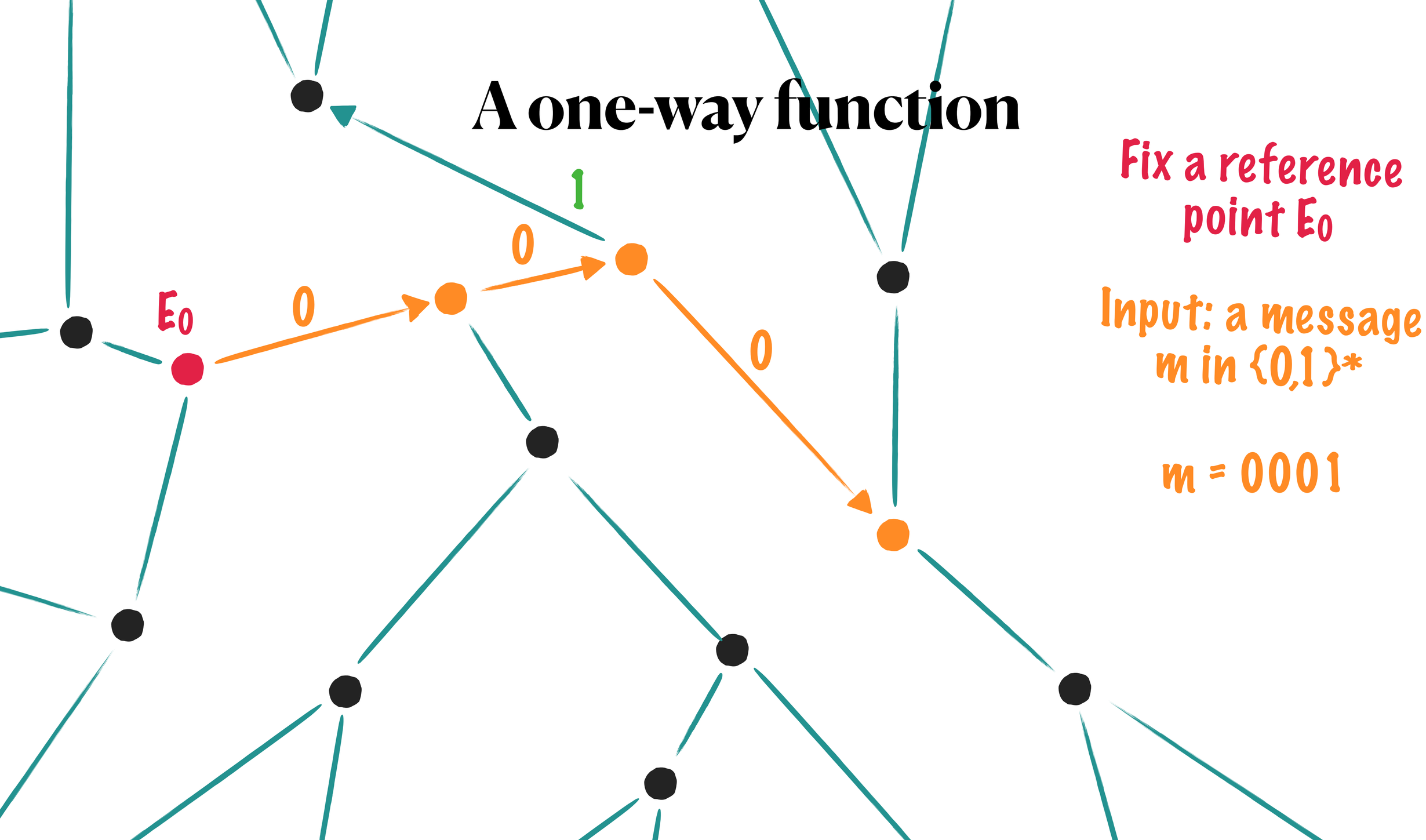


Fix a reference point E_0

Input: a message m in $\{0,1\}^*$

$m = 0001$

A one-way function

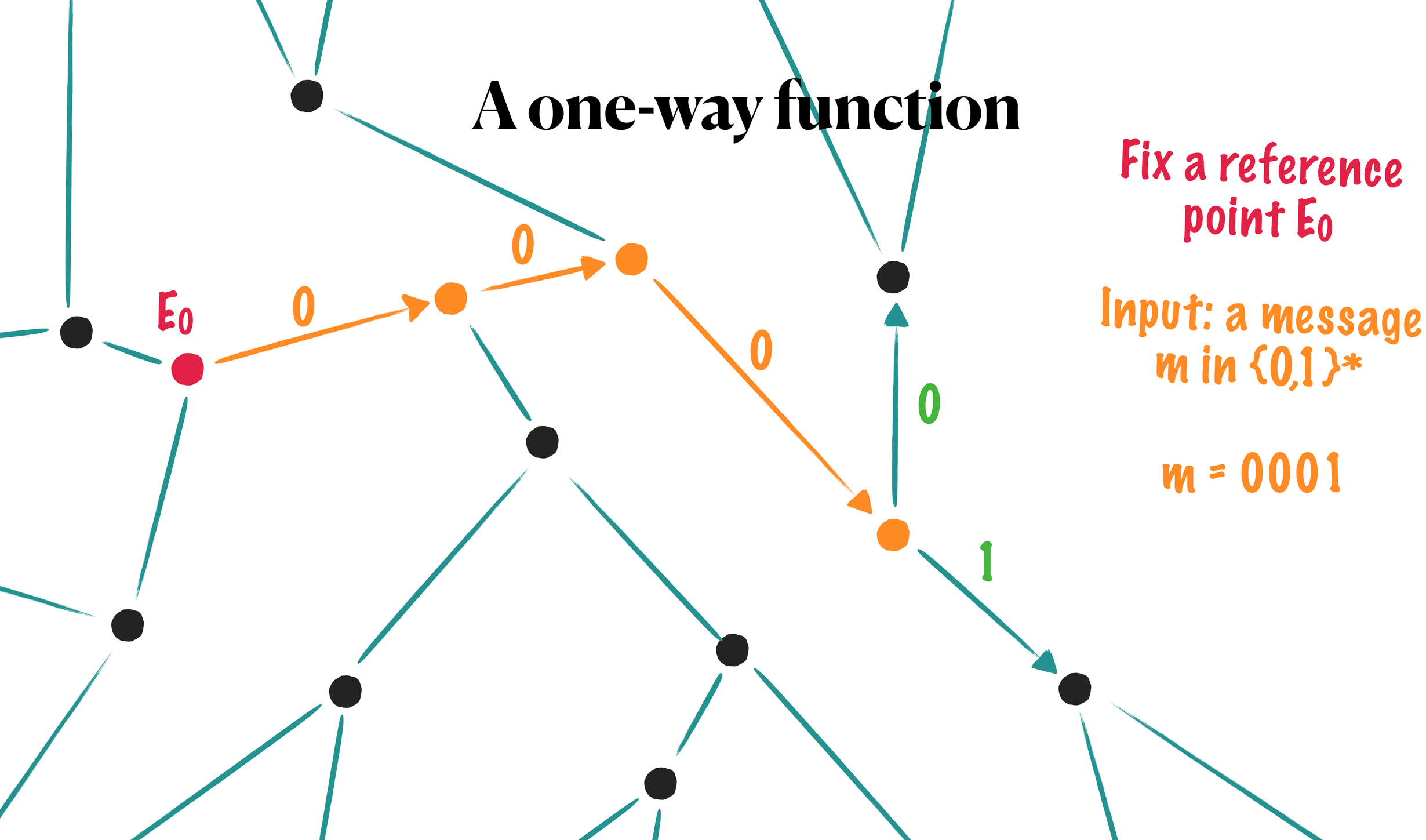


Fix a reference point E_0

Input: a message m in $\{0,1\}^*$

m = 0001

A one-way function

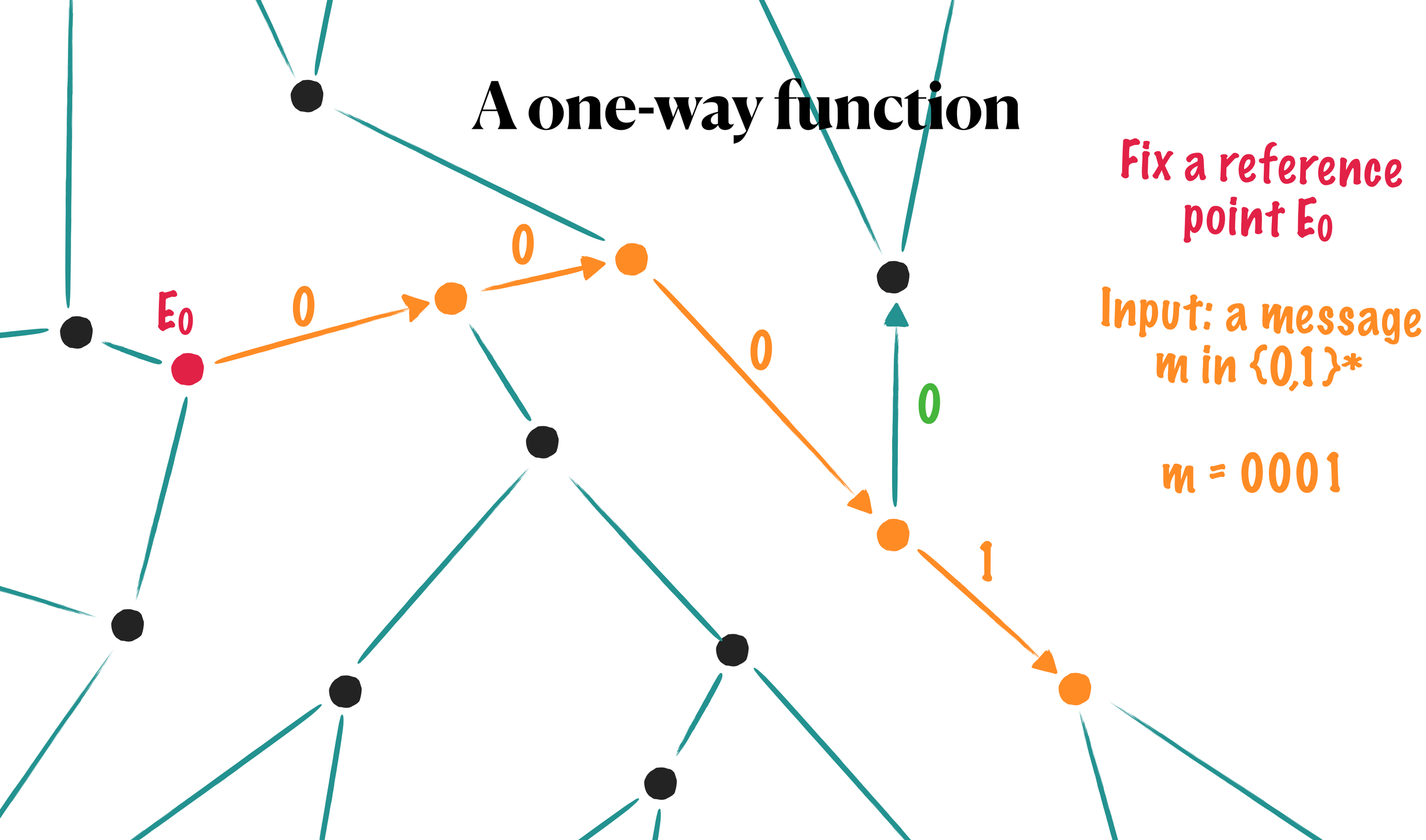


Fix a reference point E_0

Input: a message m in {0,1}*

m = 0001

A one-way function

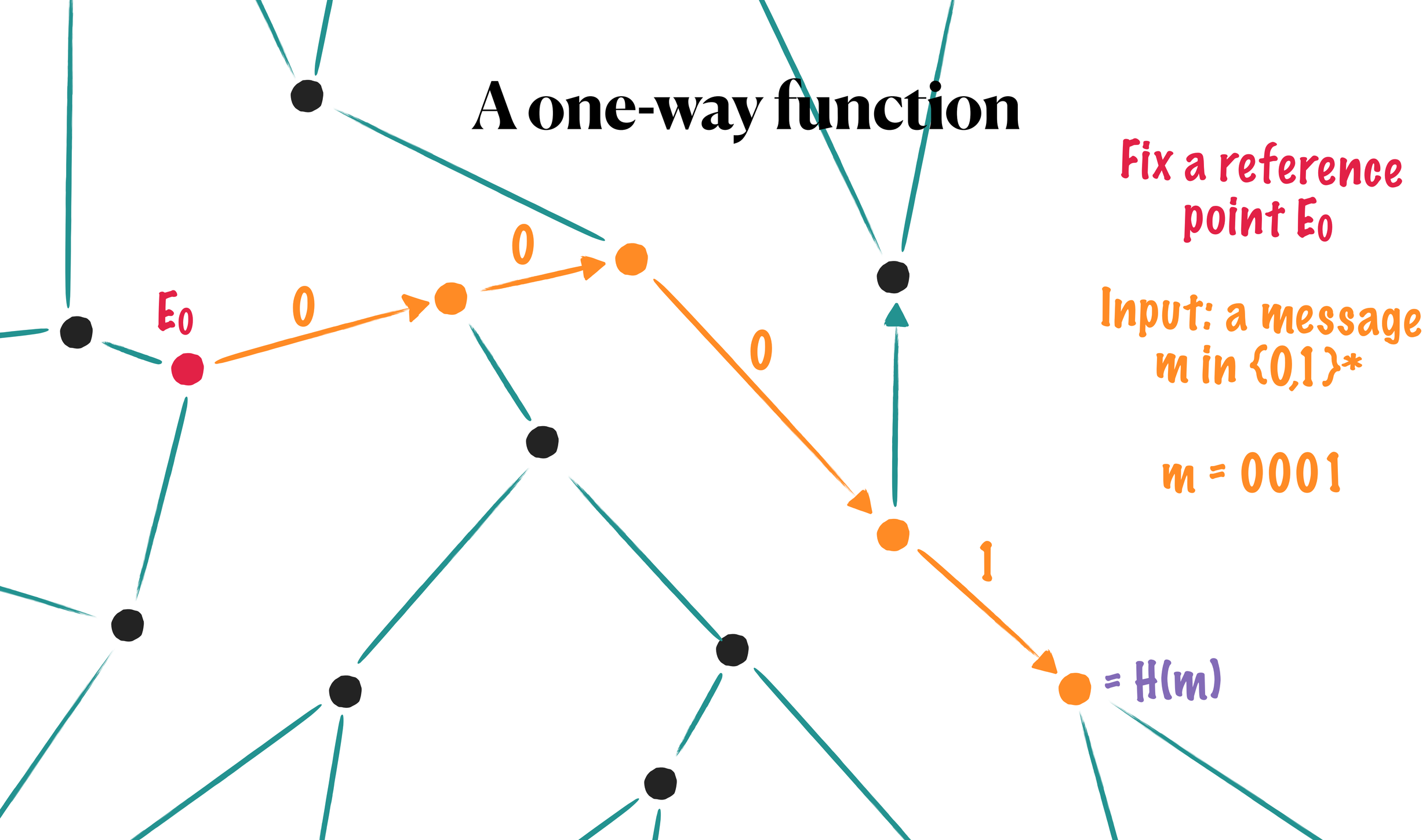


Fix a reference point E_0

Input: a message m in {0,1}*

m = 0001

A one-way function

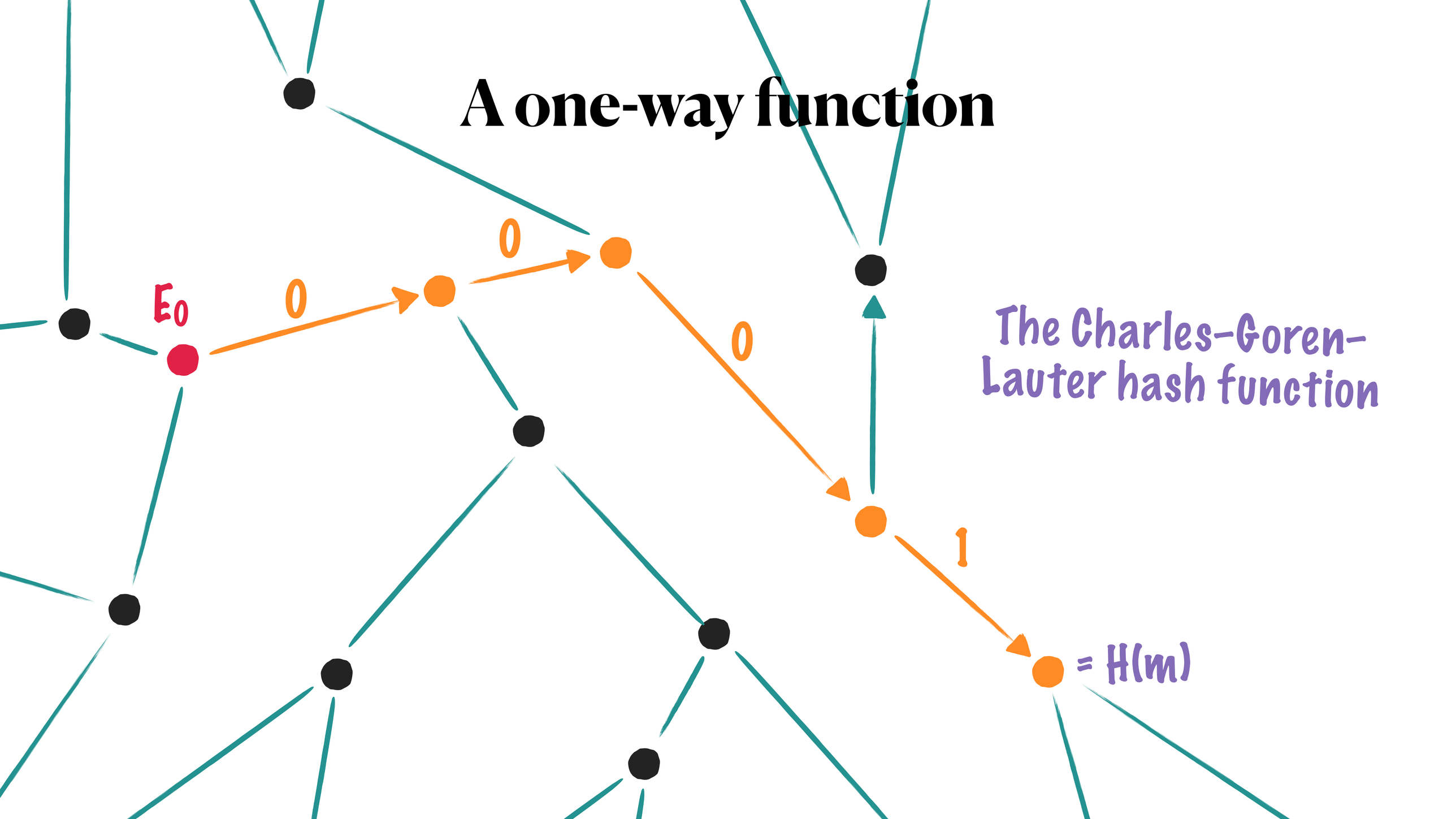


Fix a reference point E_0

Input: a message m in {0,1}*

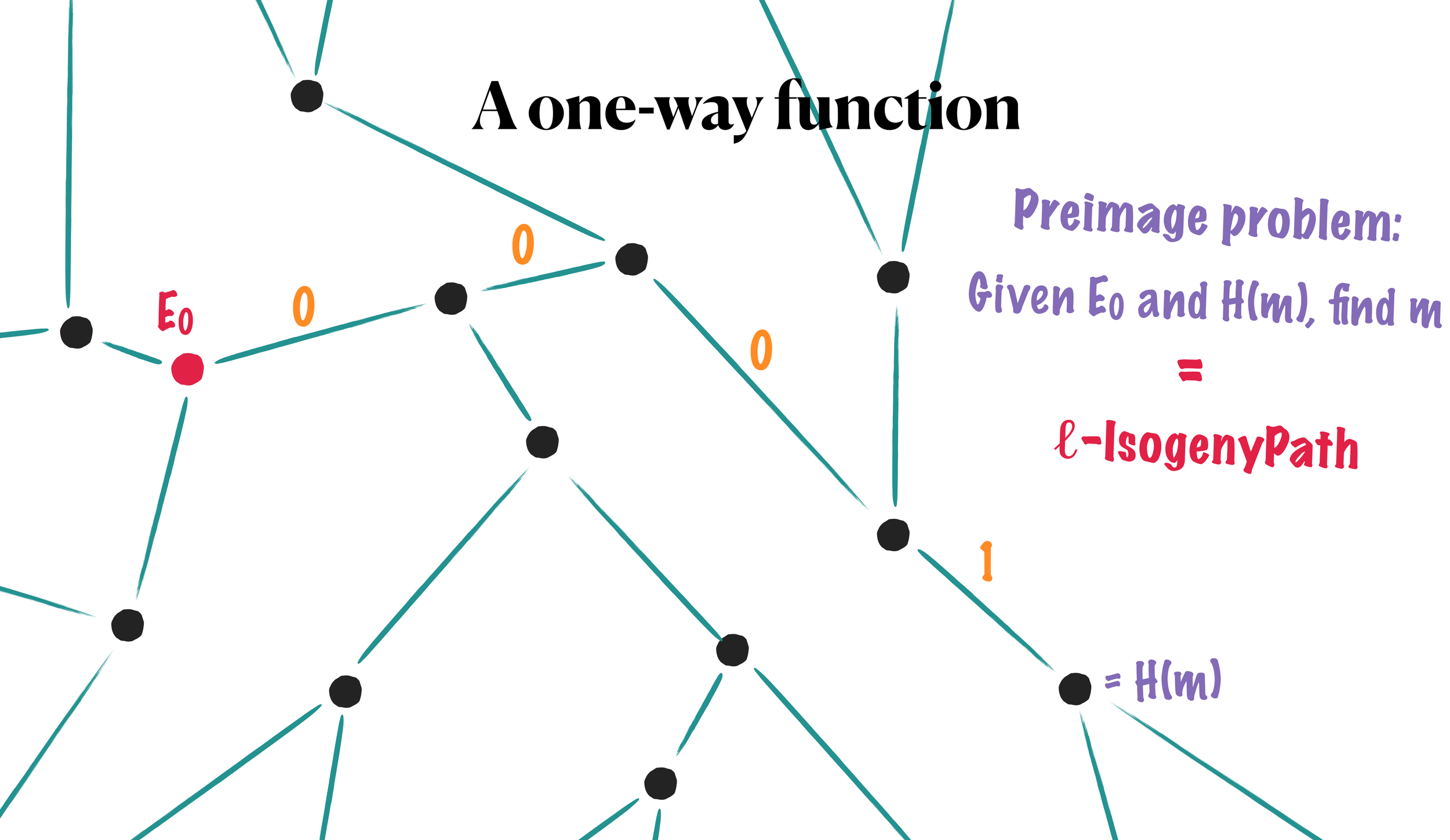
m = 0001

A one-way function



The Charles-Goren-Lauter hash function

A one-way function



Preimage problem:

Given E_0 and H(m), find m

=

ℓ-IsogenyPath

Isogeny-based cryptography

Expectations: cryptosystems as secure as isogeny problem is hard

The isogeny problem = **Security of cryptosystems**

Hard even for quantum algorithms

Post-quantum cryptography

A one-way function

Isogeny-based cryptography

Reality: a mess

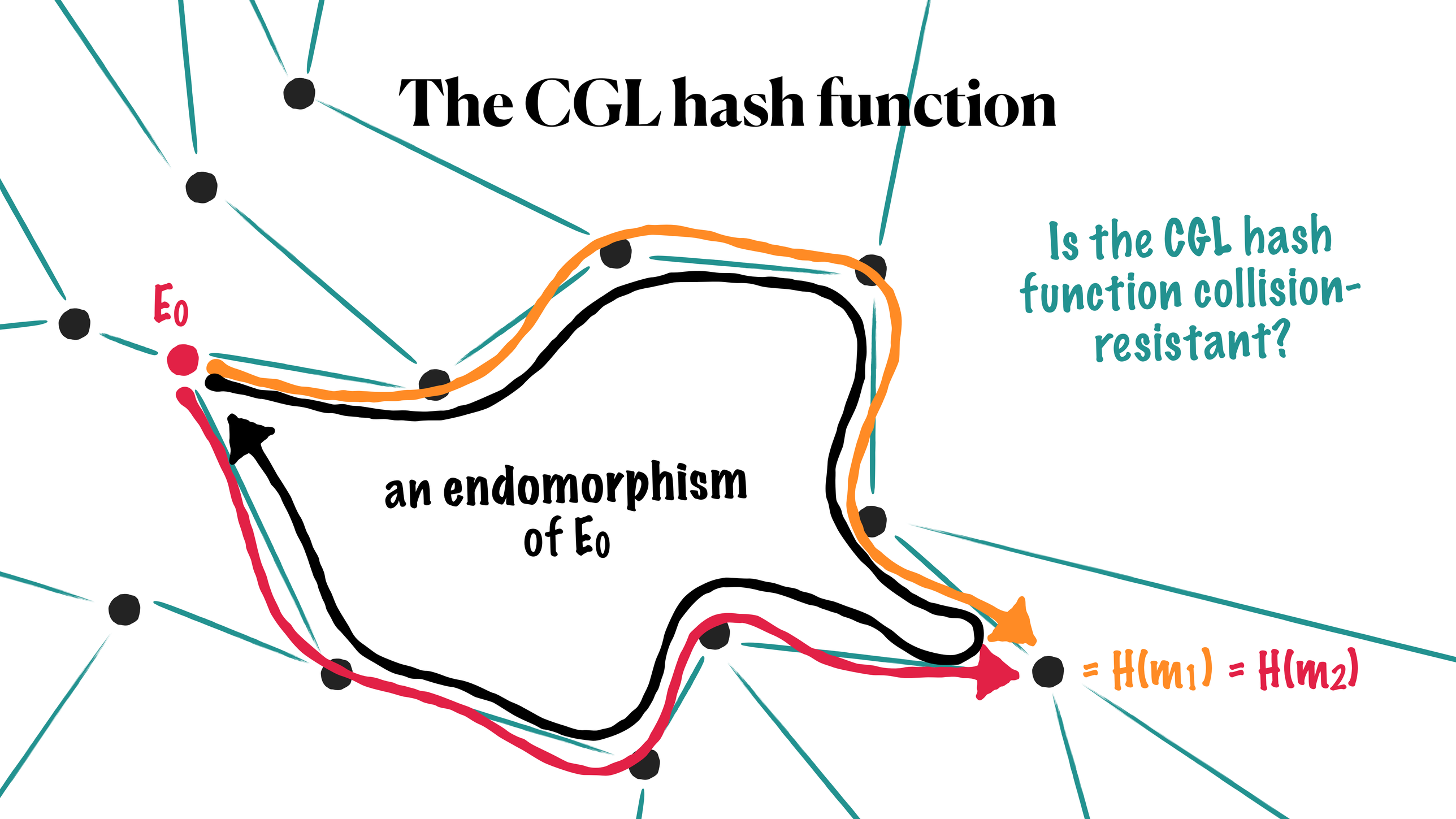
Weird scheme-dependent variants of isogeny problems $\leq$ **Security of cryptosystems** $\leq$ **The isogeny problem**

The isogeny problem	$=$	CGL hash function (preimage)
One endomorphism	$\leq$	CGL hash function (collision)
One endomorphism	$\leq$	SQIsign (soundness)
Vectorisation	$\leq$	CSIDH (key recovery)
SSI-T	$\leq$	SIDH (key recovery)

Endomorphisms

And the supersingular endomorphism ring problem

The CGL hash function



Is the CGL hash function collision-resistant?

Endomorphism ring

An **endomorphism** of E is an isogeny $\varphi : E \to E$ (or the zero map [0])

The **endomorphism ring** of E is $\mathrm{End}(E) = \{\varphi : E \to E\}$

- $\varphi + \psi$ is pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
- $\varphi\psi$ is the composition: $(\varphi\psi)(P) = \varphi(\psi(P))$

Multiplication by $m \in \mathbb{Z}$ is an endomorphism

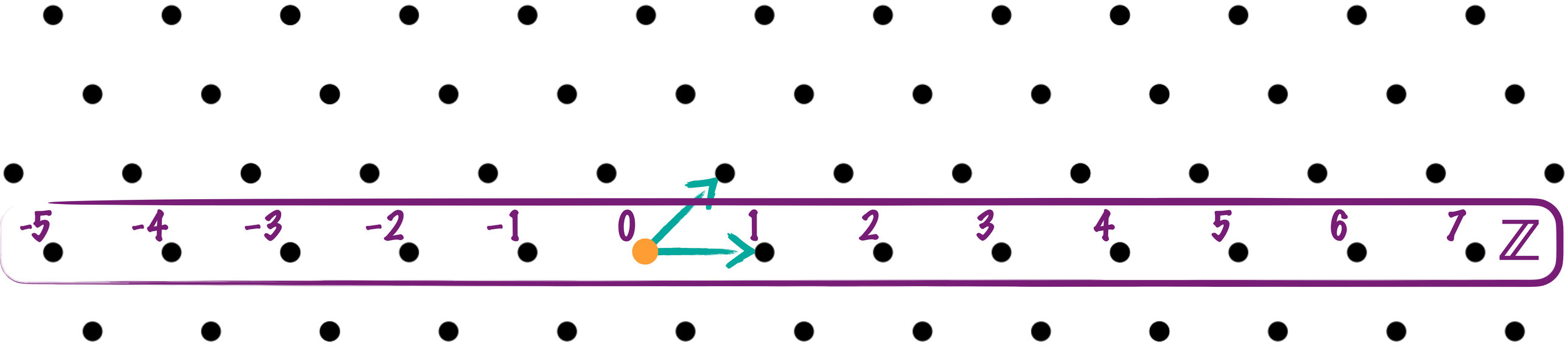
$$[m] : E \to E : P \mapsto P + \ldots + P$$

It forms a subring $\mathbb{Z} \subset \mathrm{End}(E)$

Endomorphism ring

What is the structure of End(E)?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- (End(E), +) is a **lattice** of dimension 2 or 4



Endomorphism ring

What is the structure of End(E)?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- (End(E), +) is a **lattice** of dimension 2 or 4

A curve E is **supersingular** if (End(E), +) is a lattice of dimension 4

Then, there is a $\mathbb{Z}$-basis 1, α_2, α_3, α_4: as a lattice,

$$\mathrm{End}(E) = \mathbb{Z} \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$

The endomorphism ring problem

Given a supersingular E,
"compute End(E)"...

EndRing: Find four endomorphisms that form a basis of End(E)

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-trivial endomorphisms:

- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$
- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$

$\pi^2 = [-p]$

$\iota^2 = [-1]$

and $\iota\pi = -\pi\iota$

$$\mathbf{End}(E_0) \stackrel{?}{=} \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\pi \oplus \mathbb{Z}\iota\pi$$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-trivial endomorphisms:

- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$
- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$

$\pi^2 = [-p]$

$\iota^2 = [-1]$

and $\iota\pi = -\pi\iota$

$$\mathbf{End}(E_0) = \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\,\frac{\iota + \pi}{2} \oplus \mathbb{Z}\,\frac{1 + \iota\pi}{2}$$

EndRing

The endomorphism ring problem

Given a supersingular E,
"compute End(E)"...

EndRing: Find four endomorphisms that form a basis of End(E)

MaxOrder: Compute the "abstract structure" of End(E)

- End(E) is isomorphic to a ring of quaternions. Find which!

Quaternion algebra

The **quaternion algebra $B_{p,\infty}$** is the ring (for $p \equiv 3 \pmod 4$)

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\, i \oplus \mathbb{Q}\, j \oplus \mathbb{Q}\, k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

End(E) is (isomorphic to) a discrete subrings of $B_{p,\infty}$

- End(E) is a **maximal order** in $B_{p,\infty}$
- There are **many** maximal orders in $B_{p,\infty}$

The endomorphism ring problem

Given a supersingular E,
"compute End(E)"...

EndRing: Find four endomorphisms that form a basis of End(E)

MaxOrder: Compute the "abstract structure" of End(E)

- End(E) is isomorphic to a ring of quaternions. Find which!

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-trivial endomorphisms:

- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$
- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$

$\pi^2 = [-p]$

$\iota^2 = [-1]$

and $\iota\pi = -\pi\iota$

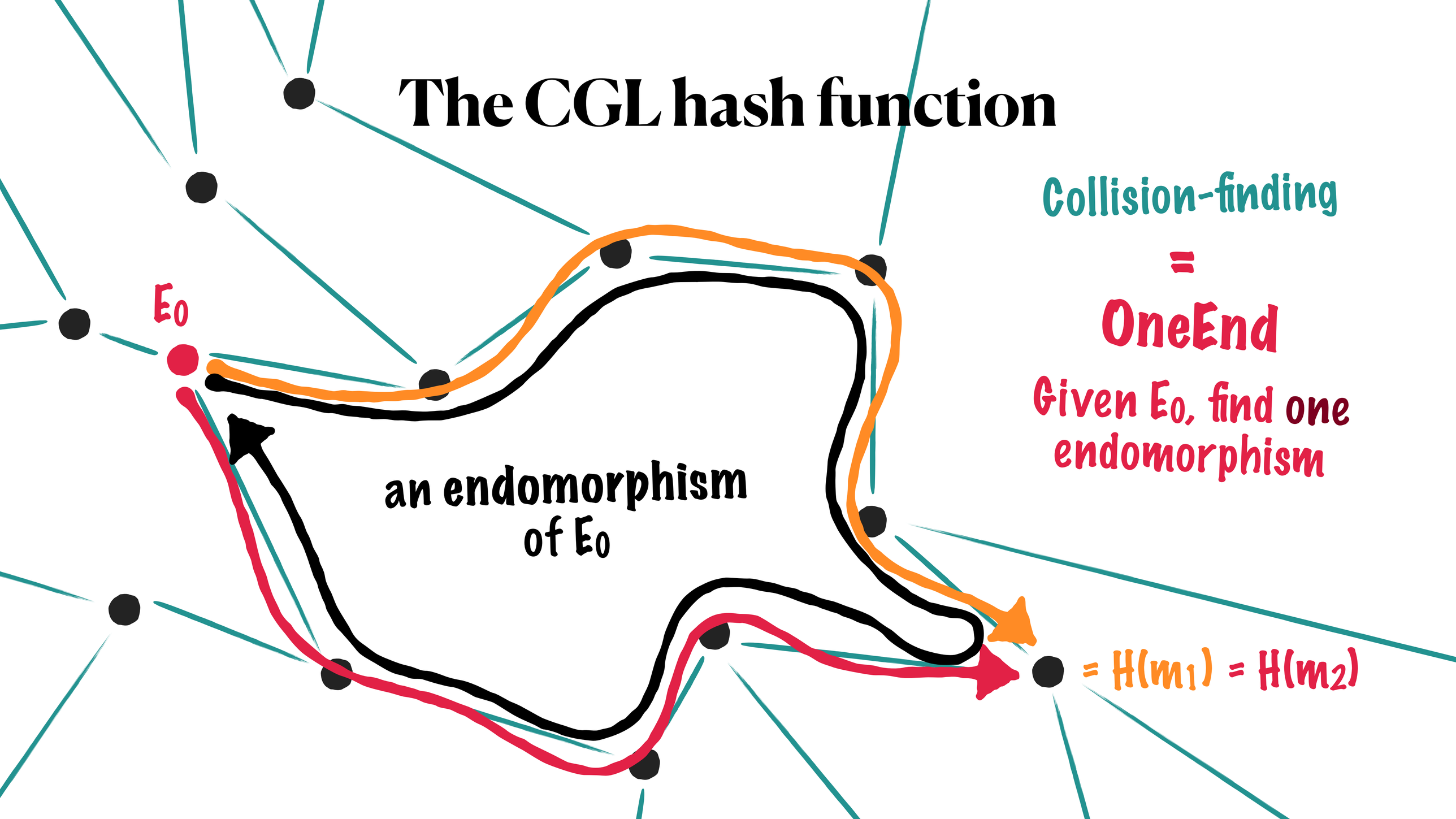
$$\textbf{End}(E_0) = \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\,\frac{\iota + \pi}{2} \oplus \mathbb{Z}\,\frac{1 + \iota\pi}{2}$$

EndRing

$$\simeq \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\,\frac{i + j}{2} \oplus \mathbb{Z}\,\frac{1 + ij}{2} \subset B_{p,\infty}$$

MaxOrder

The CGL hash function



Collision-finding

=

OneEnd

Given E_0, find one endomorphism

The endomorphism ring problem

Given a supersingular E,
"compute End(E)"...

EndRing: Find four endomorphisms that form a basis of End(E)

MaxOrder: Compute the "abstract structure" of End(E)

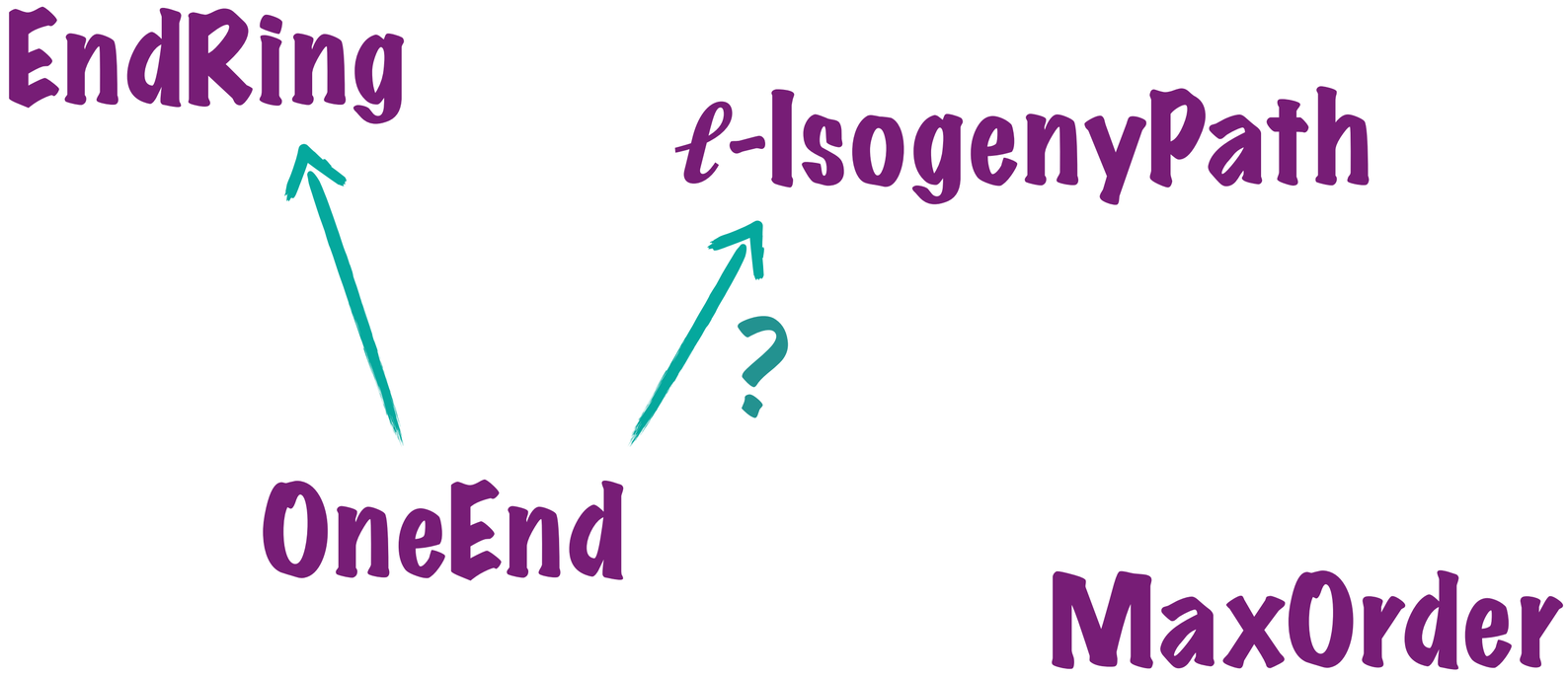
- End(E) is isomorphic to a ring of quaternions. Find which!

OneEnd: Find a single non-scalar endomorphism in $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$

Foundations

Relations between problems

Which is hardest? Easiest?



Relating OneEnd to ℓ-IsogenyPath

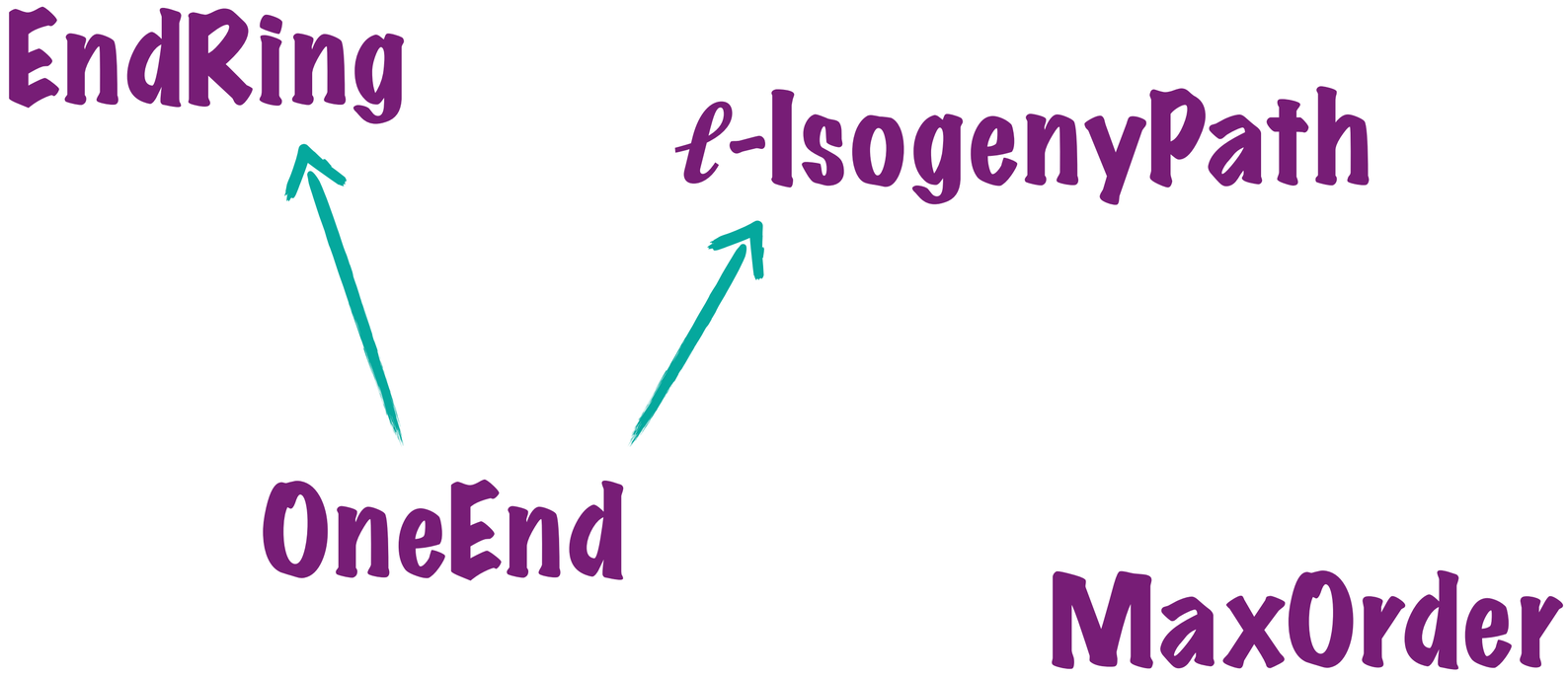
Suppose we can solve ℓ-IsogenyPath.

Can we solve OneEnd?

How to find endomorphisms of E:

- Walk randomly on the isogeny graph: get $\varphi : E \to F$
- Solve ℓ-IsogenyPath(F,E) to get $\psi : F \to E$
- $\psi \circ \varphi : E \to E$ is an endomorphism!

Which is hardest? Easiest?



They are all equivalent

We have probabilistic polynomial time reductions

[W. – FOCS 2021] *The supersingular isogeny path and endomorphism ring problems are equivalent*.

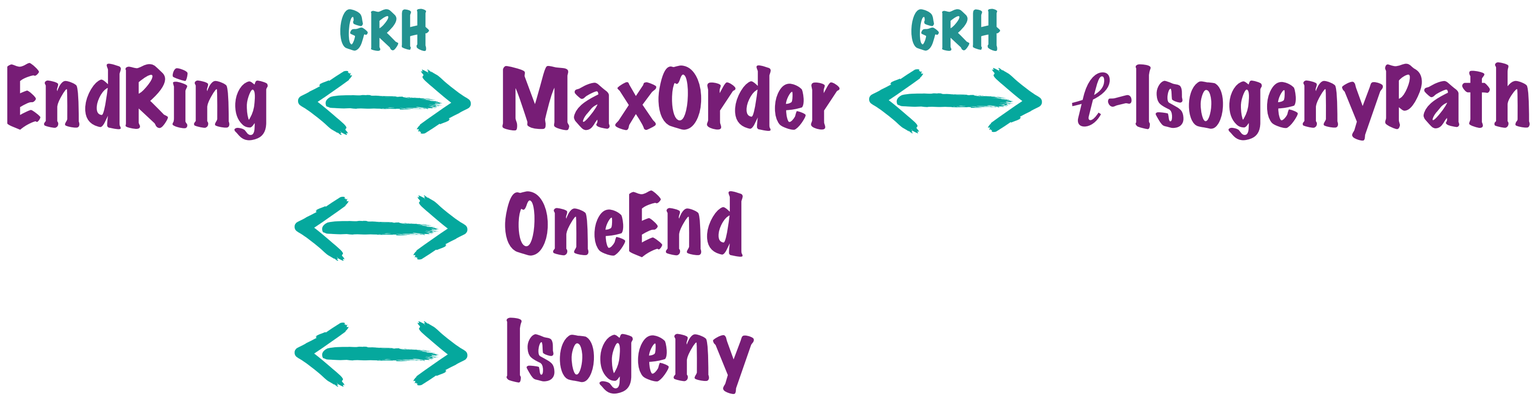
Earlier **heuristic** reductions in:

[Petit, Lauter – preprint 2017] *Hard and Easy Problems for Supersingular Isogeny Graphs*.

[Eisenträger, Hallgren, Lauter, Morrison, Petit – Eurocrypt 2018] *Supersingular isogeny graphs and endomorphism rings: Reductions and solutions*.

They are all equivalent

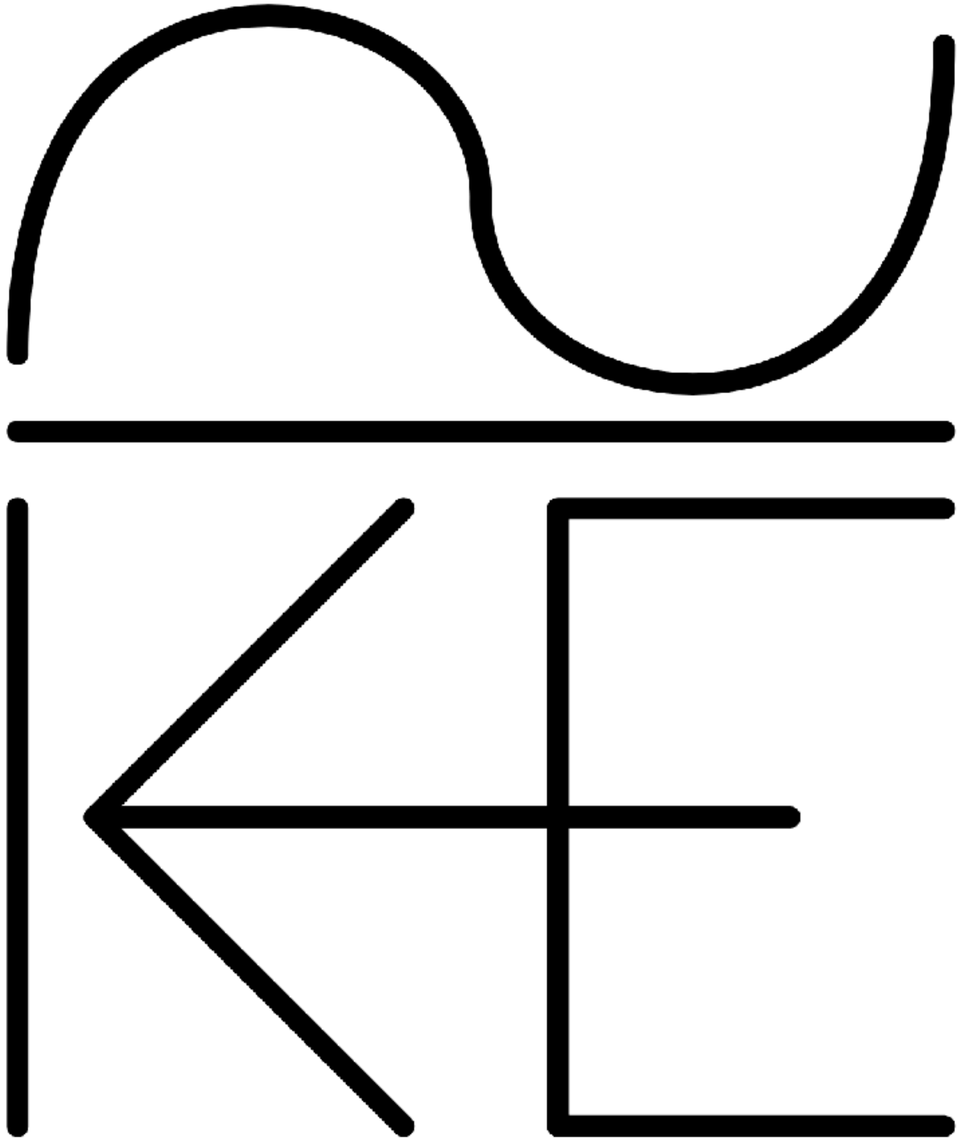
We have probabilistic polynomial time reductions



[Page, W. – Eurocrypt 2024] *The supersingular Endomorphism Ring and One Endomorphism problems are equivalent*.

SIDH

Jao–De Feo 2011



SIKE logo – Supersingular Isogeny Key Encapsulation

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems $\leq$ **Security of cryptosystems** $\leq$ **The isogeny problem**

The isogeny problem	$=$	CGL hash function (preimage)
One endomorphism	$\leq$	CGL hash function (collision)
One endomorphism	$\leq$	SQIsign (soundness)
Vectorisation	$\leq$	CSIDH (key recovery)
SSI-T	$\leq$	SIDH (key recovery)

Isogeny-based cryptography

Reality: a mess

Weird scheme-dependent variants of isogeny problems ≤ **Security of cryptosystems** ≤ **The isogeny problem**

The isogeny problem with "torsion point information"...

[Jao, De Feo] PQCrypto 2011
Isogeny-based key exchange
NIST PQC alt-finalist

The isogeny problem	≤	CGL hash function (preimage)
One endomorphism	≤	CGL hash function (collision)
One endomorphism	≤	SQISign (soundness)
Vectorisation	≤	CSIDH (key recovery)
SSI-T	≤	SIDH (key recovery)

Isogeny from a kernel

- Let E be an elliptic curve
- Let G a finite subgroup of E
- **Quotienting by G:** there is a unique (separable) isogeny

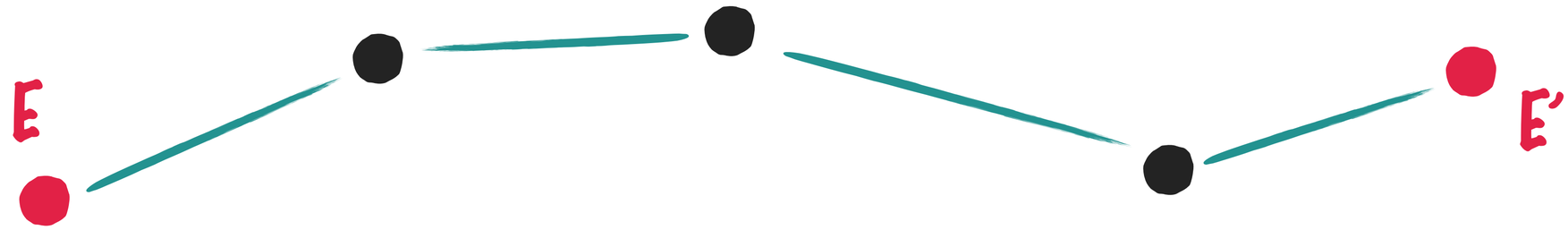
$$\varphi : E \to E/G$$

  with $\ker(\varphi) = G$

- $\deg(\varphi) = \#G$
- **Computing an isogeny from its kernel:** Given generators of G, the isogeny φ can be computed in time poly(size of input, largest prime factor of $\#G$) [Vélu 1971]

  ➡ Given a smooth kernel, can efficiently compute the isogeny

Two equivalent ways to generate an isogeny



Random path of length k in the ℓ-isogeny graph

is the same as

Random kernel G of order ℓ^k

$$\varphi : E \to E/G$$

SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

Compute $\boldsymbol{E_{AB}} = E_B/G$

Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$

Compute $\boldsymbol{E_{BA}} = E_A/H$

$$\begin{array}{ccc} E_0 & \xrightarrow{\varphi_B} & E_0/H = E_B \\ \downarrow{\scriptstyle \varphi_A} & & \downarrow \\ E_A = E_0/G & \longrightarrow & E_0/(G+H) = \boldsymbol{E_{AB}} = \boldsymbol{E_{BA}} \end{array}$$

SIDH

Fix reference elliptic curve E_0

Alice

Random subgroup G of E_0

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

Compute $\boldsymbol{E_{AB}} = E_B/G$

G is not a subgroup of E_B

$\varphi_B(G)$ is!

Bob

Random subgroup H of E_0

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$

Compute $\boldsymbol{E_{BA}} = E_A/H$

How to compute $\varphi_B(G)$?

Alice does not know φ_B...

E_A

E_B

Torsion

- The N-torsion of E is

$$E[N] = \{P \in E \mid N \cdot P = P + P + \ldots + P = 0\}$$

- $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

Idea:

- Alice picks a subgroup G of $E_0[2^n]$ ← Many choices, good entropy
- Bob gives φ_B on $E_0[2^n]$ ← φ_B remains secret everywhere else...
- Alice can compute $\varphi_B(G)$ ← Can compute shared secret $\boldsymbol{E_{AB}} = E_B/\varphi_B(G)$

SIDH

Fix: an elliptic curve E_0

Generators P_2, Q_2 of $E_0[2^n] \cong (\mathbb{Z}/2^n\mathbb{Z})^2$

Generators P_3, Q_3 of $E_0[3^m] \cong (\mathbb{Z}/3^m\mathbb{Z})^2$

Alice

Random subgroup G of $E_0[2^n]$

Compute $\varphi_A : E_0 \to E_0/G$

Let $E_A = E_0/G$

$E_A, \varphi_A(P_3), \varphi_A(Q_3)$ →

← $E_B, \varphi_B(P_2), \varphi_B(Q_2)$

Compute $\boldsymbol{E_{AB}} = E_B/\varphi_B(G)$

Bob

Random subgroup H of $E_0[3^m]$

Compute $\varphi_B : E_0 \to E_0/H$

Let $E_B = E_0/H$

Compute $\boldsymbol{E_{BA}} = E_A/\varphi_A(H)$

The SSI-T problem

Context:

- two elliptic curves E_0 and E_1
- an isogeny $\varphi : E_0 \to E_1$ (say, of degree 3^m like Bob's isogeny)
- an integer N coprime to $\deg(\varphi)$ (say, $N = 2^n$...)
- generators P and Q of $E_0[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

"torsion point information"

SSI-T: Given E_0, E_1, P, Q, $\varphi(P)$ and $\varphi(Q)$, find the isogeny $\varphi : E_0 \to E_1$

SIDH key recovery $\Leftrightarrow$ SSI-T

An interpolation problem

Polynomial interpolation: given $f(s)$ for a few $s \in K$, find f

SSI-T: given $\varphi(P)$ for a few $P \in E$, find φ

Torsion point information: a weakness?

Standard SIDH parameters remained unaffected...