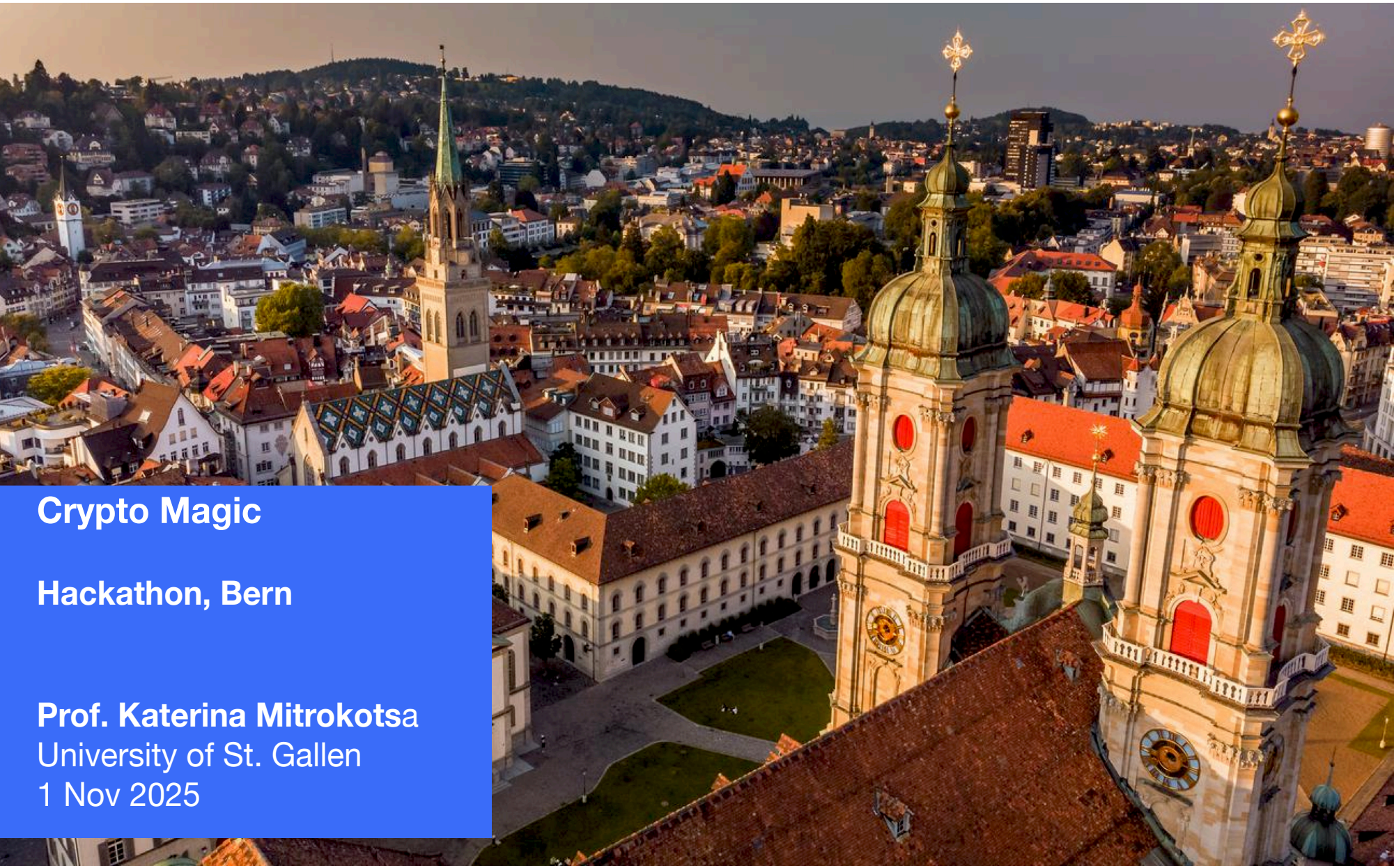


Crypto Magic

Hackathon, Bern

Prof. Katerina Mitrokotsa
University of St. Gallen
1 Nov 2025

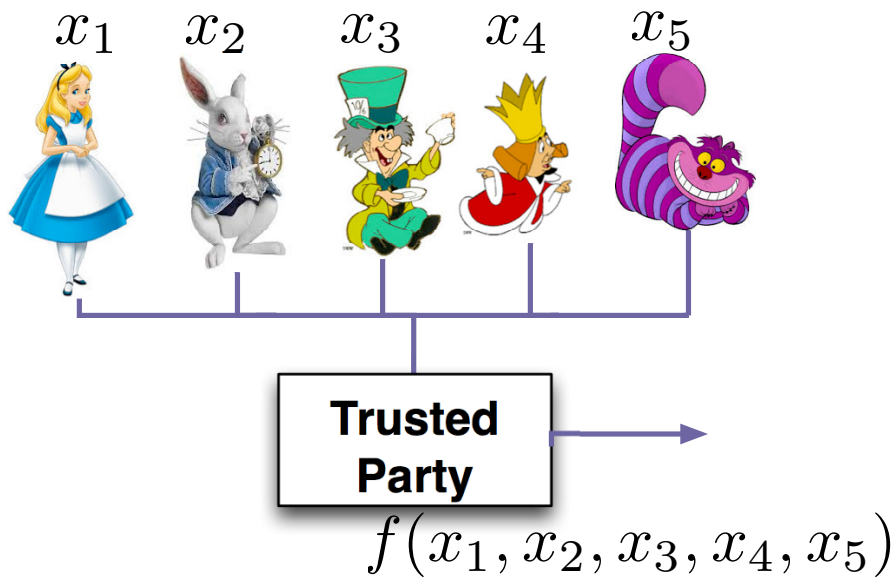
Outline

- How to Compute Privately without a Trusted party?
- How to Share a Secret?
- How to Prove I know a Secret?
- How to Compute on Secret data?

Preview of Secure Multi Party Comutation

- Multiple parties have **secret** inputs (e.g., x_1, x_2, x_3, x_4).
- Goal: compute $f(x_1, x_2, x_3, x_4)$
- The result (value of f) is revealed but **nothing else!**

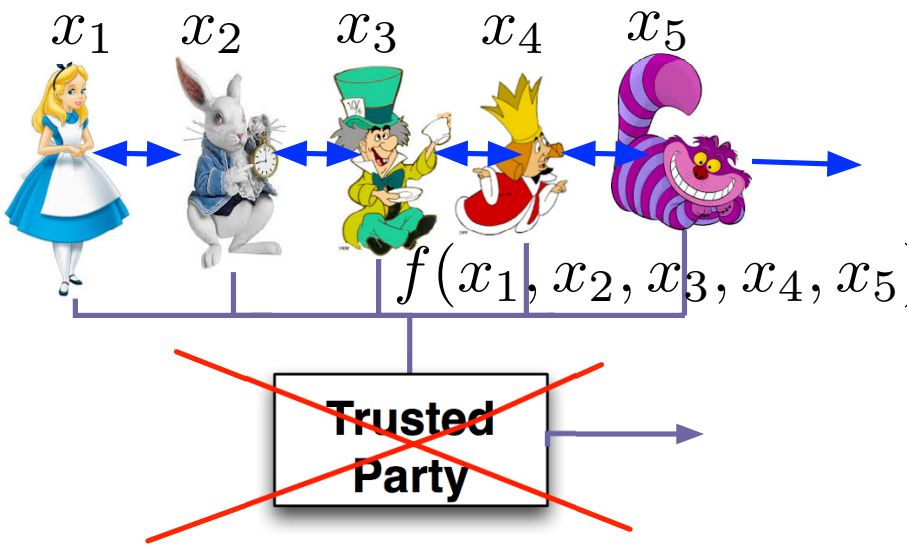
Problem: Trusted Party **single point of failure**!



Preview of Secure Multi Party Comutation

- Multiple parties have **secret** inputs (e.g., x_1, x_2, x_3, x_4).
- Goal: compute $f(x_1, x_2, x_3, x_4)$
- The result (value of f) is revealed but **nothing else!**

Problem: Trusted Party **single point of failure**!

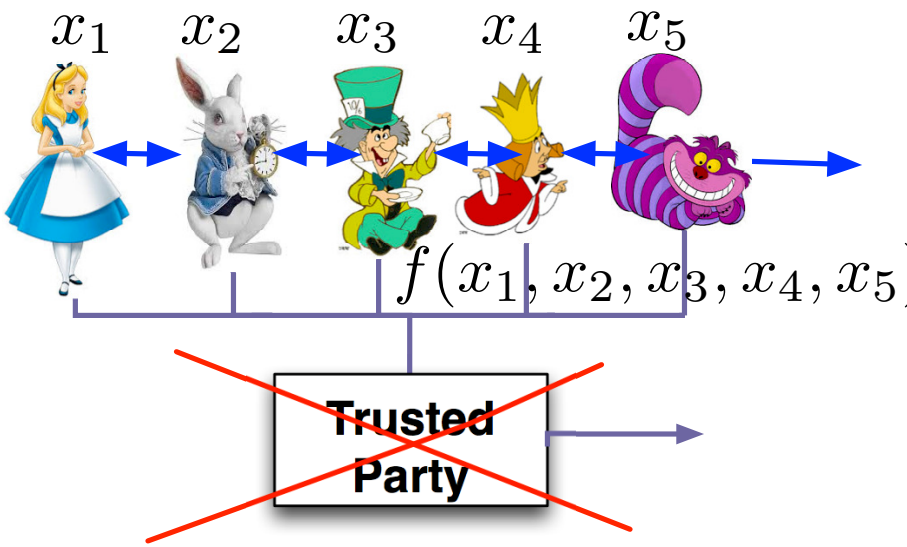


- Can we achieve that without the trusted party?

Preview of Secure Multi Party Comutation

- Multiple parties have **secret** inputs (e.g., x_1, x_2, x_3, x_4).
- Goal: compute $f(x_1, x_2, x_3, x_4)$
- The result (value of f) is revealed but **nothing else!**

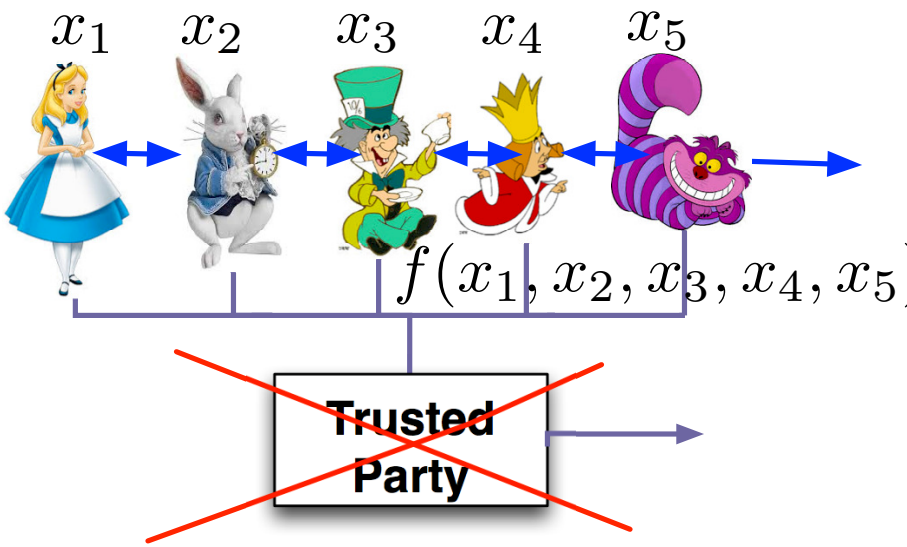
Problem: Trusted Party **single point of failure**!



- Can we achieve that without the trusted party?
- Yes! $\Rightarrow$ Secure multi-party computation!!

Preview of Secure Multi Party Comutation

- Multiple parties have **secret** inputs (e.g., x_1, x_2, x_3, x_4).
- Goal: compute $f(x_1, x_2, x_3, x_4)$
- The result (value of f) is revealed but **nothing else!**



Problem: Trusted Party **single point of failure**!

- Can we achieve that without the trusted party?
- Yes! $\Rightarrow$ Secure multi-party computation!!

Anything that can be done with trusted auth. can also be done without.

How to Share a Secret?

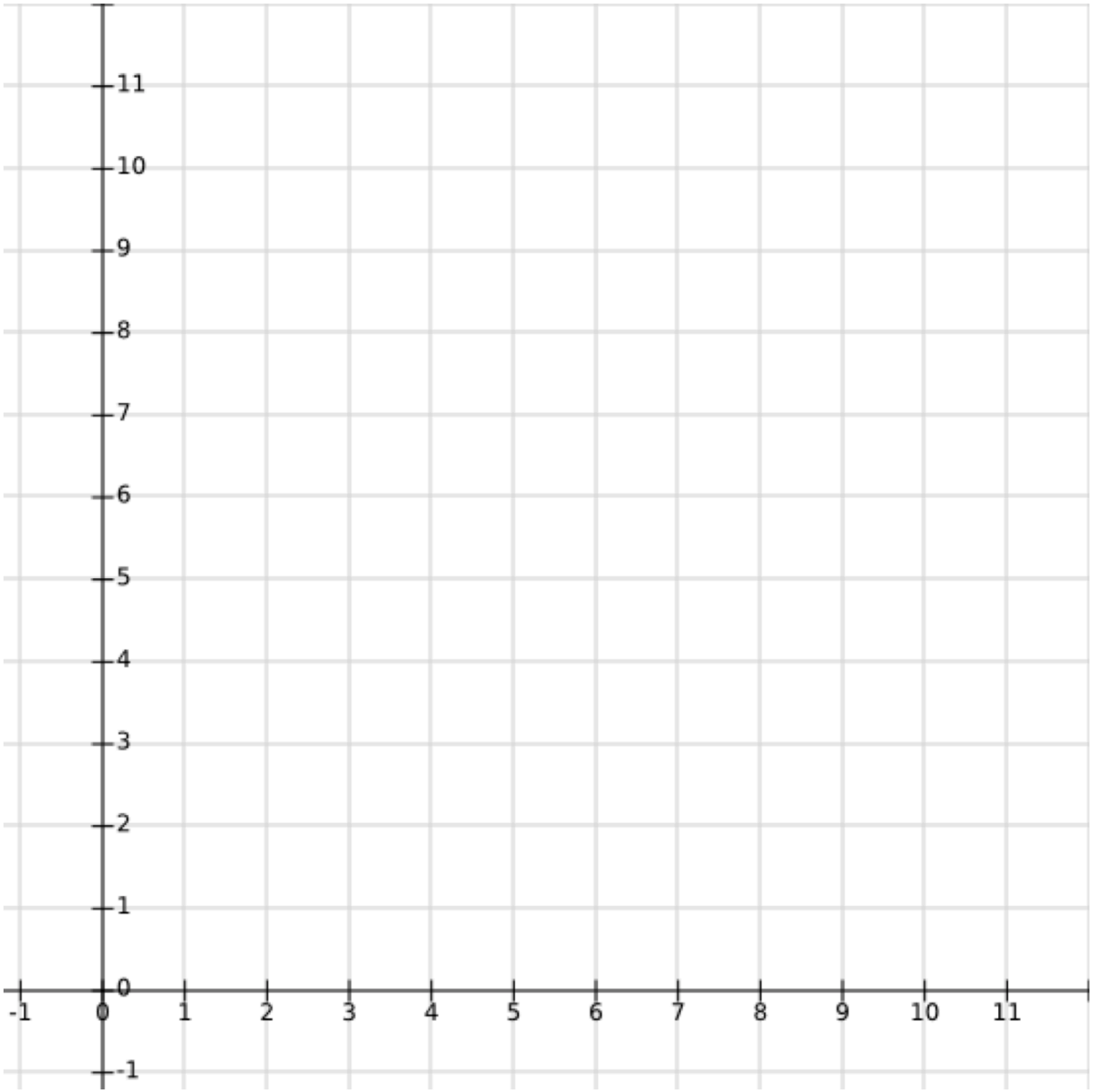
Why do we need secret sharing schemes?

Intuition: Secret Sharing schemes can be used to distribute a **secret** among many parties, so that **no-one alone** can retrieve the secret but if **enough parties** collaborate they can retrieve the secret.

Useful when a single person **cannot be trusted** with the secret (e.g., missile launch codes).

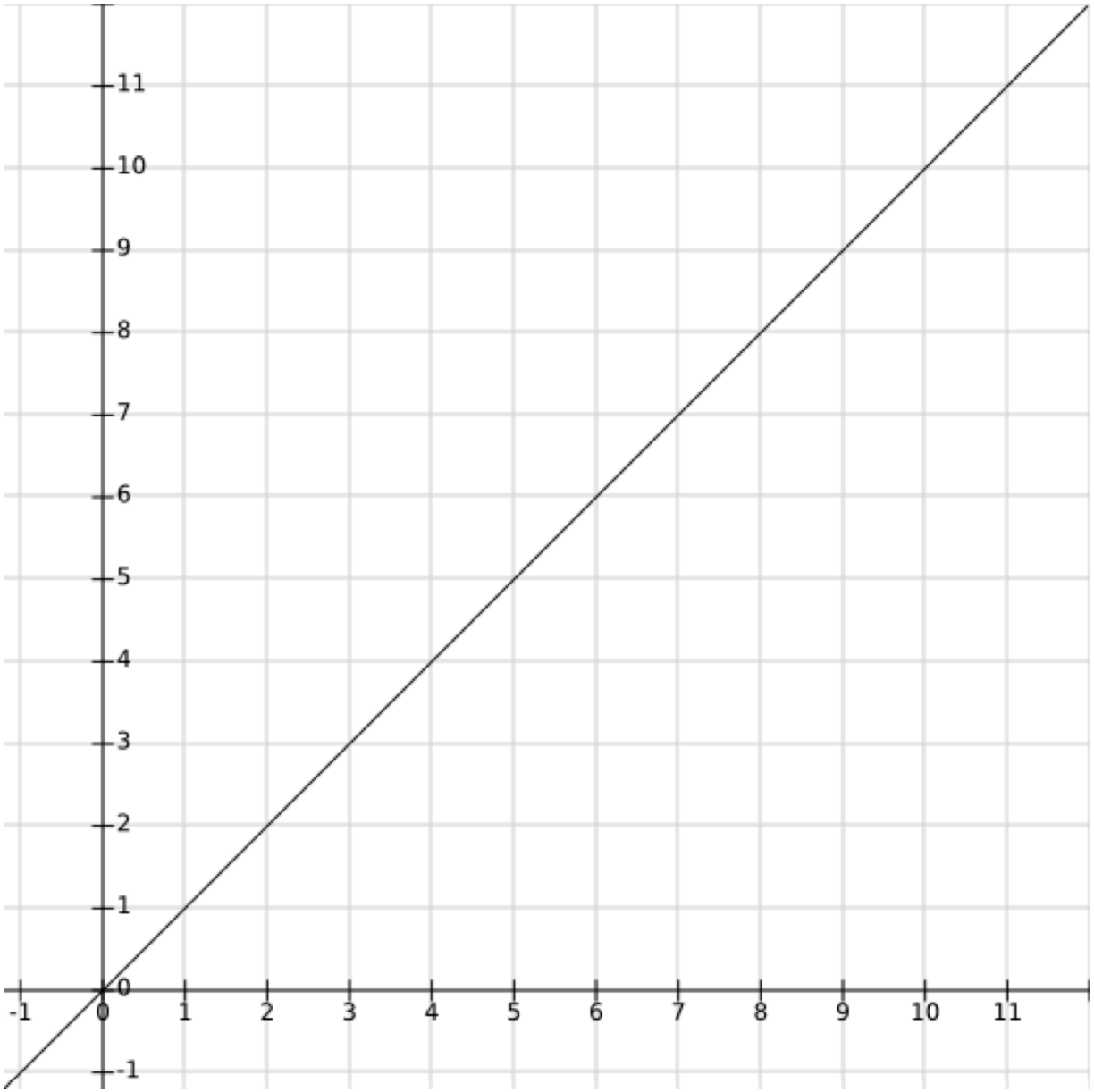
Attention: In real secret sharing schemes, the share of a secret should reveal nothing about the **secret**!

Lines, points & secrets



Lets draw some lines

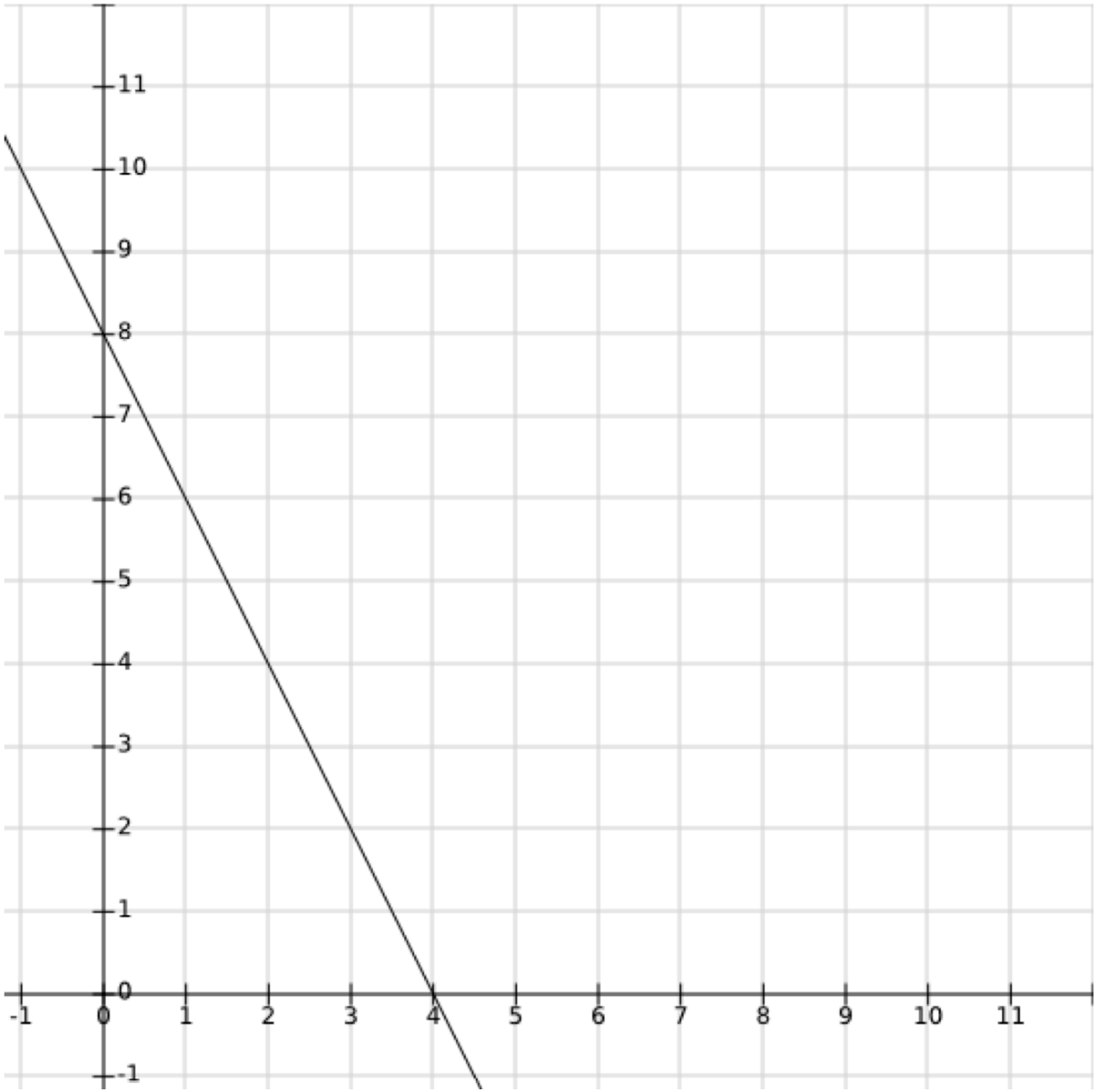
Lines, points & secrets



Lets draw some lines

- $f(x) = x$

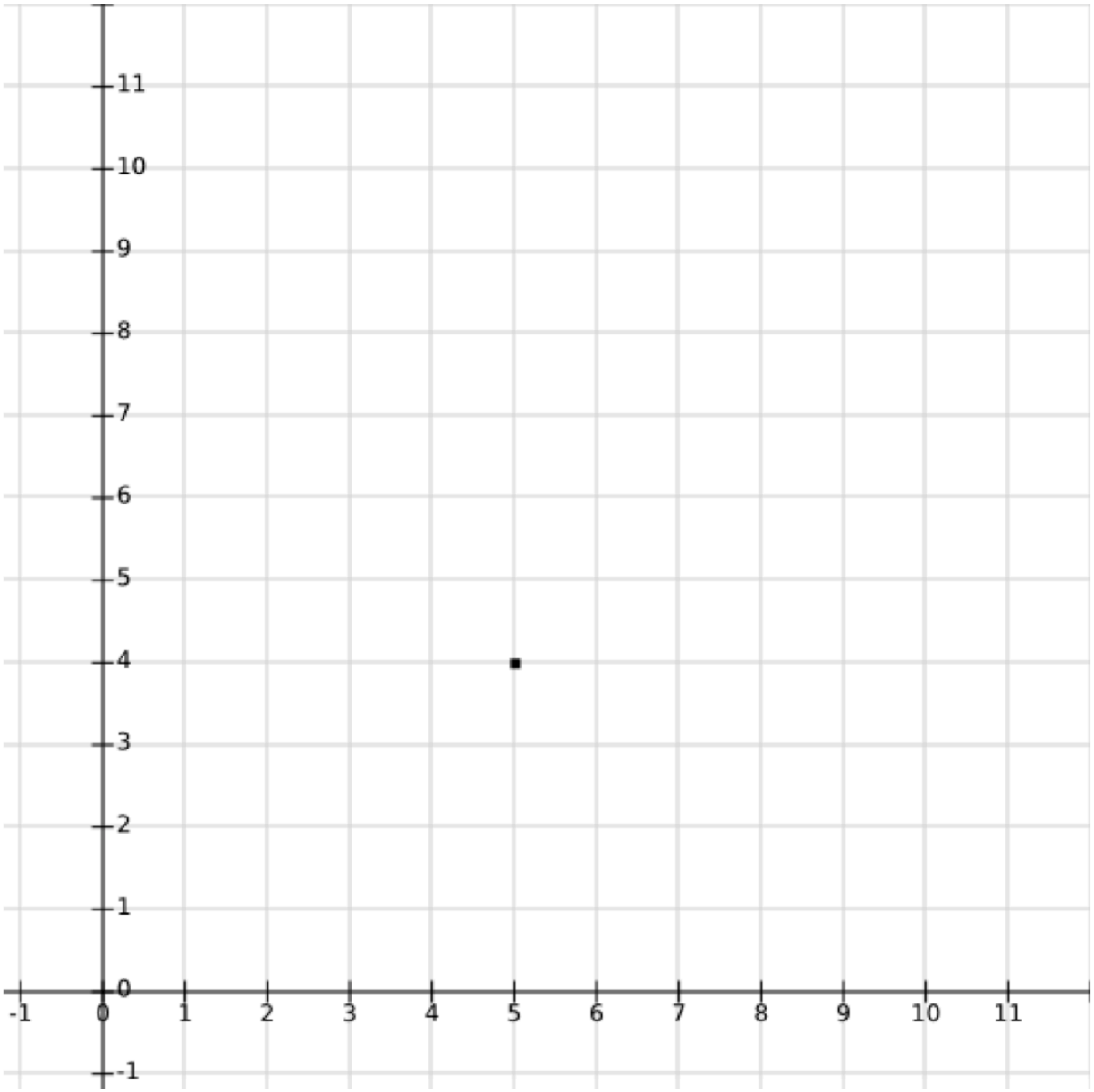
Lines, points & secrets



Lets draw some lines

- $f(x) = x$
- $f(x) = 8 - 2x$

Lines, points & secrets

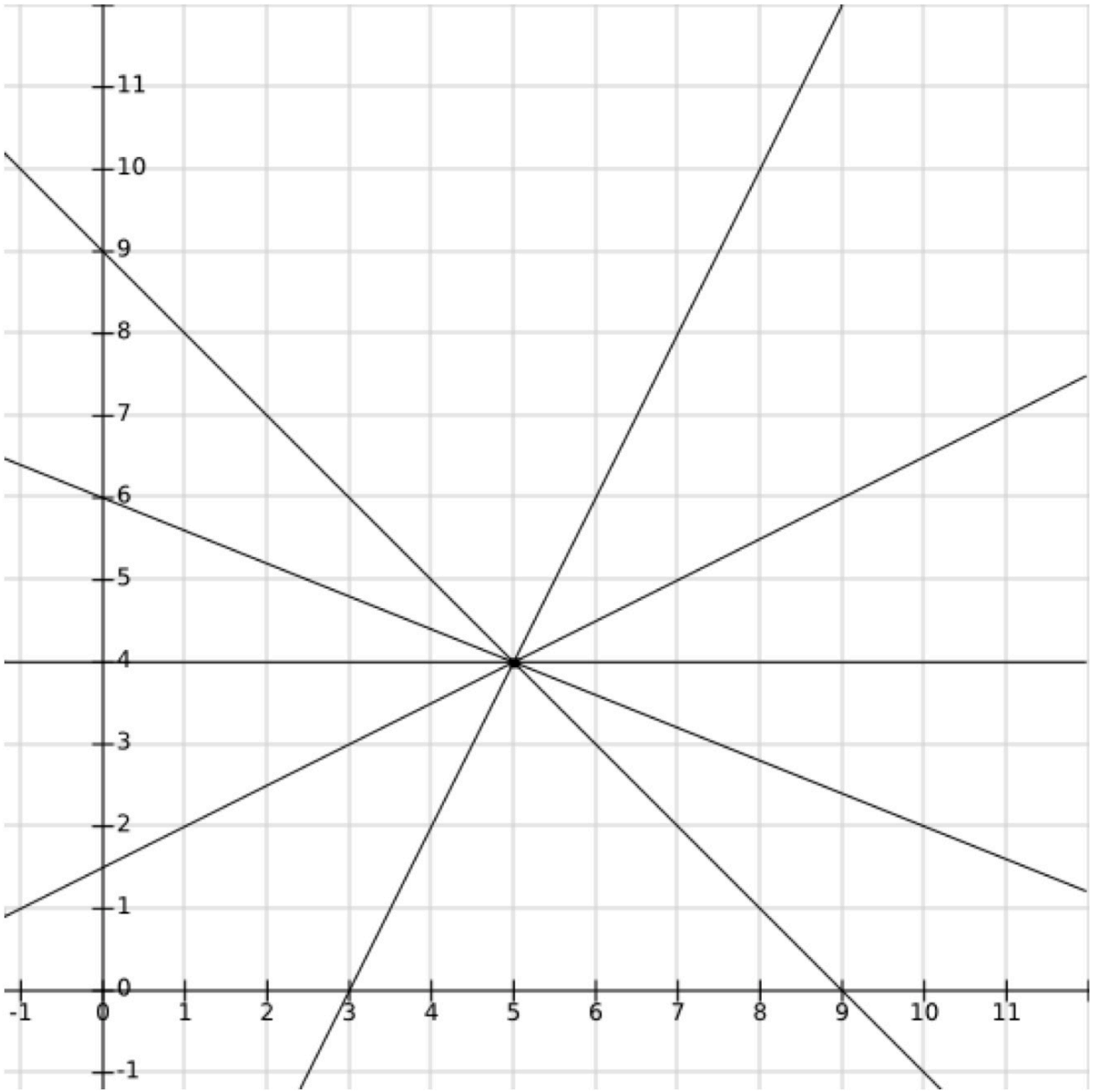


Quiz Question!

Go to:
`http://socrative.com/`
Student Login
Classroom: **SECUREHSG**

- How many **straight** lines pass from this point?

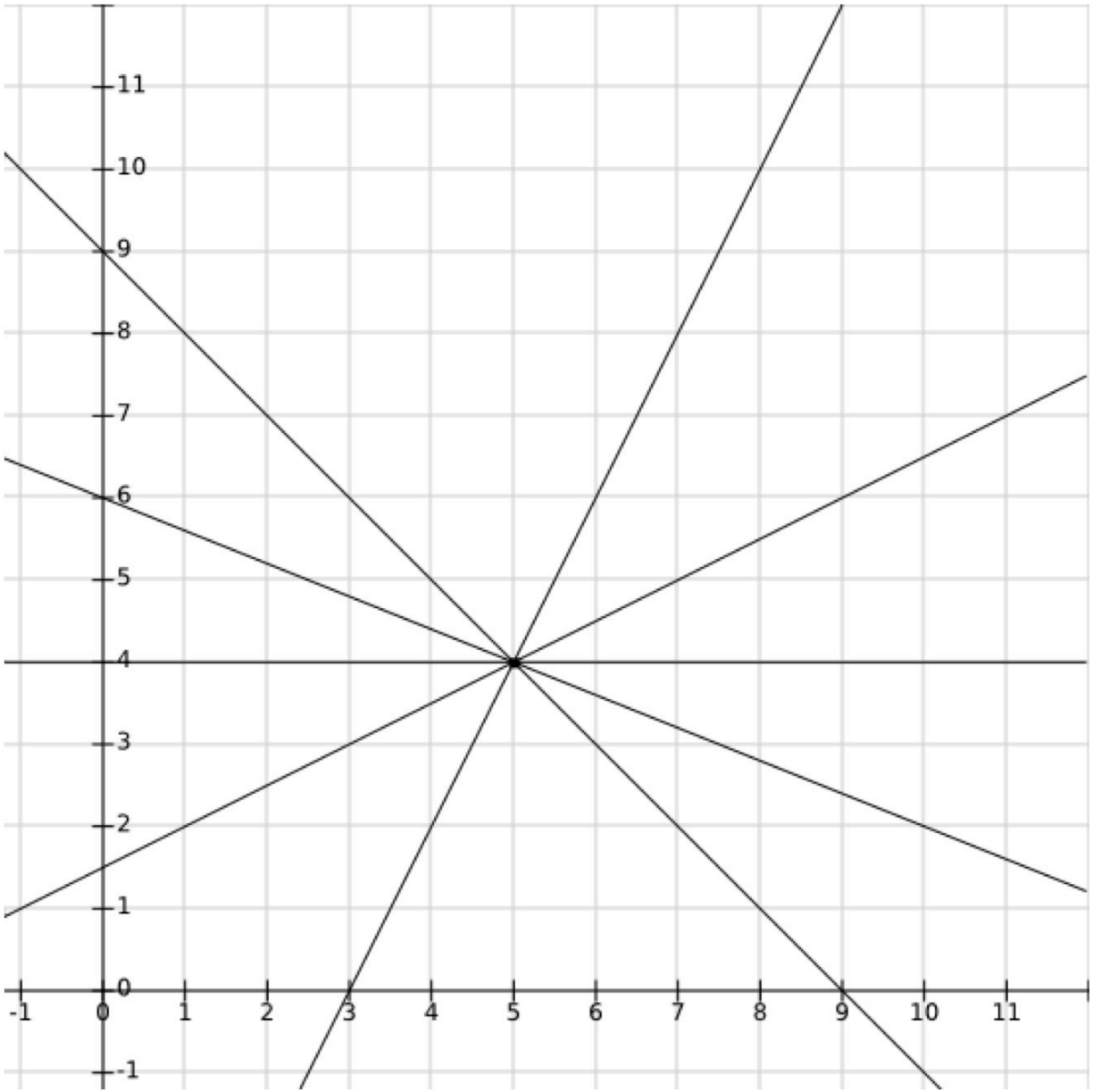
Lines, points & secrets



Quiz Question!
Go to:
`http://socrative.com/`
Student Login
Classroom: **SECUREHSG**

- How many **straight** lines pass from this point?
  Infinitely many!

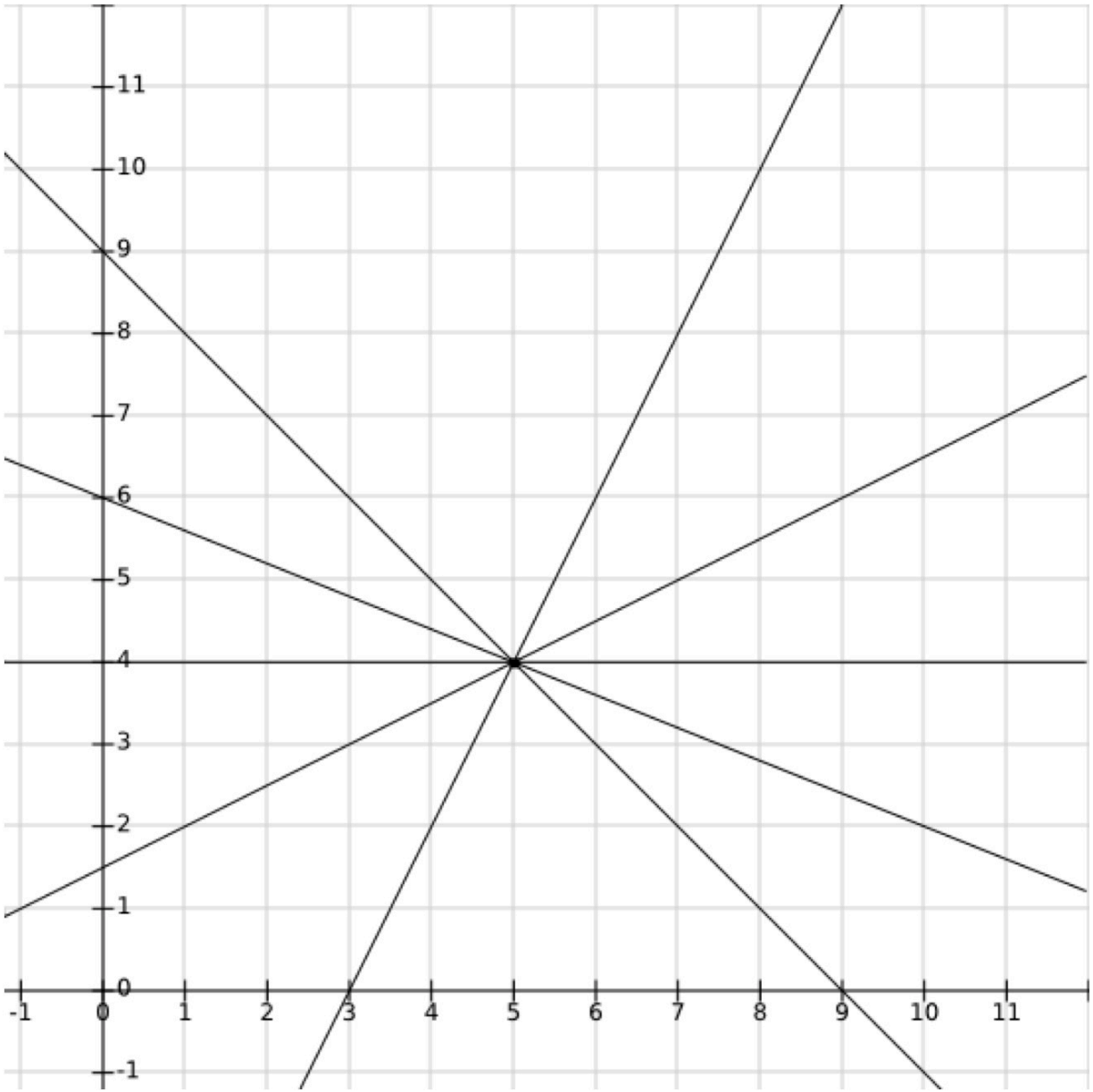
Lines, points & secrets



Quiz Question!
Go to:
`http://socrative.com/`
Student Login
Classroom: **SECUREHSG**

- How many **straight** lines pass from this point?
  Infinitely many!
- For these lines, what can be the value $\mathbf{f(0)}$?

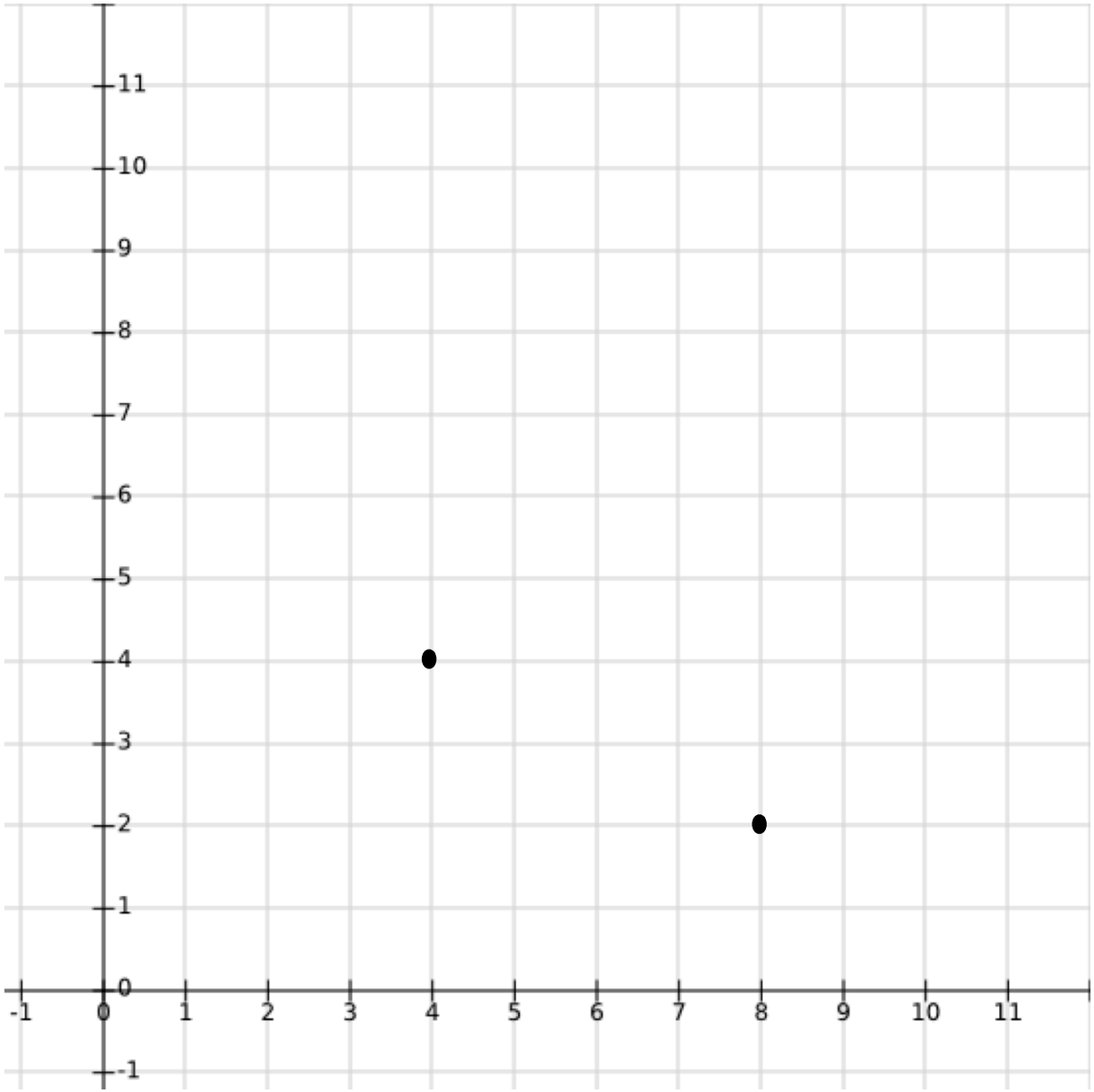
Lines, points & secrets



Quiz Question!
Go to:
`http://socrative.com/`
Student Login
Classroom: **SECUREHSG**

- How many **straight** lines pass from this point?
  Infinitely many!
- For these lines, what can be the value $\mathbf{f(0)}$?
  Anything!

Lines, points & secrets

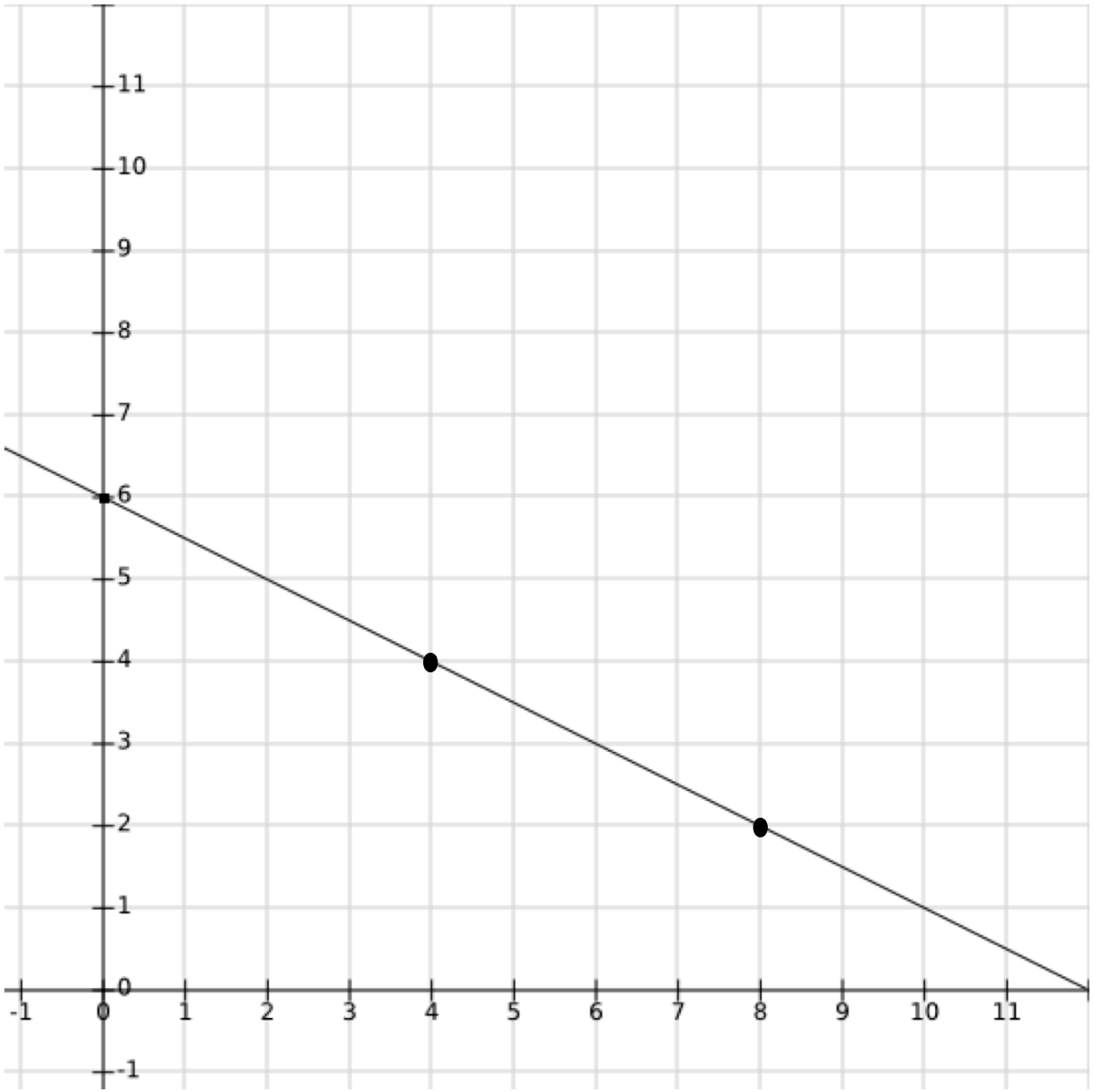


Quiz Question!

Go to:
`http://socrative.com/`
Student Login
Classroom: **SECUREHSG**

- How many lines pass from these two points?

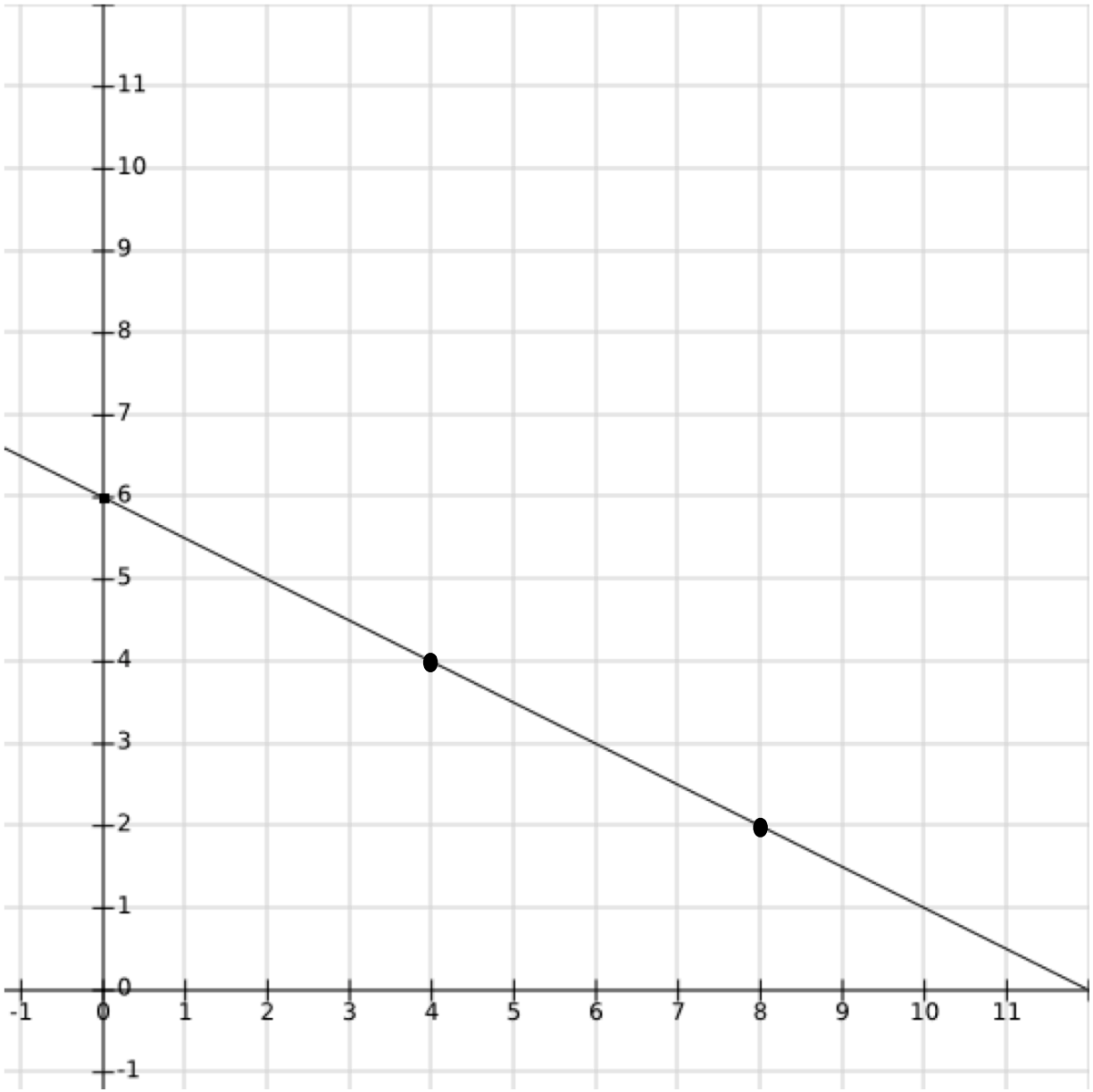
Lines, points & secrets



Quiz Question!
Go to:
`http://socrative.com/`
Student Login
Classroom: **SECUREHSG**

- How many lines pass from these two points?
  Only one straight line!

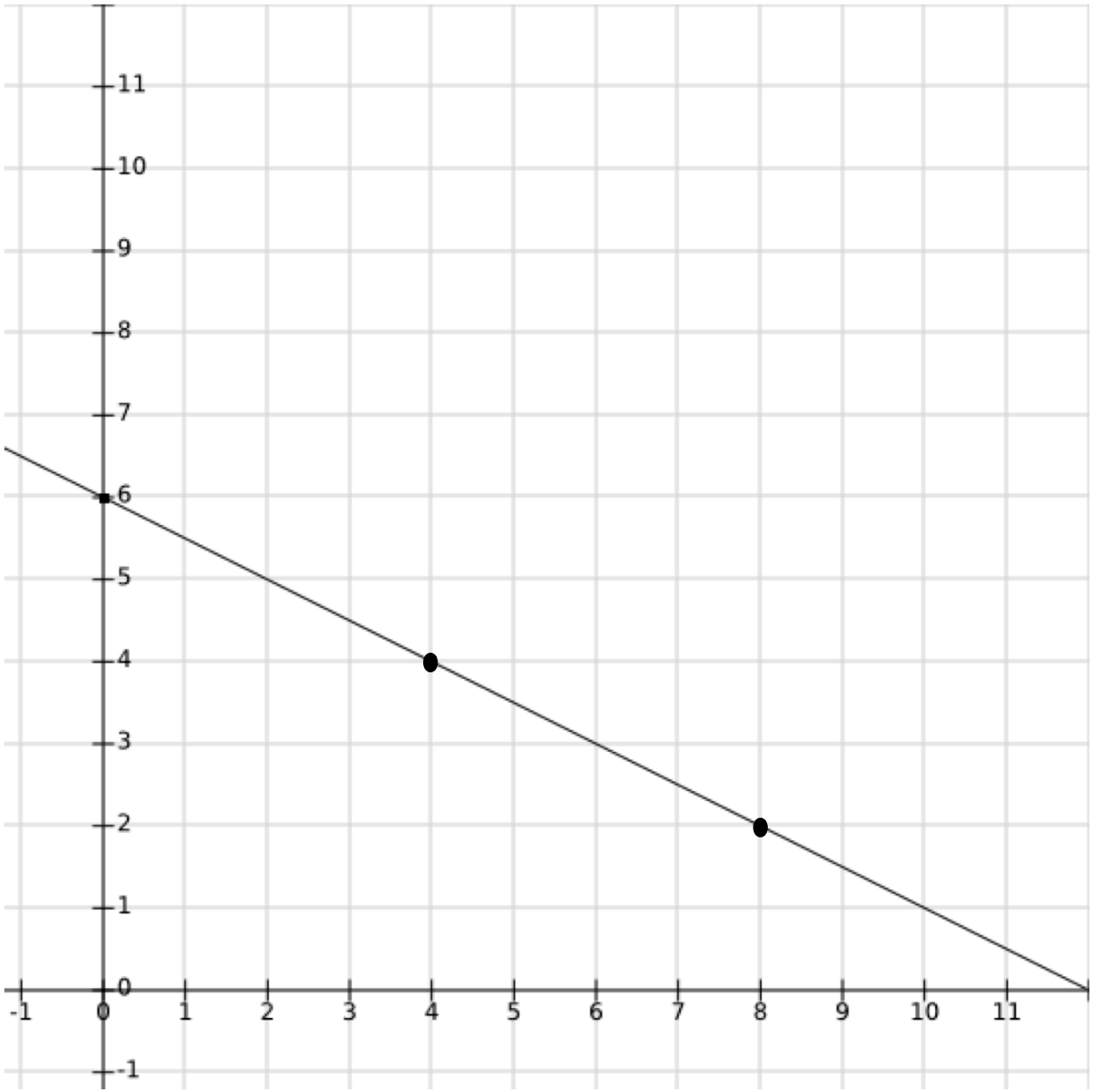
Lines, points & secrets



Quiz Question!
Go to:
`http://socrative.com/`
Student Login
Classroom: **SECUREHSG**

- How many lines pass from these two points? Only one straight line!
- For this line, what can be the value of $\mathbf{f(0)}$?

Lines, points & secrets



Quiz Question!
Go to:
`http://socrative.com/`
Student Login
Classroom: **SECUREHSG**

- How many lines pass from these two points?
  Only one straight line!
- For this line, what can be the value of $\mathbf{f(0)}$?
  6!

Lines, points & secrets

Let's summarise:

- From **one point** can pass **infinitely many straight lines** and the value of $\mathbf{f(0)}$ can be anything!

Lines, points & secrets

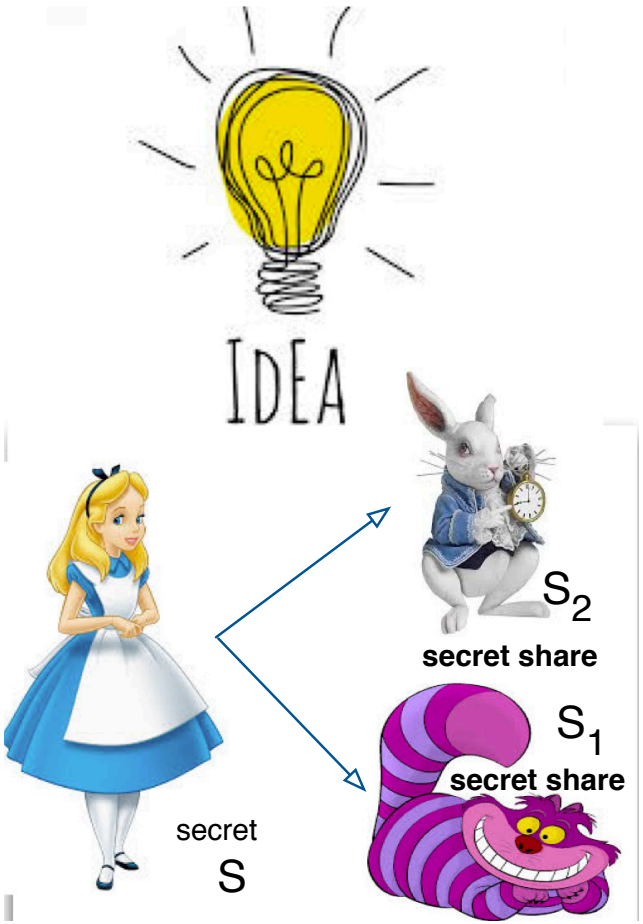
Let's summarise:

- From **one point** can pass **infinitely many straight lines** and the value of $\mathbf{f(0)}$ can be anything!
- From **two points** passes **only one straight line**, and the value of $\mathbf{f(0)}$ can be **only a single value**!

Lines, points & secrets

Let's summarise:

- From **one point** can pass **infinitely many straight lines** and the value of $\mathbf{f(0)}$ can be anything!
- From **two points** passes **only one straight line**, and the value of $\mathbf{f(0)}$ can be **only a single value**!



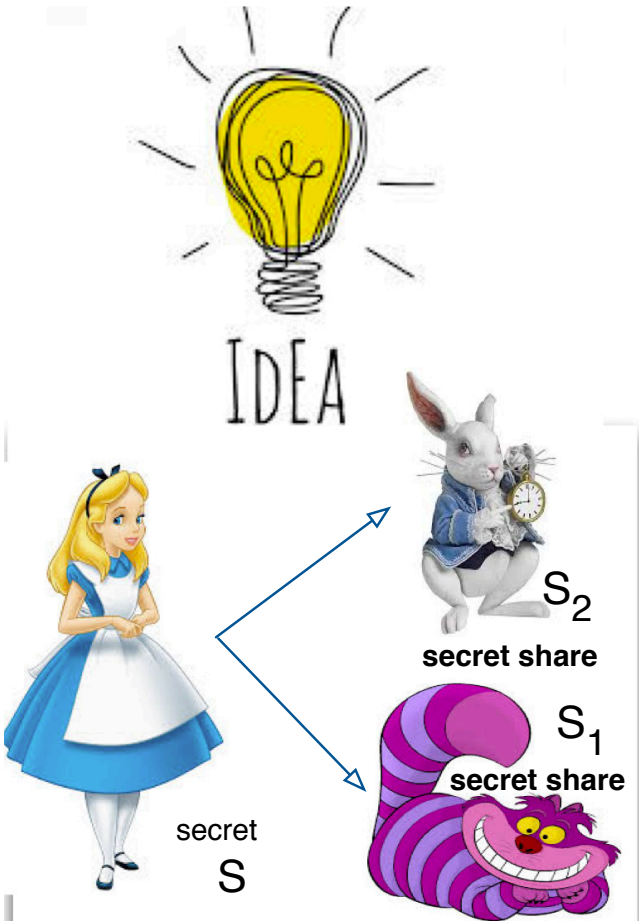
Secret Sharing!

- Alice has a **secret** and wants to split it between Bob and Charliel!

Lines, points & secrets

Let's summarise:

- From **one point** can pass **infinitely many straight lines** and the value of $\mathbf{f(0)}$ can be anything!
- From **two points** passes **only one straight line**, and the value of $\mathbf{f(0)}$ can be **only a single value**!



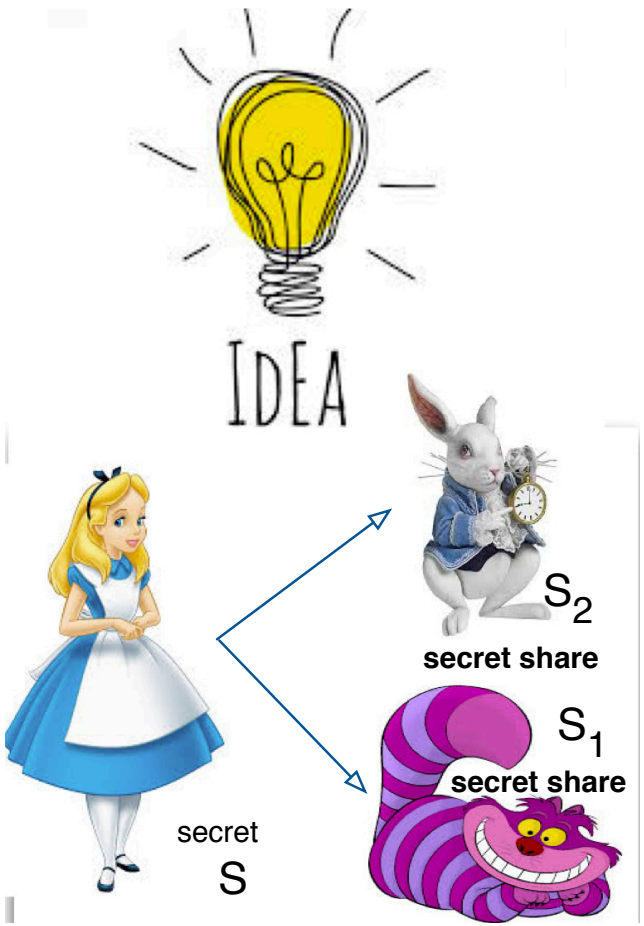
Secret Sharing!

- Alice has a **secret** and wants to split it between Bob and Charliel!
- Alice's secret is number **6**!

Lines, points & secrets

Let's summarise:

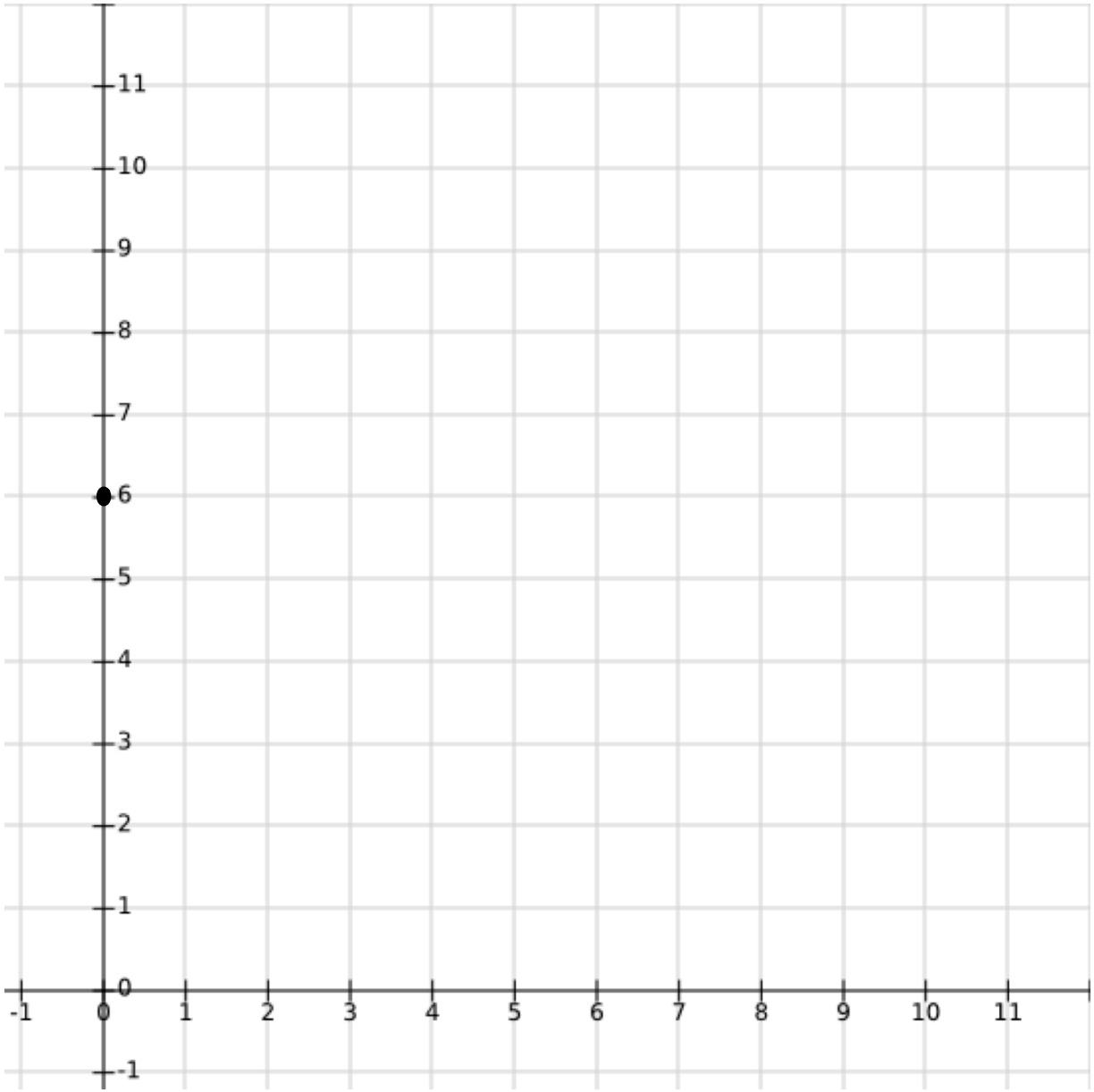
- From **one point** can pass **infinitely many straight lines** and the value of $\mathbf{f(0)}$ can be anything!
- From **two points** passes **only one straight line**, and the value of $\mathbf{f(0)}$ can be **only a single value**!



Secret Sharing!

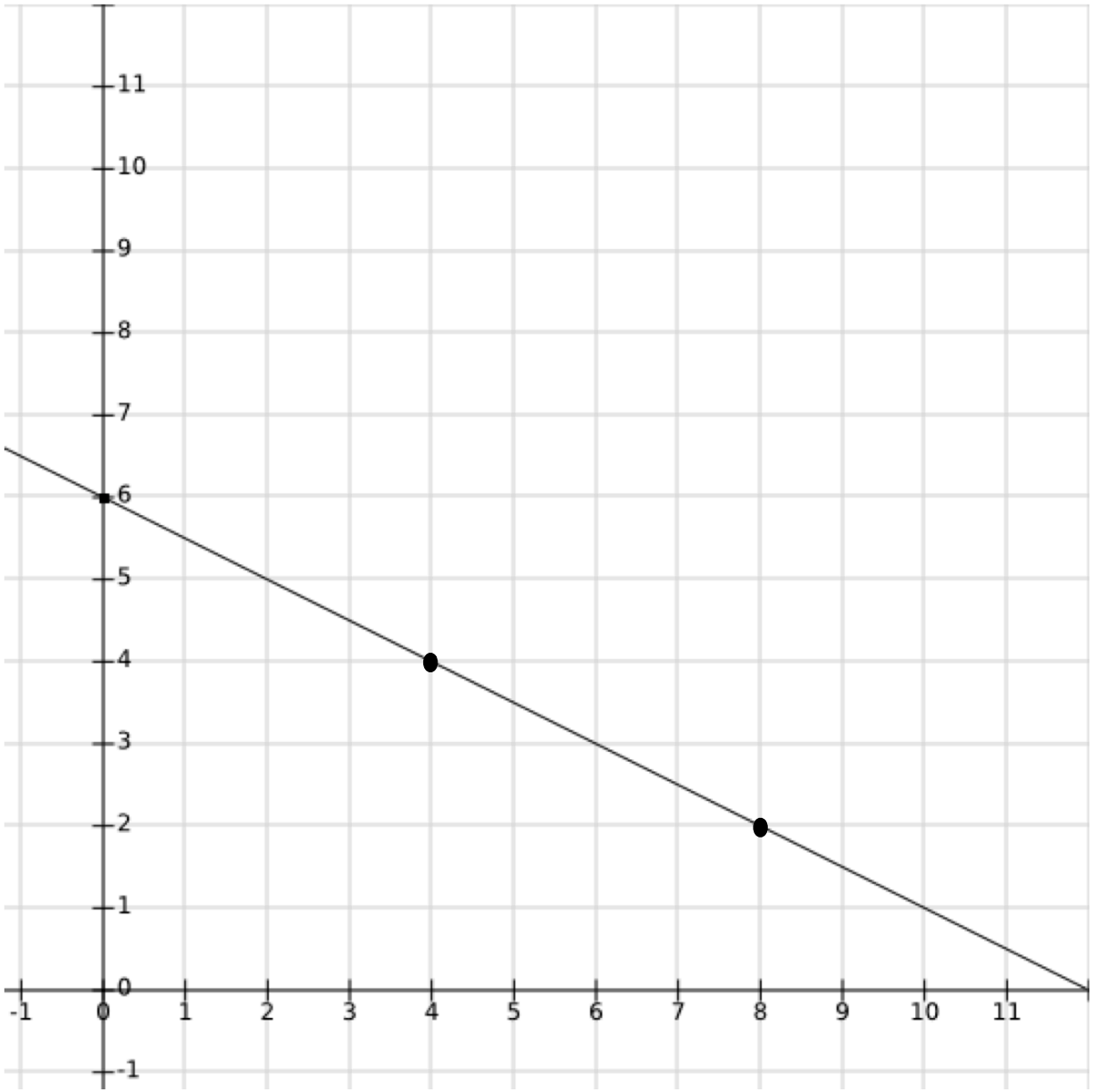
- Alice has a **secret** and wants to split it between Bob and Charliel!
- Alice's secret is number **6**!
- Alice can choose a secret line **f**, such that $\mathbf{f(0) = 6}$ and will give to each of Bob and Charlie one other point of the line.

Lines, points & secrets



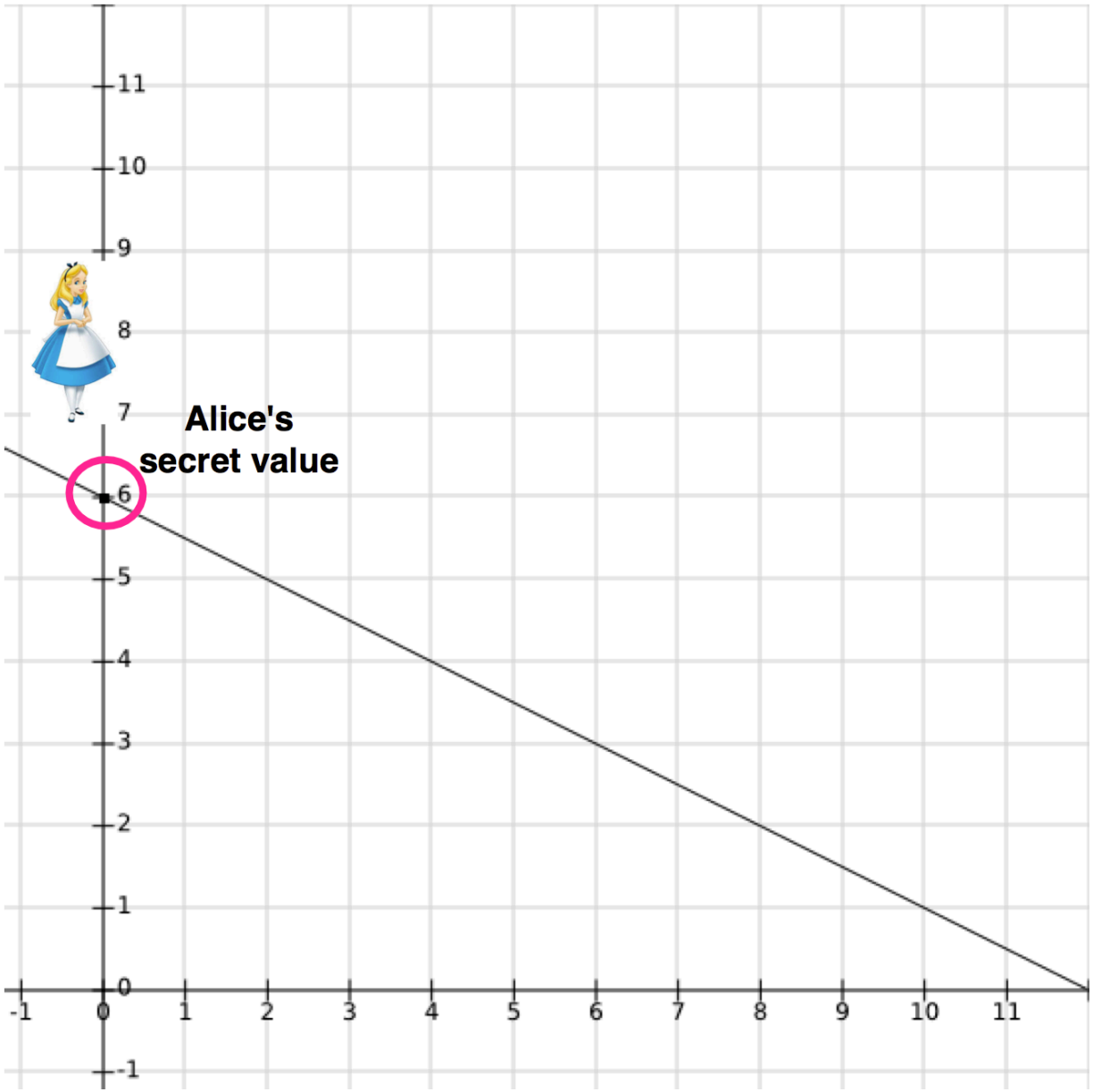
- Lets assume that the secret is $\mathbf{s} = \mathbf{6}$

Lines, points & secrets



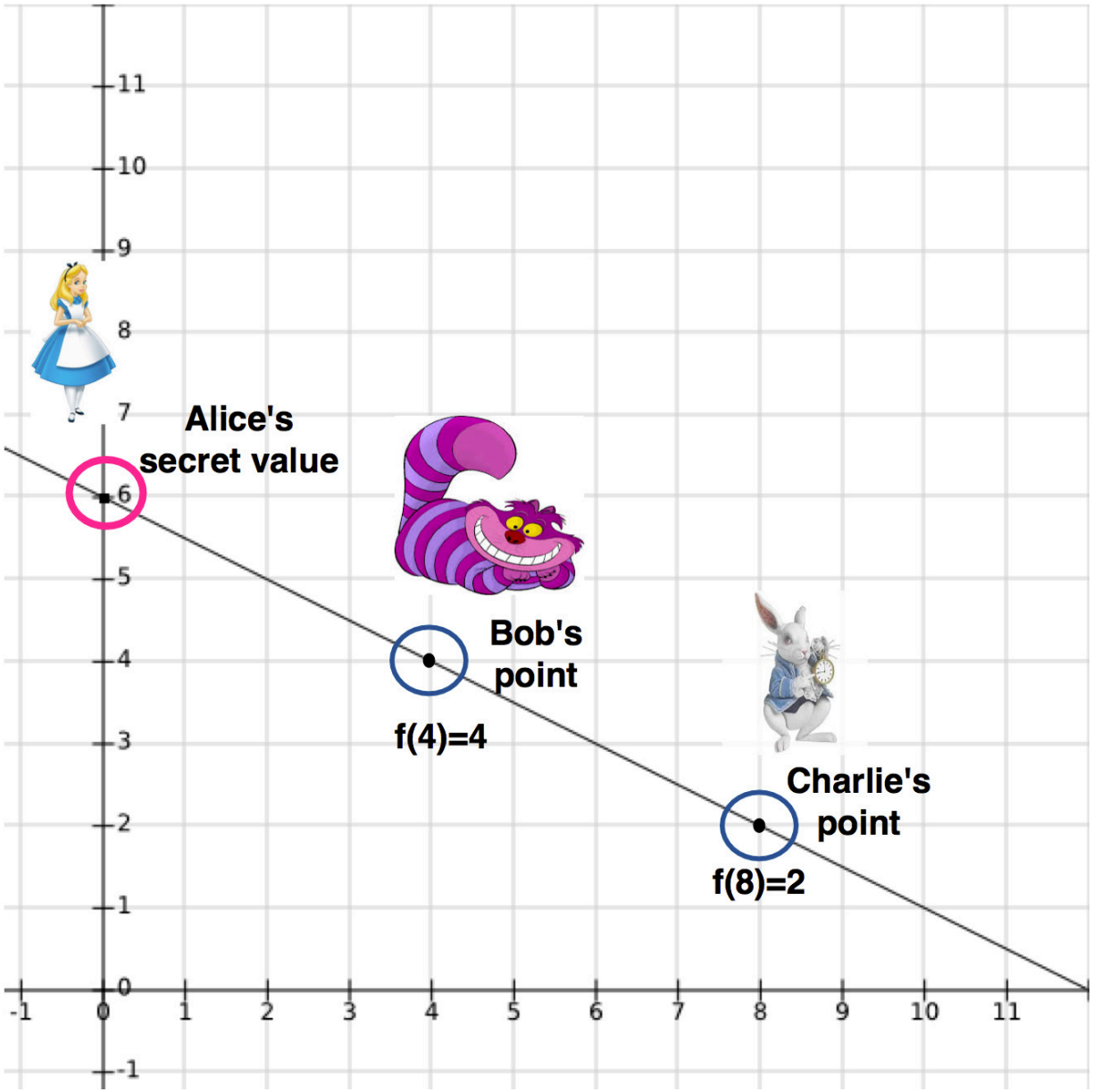
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 0.5x}$

Lines, points & secrets



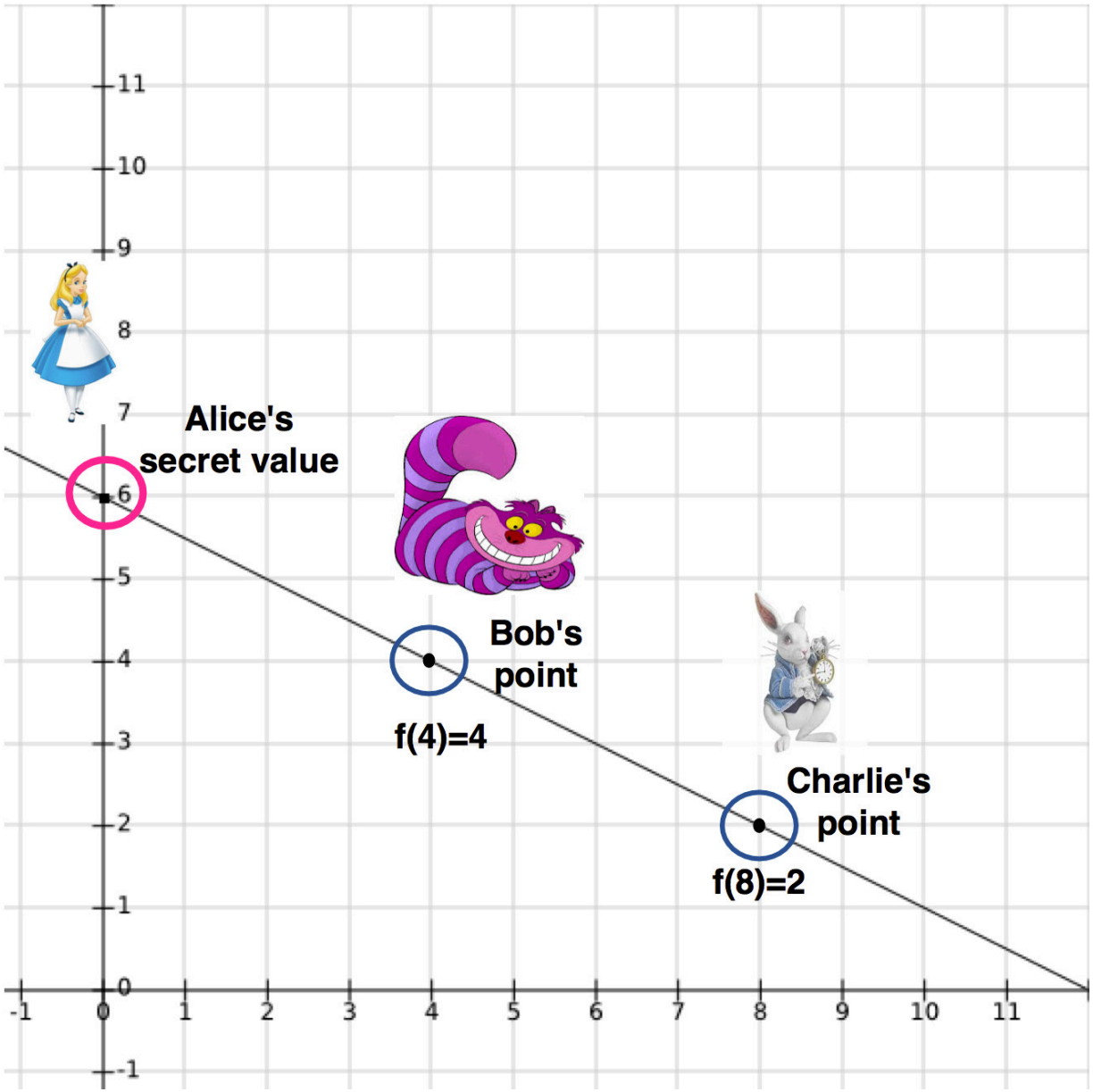
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 0.5x}$

Lines, points & secrets



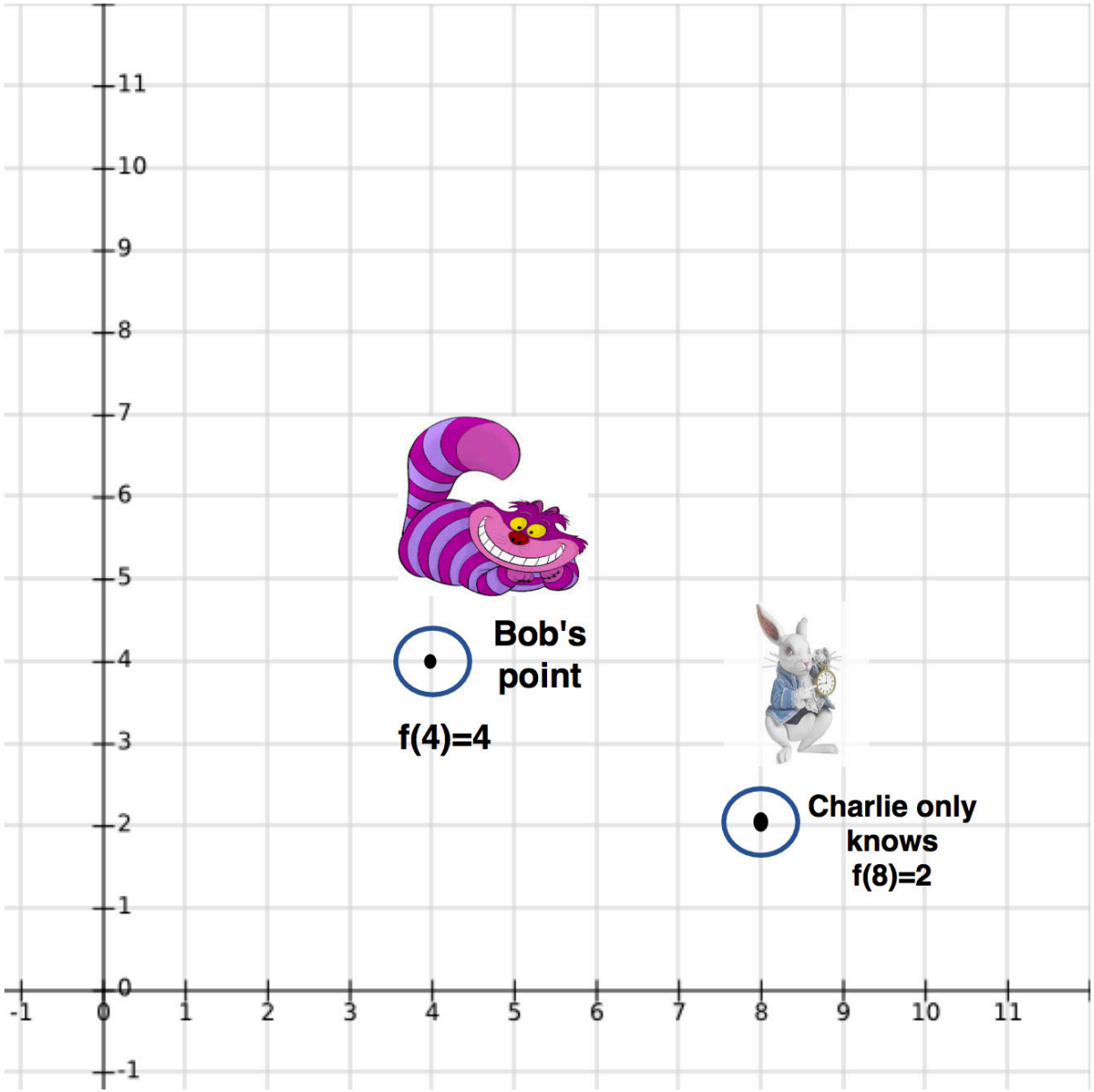
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 0.5x}$
- Alice sends two points (not $\mathbf{f(0)}$) one to Bob and one to Charlie.

Lines, points & secrets



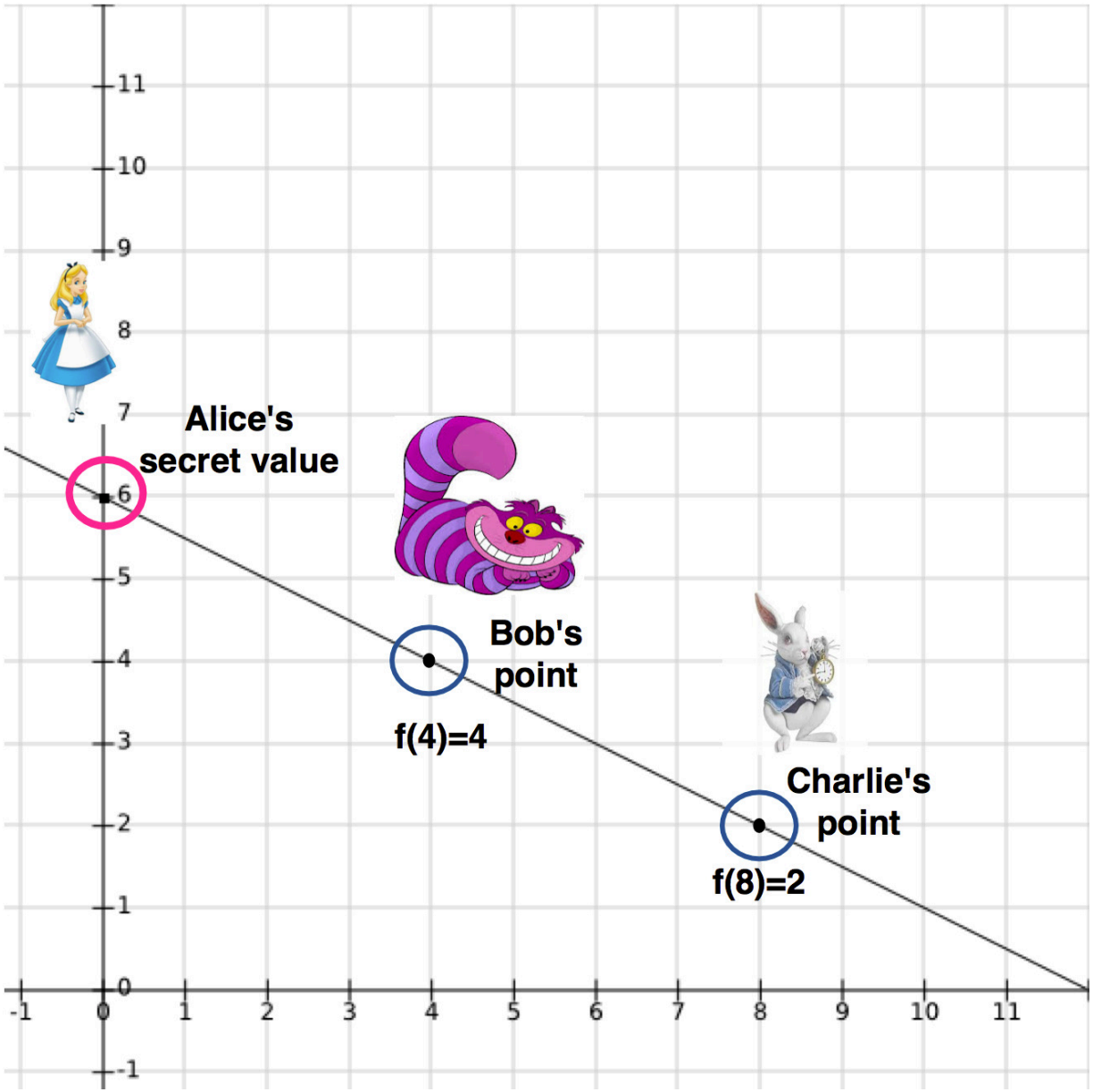
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 0.5x}$
- Alice sends two points (not $\mathbf{f(0)}$) one to Bob and one to Charlie.
- These points are the shares of the secret!

Lines, points & secrets



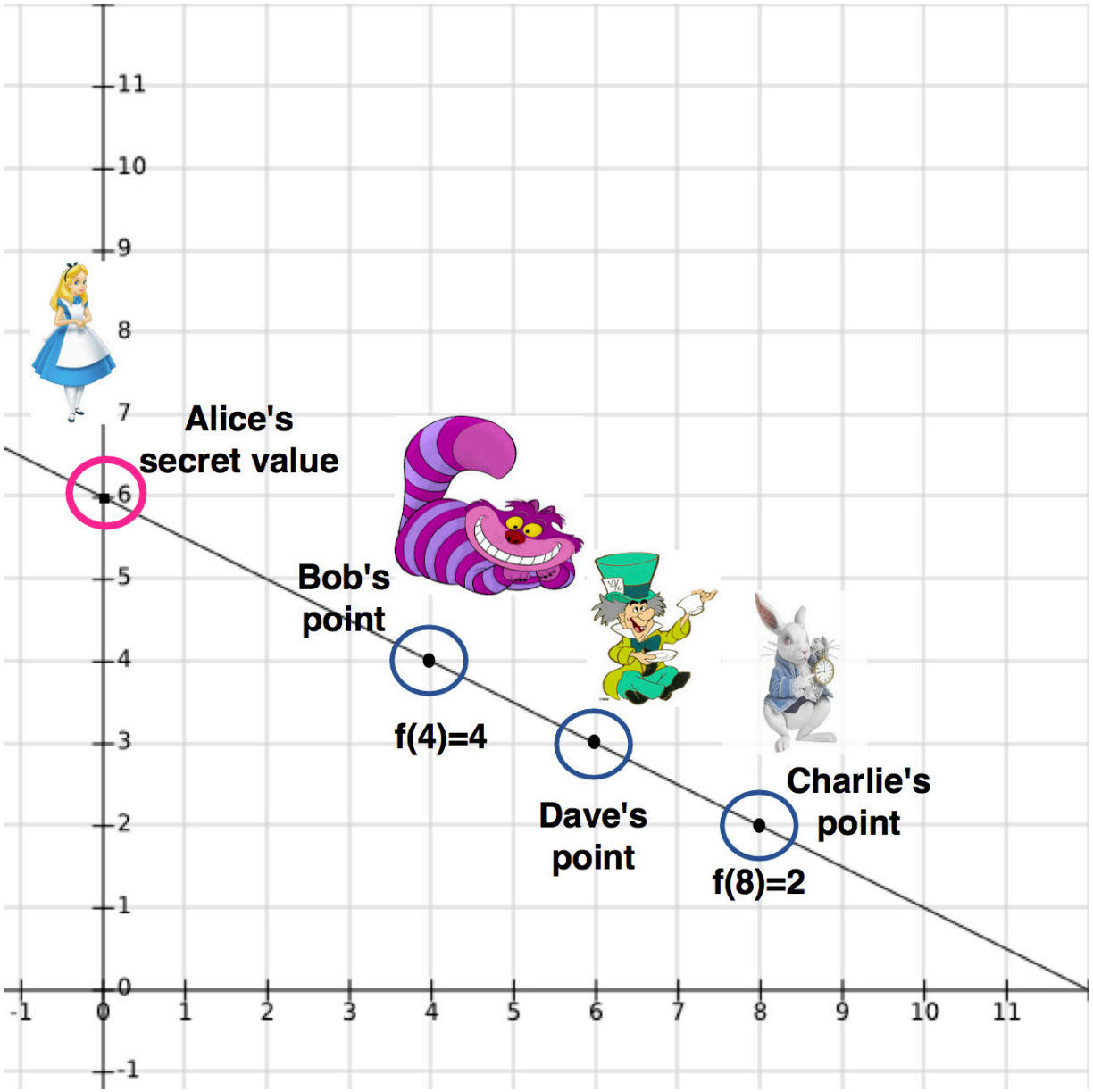
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 0.5x}$
- Alice sends two points (not $\mathbf{f(0)}$) one to Bob and one to Charlie.
- These points are the shares of the secret!
- Together Bob and Charlie can compute the secret line and find the secret $\mathbf{f(0) = 6}$.

Lines, points & secrets



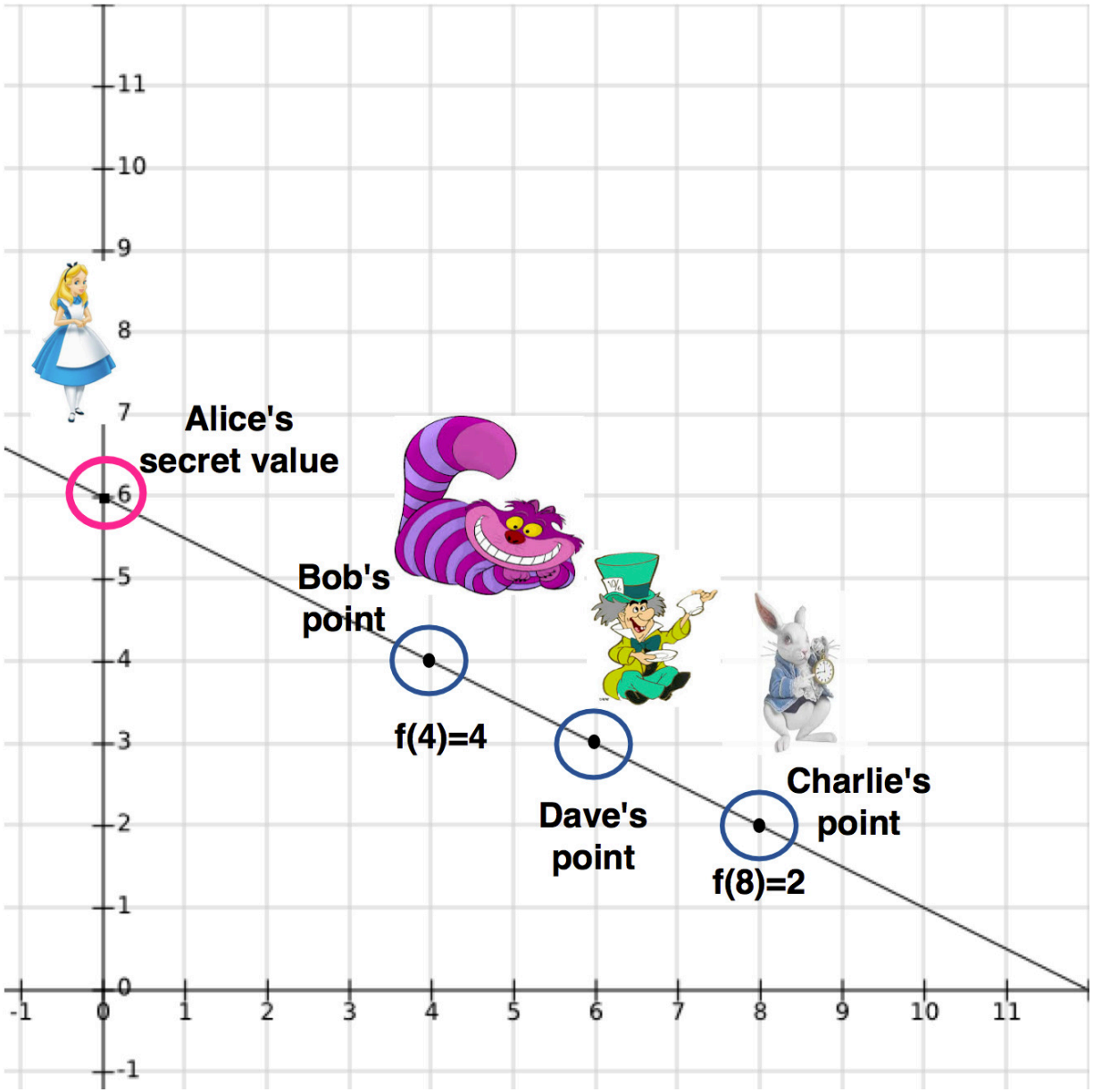
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 0.5x}$
- Alice sends two points (not $\mathbf{f(0)}$) one to Bob and one to Charlie.
- These points are the shares of the secret!
- Together Bob and Charlie can compute the secret line and find the secret $\mathbf{f(0) = 6}$.

Lines, points & secrets



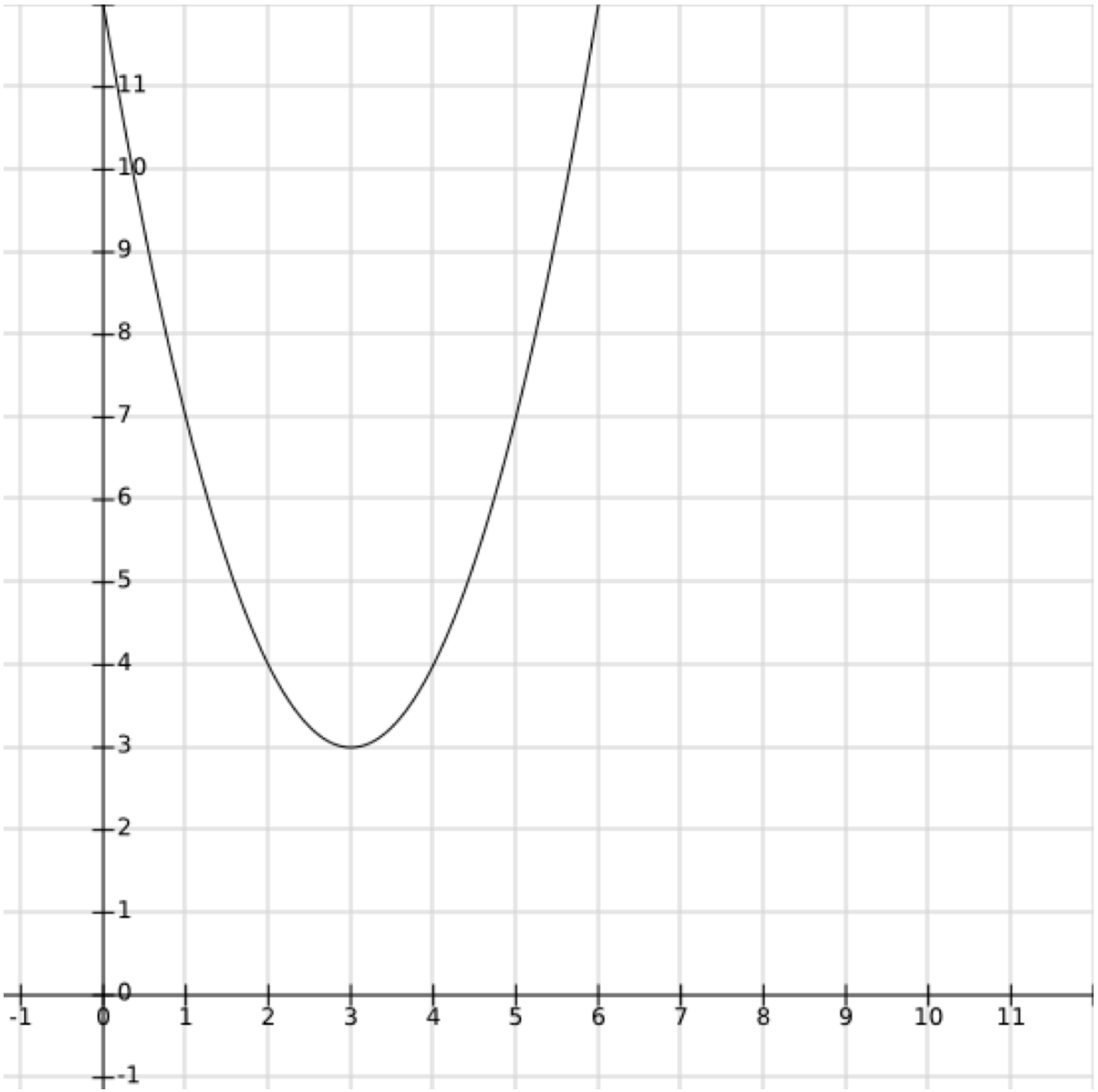
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 0.5x}$
- Alice sends two points (not $\mathbf{f(0)}$) one to Bob and one to Charlie.
- These points are the shares of the secret!
- Together Bob and Charlie can compute the secret line and find the secret $\mathbf{f(0) = 6}$.
- If Alice gives another point to Dave. Who can then compute the secret?

Lines, points & secrets



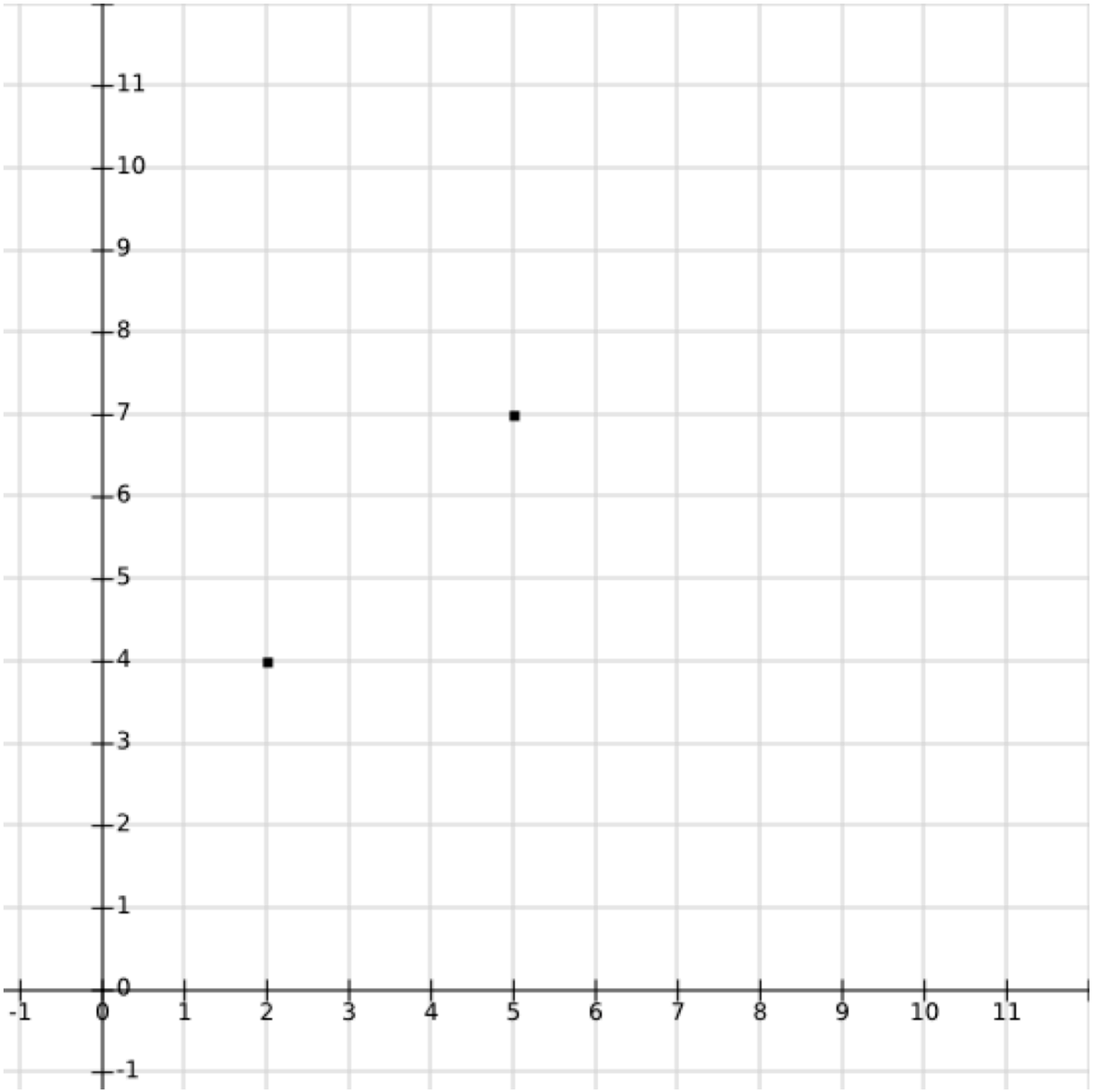
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 0.5x}$
- Alice sends two points (not $\mathbf{f(0)}$) one to Bob and one to Charlie.
- These points are the shares of the secret!
- Together Bob and Charlie can compute the secret line and find the secret $\mathbf{f(0) = 6}$.
- If Alice gives another point to Dave. Who can then compute the secret?
- Any two are sufficient!

Lines, points & secrets



A quadratic line!

Lines, points & secrets

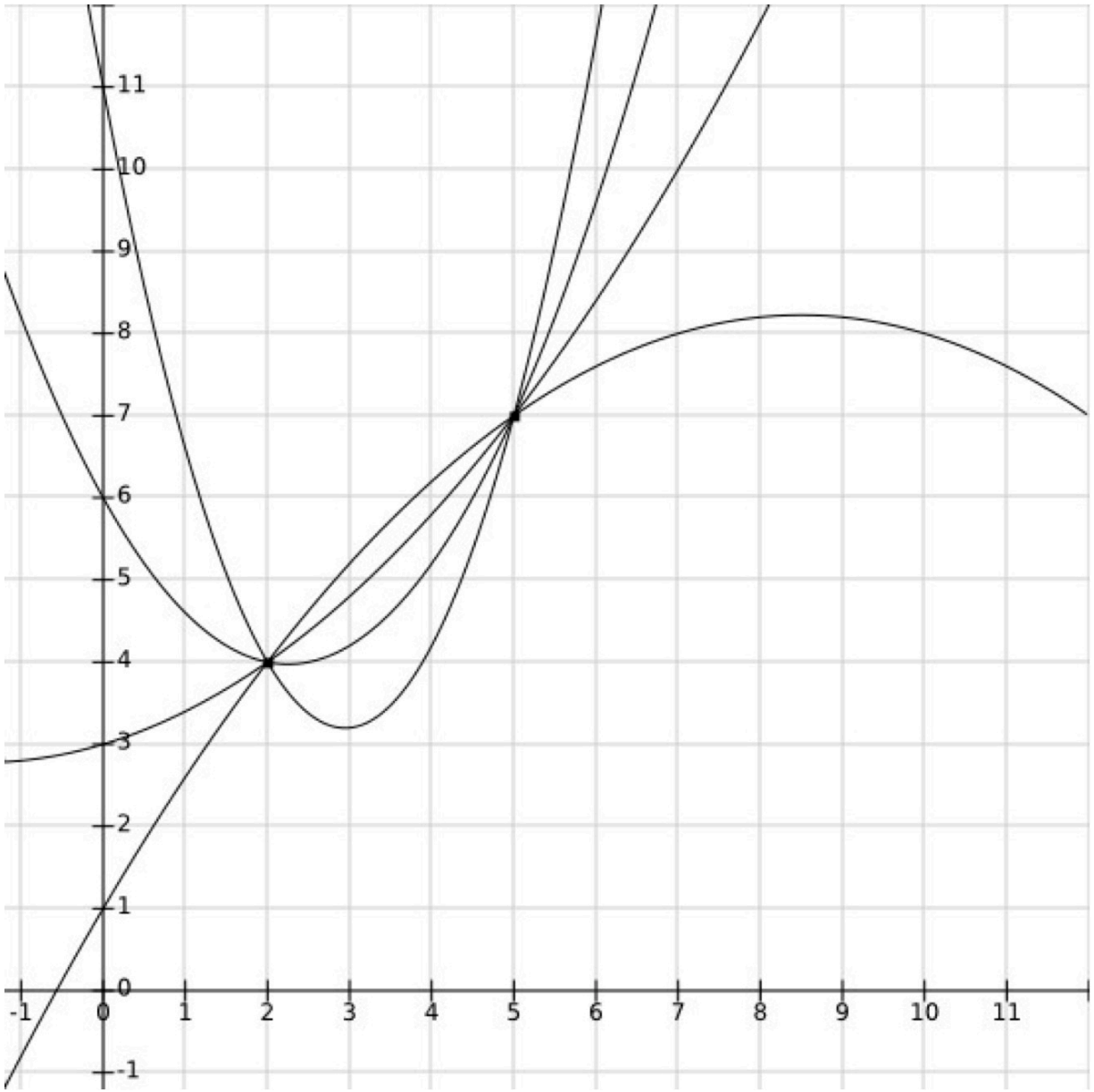


Quiz Question!

Go to:
`http://socrative.com/`
Student Login
Classroom: **SECUREHSG**

- How many **quadratic** lines pass from these two points?

Lines, points & secrets



Quiz Question!

Go to:

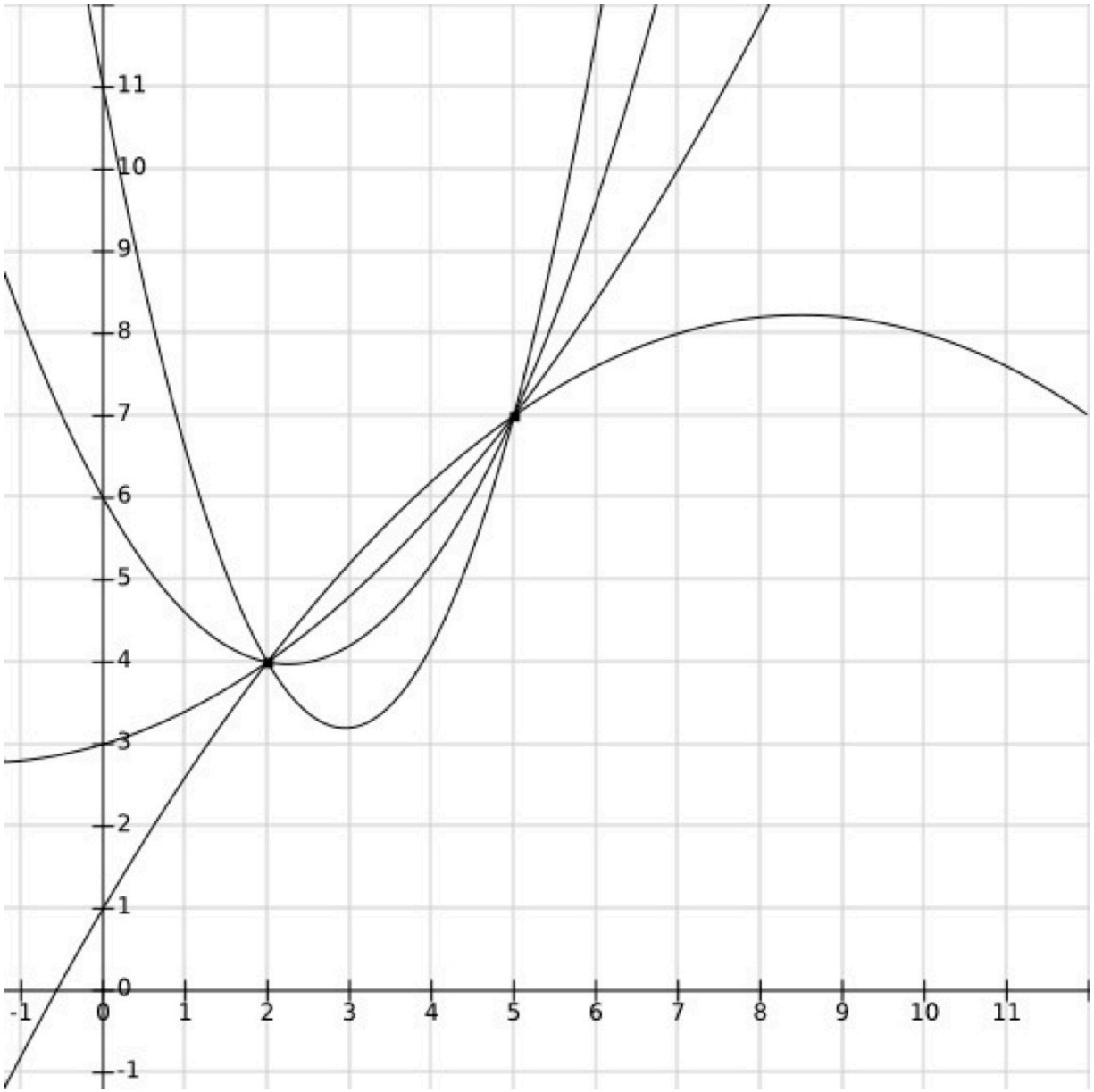
`http://socrative.com/`

Student Login

Classroom: **SECUREHSG**

- How many **quadratic** lines pass from these two points?
  Infinitely many!

Lines, points & secrets



Quiz Question!

Go to:

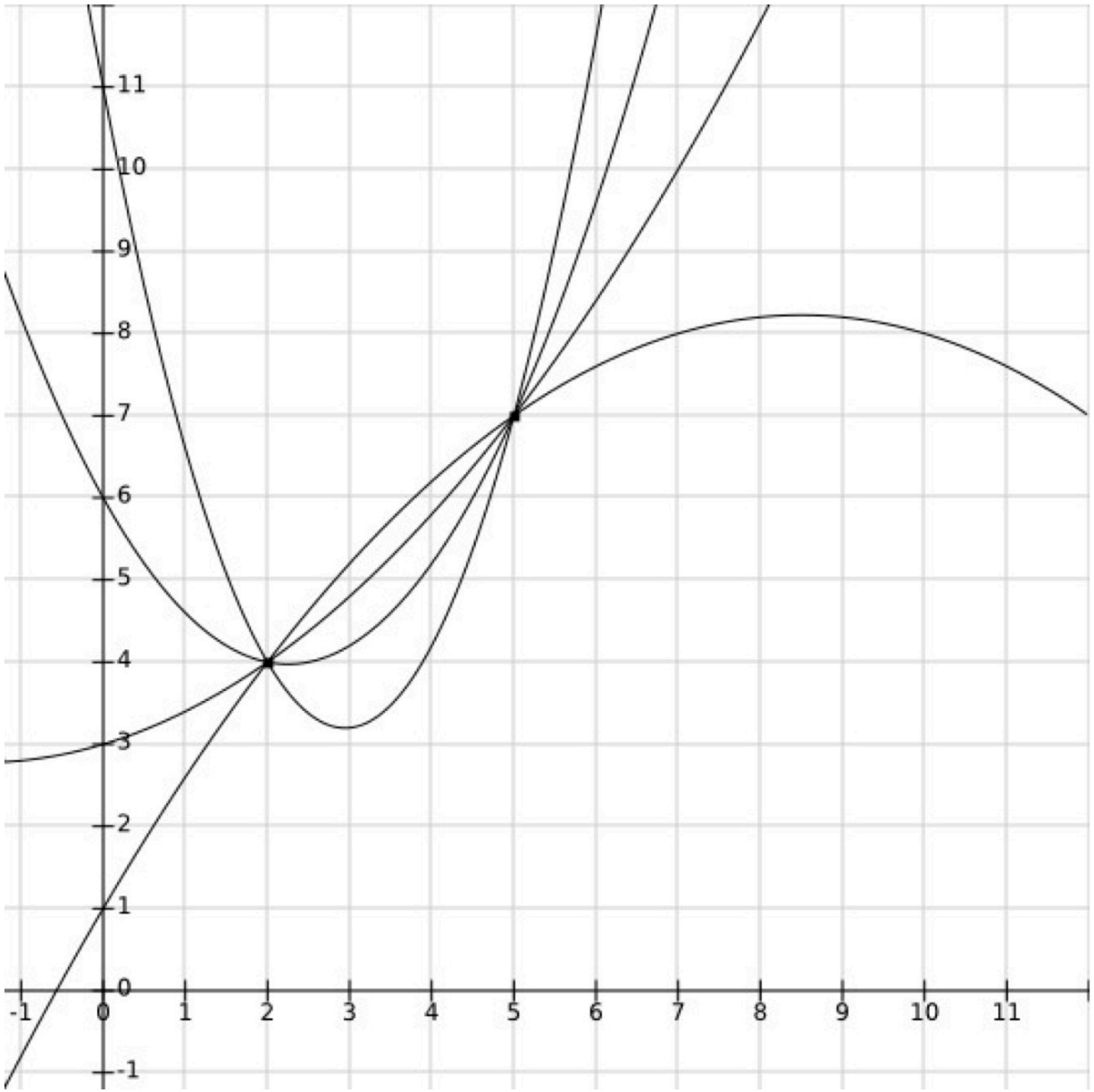
`http://socrative.com/`

Student Login

Classroom: **SECUREHSG**

- How many **quadratic** lines pass from these two points?
  Infinitely many!
- For these lines, what can be the value $\mathbf{f(0)}$?

Lines, points & secrets



Quiz Question!

Go to:

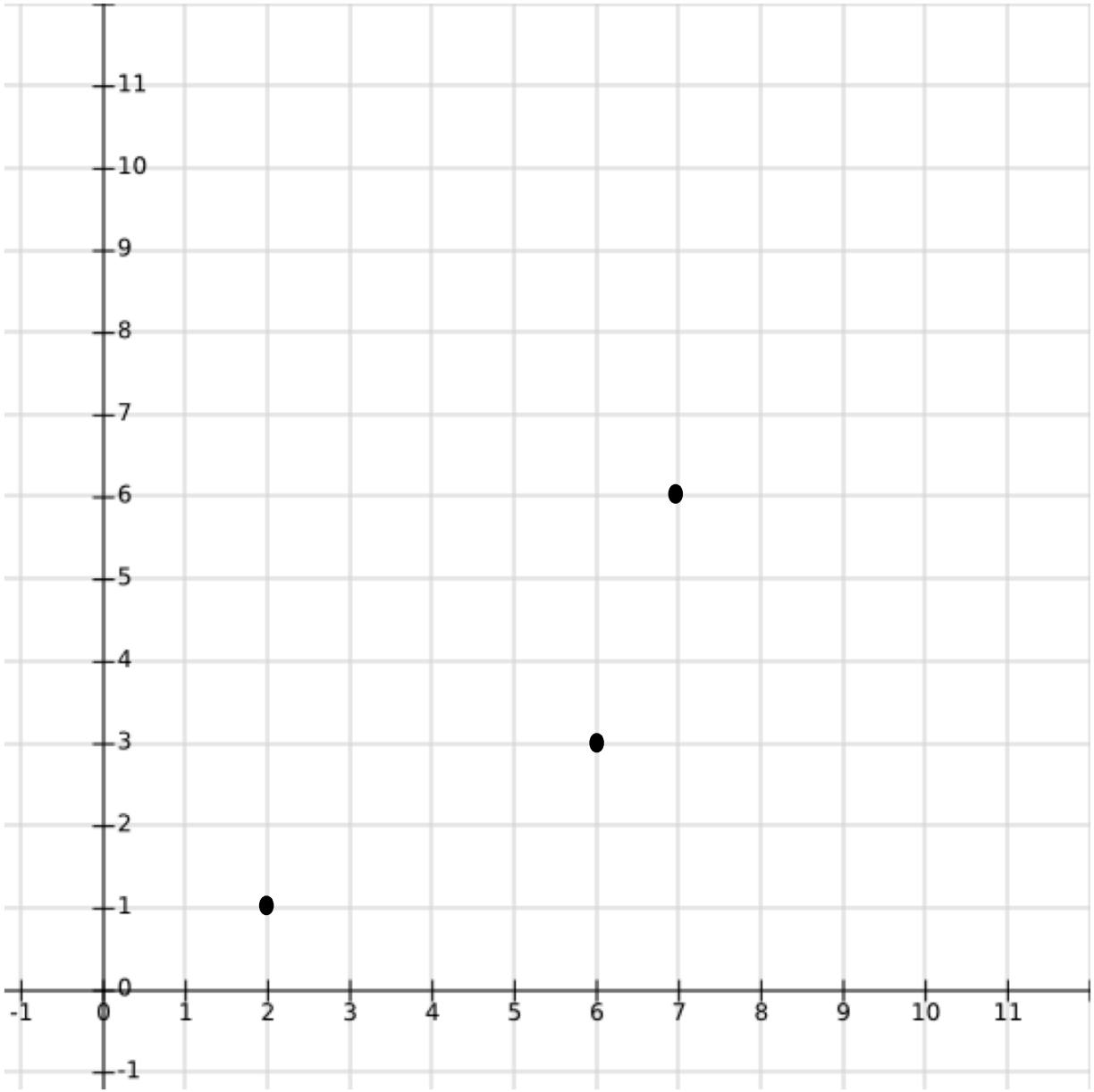
`http://socrative.com/`

Student Login

Classroom: **SECUREHSG**

- How many **quadratic** lines pass from these two points?
  Infinitely many!
- For these lines, what can be the value $\mathbf{f(0)}$?
  Anything!

Lines, points & secrets



Quiz Question!

Go to:

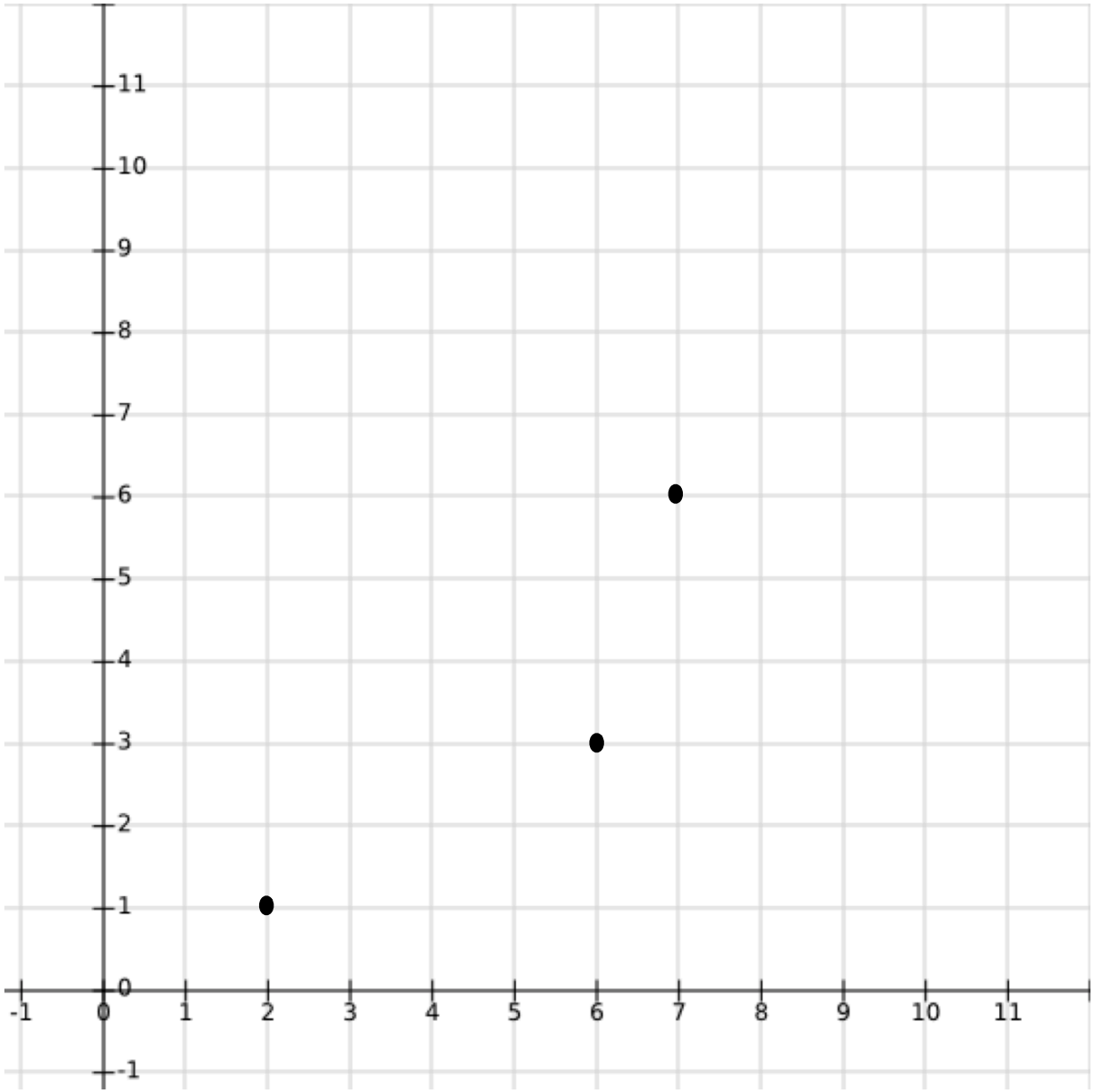
`http://socrative.com/`

Student Login

Classroom: **SECUREHSG**

- How many quadratic lines pass from these **three** points?

Lines, points & secrets



Quiz Question!

Go to:

`http://socrative.com/`

Student Login

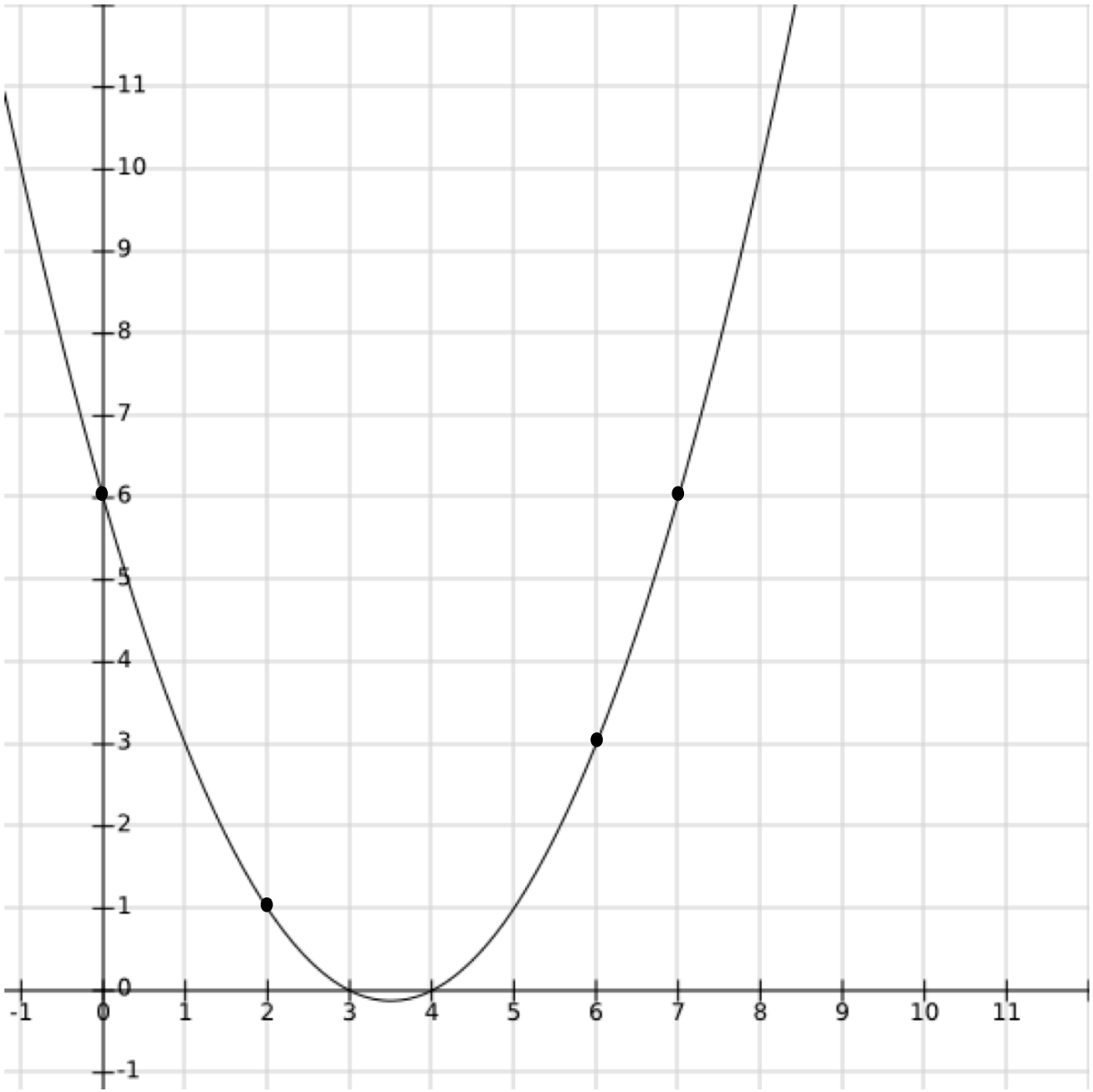
Classroom: **SECUREHSG**

- How many quadratic lines pass from these **three** points?

  Only one quadratic line!

  $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$

Lines, points & secrets



Quiz Question!

Go to:

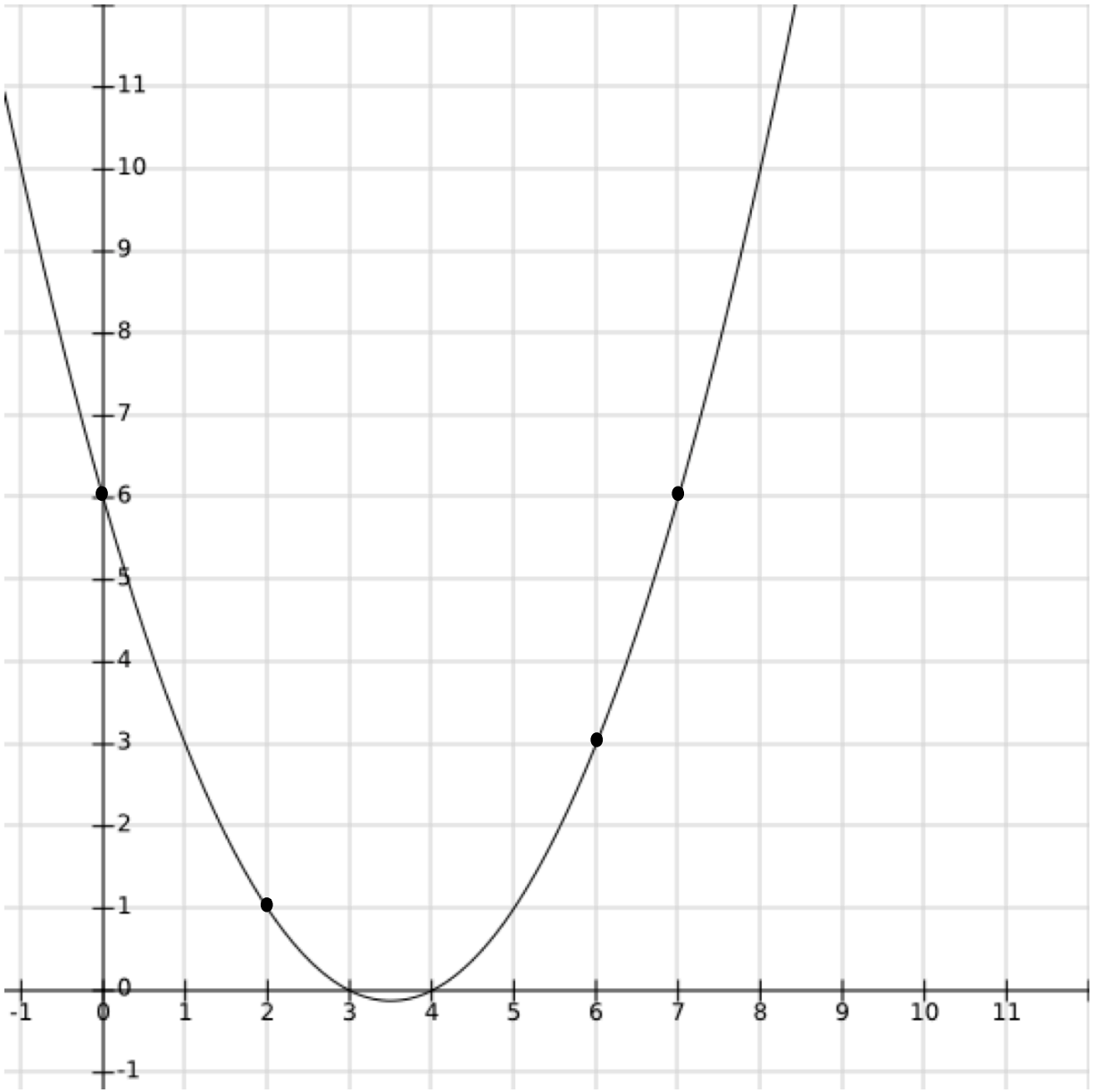
`http://socrative.com/`

Student Login

Classroom: **SECUREHSG**

- How many quadratic lines pass from these **three** points?
  Only one quadratic line!
  $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$
- For this line, what can be the value of $\mathbf{f(0)}$?

Lines, points & secrets



Quiz Question!

Go to:

`http://socrative.com/`

Student Login

Classroom: **SECUREHSG**

- How many quadratic lines pass from these **three** points?
  Only one quadratic line!
  $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$
- For this line, what can be the value of $\mathbf{f(0)}$?
  6!

Lines, points & secret sharing

Let's summarise:

- From **two points** can pass infinitely many quadratic lines lines and the value of $\mathbf{f(0)}$ can be anything!

Lines, points & secret sharing

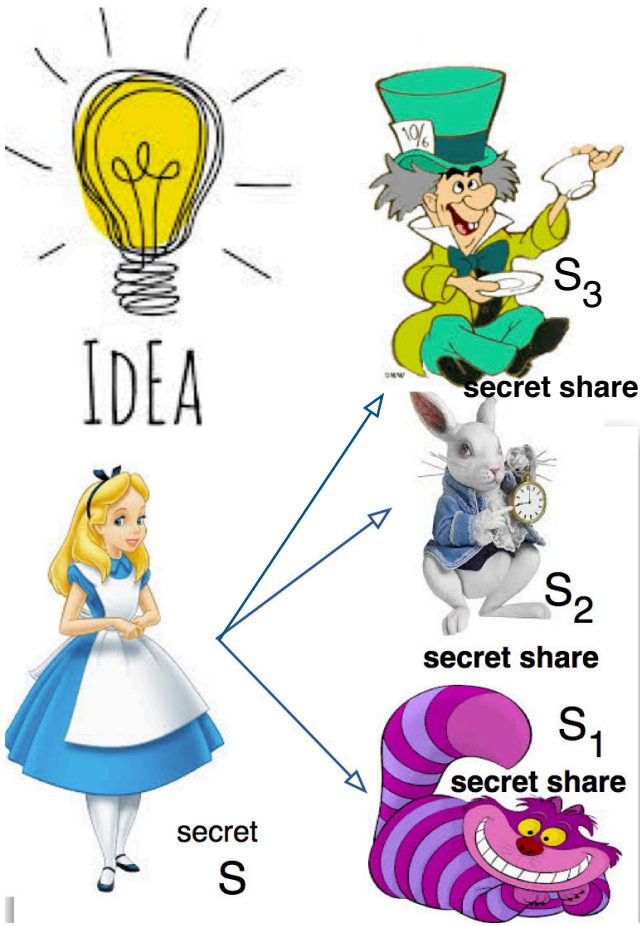
Let's summarise:

- From **two points** can pass infinitely many quadratic lines lines and the value of $\mathbf{f(0)}$ can be anything!
- From **three points** passes only one quadratic line, and the value of $\mathbf{f(0)}$ can be only a single value!

Lines, points & secret sharing

Let's summarise:

- From **two points** can pass infinitely many quadratic lines lines and the value of $\mathbf{f(0)}$ can be anything!
- From **three points** passes only one quadratic line, and the value of $\mathbf{f(0)}$ can be only a single value!



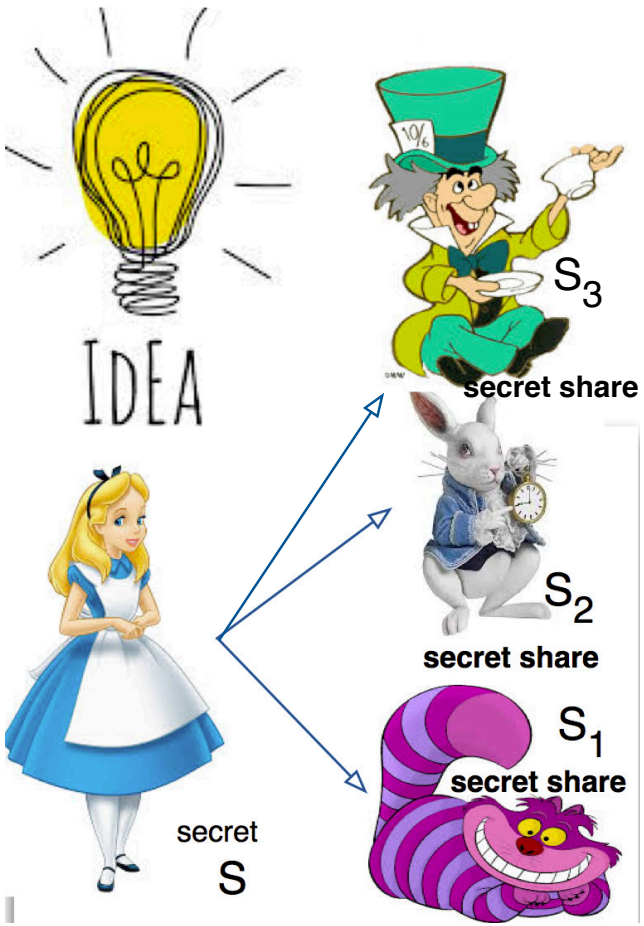
Secret Sharing!

- Alice has a **secret** and wants to split it between Bob, Charlie and Dave!

Lines, points & secret sharing

Let's summarise:

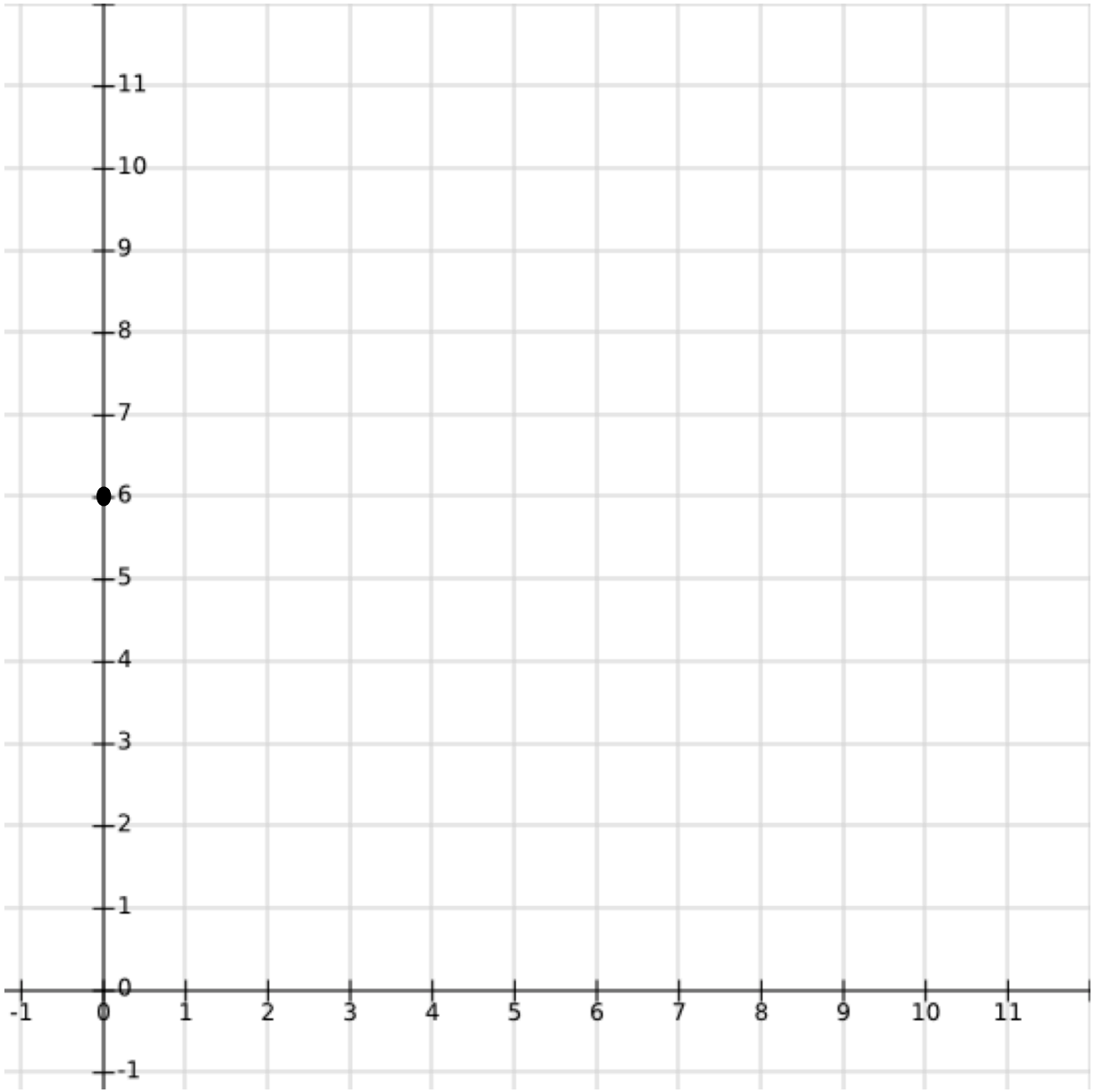
- From **two points** can pass infinitely many quadratic lines lines and the value of $\mathbf{f(0)}$ can be anything!
- From **three points** passes only one quadratic line, and the value of $\mathbf{f(0)}$ can be only a single value!



Secret Sharing!

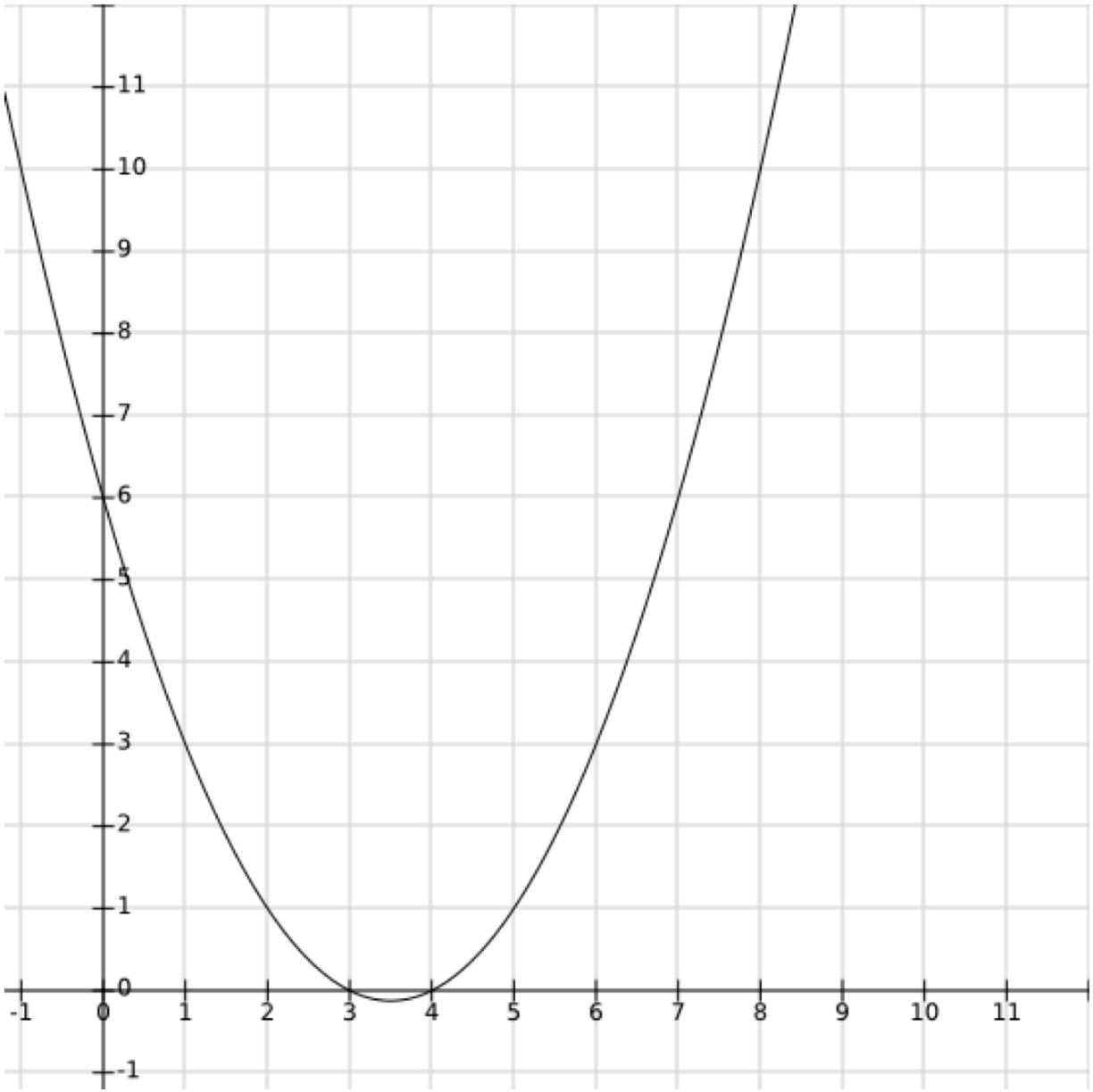
- Alice has a **secret** and wants to split it between Bob, Charlie and Dave!
- Alice's secret is number **6**!
- Alice can choose a secret quadratic line $\mathbf{f}$, such that $\mathbf{f(0) = 6}$ and will give to Bob, Charlie and Dave one other point of the line.

Lines, points & secrets



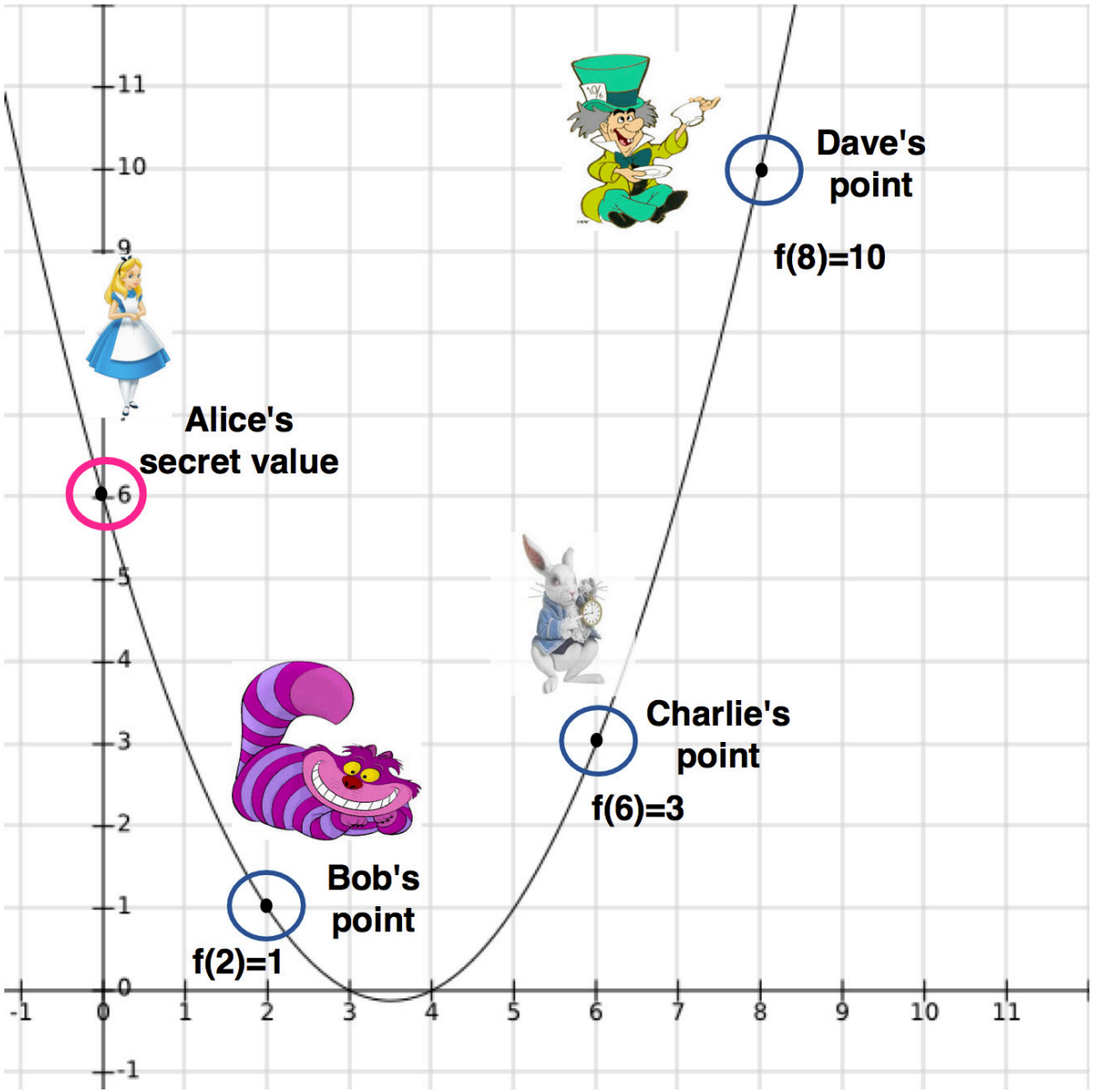
- Lets assume that the secret is $\mathbf{s} = \mathbf{6}$

Lines, points & secrets



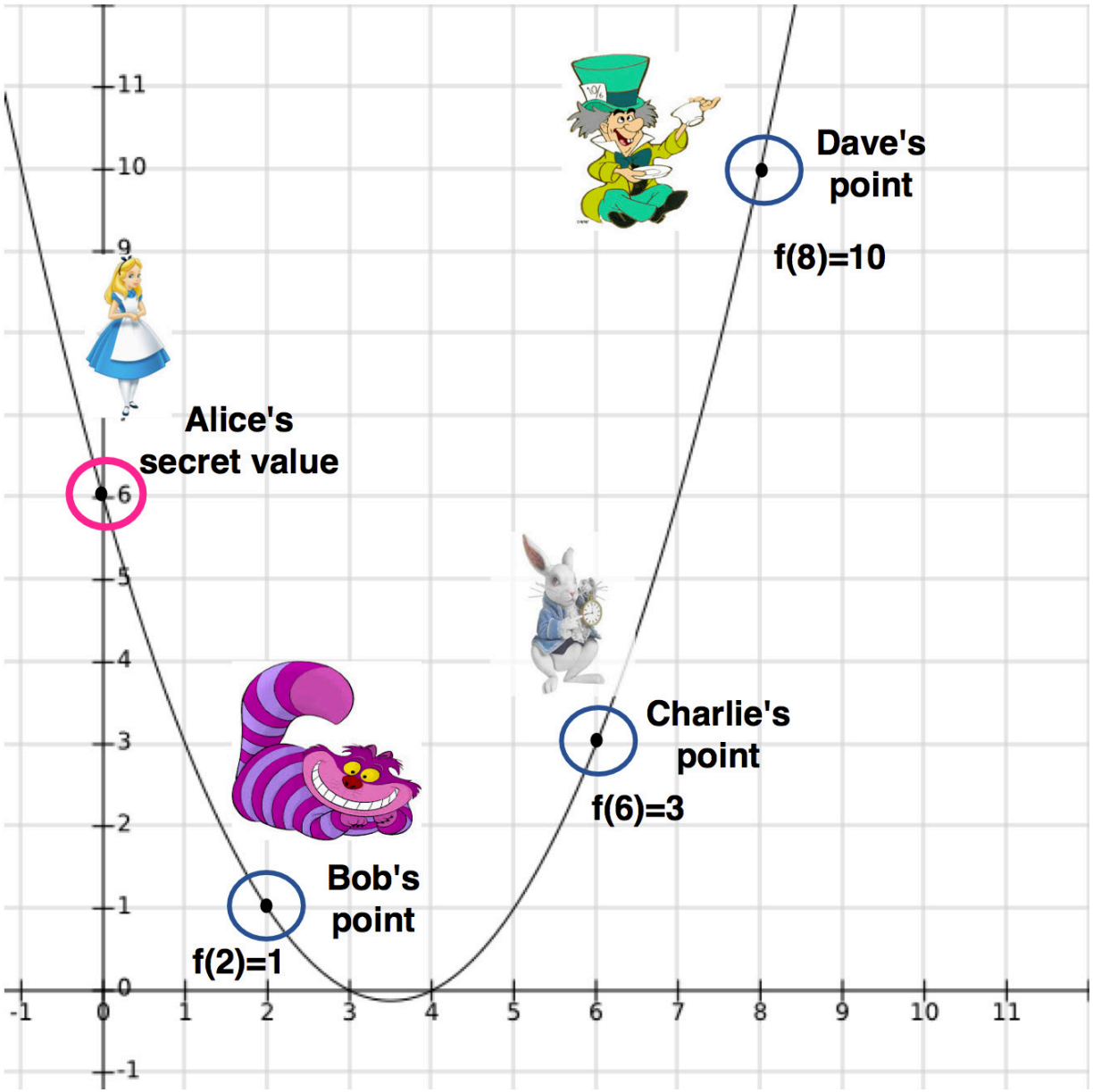
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$

Lines, points & secrets



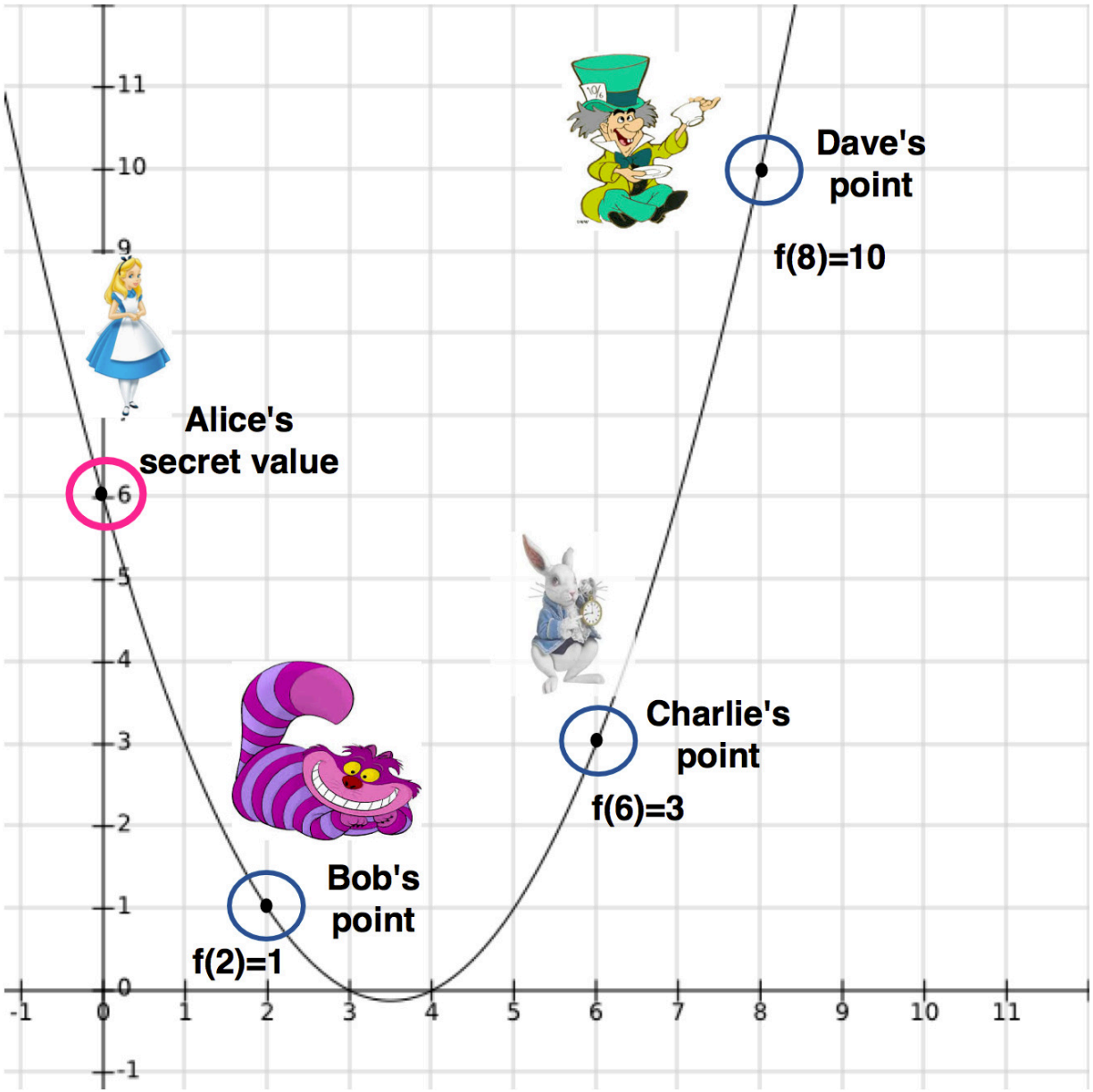
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$

Lines, points & secrets



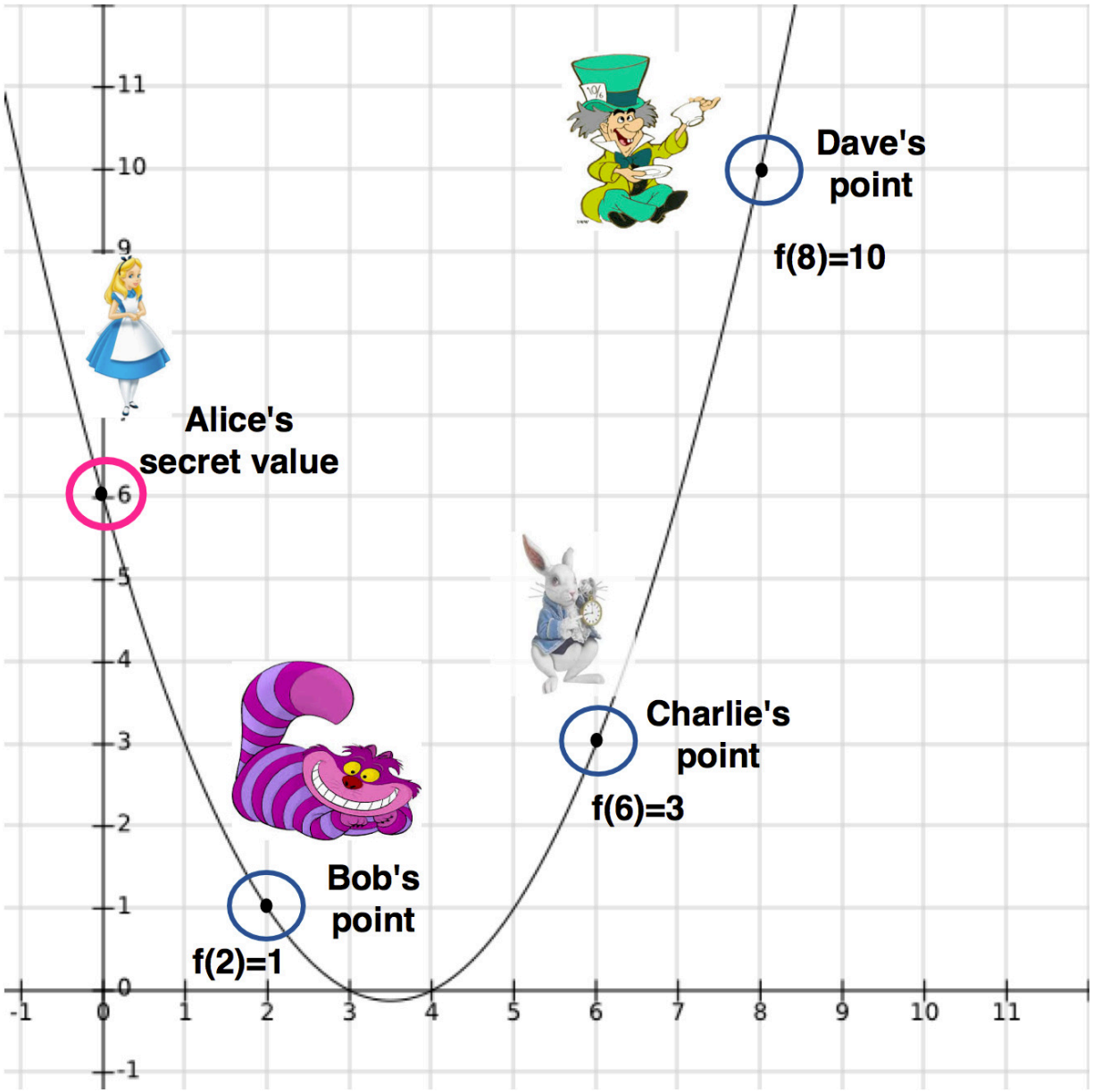
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$
- Alice sends three points (not $\mathbf{f(0)}$) one to Bob, one to Charlie and one to Dave.

Lines, points & secrets



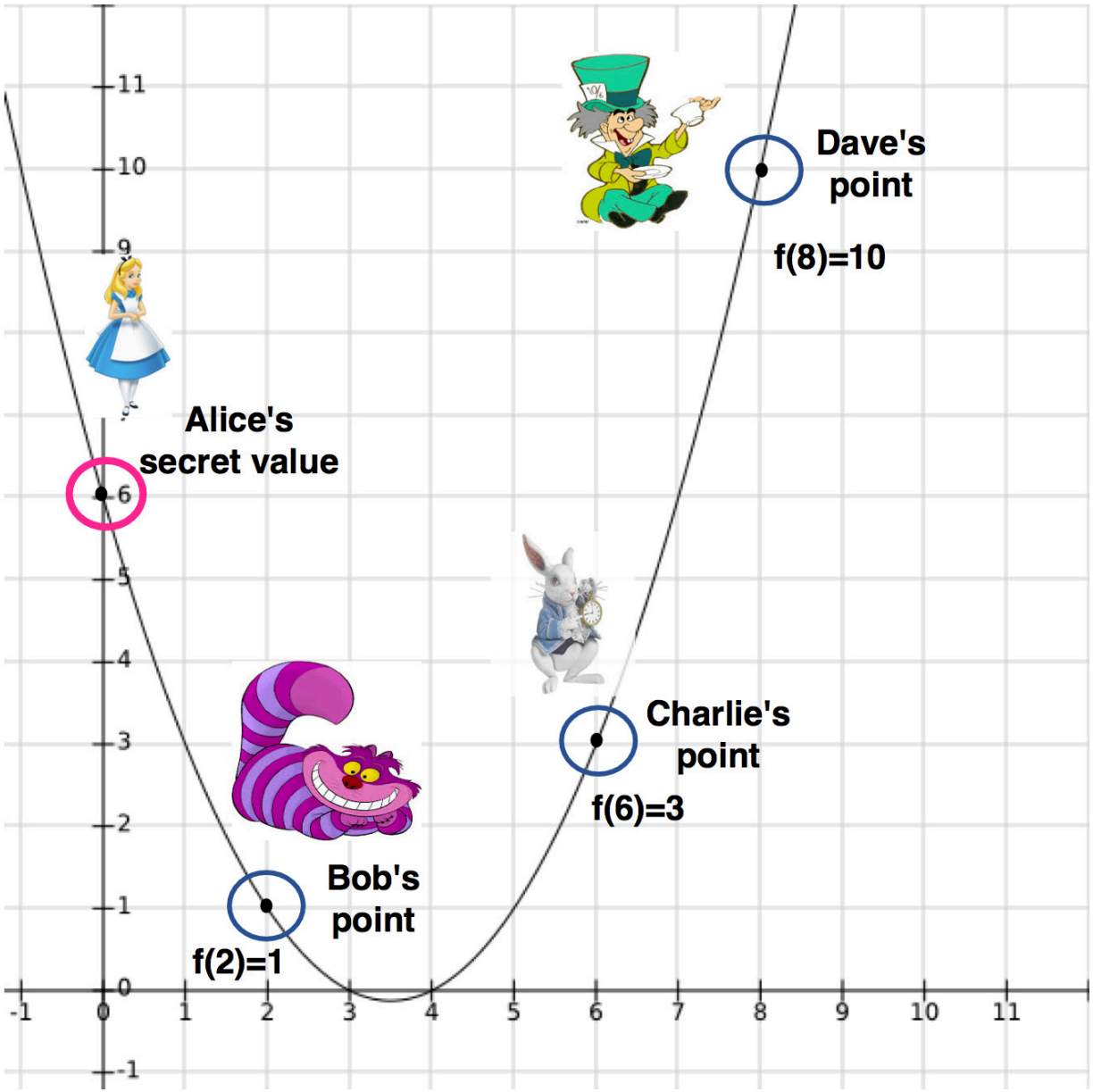
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$
- Alice sends three points (not $\mathbf{f(0)}$) one to Bob, one to Charlie and one to Dave.
- These points are the **shares** of the secret!

Lines, points & secrets



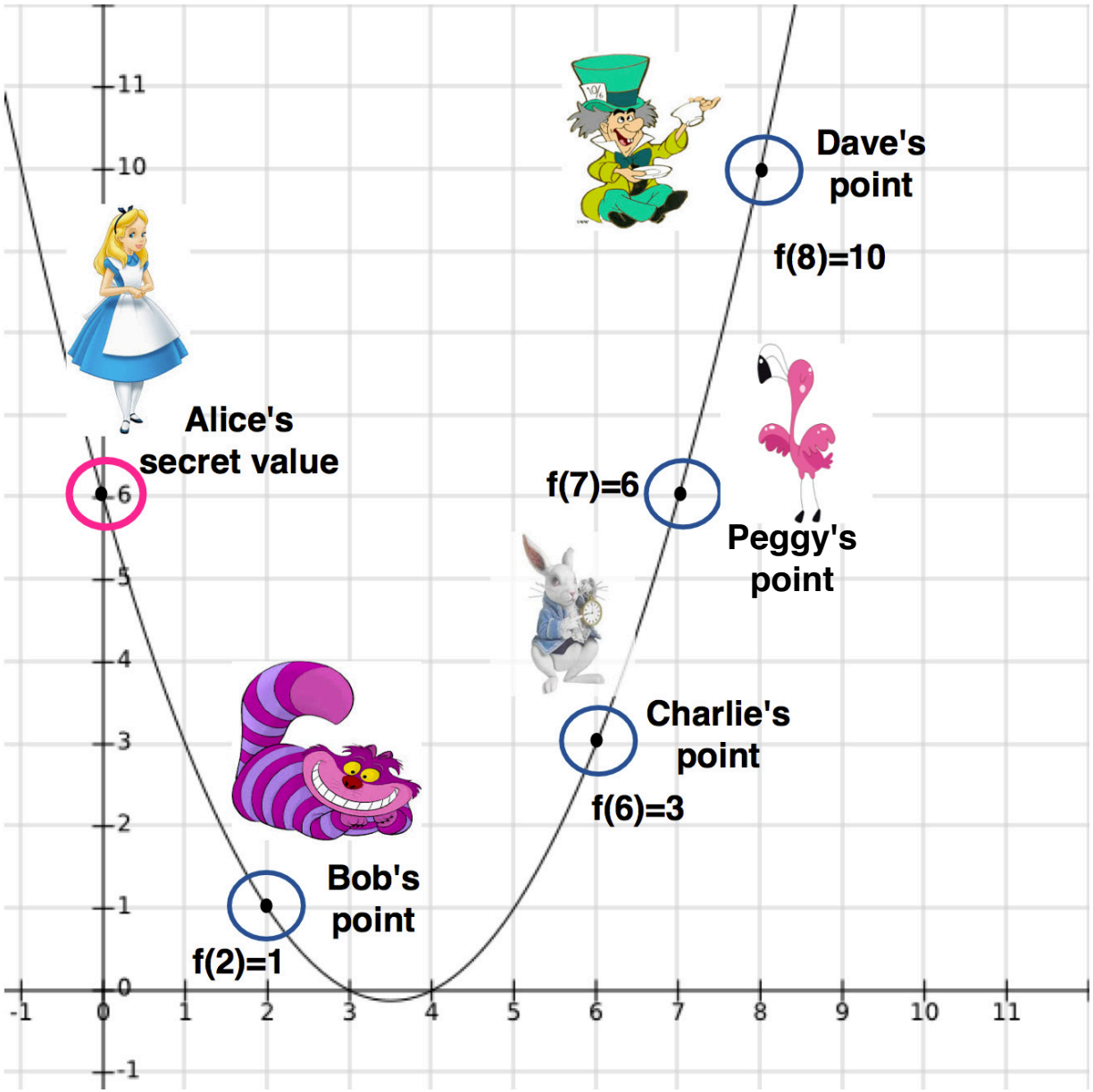
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$
- Alice sends three points (not $\mathbf{f(0)}$) one to Bob, one to Charlie and one to Dave.
- These points are the **shares** of the secret!
- Together Bob, Charlie and Dave can compute the **secret line** and find the secret $\mathbf{f(0) = 6}$.

Lines, points & secrets



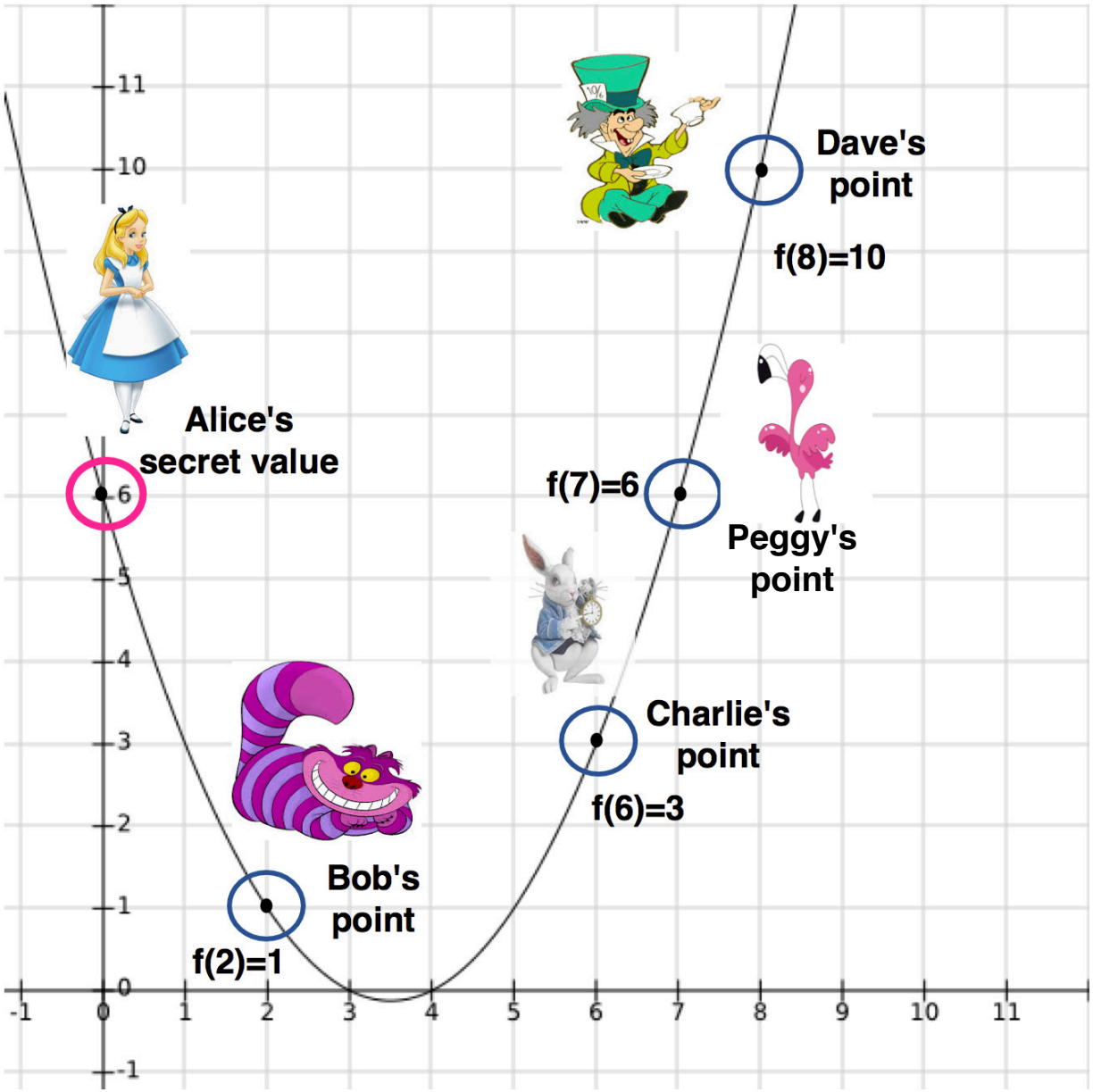
- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$
- Alice sends three points (not $\mathbf{f(0)}$) one to Bob, one to Charlie and one to Dave.
- These points are the **shares** of the secret!
- Together Bob, Charlie and Dave can compute the **secret line** and find the secret $\mathbf{f(0) = 6}$.

Lines, points & secrets



- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$
- Alice sends three points (not $\mathbf{f(0)}$) one to Bob, one to Charlie and one to Dave.
- These points are the **shares** of the secret!
- Together Bob, Charlie and Dave can compute the **secret line** and find the secret $\mathbf{f(0) = 6}$.
- If Alice gives another point to Peggy. Who can then compute the secret?

Lines, points & secrets



- Lets assume that the secret is $\mathbf{s = 6}$
- The secret line is $\mathbf{f(x) = 6 - 3.5x + 0.5x^2}$
- Alice sends three points (not $\mathbf{f(0)}$) one to Bob, one to Charlie and one to Dave.
- These points are the **shares** of the secret!
- Together Bob, Charlie and Dave can compute the **secret line** and find the secret $\mathbf{f(0) = 6}$.
- If Alice gives another point to Peggy. Who can then compute the secret?

How to Prove I know a Secret?

Victor the Verifier & Peggy the Prover

Victor the Verifier

Peggy the Prover

Goal of P

Prove a statement to V

i.e., convince that the statement is **true**

Examples of statements:

" I am Peggy" (for identification) or

"I have the secret key for this public key"

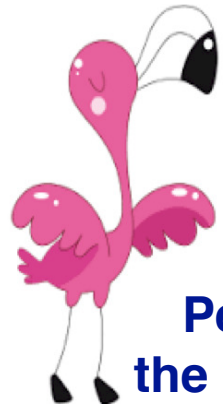
Victor the Verifier & Peggy the Prover

Victor the Verifier

Goal of V

Accept a prover P,

only if P provides a true statement!



Peggy the Prover

Goal of P

Prove a statement to V

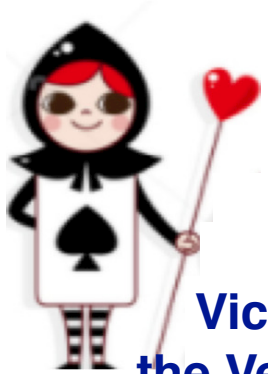
i.e., convince that the statement is **true**

Examples of statements:

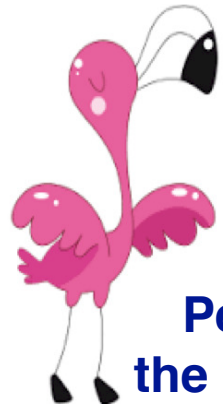
" I am Peggy" (for identification) or

"I have the secret key for this public key"

Victor the Verifier & Peggy the Prover



Victor the Verifier



Peggy the Prover

Goal of V

Accept a prover P,

only if P provides a true statement!

Goal of P

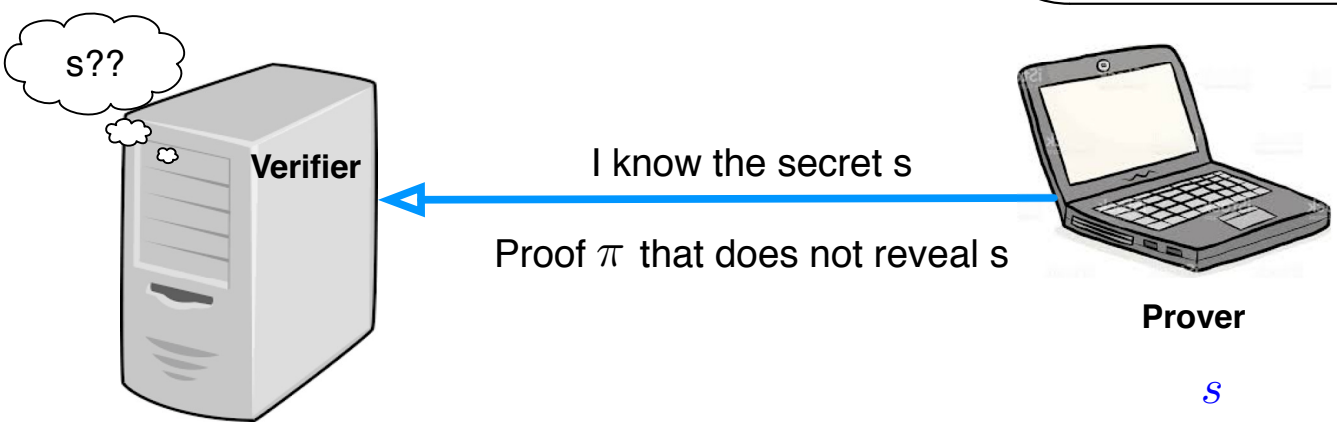
Prove a statement to V

i.e., convince that the statement is **true**

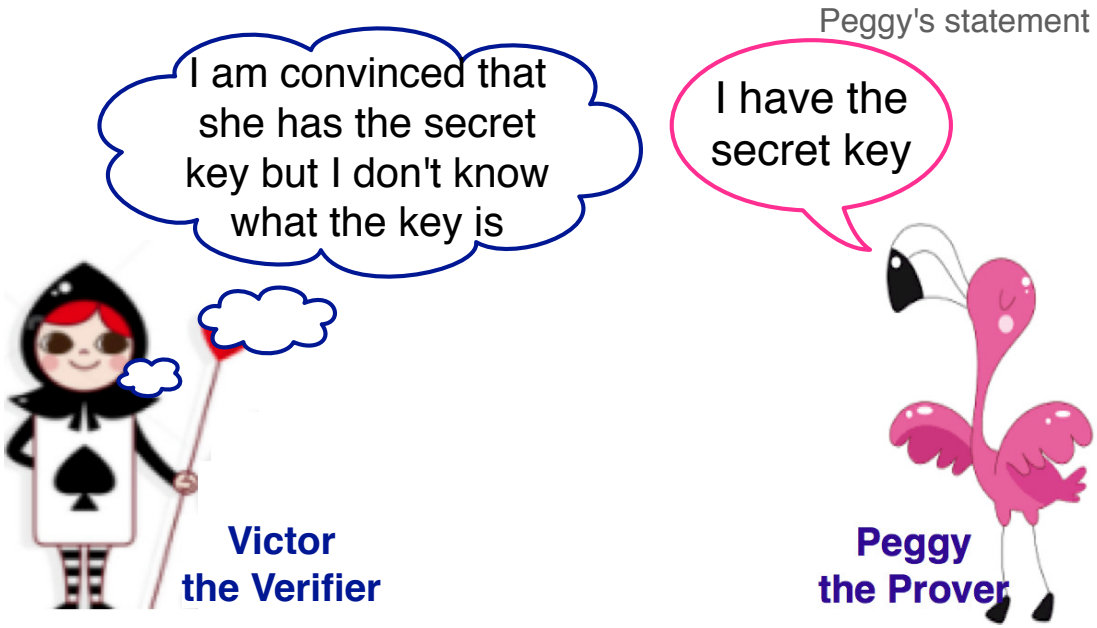
Examples of statements:

" I am Peggy" (for identification) or

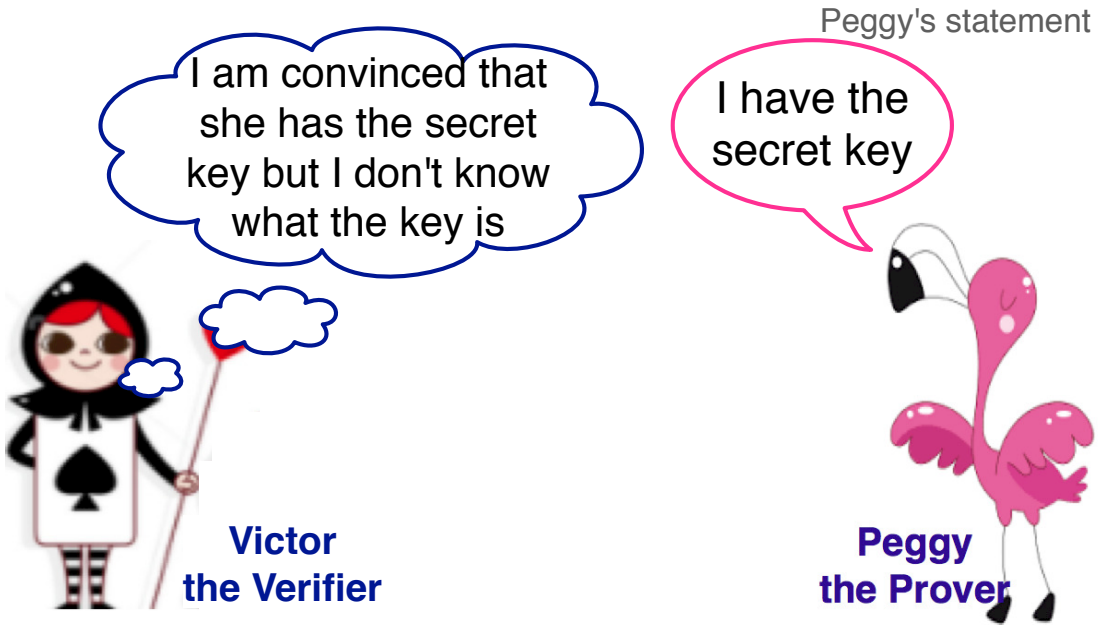
"I have the secret key for this public key"



Zero-Knowledge

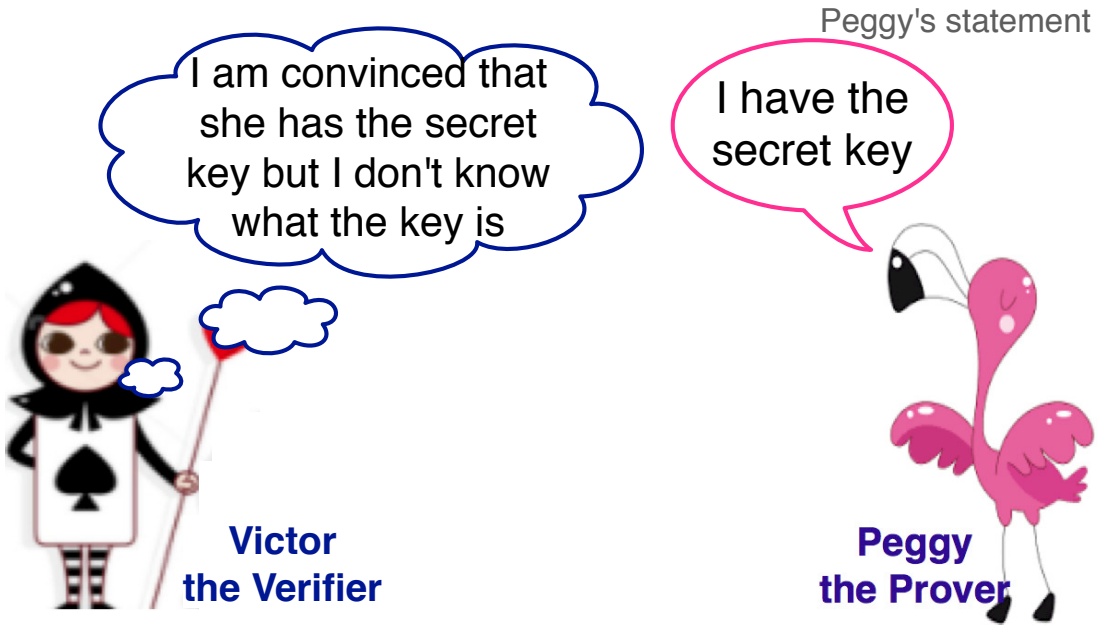


Zero-Knowledge



ZERO-KNOWLEDGE (INTUITION): A honest **P** can convince **V** of the validity of a statement **without revealing any information** beyond the truth of the statement.

Zero-Knowledge

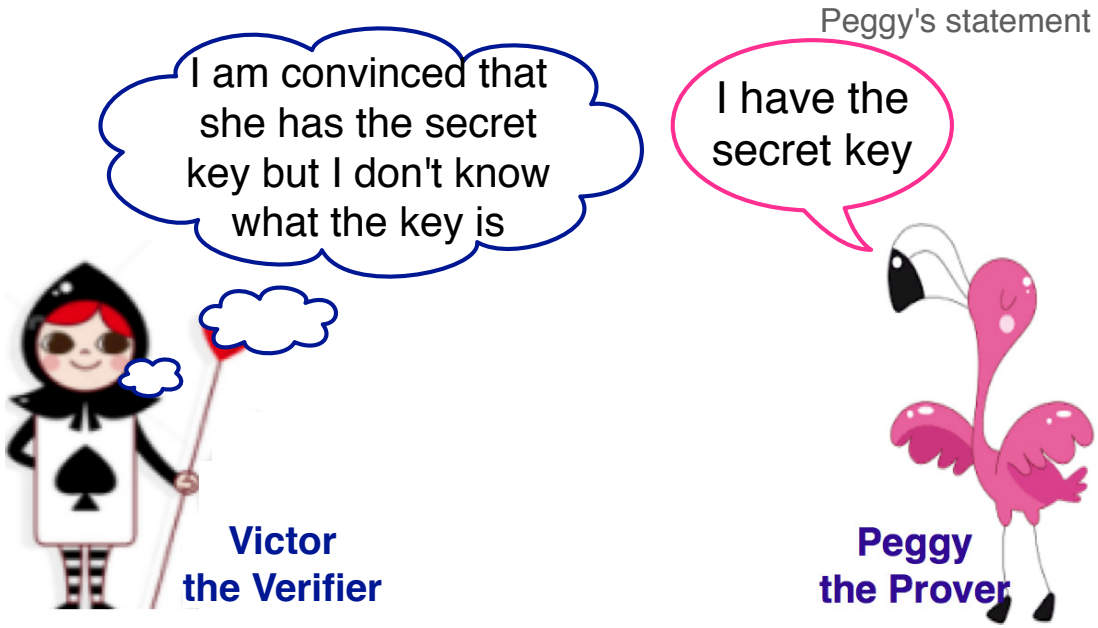


ZERO-KNOWLEDGE (INTUITION): A honest **P** can convince **V** of the validity of a statement **without revealing any information** beyond the truth of the statement.

What does this mean?

- No matter what Victor does, he will not get the secret key while, at the same time, **he will be convinced that the Peggy knows the secret**.

Zero-Knowledge



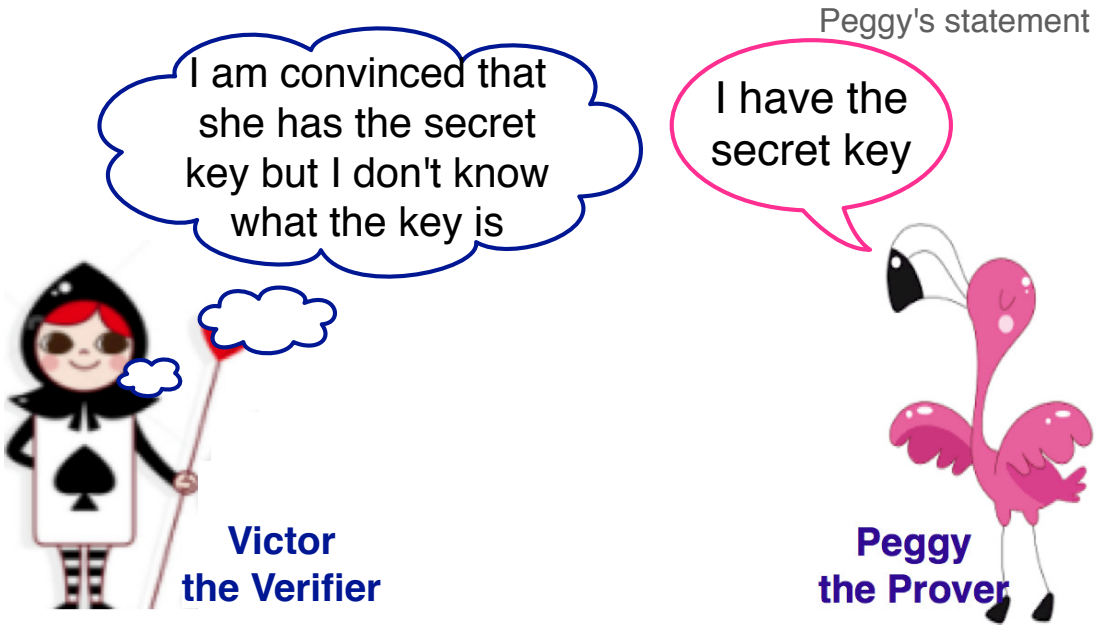
ZERO-KNOWLEDGE (INTUITION): A honest **P** can convince **V** of the validity of a statement **without revealing any information** beyond the truth of the statement.

What does this mean?

- No matter what Victor does, he will not get the secret key while, at the same time, **he will be convinced that the Peggy knows the secret**.

How is this possible?

Zero-Knowledge



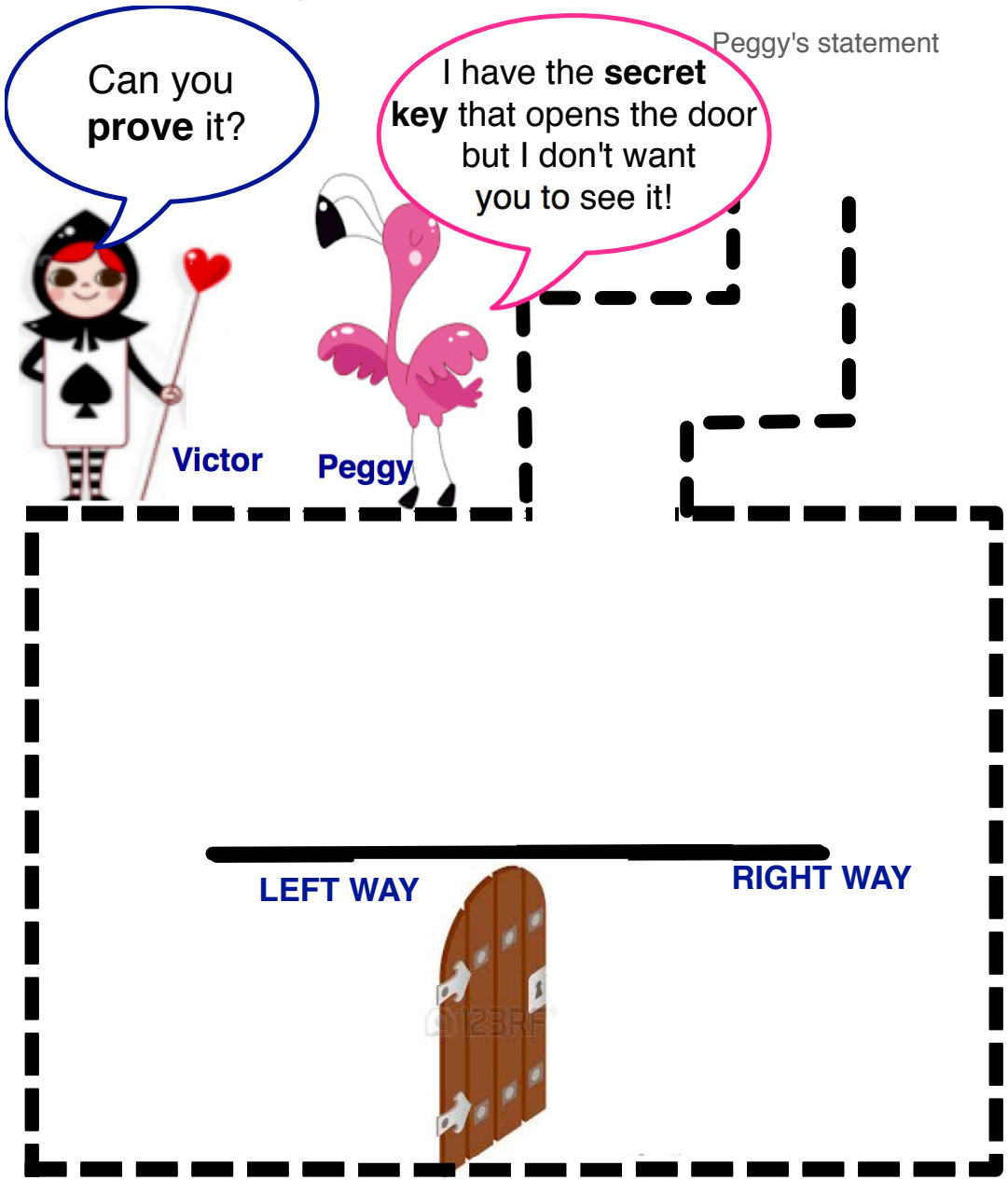
ZERO-KNOWLEDGE (INTUITION): A honest **P** can convince **V** of the validity of a statement **without revealing any information** beyond the truth of the statement.

What does this mean?

- No matter what Victor does, he will not get the secret key while, at the same time, **he will be convinced that the Peggy knows the secret**.

How is this possible? The magic of **Crypto!**

Zero-Knowledge: Ali Baba's cave

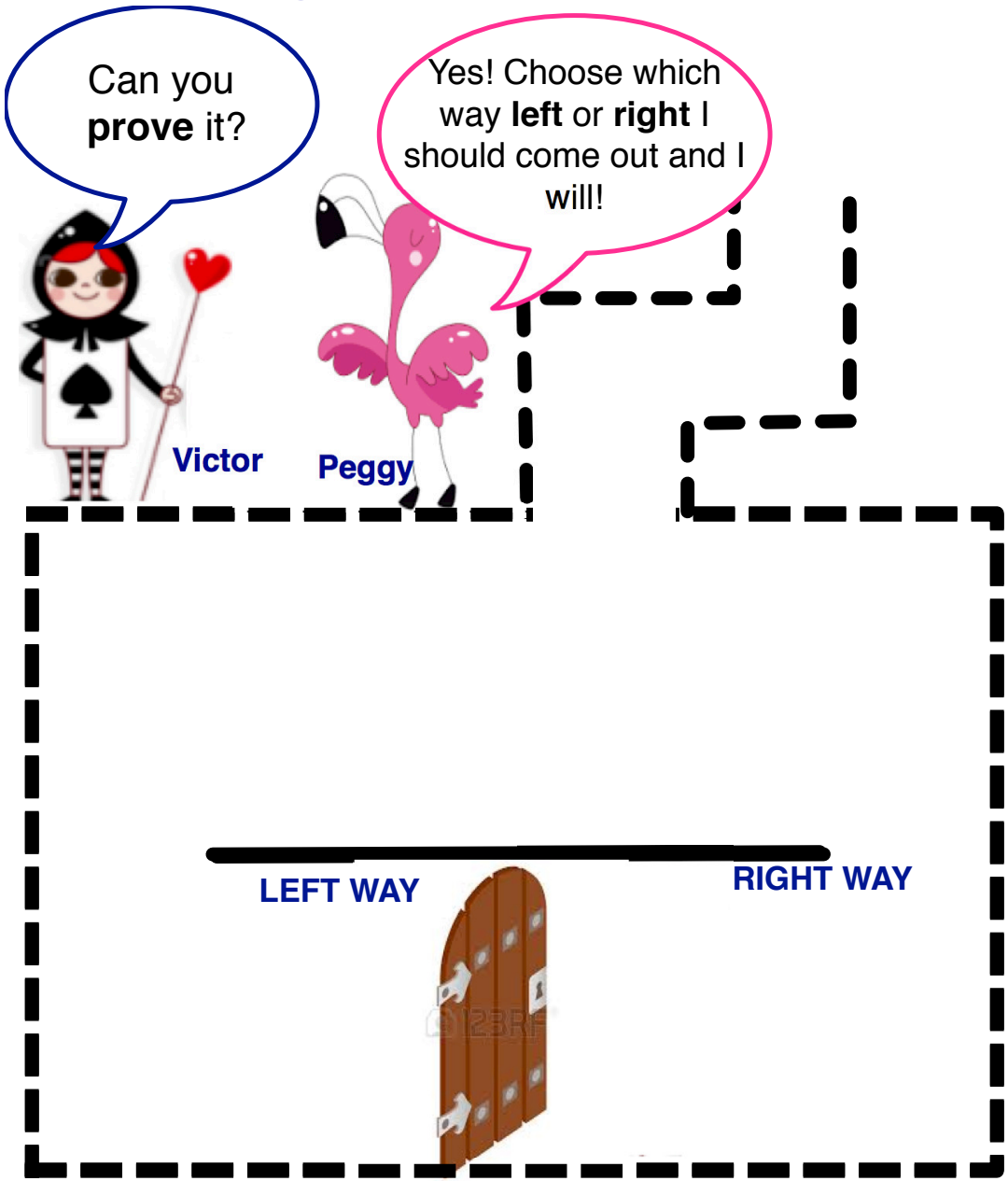


The story of Ali Baba's cave is available here:

`https://pages.cs.wisc.edu/ mkowalcz/628.pdf`!

It is used to give an intuition of Zero-knowledge protocols!

Zero-Knowledge: Ali Baba's cave

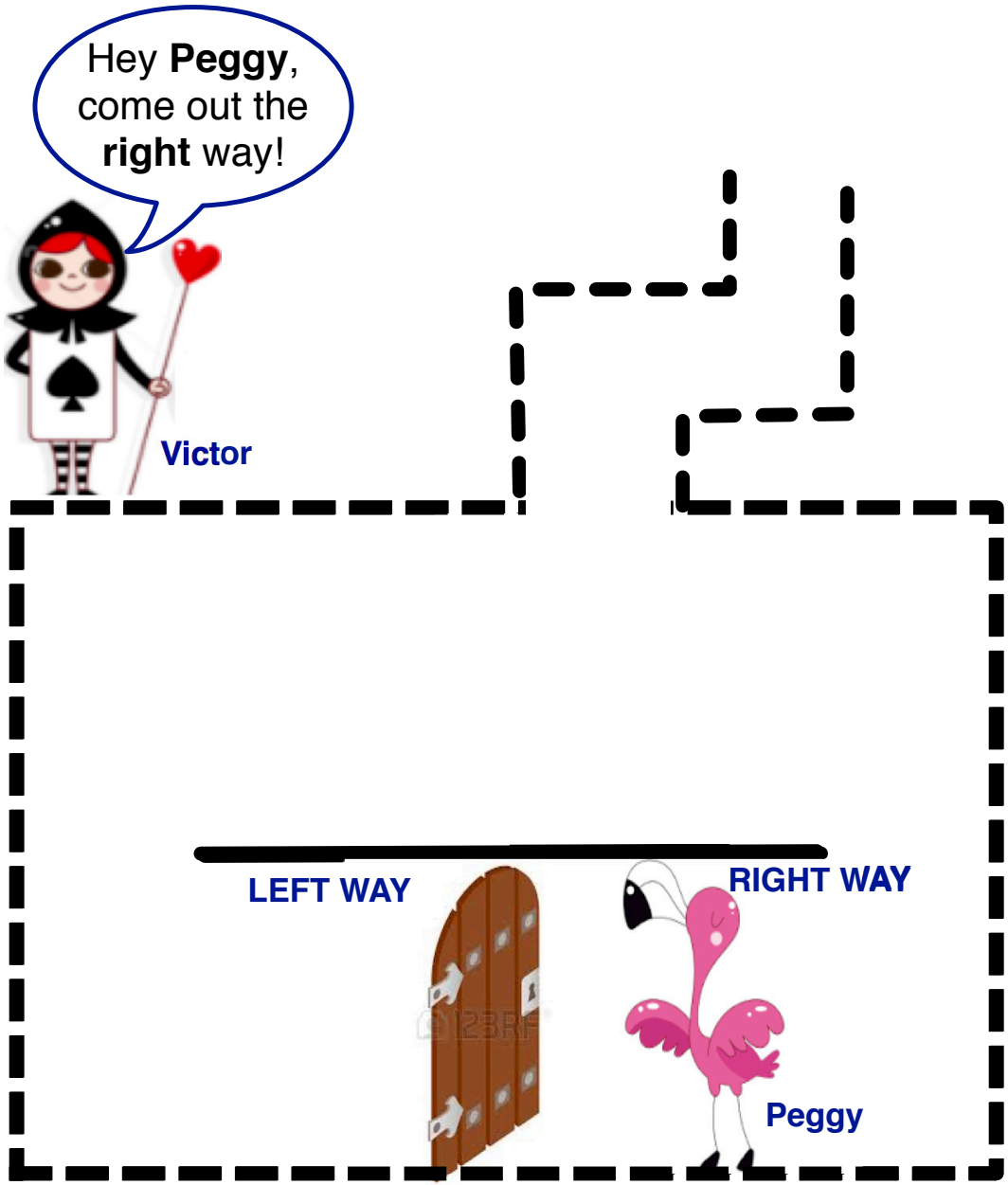


The story of Ali Baba's cave is available here:

`http://pages.cs.wisc.edu/~mkowalcz/628.pdf`!

It is used to give an intuition of Zero-knowledge protocols!

Zero-Knowledge: Ali Baba's cave

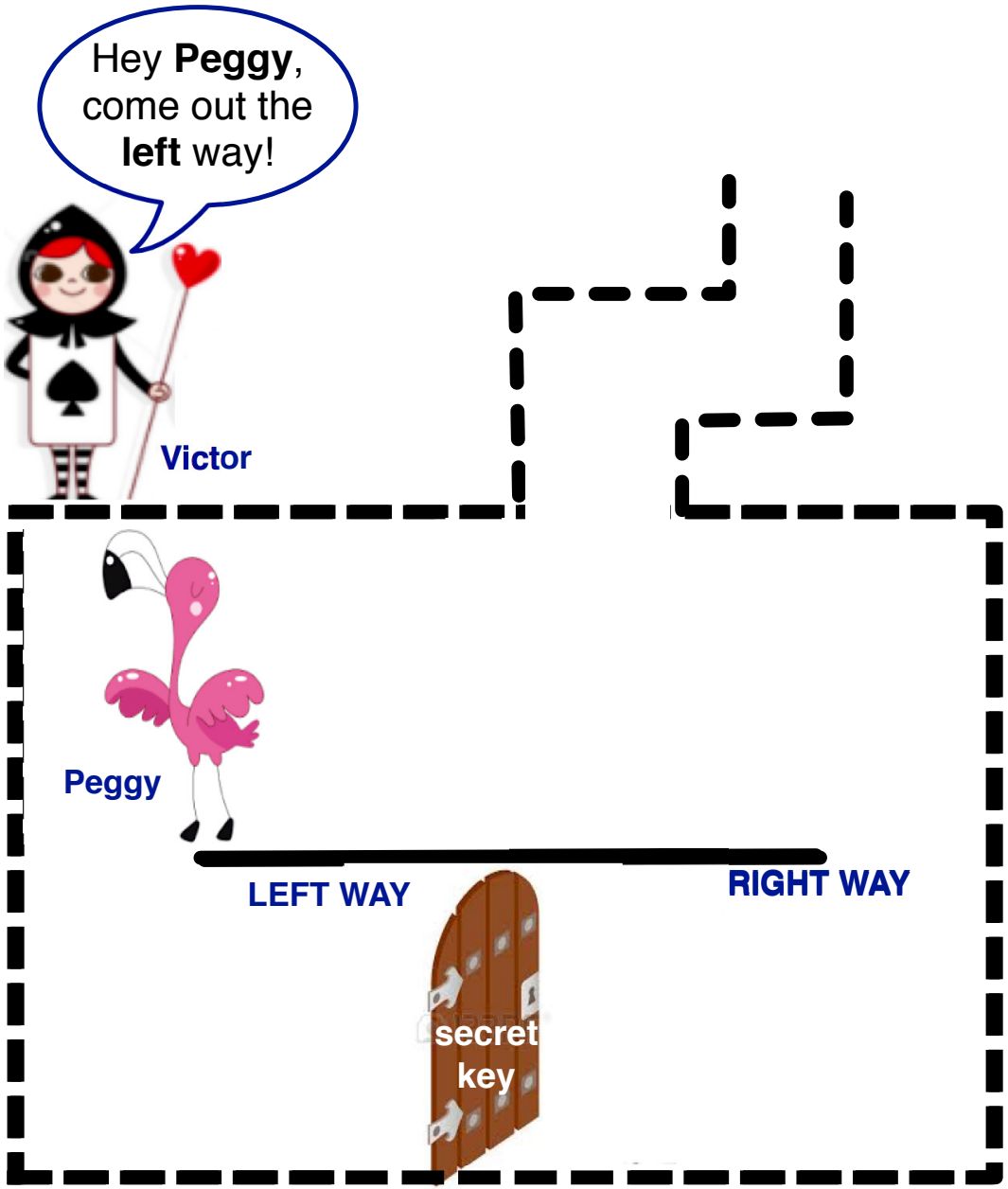


The story of Ali Baba's cave is available here:

`http://pages.cs.wisc.edu/ mkowalcz/628.pdf`!

It is used to give an intuition of Zero-knowledge protocols!

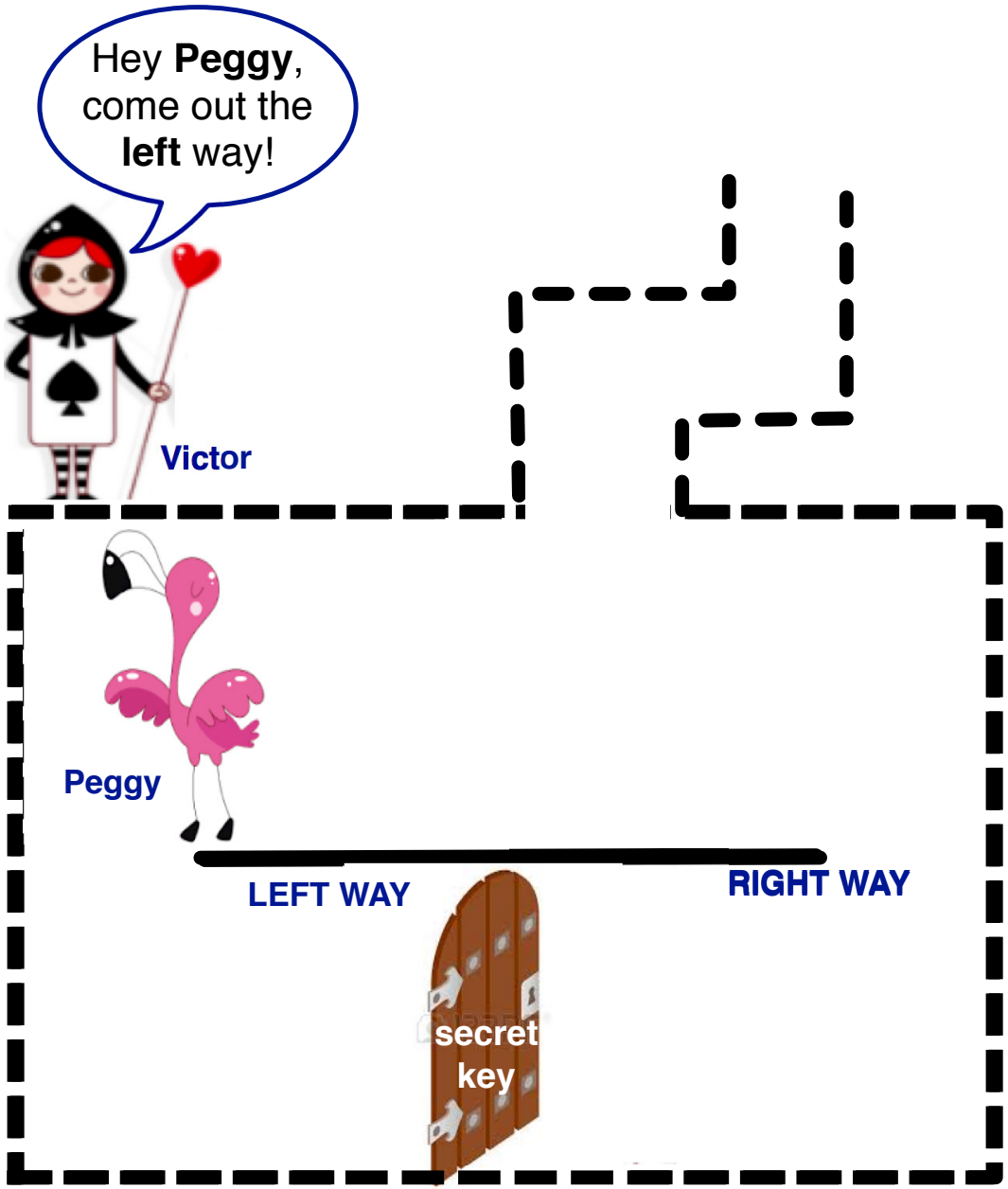
Zero-Knowledge: Ali Baba's Cave



The story of Ali Baba's cave is available here: `http://pages.cs.wisc.edu/~mkowalcz/628.pdf`! It is used to give an intuition of Zero-knowledge protocols!

- Peggy **does not know** which way Victor will choose

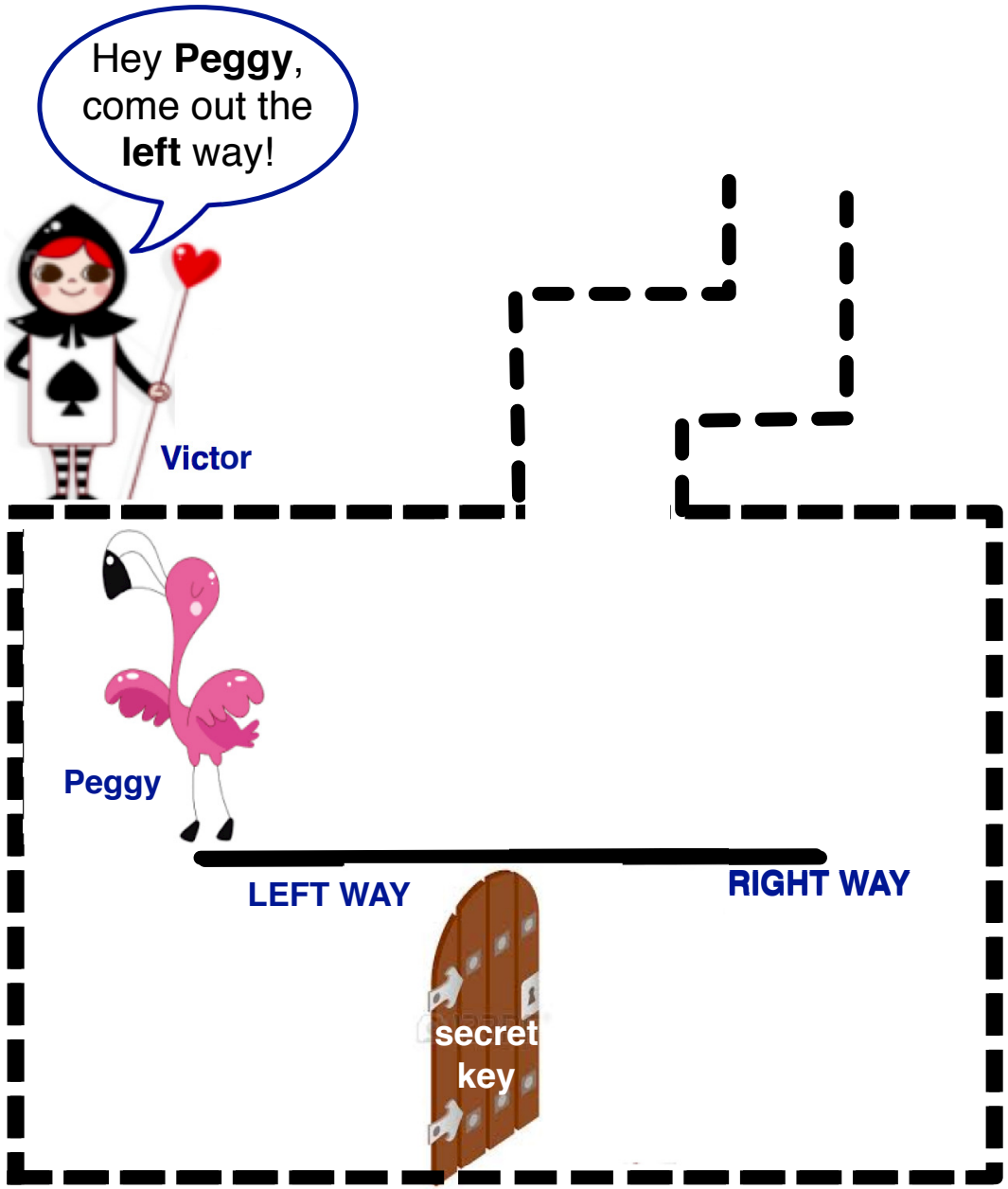
Zero-Knowledge: Ali Baba's Cave



The story of Ali Baba's cave is available here: `http://pages.cs.wisc.edu/~mkowalcz/628.pdf`! It is used to give an intuition of Zero-knowledge protocols!

- Peggy **does not know** which way Victor will choose
- If Victor decides **"the right way"** Peggy does not need to use the **"secret key"** to open the door

Zero-Knowledge: Ali Baba's Cave



The story of Ali Baba's cave is available here: `http://pages.cs.wisc.edu/~mkowalcz/628.pdf`! It is used to give an intuition of Zero-knowledge protocols!

- Peggy **does not know** which way Victor will choose
- If Victor decides **"the right way"** Peggy does not need to use the **"secret key"** to open the door
- If Victor decides **"the left way"**, only if Peggy knows the **"secret key"** can pass through the door and show up the left way.

Zero-Knowledge: Ali Baba's Cave

- **Peggy** has probability **1/2** to convince **Victor** that she knows the secret key (password).

Zero-Knowledge: Ali Baba's Cave

- **Peggy** has probability **1/2** to convince **Victor** that she knows the secret key (password).
- This also means that will probability **1/2** a dishonest prover can fool **Victor** that he knows the secret key even if he does not know it.

Zero-Knowledge: Ali Baba's Cave

- **Peggy** has probability **1/2** to convince **Victor** that she knows the secret key (password).
- This also means that will probability **1/2** a dishonest prover can fool **Victor** that he knows the secret key even if he does not know it.

How to solve this?

- Lets repeat the protocol n times so that a dishonest Peggy has very low probability to cheat.

Zero-Knowledge: Ali Baba's Cave

- **Peggy** has probability **1/2** to convince **Victor** that she knows the secret key (password).
- This also means that will probability **1/2** a dishonest prover can fool **Victor** that he knows the secret key even if he does not know it.

How to solve this?

- Lets repeat the protocol n times so that a dishonest Peggy has very low probability to cheat.
- **Quiz Question:** How much exactly is this low probability?

Zero-Knowledge: Ali Baba's Cave

- **Peggy** has probability **1/2** to convince **Victor** that she knows the secret key (password).
- This also means that will probability **1/2** a dishonest prover can fool **Victor** that he knows the secret key even if he does not know it.

How to solve this?

- Lets repeat the protocol n times so that a dishonest Peggy has very low probability to cheat.
- **Quiz Question:** How much exactly is this low probability?

Answer: $(\frac{1}{2})^n$

How to Compute on Secret Values?

Crypto Magic! Homomorphic Property

What is it?

A way to do math computations on secret numbers, **without seeing them**!

Crypto Magic! Homomorphic Property

What is it?

A way to do math computations on secret numbers, **without seeing them**!

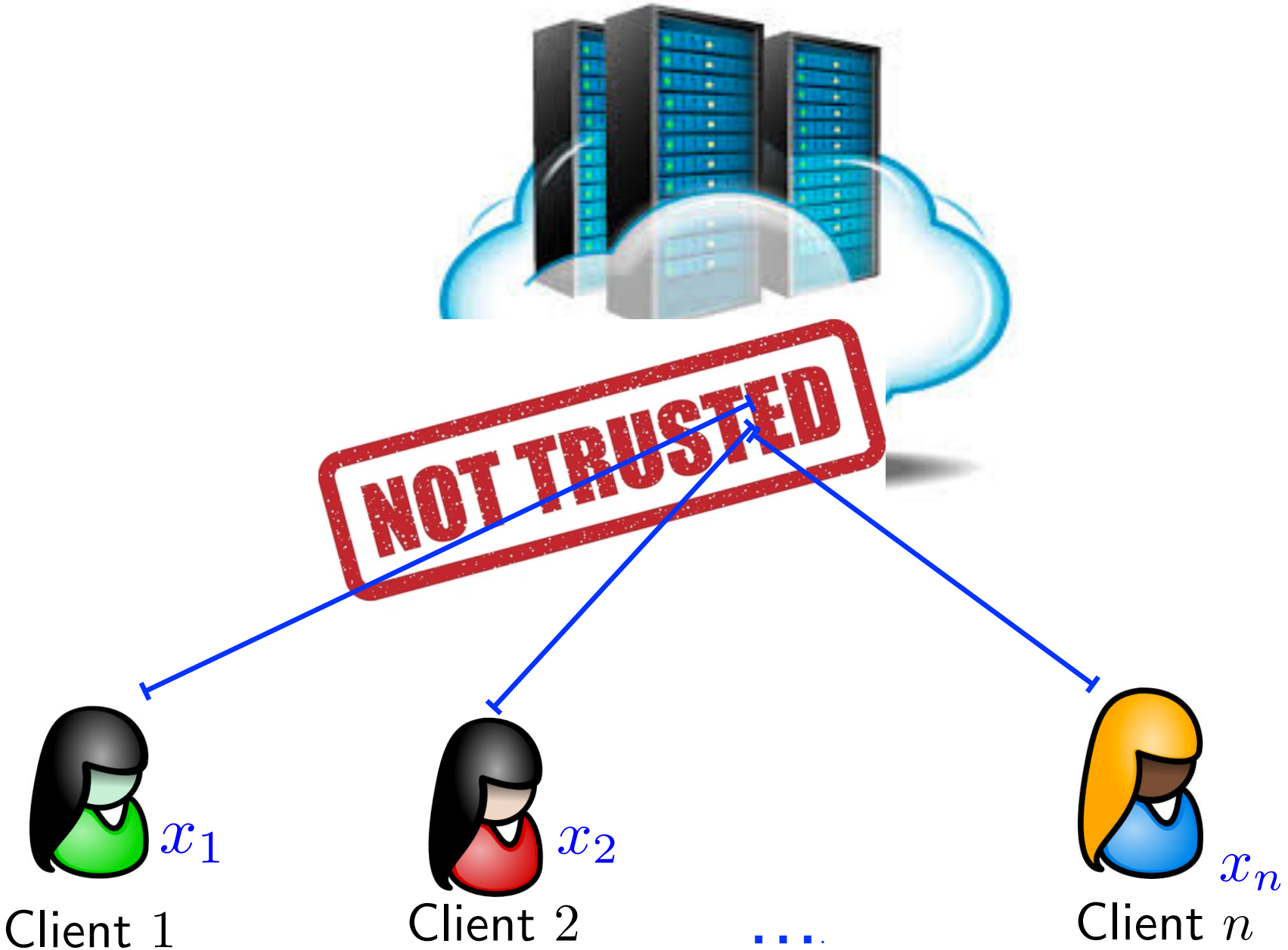
Let us encrypt two messages, $\mathbf{m_1}$ and $\mathbf{m_2}$.

With an Homomorphic Encryption Scheme we can have:

$$\mathbf{Enc}(\mathrm{m}_1) \cdot \mathbf{Enc}(m_2) = \mathbf{Enc}(m_1 \cdot m_2), \textit{or}$$
$$\mathbf{Enc}(\mathrm{m}_1) \cdot \mathbf{Enc}(m_2) = \mathbf{Enc}(m_1 + m_2)$$

The same can apply in Digital Signatures:
$\mathbf{Sign}(\mathrm{m}_1) \cdot \mathbf{Sign}(m_2) = \mathbf{Sign}(m_1 \cdot m_2)$

Why the Homomorphic Property is Useful?



Thank you for your attention!

https://cybersecurity.unisg.ch/
katerina.mitrokotsa@unisg.ch

Fiat-Shamir Identification Protocol

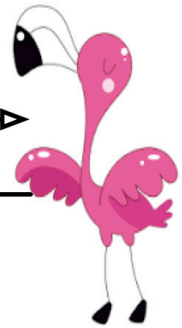
One-Time Set-Up

a TTP generates an **N=pq** where **p** and **q** are prime

check that $GCD(s, N) = 1$

N →

← v



pick a random $s \in \mathbb{Z}_N$ such that $GCD(s, N) = 1$
compute $\mathrm{v} = s^2 \pmod N$

P will identify herself by proving that she knows s without revealing s

(N, v)

Victor the Verifier

Main part of Protocol

(N, s, v)

Peggy the Prover

pick a random $r \in \{1, 2, \ldots, N-1\}$

pick a random $c \in \{0, 1\}$

w ←

compute $w = r^2 \pmod N$

c →

compute $z = rs^c \pmod N$

← z

check $z^2 = w\mathrm{v}^c \pmod N$

Repeat this part of the protocol n times every time with different (w,c,z)