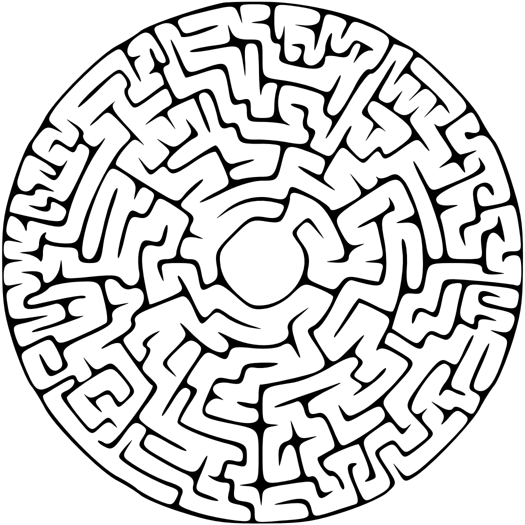
Cryptography on Isogeny Graphs

lekenpraatje

Lorenz Panny

online, 18th February 2021

You're stuck in the center. How do you get out?



You're stuck in the center. How do you get out?

This was easy thanks to our global view.

This was easy thanks to our global view. What about now?

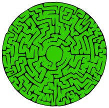
Photo: `https://unsplash.com/@jonminnema`

Finding a way out

Generally fastest strategy: Explore all possible paths.

Finding a way out

Generally fastest strategy: Explore all possible paths.

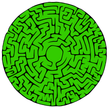


- Time taken: proportional to the *size* of the maze.

Finding a way out

Generally fastest strategy: Explore all possible paths.

- Time taken: proportional to the *size* of the maze.

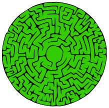


Getting lost, on the other hand, is easy:

Finding a way out

Generally fastest strategy: Explore all possible paths.

- Time taken: proportional to the *size* of the maze.



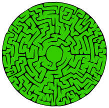
Getting lost, on the other hand, is easy:

1. Walk somewhere (randomly).

Finding a way out

Generally fastest strategy: Explore all possible paths.

- Time taken: proportional to the *size* of the maze.

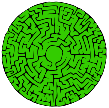


Getting lost, on the other hand, is easy:

1. Walk somewhere (randomly).
2. Forget how you got there.

Finding a way out

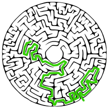
Generally fastest strategy: Explore all possible paths.



- Time taken: proportional to the *size* of the maze.

Getting lost, on the other hand, is easy:

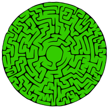
1. Walk somewhere (randomly).
2. Forget how you got there.



- Time taken: just *one path* instead of *all* paths.

Finding a way out

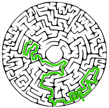
Generally fastest strategy: Explore all possible paths.



- Time taken: proportional to the *size* of the maze.

Getting lost, on the other hand, is easy:

1. Walk somewhere (randomly).
2. Forget how you got there.



- Time taken: just *one path* instead of *all* paths.

$\Longrightarrow$ Huge asymmetry in effort!

Cryptography

uses this kind of asymmetry to win an unequal battle.

Cryptography

uses this kind of asymmetry to win an unequal battle:

you
vs.
attackers

Cryptography

uses this kind of asymmetry to win an unequal battle:

you with a tiny computer and milliseconds of patience
vs.
attackers with almost infinite resources and plenty of time

Cryptography

uses this kind of asymmetry to win an unequal battle:

you with a tiny computer and milliseconds of patience
vs.
attackers with almost infinite resources and plenty of time

Example: (public-key) encryption

- Encrypt using the "easy" random walking.
- Force bad guys to solve the "hard" path finding to decrypt.
- Somehow still enable the recipient to decrypt easily.
  (This is the tricky part.)

Alice and Bob want to agree on a secret.

But everyone between them can listen in!

Alice and Bob want to agree on a secret.

But everyone between them can listen in!

Clearly impossible?

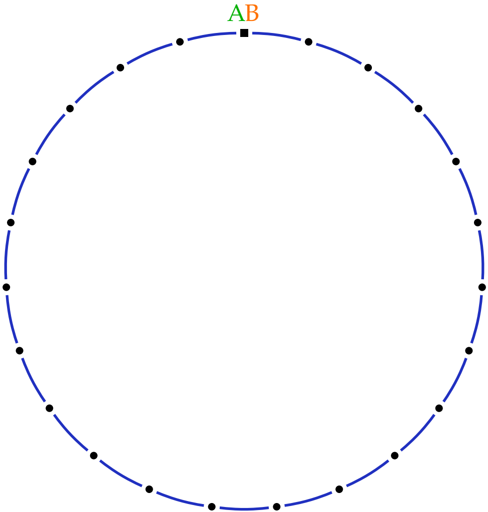
Alice and Bob want to agree on a secret.

But everyone between them can listen in!

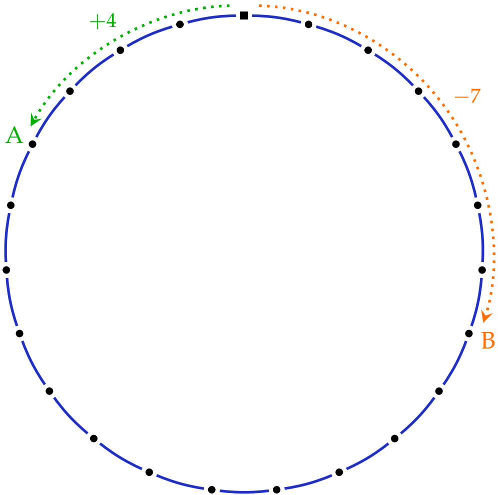
Clearly impossible? No! 🎉

[Diffie & Hellman, 1976]

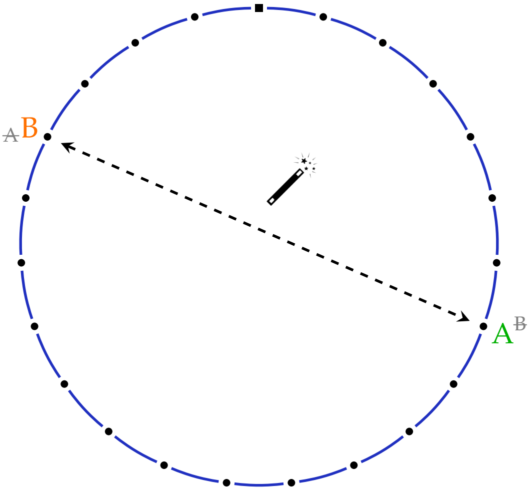
Let’s drop Alice and Bob in this strange-looking “maze”.



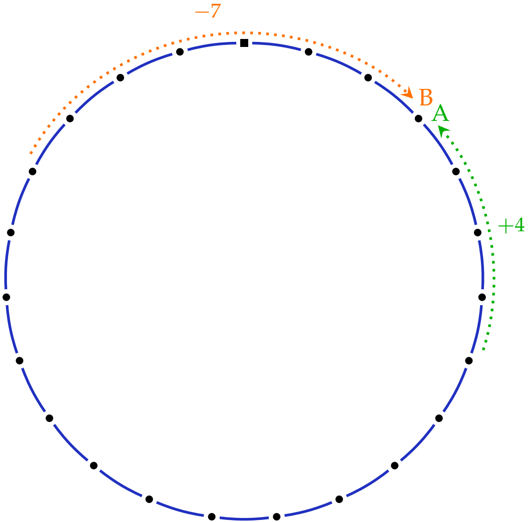
They both pick a random number and walk that many steps.



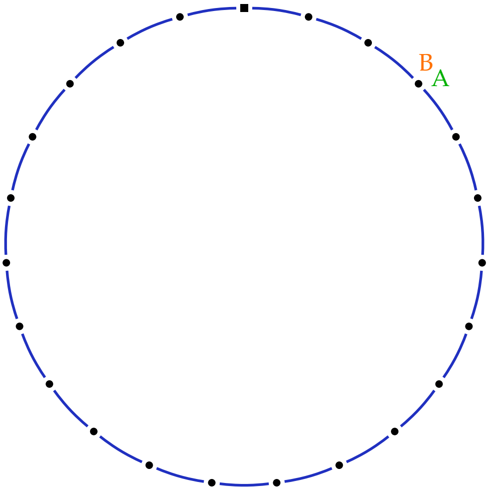
We swap Alice and Bob. (This step requires wizardry.)



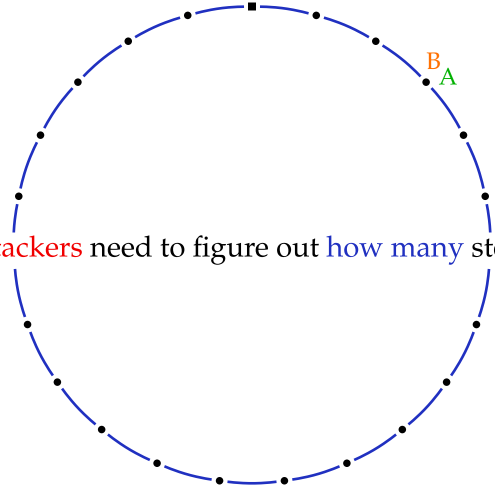
They both walk the same number of steps as before.



Alice and Bob arrive at the same location!



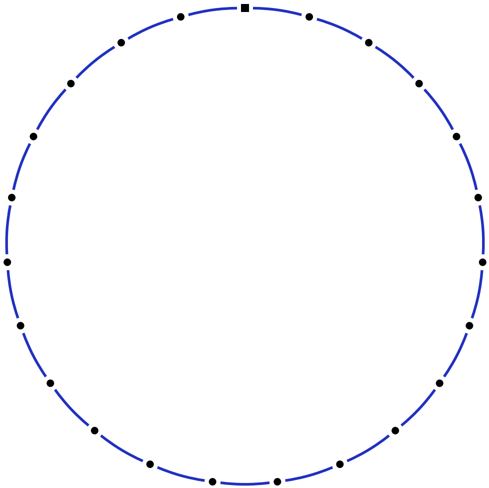
Alice and Bob arrive at the same location!



Attackers need to figure out how many steps.

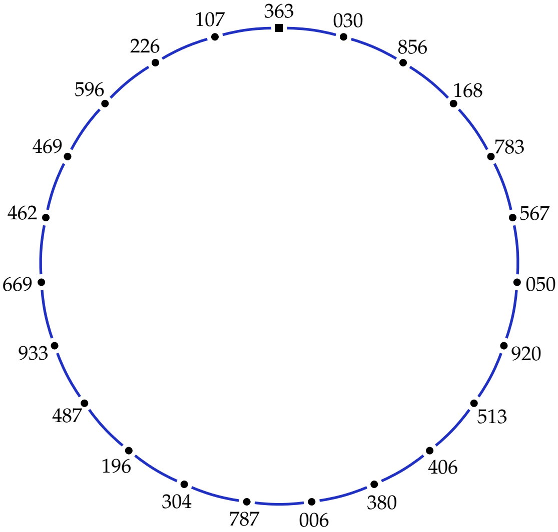
In cryptography, ...

We are doing this in a virtual reality.



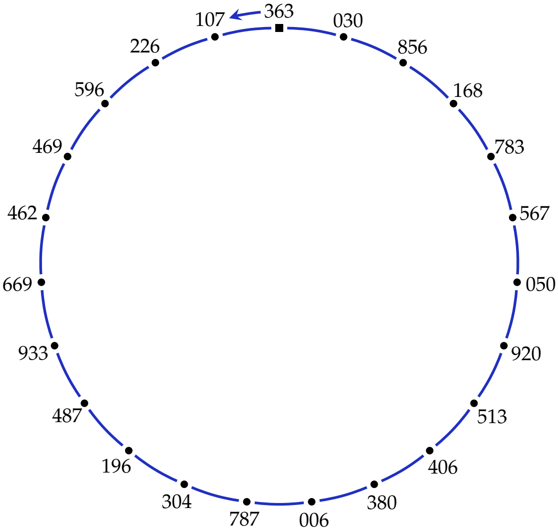
In cryptography, ...

Each location has a *name*.



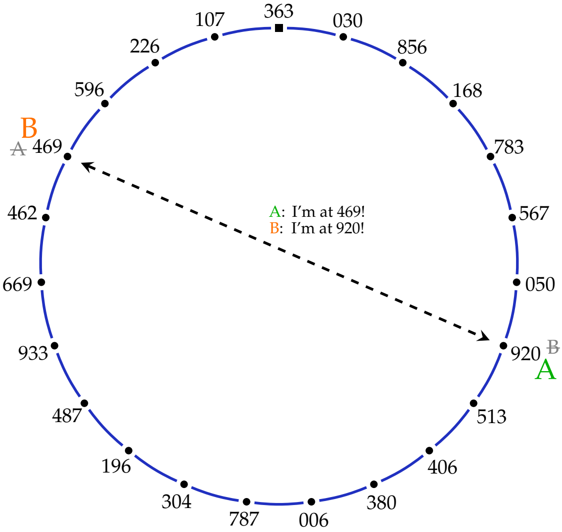
In cryptography, ...

Each step is a *computation*: $(363, \text{left}) \longmapsto 107.$



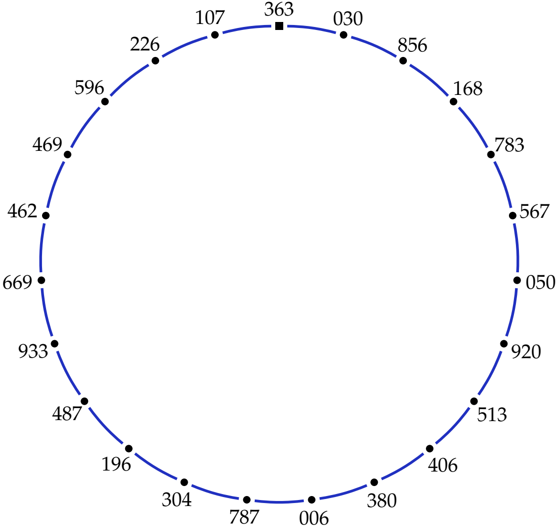
In cryptography, ...

To swap A↔B, we simply exchange place names.



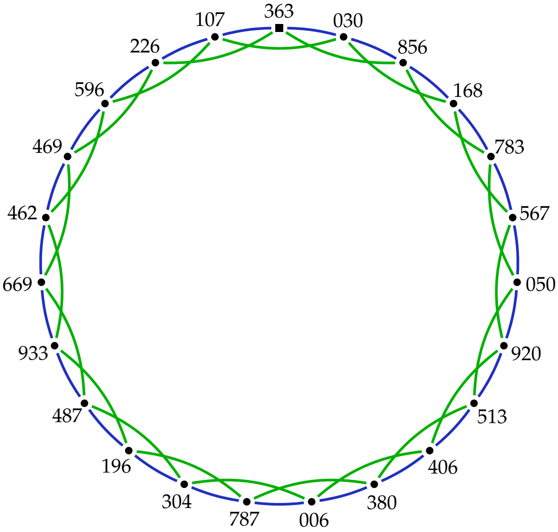
In cryptography, ...

Problem: In this maze, attackers are as fast as Alice and Bob.



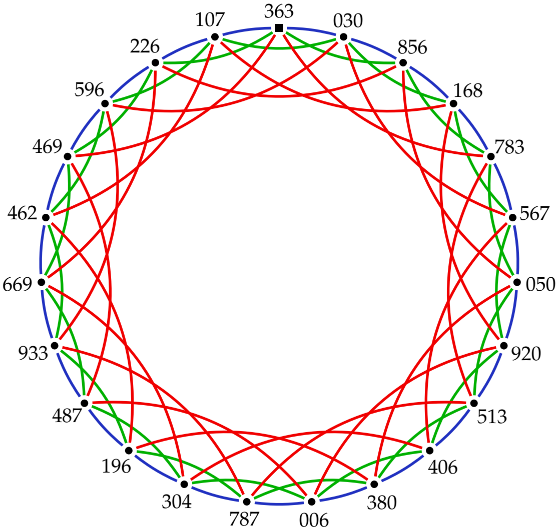
In cryptography, ...

⇝ Let's add *shortcuts*!



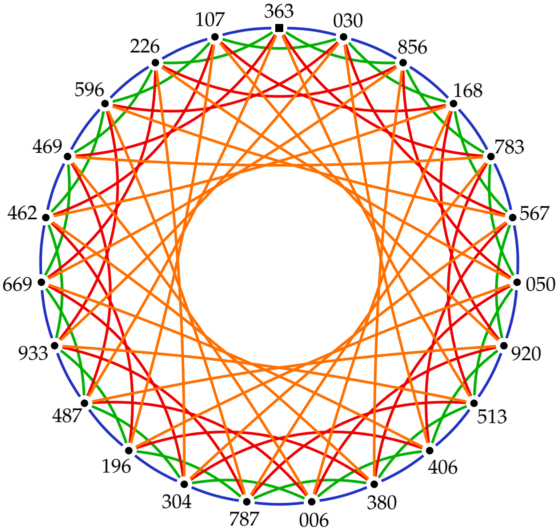
In cryptography, ...

⇝ Let's add *shortcuts*!



In cryptography, ...

⇝ Let's add *shortcuts*!



In cryptography, ...

Important: Make it big.

In cryptography, ...

Important: Make it big. *Number-of-atoms-in-the-universe big*.

Photo: `https://unsplash.com/@gferla`

In cryptography, ...

Important: Make it big. *Number-of-atoms-in-the-universe big*.

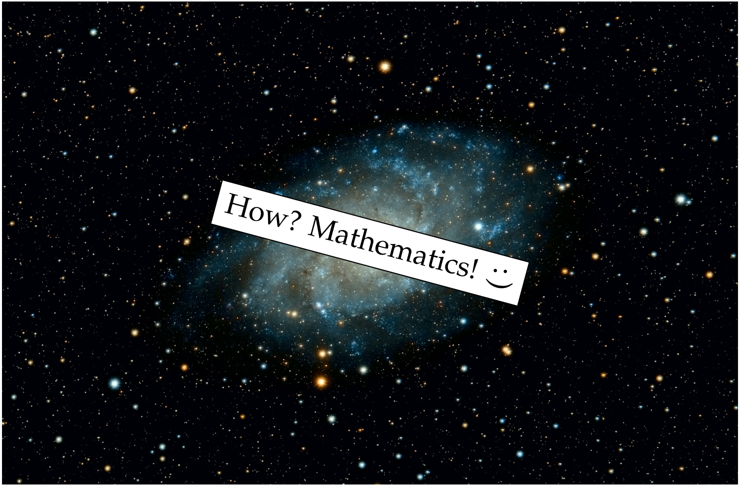
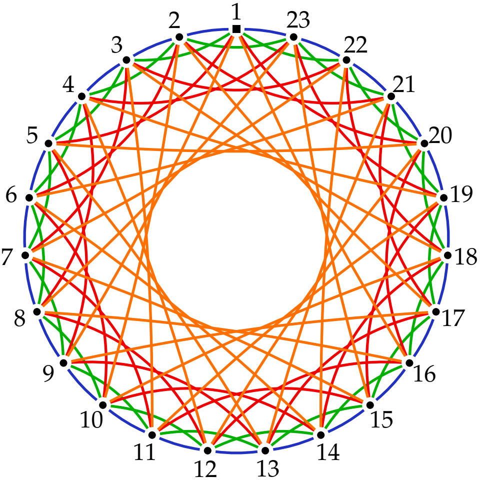


Photo: `https://unsplash.com/@gferla`

In cryptography, ...

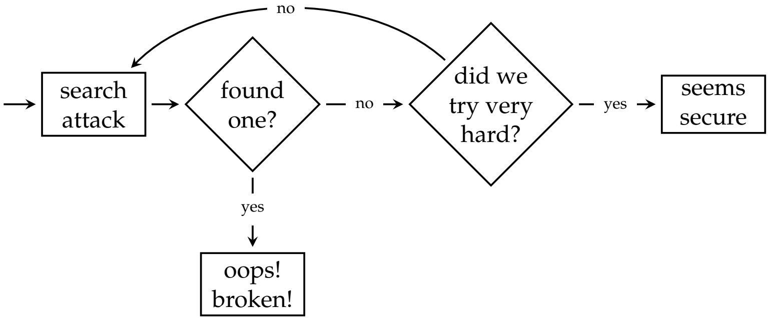
Place *names* must not reveal too much about *where* they are.



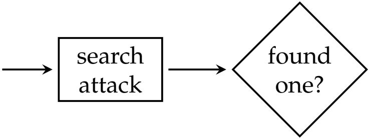
In cryptography, ...

Place *names* must not reveal too much about *where* they are.

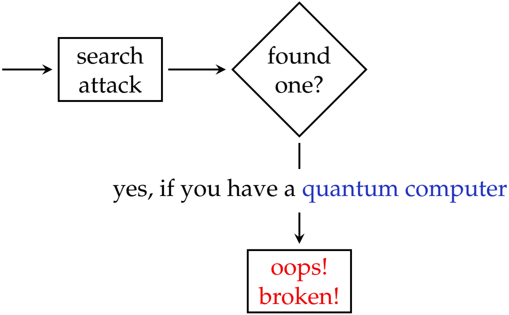
Only method to guarantee this in most cases: *Cryptanalysis*.



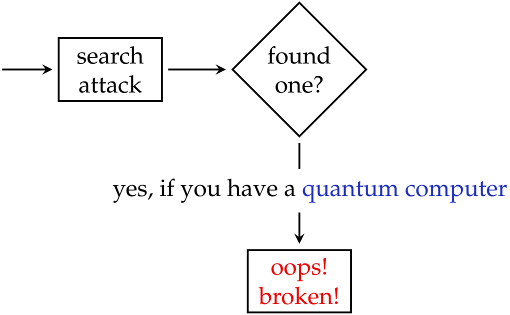
The situation for large parts of present-day cryptography:



The situation for large parts of present-day cryptography:



The situation for large parts of present-day cryptography:

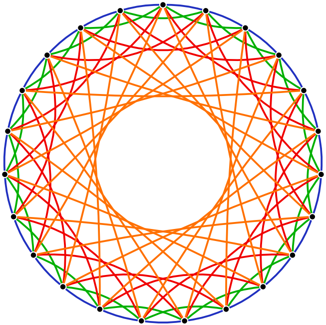


Good news: We are working on ***post-quantum cryptography***!

My thesis...

My thesis...

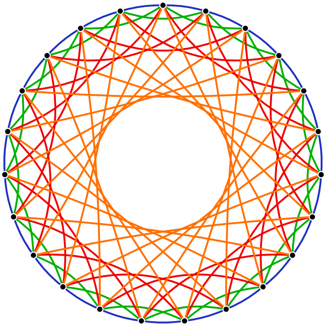
...is about this:



(but post-quantum!)

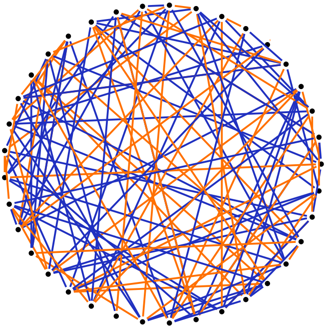
My thesis...

...is about this:



(but post-quantum!)

...and this:



(also post-quantum,
and similar math.)

Next up: Questioning!

Bumbling through a conversation with an eminent professor, the grad student outdoes his own stupidity with every remark he makes.

Picture: https://legogradstudent.tumblr.com/post/187145246746