MARCO MARTINOLI
10 - 05 - 2022

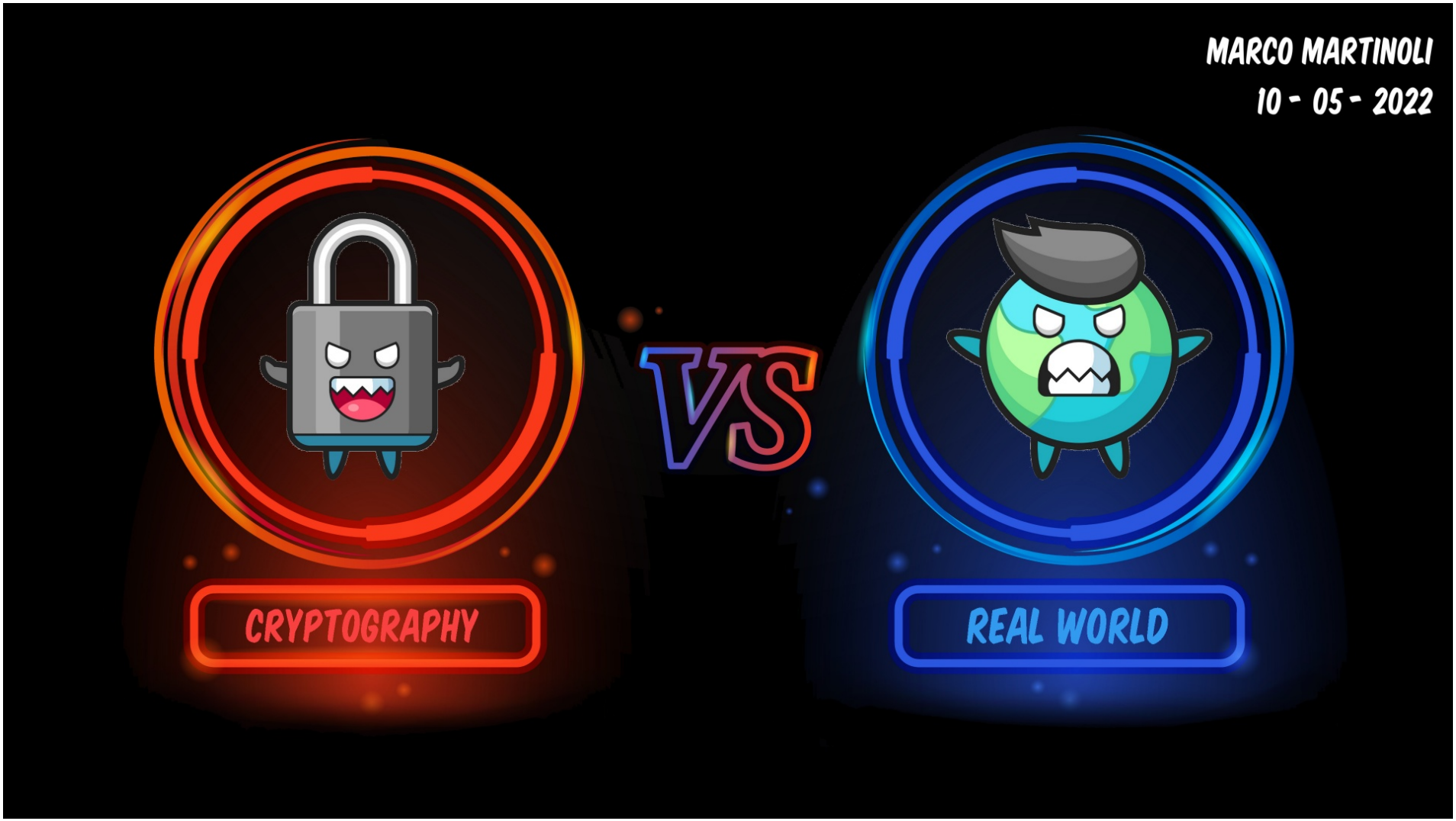
Some properties

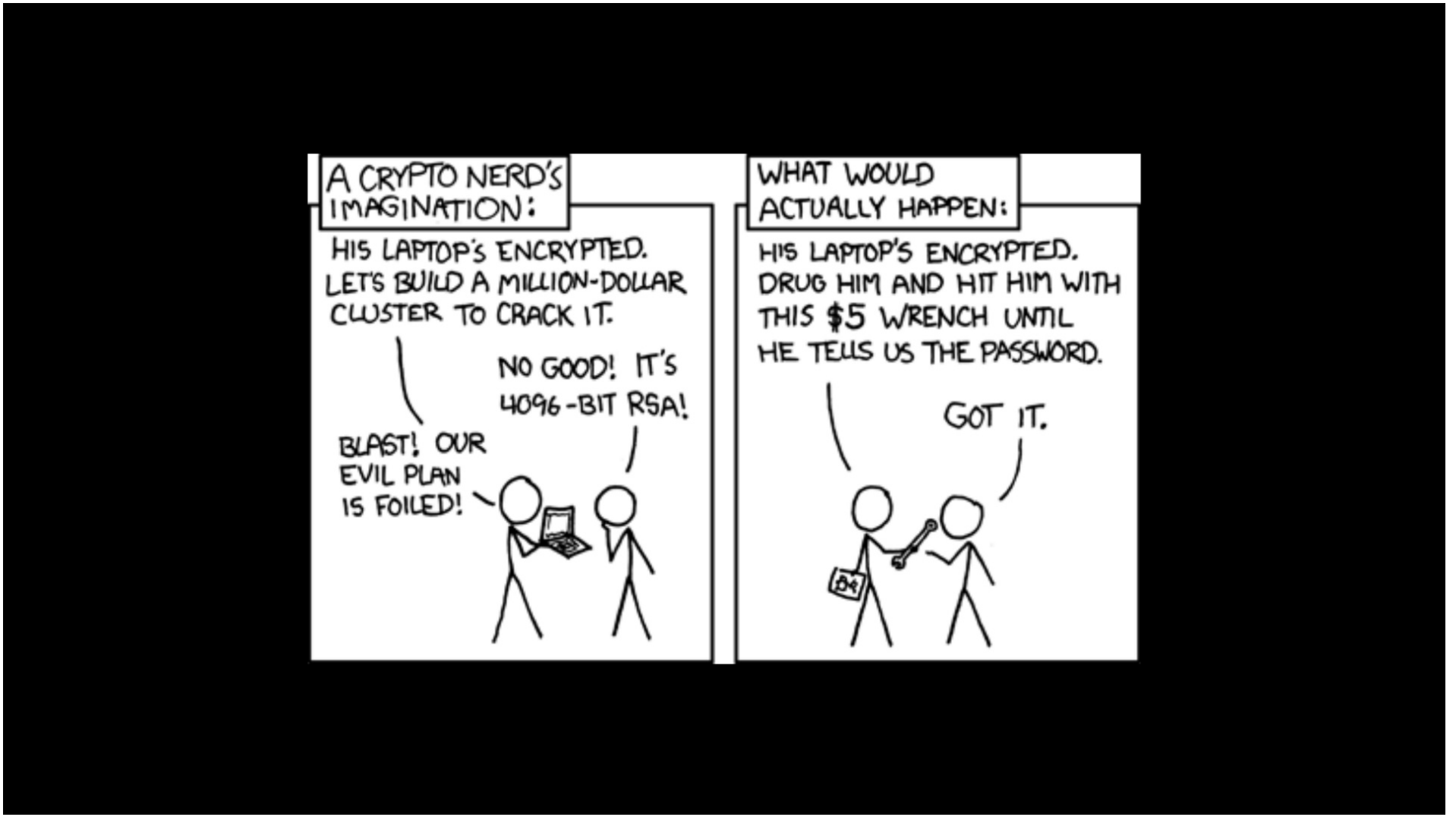
- Merkle tree provides integrity
- New Merkle trees generated at regular intervals
- VRF prevents enumeration

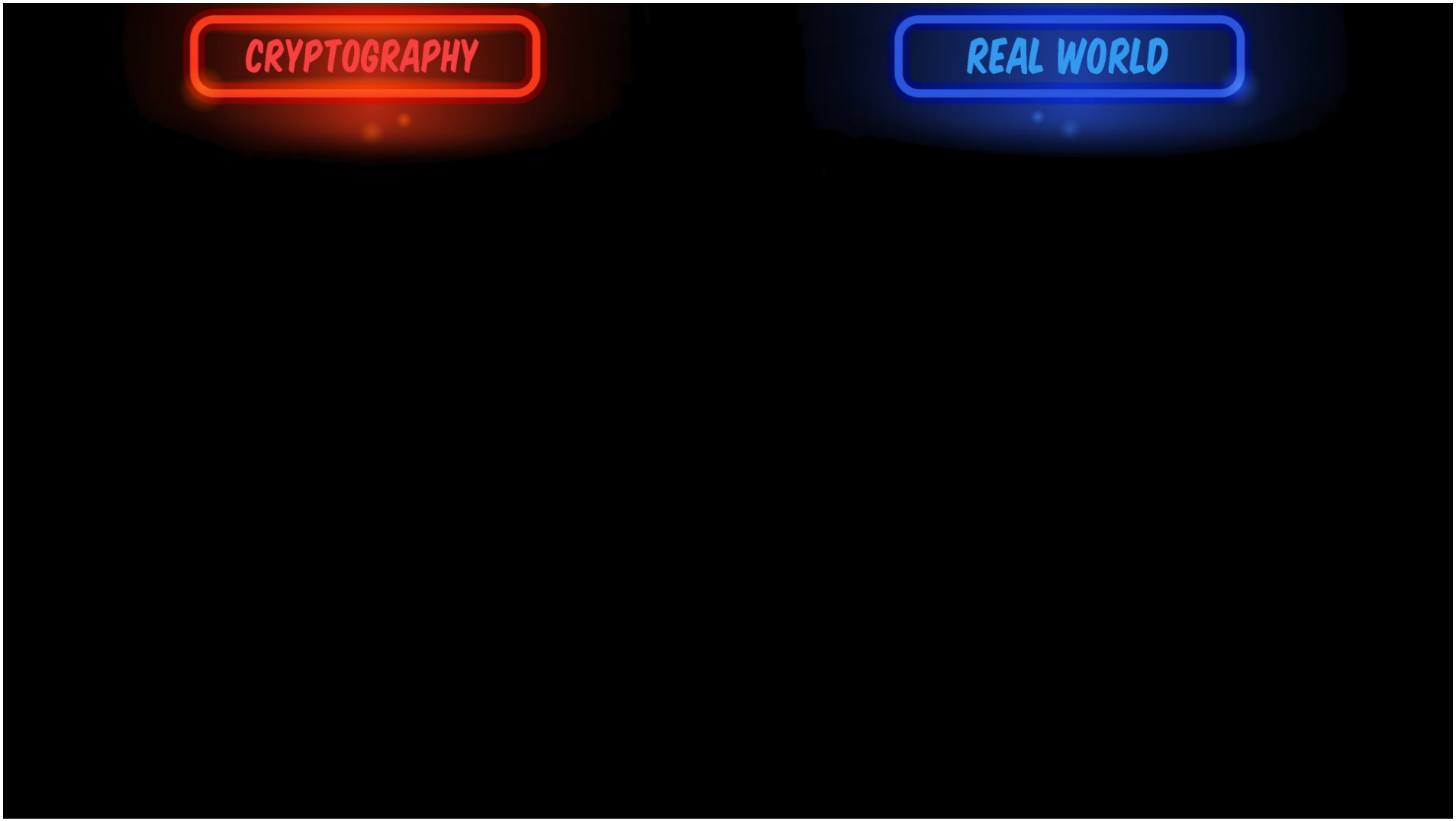
SIDE-CHANNEL
ANALYSIS

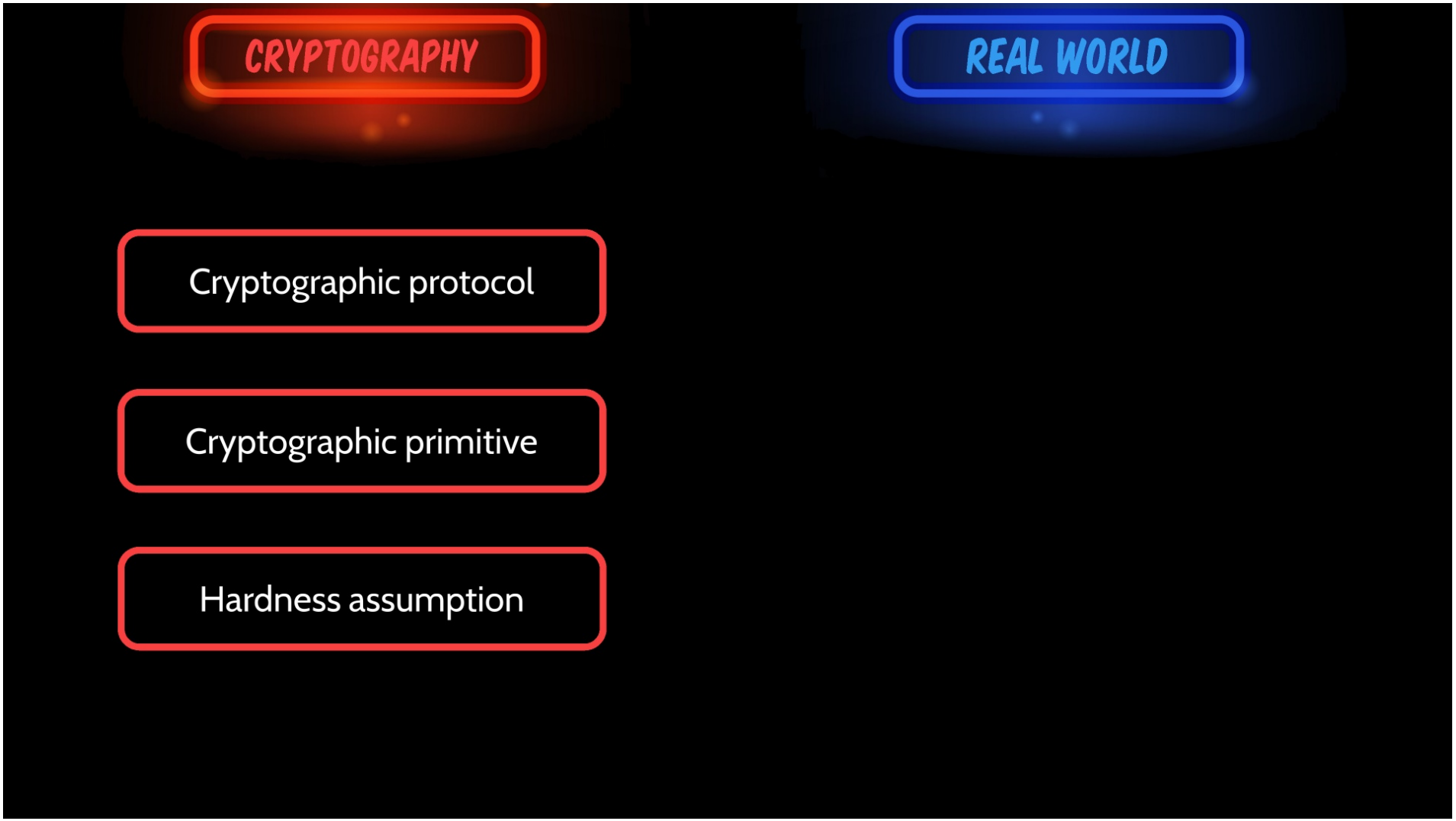
Images credits

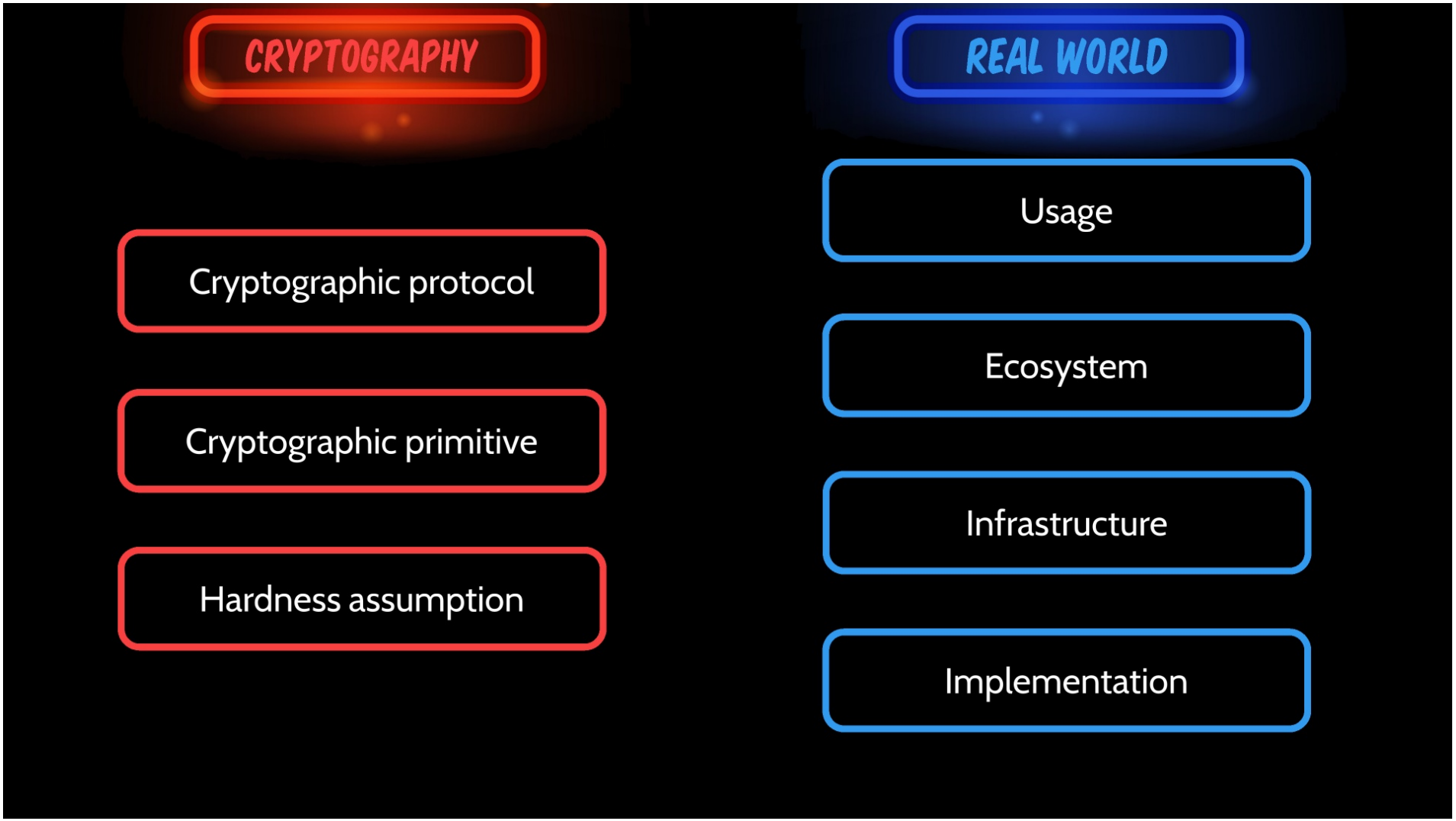
- *vecteezy.com*
- *xkcd.com*
- *"Intro to DPA"*
- *Proton AG*

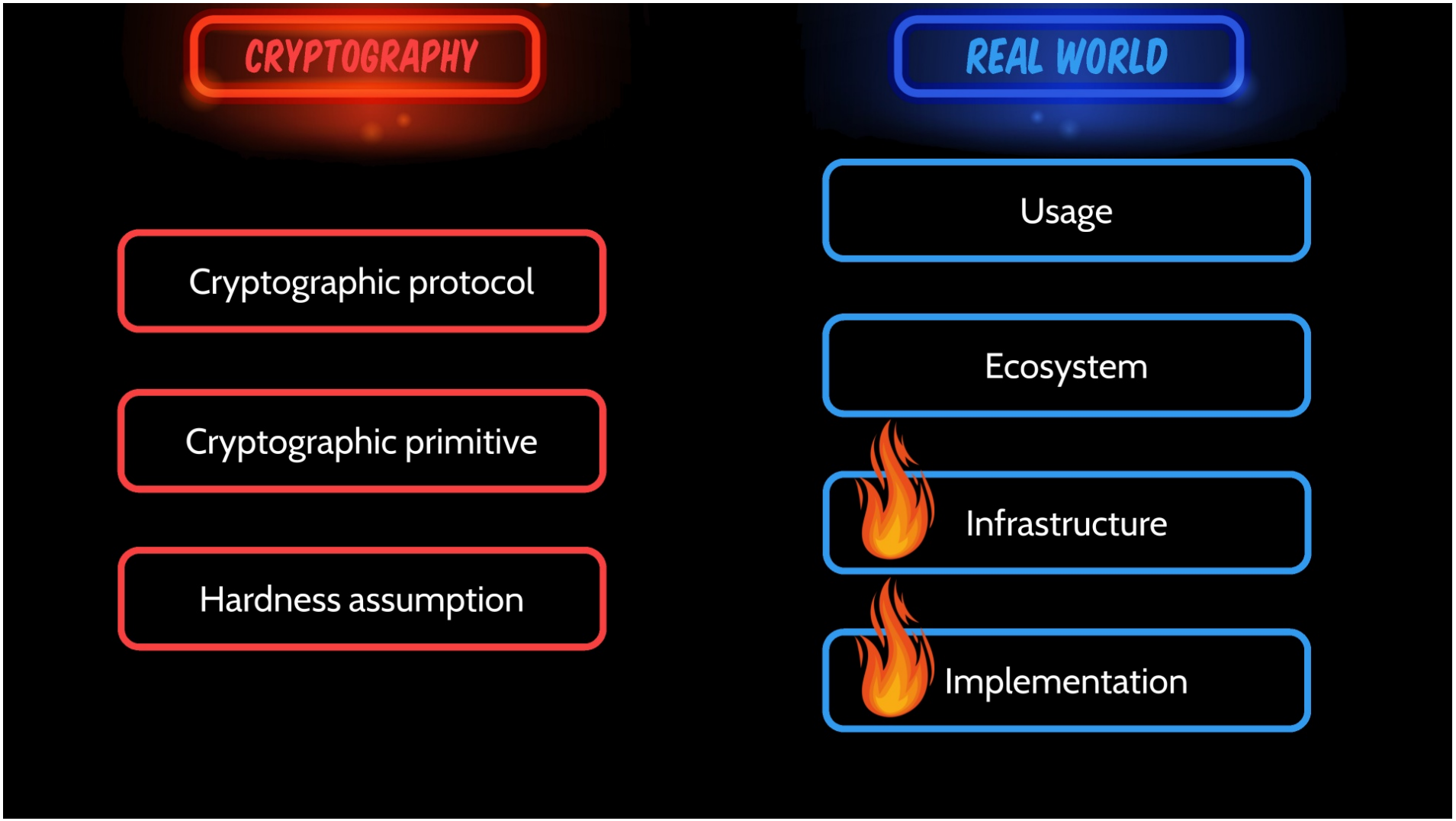

MARCO MARTINOLI
10 - 05 - 2022
VS
CRYPTOGRAPHY
REAL WORLD

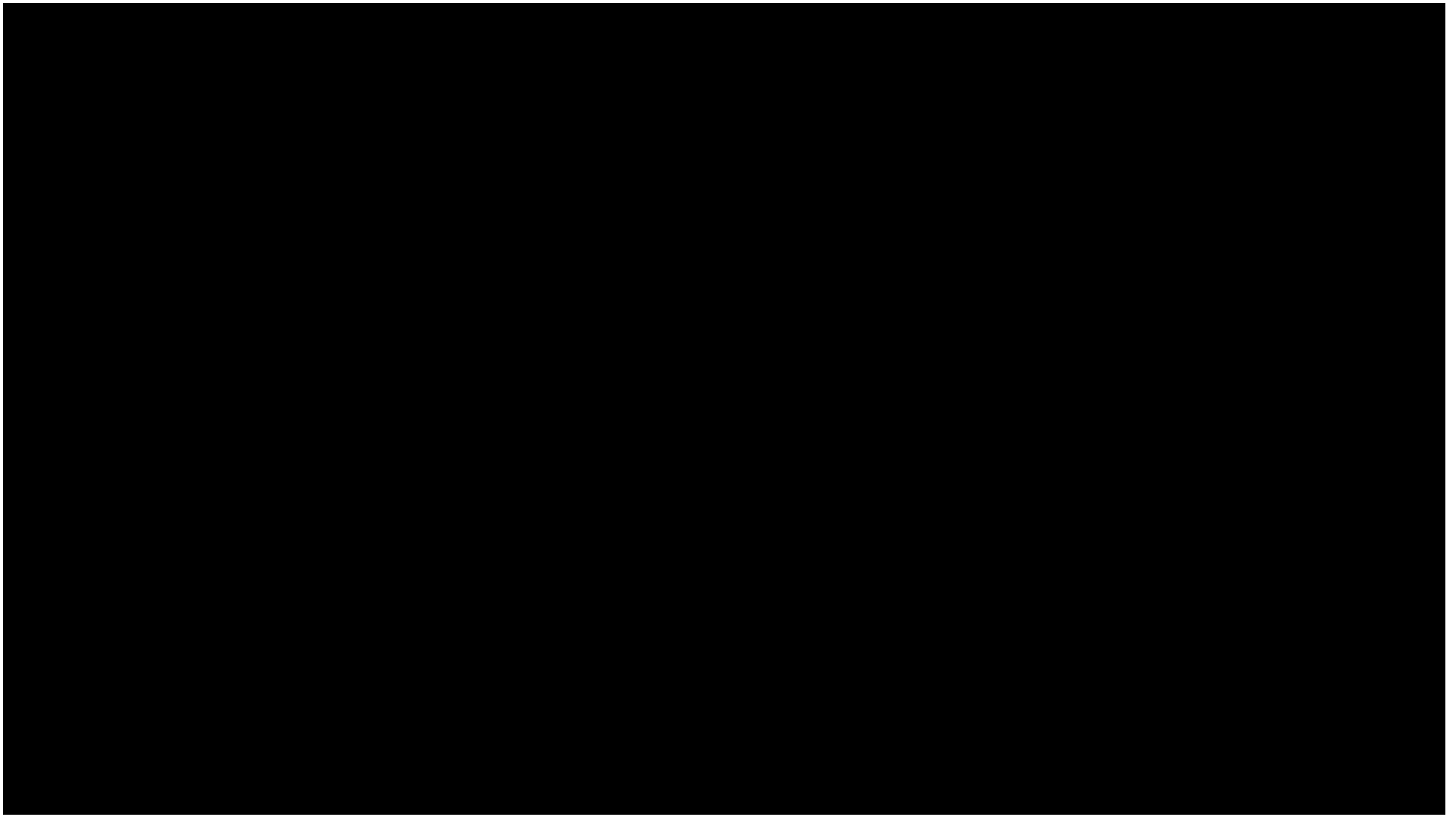

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

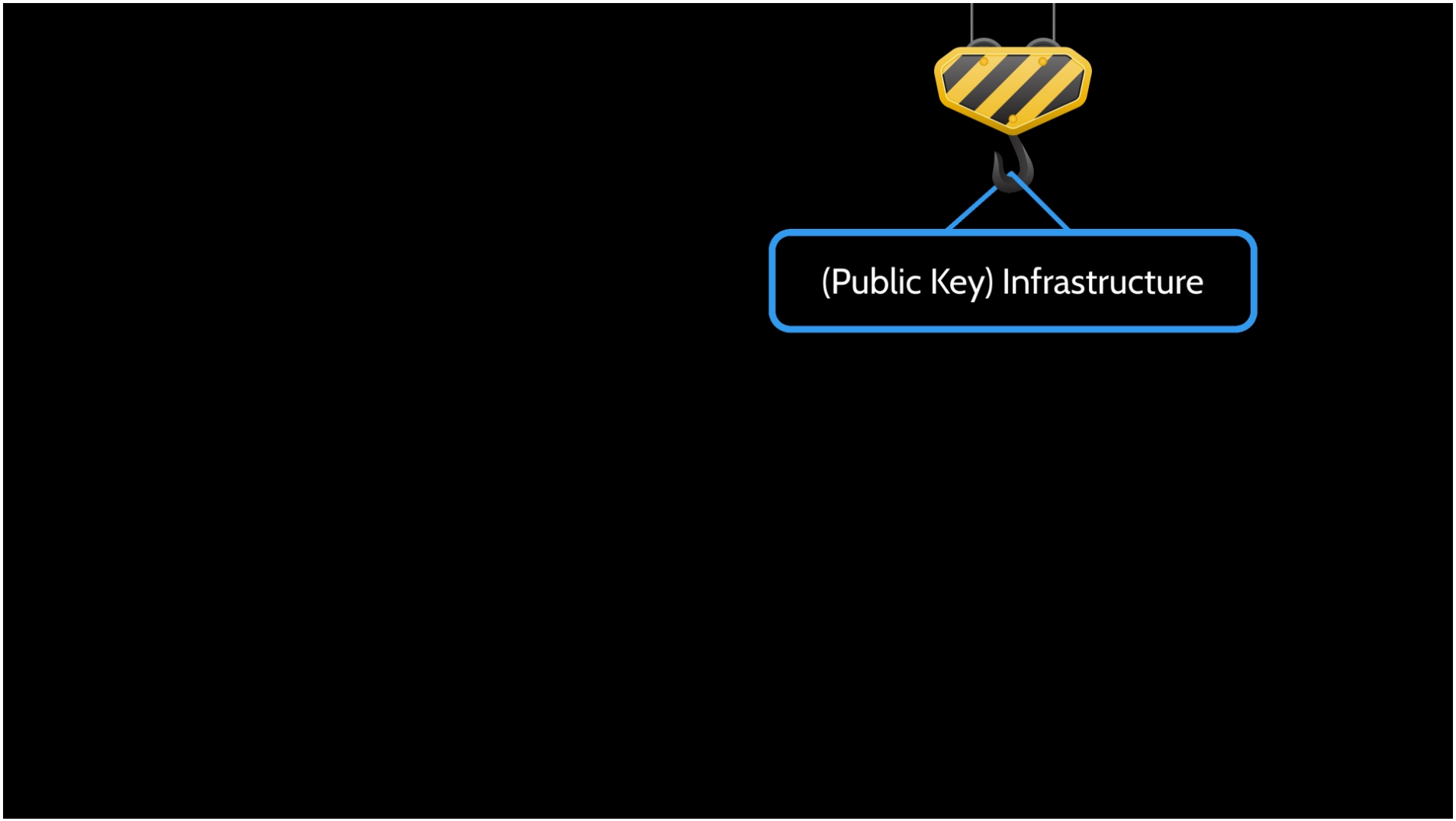

CRYPTOGRAPHY
REAL WORLD

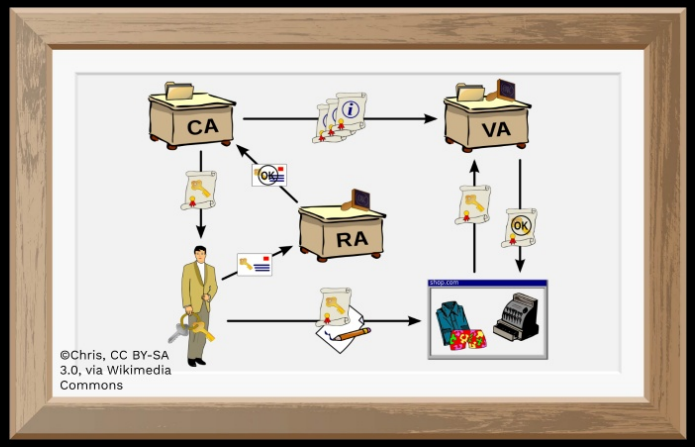

CRYPTOGRAPHY
REAL WORLD
Cryptographic protocol
Cryptographic primitive
Hardness assumption

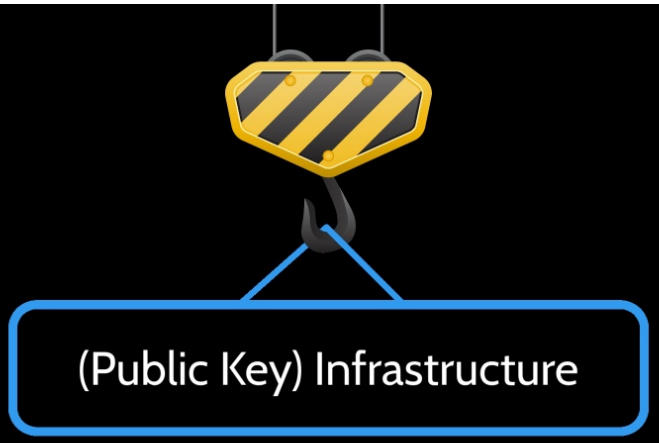

CRYPTOGRAPHY
REAL WORLD
Cryptographic protocol
Cryptographic primitive
Hardness assumption
Usage
Ecosystem
Infrastructure
Implementation

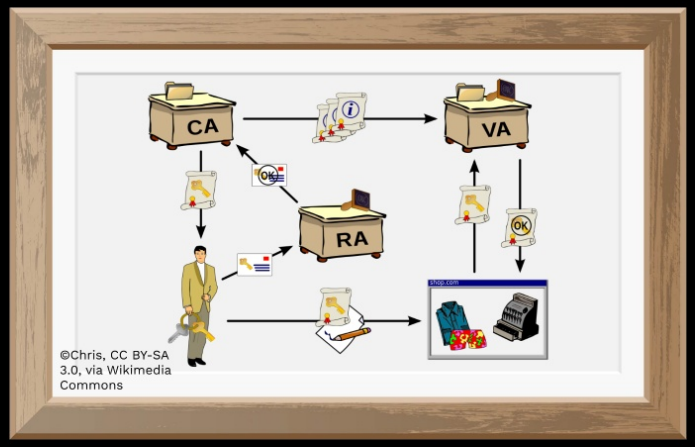

CRYPTOGRAPHY
REAL WORLD
Cryptographic protocol
Cryptographic primitive
Hardness assumption
Usage
Ecosystem
Infrastructure
Implementation

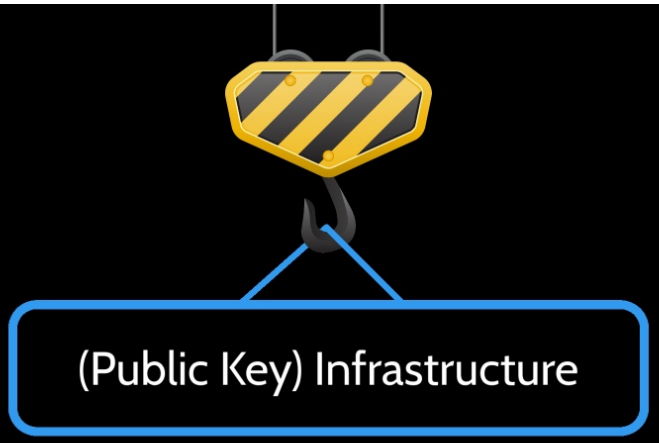


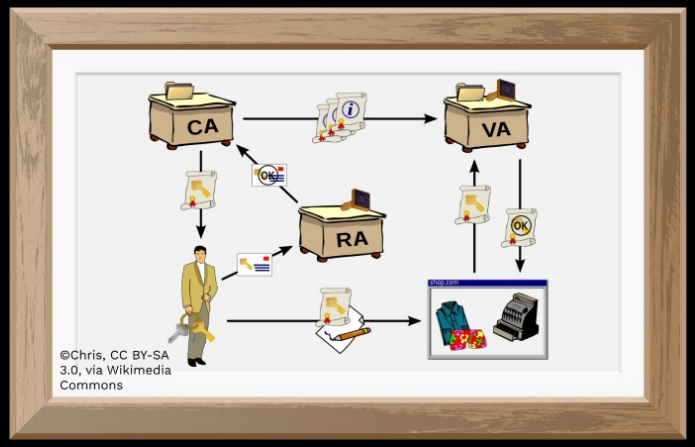

(Public Key) Infrastructure

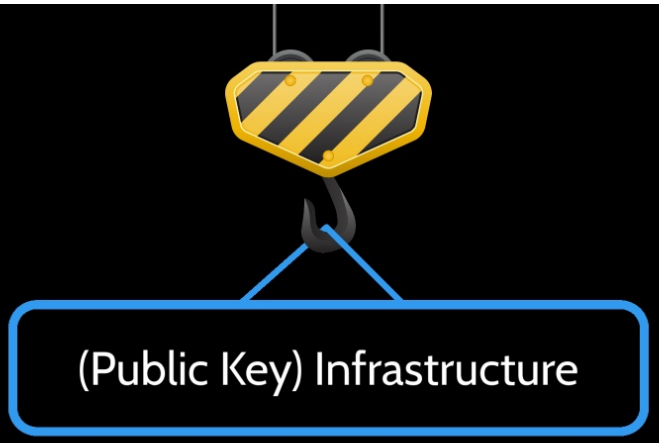

CA
VA
RA
OK
OK
©Chris, CC BY-SA 3.0, via Wikimedia Commons


(Public Key) Infrastructure

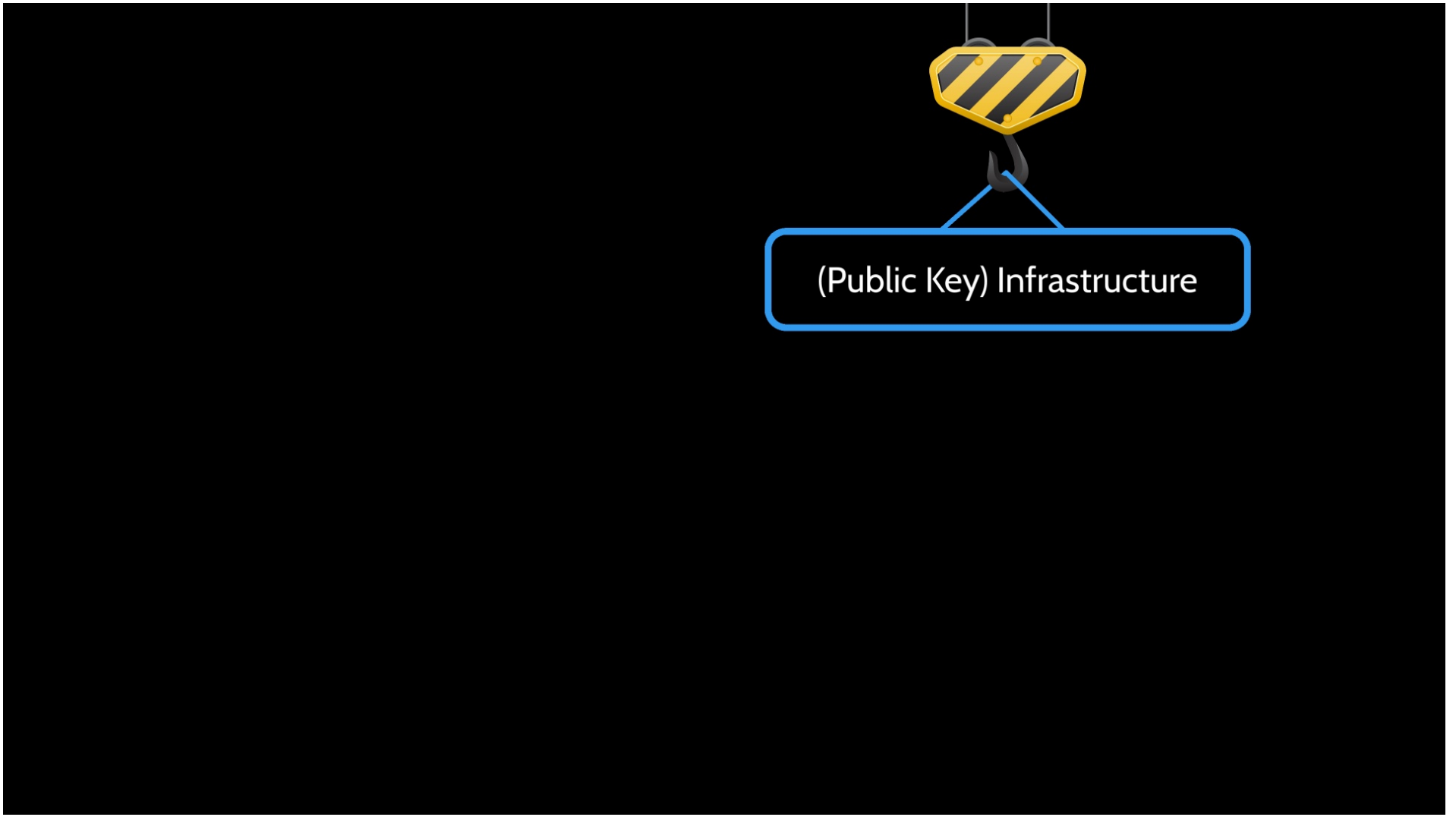

CA
VA
RA
OK
OK
©Chris, CC BY-SA 3.0, via Wikimedia Commons

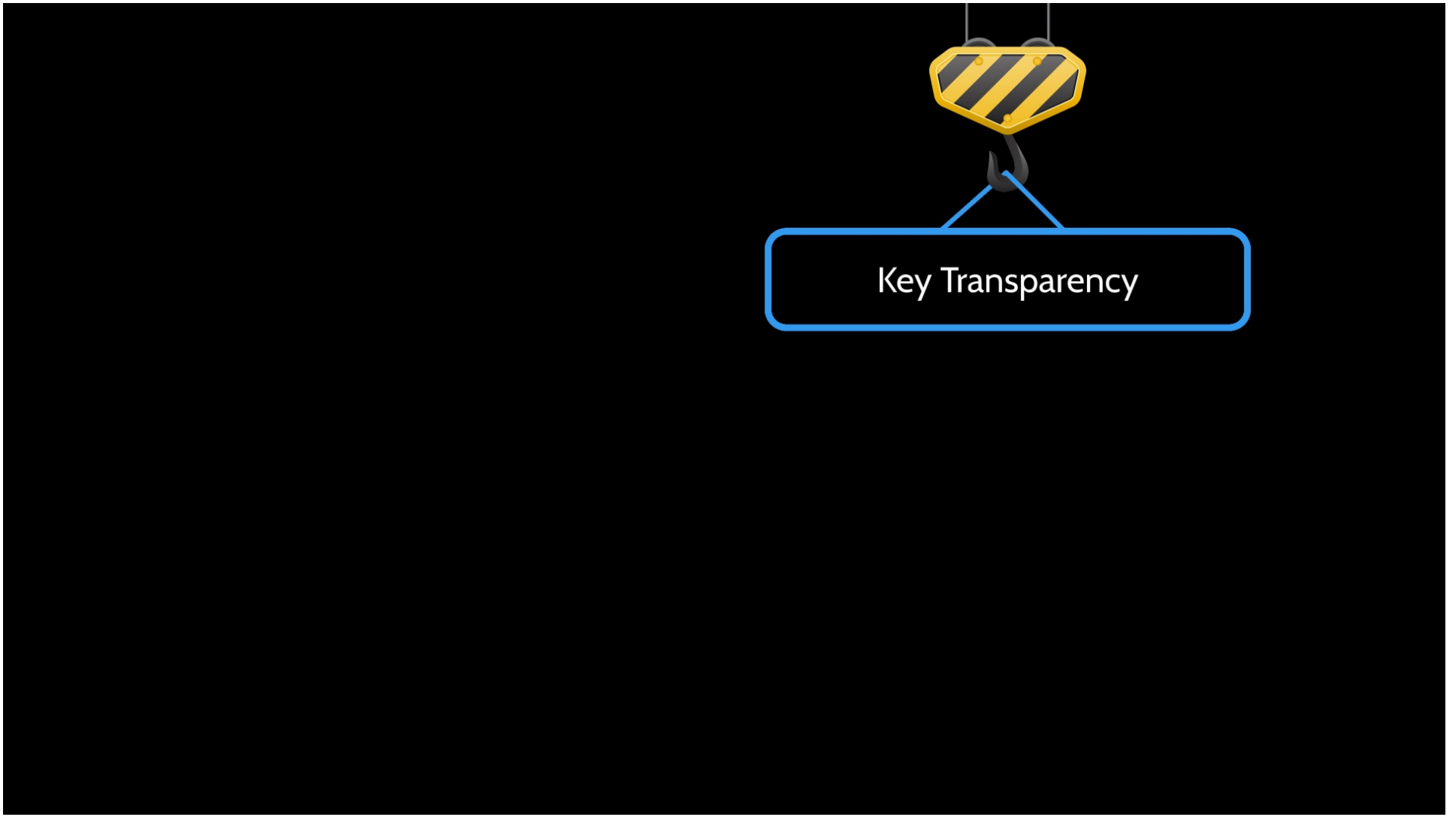

(Public Key) Infrastructure

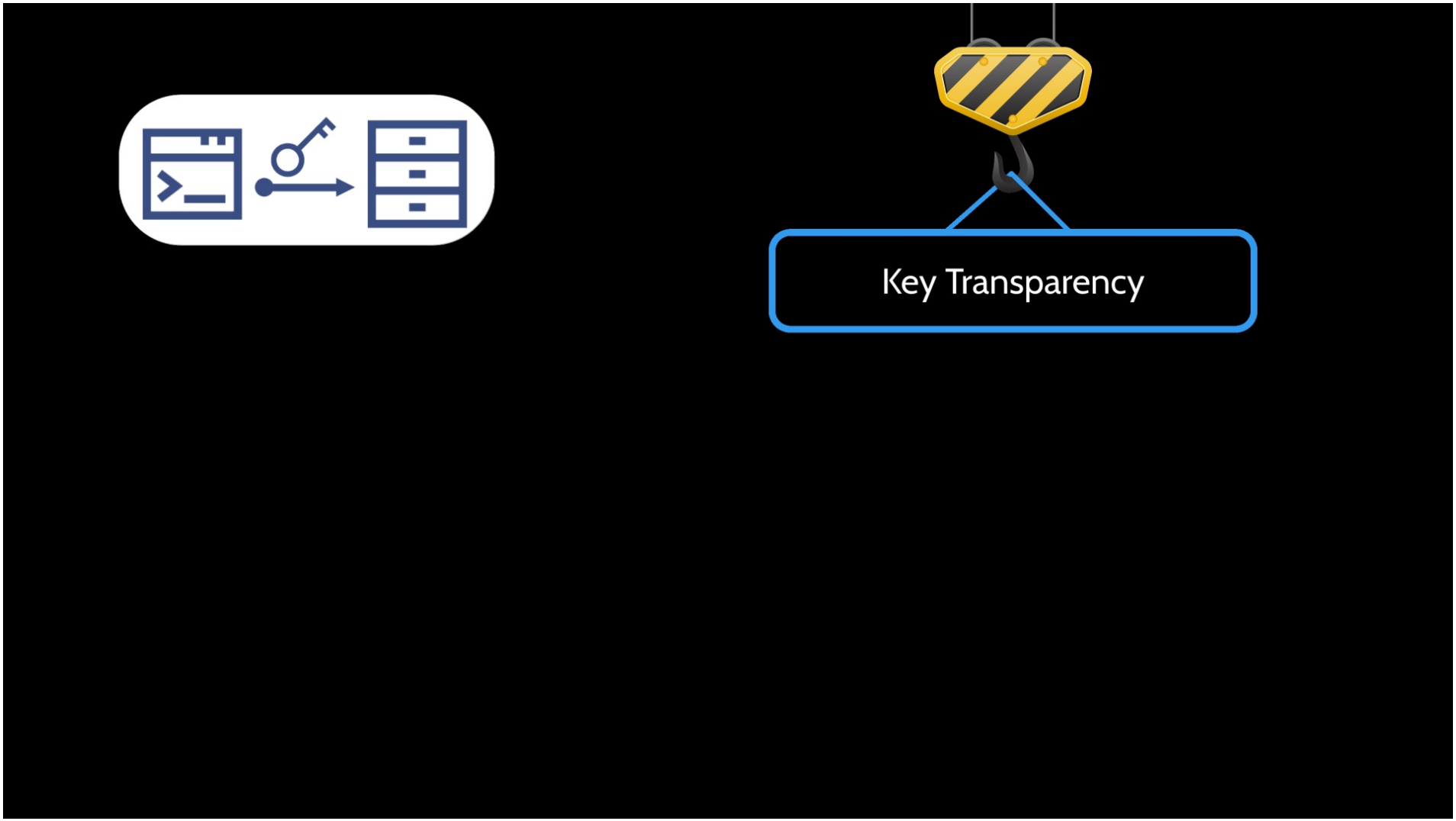

CA
VA
RA
OK
OK
©Chris, CC BY-SA 3.0, via Wikimedia Commons

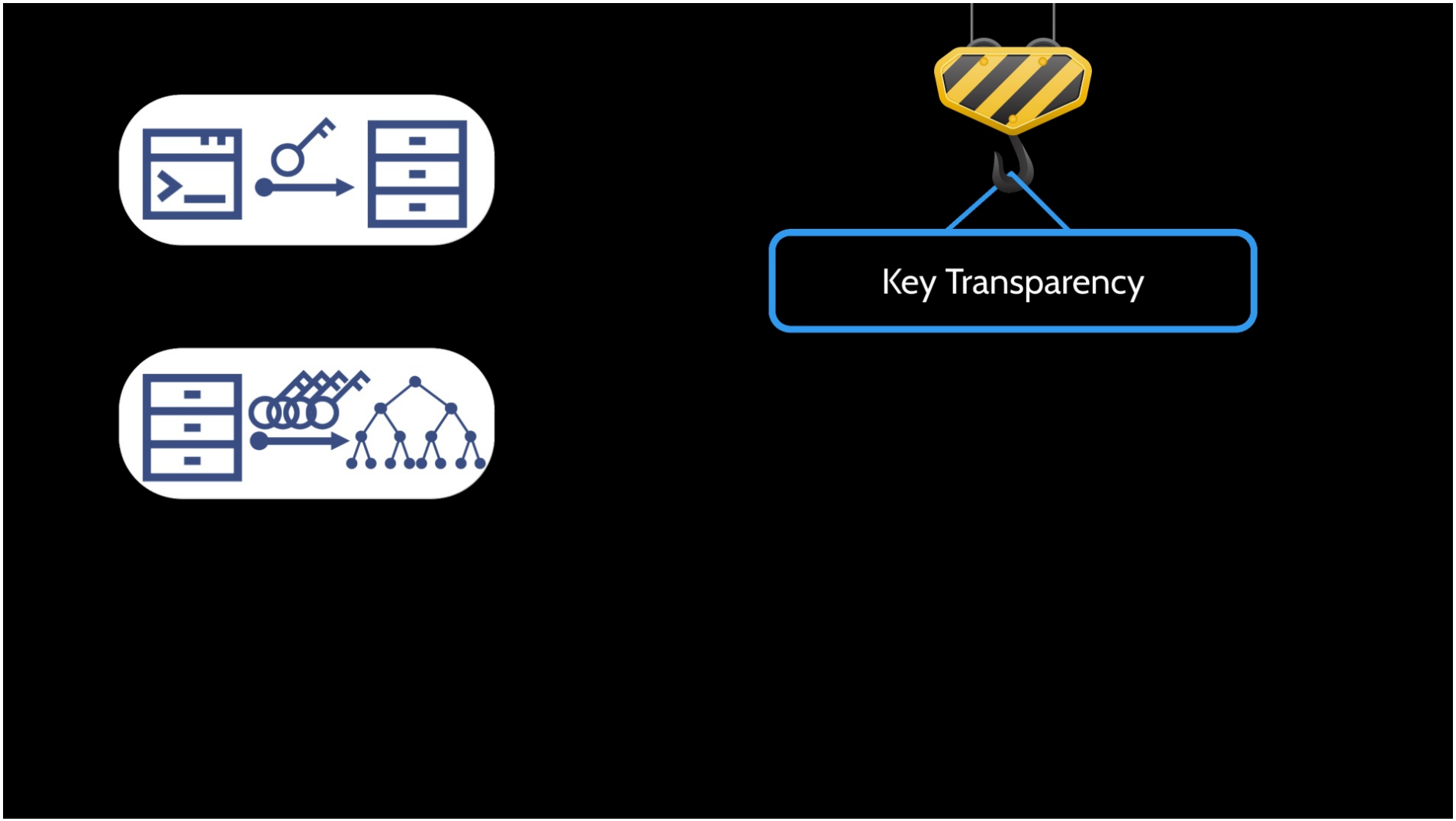

(Public Key) Infrastructure

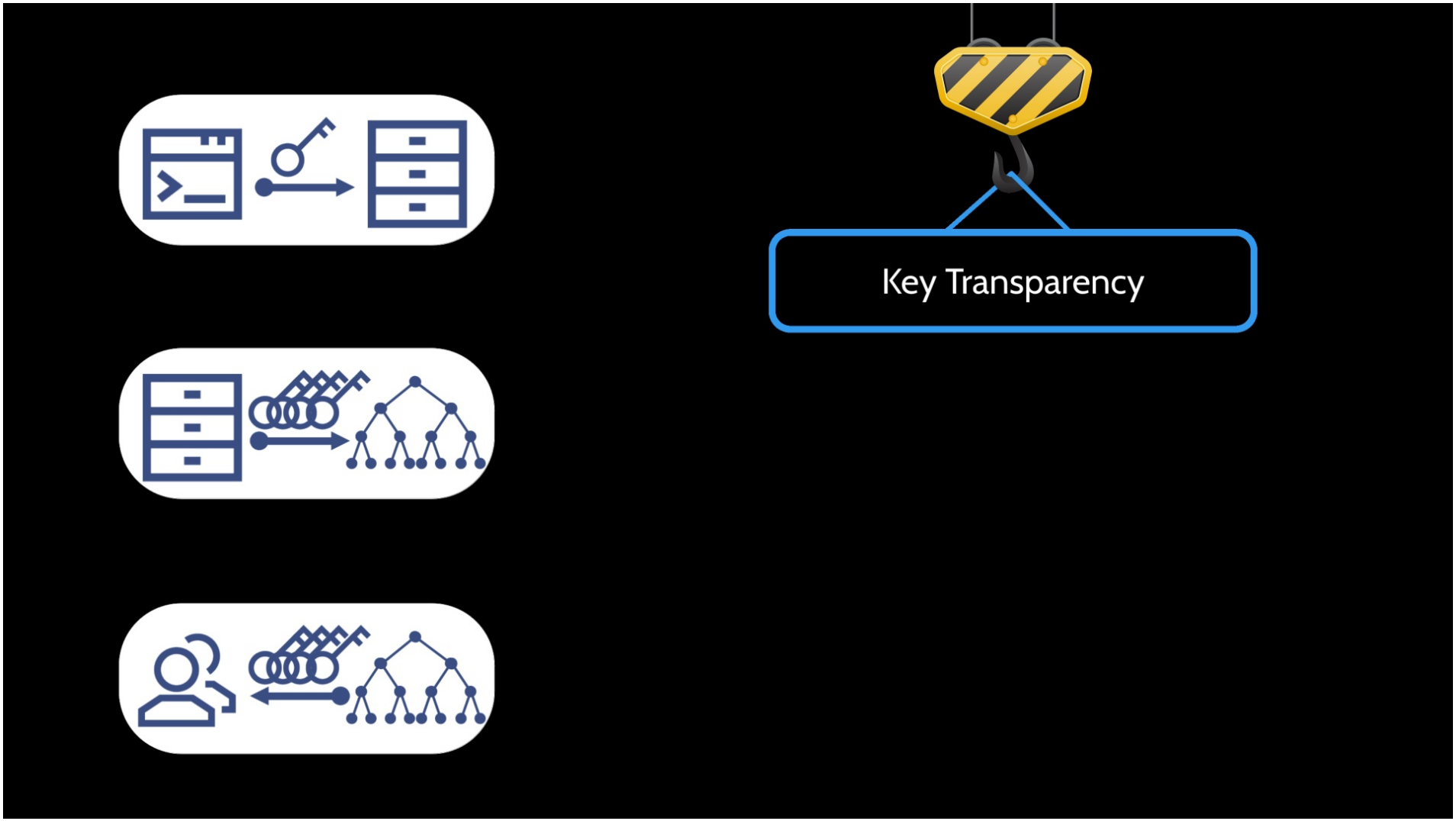

21328 93021 73807 82910
37892 01378 89347 34299
34219 03821 90381 29031

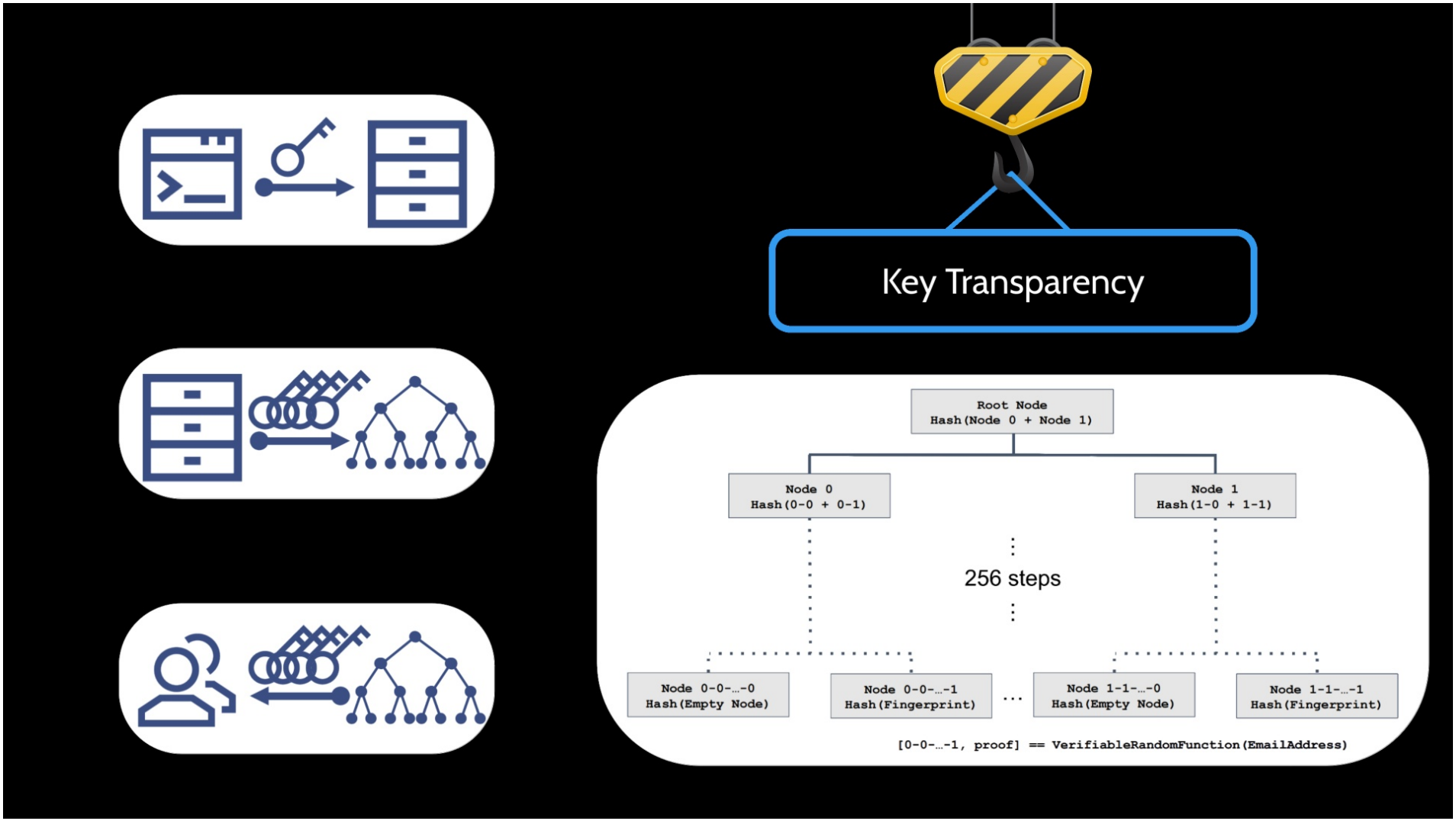

(Public Key) Infrastructure

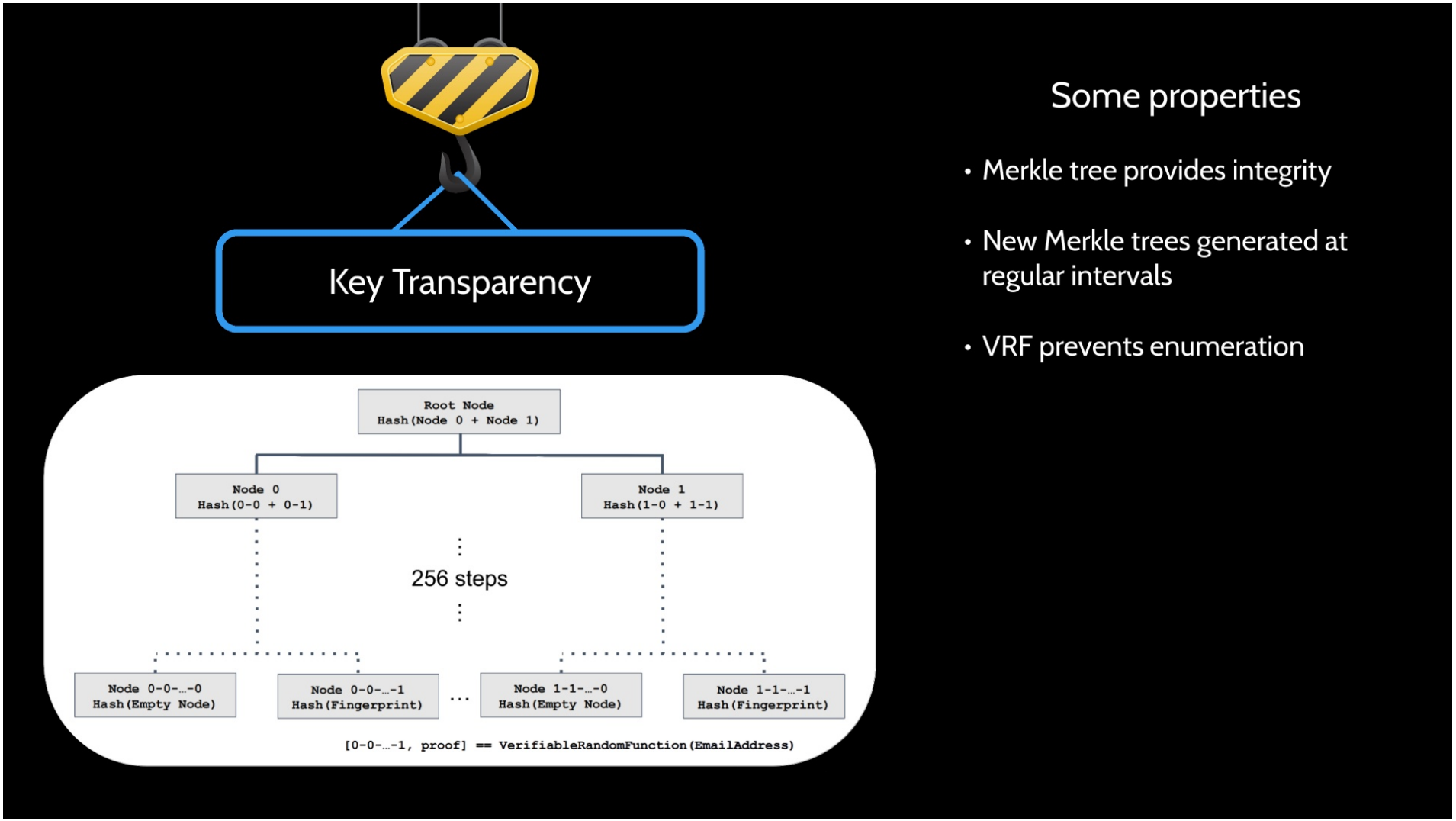

Key Transparency


Key Transparency


Key Transparency

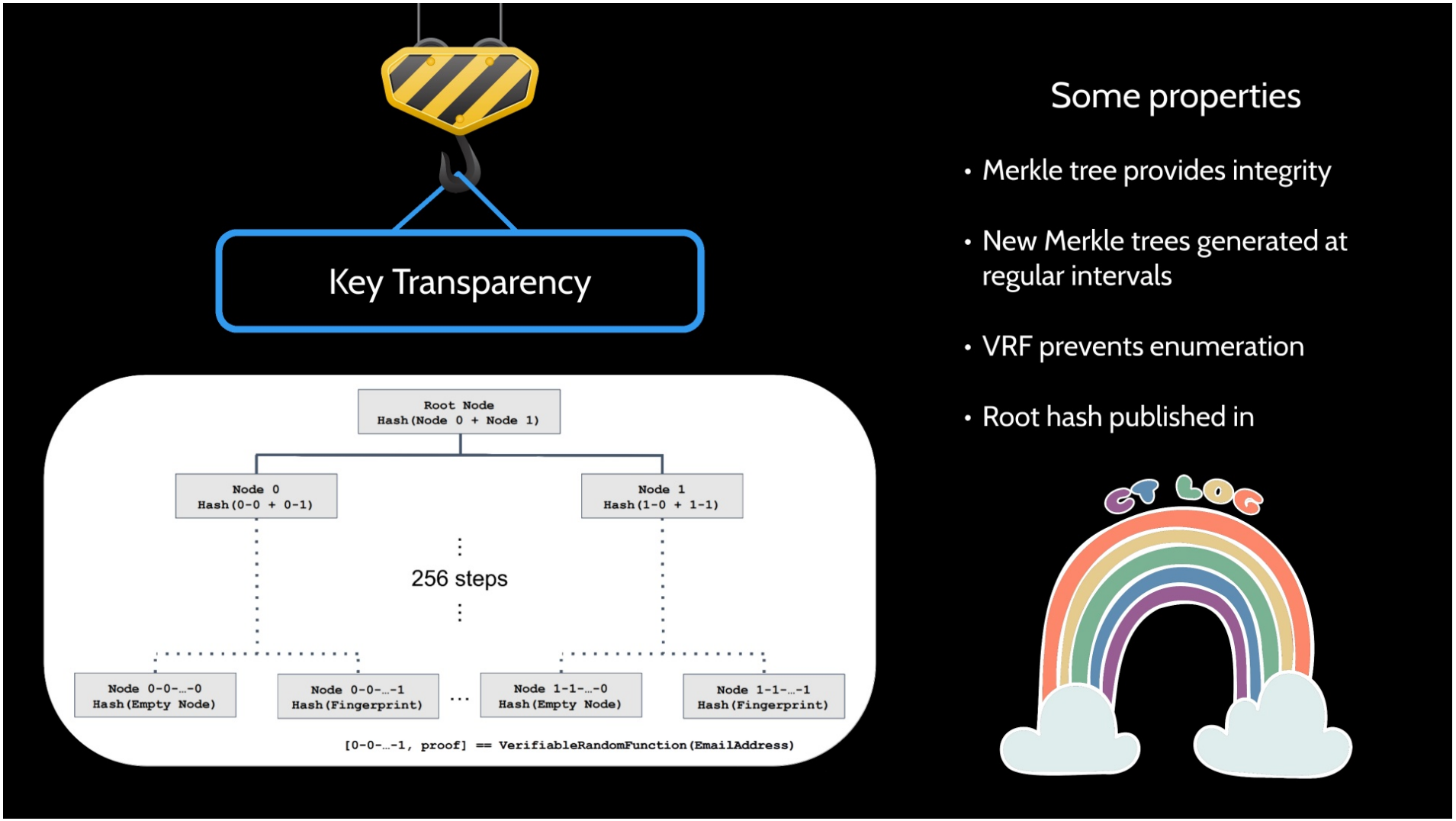

Key Transparency


Key Transparency
Root Node
Hash(Node 0 + Node 1)
Node 0
Hash(0-0 + 0-1)
Node 1
Hash(1-0 + 1-1)
256 steps
Node 0-0-…-0
Hash(Empty Node)
Node 0-0-…-1
Hash(Fingerprint)
Node 1-1-…-0
Hash(Empty Node)
Node 1-1-…-1
Hash(Fingerprint)
[0-0-…-1, proof] == VerifiableRandomFunction(EmailAddress)



Some properties

- Merkle tree provides integrity
- New Merkle trees generated at regular intervals
- VRF prevents enumeration

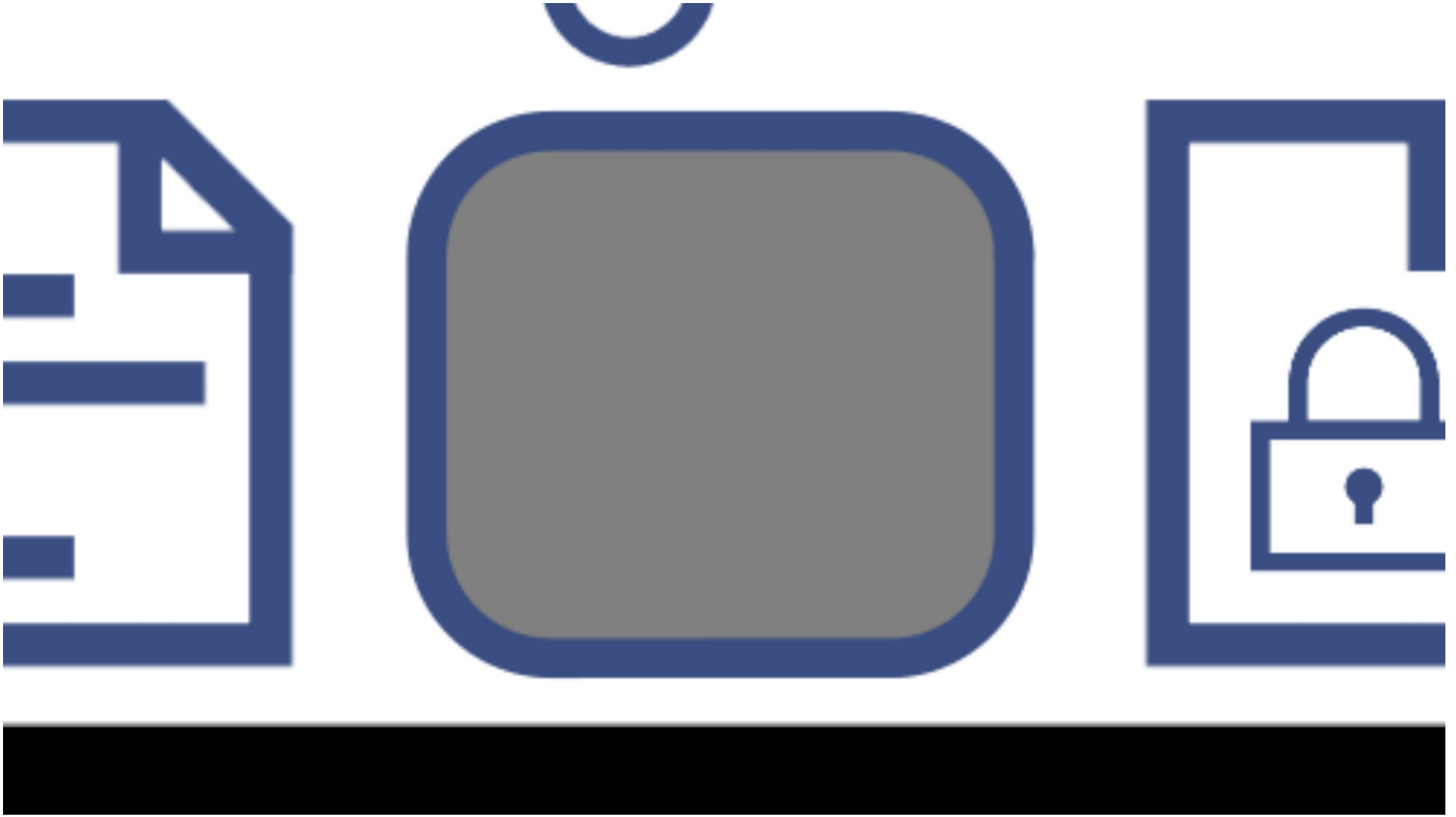

Key Transparency
Root Node
Hash(Node 0 + Node 1)
Node 0
Hash(0-0 + 0-1)
Node 1
Hash(1-0 + 1-1)
256 steps
Node 0-0-…-0
Hash(Empty Node)
Node 0-0-…-1
Hash(Fingerprint)
Node 1-1-…-0
Hash(Empty Node)
Node 1-1-…-1
Hash(Fingerprint)
[0-0-…-1, proof] == VerifiableRandomFunction(EmailAddress)
Some properties
• Merkle tree provides integrity
• New Merkle trees generated at regular intervals
• VRF prevents enumeration
• Root hash published in
CT LOG

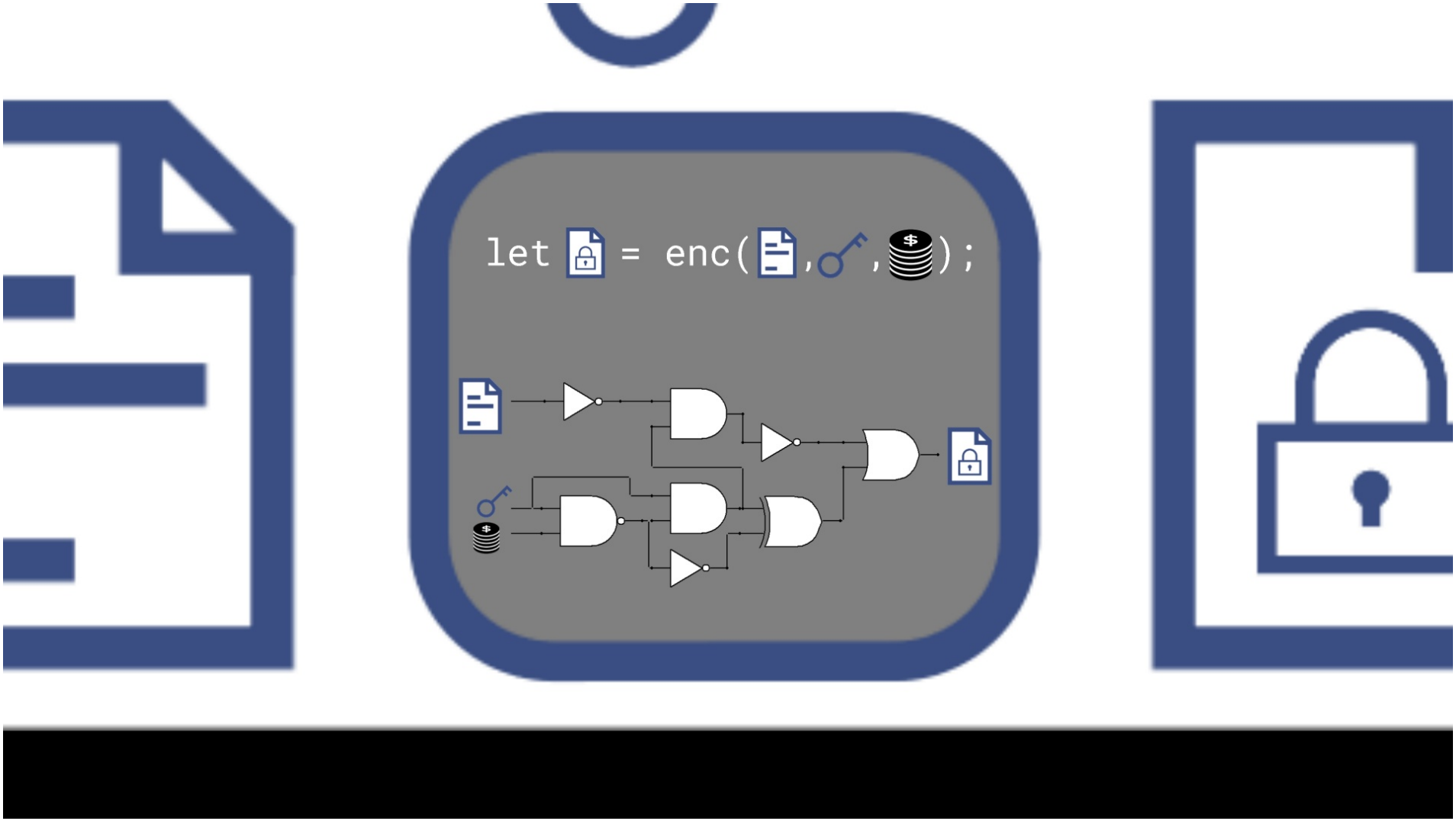

SIDE-CHANNEL
ANALYSIS


SIDE-CHANNEL
ANALYSIS


SIDE-CHANNEL
ANALYSIS

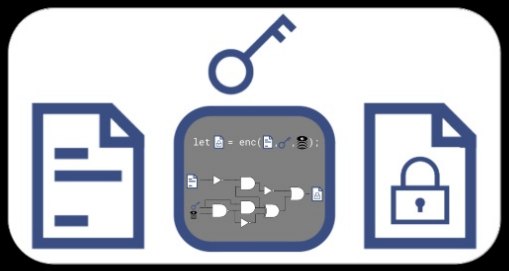

SIDE-CHANNEL
ANALYSIS

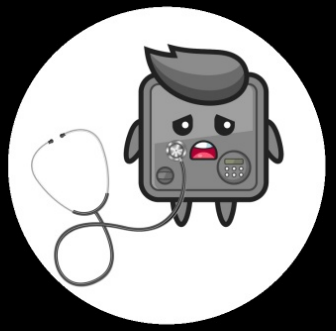



let = enc(, ,);


SIDE-CHANNEL
ANALYSIS

```
const strCompare = (str1, str2) => {
  if (str1.length !== str2.length) {
    return false;
  }

  for(let i = 0; i < str1.length; i++) {
    if (str1[i] !== str2[i]) {
      return false;
    }
  }

  return true;
};
```

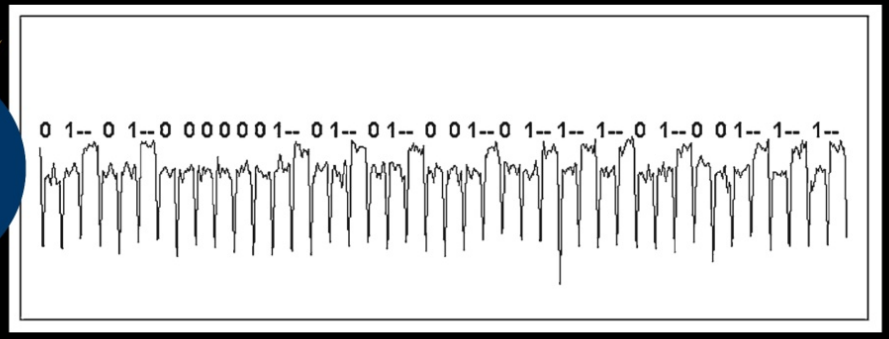




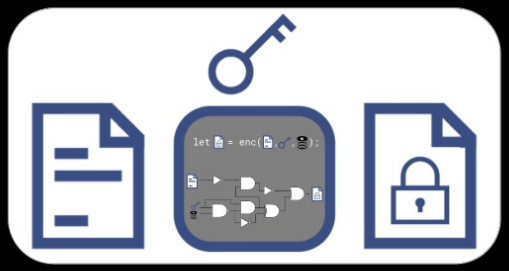
SIDE-CHANNEL

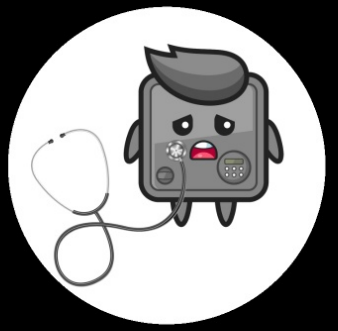
ANALYSIS

```
const strCompare = (str1, str2) => {
  if (str1.length !== str2.length) {
    return false;
  }

  for(let i = 0; i < str1.length; i++) {
    if (str1[i] !== str2[i]) {
      return false;
    }
  }

  return true;
};
```



Introduction to Differential Power Analysis
Journal of Cryptographic Engineering, April 2011
P. Kocher, J. Jaffe, B. Jun, P. Rohatgi

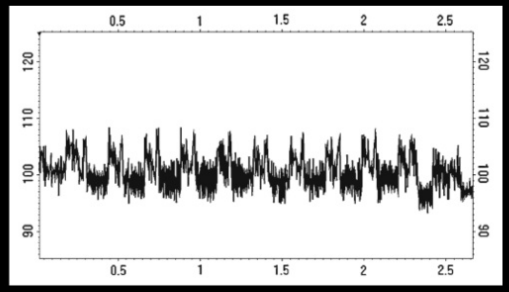




SIDE-CHANNEL

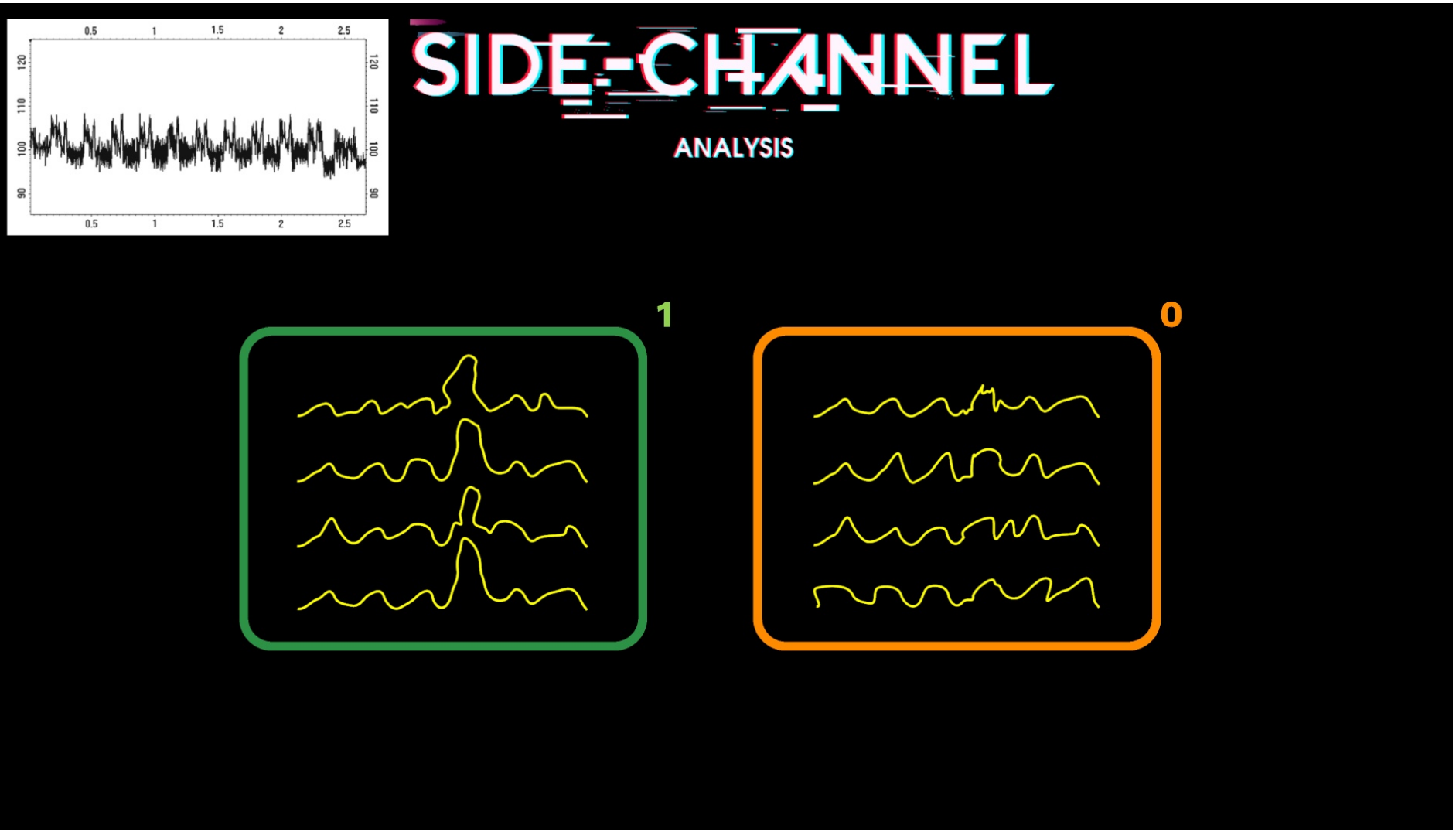
ANALYSIS

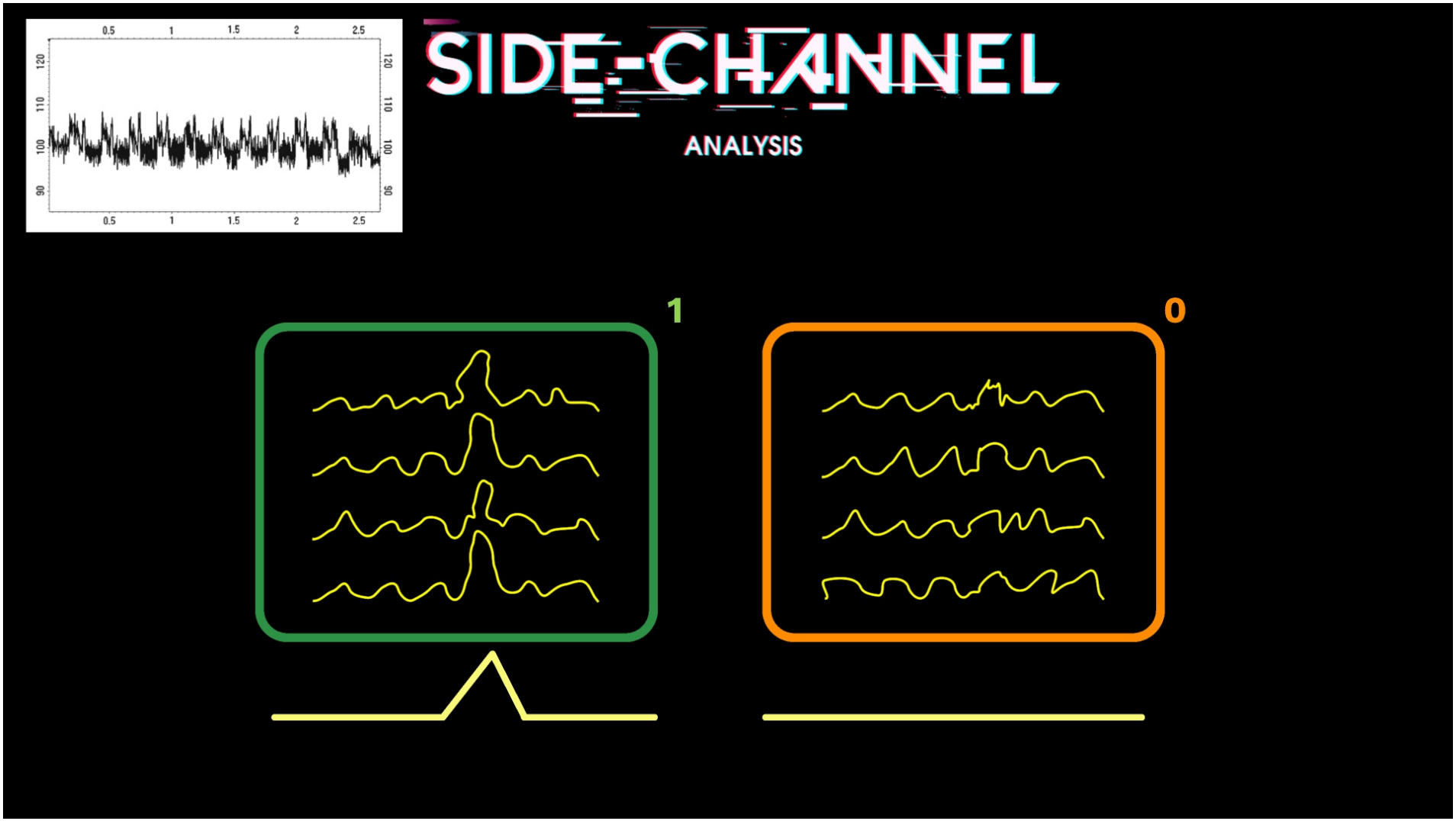

SIDE-CHANNEL
ANALYSIS

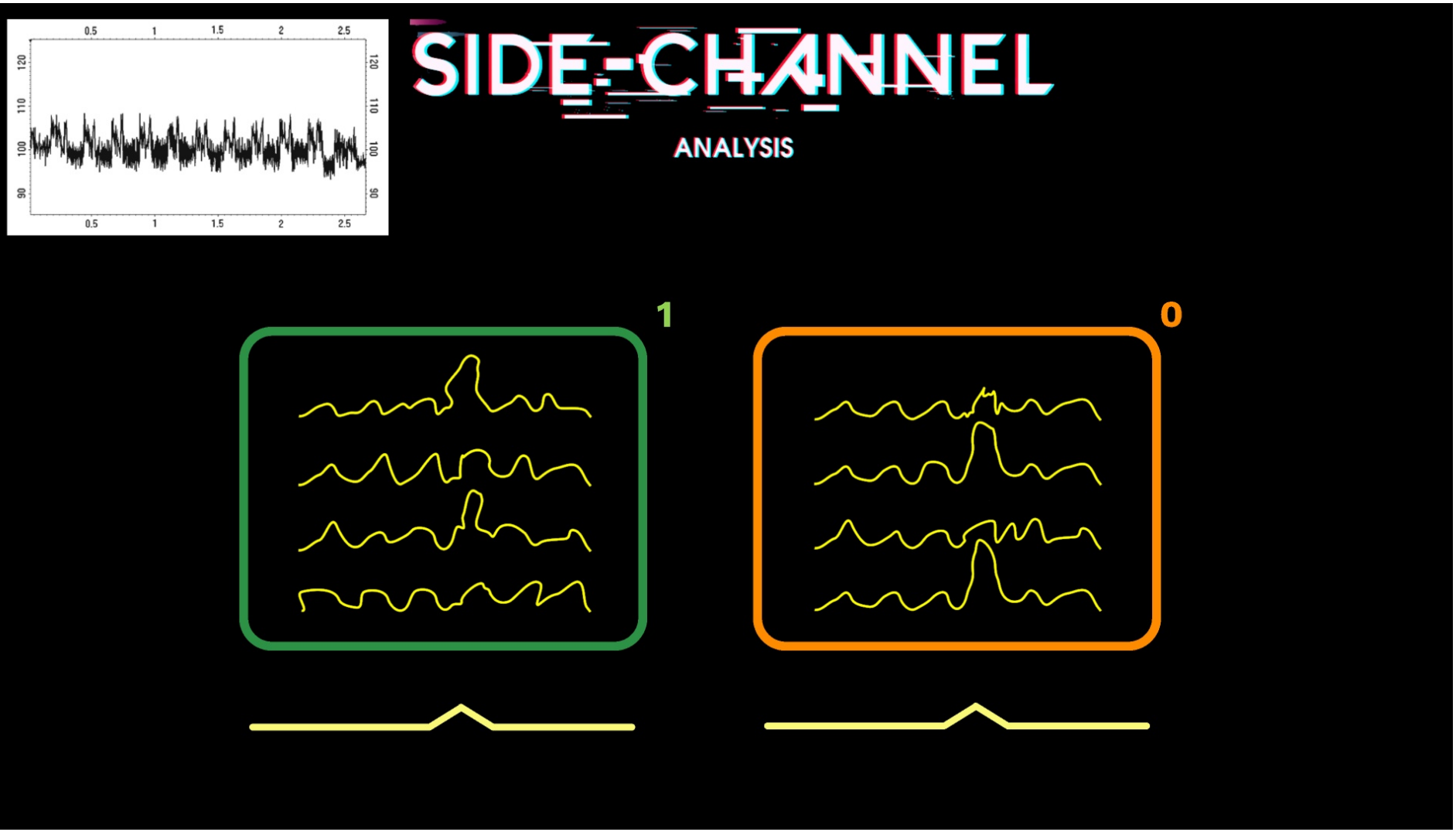


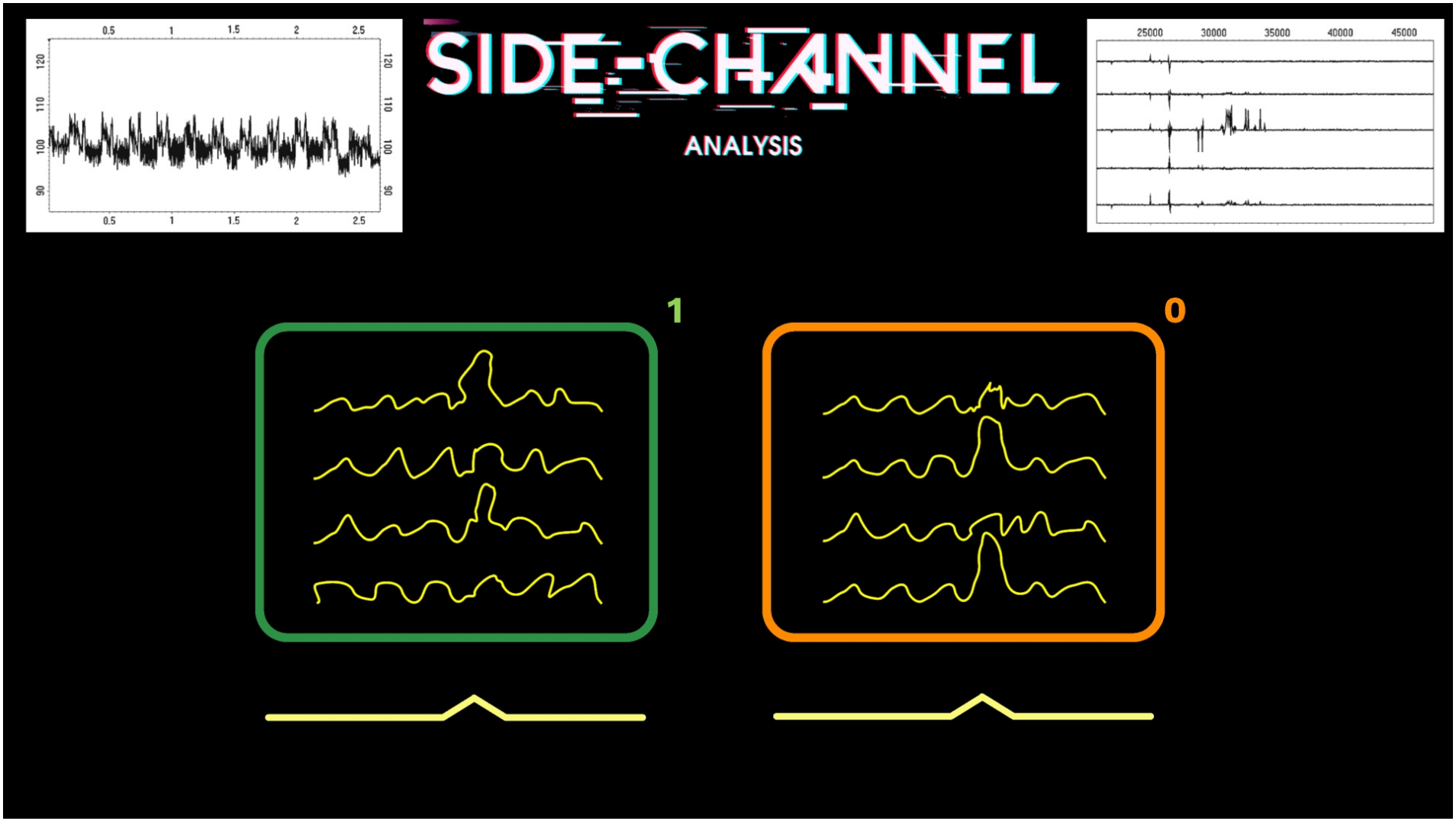
SIDE-CHANNEL

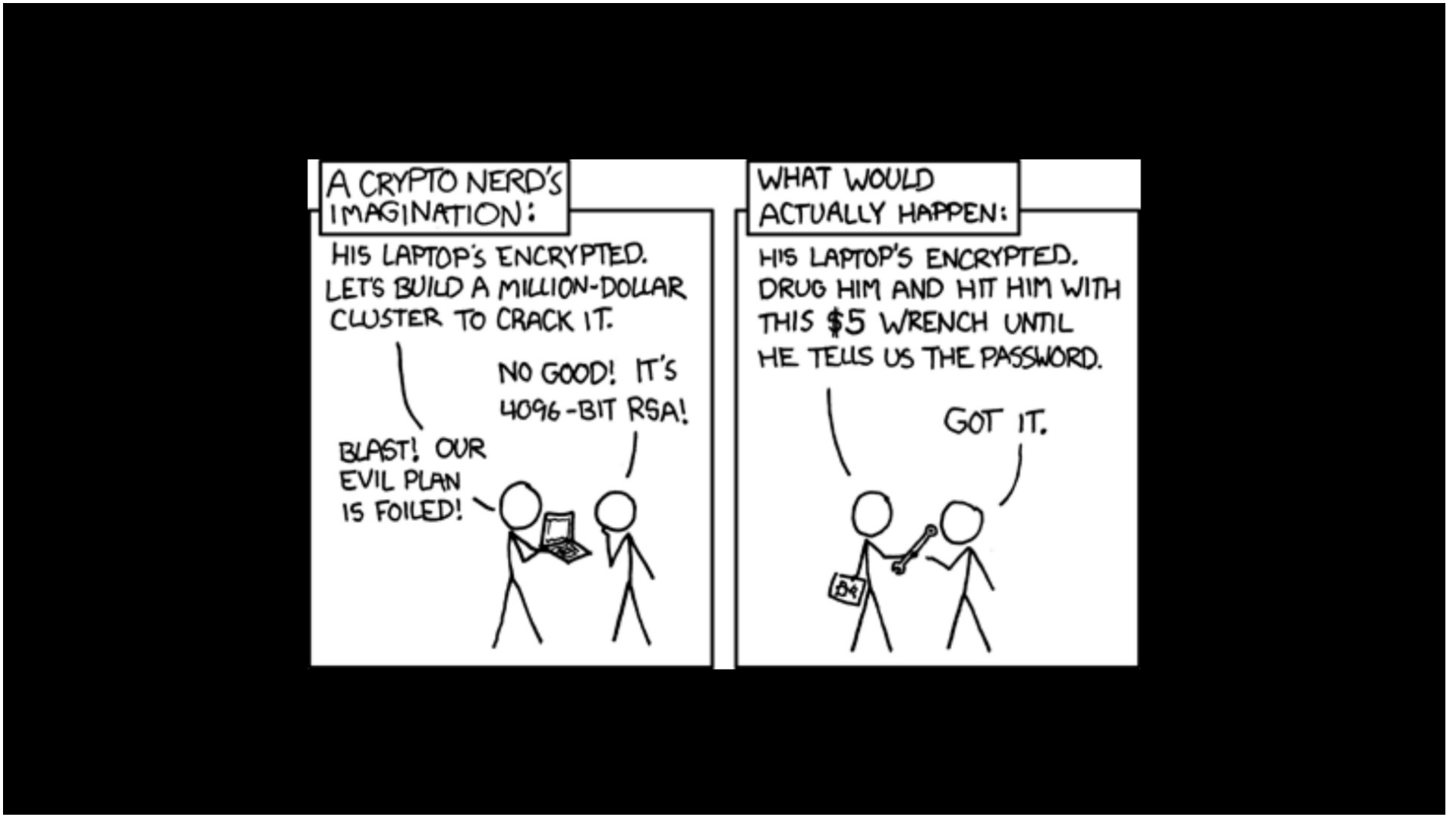
ANALYSIS

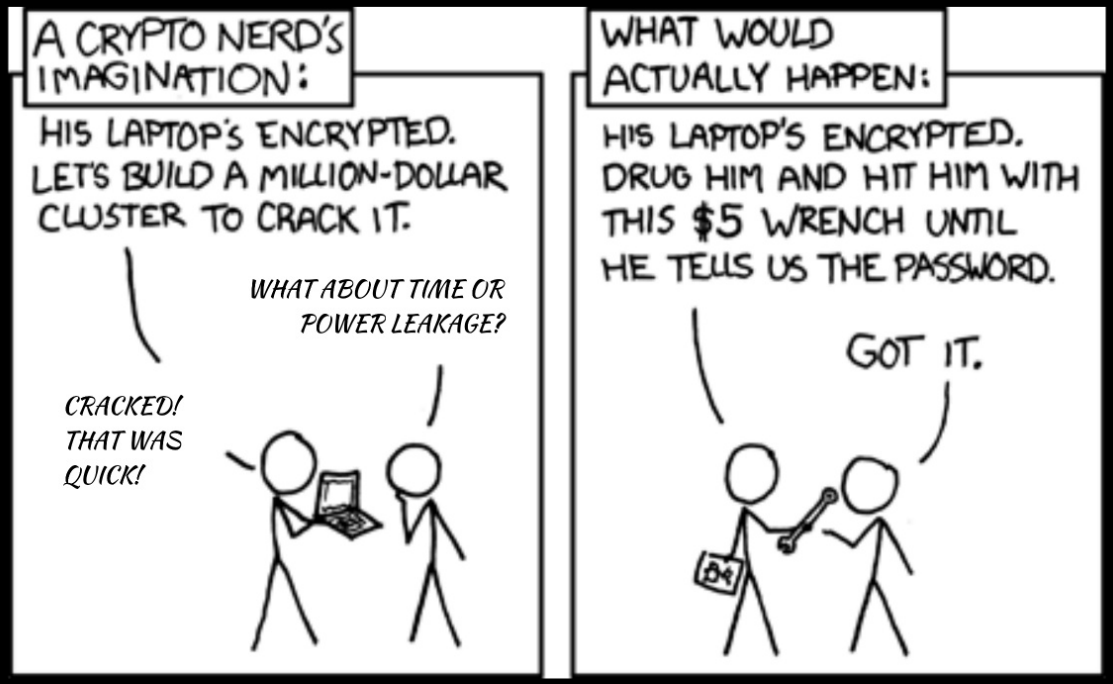

SIDE-CHANNEL
ANALYSIS
1
0


SIDE-CHANNEL
ANALYSIS
1
0


SIDE-CHANNEL
ANALYSIS
1
0


SIDE-CHANNEL
ANALYSIS
1
0


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

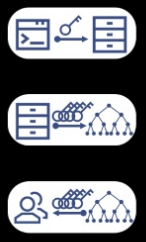

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
WHAT ABOUT TIME OR POWER LEAKAGE?
CRACKED! THAT WAS QUICK!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

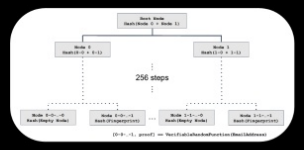
MARCO MARTINOLI
10 - 05 - 2022

VS

- Cryptographic protocol
- Cryptographic primitive
- Hardness assumption

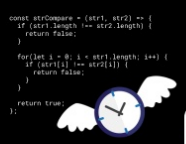
- Usage
- Ecosystem
- Infrastructure
- Implementation

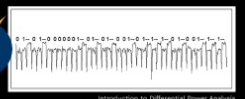




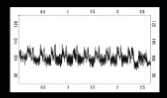
Some properties

- Merkle tree provides integrity
- New Merkle trees generated at regular intervals
- VRF prevents enumeration
- Root hash published in

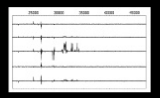


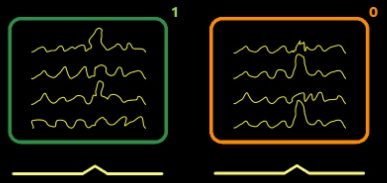


Introduction to Differential Power Analysis
Journal of Cryptographic Engineering, April 2011
P. Kocher, J. Jaffe, B. Jun, P. Rohatgi



SIDE-CHANNEL
ANALYSIS





Images credits

- *vecteezy.com*
- *xkcd.com*
- *"Intro to DPA"*
- *Proton AG*