Trojan-tolerant Hardware & Supply Chain Security in Practice

Who we are

Vasilios Mavroudis
Doctoral Researcher, UCL

Dan Cvrcek
CEO, Enigma Bridge

George Danezis
Professor, UCL

Petr Svenda
CTO, Enigma Bridge
Assistant Professor, MUni

Highlights

- HSMs & Shortcomings
- Existing Solutions
- Lessons learned from airplanes
- Hardware Prototype
- Crypto Protocols
- Attack-Defense Demo
- Politics, Distrust & Hardware Security

Hardware Security Modules

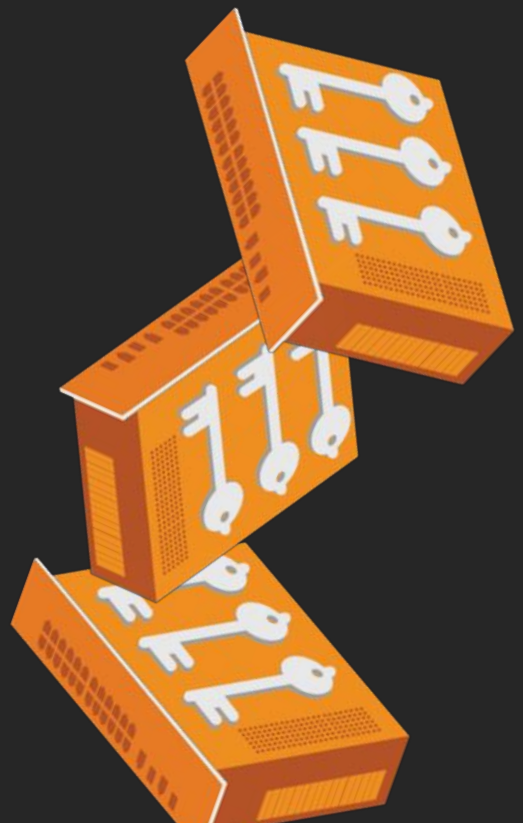
Physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.

Applications:

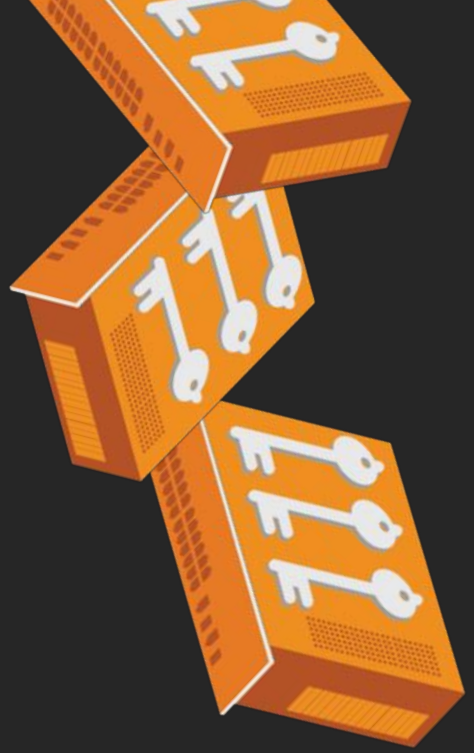
- Cryptographic key generation, storage, management
- Sensitive data handling and storage
- Application servers offloading

Crypto Operations are carried out in the device

No need to output the private keys!



HSM Threat Model



Common Use cases:

PKIs, Card payment systems, SSL connections, DNSSEC, &Transparent Data Encryption for Databases

Certified to Common Criteria or FIPS 140:

- Anti-Tampering Protection
- Strong Random Number Generator
- Cryptographic key management

- Bugs

CVE-2015-5464
The HSM allows remote authenticated users to bypass intended key-export restrictions …

- Errors

MiFare Classic RFID chip: the 16-bit random number generator was easy to manipulate

- Backdoors/HT

THIS 'DEMONICALLY CLEVER' BACKDOOR HIDES IN A TINY SLICE OF A COMPUTER CHIP

NSA's Own Hardware Backdoors May Still Be a "Problem from Hell"

Expert Says NSA Have Backdoors Built Into Intel And AMD Processors

Snowden: The NSA planted backdoors in Cisco products

Existing Solutions

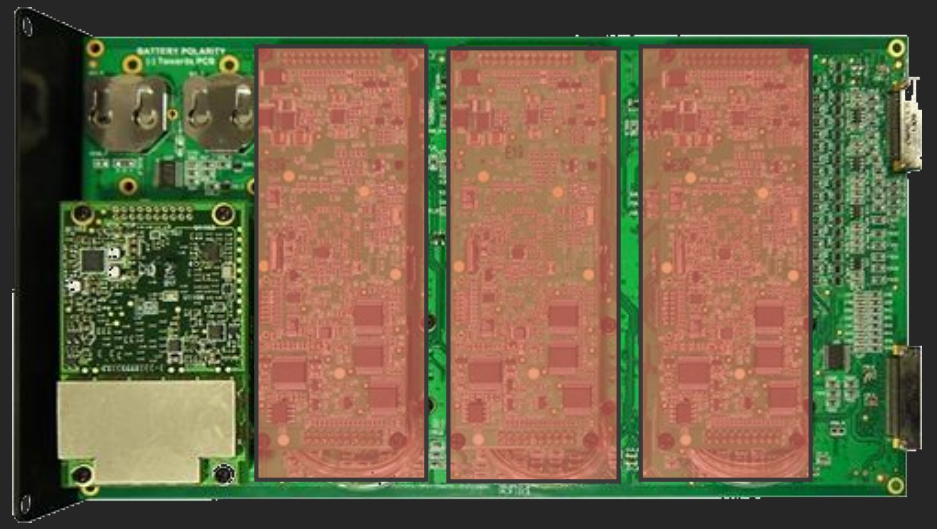
- Trusted Foundries
  - Very expensive
  - Prone to errors
- Split-Manufacturing
  - Still Expensive
  - Again prone to errors
  - Not 100% secure
- Post-fabrication Inspection
  - Expensive
  - A huge pain, doesn’t scale
- Secret-sharing
  - Keys generated by a trusted party
  - Only for key storage

Alternative approaches?

A solution from the sky (not the cloud)

Lockstep systems *are fault-tolerant computer systems that run the same set of operations at the same time in parallel.*

- Dual redundancy
  allows error detection and error correction
- Triple redundancy
  automatic error correction, via majority vote
  → Triple Redundant 777 Primary Flight Computer



Not so fast...

- Fault-tolerant systems are built for safety
- The computations are simply replicated
- The majority vote part is using a *trusted* IC

Not enough for security!

Redundancy for security?

We did it!

Supported Crypto

- Random number Generation
- Key Generation & Management
- Decryption
- Signing

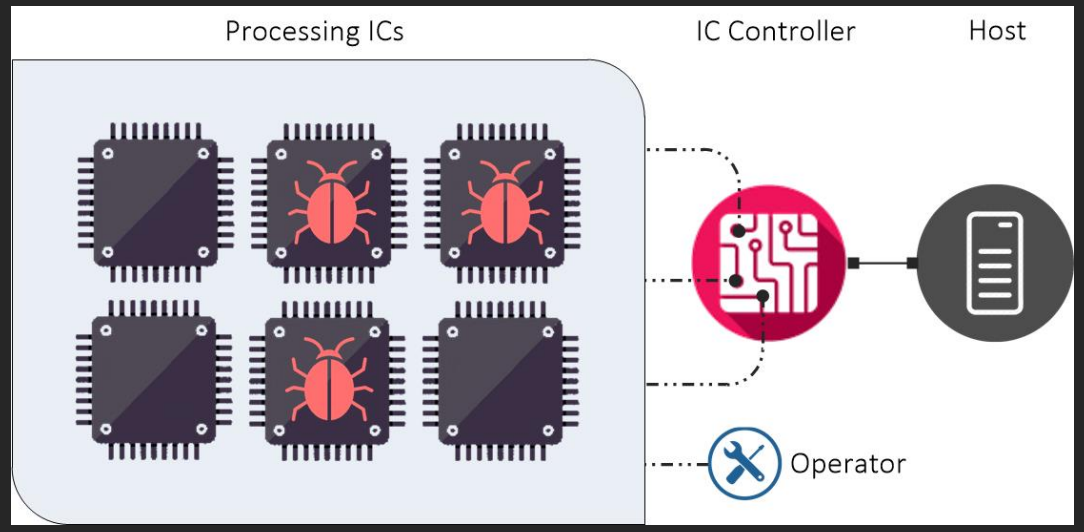
Features

- Tolerates:
  - faulty hardware components
  - multiple backdoored components
  - Colluding adversaries
- Provides resilience
- Tamper-resistant (FIPS-4)
- Easily Programmable (Java variant)

We did it!

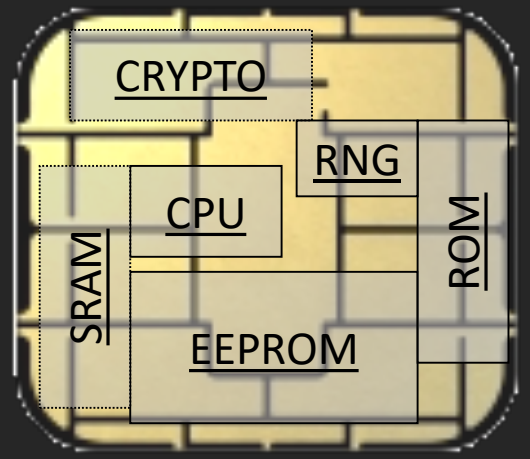
Components

- 120 SmartCards
- Quorums of three cards
- 1.2Mbps dedicated inter-IC buses
- ARTIX FPGA controls the comm. bus
- 1Gbit/s bandwidth for incoming requests



Smart Cards?

- 8-32 bit processor @ 5-20MHz
- Persistent memory 32-150kB (EEPROM)
- Volatile fast RAM, usually <<10kB
- True Random Number Generator
- Cryptographic Coprocessor (3DES,AES,RSA-2048,...)
- Limited attack surface, small trusted computing base



Smart Cards?

Intended for physically unprotected environment

- NIST FIPS140-2 standard, Level 4
- Common Criteria EAL4+/5+

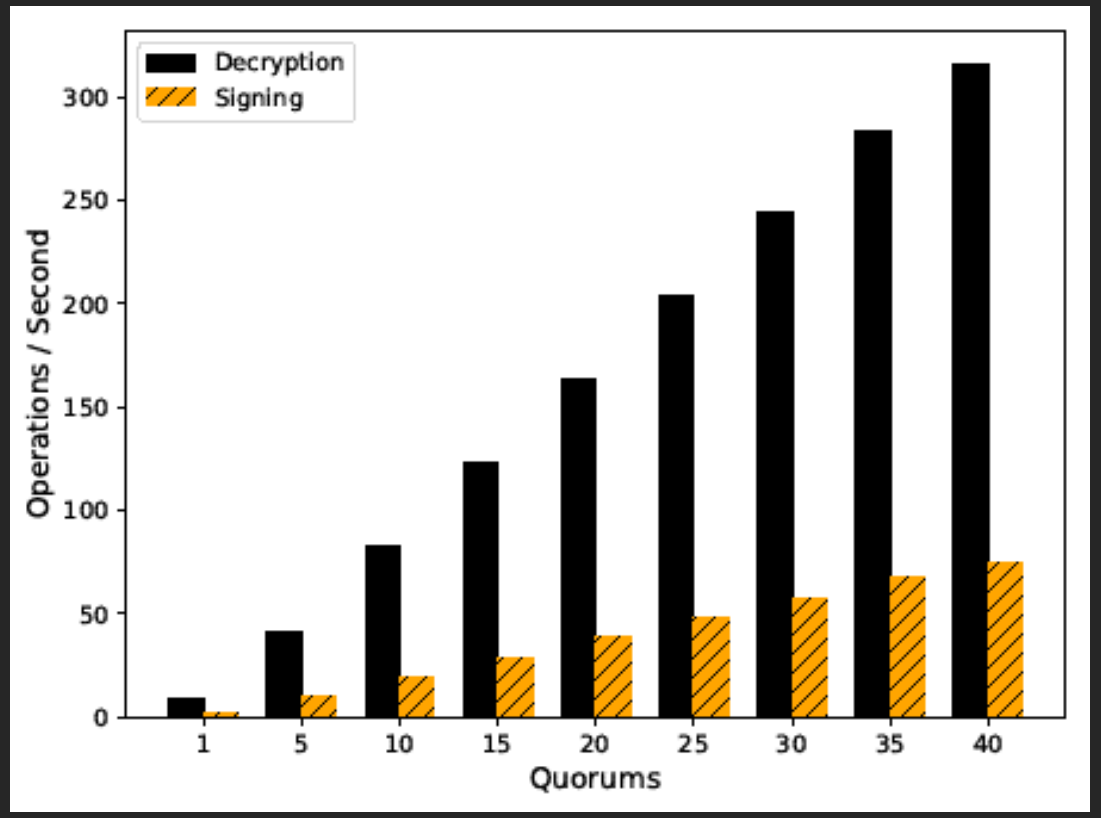
Tamper protection

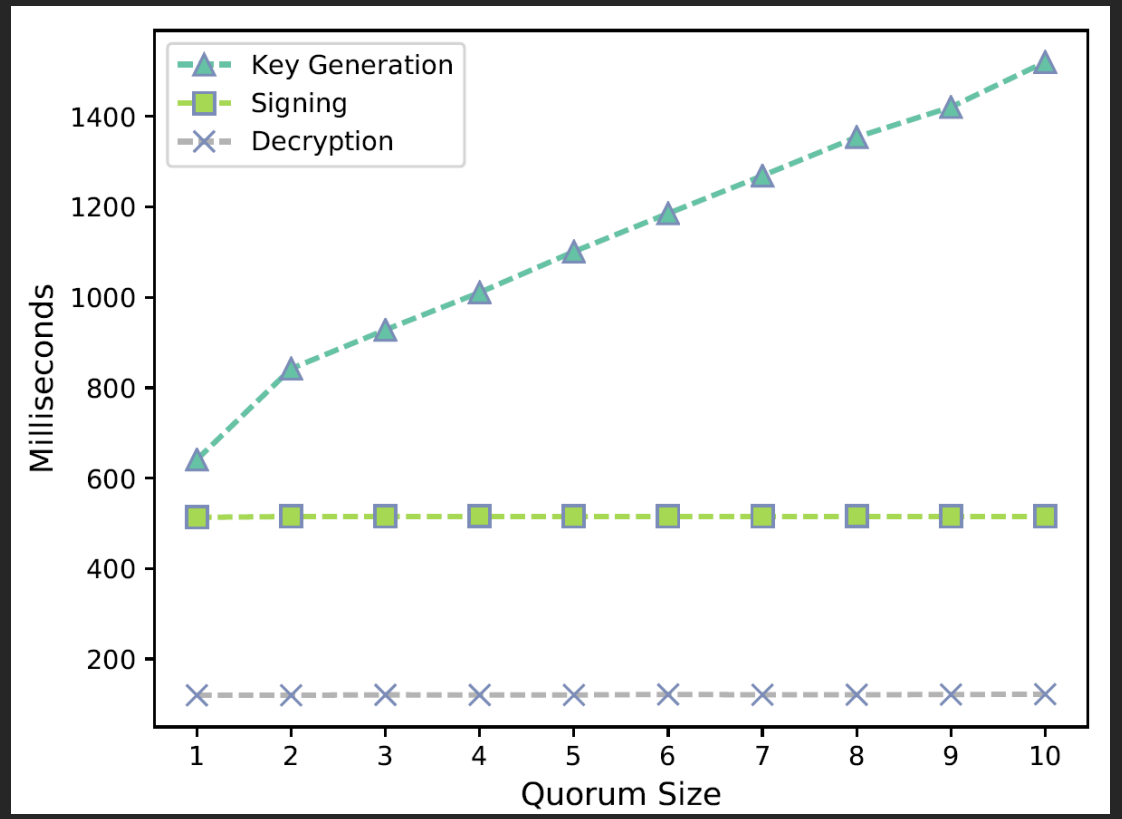
- Tamper-evidence (visible if physically manipulated)
- Tamper-resistance (can withstand physical attack)
- Tamper-response (erase keys…)

Protection against side-channel attacks (power,EM,fault)

Periodic tests of TRNG functionality

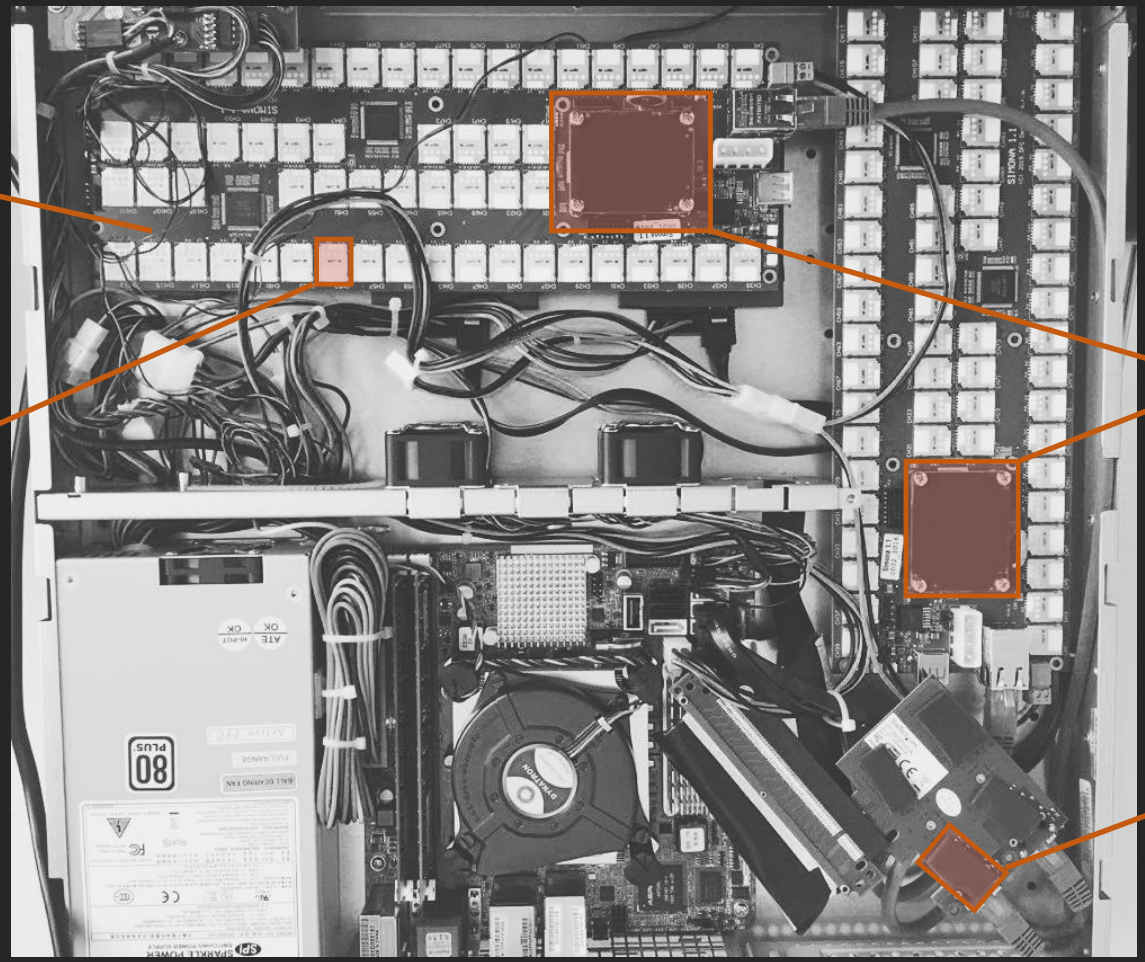
Performance





THE PROTOTYPE

Hardware Pic!

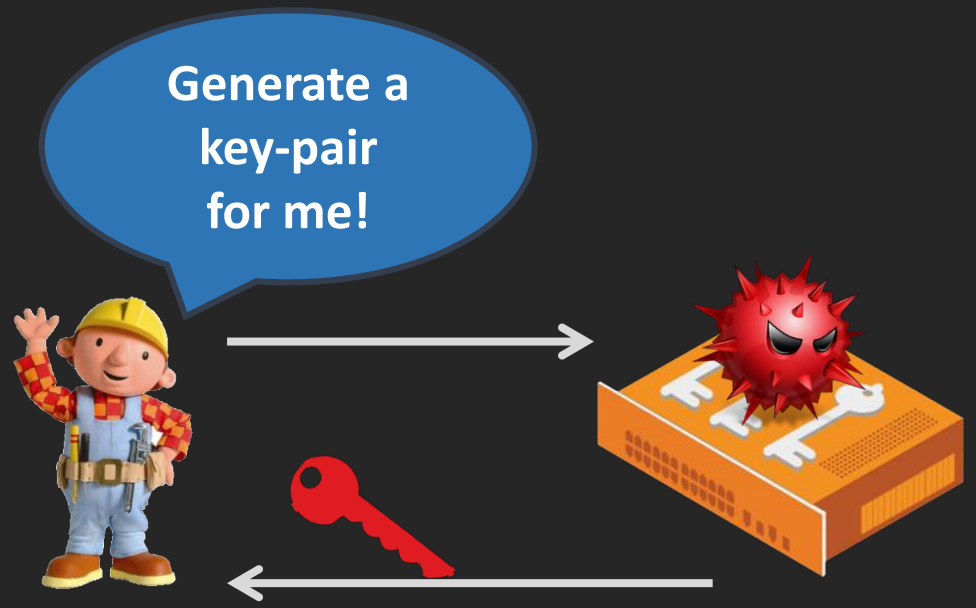


PROTOCOLS

Classic Key Generation

Single IC System

1. Bob asks for new key pair
2. Faulty/Backdoored IC generates key using broken RNG
3. Private Key is “securely” stored
4. Weak public key is returned

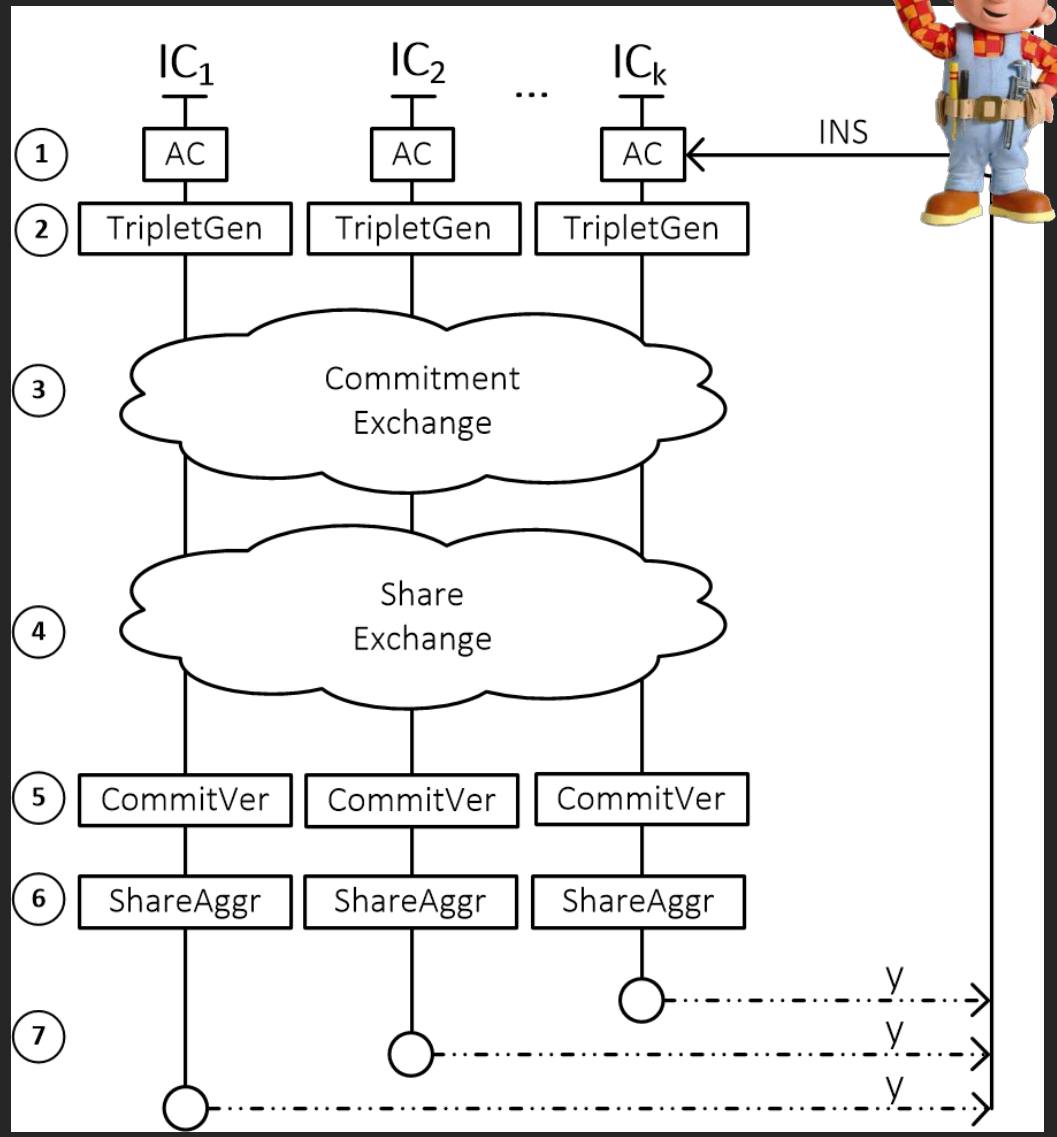


Properties

- Private key never leaves the box
- IC has full access to the private key
- Bob can’t tell if he got a “bad” key

Distributed Key Generation

1. User asks for new key pair
2. ICs generate their key pairs
3. ICs exchange hashes of their shares
4. ICs reveal their shares
5. ICs verify each others' shares
6. ICs compute the common public key
7. ICs return the common public keys
8. Bob verifies that all the keys are same

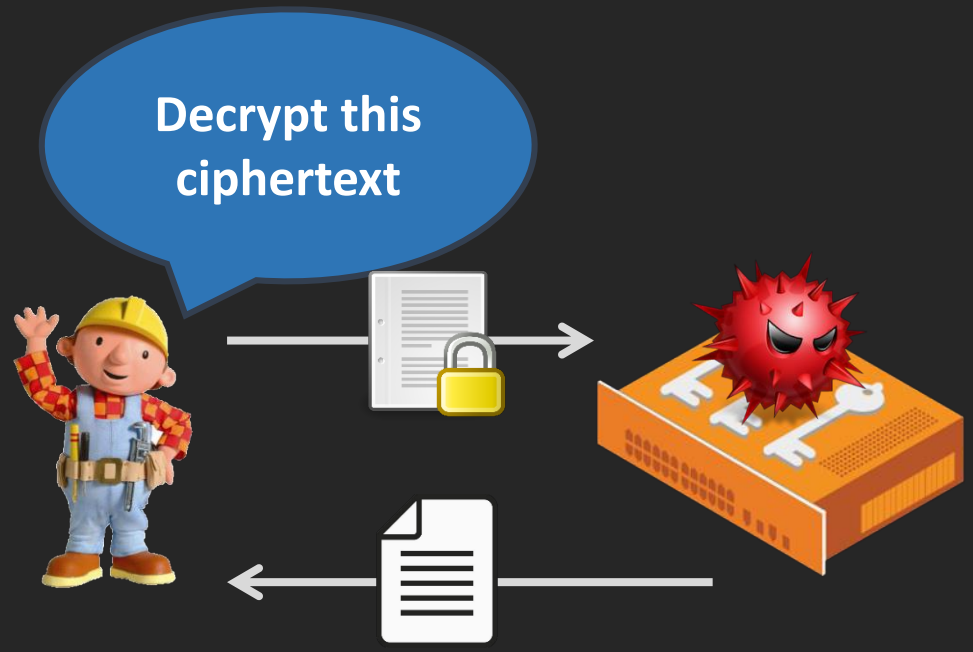


DEMO

Classic Decryption

Single IC System

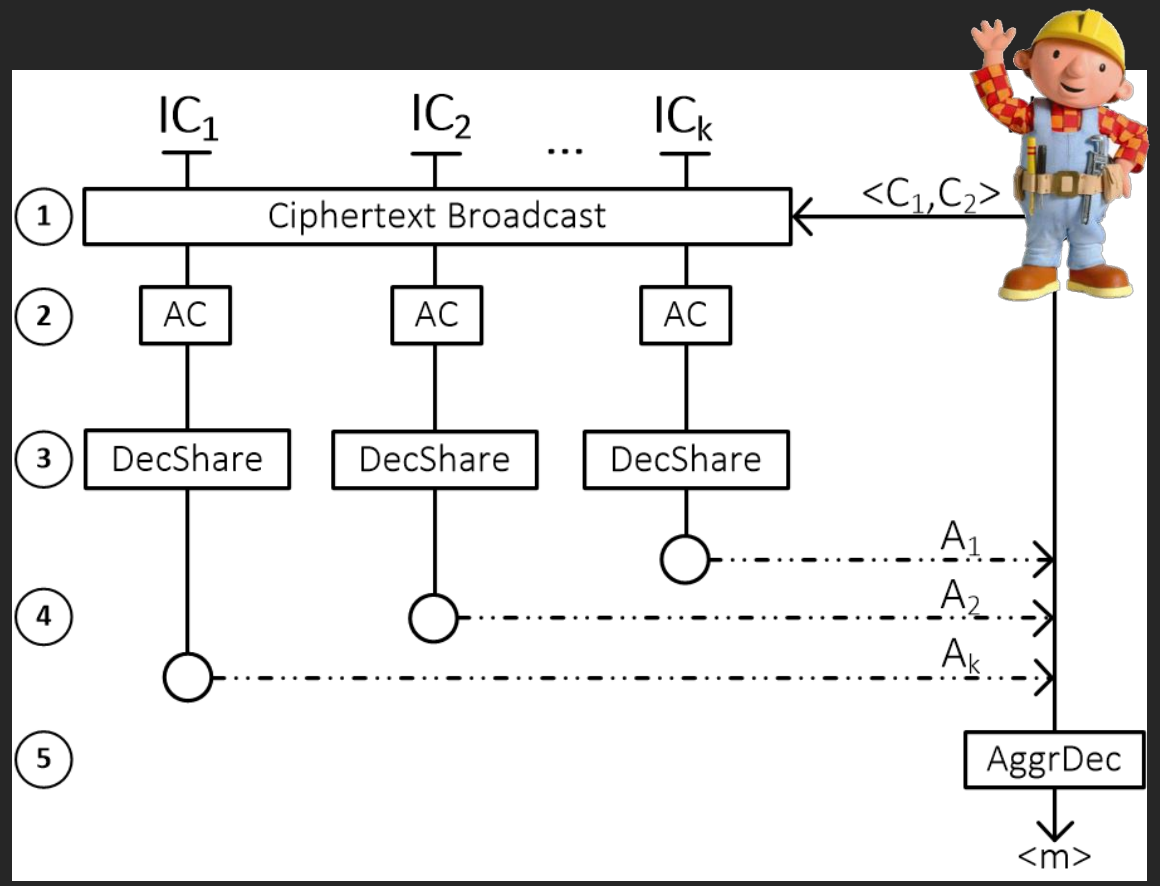
1. Bob asks for ciphertext decryption
2. Faulty/Backdoored IC decrypts ciphertext
3. Bob retrieves plaintext



The IC need full access to the private key to be able to decrypt ciphertexts.

Distributed Decryption

1. Bob asks for ciphertext decryption
2. His authorization is verified
3. ICs compute their decryption shares
4. Bob receives the shares and combines them to retrieve the ciphertext



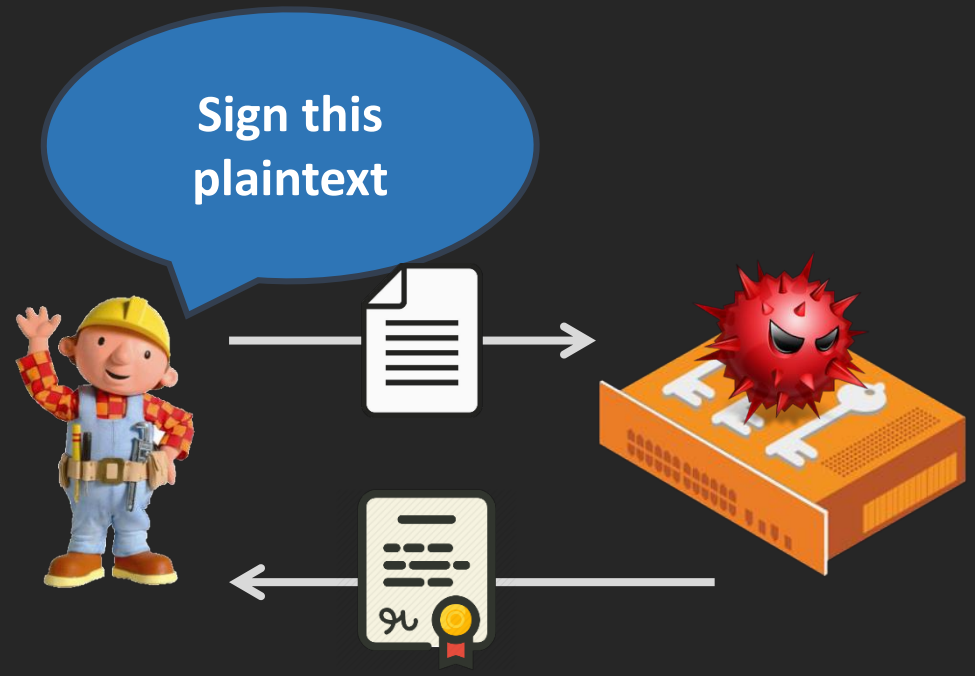
Properties

- No single authority gains access to the full private key for the decryption
- If one IC abstains, decryption fails

Classic Signing

Single IC System

1. Bob asks for document signing
2. Faulty/Backdoored IC signs the plaintext and retains contents
3. Bob retrieves signature



The IC need full access to the private key to be able to sign plaintexts.

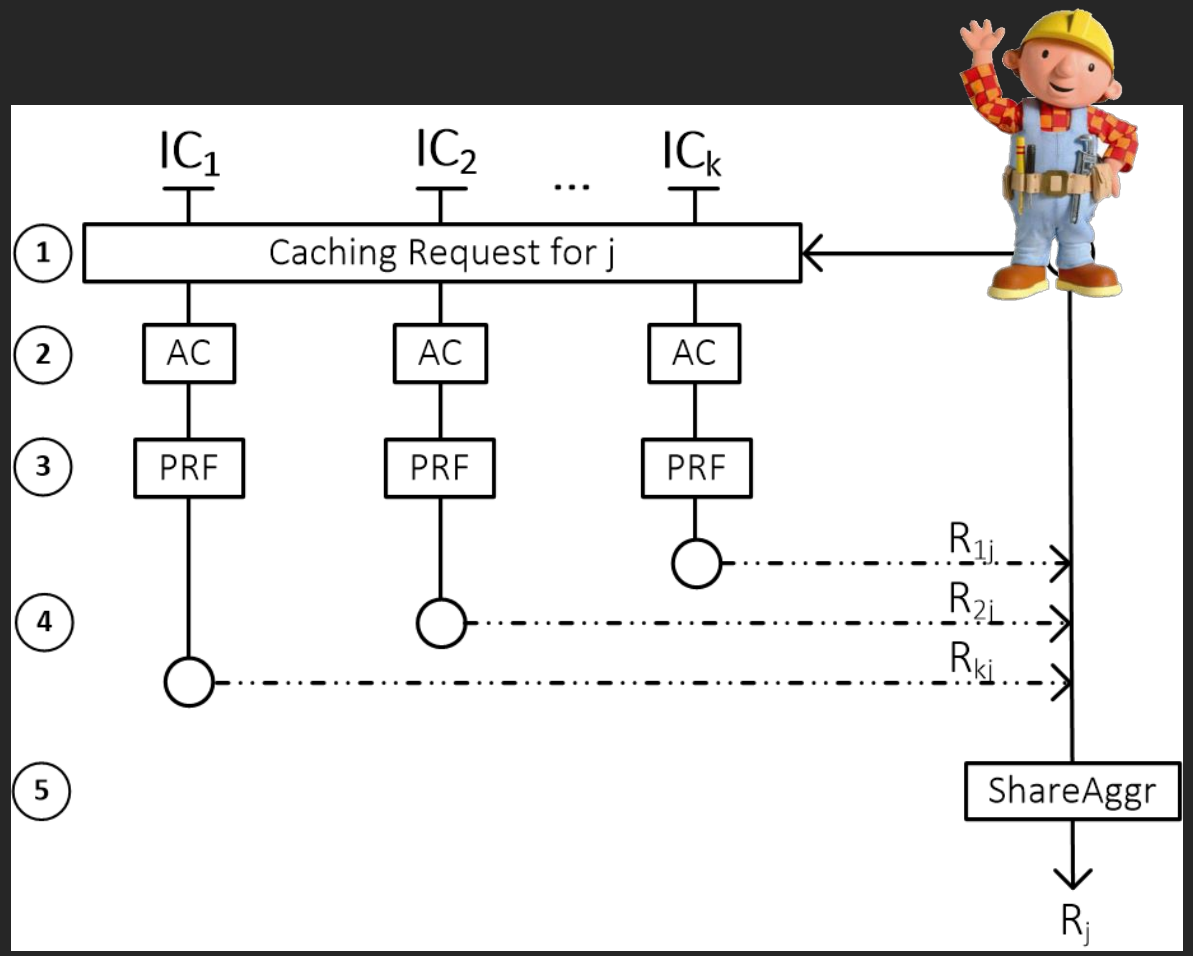
Distributed Signing I

Caching

1. Bob sends a caching request
2. The ICs verify Bob's authorization
3. Generate a random group element based on j
4. Bob sums the random elements

Properties

- Caching for thousands of rounds (j)
- Bob stores R_j



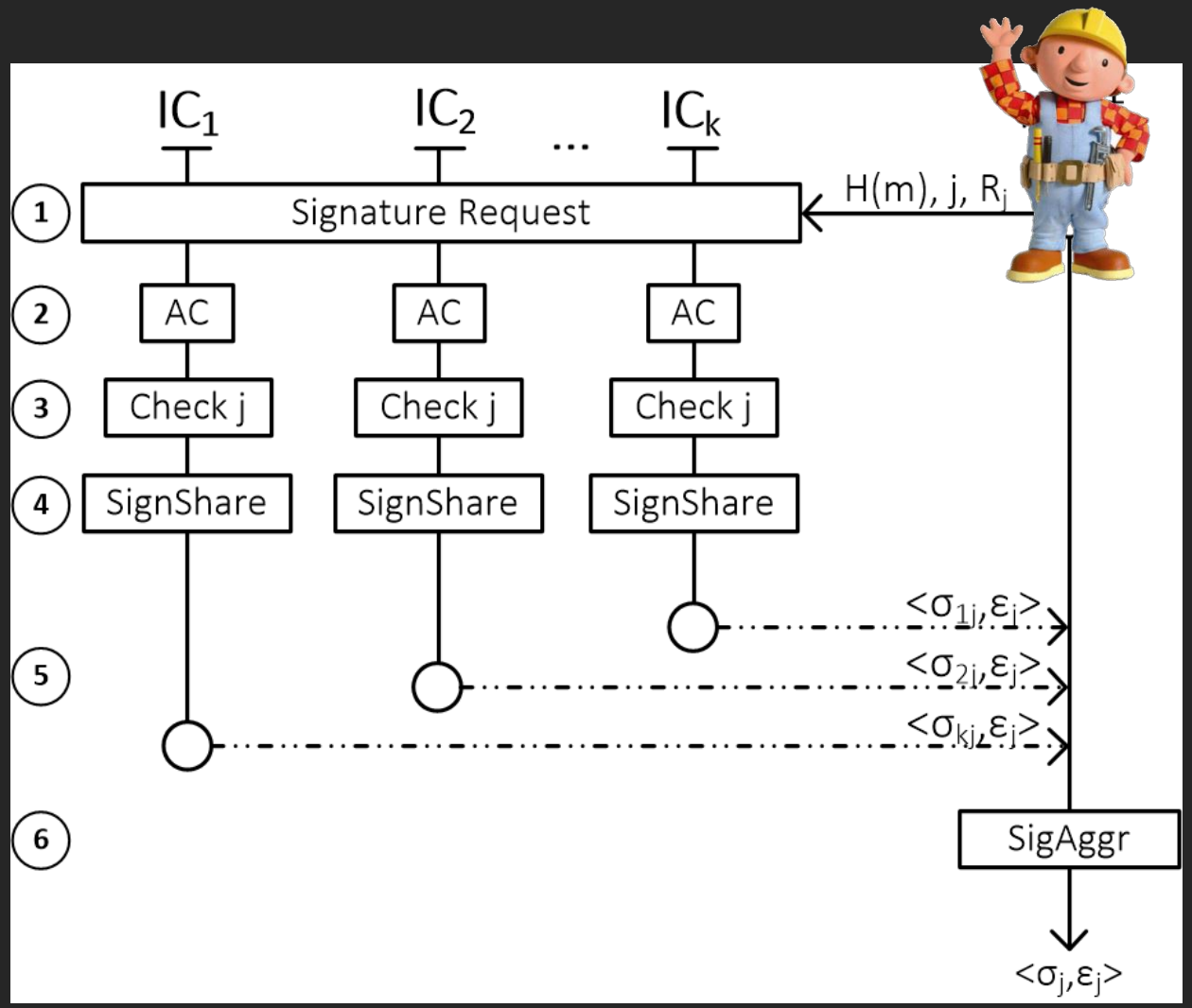
Distributed Signing II

Signing

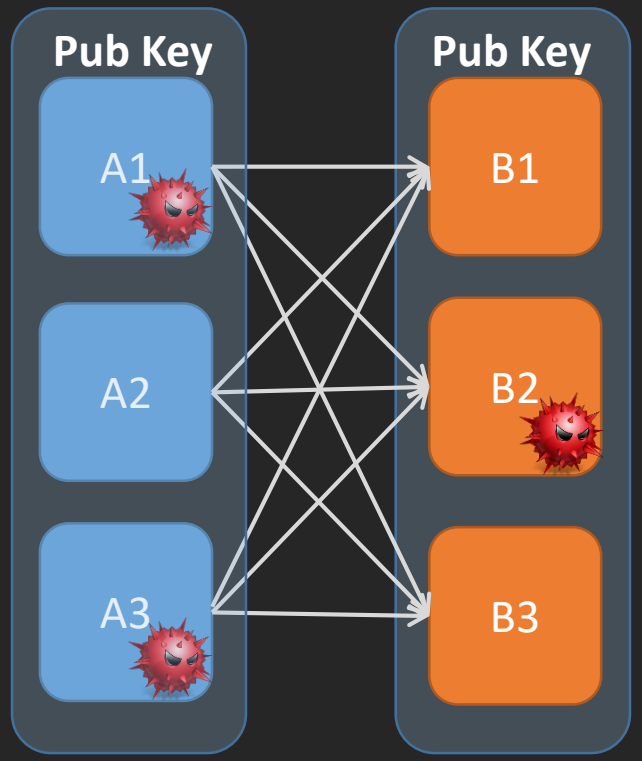
1. Bob asks for document signing & sends R_j, j, and the hash of m
2. ICs verify his authorization
3. ICs check if j has been used again
4. ICs compute their signature share
5. Bob sums all signature shares

Properties

- All ICs must participate
- Significant speed up with caching



Key Propagation



1. Quorum A generates a public key
2. Then each IC in A splits its private key in three shares and sends them to B1, B2, B3
3. Each IC in B receives shares from A1, A2, A3
4. Each IC in B combines the 3 shares and retrieves its private key

The full public keys of A and B are the same!

Mutual Distrust & Hardware Security

So far our argument was:

"We can guarantee security if t*here is at least one honest IC that doesn't incorporate a backdoor or an error.*"

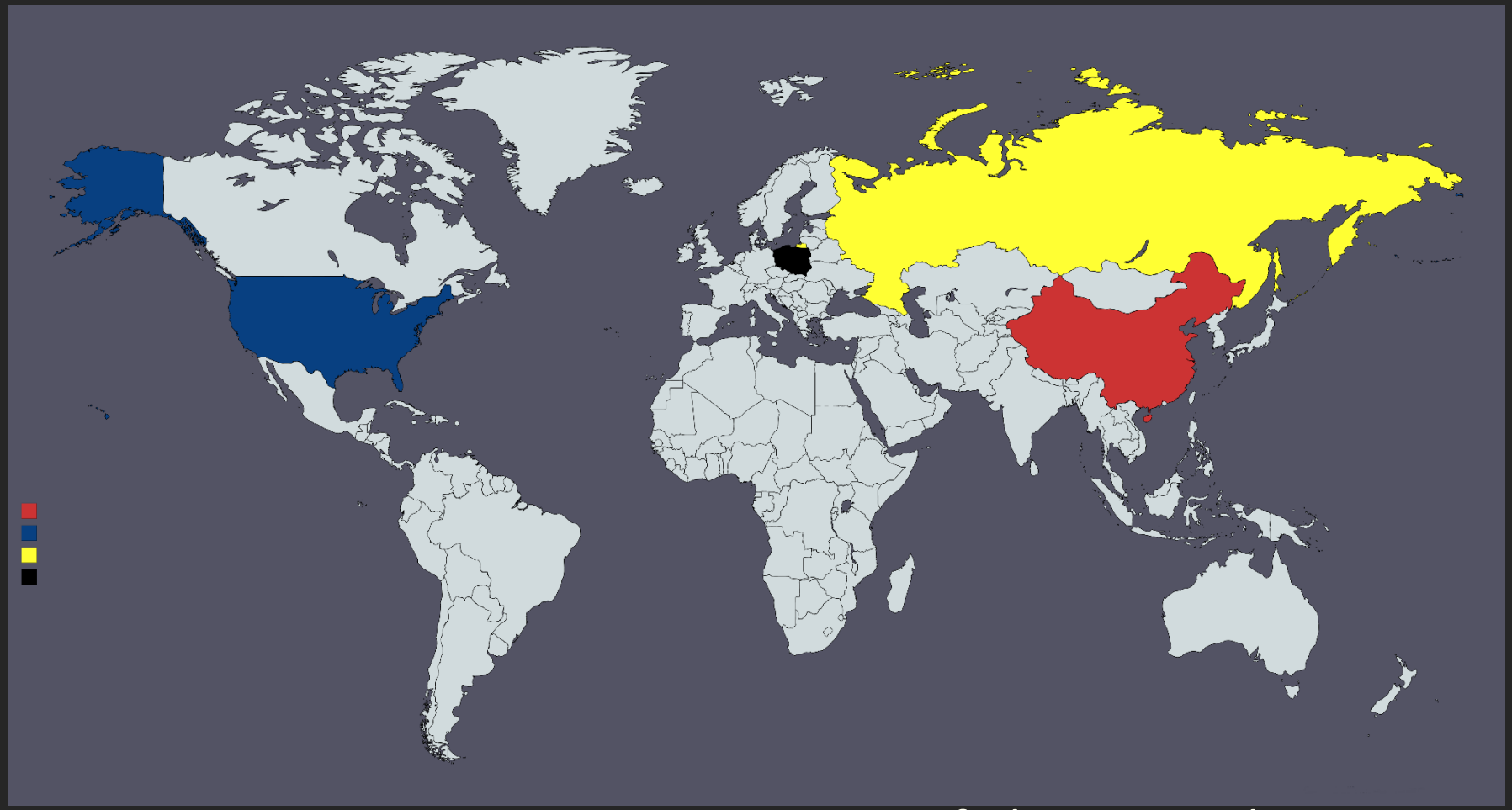
However, when using COTS components it can be hard to even trust that a single IC is not backdoored.

Mutual Distrust & Hardware Trojans

Government-level adversaries are unlikely to collude and/or share their backdoor details. Hence, we can reform our argument to be:

"We can guarantee security if t*here is at least one non-colluding IC, even if it is untrusted.*"

Mutual Distrust & Hardware Trojans

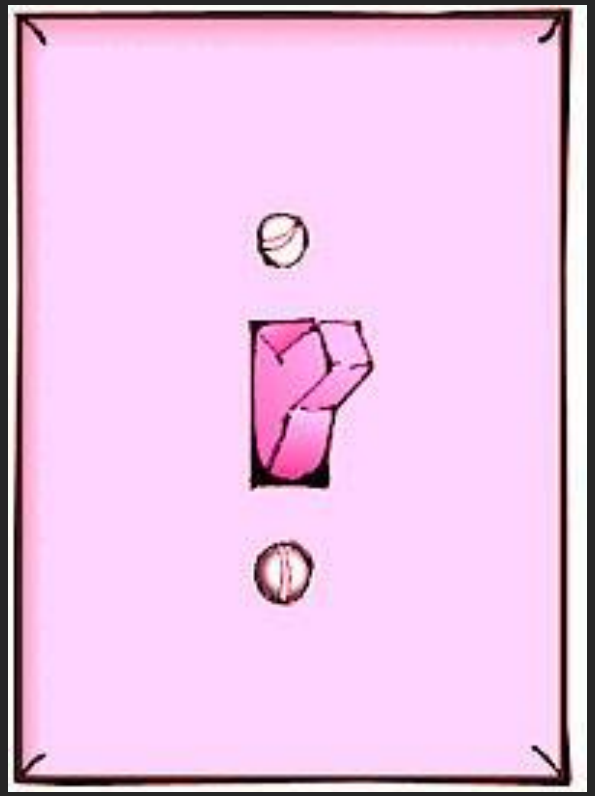


We can guarantee security if t*here is at least one non-colluding IC, even if it is untrusted.*

A Kill Switch?

The Pentagon is worried that "backdoors" in computer processors might leave the American military vulnerable to an instant electronic shut-down. Those fears only grew, after an Israeli strike on an alleged nuclear facility in Syria. Many speculated that Syrian air defenses had been sabotaged by chips with a built-in 'kill switch" – commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden "backdoor" inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips' function and temporarily blocked the radar."

wired.com



A Kill Switch?

That same basic scenario is cropping up more frequently lately, and not just in the Middle East, where conspiracy theories abound. According to a U.S. defense contractor who spoke on condition of anonymity, a "European chip maker" recently built into its microprocessors a kill switch that could be accessed remotely. French defense contractors have used the chips in military equipment, the contractor told *IEEE Spectrum*. If in the future the equipment fell into hostile hands, "the French wanted a way to disable that circuit," he said. *Spectrum* could not confirm this account independently, but spirited discussion about it among researchers and another defense contractor last summer at a military research conference reveals a lot about the fever dreams plaguing the U.S. Department of Defense (DOD).

IEEE Spectrum

Conclusions & Future

New architecture

- Decent performance & Small overhead compared to a single IC
- Existing malicious insertion countermeasure are very welcome!
- Suitable for commercial-off-the-shelf components
- Faulty hardware is no longer an end-game but a manageable problem

Future

- Distributed Symmetric crypto? SSL-accelerators etc
- Does it transfer to a more generic architecture?

Q & A