

Hardware Security Attacks and Defense in Satellite Communication

Marc Witteman
Senior Director, Keysight Device Security

Battlefield security challenges in satellite communication

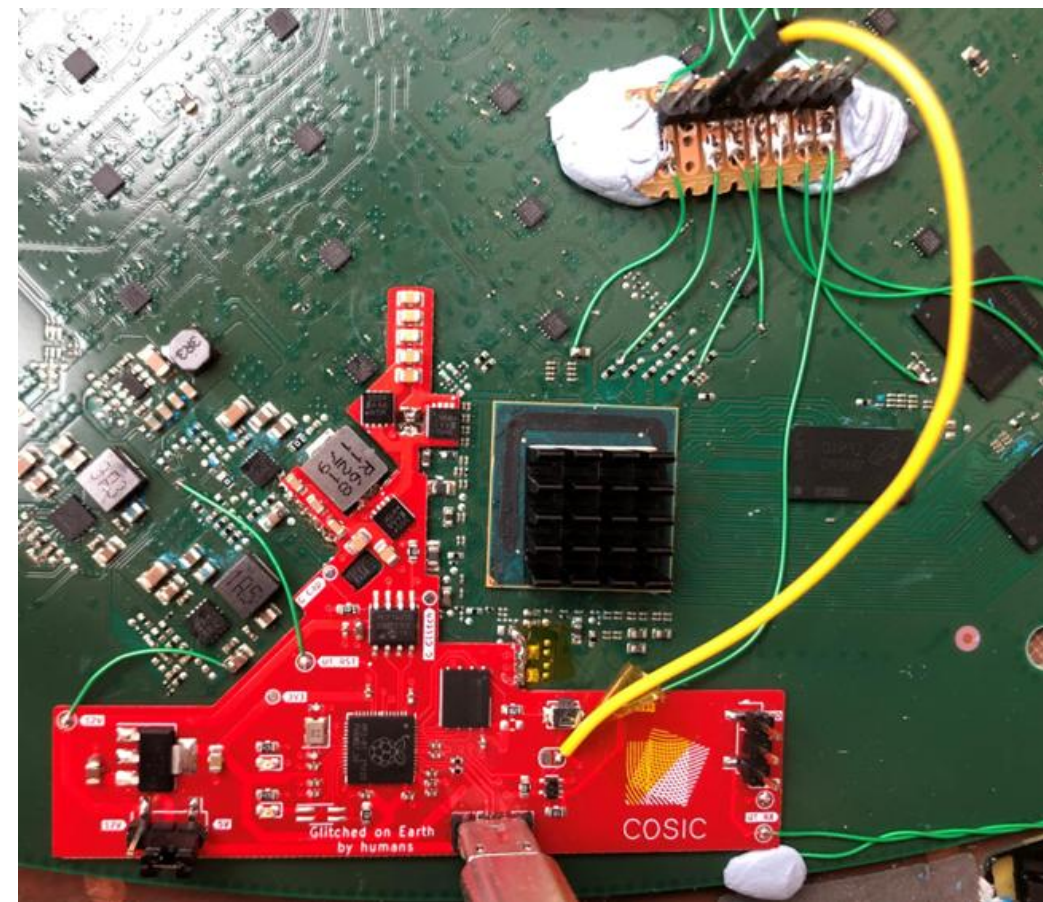
How do you stop adversarial drones using satellite communication in your airspace?



Practical attack on Starlink terminal

Work by Lennert Wouters from KU Leuven

- Extracted firmware
- Used Side Channel Analysis and Fault Injection
- Broke secure boot
- Could load arbitrary code
- But did not break the authentication mechanism and could not clone terminals



Which component in the Starlink terminal had not been broken?

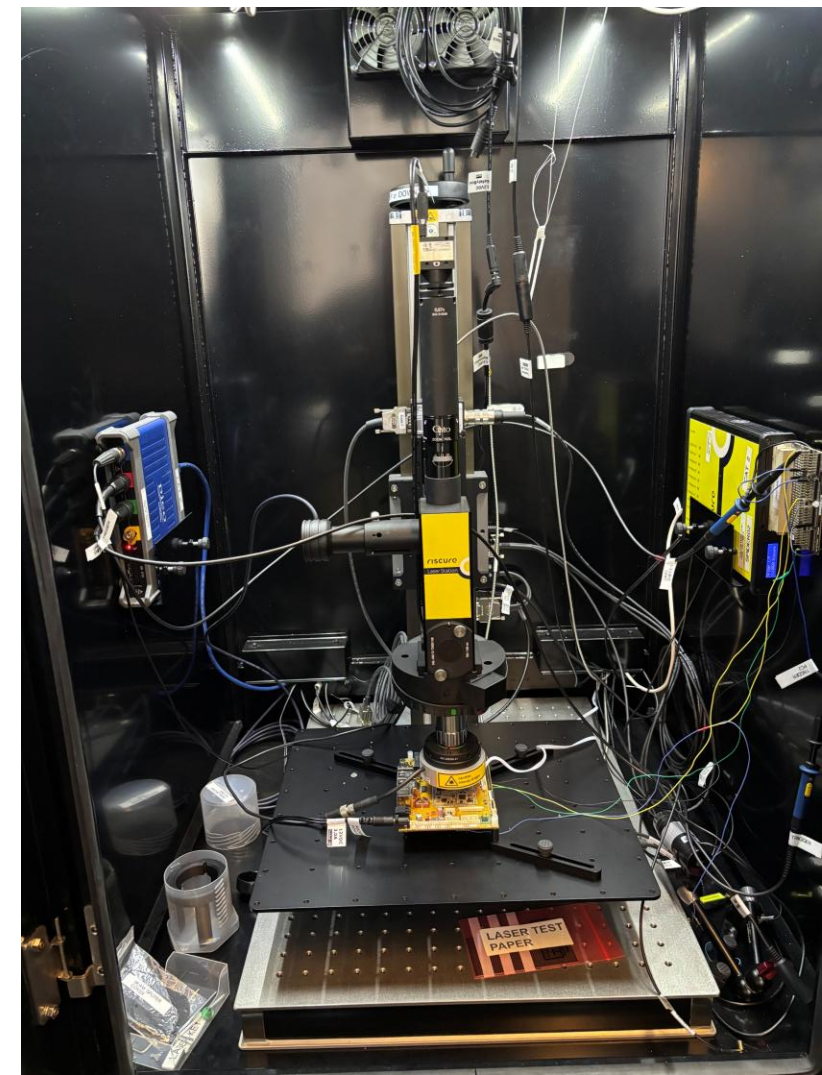


- A = System on Chip
- B = Secure Element ➡ **A certified chip with advanced security protection**
- C = Persistent Memory Can we expect this chip to remain secure going forward?
- D = Volatile Memory

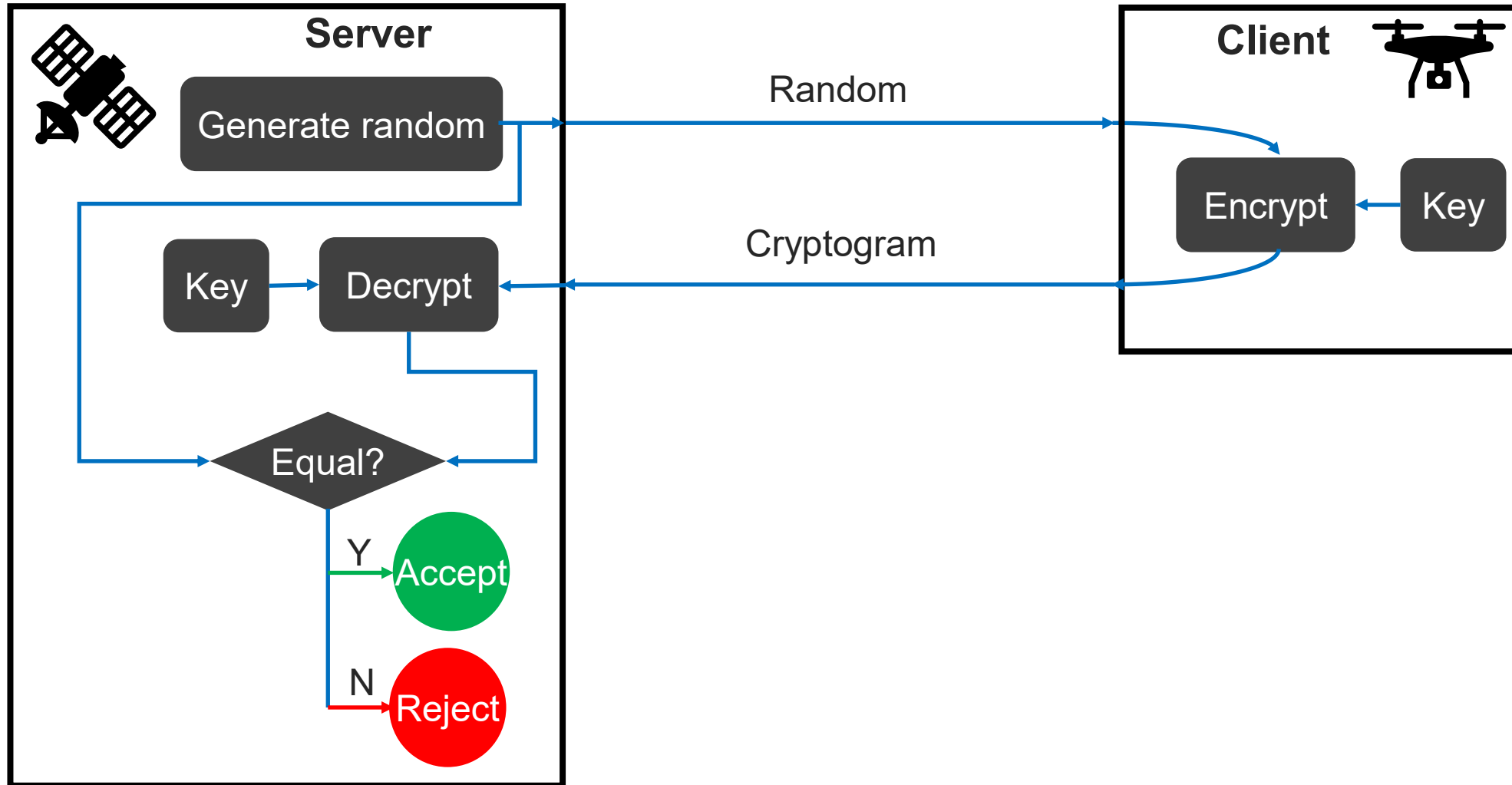
How are Secure Elements certified?



- Risk-based testing process originating from payment card security needs
- Certification done by professional labs that spend several months collecting evidence
- Testing includes hardware testing such as Side Channel Analysis and Fault Injection
- Products typically pass when breaking them takes more than a few months
 - Enough to stop the business case of a common criminal
 - Is it enough to stop organized crime / terrorism / nation state actors?

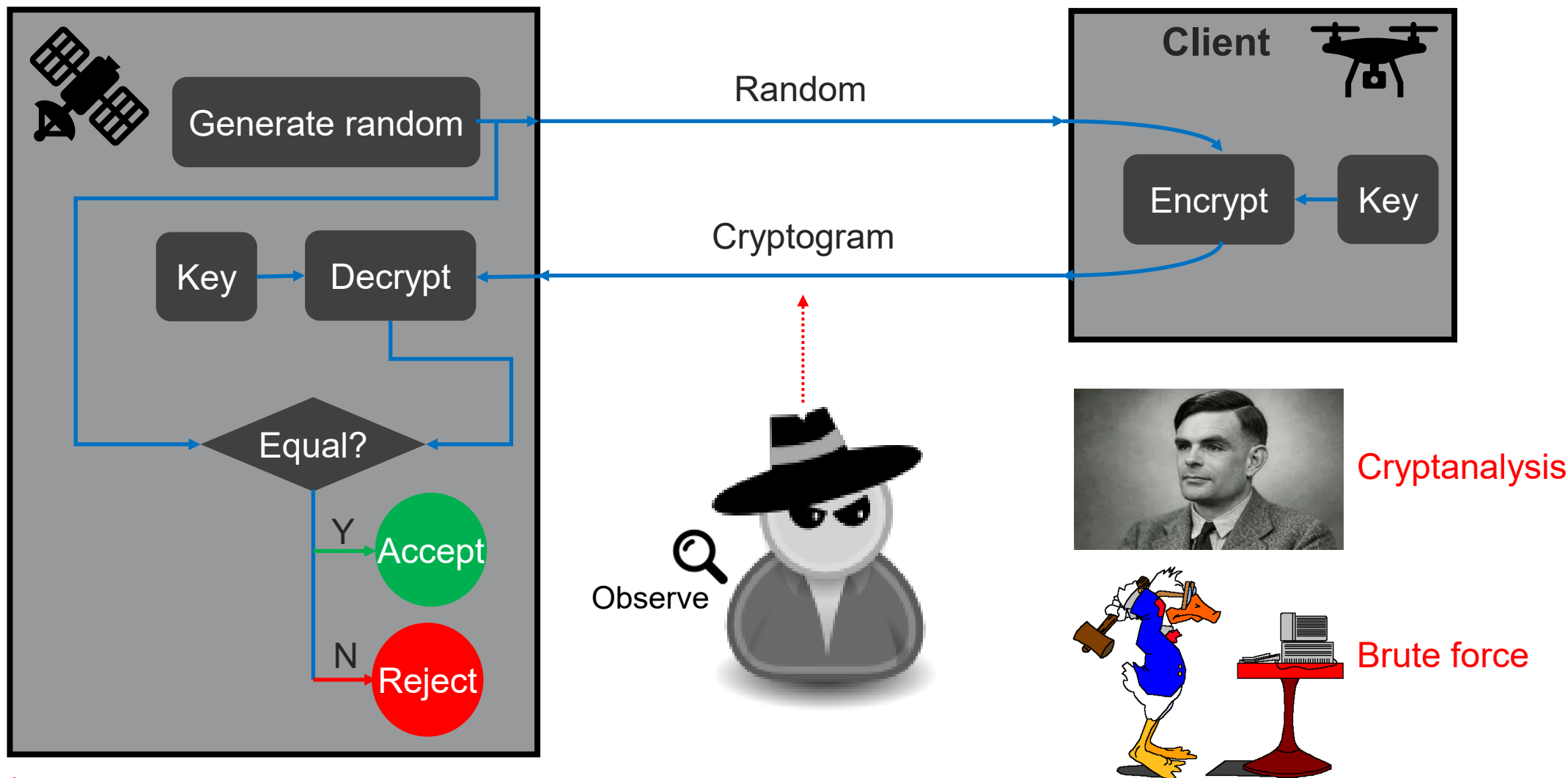


Cryptographic authentication



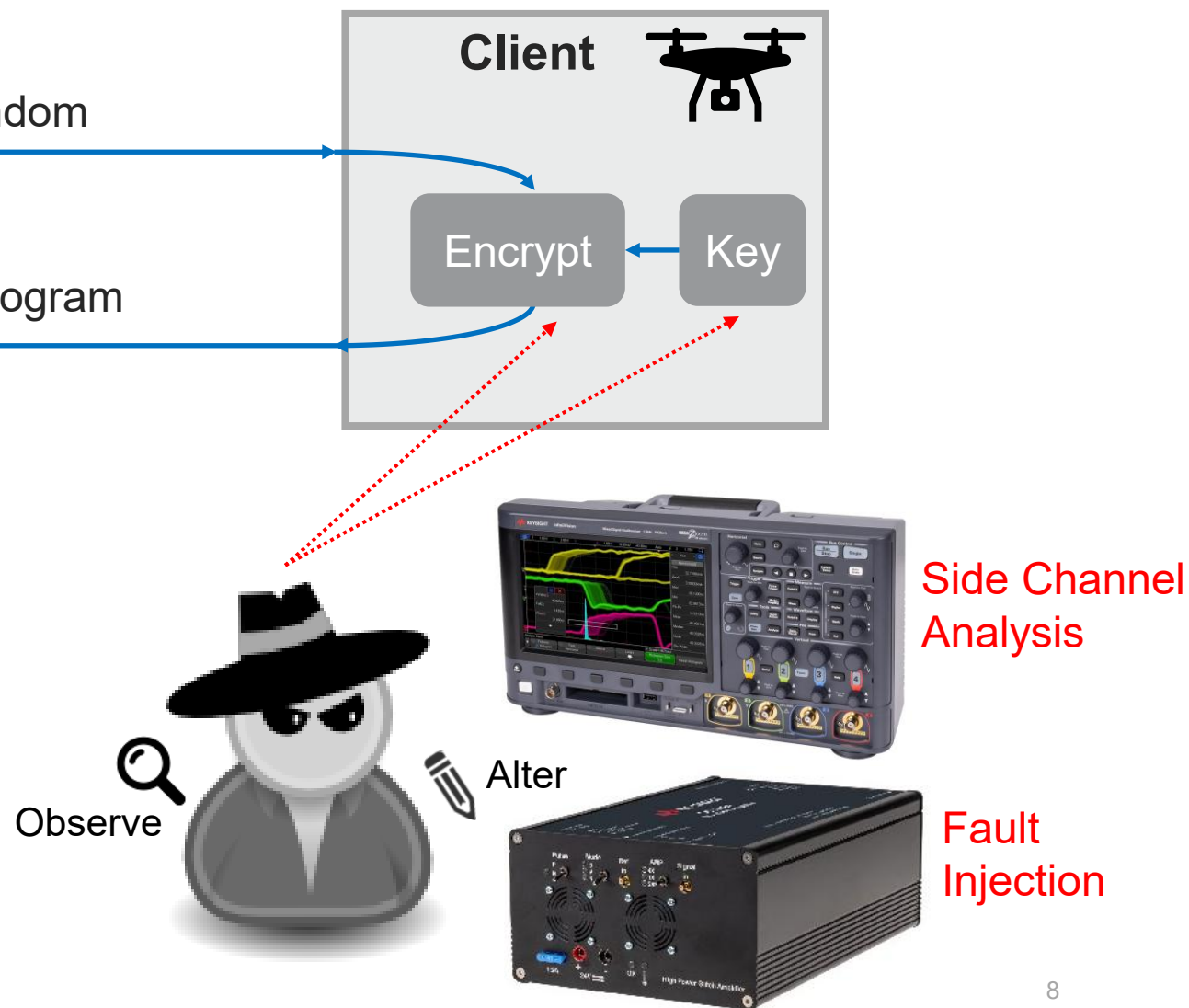
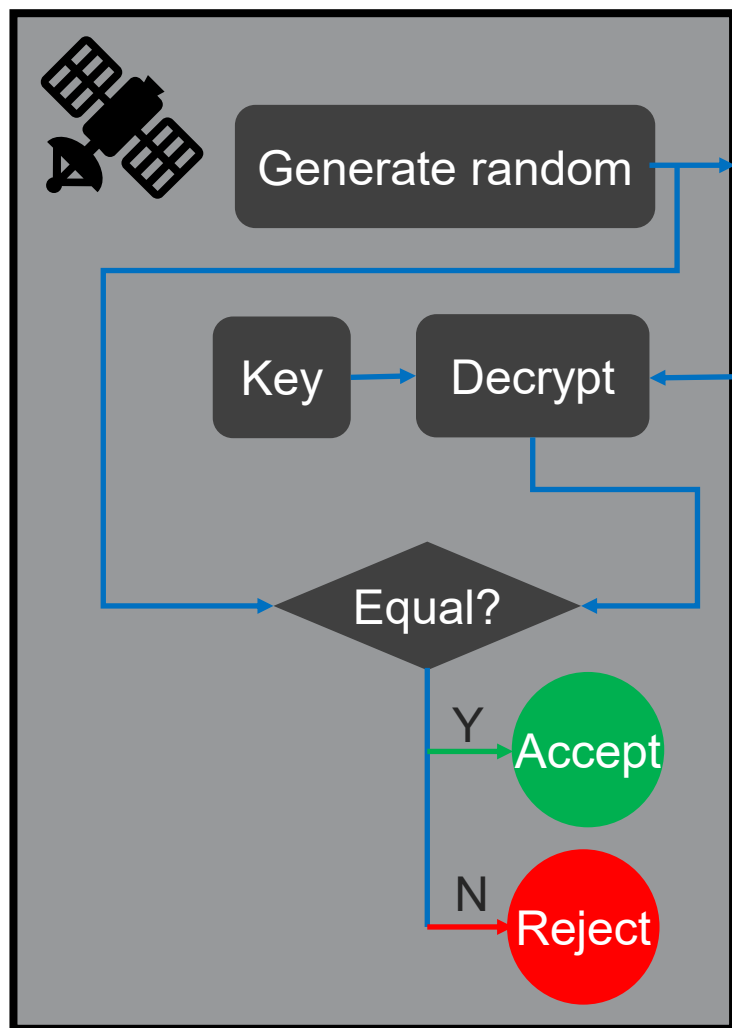
Traditional Cryptographic communication attacks:

Black Box

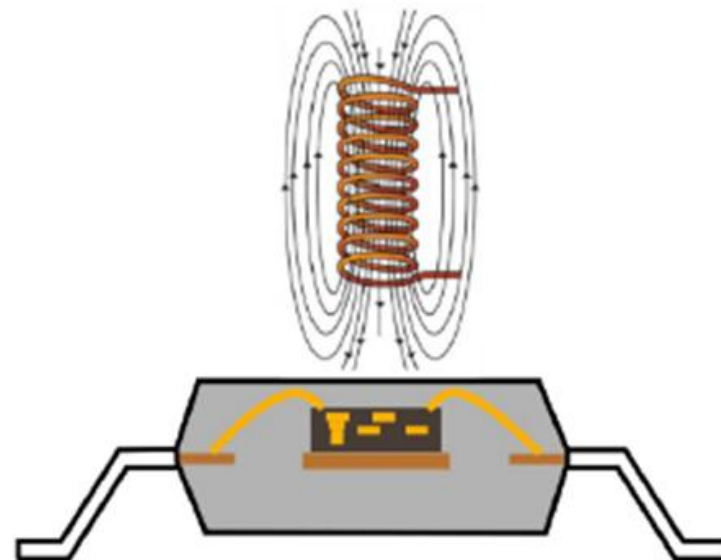
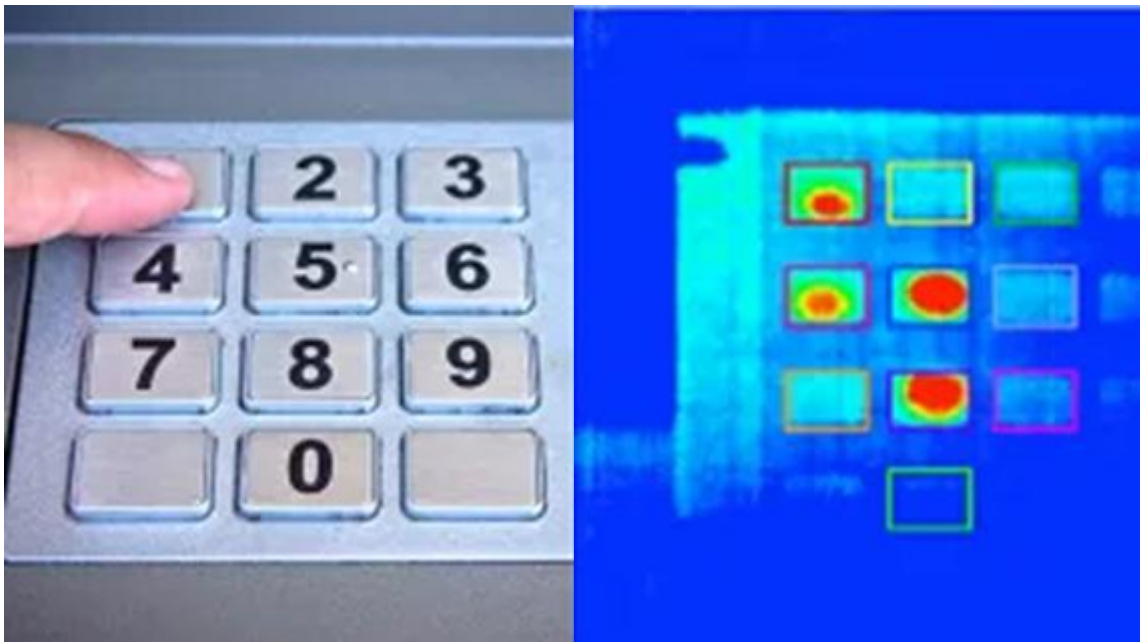


Modern Cryptographic implementation attacks:

Gray Box



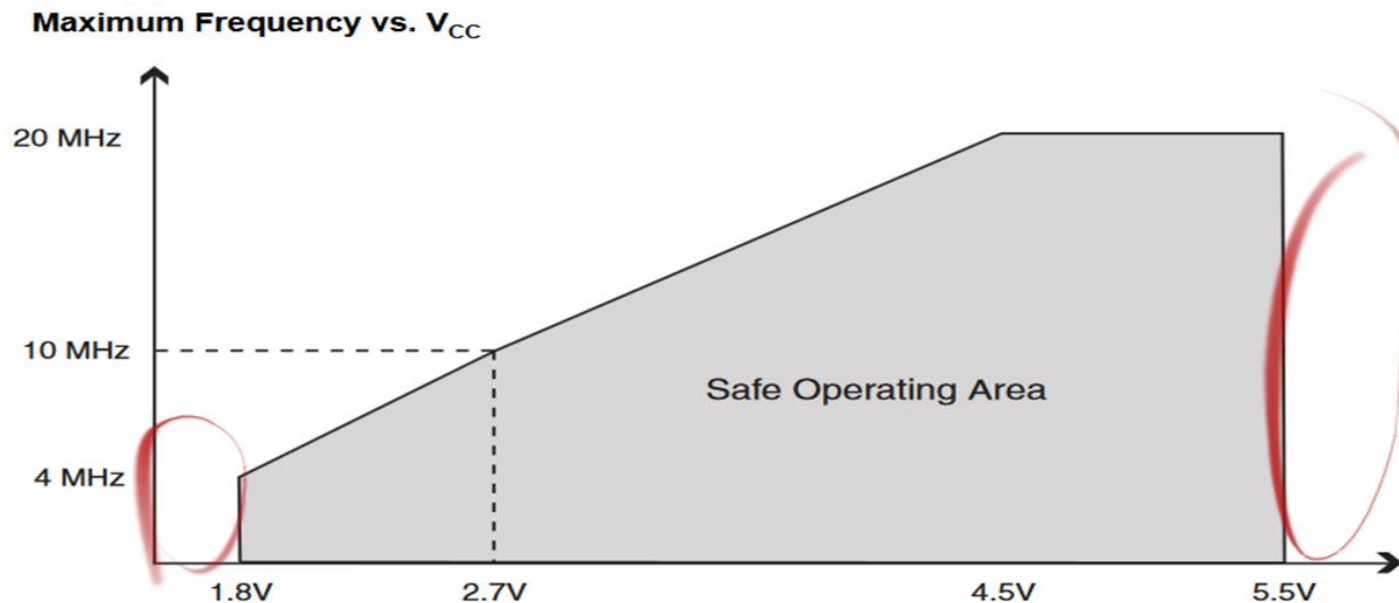
Side Channel Analysis: reading the signs



Side channels can reveal secrets



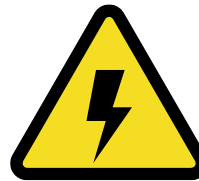
Fault Injection: overriding the code



Digital chips need environmental parameters to be within safe bounds

Behavior can be changed by short glitches

Faults can be injected through:



voltage



clock



EM

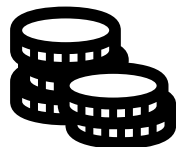


laser

or

Can hardware attacks be mitigated?

Yes! but it comes at a cost



- Development requires more expertise and time



- Bigger chip area needed



- Performance slowdown



- Power drain

In practice vendors will make a threat analysis and design a mix of countermeasures balancing security need vs cost

Vendors who work with a security evaluation lab to assess the strength of their countermeasures are more likely to find a cost-effective solution



Is terminal/drone cloning a realistic threat?

Look at the example business case

Smuggling

- Acquire terminal: \$ 10K



Cloning

- One time:
 - Develop key extraction procedure: \$1M
 - Develop programmable terminal: \$1M
- Recurring: produce terminal: \$1K

Cloning is financially viable when more than 223 drones are needed

Conclusion

- Armies want to use Starlink on the battlefield, but terminal cloning is not trivial
- Hardware attacks are a realistic threat and enable cloning
- Commercial chip security certification anticipates a modestly funded attacker that may not be realistic for critical infrastructure or military applications
- National security suggests the need for stronger hardware security and compliance procedures

Thank you

Marc.Wittelman@keysight.com

Backup slides