Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Optimal signed-encrypted Messages

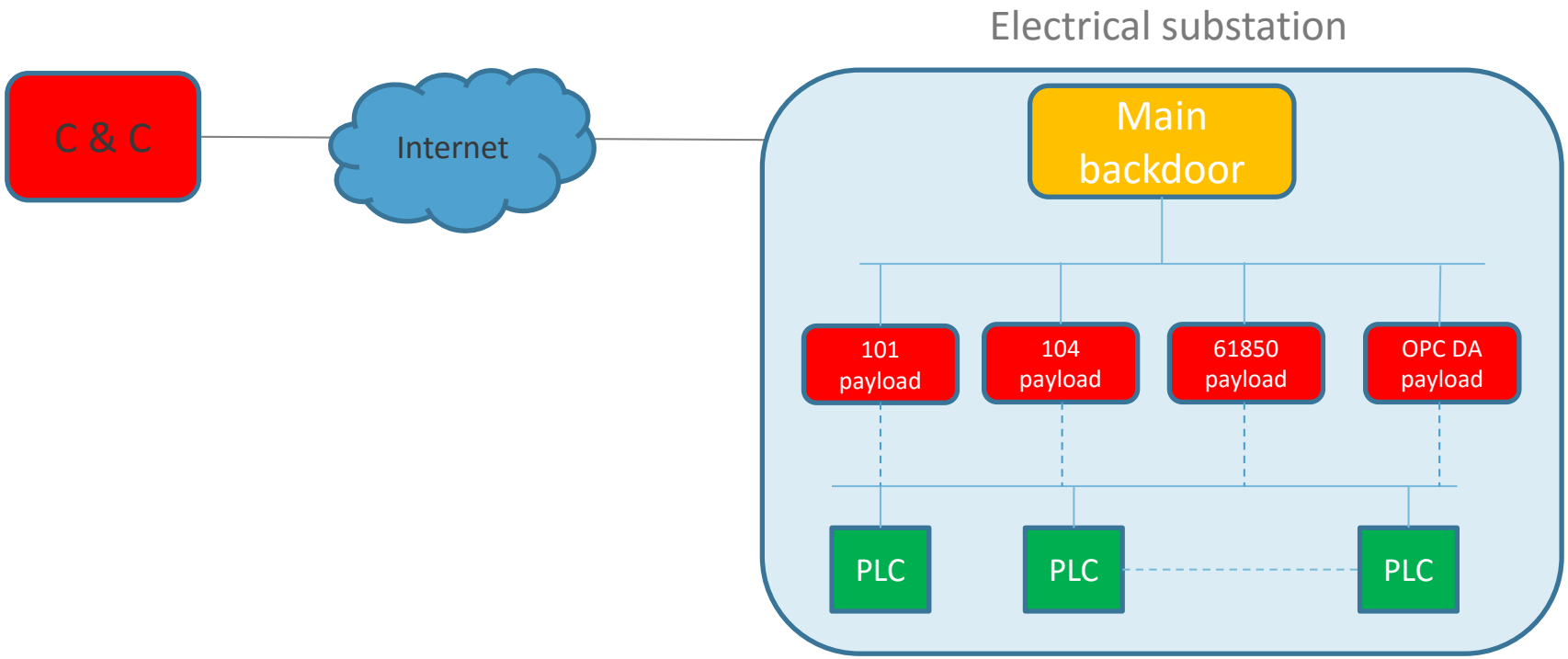
Hes·so
Haute École Spécialisée de Suisse occidentale
Fachhochschule Westschweiz

jean-roland.schuler@hefr.ch

Industrial Attacks 1: Industroyer

Industroyer or CrashOverRide

- It is a new threat for industrial control systems
- It was carried out against the Ukrainian Electric power grid in December 2016. For 1h tens of thousands of consumers had no electricity.



Industrial attacks 2: Dragonfly

[https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html]
[https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group]

2017: The Symantec company has many computers around the world. These computers analyze a huge quantity of messages. Symantec has found that since the beginning of this year, the hacking group Dragonfly has infiltrated US, Turkey and Swiss electrical companies

- It seems that currently the main goals of this infiltration are to map out the computer network of these companies. No doubt, in order to attack them later.
- In order to attack a company, DragonFly uses mainly these techniques:
  - Spear phishing Emails: These fraudulent emails are sent to specific persons or companies and the content appears realistic
  - Trojan Softwares: These malwares are inside known programs
  - Watering Holes Website: The hackers infect sites frequently used by the victim. The victim goes to the infected sites and a malware can be installed on the victim's computer.

Industrial attacks 3

[http://time.com/4270728/iran-cyber-attack-dam-fbi/]

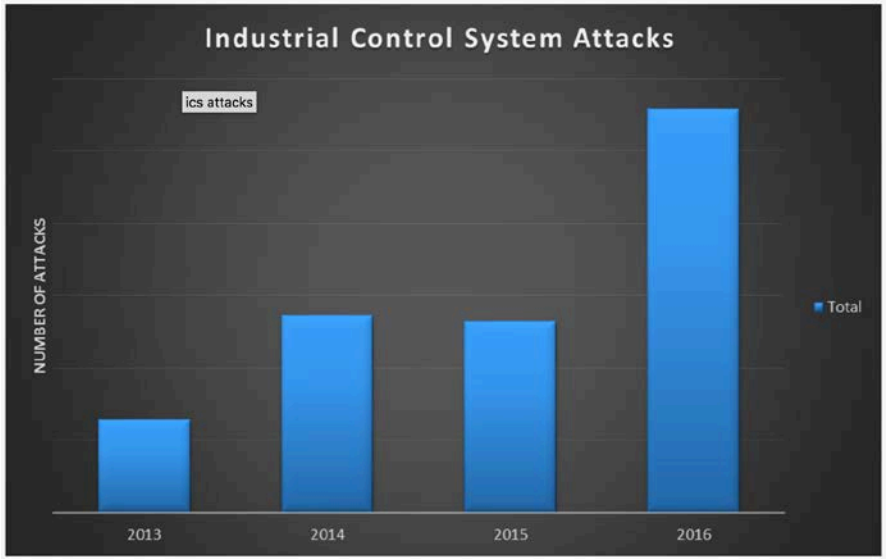
Example: Dam hacked

- In March 2016, the U.S. Justice Department claimed that Iran had attacked U.S. infrastructure by infiltrating the industrial controls of a dam in Rye Brook, New York.

Industrial attacks 4

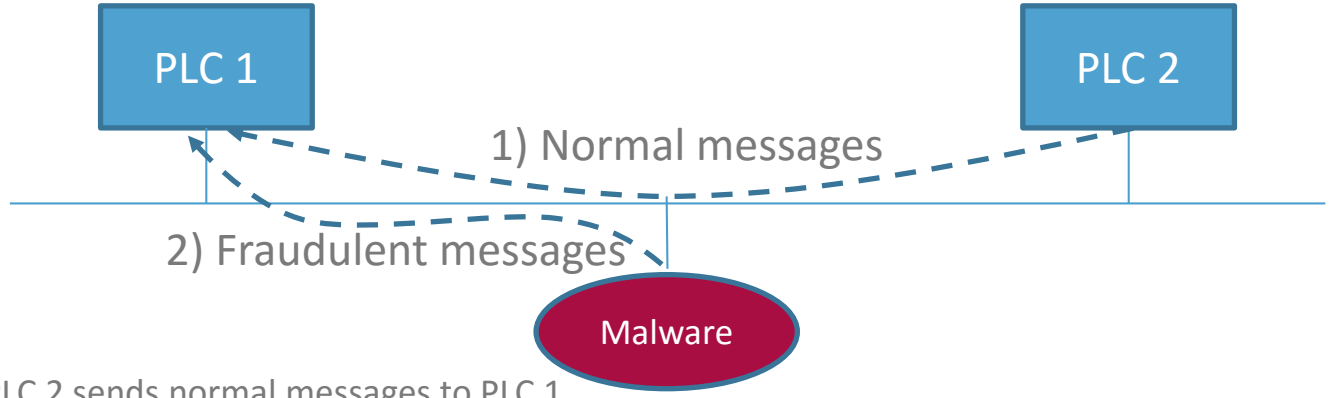
https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/]

Attack numbers against Industrial systems



- Since the malware stuxnet in 2010, there have been many other attacks against industrial systems.
- It is mandatory to incorporate security into the industrial systems and, if it is possible, right from the beginning of a new development

Main problems of the industrial protocols



1) The PLC 2 sends normal messages to PLC 1
2) The malware sends fraudulent messages to PLC 1
3) After theses fraudulent messages, the PCL 1 has a bad behavior

Main problems

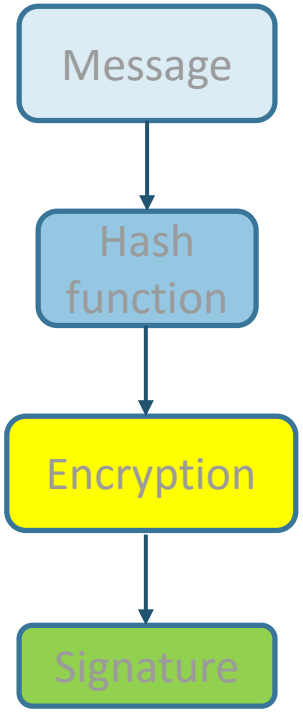
- Generally the industrial protocols don't include the security
- The messages are not authenticated and/or encrypted
- This problem can be solved with the use of digital signature and encryption of each message

Challenges

- Cryptographic algorithms are used for the signature and encryption. These algorithms can be slow.
- Often the industrial systems are time critical and it is not compatible with cryptographic algorithms
- The challenge is to find effective algorithms in order to sign and/or encrypt each message

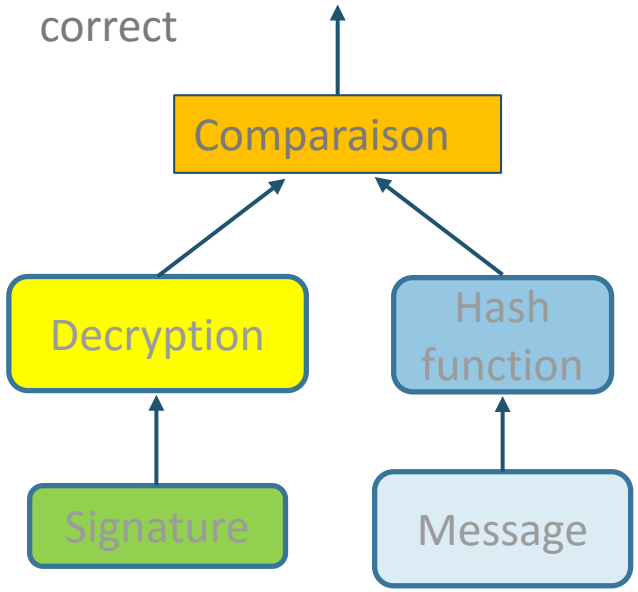
Digital signature principle

1) Signature

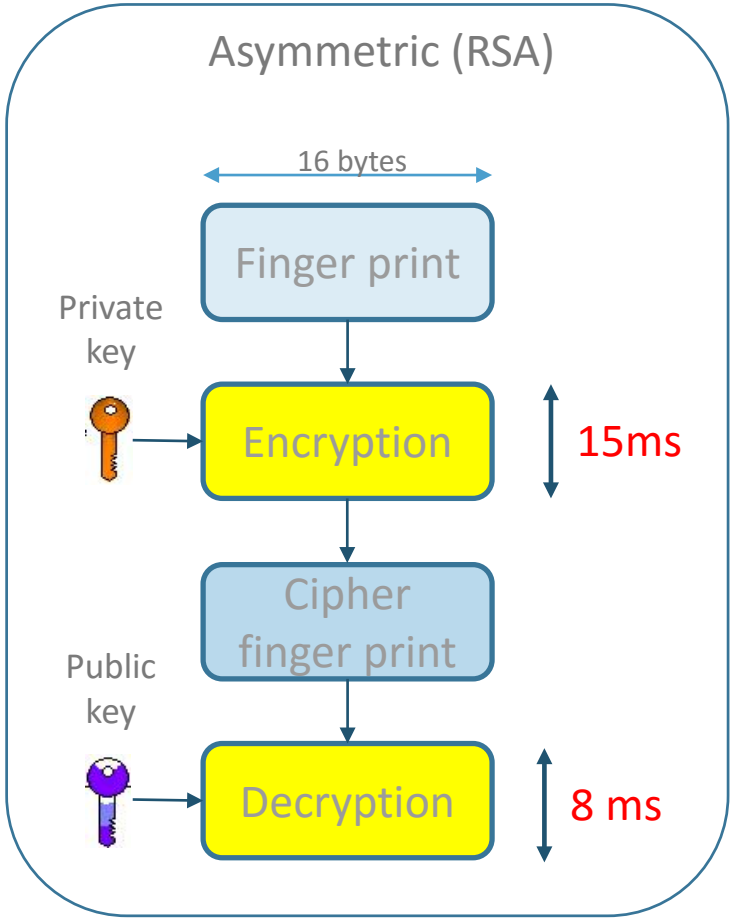


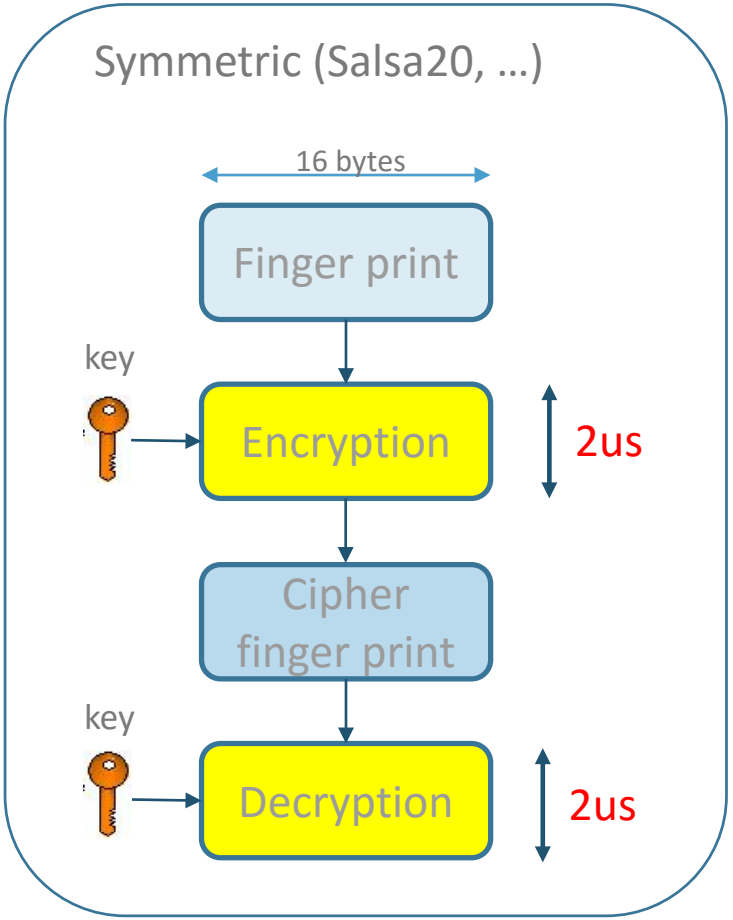
3) Verify the signature

If the 2 parts are equal
The message integrity and source authentication are correct



Asymmetric vs symmetric ciphers





Choice of algorithms

Algorithms:

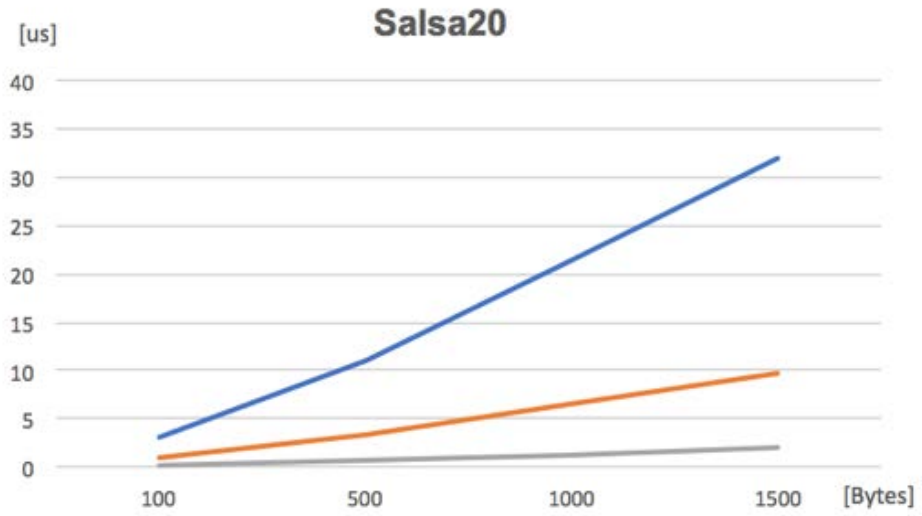
- Libsodium library (libsodium.org, Daniel J. Bernstein)

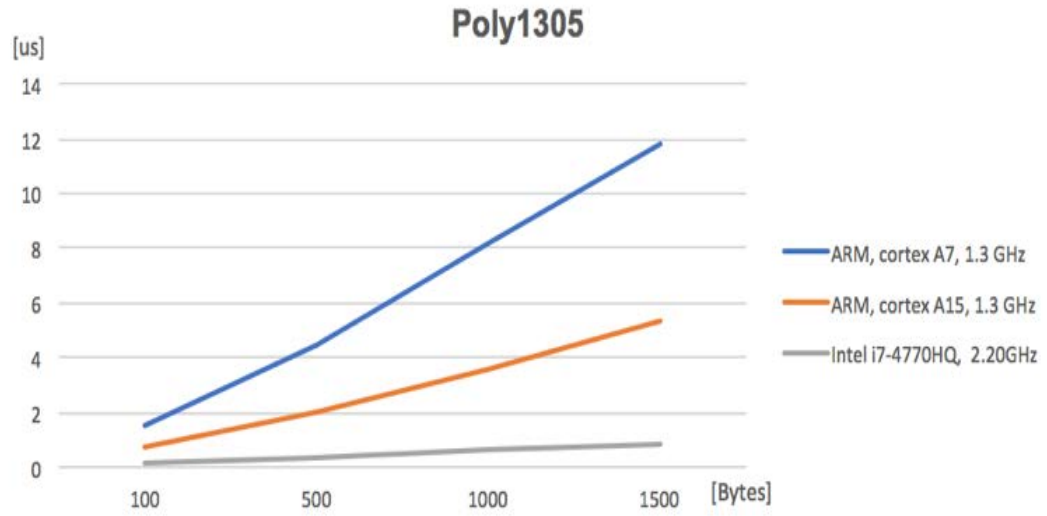
- Symmetric algorithms: AES, Chacha20, Salsa20
- Hash functions: poly1305, sha256, blake2d, shorthash, HMAC

The processors used:

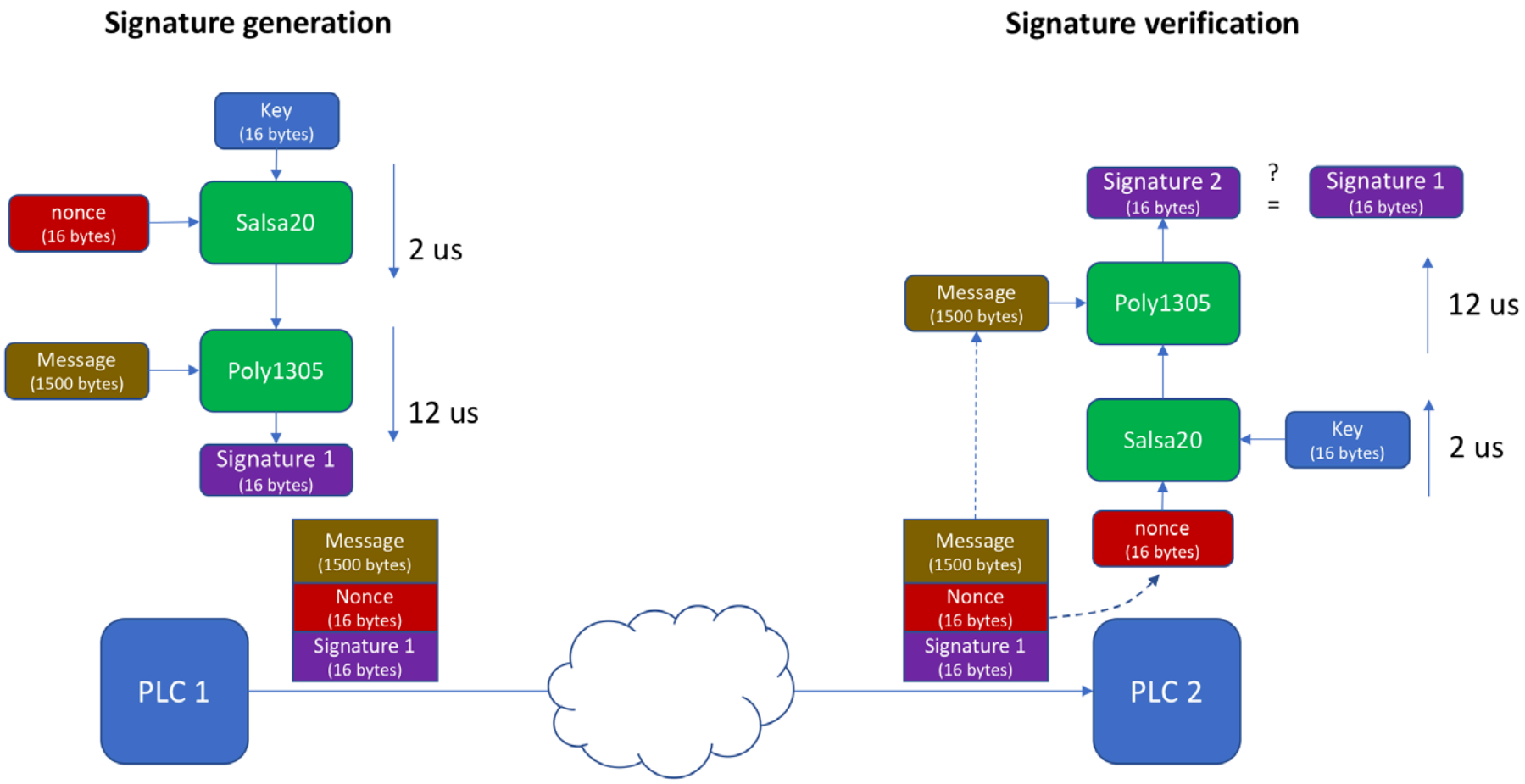
- Intel i7, 2.2 Ghz, 75000 MIPS
- ARM, cortex A15, 1.3 GHz, 4300 MIPS
- ARM, cortex A7, 1.3 GHz, 2400 MIPS.

Optimal algorithms

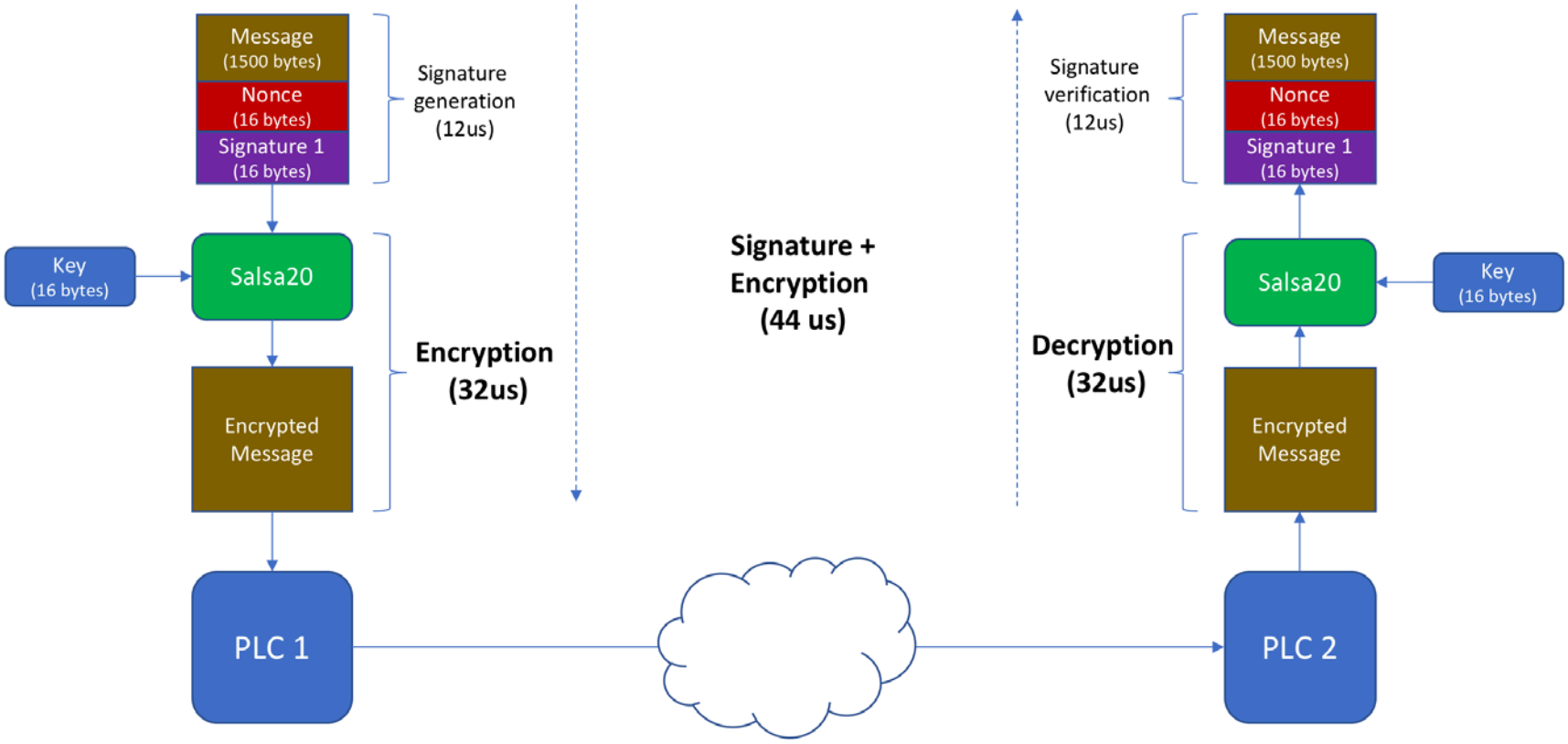




Signature of each messages



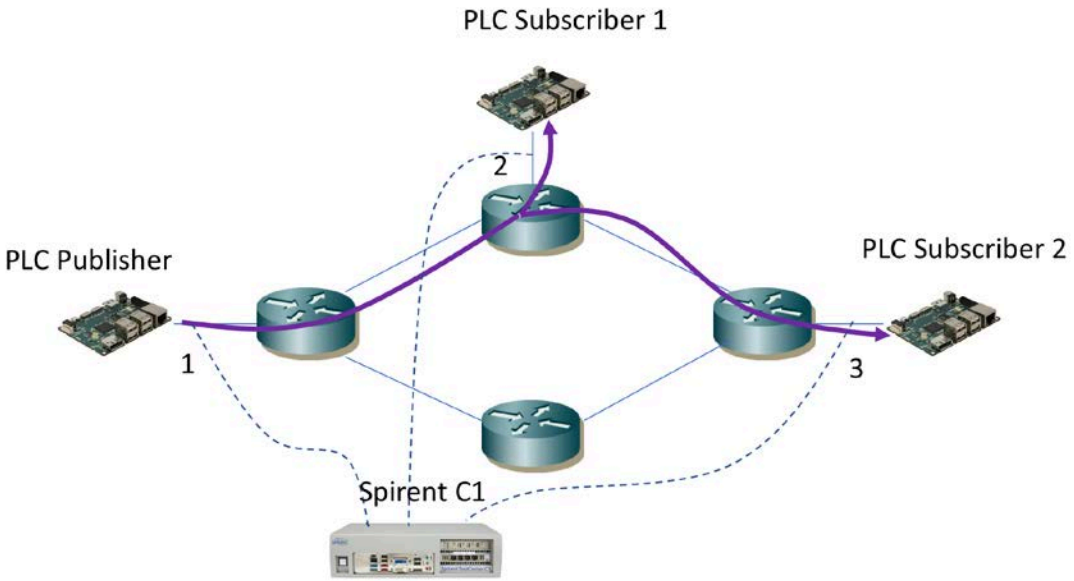
Signature and encryption of each messages



Tests: network times

- Embedded systems, Linux 4.4
- GOOSE, SV: Libiec61850 modified
- All lines: 1GBits/s
- Standard Router without QoS (Quality of Service)
- Measured times: Spirent TestCenter C1 (accuracy < 1us)

- Publisher → Subscriber 1: 130us (max 305us)
- Publisher → Subscriber 2: 200us (max 410us)



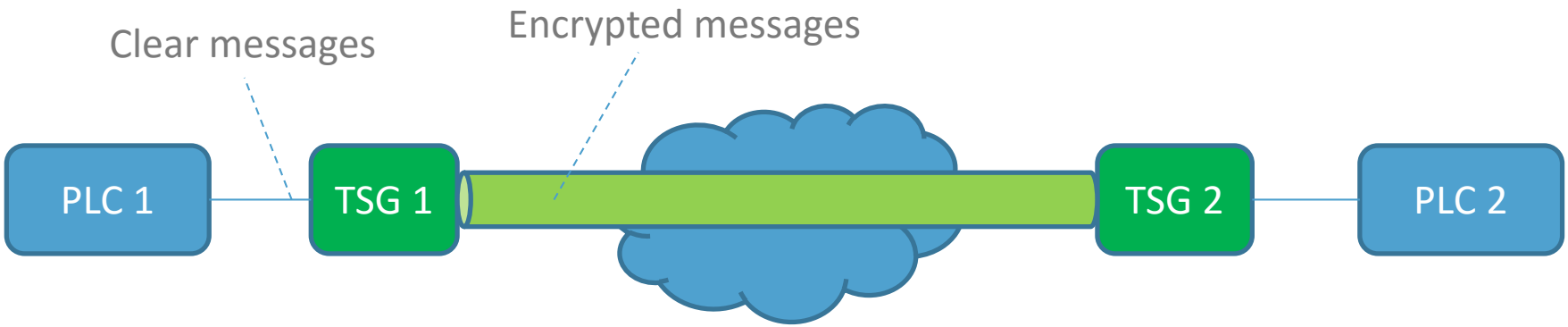
Tests, signature + encryption

- In real networks, the line propagation time of 5us/km must be added.
- For example, a real network has two routers with 100km between them.
- 1GBits/s for each line

- The total end-to-end transfer time is given by:
  - the signature and encryption (2*44us)
  - the data serialization to the line (2*12us)
  - the routing time (2*70us)
  - and the propagation time (500us)
- Total = 752us .

Transparent Secure Gateway

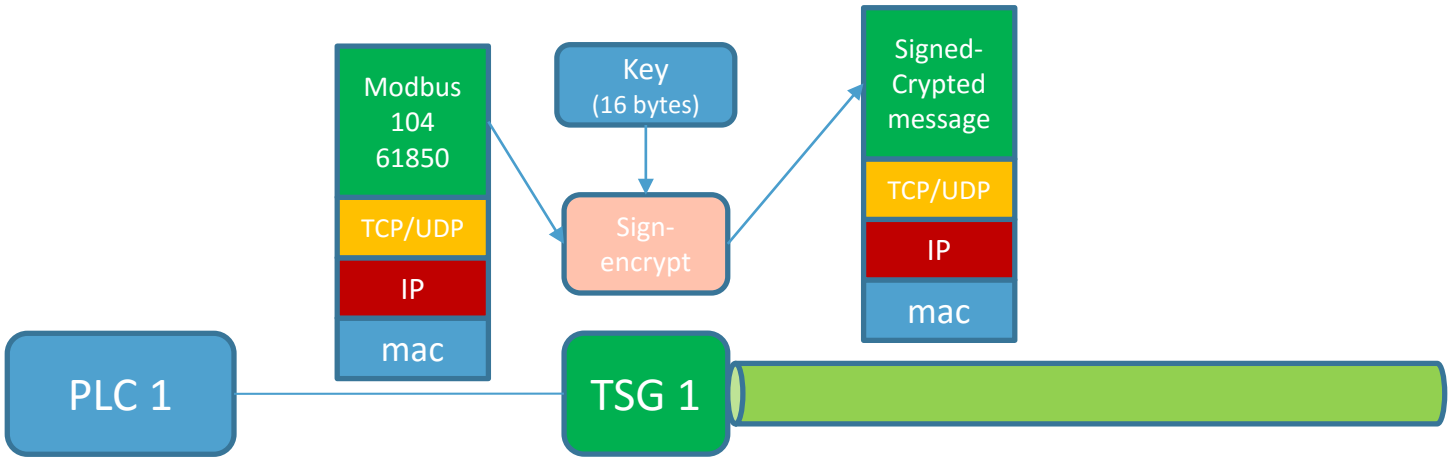
- Problem: Generally, the PLC don't know the cryptographic algorithms
- In order to solve this problem, a Transparent Secure Gateway (TSG) was created



- For the two PLC, the TSG are transparent
- PLC 1 sends usual clear messages
- TSG 1 captures the desired messages, it signs and crypts the messages and sends the messages to TSG 2
- TSG 2 decrypts and check the signature, then sends the clear message to PLC 2

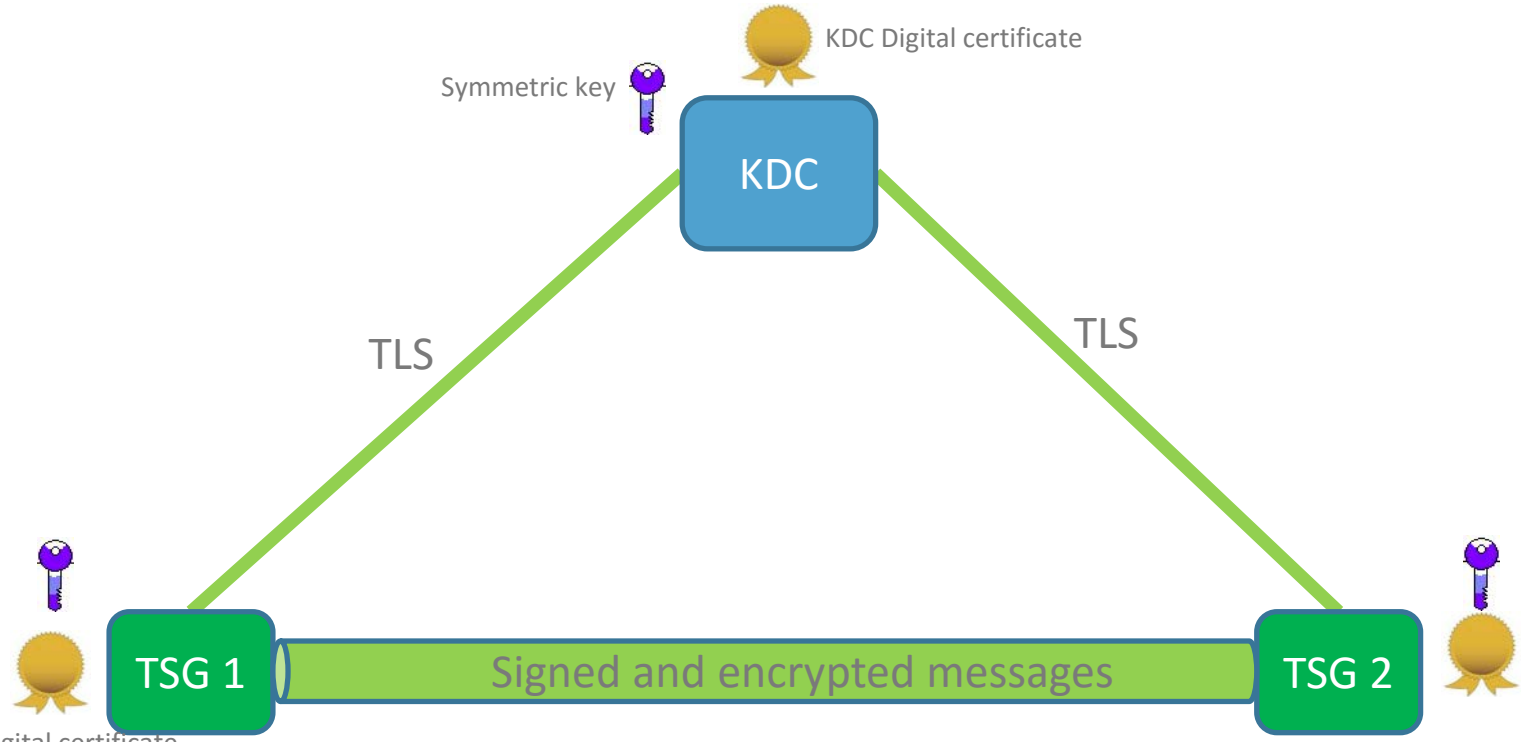
TSG: Capture messages

- The TSG is created with Linux
- Under Linux, with iptables, it is easy to filter and capture the good messages (layers IP, TCP/UDP)



TSG: Key distribution Center (KDC)

- KDC, TGS 1, TGS 2 have digital certificates. They are used for the authentication
- There are TLS tunnels between KDC – TSG1, KDC - TSG2.
- The KDC generates a random value, it is the symmetric key
- The symmetric key is sent to TSG1 and TSG2
- TSG1 and TSG2 can sign et encrypt each message



TSG: implementation

- An implementation of the TSG was made on a small hardware (WT3020H of Nexx)
- It is MIPS processor at 580MHz
- Linux 3.x

Questions?