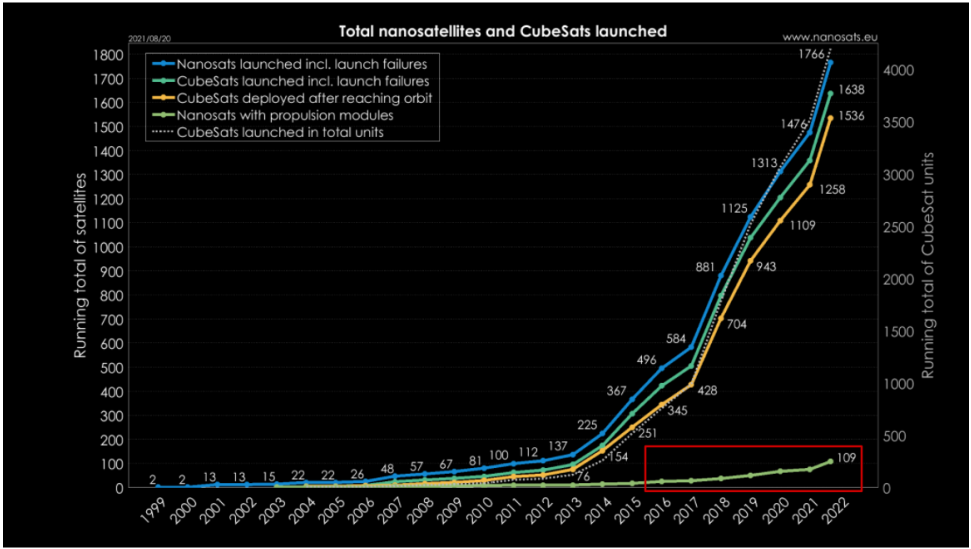
CubeCrypt - An Open-Source Implementation of Self-Signed ECC Certificates for CubeSat Telecommunication

Yannick Roelvink[1]

Jonathan Detchart[2] **Thibault Gateau**[3] **Jérôme Lacan**[2]

[1]MAE - Embedded Systems Major
[2]Department of Complex Systems Engineering (DISC)
[3]Department of Aerospace Vehicle Design and Control (DCAS)

Cubesats: A Reason for Concern ?

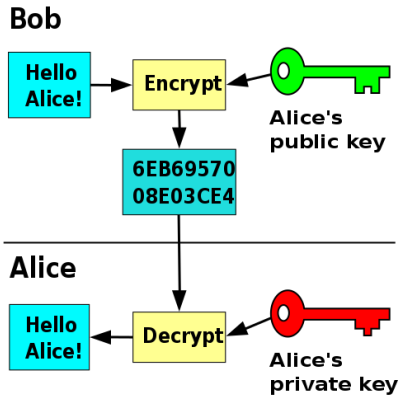


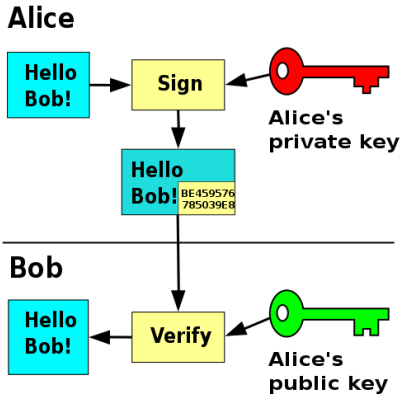
Source: [Erik Kulu 2021]

What is Public Key Cryptography ?

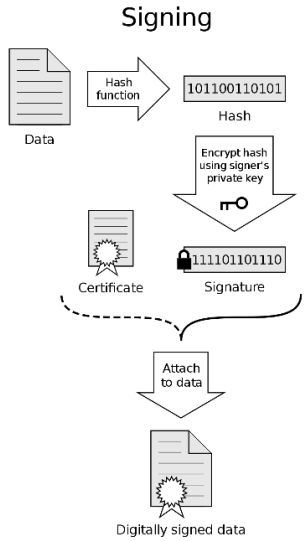
Definition

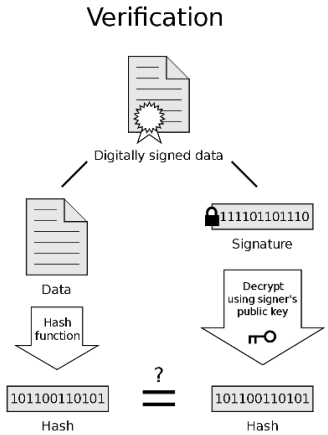
Public key (asymmetric) cryptography uses pairs of private and public keys to **encrypt** or **authenticate** data





Self-Signed Digital Certificates





If the hashes are equal, the signature is valid.

State of the Art

Examples

Uplink control of NUTS (Norwegian Cubesat)

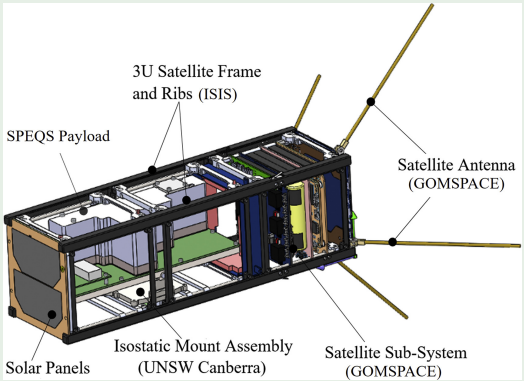
- Investigate nanosatellite cryptography
- **Symmetric key** encryption

Source: [Sandesh Prasai 2012]

State of the Art

Examples

SpooQySats: CubeSat quantum key distribution



- Entangled photon pairs
- **Symmetric key** distribution

Source: [James A. Grieve 2018]

State of the Art

Examples

A security system for satellite networks by [H. S. Cruickshank 1996]:

- Asymmetric cryptography
- Certificate authentication
- **Large** satellite implementation

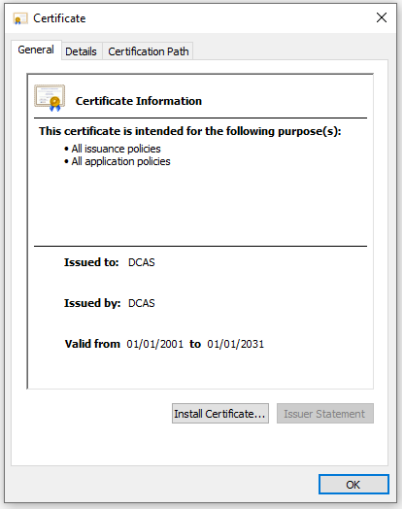
Current State

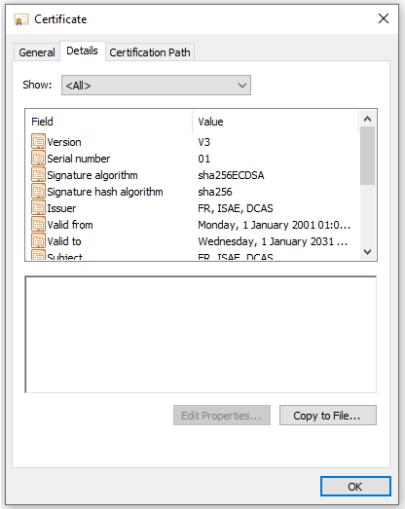
- Able to generate cryptographic **key-pairs** & **self-signed certificates**

```
-----BEGIN EC PRIVATE KEY-----
MIHcAgEBBEIAjrWaWKyDV8Vk0wVqhUzoD8YLtiovDizJtFIb66s6okAEwUz5vo04
VDxrSJFYY9gZ6l/gDv0pHfmTUOnqtMMw122gBwYFK4EEACOhgYkDgYYABAHAUnaK
7VBSyG4H4ncWNkGVo//e/UAembr2uzatQIG+IMge0vXIhOX3qlhjk0BjVP6H8w72
8417lrLKmrwG8SswtwDtQwGmlwzDqzHRAL8pJbBGzr8Dz63pFjjhlDZfRoxf7SzU
z8nBeLivYCHhzmPyI9Dqtl1/w++urFJXCSuGfKU1NA==
-----END EC PRIVATE KEY-----
```

Current State

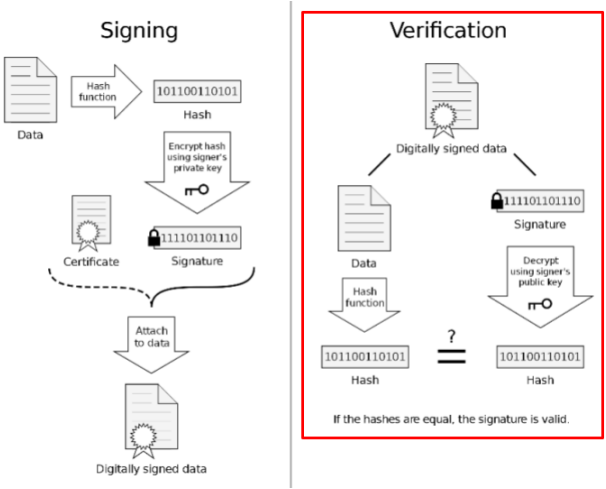
- Able to generate cryptographic **key-pairs** & **self-signed certificates**





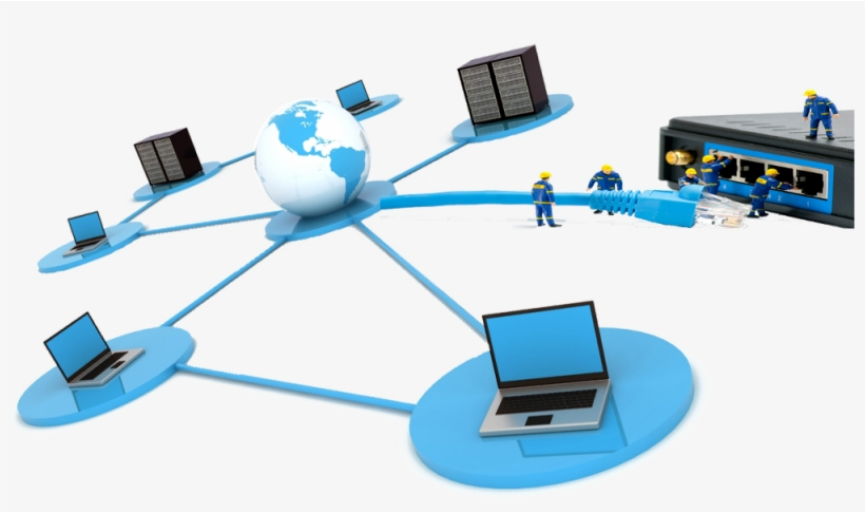
Next Steps

- Signature verification implementation



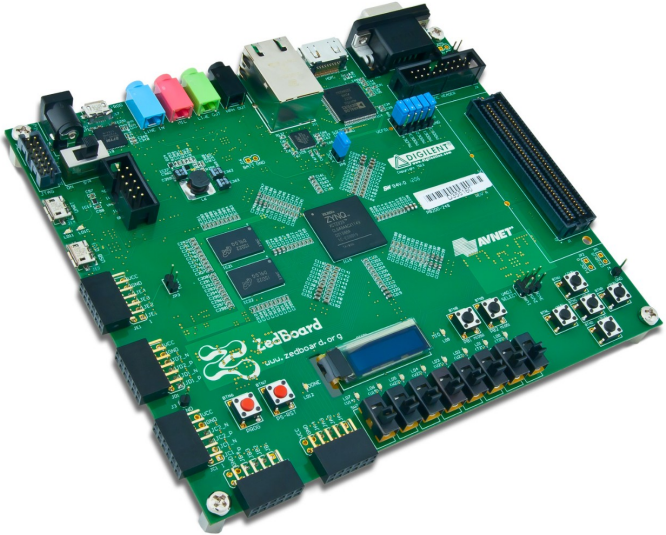
Next Steps

- On-Ground communication testing



Next Steps

- Bare-metal embedding into Zedboard

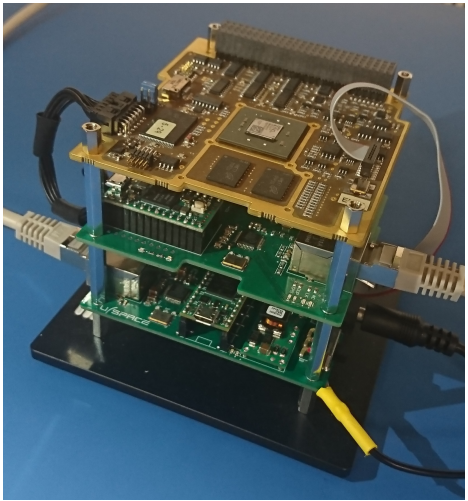


Next Steps

- Benchmark ECC curves for performance and memory usage

Next Steps

- Implementation into ISAE-SUPAERO's Ninano board*



Next Steps

- Publish final results

References I

Erik Kulu.
Nanosats Database.
https://www.nanosats.eu/index.html, August 2021.

H. S. Cruickshank.
A security system for satellite networks.
In Fifth International Conference on Satellite Systems for Mobile Communications and Navigation, pages 187–190, London, UK, May 1996.
Publisher: IET Digital Library.

James A. Grieve, Robert Bedington, Zhongkan Tang, Rakhitha C. M. R. B. Chandrasekara et Alexander Ling.
SpooQySats: CubeSats to demonstrate quantum key distribution technologies.
Acta Astronautica, vol. 151, pages 103–106, October 2018.

References II

Sandesh Prasai.
Access control of NUTS uplink.
Master's thesis, Norwegian University of Science and Technology, Trondheim, July 2012.

Thank you for your attention !

Feel free to contact me:
yannick.roelvink@student.isae-supaero.fr

Institut Supérieur de l'Aéronautique et de l'Espace

10 avenue Édouard Belin – BP 54032

31055 Toulouse Cedex 4 – France

Phone: +33 5 61 33 80 80

www.isae-supaero.fr

isae
Institut Supérieur de l'Aéronautique et de l'Espace
SUPAERO