



**HAL**  
open science

# Building Light but not Weak Protections for the IoT

Léo Perrin

► **To cite this version:**

Léo Perrin. Building Light but not Weak Protections for the IoT. PhD Graduation Ceremony of the University of Luxembourg (2018), Dec 2018, Belval, Luxembourg. hal-01959751

**HAL Id: hal-01959751**

**<https://inria.hal.science/hal-01959751>**

Submitted on 18 Dec 2018

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Building Light but not Weak Protections for the IoT



Léo Perrin

CryptoLux.org

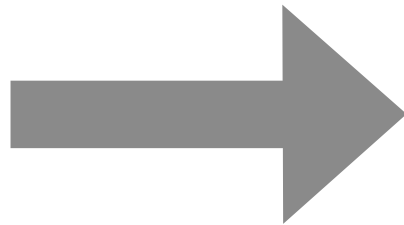
# The Internet is about exchanging messages



# The Internet is about exchanging messages



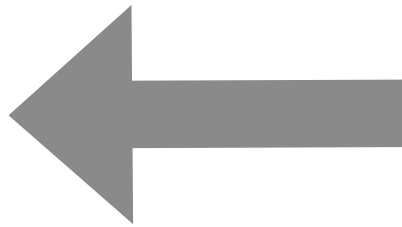
Show me my bank website



# The Internet is about exchanging messages



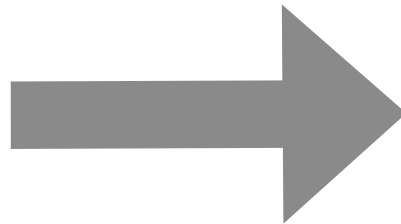
Here is the file you wanted



# The Internet is about exchanging messages

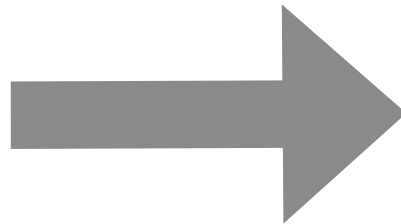


Here are my credentials

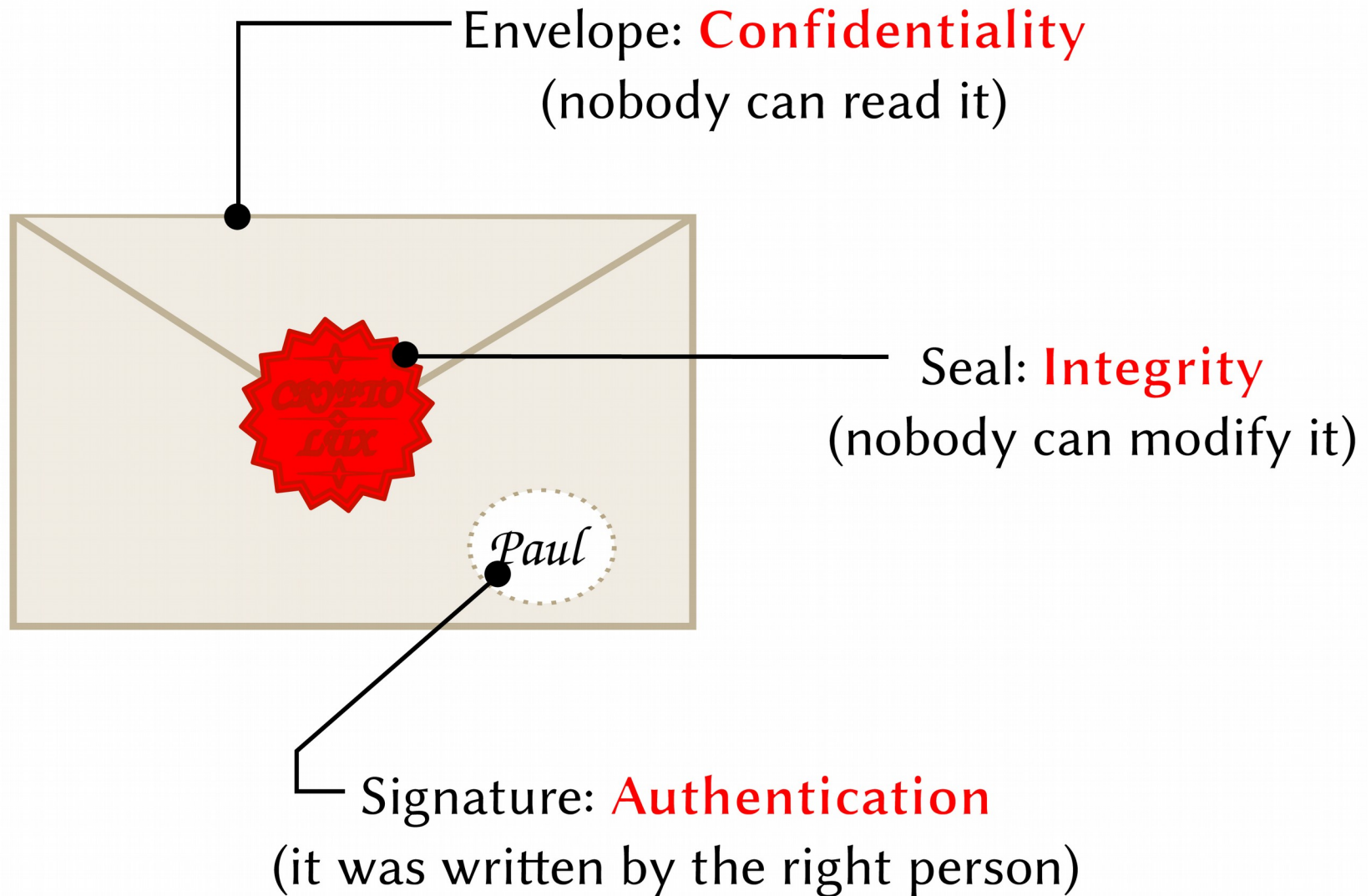


# The Internet is about exchanging messages

Here are her credentials!  
Mwahaha!



# Cryptography protects messages





# Cryptography in practice

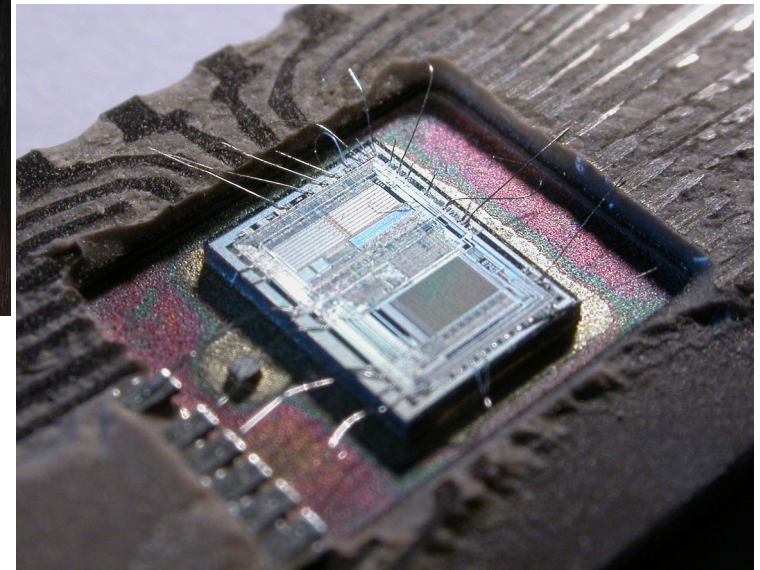
- Paper has become **bits**.
- Envelope, seal and signatures have become **algorithms**.
- Algorithms have a **cost** (time, RAM consumption...).

```
void sparx_encrypt(uint16_t * x, uint16_t k[][2*ROUNDS_PER_STEPS])
{
    uint8_t s, r, b;

    s=0; b=0; r=0;
    for (s=0 ; s<N_STEPS ; s++)
    {
        for (b=0 ; b<N_BRANCHES ; b++)
        {
            for (r=0 ; r<ROUNDS_PER_STEPS ; r++)
            {
                x[2*b ] ^= k[N_BRANCHES*s + b][2*r ];
                x[2*b+1] ^= k[N_BRANCHES*s + b][2*r + 1];
                A(x + 2*b, x + 2*b+1);
            }
        }
        L(x);
    }
    for (b=0 ; b<N_BRANCHES ; b++)
    {
        x[2*b ] ^= k[N_BRANCHES*N_STEPS][2*b ];
        x[2*b+1] ^= k[N_BRANCHES*N_STEPS][2*b+1];
    }
}
```

# Connecting devices : the IoT

Computers are replaced by micro-controllers, RFID tags...



*Things with very little computing power !*

# Light but not weak protection

When cryptography is  
too expensive...

...**Lightweight** cryptography  
comes to the rescue !

# Lightweight cryptography



We know how  
to make  
cryptographic  
**steel plates**

We need to  
invent  
cryptographic  
**carbon fiber**



# Standardization process started

## NIST Issues First Call for ‘Lightweight Cryptography’ to Protect Small Electronics

April 18, 2018

Cryptography experts at the National Institute of Standards and Technology (NIST) are kicking off an effort to protect the data created by innumerable tiny networked devices such as those in the “internet of things” (IoT), which will need a new class of cryptographic defenses against cyberattacks.



*Credit: N. Hanacek/NIST*

<https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics>

# A new challenger appears!

## **Sparx MARK II**

Joint work with

A. Biryukov, C. Beierle, J. Großschädl, A. Udovenko, Q. Wang

- Efficient on all micro-controllers
- Uses state of the art design approaches (sponge...)
- Based on **Sparx**, which we designed during my PhD

# More importantly...

## Congratulations!