



HAL
open science

Towards New International Cryptographic Standards

Léo Perrin

► **To cite this version:**

Léo Perrin. Towards New International Cryptographic Standards. FIC 2020 - International Cybersecurity Forum, Jan 2020, Lille, France. hal-03136274

HAL Id: hal-03136274

<https://hal.inria.fr/hal-03136274>

Submitted on 9 Feb 2021

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.

Towards New International Cryptographic Standards

Designing and Breaking Cryptography

Léo Perrin

Cosmiq TEAM

Inria, Paris, France

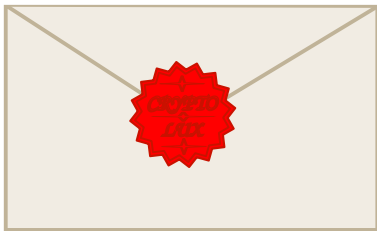
FIC 2020, Lille



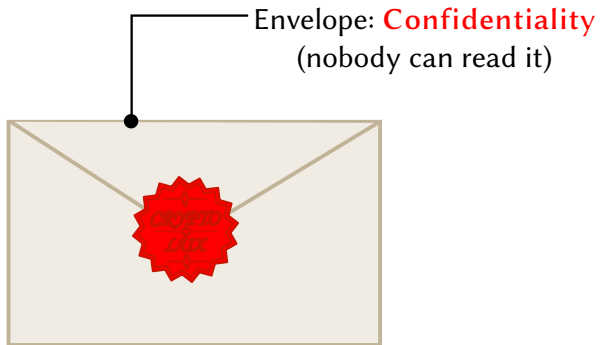
We (the **Cosmiq** team) are working on the foundations of cryptography.

- 1 What kind of algorithms do we study?
- 2 Why do we design new ones?
- 3 What kind of flaws do we find in other ones?

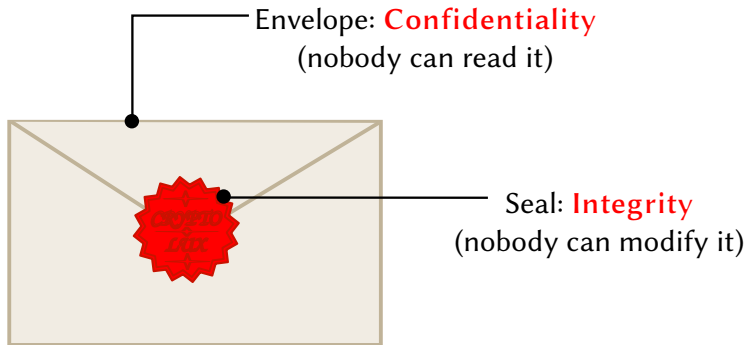
What is Cryptography?



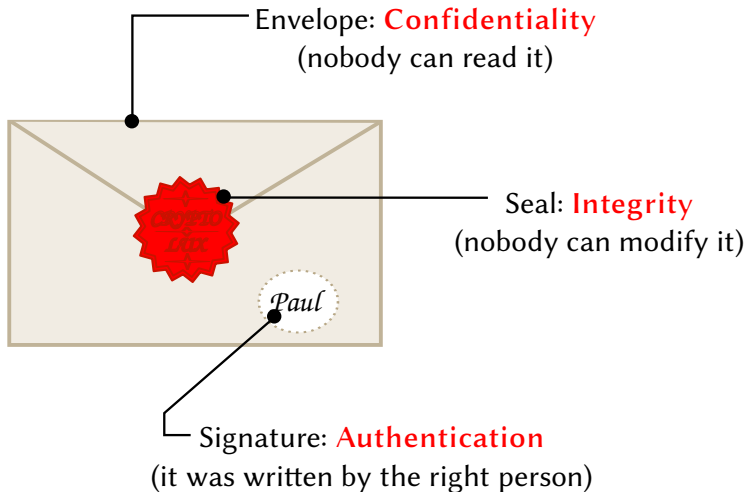
What is Cryptography?



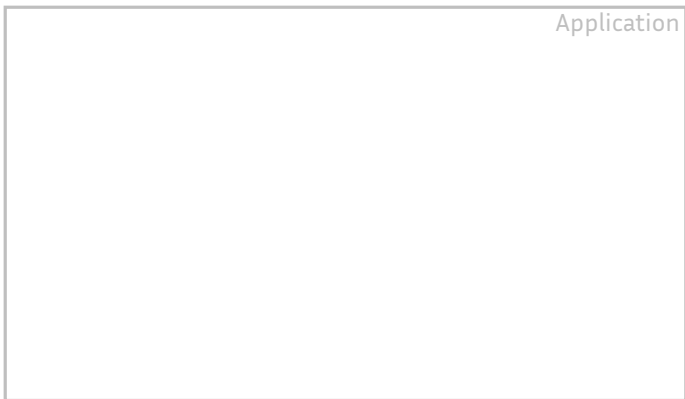
What is Cryptography?



What is Cryptography?



How Is It Used?



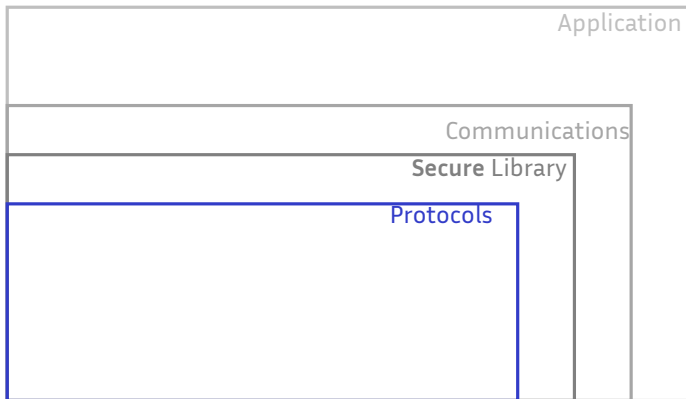
How Is It Used?



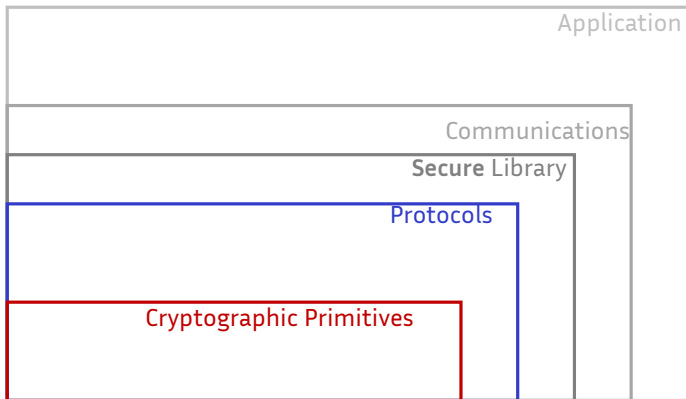
How Is It Used?



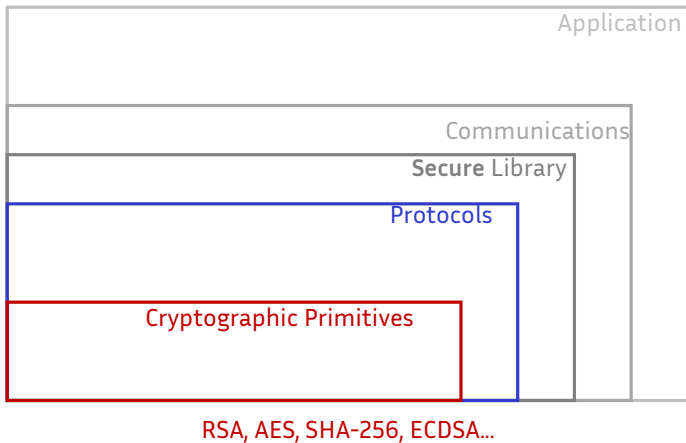
How Is It Used?



How Is It Used?



How Is It Used?



What Do Primitives Do?

A **cryptographic primitive** is a **basic building block** ; it has a very simple API but very sophisticated inner workings!

The block cipher

For any k -bit long key κ , E_{κ} is a **permutation** of $\{0, 1\}^n$.

Typically, $n \in \{64, 128\}$ and $k \in \{128, 256\}$.

To ensure **security**: no matter how many pairs $(x, E_{\kappa}(x))$ are known, it is impossible to recover κ ¹

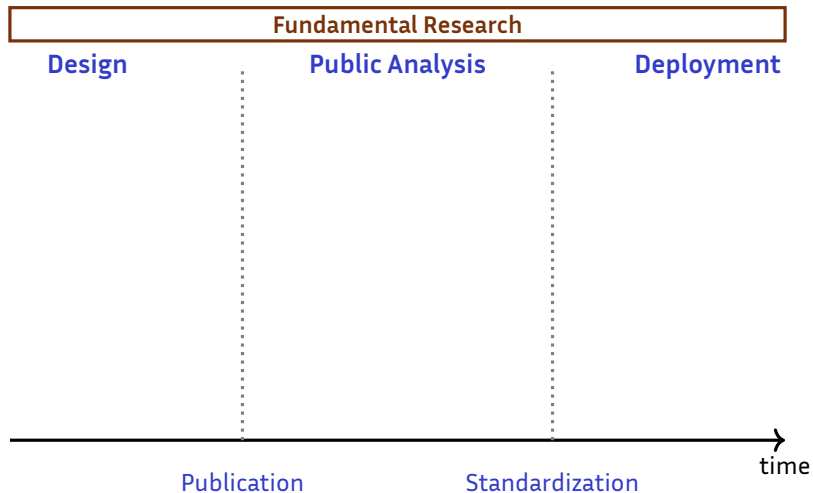
¹Except by trying all possible κ which has 2^k possible values.

How are the **primitives** used in practice chosen?

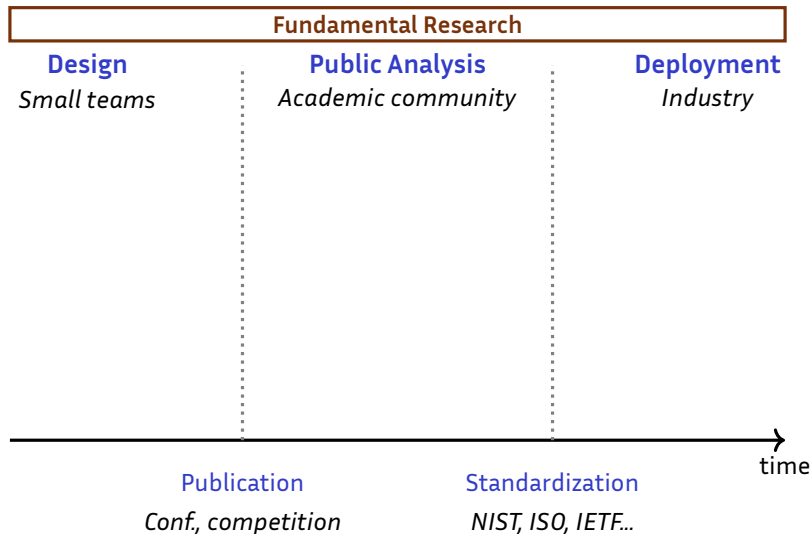
Life Cycle of a Cryptographic Primitive

Fundamental Research

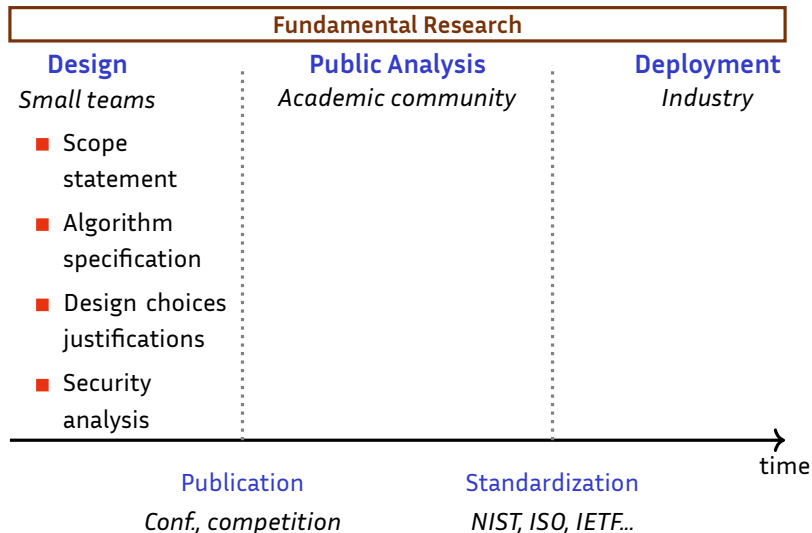
Life Cycle of a Cryptographic Primitive



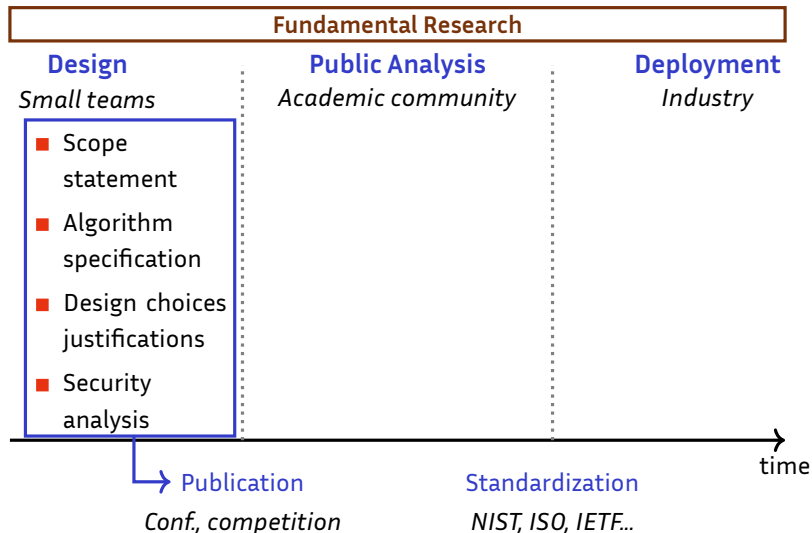
Life Cycle of a Cryptographic Primitive



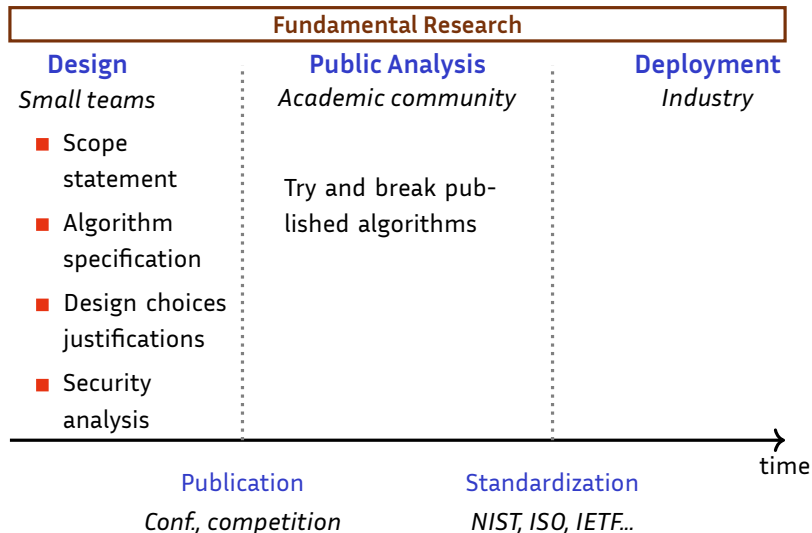
Life Cycle of a Cryptographic Primitive



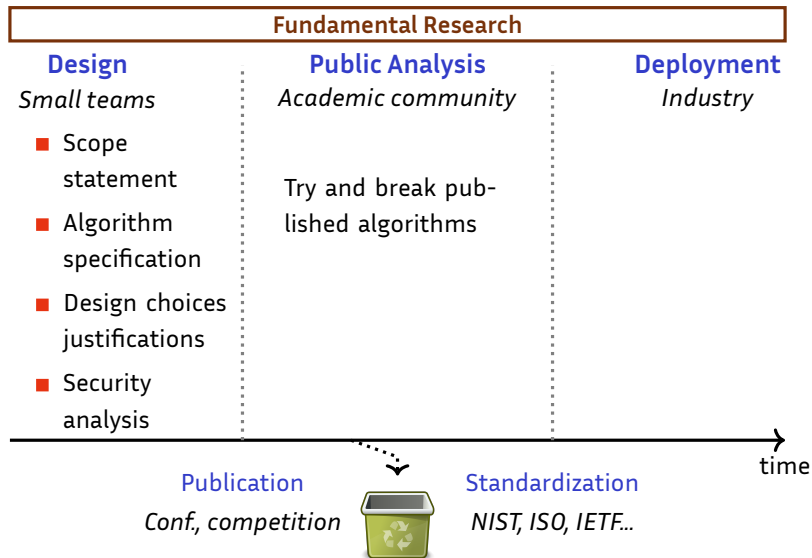
Life Cycle of a Cryptographic Primitive



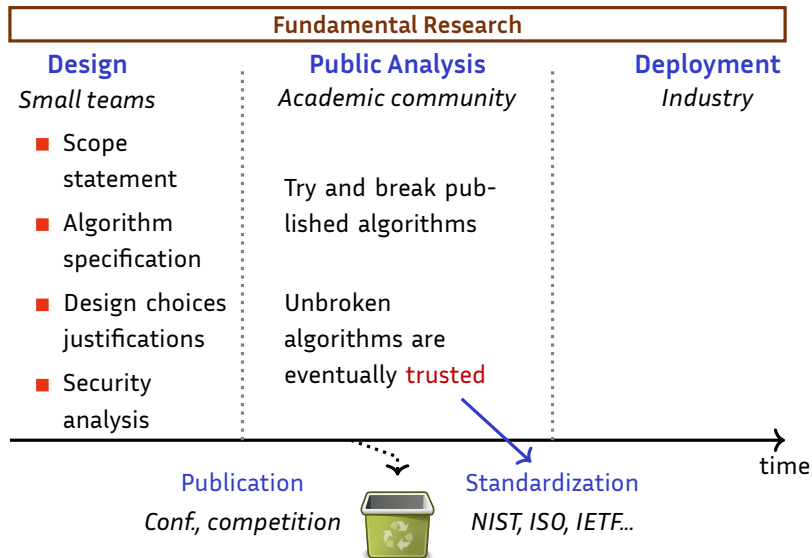
Life Cycle of a Cryptographic Primitive



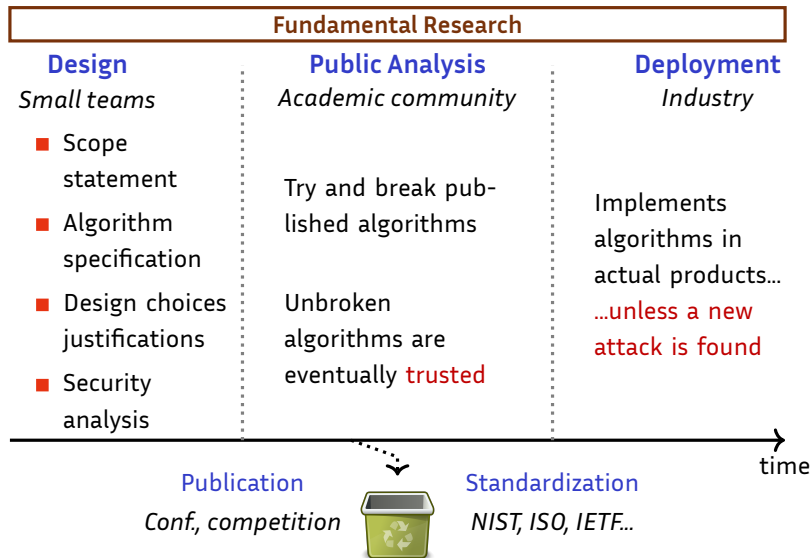
Life Cycle of a Cryptographic Primitive



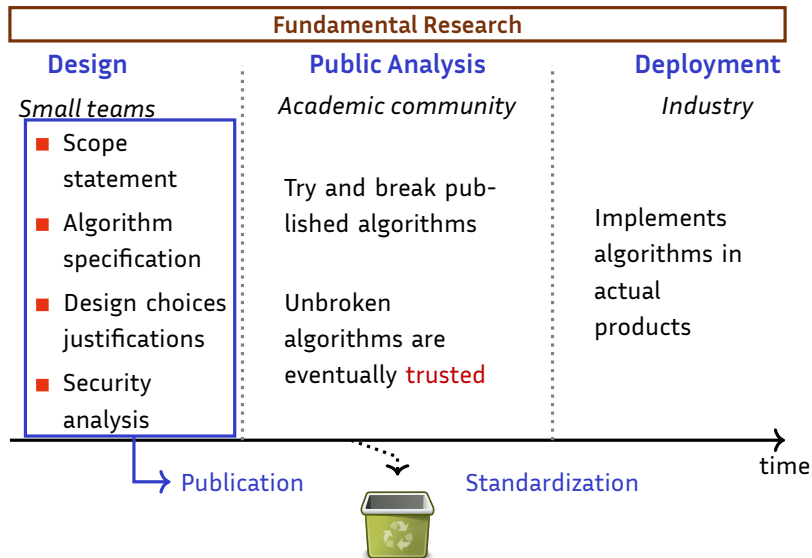
Life Cycle of a Cryptographic Primitive



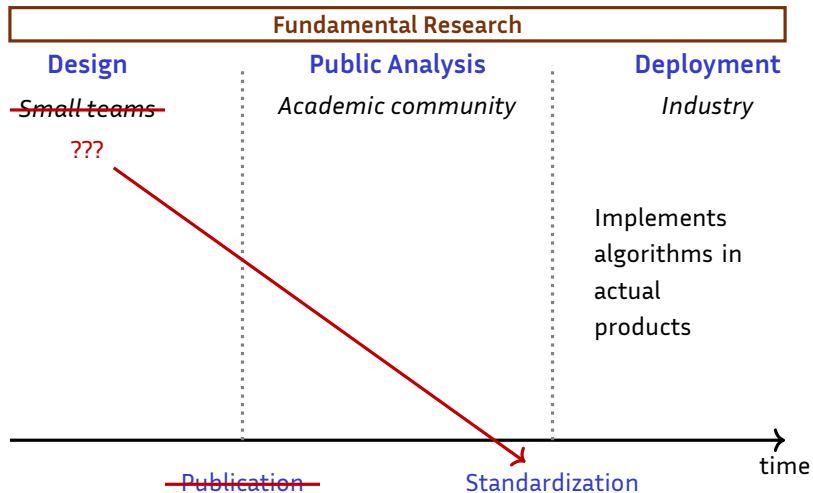
Life Cycle of a Cryptographic Primitive



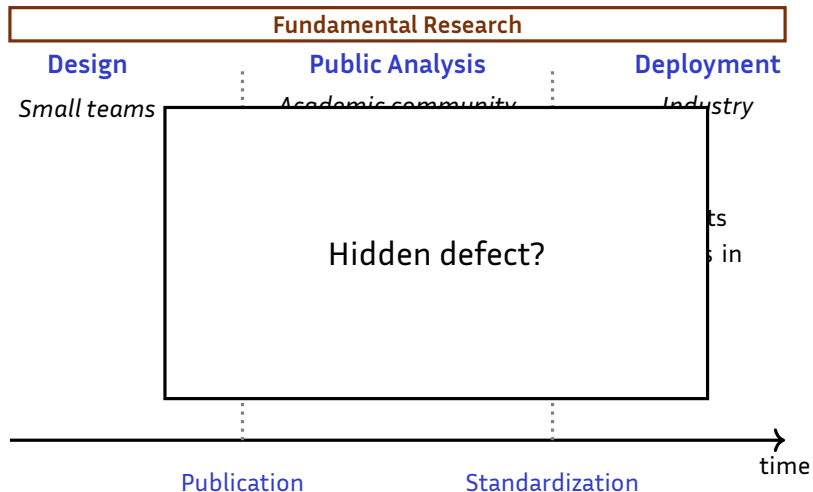
Breaking the Pipeline



Breaking the Pipeline



Breaking the Pipeline



Primitives we designed
Primitives we attacked

Primitives we designed
Primitives we attacked

Post-Quantum Public Key

The screenshot shows the NIST CSRC website. At the top left is the NIST logo, and at the top right is a search bar labeled "Search CSRC". Below the header, it says "Information Technology Laboratory" and "COMPUTER SECURITY RESOURCE CENTER" with the CSRC logo on the right. A green "PROJECTS" button is visible. The main heading is "Post-Quantum Cryptography" with social media icons for Facebook, Google+, and Twitter. Underneath is a "Project Overview" section with text: "NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Full details can be found in the [Post-Quantum Cryptography Standardization page](#). The [Round 2 candidates](#) were announced January 30, 2019. [NISTIR 8240](#), Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process is now available." To the right is a "PROJECT LINKS" sidebar with links for "Overview", "FAQs", "News & Updates", and "Events".

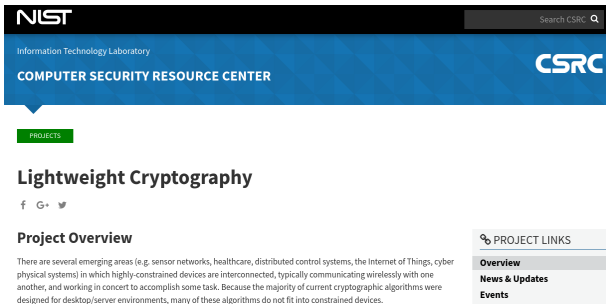
Quantum computers will **break** current public key algorithms

⇒ we need new algorithms!

Cosmiq Involvement

3 Cosmiq candidates made it to the second round! (**Bike, Classic McEliece, and Rollo**)

Lighthweight Secret Key



The screenshot shows the NIST CSRC website. At the top, there is a black header with the NIST logo on the left and a search bar labeled "Search CSRC" on the right. Below this is a blue banner with the text "Information Technology Laboratory" and "COMPUTER SECURITY RESOURCE CENTER" on the left, and the CSRC logo on the right. A green button labeled "PROJECTS" is positioned below the banner. The main heading is "Lightweight Cryptography" in a large, bold font. Below the heading are social media icons for Facebook, Google+, and Twitter. A "Project Overview" section follows, containing a paragraph of text. To the right of the overview is a "PROJECT LINKS" sidebar with three items: "Overview", "News & Updates", and "Events".

NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS

Lightweight Cryptography

f G+ ✈

Project Overview

There are several emerging areas (e.g. sensor networks, healthcare, distributed control systems, the Internet of Things, cyber physical systems) in which highly-constrained devices are interconnected, typically communicating wirelessly with one another, and working in concert to accomplish some task. Because the majority of current cryptographic algorithms were designed for desktop/server environments, many of these algorithms do not fit into constrained devices.

PROJECT LINKS

- Overview
- News & Updates
- Events

IoT devices cannot handle the (low!) **complexity** of current symmetric ciphers.

⇒ we need new algorithms!

Cosmiq Involvement

3 Cosmiq candidates made it to the second round! (Saturnin, Sparkle, Spook)

Primitives we designed
Primitives we attacked

Breaking SHA-1

SHA-1 is a **hash function**.

Collision Resistance

For a hash function H , it should not be possible to find messages x and y such that

$$H(x) = H(y).$$

Cosmiq Involvement

It is possible **in practice** to find **meaningful** messages $a||x$ and $a||y$ where a and b are meaningful and such that

$$H(a||x) = H(a||y)$$

G. Leurent, T. Peyrin. *From Collisions to Chosen-Prefix Collisions – Application to Full SHA-1*. Eurocrypt 2019.

Finding Weird Patterns in Russian Standards

questioned is the S-box π . This S-box was chosen from Streebog hash-function and it was synthesized in 2007. Note that through many years of cryptanalysis no weakness of this S-box was found. The S-box π was obtained by pseudo-random search and the following properties were taken into account.

[...]

No secret structure was enforced during construction of the S-box. At the same time, it is obvious that for any transformation a lot of representations are possible (see, for example, a lot of AES S-box representations).

Cosmiq Involvement

The designers of Streebog and Kuznyechik **are lying**. The probability that a **random** S-box is as **structured** as theirs is $< 2^{-1000}$ (\approx winning the “loto” 60 times in a row).

Scientific publication: **X. Bonnetain, L. Perrin, S. Tian**. *Anomalies and Vector Space Search: Tools for S-box Analysis*. Asiacrypt 2019.

Conclusion

Cryptography is an **active** research area motivated by concrete needs for **standard** algorithms.

Conclusion

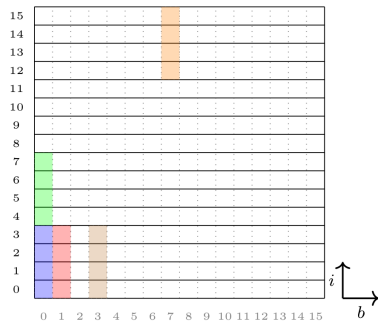
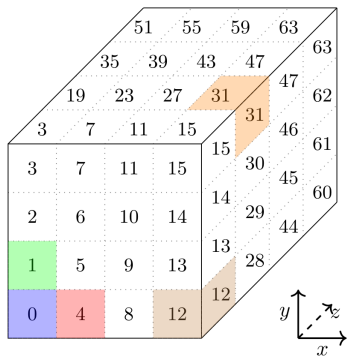
Cryptography is an **active** research area motivated by concrete needs for **standard** algorithms.

Thank you!

Delenda Russian Algo

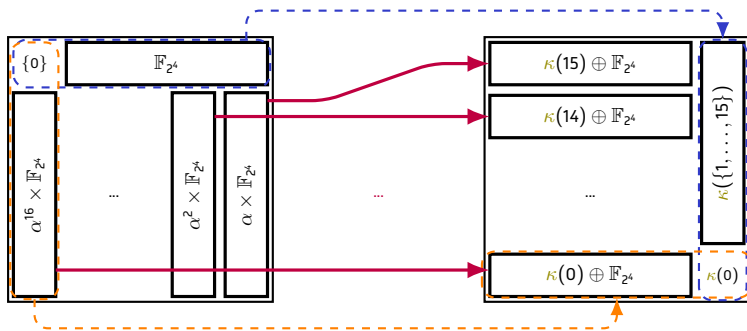
Appendix

Saturnin



The TKlog Structure

$$\pi : \begin{cases} \mathbb{F}_{2^8} & \rightarrow \mathbb{F}_{2^8} \\ 0 & \mapsto \kappa(0) \\ \alpha^{17j} & \mapsto \kappa(16 - j) & \text{for } 1 \leq j \leq 15 \\ \alpha^{i+17j} & \mapsto \kappa(16 - i) \oplus (\alpha^{17})^{s(j)} & \text{for } 0 < i, 0 \leq j < 16 \end{cases}$$



Definition

```
p(x){unsigned char*k="@`rFTDVbpPB
vdtfR@\xacp?\xe2>4\xa6\xe9{z\xe3q
5\xa7\xe8",a=2,l=0,b=17;while(x&&
(l++,a^x))a=2*a^a/128*29;return l
%b?k[l%b]^k[b+l/b]^b:k[l/b]^188;}
```

165 ASCII characters that fit on 7 bits: this program is 1155-bit long.

<https://codegolf.stackexchange.com/questions/186498/>

proving-that-a-russian-cryptographic-standard-is-too-structured

Let $P(S)$ be the bitlength of a C implementation of $S \in \mathfrak{S}_{2^n}$.

Definition (Kolmogorov Anomaly)

The **Kolmogorov Anomaly** of S for C is the opposite of the \log_2 of the probability that a random S-box has a C implementation at most as long as that of S .

Estimating the Kolmogorov Anomaly

How to estimate it?



- (≤ 1155)-bit C programs implementing 8-bit permutations
- (≤ 1155)-bit strings
- \mathfrak{S}_{2^8}

For π , we get:

$$\frac{\#(\leq 1155)\text{-bit C prog.}}{|\mathfrak{S}_{2^8}|} \leq \frac{\#(\leq 1155)\text{-bit strings.}}{|\mathfrak{S}_{2^8}|} = \frac{2^{1156} - 1}{256!} \approx 2^{-528},$$

meaning that the Kolmogorov anomaly of π for C is at least 528.