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?
Envelope: **Confidentiality**
(nobody can read it)
What is Cryptography?

Envelope: **Confidentiality**
(nobody can read it)

Seal: **Integrity**
(nobody can modify it)
What is Cryptography?

- **Envelope**: Confidentiality (nobody can read it)
- **Seal**: Integrity (nobody can modify it)
- **Signature**: Authentication (it was written by the right person)
How Is It Used?

Application
How Is It Used?
How Is It Used?

Application

Communications

Secure Library
How Is It Used?

- Application
- Communications
- Secure Library
- Protocols

Cryptographic Primitives
- RSA, AES, SHA-256, ECDSA...
How Is It Used?

- Cryptographic Primitives
  - RSA, AES, SHA-256, ECDSA...

- Secure Library

- Protocols

- Communications

- Application
How Is It Used?

- Application
- Communications
- Secure Library
- Protocols
- Cryptographic Primitives

RSA, AES, SHA-256, ECDSA...
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 $\kappa$, $E_\kappa$ 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 $k^1$

$^1$Except by trying all possible $\kappa$ which has $2^k$ possible values.
Towards New International Cryptographic Standards

How Are They Picked?

How are the **primitives** used in practice chosen?
Life Cycle of a Cryptographic Primitive

Fundamental Research
Life Cycle of a Cryptographic Primitive

Fundamental Research

- Design
- Public Analysis
- Deployment

Publication

Standardization

- Time
- Small teams
- Academic community
- Industry
- Conf., competition
- NIST, ISO, IETF...
- Scope
- Statement
- Algorithm
- Specification
- Design choices
- Justifications
- Security analysis
- Try and break published algorithms
- Unbroken algorithms are eventually trusted
- Implements algorithms in actual products...
- ...unless a new attack is found
Towards New International Cryptographic Standards

How Are They Picked?

Life Cycle of a Cryptographic Primitive

- **Fundamental Research**
  - **Design**
    - Small teams
  - **Public Analysis**
    - Academic community
  - **Deployment**
    - Industry

- **Publication**
  - Conf., competition

- **Standardization**
  - NIST, ISO, IETF...
Life Cycle of a Cryptographic Primitive

**Fundamental Research**

- **Design**
  - Small teams
  - Scope statement
  - Algorithm specification
  - Design choices justifications
  - Security analysis

- **Public Analysis**
  - Academic community

- **Deployment**
  - Industry

**Publication**
- Conf., competition

**Standardization**
- NIST, ISO, IETF...
Towards New International Cryptographic Standards

How Are They Picked?

Life Cycle of a Cryptographic Primitive

Fundamental Research

Design
Small teams
- Scope statement
- Algorithm specification
- Design choices justifications
- Security analysis

Public Analysis
Academic community
Publication
Conf., competition

Deployment
Industry
Standardization
NIST, ISO, IETF...
## Life Cycle of a Cryptographic Primitive

<table>
<thead>
<tr>
<th>Fundamental Research</th>
<th>Design</th>
<th>Public Analysis</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design</strong></td>
<td>Small teams</td>
<td><strong>Public Analysis</strong></td>
<td><strong>Deployment</strong></td>
</tr>
<tr>
<td>- Scope statement</td>
<td>- Algorithm specification</td>
<td>- Try and break published algorithms</td>
<td>- Industry</td>
</tr>
<tr>
<td>- Design choices justifications</td>
<td>- Security analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Publication</td>
<td>Standardization</td>
<td></td>
</tr>
<tr>
<td>- Conf., competition</td>
<td>NIST, ISO, IETF...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Life Cycle of a Cryptographic Primitive

**Fundamental Research**

- **Design**
  - *Small teams*
  - Scope statement
  - Algorithm specification
  - Design choices justifications
  - Security analysis

- **Public Analysis**
  - *Academic community*
  - Try and break published algorithms

- **Deployment**
  - *Industry*

**Publication**
- *Conf., competition*

**Standardization**
- *NIST, ISO, IETF...*
Life Cycle of a Cryptographic Primitive

**Fundamental Research**

- **Design**
  - Small teams
  - Scope statement
  - Algorithm specification
  - Design choices justifications
  - Security analysis

- **Public Analysis**
  - Academic community
  - Try and break published algorithms
  - Unbroken algorithms are eventually trusted

- **Deployment**
  - Industry

**Publication**
- Conf., competition

**Standardization**
- NIST, ISO, IETF...
Life Cycle of a Cryptographic Primitive

**Fundamental Research**

- **Design**
  - Small teams
  - Scope statement
  - Algorithm specification
  - Design choices justifications
  - Security analysis

- **Public Analysis**
  - Academic community
  - Try and break published algorithms
  - Unbroken algorithms are eventually trusted

- **Deployment**
  - Industry
  - Implements algorithms in actual products...
  - ...unless a new attack is found

**Publication**

- Conf., competition

**Standardization**

- NIST, ISO, IETF...
Breaking the Pipeline

Fundamental Research

Design
- Small teams
  - Scope statement
  - Algorithm specification
  - Design choices justifications
  - Security analysis

Public Analysis
- Academic community
  - Try and break published algorithms
  - Unbroken algorithms are eventually trusted

Deployment
- Industry
  - Implements algorithms in actual products

Publication

Standardization

Time
Breaking the Pipeline

Fundamental Research

- **Design**
  - Small teams

- **Public Analysis**
  - Academic community

- **Deployment**
  - Industry

---

- Publication
- Standardization

- Implements algorithms in actual products

- Time
Breaking the Pipeline

Fundamental Research

Design

Public Analysis

Deployment

Small teams

Academic community

Industry

Publication

Standardization

Hidden defect?
Primitives we designed
Primitives we attacked
Towards New International Cryptographic Standards

Primitives we designed

Primitives we attacked
Towards New International Cryptographic Standards

Primitives We Designed

Post-Quantum Public Key

Post-Quantum Cryptography

Project Overview

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.

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)
Towards New International Cryptographic Standards

Primitives We Designed

Lightweight Secret Key

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 \( \pi \). 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 \( \pi \) 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).

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
On the Russian Standards

Saturnin
The TKlog Structure

\[
\Pi : \begin{cases} 
\mathbb{F}_{2^8} & \rightarrow \mathbb{F}_{2^8} \\
0 & \mapsto \kappa(0) \\
\alpha^{17j} & \mapsto \kappa(16 - j) \\
\alpha^i \cdot \alpha^{17j} & \mapsto \kappa(16 - i) \oplus (\alpha^{17})^{s(j)} 
\end{cases}
\]

for \(1 \leq j \leq 15\)

for \(0 < i, 0 \leq j < 16\)
Definition

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

**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?

- $(\leq 1155)$-bit C programs implementing 8-bit permutations
- $(\leq 1155)$-bit strings
- $\mathcal{S}_{2^8}

For $\pi$, we get:

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

meaning that the Kolmogorov anomaly of $\pi$ for C is at least 528.