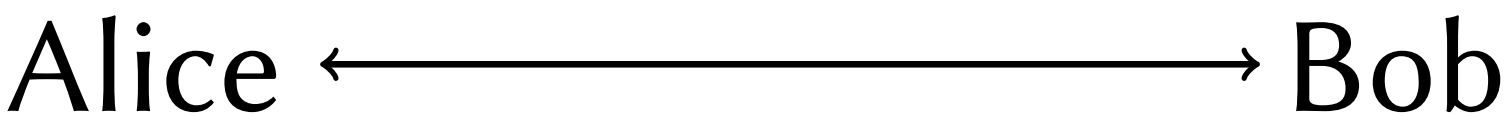
Cryptanalysis, Reverse-Engineering and Design of Symmetric Cryptographic Algorithms

Léo Perrin

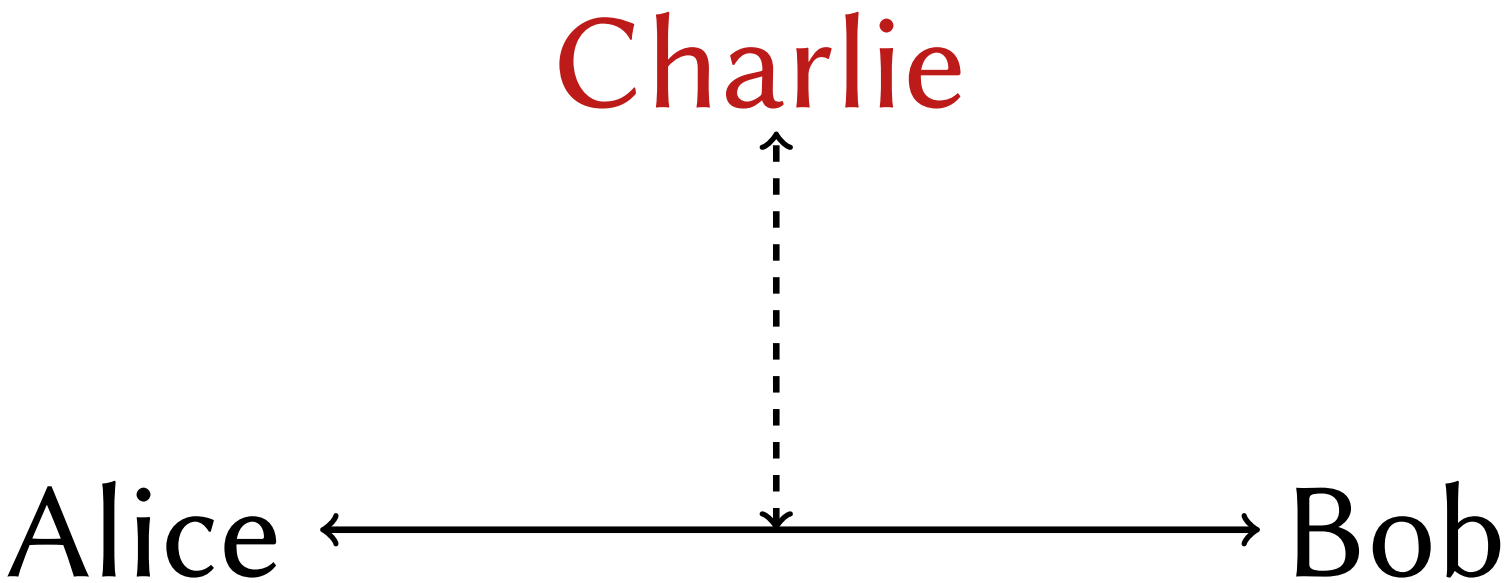
CSC & SnT, University of Luxembourg
CryptoLUX Team ; supervised by Alex Biryukov

July 5th 2018

Cryptography? (1/3)



Cryptography? (1/3)

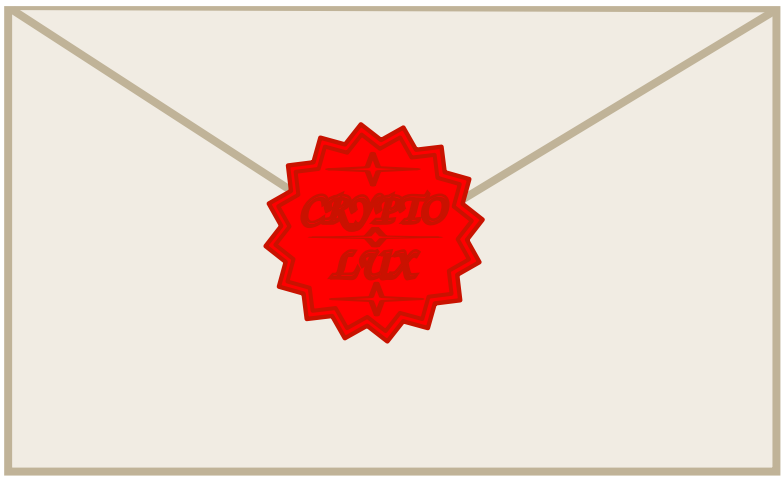


Cryptography? (1/3)

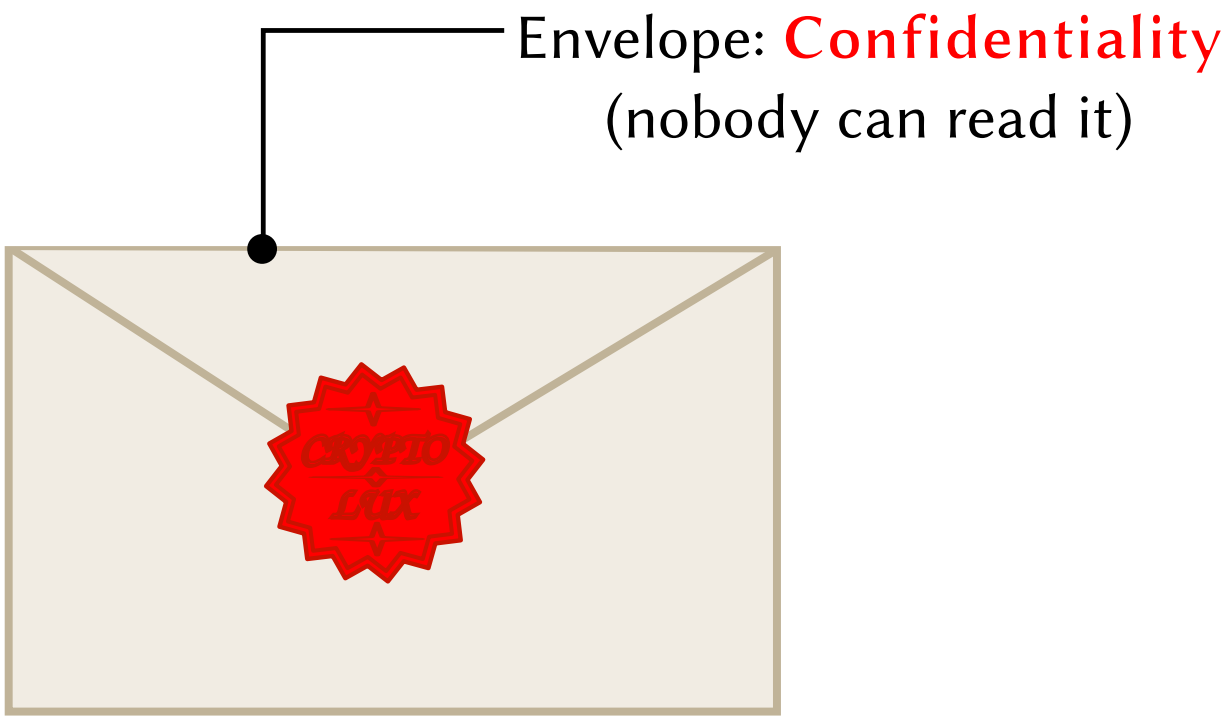
Cryptography? (2/3)

Cryptography is everywhere!

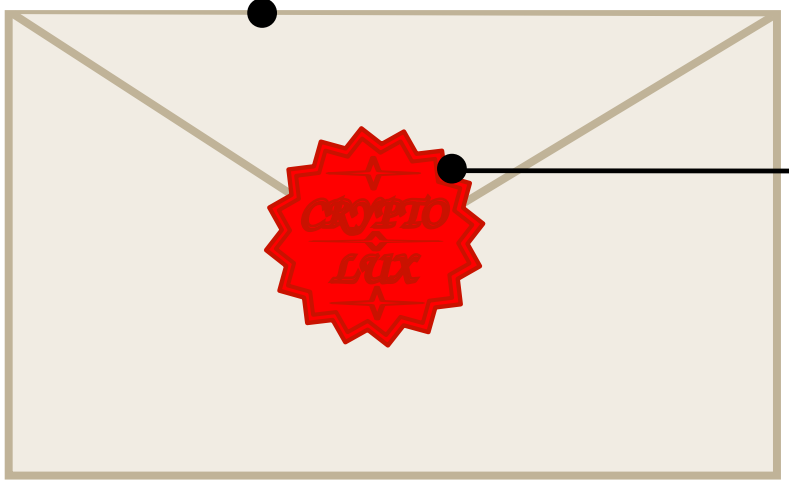
Cryptography? (3/3)



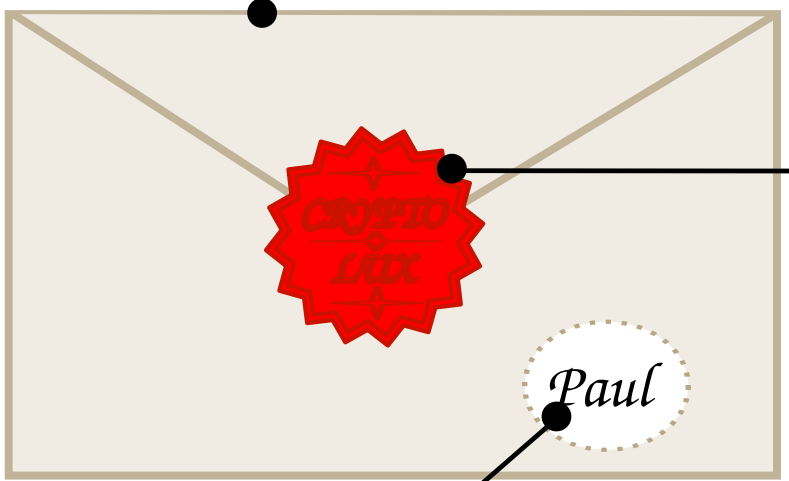
Cryptography? (3/3)



Cryptography? (3/3)



Cryptography? (3/3)



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

Seal: **Integrity**
(nobody can modify it)

Signature: **Authentication**
(it was written by the right person)

Modern Cryptography

	Before
Data encrypted	Letters/Digits
Method	By hand/ machine
Cryptographers	Linguists inventors
Example	

Modern Cryptography

	Before	Now
Data encrypted	Letters/Digits	0,1 (bits)
Method	By hand/ machine	Computer program
Cryptographers	Linguists inventors	Mathematicians Computer scientists
Example		

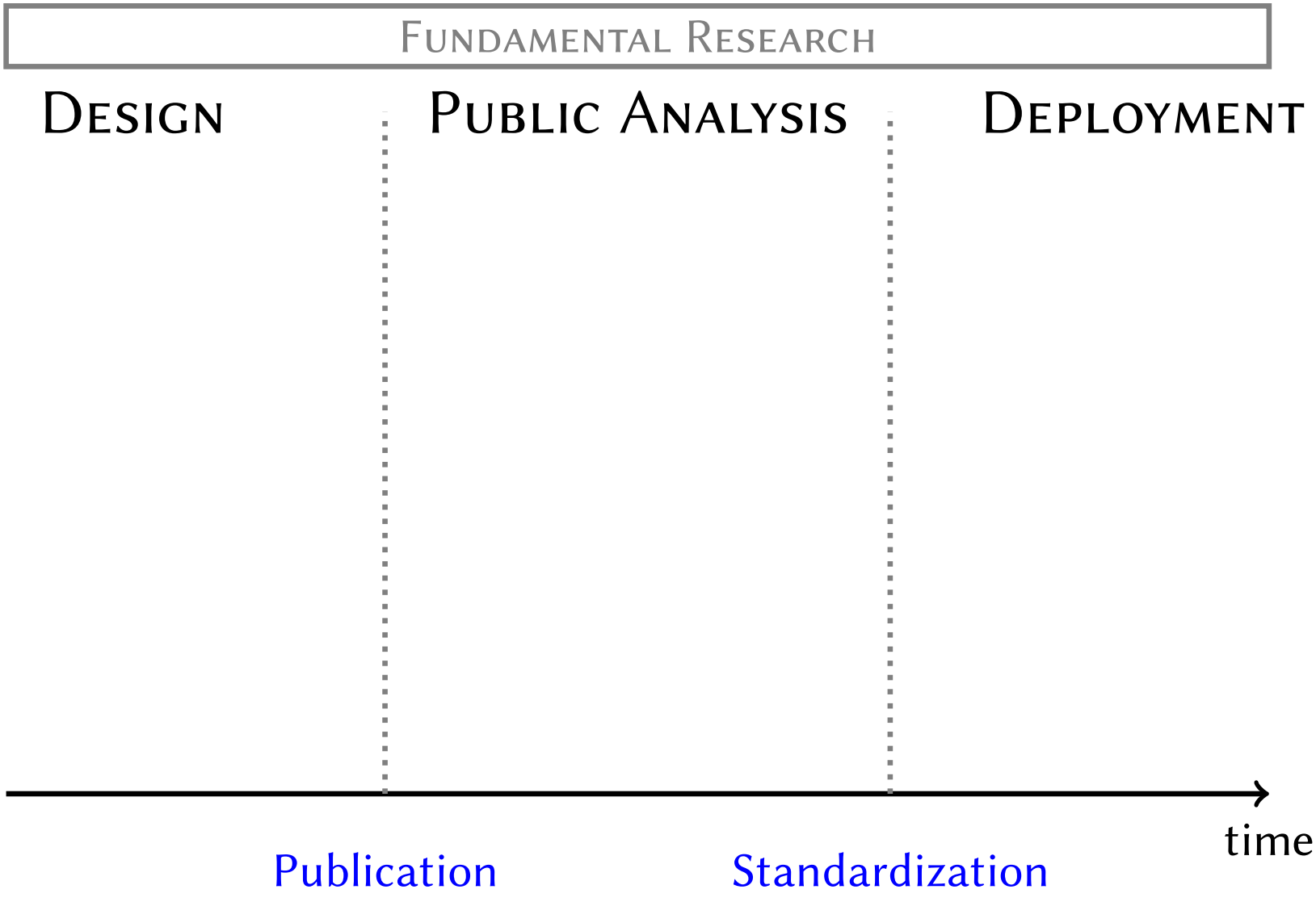
```
void sparx_encrypt(uint16_t * x, uint16_t k[][2*R_S]) {
    unsigned int s, r, b;
    for (s=0 ; s<N_S ; s++) {
        for (b=0 ; b<N_B ; b++)
            for (r=0 ; r<R_S ; r++) {
                x[2*b  ] ^= k[N_B*s + b][2*r    ];
                x[2*b+1] ^= k[N_B*s + b][2*r + 1];
                A(x[2*b], x[2*b+1]);
            }
        L(x);
    }
    for (b=0 ; b<N_B ; b++) {
        x[2*b  ] ^= k[N_B*N_S][2*b  ];
        x[2*b+1] ^= k[N_B*N_S][2*b+1];
    }
}
```

How do we design such algorithms?

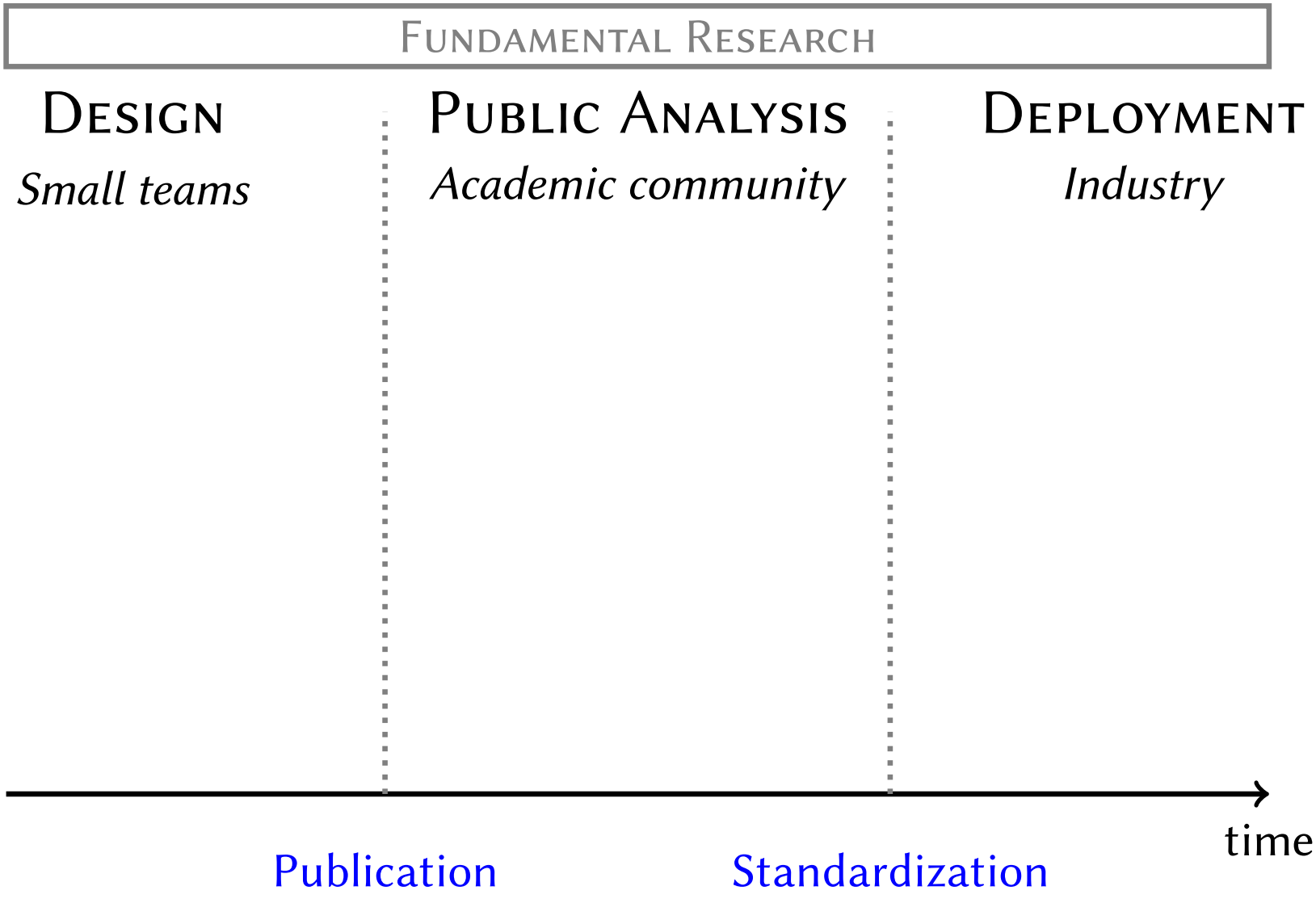
"Cryptographic Pipeline"

Fundamental Research

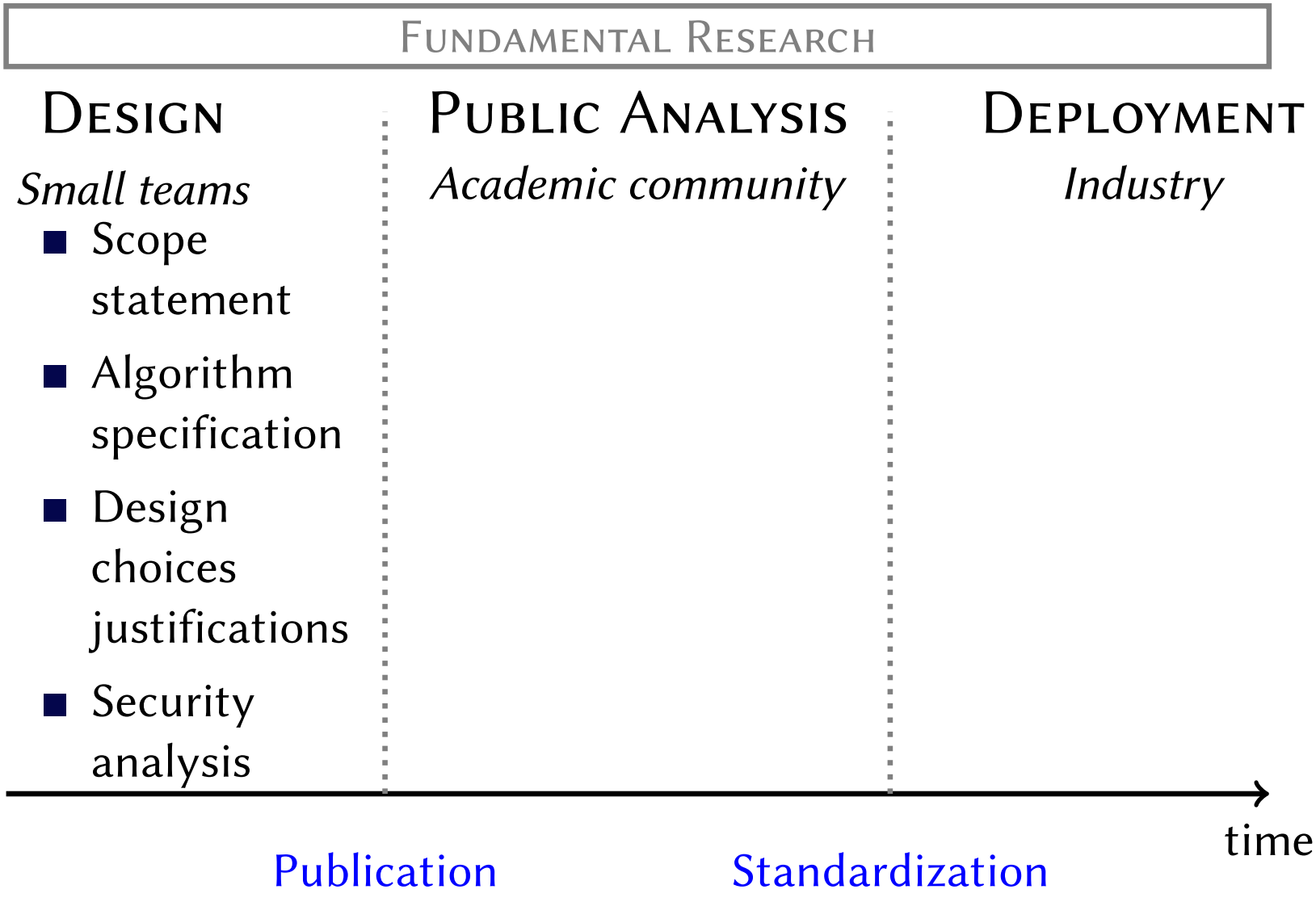
"Cryptographic Pipeline"



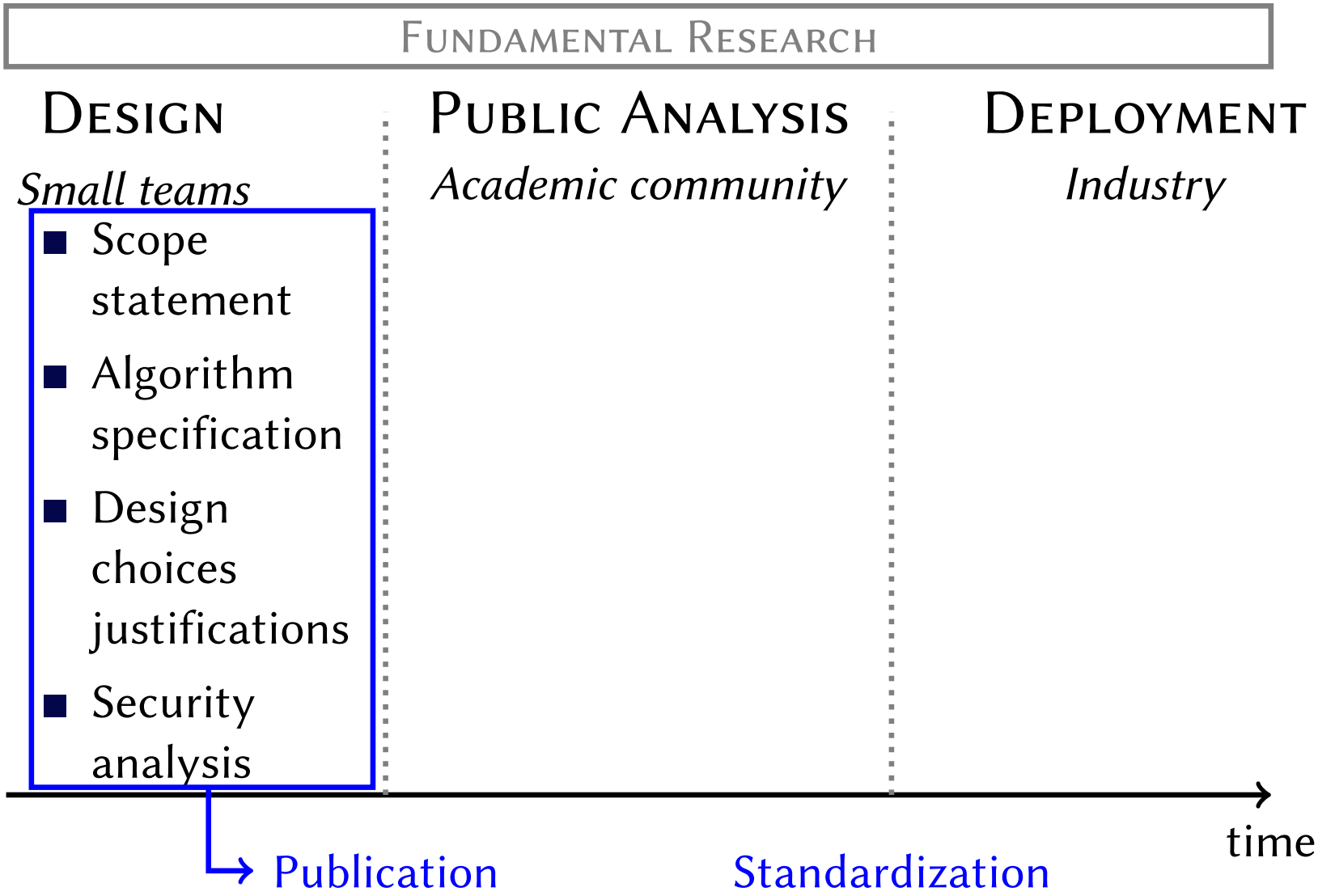
"Cryptographic Pipeline"



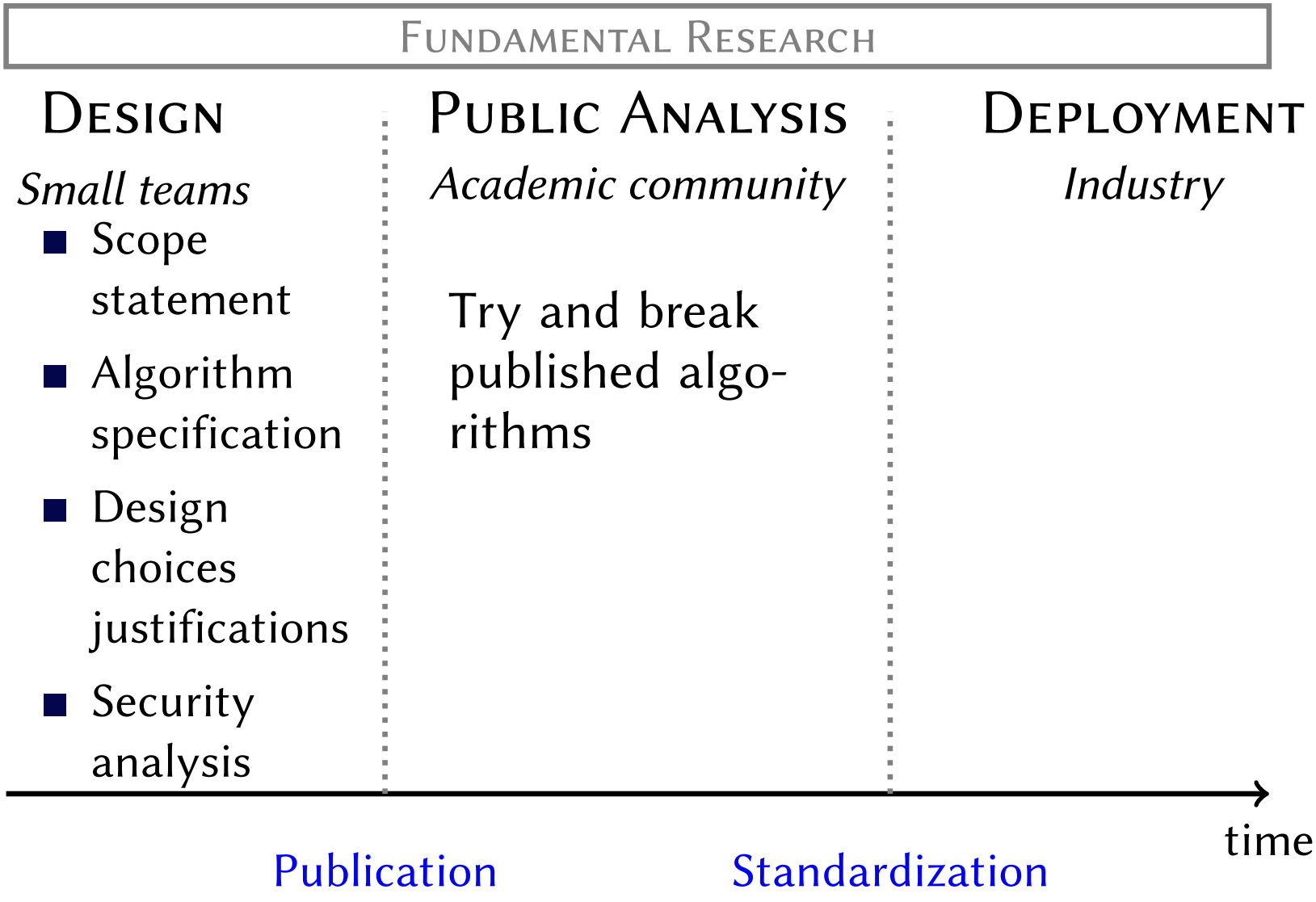
"Cryptographic Pipeline"



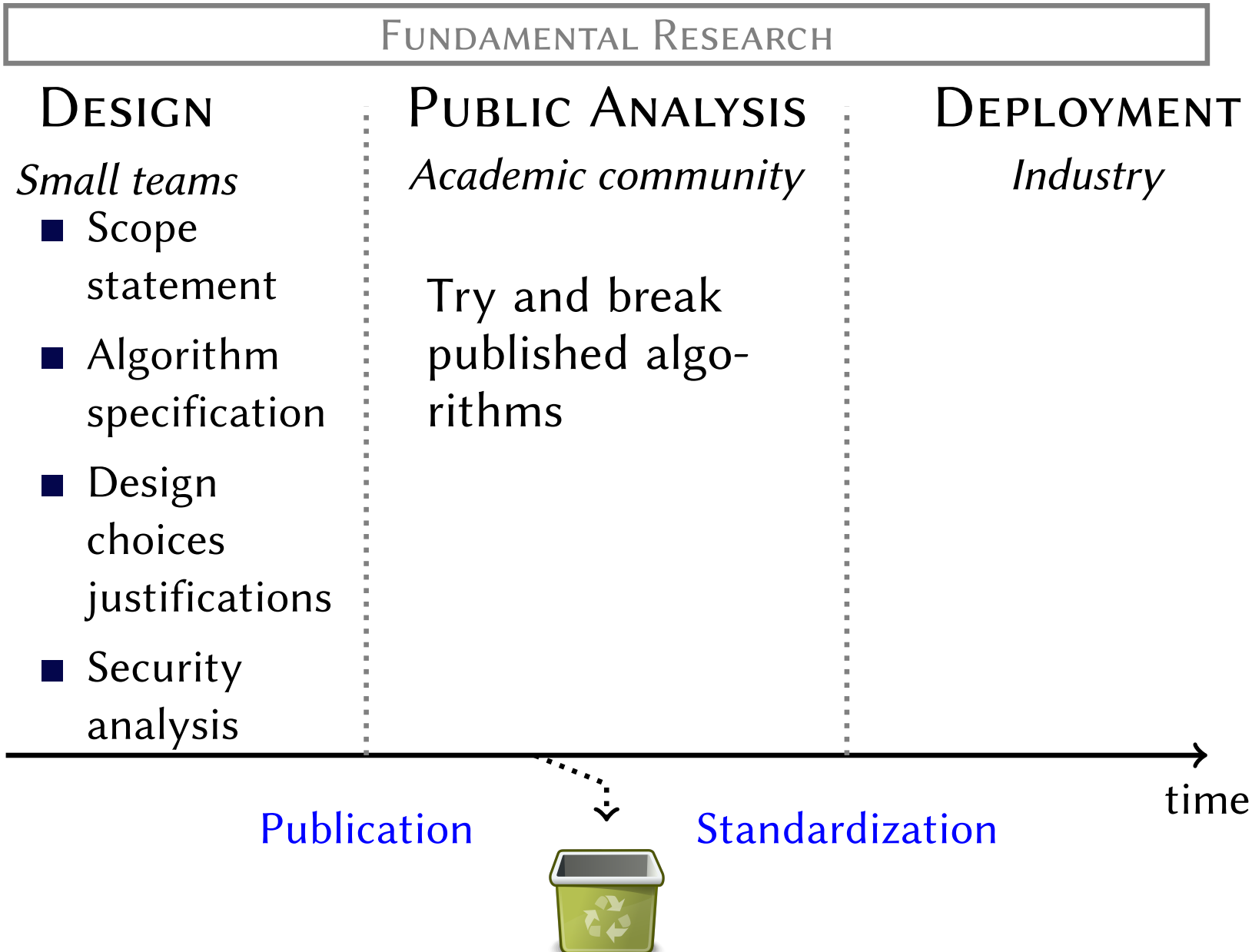
"Cryptographic Pipeline"



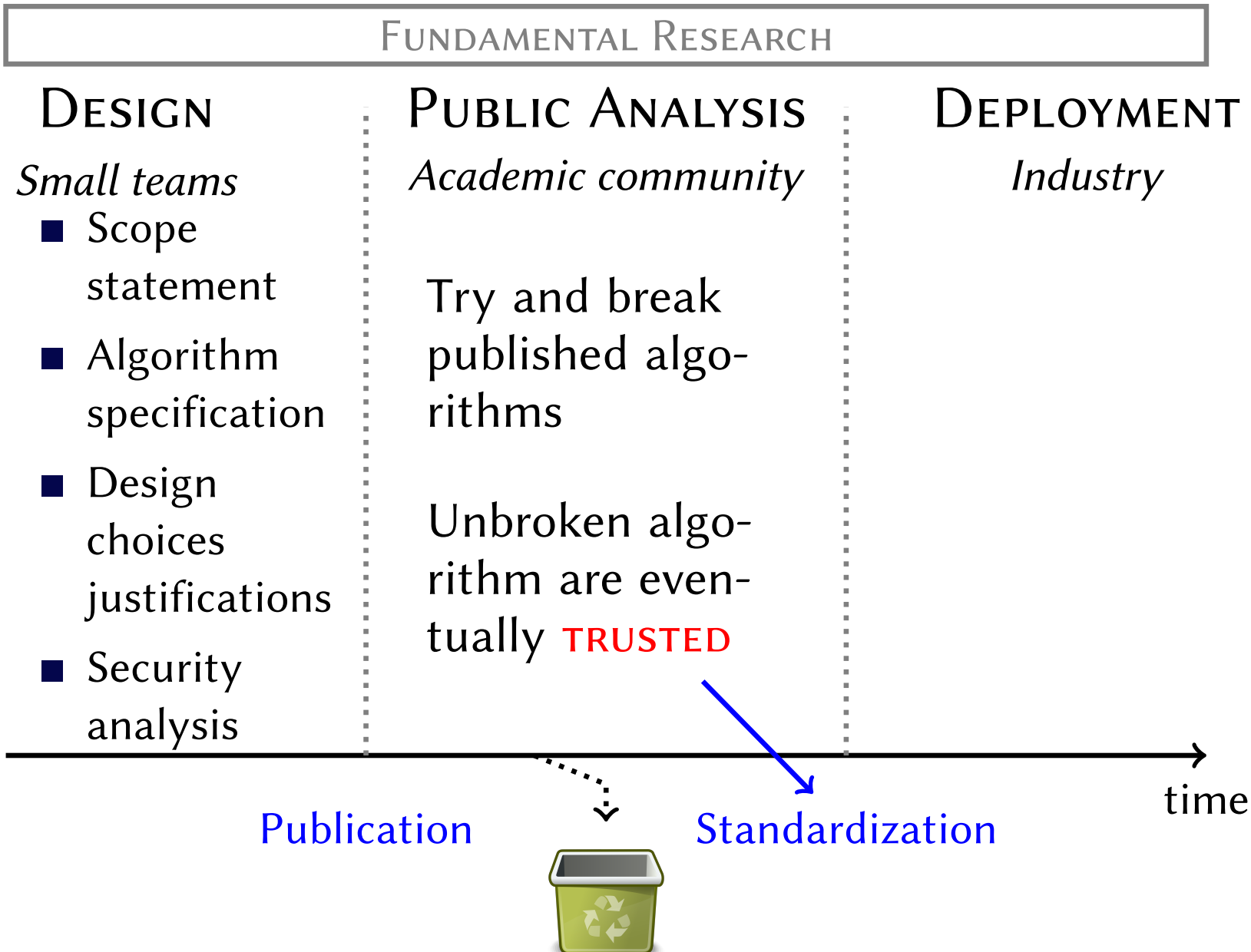
"Cryptographic Pipeline"



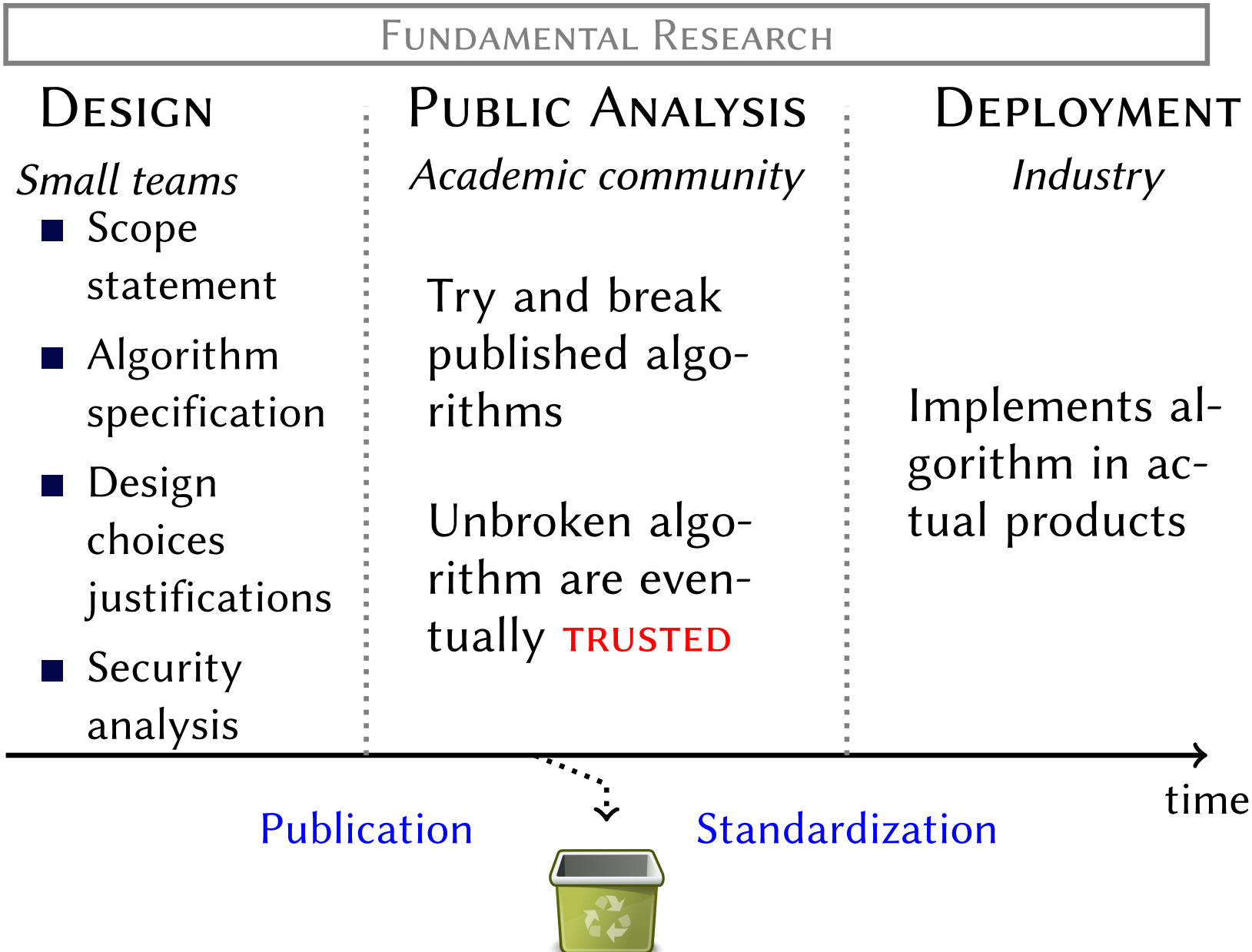
"Cryptographic Pipeline"



"Cryptographic Pipeline"



"Cryptographic Pipeline"



What about my thesis?

What about my thesis?

Funded by the FNR (ACRYPT Project)

3 Different Directions

Lightweight Cryptography

- 5 papers (FSE, ASIACRYPT, JoCEn), 2 invited talks
- 1 new block cipher

3 Different Directions

Lightweight Cryptography

- 5 papers (FSE, ASIACRYPT, JoCEn), 2 invited talks
- 1 new block cipher

S-Box Reverse-Engineering

- 8 conference papers (CRYPTO, EUROCRYPT...), 7 invited talks
- Discussions with ISO

3 Different Directions

Lightweight Cryptography

- 5 papers (FSE, ASIACRYPT, JoCEn), 2 invited talks
- 1 new block cipher

S-Box Reverse-Engineering

- 8 conference papers (CRYPTO, EUROCRYPT...), 7 invited talks
- Discussions with ISO

Purposefully Hard Cryptography

- 1 paper (ASIACRYPT)
- 1 patent (+1 paper under submission)

Outline

Outline

Internet of Things

Everything is being connected to the internet.

Internet of Things

Everything

Internet of Things

Everything

Internet of Things

Everything

Security

"In IoT, the S is for Security."

- Internet-enabled devices have security flaws.
- Security is an afterthought (at best).

Security

"In IoT, the S is for Security."

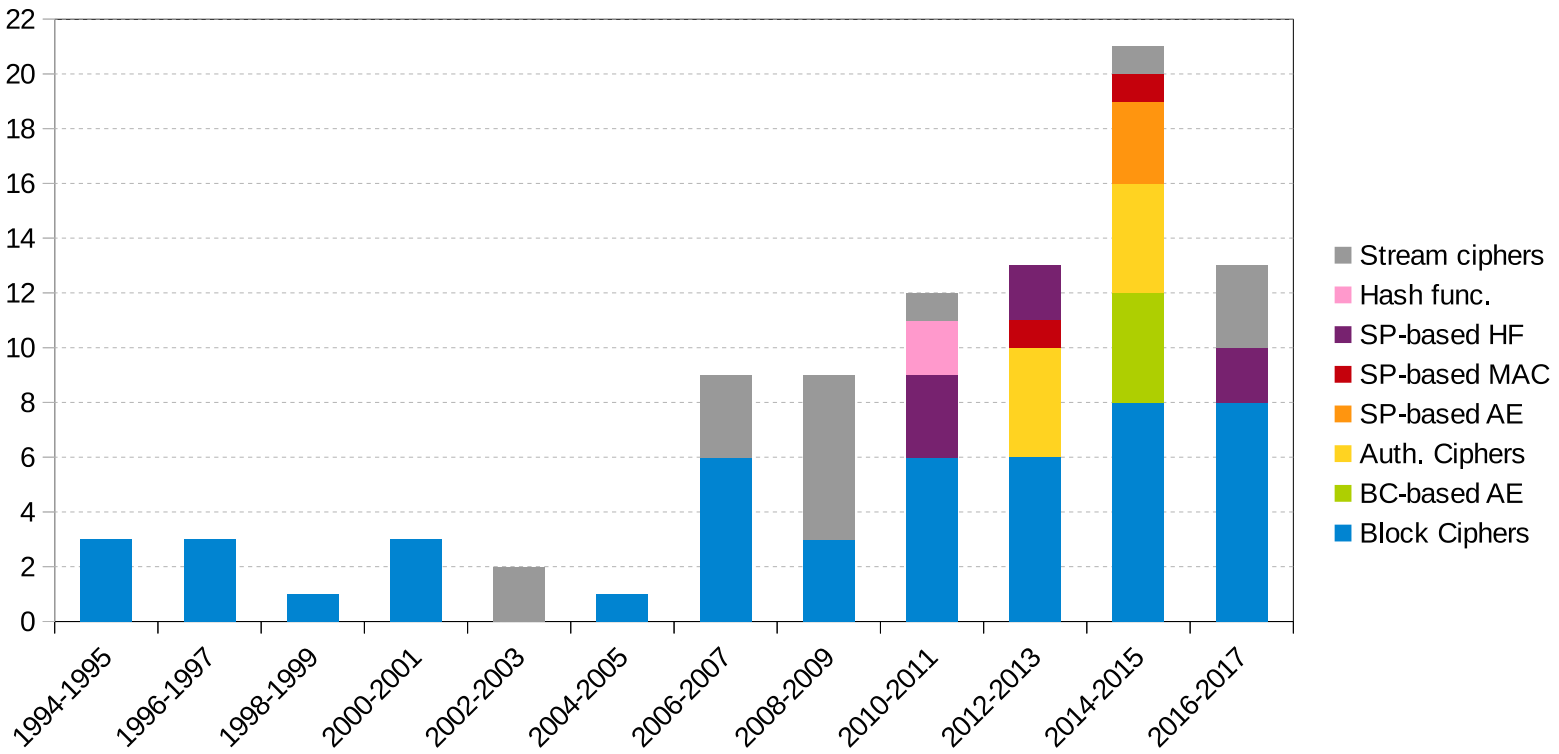
- Internet-enabled devices have security flaws.
- Security is an afterthought (at best).
- Security has a cost in terms of engineering...
- ... and computationnal resources!

Lightweight Cryptography

Lightweight cryptography uses little resources.

Lightweight Cryptography

Lightweight cryptography uses little resources.



LWC is a very active research area!

Overview

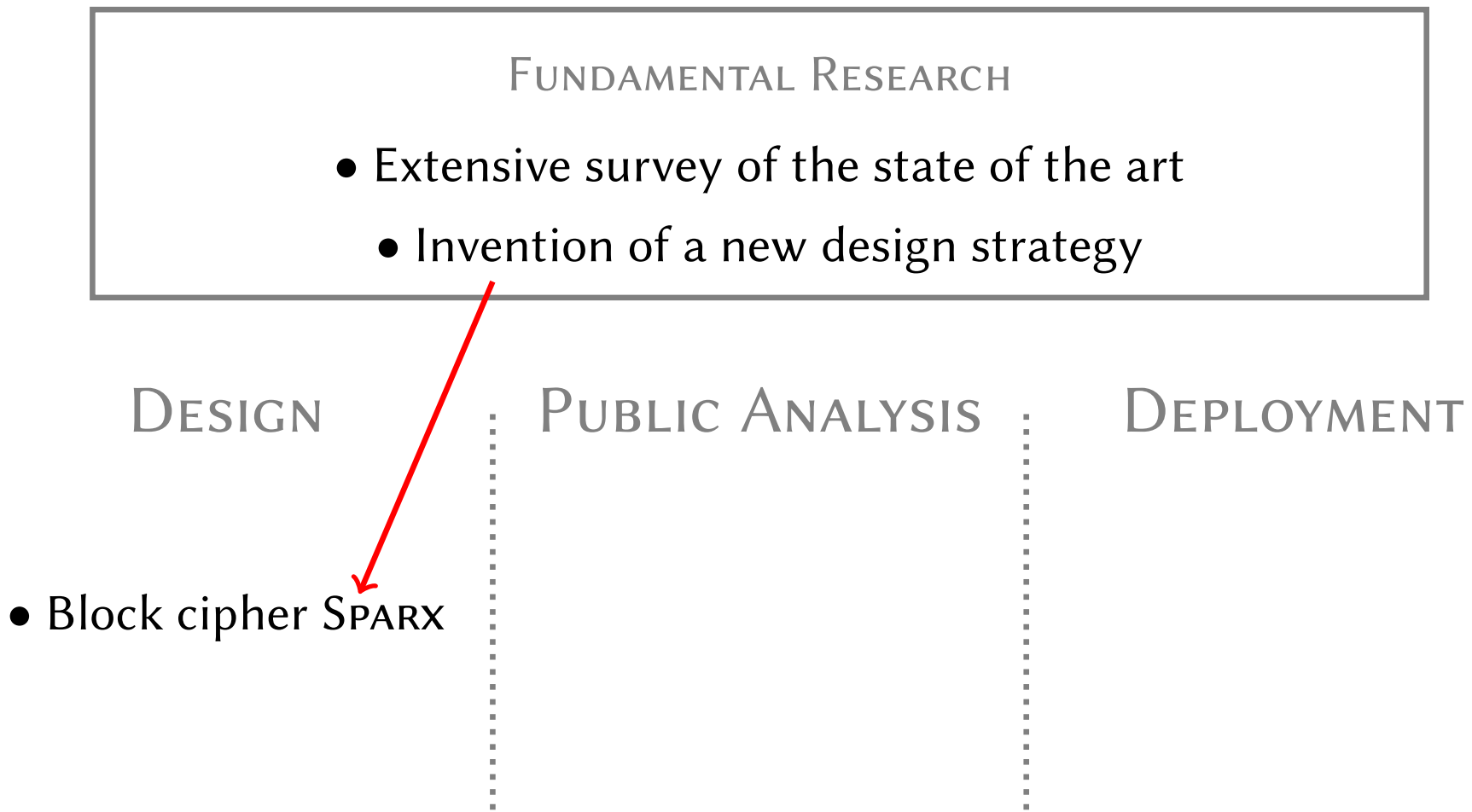
Overview

Fundamental Research

- Extensive survey of the state of the art

Design | Public Analysis | Deployment

Overview


Fundamental Research
• Extensive survey of the state of the art
• Invention of a new design strategy
Design
Public Analysis
Deployment
• Block cipher Sparx

Overview

Fundamental Research

- Extensive survey of the state of the art
- Invention of a new design strategy

Design

- Block cipher Sparx

Public Analysis

- Attacks on Gluon
- Results on Prince
- Results on Twine

Deployment

Highlights

Attacks on PRINCE

- We won round 1 of the "PRINCE challenge"
- The corresponding paper was selected in the top 3 papers at FSE'15;

Highlights

Attacks on PRINCE

- We won round 1 of the "PRINCE challenge"
- The corresponding paper was selected in the top 3 papers at FSE'15;

SPARX

- First *ARX-based* block cipher proven secure against some attacks.
- Design strategy re-used by third parties from Waterloo (Canada) to build *sLiSCP*

Highlights

Attacks on PRINCE

- We won round 1 of the "PRINCE challenge"
- The corresponding paper was selected in the top 3 papers at FSE'15;

SPARX

- First *ARX-based* block cipher proven secure against some attacks.
- Design strategy re-used by third parties from Waterloo (Canada) to build *sLiSCP*

NIST

- Survey greatly appreciated (and cited) by NIST in their ongoing standardization effort
- I presented SPARX at a NIST workshop

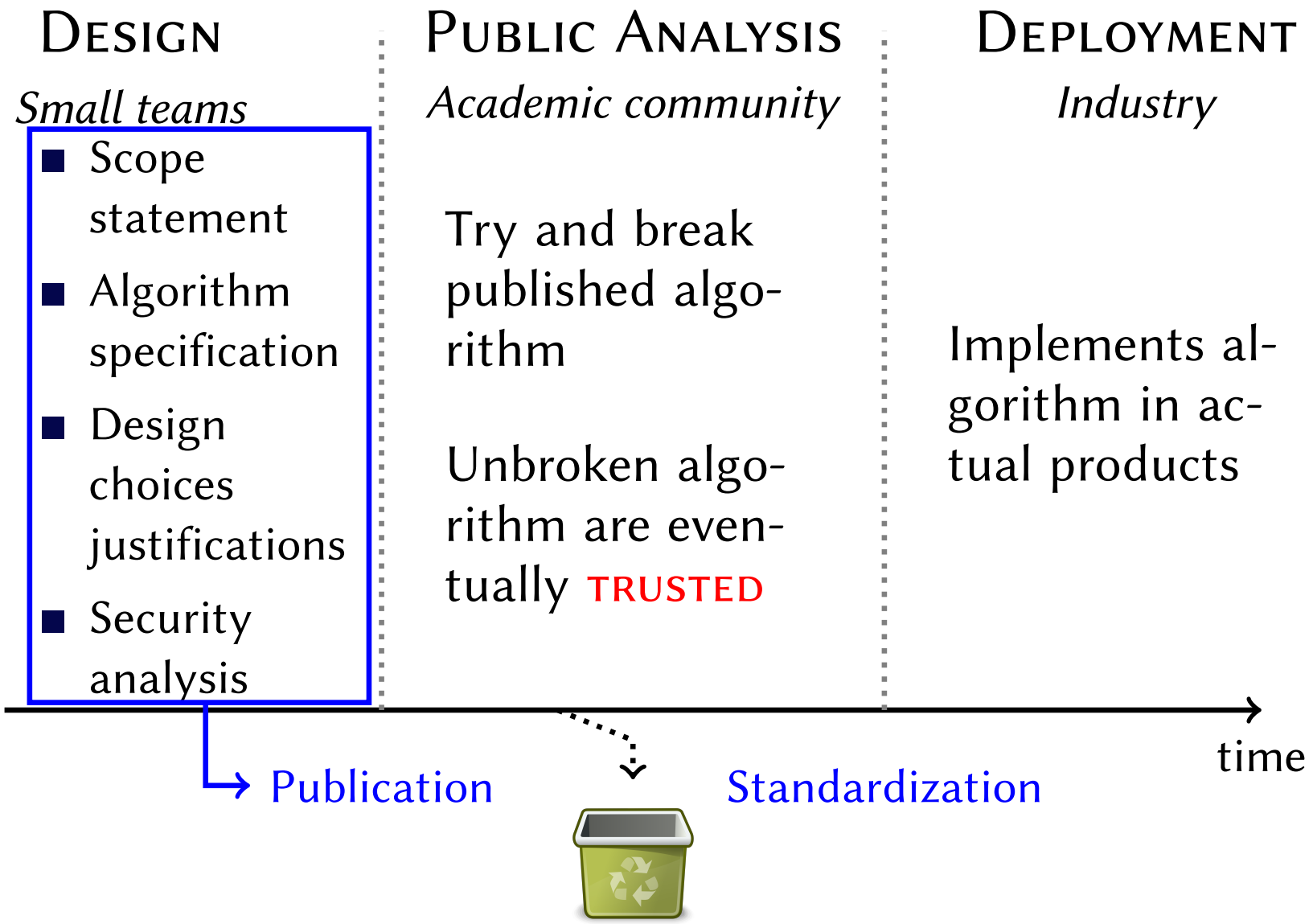
Outline

What is an S-Box?

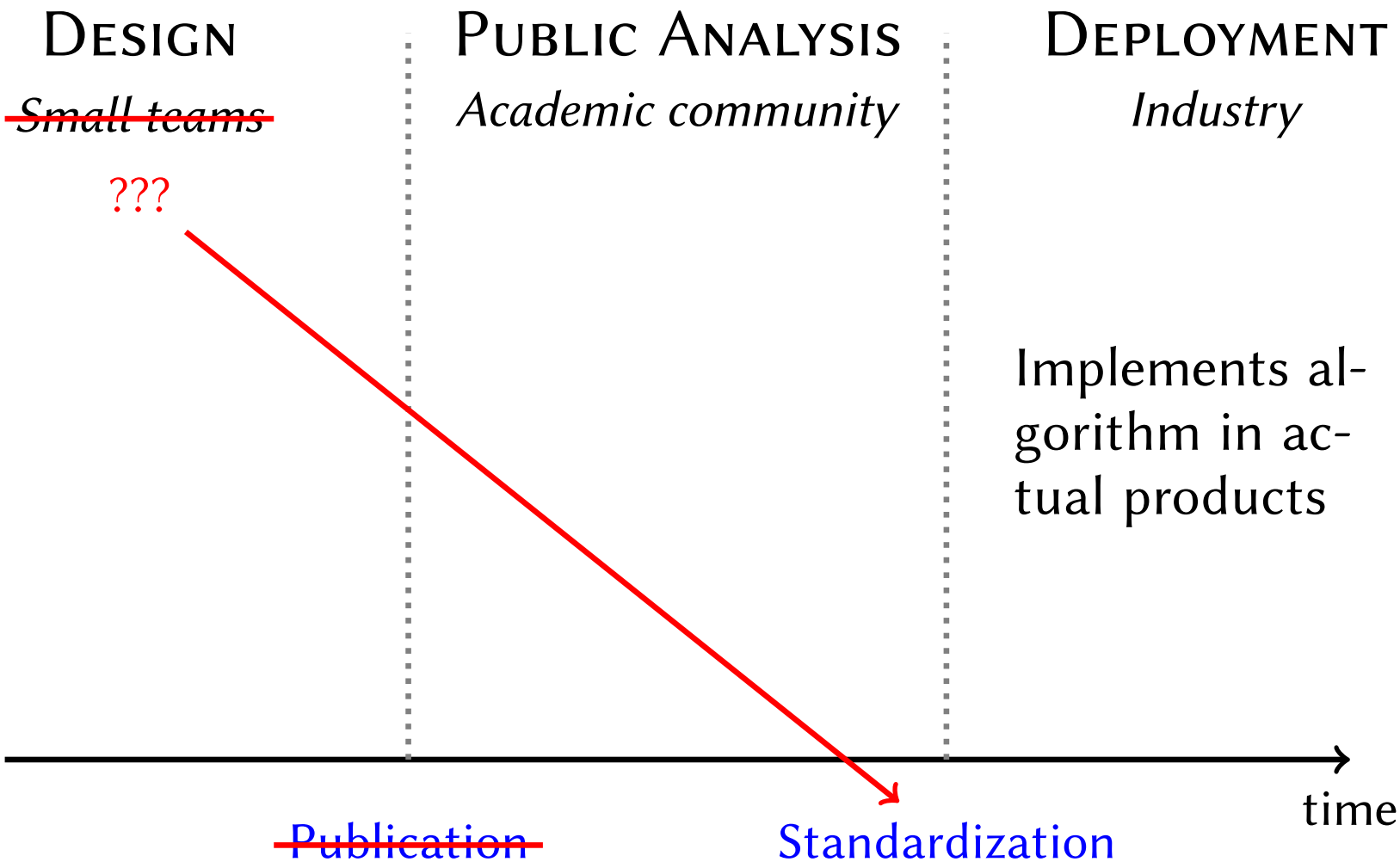
π' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241. 187, 20, 205, 95, 193, 249, 24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171, 242, 42, 104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18, 191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144, 202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9, 91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182).

The “S-Box” of the last Russian standards

Breaking the Pipeline



Breaking the Pipeline



The Need for Reverse-Engineering

A malicious designer can easily hide a structure in an S-Box.

The Need for Reverse-Engineering

A malicious designer can easily hide a structure in an S-Box.

To keep an advantage in implementation...

The Need for Reverse-Engineering

A malicious designer can easily hide a structure in an S-Box.

To keep an advantage in implementation...
... or an advantage in cryptanalysis (backdoor).

Kuznyechik/Stribog

Stribog

Type Hash function

Publication 2012

Kuznyechik

Type Block cipher

Publication 2015

Kuznyechik/Stribog

Stribog

Type Hash function

Publication 2012

Kuznyechik

Type Block cipher

Publication 2015

Common ground

- Both are standard symmetric primitives in Russia.
- Both were designed by the FSB (TC26).
- Both use the same 8×8 S-Box, π.

How?

Given an S-Box... Where do we even start?

Fourier to the Rescue

Linear Approximations Table (LAT)

The LAT of $S : \{0,1\}^n \to \{0,1\}^n$ is a $2^n \times 2^n$ matrix such that

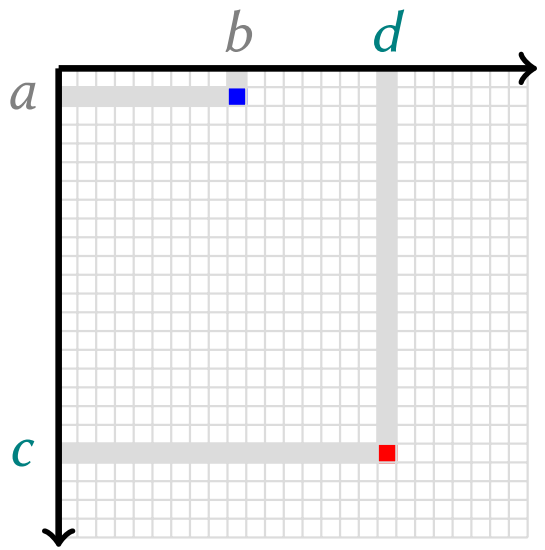
$$\mathrm{LAT}_S[a,b] = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x \oplus b \cdot S(x)} .$$

Fourier to the Rescue

Linear Approximations Table (LAT)

The LAT of $S : \{0,1\}^n \to \{0,1\}^n$ is a $2^n \times 2^n$ matrix such that

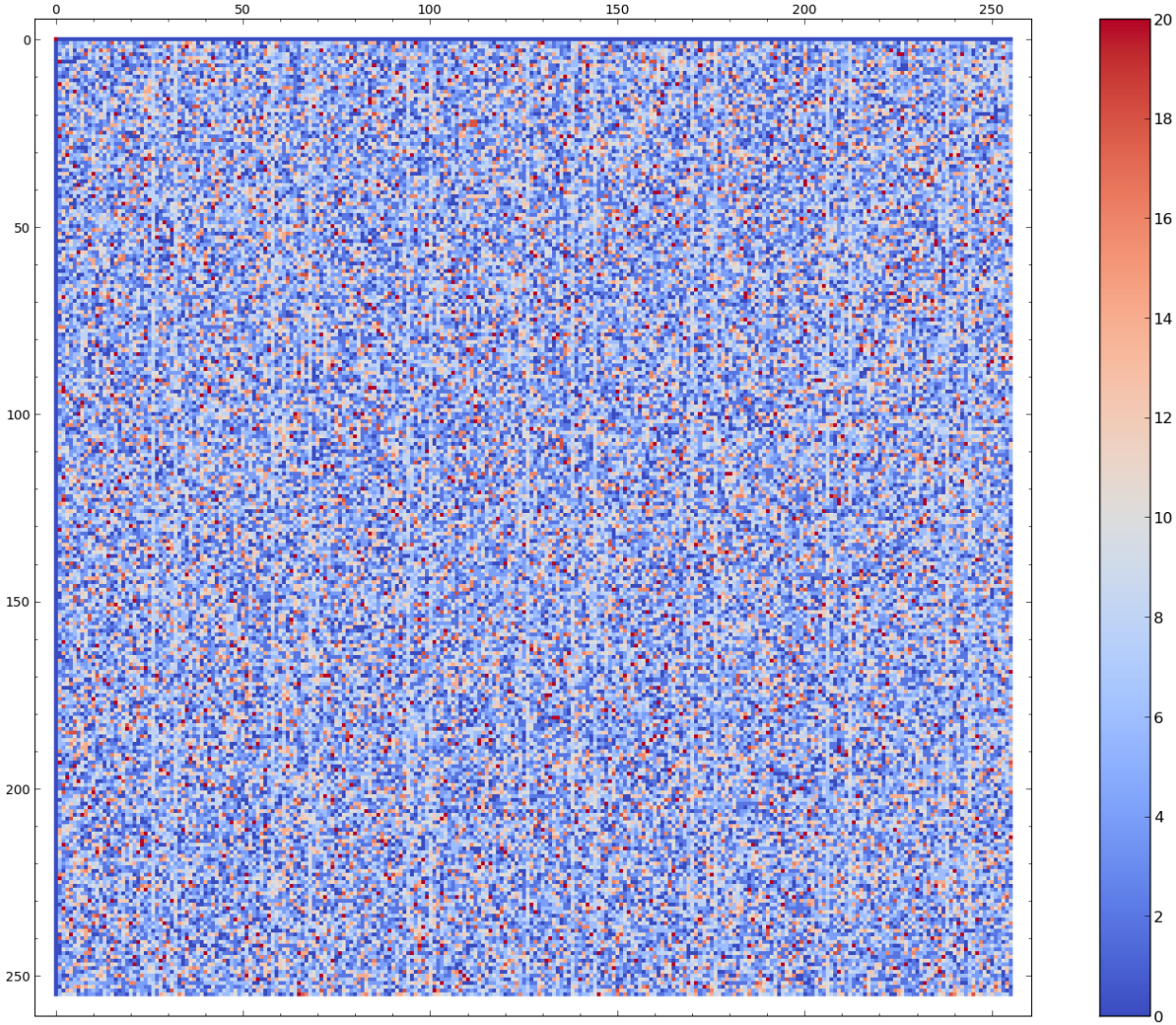
$$\mathrm{LAT}_S[a,b] = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x \oplus b \cdot S(x)} .$$



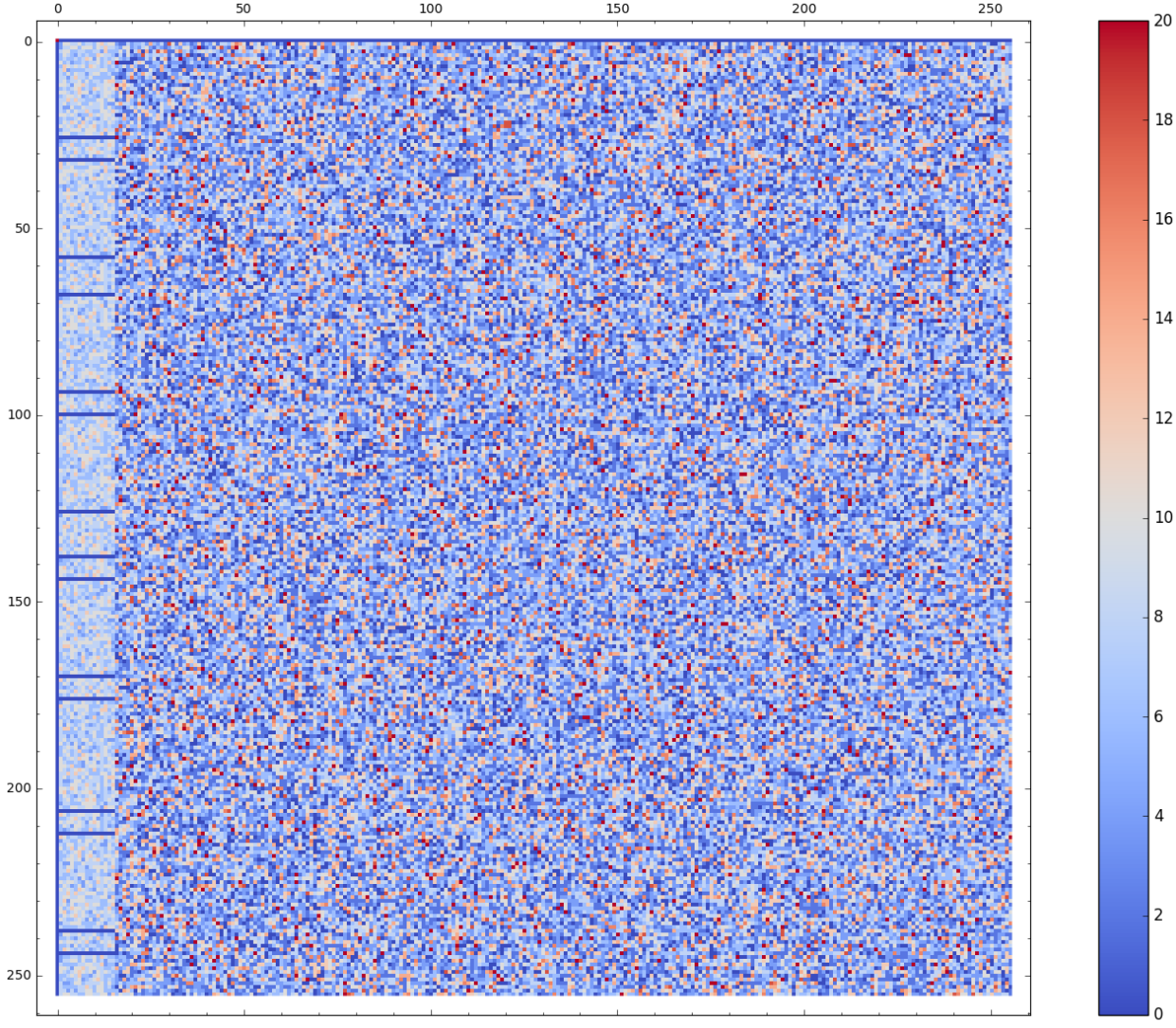
$$|\mathrm{LAT}_S[a,b]| = 0$$

$$|\mathrm{LAT}_S[c,d]| \geq 20$$

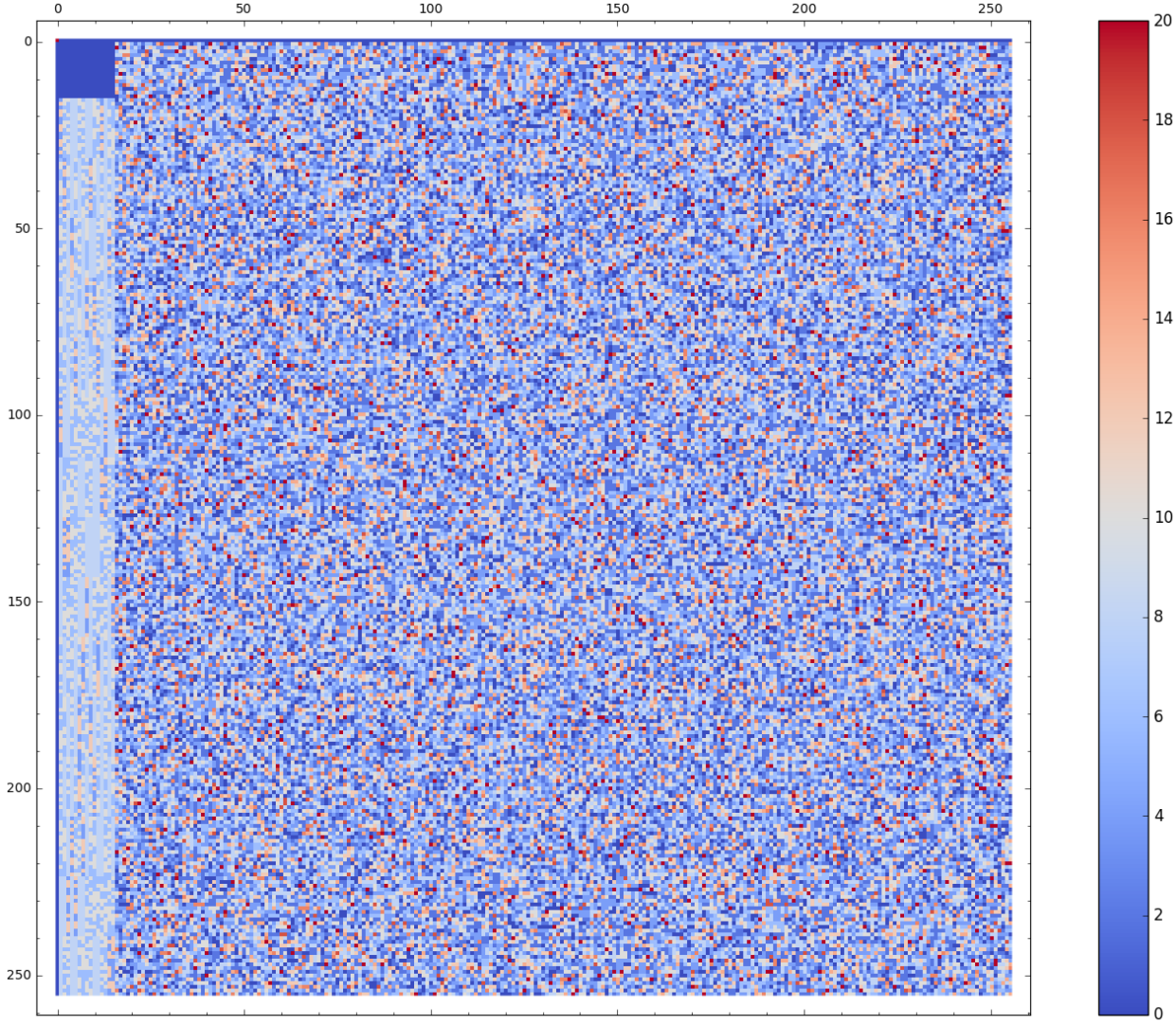
The LAT of π



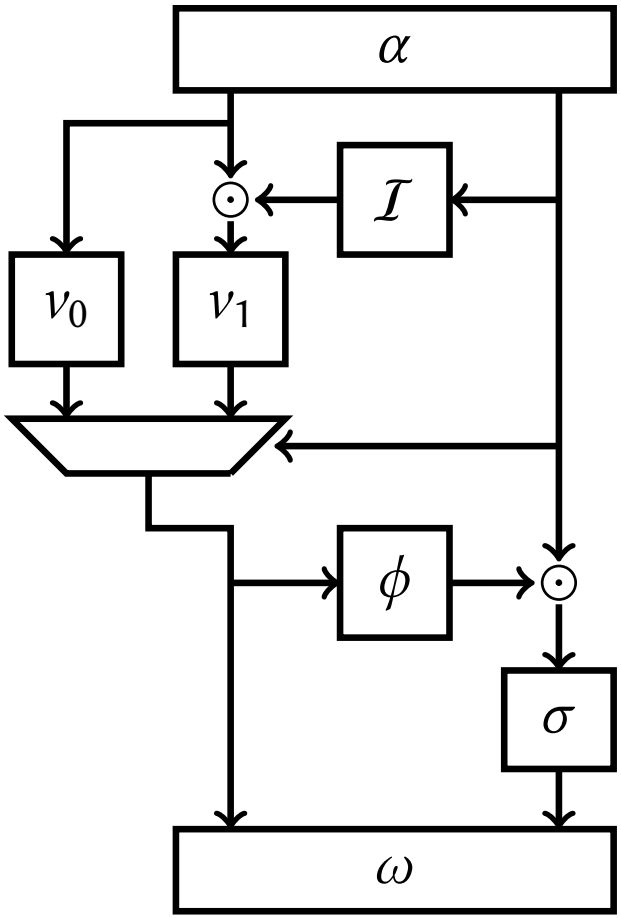
The LAT of π (reordered columns)



The LAT of $\eta \circ \pi \circ \mu$



Final Decomposition Number 1



- $\odot$ Multiplication in $\mathbb{F}_{2^4}$
- α Linear permutation
- $\mathcal{I}$ Inversion in $\mathbb{F}_{2^4}$
- ν_0, ν_1, σ 4×4 permutations
- ϕ 4×4 function
- ω Linear permutation

S-Box Reverse-Engineering: Summary

- Set up a process and tools to recover hidden structures and/or design criteria for S-Boxes.
- Successful applications to Streebog/Kuznyechik (FSB), Skipjack (NSA)... and a theorem!
- Found new cryptographic attacks.

S-Box Reverse-Engineering: Summary

- Set up a process and tools to recover hidden structures and/or design criteria for S-Boxes.
- Successful applications to Streebog/Kuznyechik (FSB), Skipjack (NSA)... and a theorem!
- Found new cryptographic attacks.
- Hopefully, deterred publications of unjustified algorithms.

S-Box Reverse-Engineering: Summary

- Set up a process and tools to recover hidden structures and/or design criteria for S-Boxes.
- Successful applications to Streebog/Kuznyechik (FSB), Skipjack (NSA)... and a theorem!
- Found new cryptographic attacks.
- Hopefully, deterred publications of unjustified algorithms.
- Caught the attention of the community: I gave many invited talks on this topic.

Outline

Conclusion

- My co-authors and I made significant contribution to lightweight cryptography.

Conclusion

- My co-authors and I made significant contribution to lightweight cryptography.
- We pioneered the field of S-Box reverse-engineering and obtained important results in cryptography *and* in mathematics.

Conclusion

- My co-authors and I made significant contribution to lightweight cryptography.
- We pioneered the field of S-Box reverse-engineering and obtained important results in cryptography *and* in mathematics.
- We worked on another topic ("Purposefully hard cryptography", useful for crypto-currencies, DRM systems, spam mitigation...).

Conclusion

- My co-authors and I made significant contribution to lightweight cryptography.
- We pioneered the field of S-Box reverse-engineering and obtained important results in cryptography *and* in mathematics.
- We worked on another topic ("Purposefully hard cryptography", useful for crypto-currencies, DRM systems, spam mitigation...).

I am grateful to...

- my PhD advisor Alex Biryukov,
- the uni.lu for providing such a good research environment,

I am grateful to...

- my PhD advisor Alex Biryukov,
- the uni.lu for providing such a good research environment,
- my colleagues and co-authors,

I am grateful to...

- my PhD advisor Alex Biryukov,
- the uni.lu for providing such a good research environment,
- my colleagues and co-authors,
- my friends and family,

I am grateful to...

- my PhD advisor Alex Biryukov,
- the uni.lu for providing such a good research environment,
- my colleagues and co-authors,
- my friends and family,
- the *Amis de l'Université* and their sponsors...

... and to you for listening!