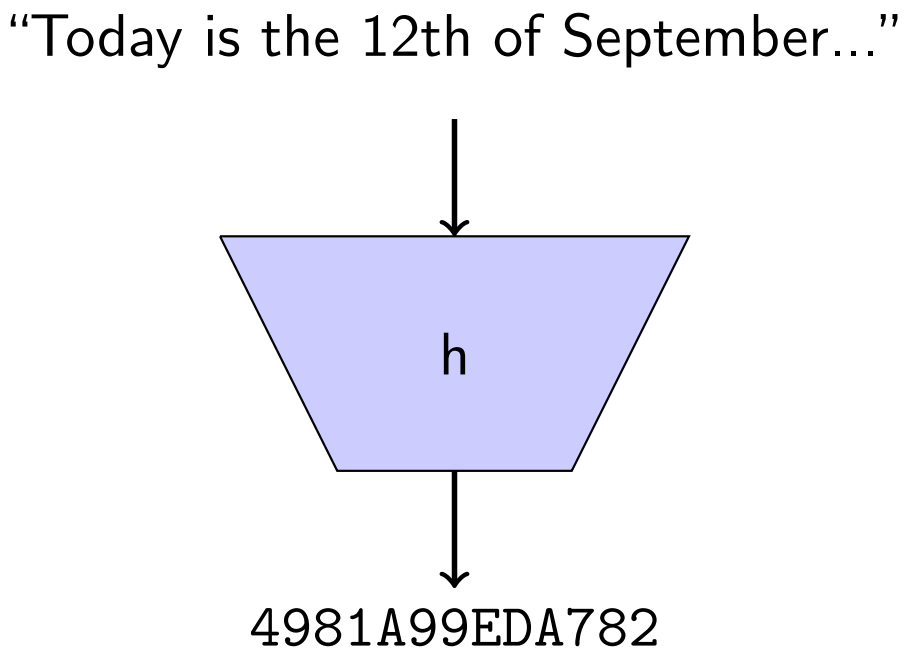
Practical attacks on AES-like cryptographic hash functions

Stefan Kölbl, Christian Rechberger

DTU - Technical University of Denmark

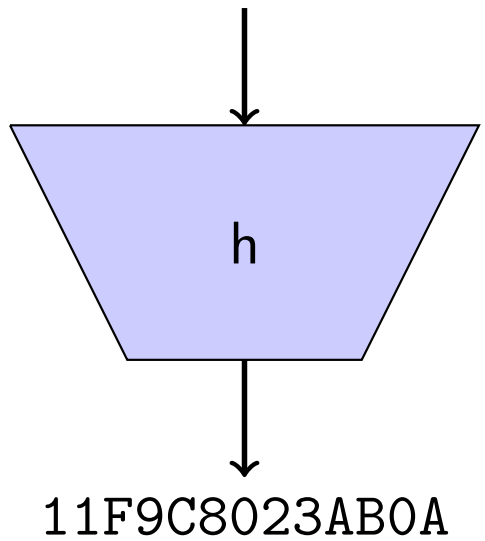
September 12, 2014

Cryptographic Hash Functions



Cryptographic Hash Functions

"Today is the 13th of September..."



Cryptographic Hash Functions

Applications:

- Message Integrity
- Digital Signature Schemes
- Password Protection
- Key Derivation
- Payment Schemes (Bitcoin)
- ...

Features:

- No secret parameter is involved.
- Fast to compute.

Cryptographic Hash Functions

Security Requirements

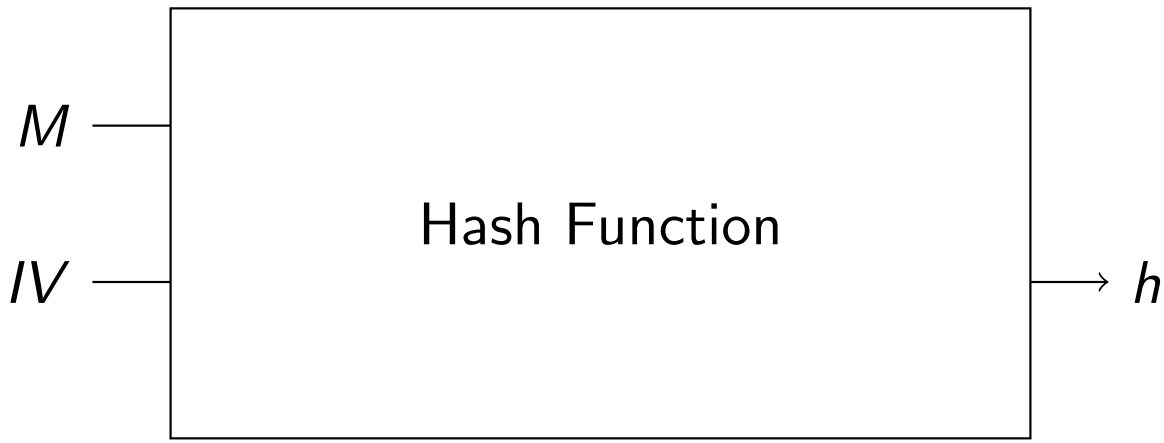
- Preimage Resistance:
  Given $h(x)$ find x
- Second-Preimage Resistance:
  Given $x, h(x)$ find $y \neq x$ s.t. $h(x) = h(y)$
- Collision Resistance:
  Find x, y with $x \neq y$ s.t. $h(x) = h(y)$

Generic Attack

Complexity 2^n for (second) preimage and $2^{n/2}$ for collisions.

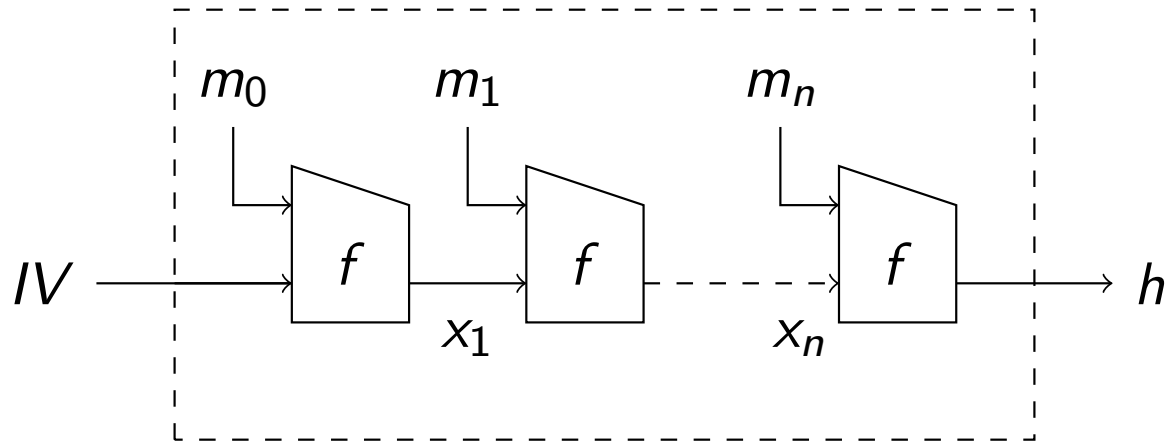
Cryptographic Hash Functions

Security Properties



Cryptographic Hash Functions

Security Properties



Analyze the collision resistance of the compression function f

- **semi-free-start collision**: Find $\{m_i, m_i', x_i\}$ s.t. $f(m_i, x_i) = f(m_i', x_i)$
- **free-start collision**: Find $\{m_i, m_i', x_i, x_i'\}$ s.t. $f(m_i, x_i) = f(m_i', x_i')$

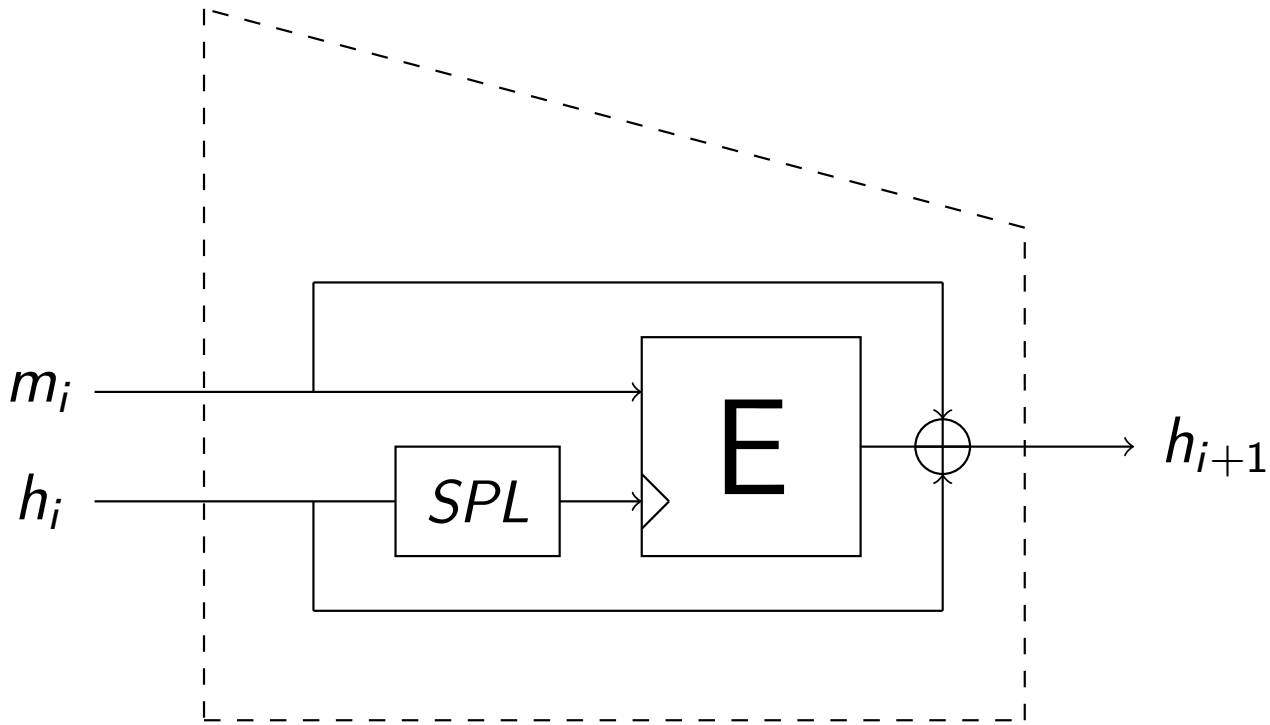
AES-based hash functions

Compression functions based on AES are common

- Whirlpool (ISO/IEC 10118-3)
  - Maelstrom
  - Whirlwind
- Streebog (GOST R 34.11-2012)
- SHA-3 Competiton
  - Grøstl
  - ECHO
  - LANE

GOST R 34.11-2012

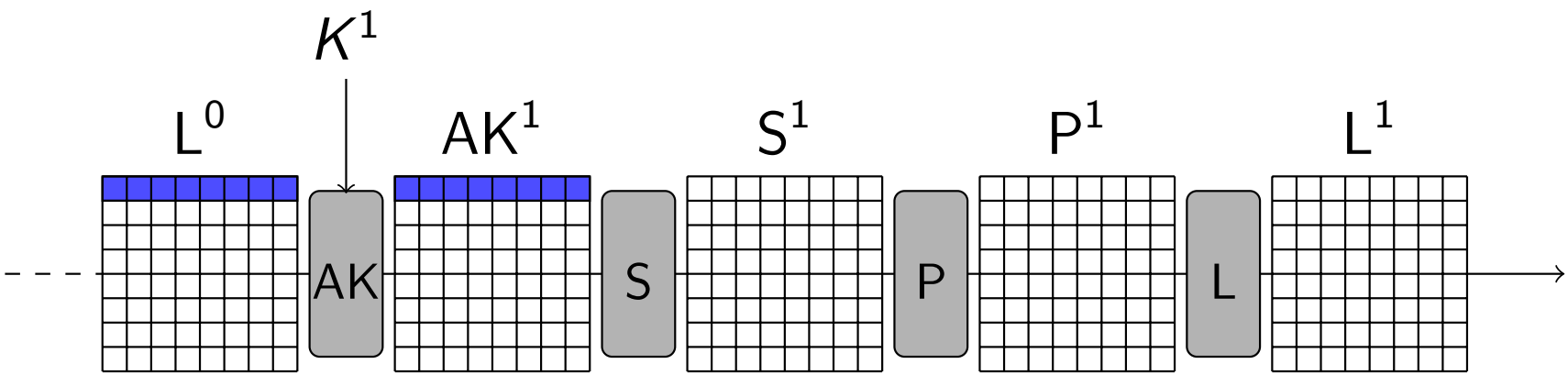
Compression Function



GOST R 34.11-2012

Block Cipher **E** with 12 rounds of

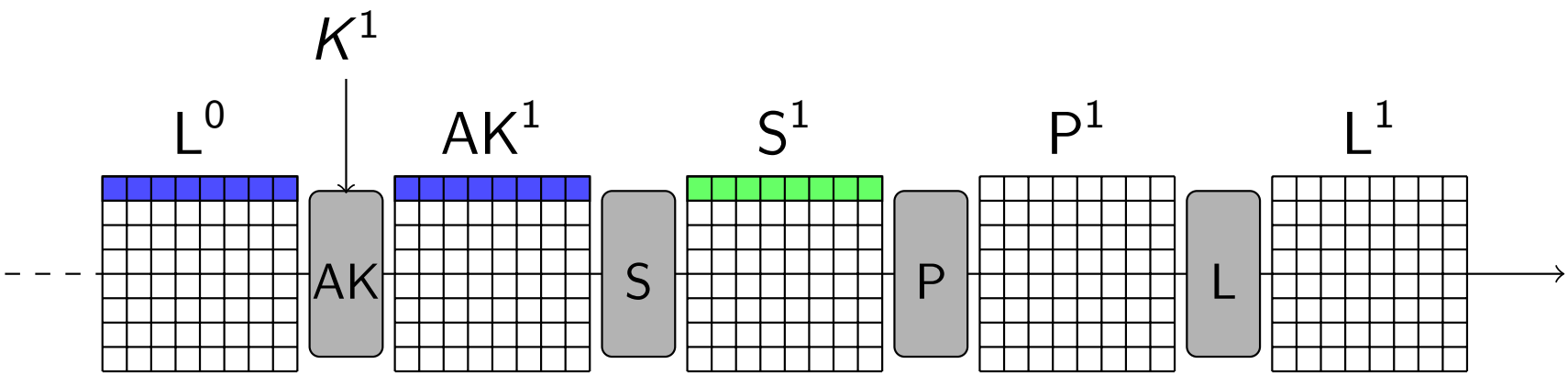
- **AK** Adds the key byte-wise by XORing it to the state.
- **S** Substitutes each byte of the state independently using an 8-bit S-Box.
- **P** Transposes the state.
- **L** Multiplies each row by an 8×8 MDS matrix.



GOST R 34.11-2012

Block Cipher **E** with 12 rounds of

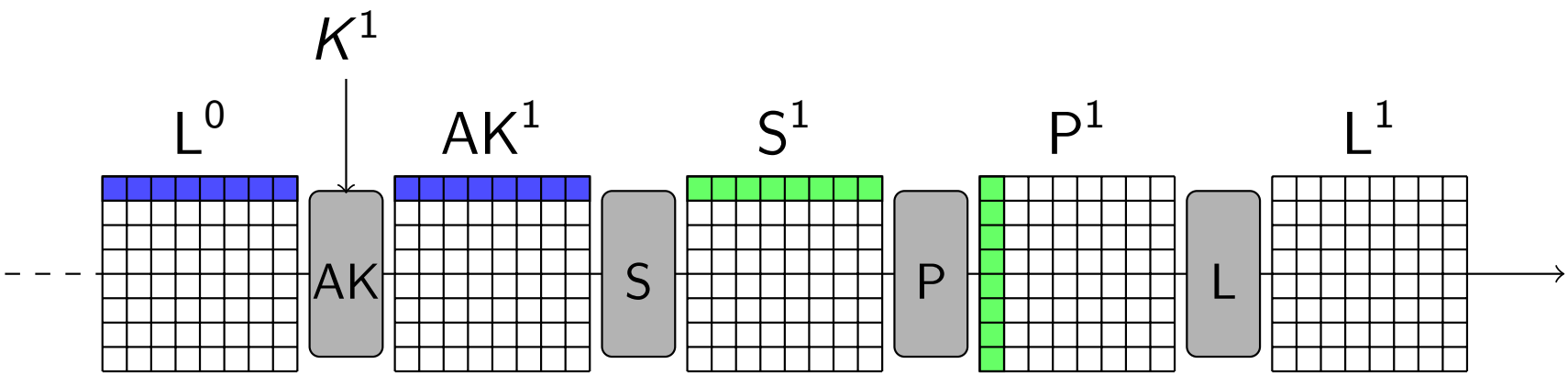
- **AK** Adds the key byte-wise by XORing it to the state.
- **S** Substitutes each byte of the state independently using an 8-bit S-Box.
- **P** Transposes the state.
- **L** Multiplies each row by an 8×8 MDS matrix.



GOST R 34.11-2012

Block Cipher **E** with 12 rounds of

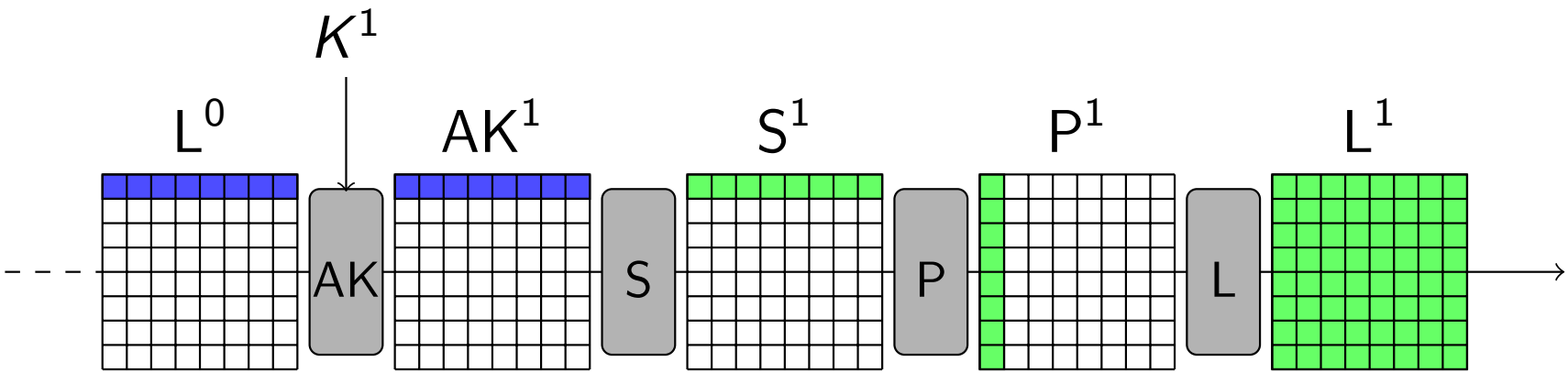
- **AK** Adds the key byte-wise by XORing it to the state.
- **S** Substitutes each byte of the state independently using an 8-bit S-Box.
- **P** Transposes the state.
- **L** Multiplies each row by an 8×8 MDS matrix.



GOST R 34.11-2012

Block Cipher **E** with 12 rounds of

- **AK** Adds the key byte-wise by XORing it to the state.
- **S** Substitutes each byte of the state independently using an 8-bit S-Box.
- **P** Transposes the state.
- **L** Multiplies each row by an 8×8 MDS matrix.



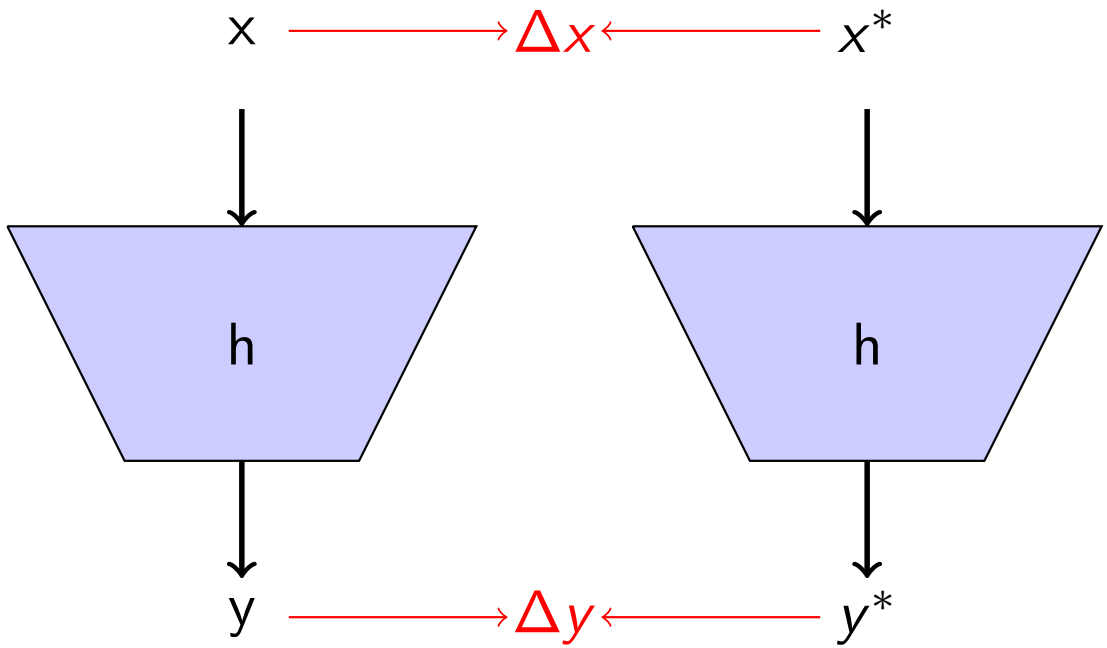
Related Work

Overview of practical attacks on the compression function

Function	Rounds	Time	Memory	Type	Reference
GOST R	4.5	2^{64}	2^{16}	collision	[WYW13]
	4.75	practical	2^{8}	near-collision	[AKY13]
	4	$2^{19.8}$	2^{16}	collision	this work
	4.5	$2^{19.8}$	2^{16}	collision	this work
	5.5	2^{64}	2^{64}	collision	[WYW13]
	6.5	2^{64}	2^{16}	collision	this work
Whirlpool	4	$2^{25.1}$	2^{16}	collision	this work
	6.5	$2^{25.1}$	2^{16}	near-collision	this work
	4	2^{8}	2^{8}	collision[1]	[WYW13]
	7	2^{64}	2^{8}	collision[1]	[SWWW12]

[1] free-start collision

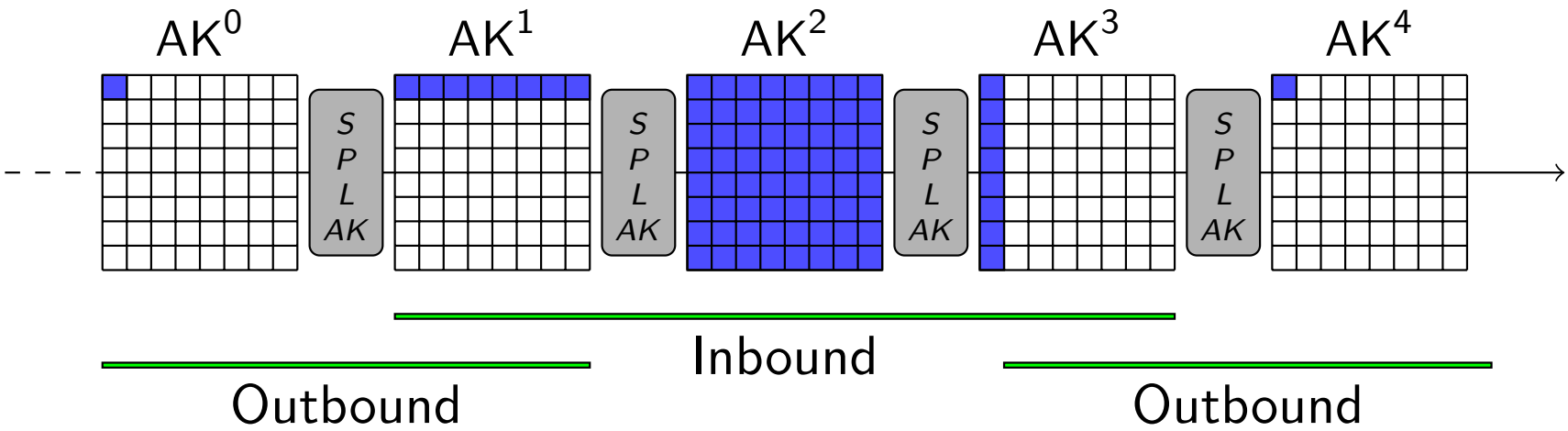
Differential Cryptanalysis



- $\Delta x \neq 0$ and $\Delta y = 0$ gives a collision.
- Find a differential characteristic leading to zero output difference.
- Find a confirming message pair.

Rebound Attacks

Powerful technique for analysis of hash functions [MRST09]



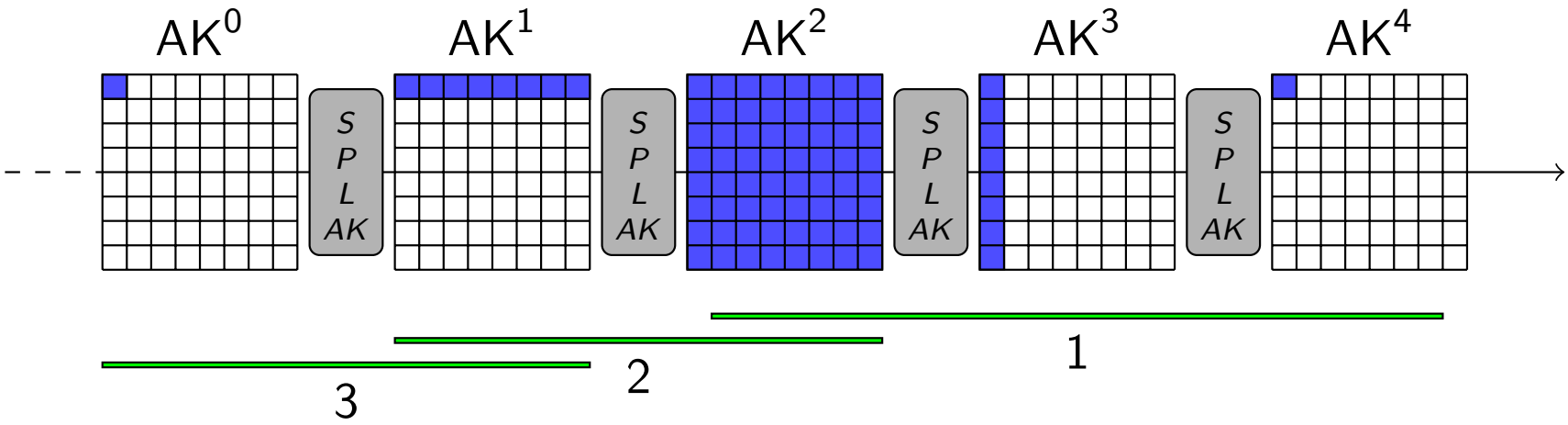
Two parts:

- Inbound phase: Match-in-the-middle
- Outbound phase: Probabilistic

Many improvements over the last few years...

Finding the characteristic

Technique similar to start-from-the-middle



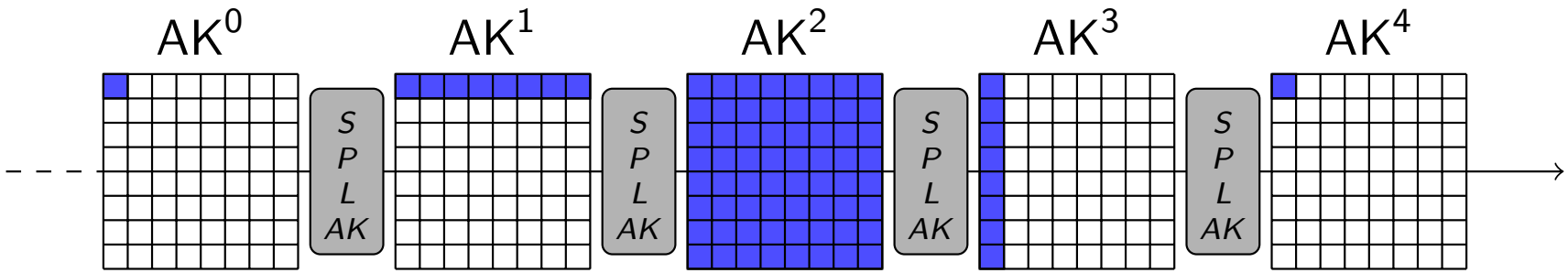
1. Propagate difference from AK^4 to S^2.
2. Choose differences in AK^2 to ensure 64–8 by using freedom of S-Box.
3. Solve 8–1 by swapping values $(a, b) \leftrightarrow (b, a)$.

Complexity

Finding the characteristic $2^{19.8}$

Finding the message pair

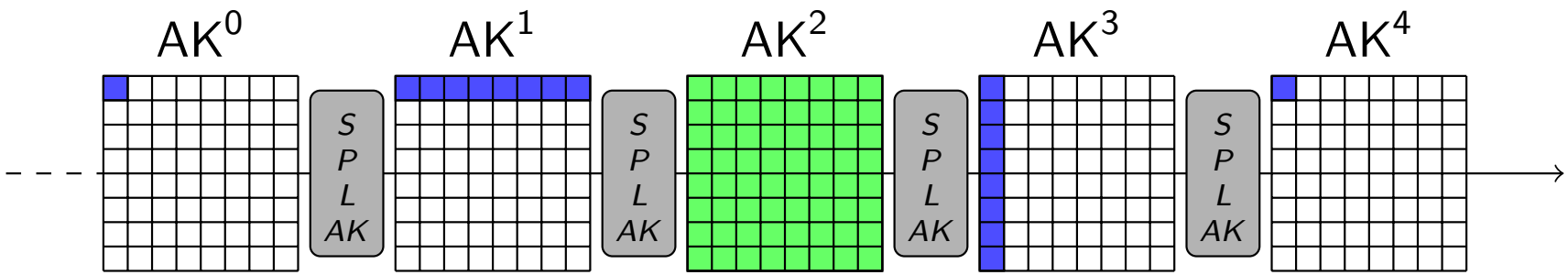
We need to fulfill conditions on 81 bytes.



- First we fix the values of AK^2 such that $S^2 = S(AK^2)$.
- This solves 64 byte conditions but uses all degrees of freedom we have for the state.

Finding the message pair

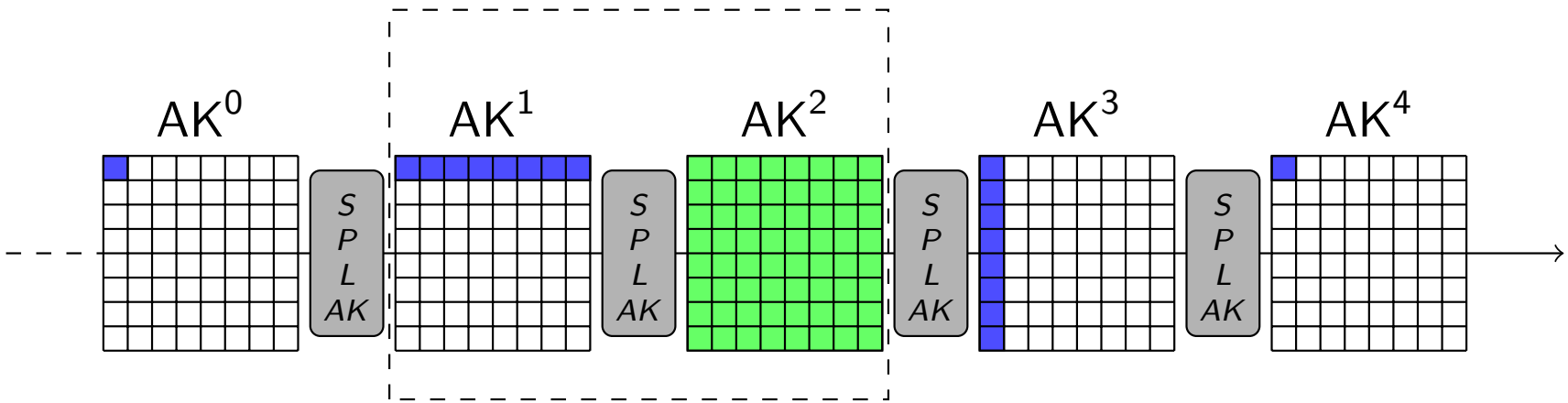
We need to fulfill conditions on 81 bytes.



- First we fix the values of AK^2 such that $S^2 = S(AK^2)$.
- This solves 64 byte conditions but uses all degrees of freedom we have for the state.

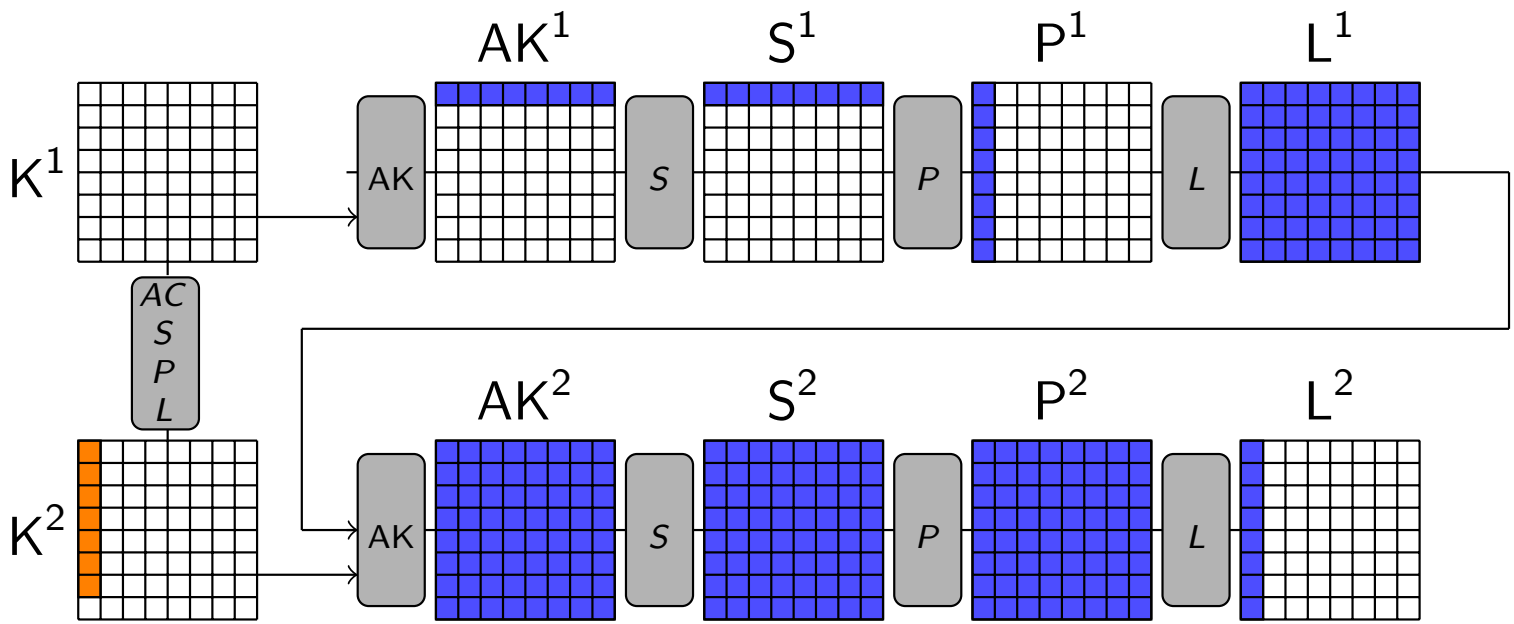
Finding the message pair

We need to fulfill conditions on 81 bytes.

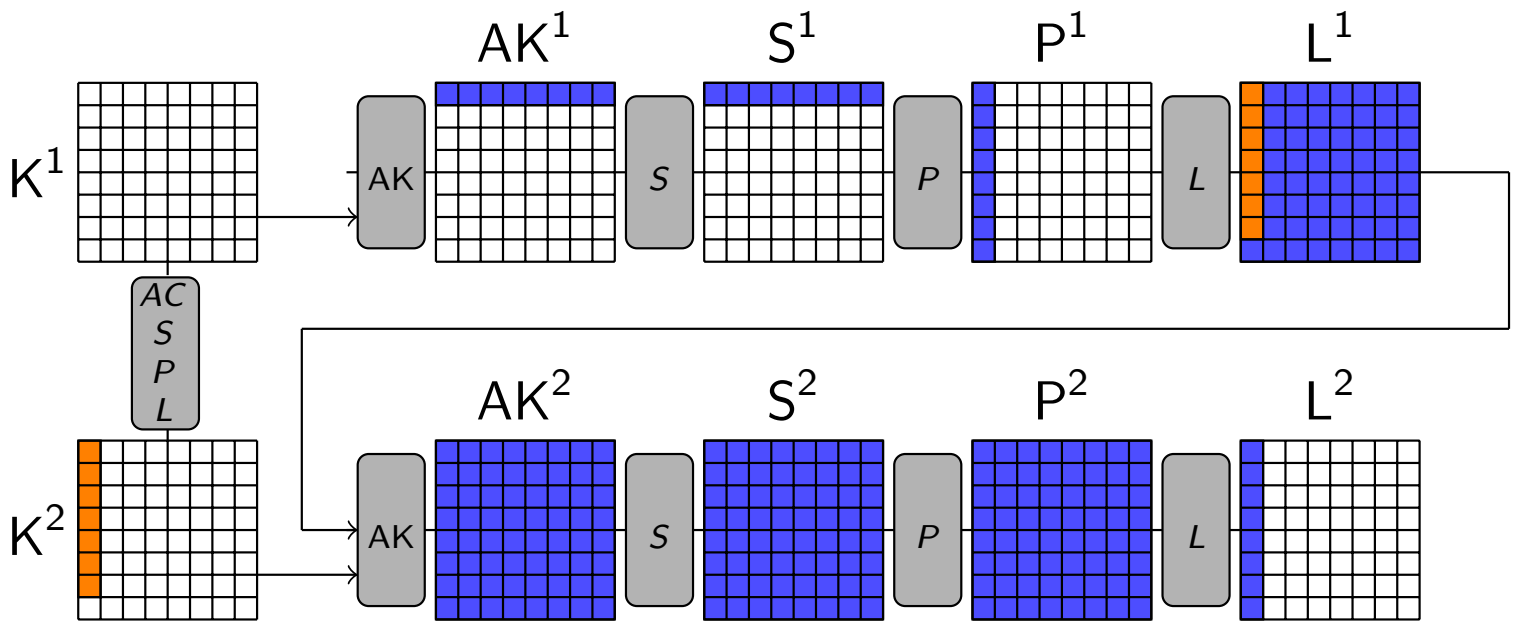


- How to solve the conditions for $AK^1 = S(S^1)$...

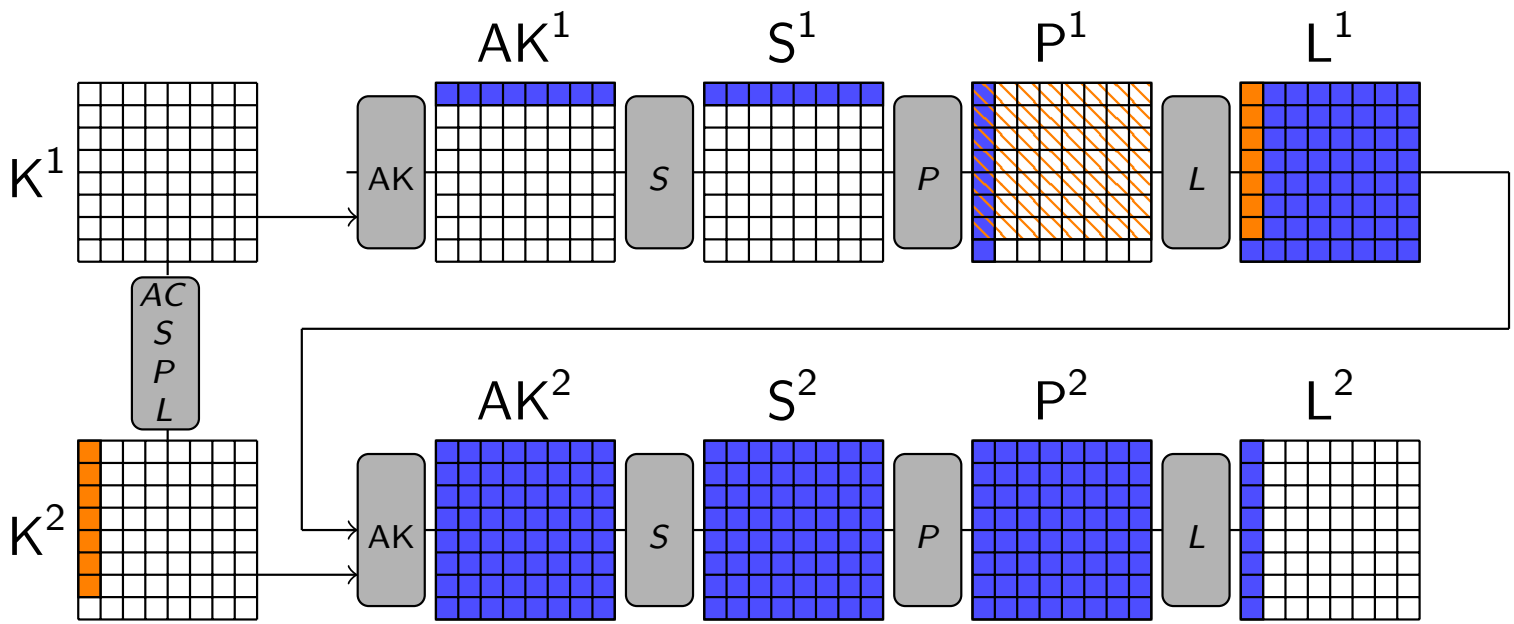
Finding the message pair



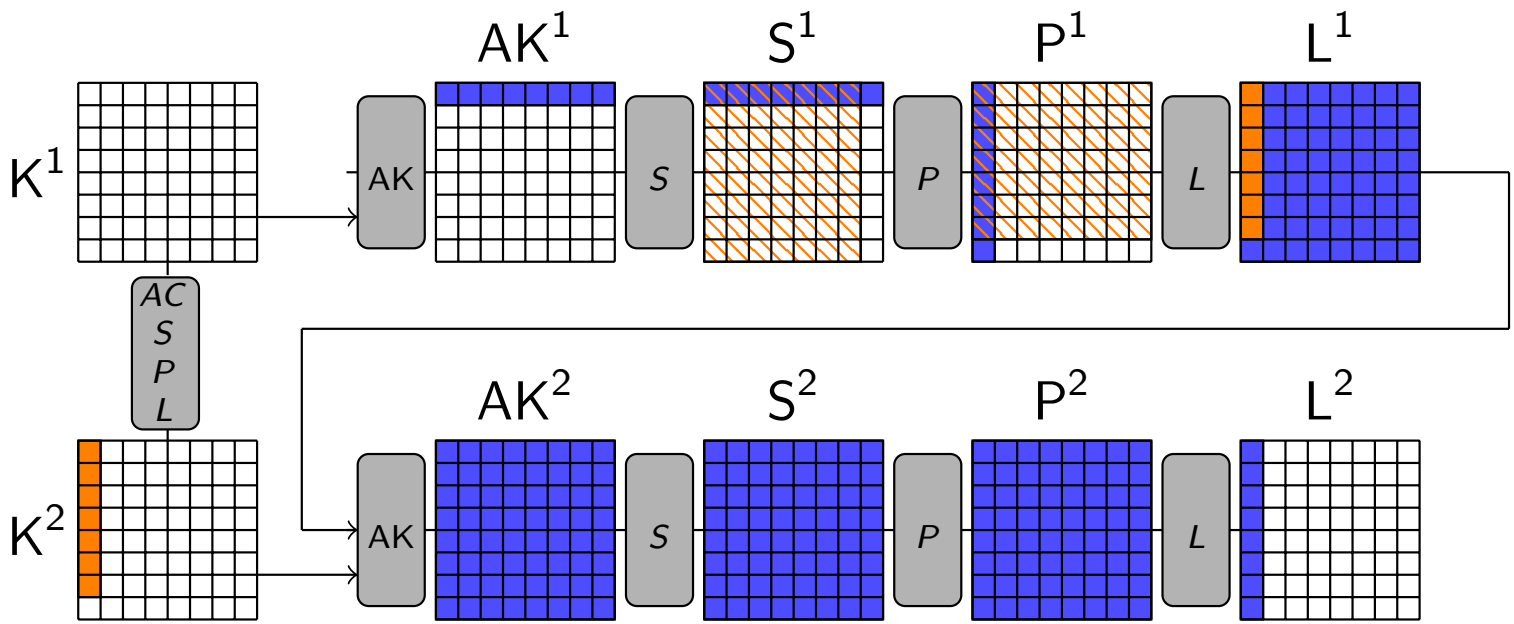
Finding the message pair



Finding the message pair

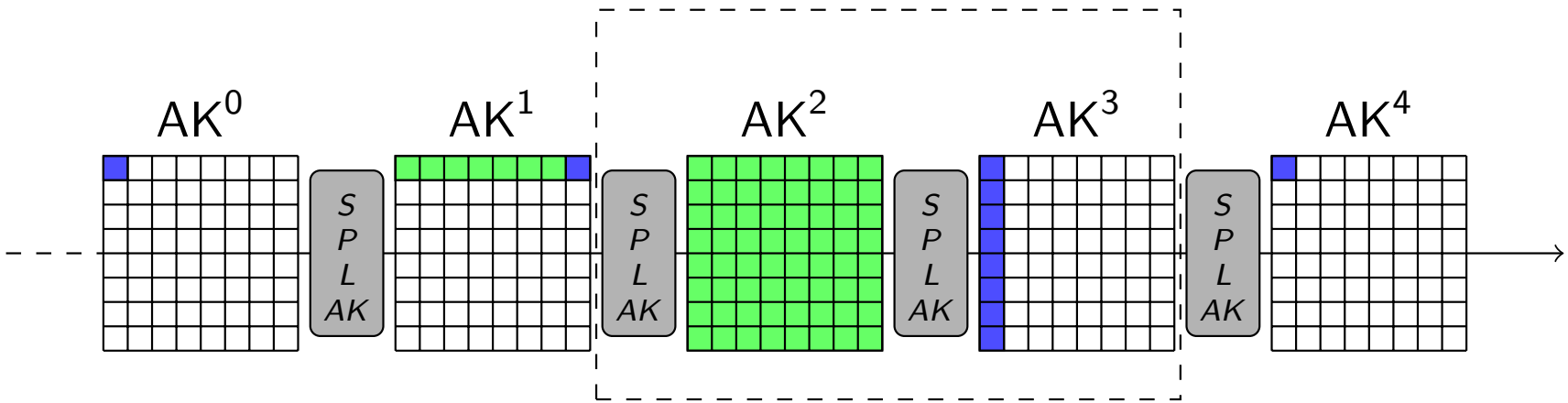


Finding the message pair



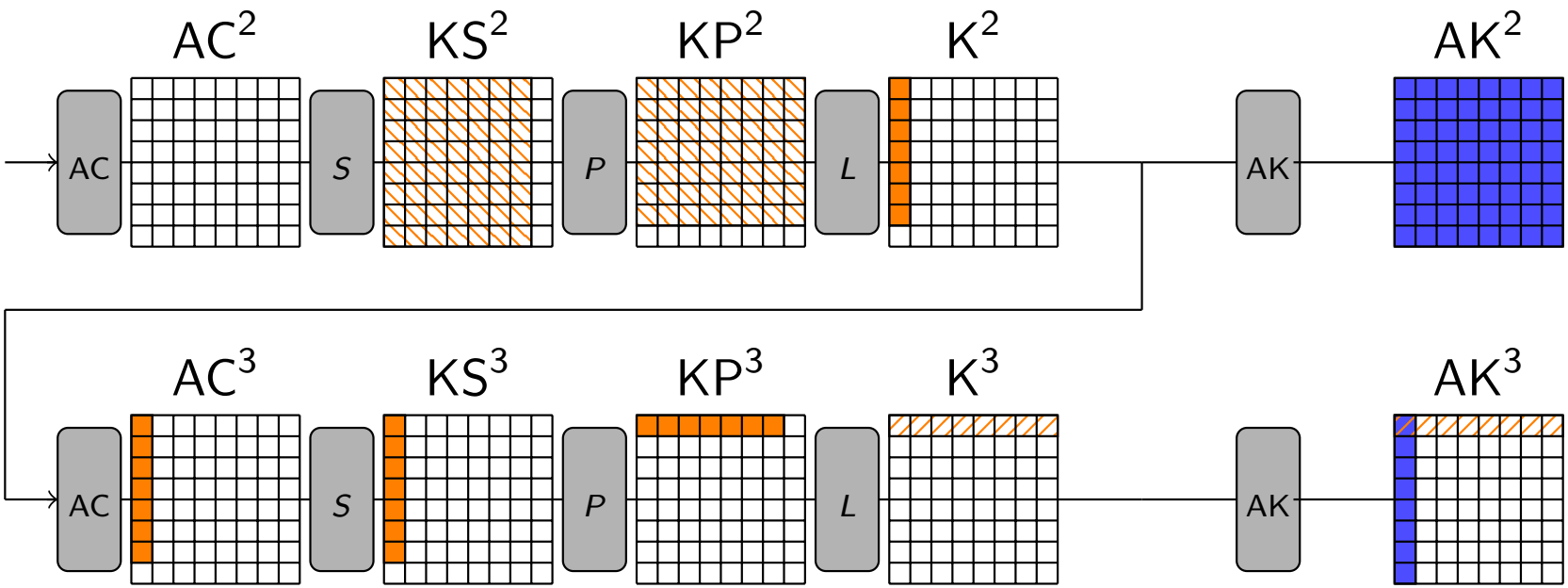
Finding the message pair

We need to fulfill conditions on 81 bytes.

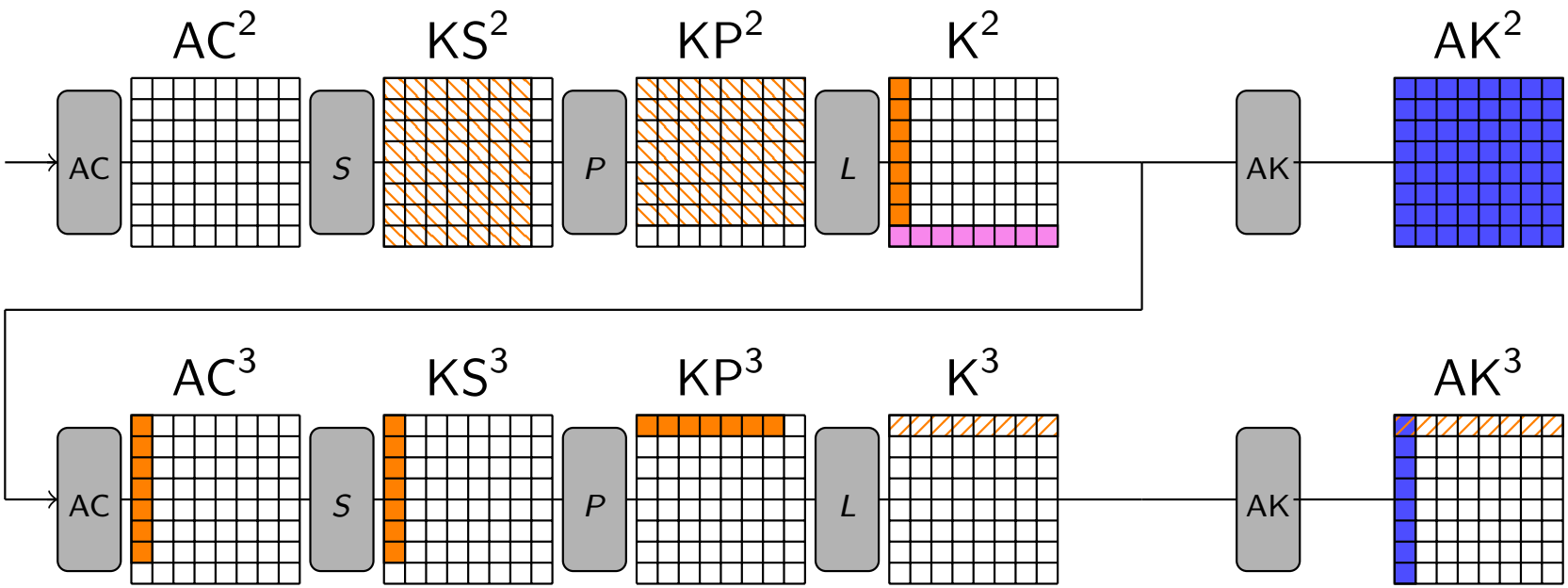


- How to solve the conditions for $AK^3 = S(S^3)$...

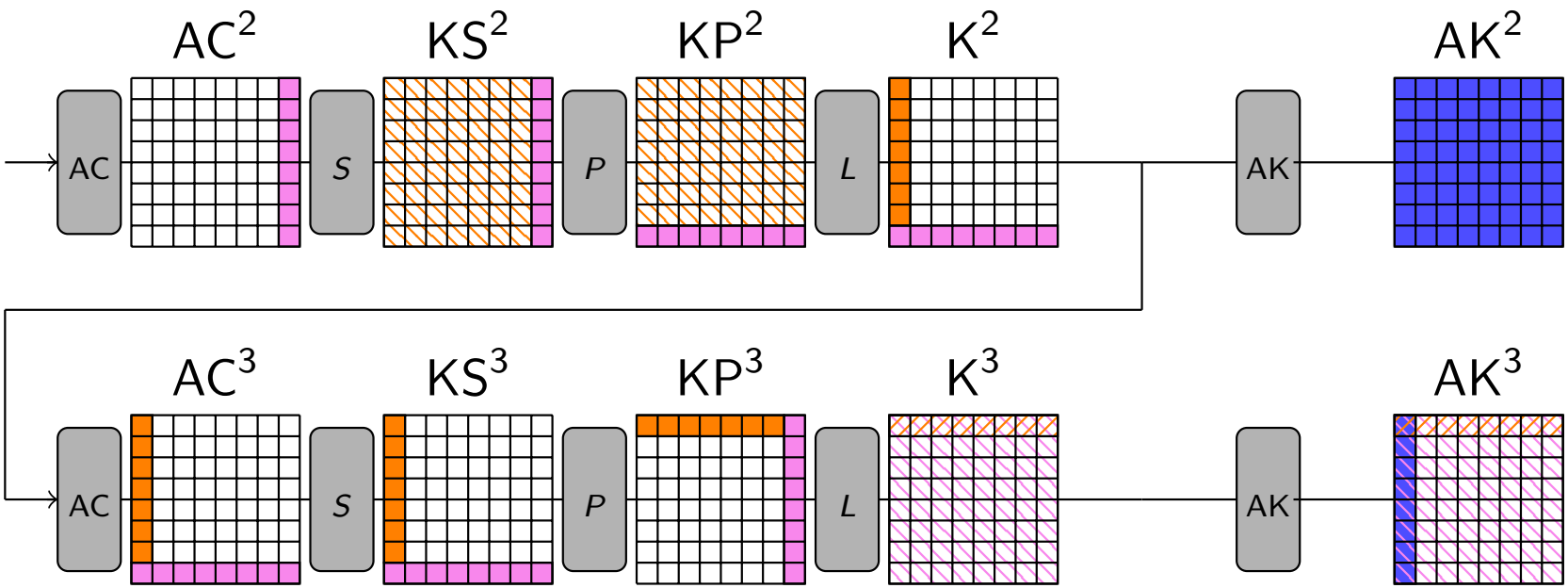
Finding the message pair



Finding the message pair

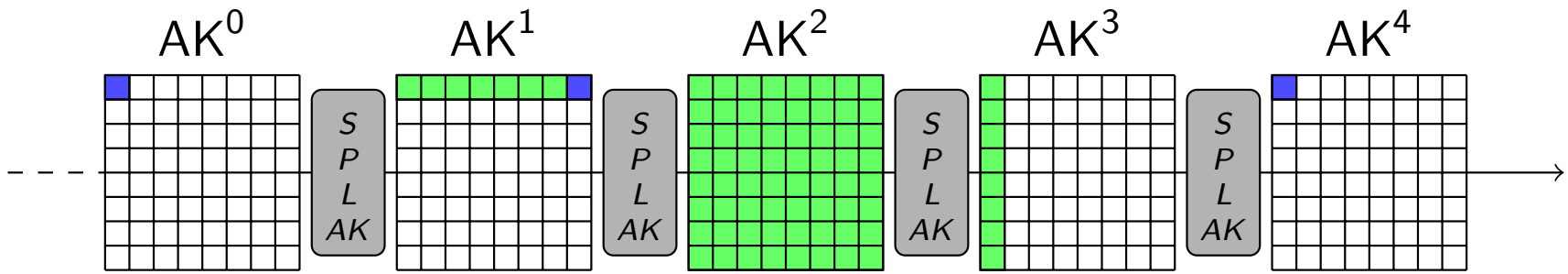


Finding the message pair



Finding the message pair

We need to fulfill conditions on 81 bytes.



- One byte condition remaining in AK^1.
- $\Delta AK^0 = \Delta AK^4$.

Complexity

Repeat message finding procedure 2^{16} times.

Attack

Summary of Attack on GOST R

- Finding Characteristic: $2^{19.8}$
- Finding Message Pair: 2^{16}

Costs depend on properties of the S-Box

S-Box	MDP	ANS	Matching Costs	$\#S^2$
AES	2^{-6}	127	$2^{6.42}$	$2^{55.91}$
Whirlpool	2^{-5}	101.49	$2^{25.10}$	$2^{53.32}$
GOST R	2^{-5}	107.05	$2^{19.77}$	$2^{53.94}$

Conclusion

Function	Rounds	Time	Memory	Type
GOST R	4	$2^{19.8}$	2^{16}	collision
	4.5	$2^{19.8}$	2^{16}	collision
	6.5	2^{64}	2^{16}	collision
Whirlpool	4	$2^{25.1}$	2^{16}	collision
	6.5	$2^{25.1}$	2^{16}	near-collision

- Technique could be used to fulfill more conditions
- Application on other designs
- `https://github.com/kste/aeshash`

Thank you for your attention!

References I


Riham AlTawy, Aleksandar Kircanski, and Amr M. Youssef, *Rebound Attacks on Stribog*, Cryptology ePrint Archive, Report 2013/539, 2013, `http://eprint.iacr.org/`.


Mario Lamberger, Florian Mendel, Martin Schläffer, Christian Rechberger, and Vincent Rijmen, *The Rebound Attack and Subspace Distinguishers: Application to Whirlpool*, Journal of Cryptology (2013), 1–40 (English).


Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen, *The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl*, FSE (Orr Dunkelman, ed.), Lecture Notes in Computer Science, vol. 5665, Springer, 2009, pp. 260–276.

References II


Yu Sasaki, Lei Wang, Shuang Wu, and Wenling Wu, *Investigating Fundamental Security Requirements on Whirlpool: Improved Preimage and Collision Attacks*, vol. 7658, pp. 562–579, Springer Berlin Heidelberg, 2012.


Zongyue Wang, Hongbo Yu, and Xiaoyun Wang, *Cryptanalysis of GOST R Hash Function*, Cryptology ePrint Archive, Report 2013/584, 2013, `http://eprint.iacr.org/`.