SPARX: A Family of ARX-based Lightweight Block Ciphers with Provable Bounds

Daniel Dinu, Léo Perrin, Aleksei Udovenko,
Vesselin Velichkov, Johann Großschädl, Alex Biryukov

SnT, University of Luxembourg

https://www.cryptolux.org

March 9, 2017
Grande Region Security and Reliability Day

Introducing the SPARX family of block ciphers

Introducing the SPARX family of block ciphers

- Lightweight in software: suitable for IoT.

Introducing the SPARX family of block ciphers

- Lightweight in software: suitable for IoT.
- Resilient to SCA.

Introducing the SPARX family of block ciphers

- Lightweight in software: suitable for IoT.
- Resilient to SCA.
- Provable differential/linear bounds.

Introducing the SPARX family of block ciphers

- Lightweight in software: suitable for IoT.
- Resilient to SCA.
- Provable differential/linear bounds.
- First such ARX-based ciphers!

Efficiency of the SPARX Ciphers

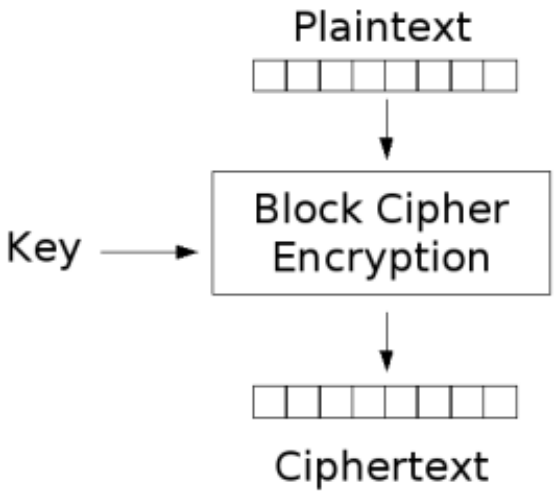
Rank	Cipher	Block size	Key size	Scenario 1 FOM	Security margin
1	Speck	64	128	5.0	27 %
2	Chaskey-LTS	128	128	5.0	42 %
3	Simon	64	128	6.9	32 %
4	RECTANGLE	64	128	7.8	28 %
5	LEA	128	128	8.0	33 %
6	**Sparx**	**64**	**128**	**8.6**	**38 %**
7	**Sparx**	**128**	**128**	**12.9**	**31 %**
8	HIGHT	64	128	14.1	19 %
9	**AES**	**128**	**128**	**15.3**	**30 %**
10	Fantomas	128	128	17.2	?? %

(FELICS framework, block ciphers with key size at least 128 bits)

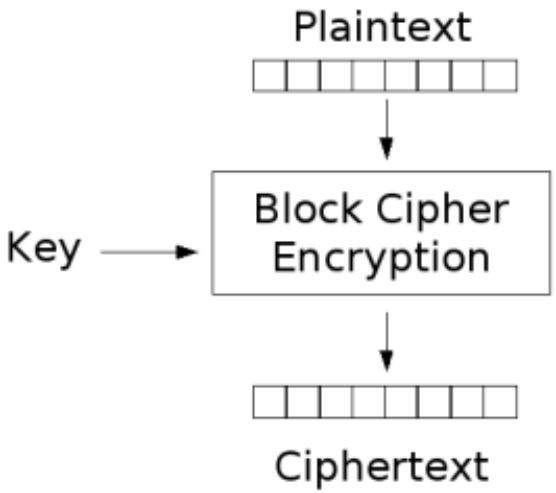
Outline

Plan

Block Ciphers

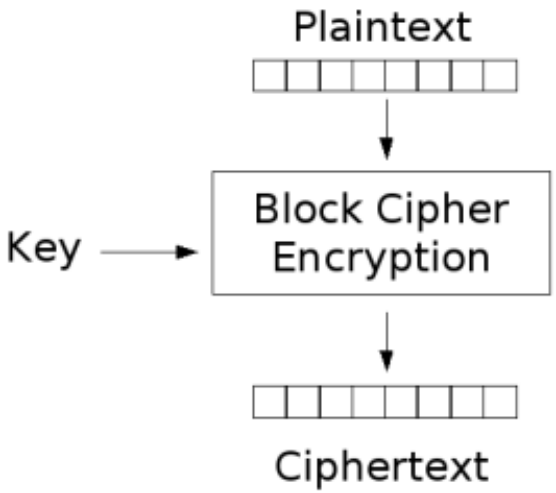


Block Ciphers



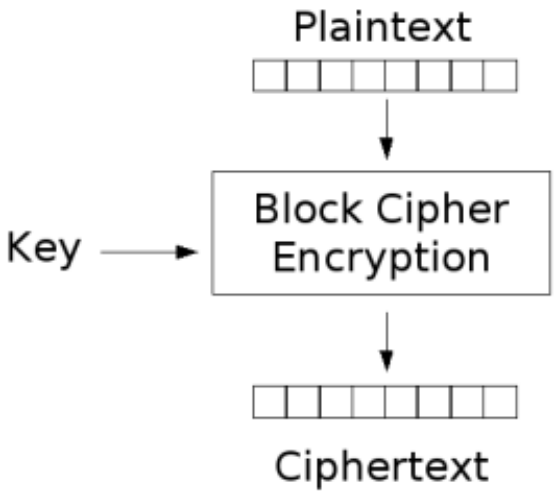
1. Primitive: must be used in modes (authenticated encryption).

Block Ciphers



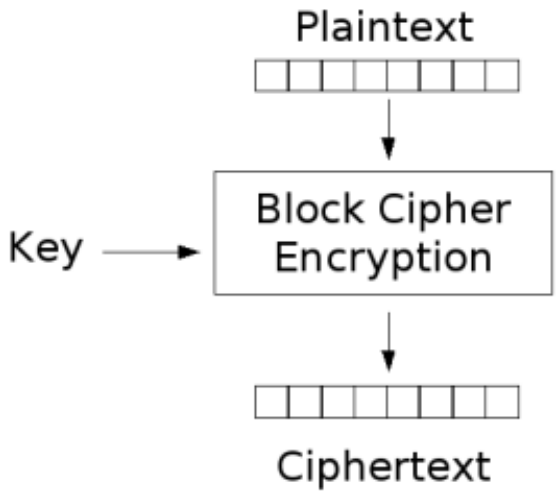
1. Primitive: must be used in modes (authenticated encryption).
2. Modes have security proofs.

Block Ciphers

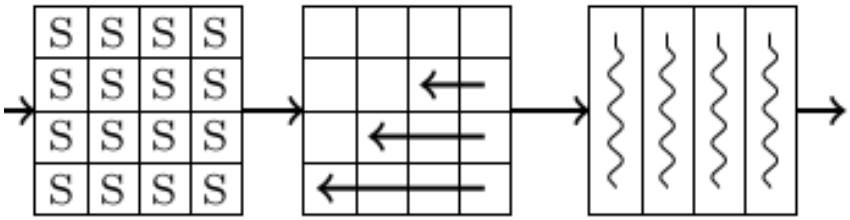


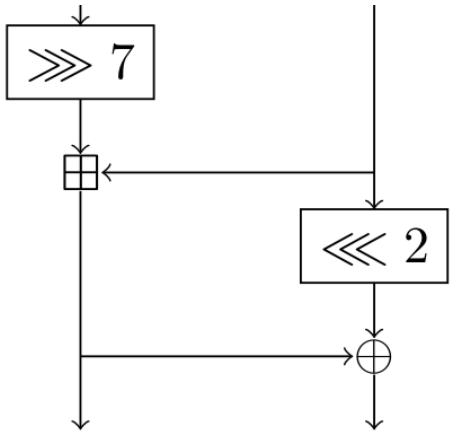
1. Primitive: must be used in modes (authenticated encryption).
2. Modes have security proofs.
3. BCs may have security proofs but only against some attacks.

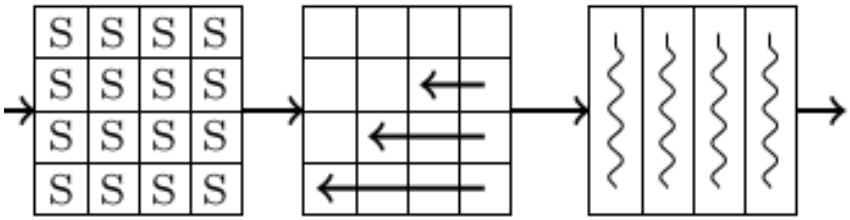
Block Ciphers

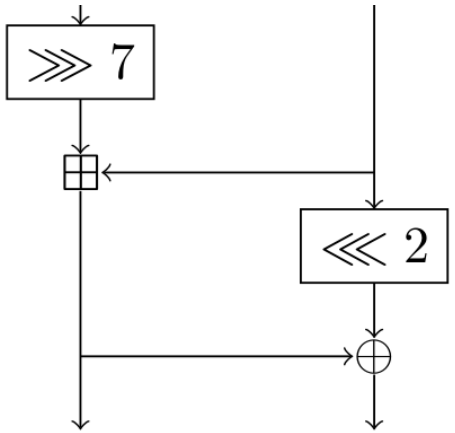


1. Primitive: must be used in modes (authenticated encryption).
2. Modes have security proofs.
3. BCs may have security proofs but only against some attacks.
4. $\Rightarrow$ BC is the weakest part.


S S S S
S S S S
S S S S
S S S S


≫ 7
≪ 2





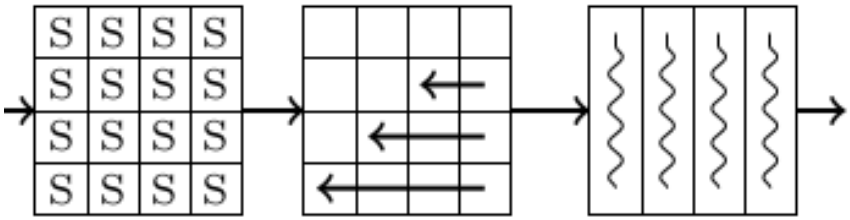
S-Box Based

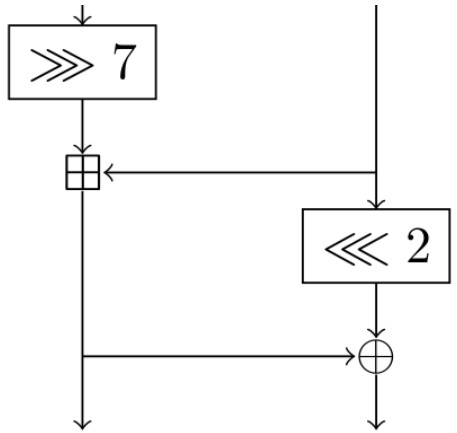
Pros.

- Easy security argument (*wide trail strategy*).

Cons.

- Might store "big" table.
- Vulnerable to side-channel attacks.





S-Box Based

Pros.

- Easy security argument (*wide trail strategy*).

Cons.

- Might store "big" table.
- Vulnerable to side-channel attacks.

ARX Based

Pros.

- Lightweight implementations.
- Less vulnerable to side-channel attacks.

Cons.

- Security hard to justify.

How can we take the best of both worlds?

How can we take the best of both worlds?

Introducing the **SPARX** family

- ARX-based...
  - Lightweight in software.
  - Resilience to SCA.

How can we take the best of both worlds?

Introducing the **SPARX** family

- ARX-based...
  - Lightweight in software.
  - Resilience to SCA.
- ... Substitution-Permutation Networks
  - Provable differential/linear bounds.
  - First such ARX-based ciphers!

How can we take the best of both worlds?

Introducing the **SPARX** family

- ARX-based...
  - Lightweight in software.
  - Resilience to SCA.
- ... Substitution-Permutation Networks
  - Provable differential/linear bounds.
  - First such ARX-based ciphers!

Substitution-Permutation, **ARX**-Based $\Longrightarrow$ **SPARX**

Plan

High Level View

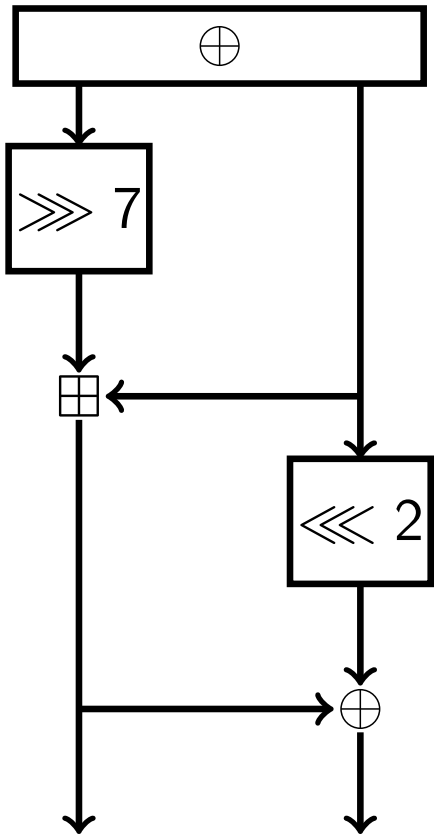
SPARX family of block ciphers

- Designed using a long trail strategy (our contribution).
- 64 or 128 bit **block**, 128 or 256 bit **key**.
- Only 16-bit operations: $\lll i$, $\oplus$, $\boxplus$.

ARX-Boxes

SPECKEY

1. Start from SPECK-32
2. XOR key in full state (Markov assumption)
3. Find best trails



SPECKEY

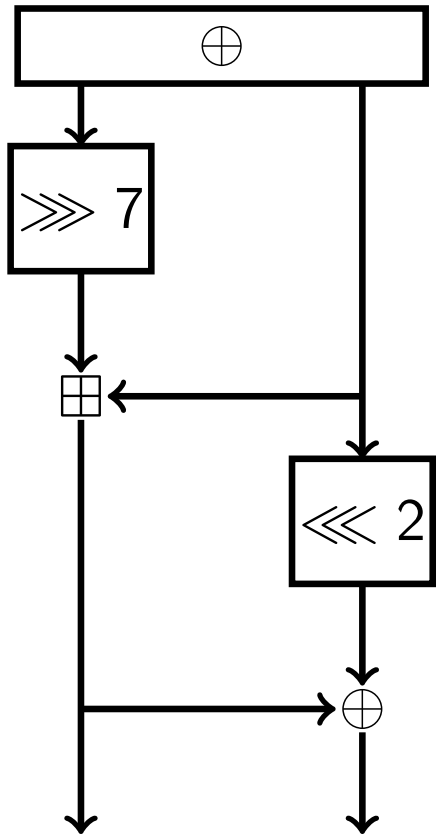
ARX-Boxes

SPECKEY

1. Start from SPECK-32
2. XOR key in full state (Markov assumption)
3. Find best trails

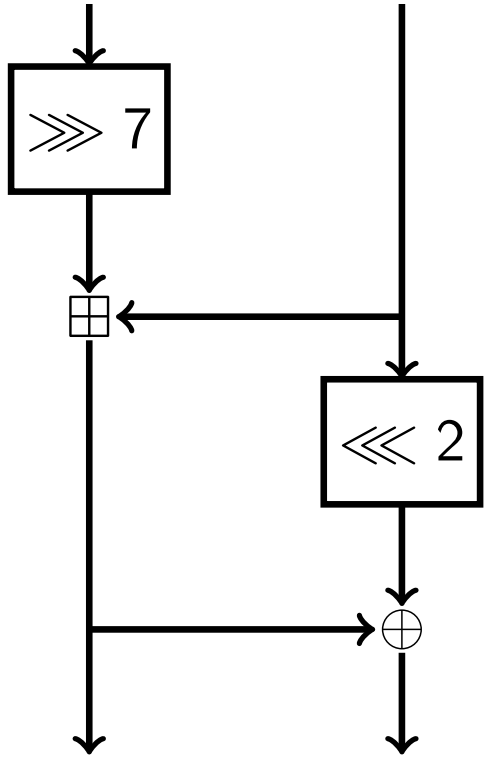
Parameter Search

- Rotations $7, -2$
- Second best crypto properties, lightest
- NSA design strategy?

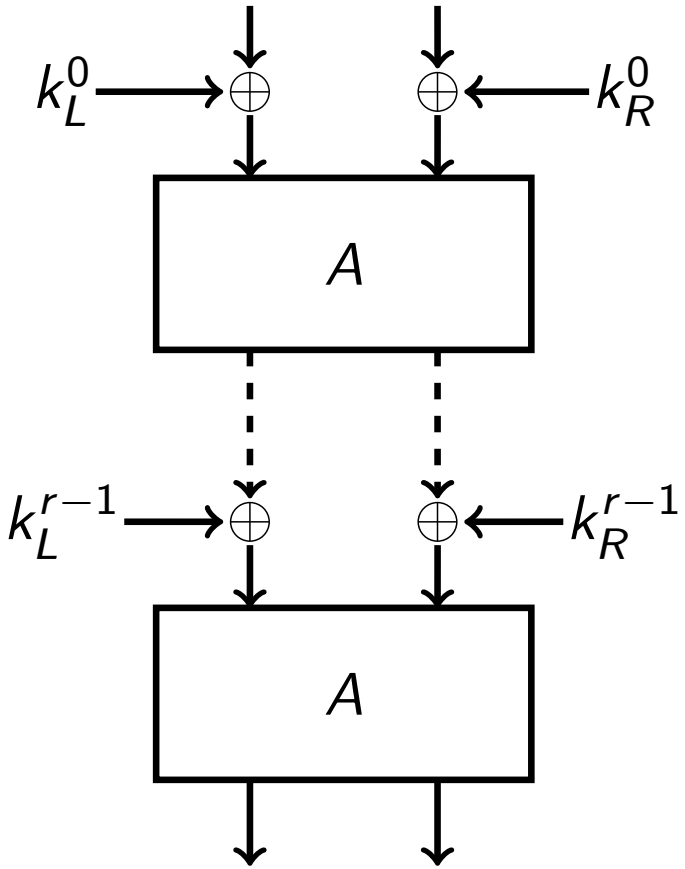


SPECKEY

Notations

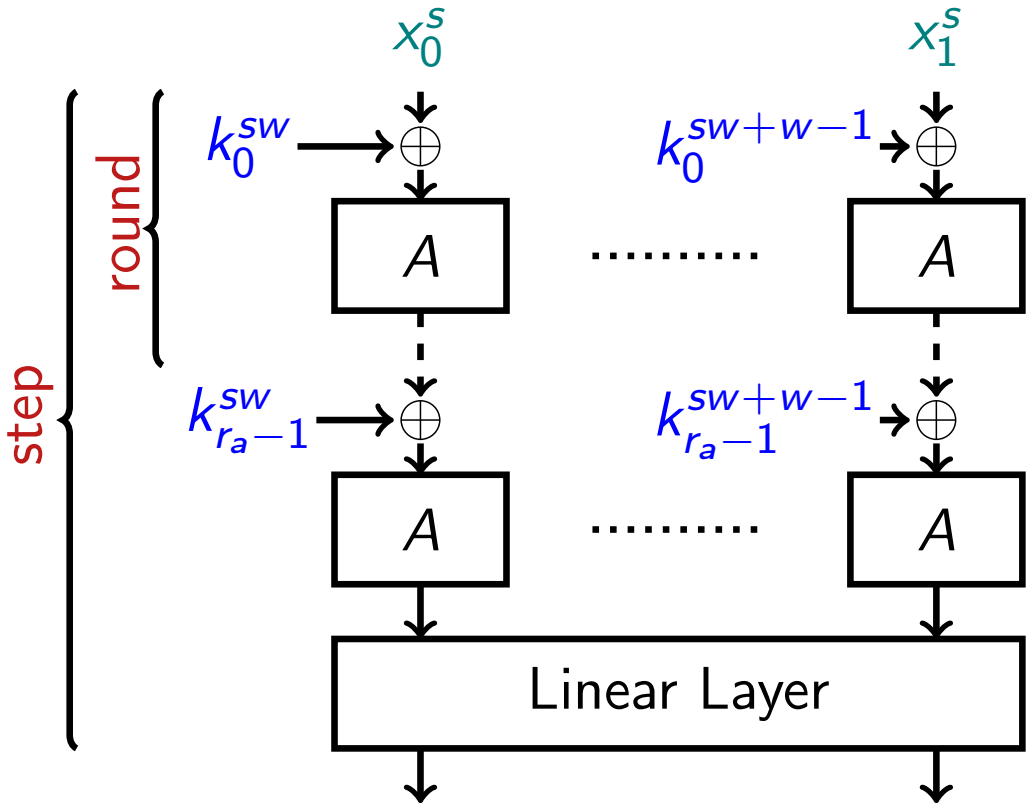


A



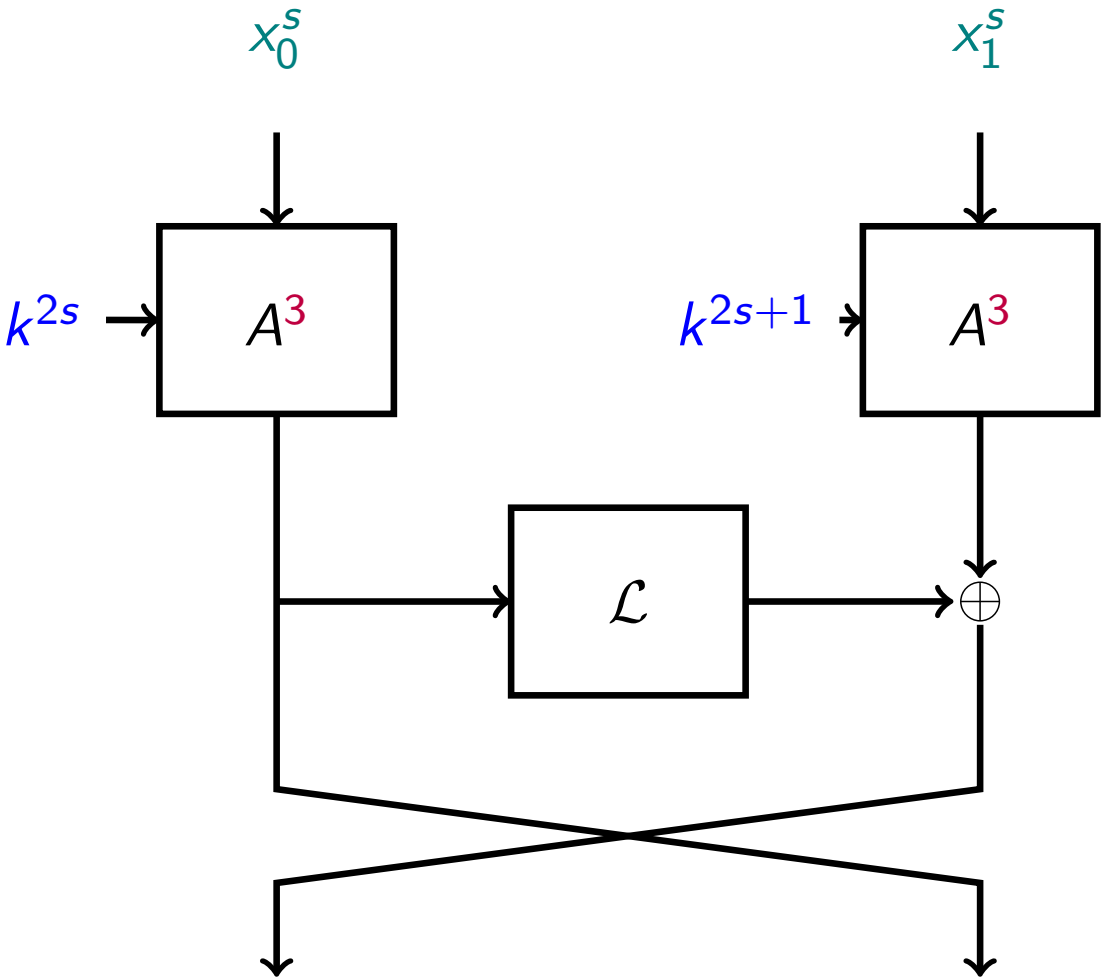
A_k^r

High level view

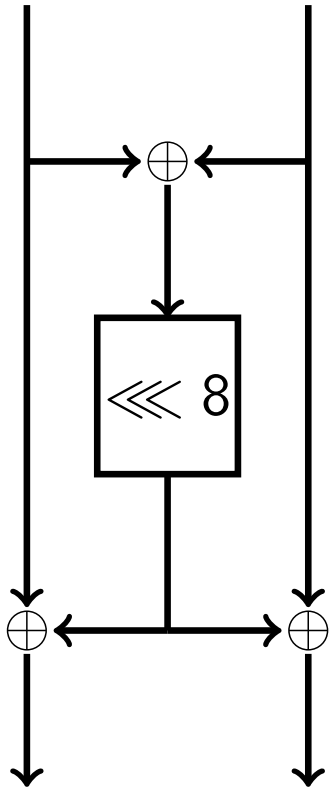


Round function of SPARX.

SPARX-64/128

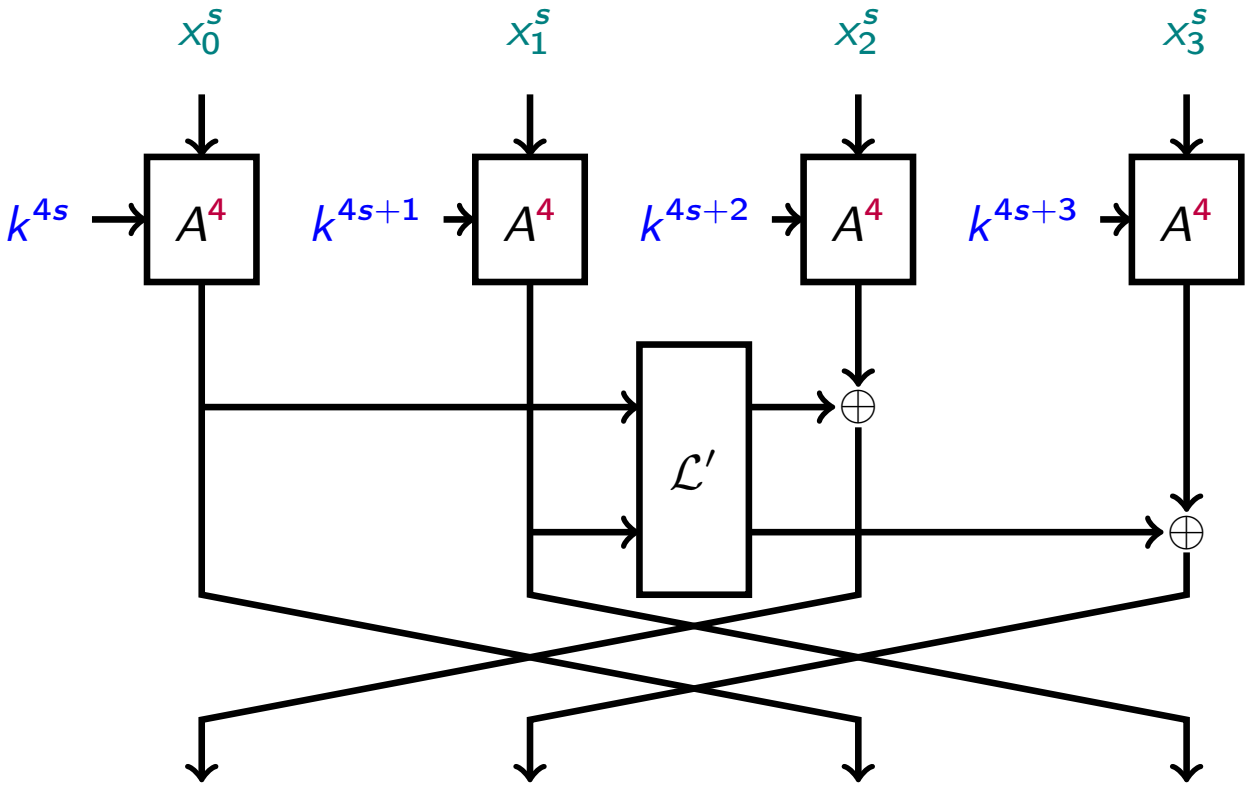


Step Function.

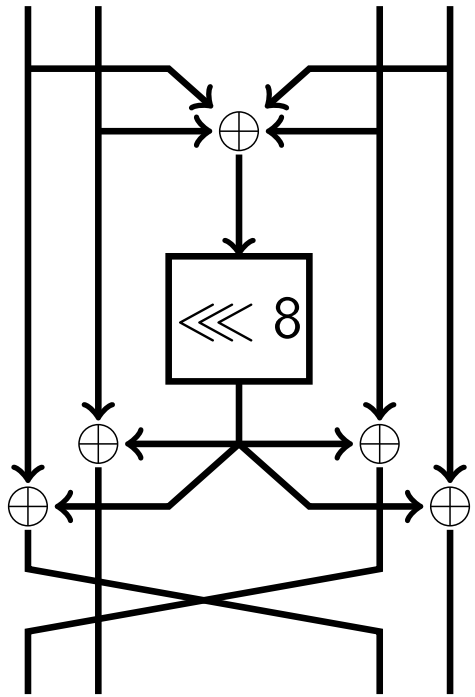


$\mathcal{L}$.

SPARX-128/128 and SPARX-128/256



Step Function.



$\mathcal{L}'$.

Security

Long Trail Argument

$$P[\text{any diff. trail covering at least 5 steps}] < 2^{-n}$$

Security

Long Trail Argument

$$P[\text{any diff. trail covering at least 5 steps}] < 2^{-n}$$

Integral Attacks

Todo's division property: distinguishers for 4-5 steps.

Security

Long Trail Argument

$$P[\text{any diff. trail covering at least 5 steps}] < 2^{-n}$$

Integral Attacks

Todo's division property: distinguishers for 4-5 steps.

n/k	64/128	128/128	128/256
rounds attacked/total	15/24	22/32	24/40
security margin	38 %	31 %	40 %

"Attack" means recovering secret key faster than exhaustive search.

Plan

Benchmarking

`https://www.cryptolux.org/index.php/FELICS`

- **F**air **E**valuation of **L**ightweight **C**ryptographic **S**ystems
- 8-bit ATMEL AVR ; 16-bit TI MSP ; 32-bit ARM Cortex-M3
- Usage scenarios (e.g. CBC encryption of 128 bytes)
- Extracts RAM usage, ROM usage, # CPU cycles.

Benchmarking

`https://www.cryptolux.org/index.php/FELICS`

- **F**air **E**valuation of **L**ightweight **C**ryptographic **S**ystems
- 8-bit ATMEL AVR ; 16-bit TI MSP ; 32-bit ARM Cortex-M3
- Usage scenarios (e.g. CBC encryption of 128 bytes)
- Extracts RAM usage, ROM usage, # CPU cycles.
- Figure Of Merit aggregates: all metrics accross all platforms for the best implementations of one algorithm.

Efficiency of the SPARX Ciphers

Rank	Cipher	Block size	Key size	Scenario 1 FOM	Security margin
1	Speck	64	128	5.0	27 %
2	Chaskey-LTS	128	128	5.0	42 %
3	Simon	64	128	6.9	32 %
4	RECTANGLE	64	128	7.8	28 %
5	LEA	128	128	8.0	33 %
6	**Sparx**	**64**	**128**	**8.6**	**38 %**
7	**Sparx**	**128**	**128**	**12.9**	**31 %**
8	HIGHT	64	128	14.1	19 %
9	**AES**	**128**	**128**	**15.3**	**30 %**
10	Fantomas	128	128	17.2	?? %

(FELICS framework, block ciphers with key size at least 128 bits)

Efficiency of the SPARX Ciphers

Rank	Cipher	Block size	Key size	Scenario 1 FOM	Security margin
–	Speck	64	128	5.0	27 %
–	Chaskey-LTS	128	128	5.0	42 %
–	Simon	64	128	6.9	32 %
1	RECTANGLE	64	128	7.8	28 %
–	LEA	128	128	8.0	33 %
2	**Sparx**	**64**	**128**	**8.6**	**38 %**
3	**Sparx**	**128**	**128**	**12.9**	**31 %**
–	HIGHT	64	128	14.1	19 %
4	**AES**	**128**	**128**	**15.3**	**30 %**
5	Fantomas	128	128	17.2	?? %

(FELICS framework, block ciphers with key size at least 128 bits)

Gray: designers did not provide differential/linear bounds.

Flexibility of the Implementation

Implem.	Block size [bits]	AVR			MSP			ARM		
		Time [cyc.]	Code [B]	RAM [B]	Time [cyc.]	Code [B]	RAM [B]	Time [cyc.]	Code [B]	RAM [B]
1-step ro	64	1789	248	2	1088	166	14	1370	176	28
1-step un		1641	424	1	907	250	12	1100	348	24
2-steps ro		1677	356	2	1034	232	10	1331	304	28
2-steps un		1529	712	1	853	404	8	932	644	24
1-step ro	128	4553	504	11	2809	300	26	3463	348	44
1-step un		4165	1052	10	2353	584	24	2784	884	40
2-steps ro		4345	720	11	2593	432	18	3399	620	40
2-steps un		3957	1820	10	2157	1004	16	2377	1692	36

"ro": rolled ; "un": unrolled.

Plan

Conclusion (1/2)

The SPARX ciphers are:

1. lightweight and SCA-secure as ARX-based ciphers,
2. provably secure against some attacks as SPNs (the first!),
3. flexible: different implementation trade-offs are possible.

Conclusion (2/2)

- Visit `https://www.cryptolux.org/index.php/SPARX`
- Check `https://eprint.iacr.org/2016/984`
- Study the SPARX ciphers!

Conclusion (2/2)

- Visit `https://www.cryptolux.org/index.php/SPARX`
- Check `https://eprint.iacr.org/2016/984`
- Study the SPARX ciphers!

Thank you!