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

Daniel Dinu\textsuperscript{1}, Léo Perrin\textsuperscript{1}, Aleksei Udovenko\textsuperscript{1}, Vesselin Velichkov\textsuperscript{1}, Johann Großschädl\textsuperscript{1}, Alex Biryukov\textsuperscript{1}

\textsuperscript{1}SnT, University of Luxembourg
https://www.cryptolux.org

October 18, 2016
NIST workshop on Lightweight Crypto
Introduction

S-Bo x 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.

Intro duction
Cryptolux Team
SPARX: A Family of ARX-based Lightweight Block Ciphers
**S-Box Based**

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

**Cons.**
- Might store “big” table.
- Vulnerable to side-channel attacks.
Introduction

S-Box Based

Pros.
- Easy security argument \textit{(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.
Introducing the SPARX family

Lightweight in software.
Resilience to SCA.

Substitution-Permutation Networks

Provable differential/linear bounds.

First such ARX-based ciphers!

Substitution-Permutation, ARX-Based $\Rightarrow$ SPARX

Introduction

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!
Introduction

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** $\implies$ **SPARX**
Introduction

Outline

1. A New Design Strategy
2. Description of SPARX
3. Implementation
4. Conclusion
## Plan

1. A New Design Strategy
   - The Wide Trail Strategy
   - ARX-Boxes
   - The Long Trail Strategy

2. Description of SPARX

3. Implementation

4. Conclusion
The Wide Trail Strategy (WTS)

Wide Trail Argument

\[
\text{MEDCP}(F^r) \leq pS^{a(r)}
\]

- MEDCP\( (F^r) = \max (P[\text{any trail covering } r \text{ rounds of } F]) \)
- \( P[S(x \oplus c) \oplus S(x) = d] \leq pS \)
- \( \#\{\text{active S-Boxes on } r \text{ rounds}\} \geq a(r) \)
The Wide Trail Strategy (WTS)

Wide Trail Argument

\[ \text{MEDCP}(F^r) \leq pS^{a(r)} \]

- MEDCP\((F^r) = \max(P[\text{any trail covering } r \text{ rounds of } F])\)
- \(P[S(x \oplus c) \oplus S(x) = d] \leq ps\)
- \#\{active S-Boxes on } r \text{ rounds}\} \geq a(r)\)

Used to design the AES!
The Wide Trail Strategy (WTS)

Wide Trail Argument

\[ \text{MEDCP}(F^r) \leq ps^{a(r)} \]

- MEDCP\((F^r) = \max(P[\text{any trail covering } r \text{ rounds of } F])\)
- \(P[S(x \oplus c) \oplus S(x) = d] \leq ps\)
- \(\#\{\text{active S-Boxes on } r \text{ rounds}\} \geq a(r)\)

Used to design the AES!

Application to ARX

Can we use this to build an ARX-based cipher?
ARX-Boxes (1/2)

**SPECKEY**

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

---

SPECKEY.
ARX-Boxes (1/2)

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?
### ARX-Boxes (2/2)

#### Differential/Linear bounds

<table>
<thead>
<tr>
<th>$r$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDCP($A^r$)</td>
<td>−0</td>
<td>−1</td>
<td>−3</td>
<td>−5</td>
<td>−9</td>
<td>−13</td>
<td>−18</td>
<td>−24</td>
<td>−30</td>
<td>−34</td>
</tr>
<tr>
<td>MELCC($A^r$)</td>
<td>−0</td>
<td>−0</td>
<td>−1</td>
<td>−3</td>
<td>−5</td>
<td>−7</td>
<td>−9</td>
<td>−12</td>
<td>−14</td>
<td>−17</td>
</tr>
</tbody>
</table>

Maximum expected differential characteristic probabilities (MEDCP) and maximum expected absolute linear characteristic correlations (MELCC) of SPECKEY ($\log_2$ scale); $r$ is the number of rounds.
Notations
Naive Approach

S-Box: $A_1^1$; Linear layer: 128-bit MixColumns.

\[ A_k^1 \quad A_k^1 \quad A_k^1 \quad A_k^1 \]

MixColumns

\[ A_k^1 \quad A_k^1 \quad A_k^1 \quad A_k^1 \]

MixColumns
Naive Approach

S-Box: $A^1$; Linear layer: 128-bit MixColumns.

- Active ARX-Boxes: $a(2s) \geq 5s$,
- $\log_2(\text{MEDCP}(A^1)) = 0$
A New Design Strategy

Description of SPARX

Implementation

Conclusion

Naive Approach

S-Box: $A^1$ ; Linear layer: 128-bit MixColumns.

1 step

$A_k^1$ $A_k^1$ $A_k^1$ $A_k^1$

MixColumns

$A_k^1$ $A_k^1$ $A_k^1$ $A_k^1$

MixColumns

- Active ARX-Boxes: $a(2s) \geq 5s$,
- $\log_2 (\text{MEDCP}(A^1)) = 0$

$\log_2 (P[\text{diff. trail on 2s steps}]) \leq 5s \times \text{MEDCP}(A^1)$

$\log_2 (P[\text{diff. trail on 2s steps}]) \leq 0$
Naive Approach

S-Box: $A^1$; Linear layer: 128-bit MixColumns.

- Active ARX-Boxes: $a(2s) \geq 5s$,
- $\log_2(MEDCP(A^1)) = 0$

$$\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq 5s \times MEDCP(A^1)$$

$$\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq 0$$

[FAIL]
Less Bad Approach

S-Box: $A^4$; Linear layer: 128-bit MixColumns.

1 step

$A^4_k$ $A^4_k$ $A^4_k$ $A^4_k$

MixColumns

$A^4_k$ $A^4_k$ $A^4_k$ $A^4_k$

MixColumns
Less Bad Approach

S-Box: $A^4$; Linear layer: 128-bit MixColumns.

- Active ARX-Boxes: $a(2s) \geq 5s$,
- $\log_2 (\text{MEDCP}(A^4)) = -5$
Less Bad Approach

S-Box: $A^4$; Linear layer: 128-bit MixColumns.

- Active ARX-Boxes: $a(2s) \geq 5s$,
- $\log_2(\text{MEDCP}(A^4)) = -5$

\[
\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq 5s \times \text{MEDCP}(A^4)
\]
\[
\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq -25s
\]
Less Bad Approach

S-Box: $A^4$; Linear layer: 128-bit MixColumns.

Active ARX-Boxes:
- $a(2s) \geq 5s$,
- $\log_2(\text{MEDCP}(A^4)) = -5$

\[
\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq 5s \times \text{MEDCP}(A^4)
\]
\[
\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq -25s
\]

Need $2\lceil 128/25 \rceil = 12$ steps, i.e. 48 ARX rounds!
Drawbacks

The Wide Trail Strategy fails here

Two (bad) options:

1. design a very weak cipher, or
2. design a very slow cipher.
Drawbacks

The Wide Trail Strategy fails here

Two (bad) options:

1. design a very weak cipher, or
2. design a very slow cipher.

A New Hope

- \( \log_2 (\text{MEDCP}(A^4)) = -5 \)
- \( \log_2 (\text{MEDCP}(A^8)) = -24 \ll -5 \times 2 \)
Better Approach

- New linear layer “chaining” ARX-Boxes.
New linear layer “chaining” ARX-Boxes.
Better Approach

- New linear layer “chaining” ARX-Boxes.
- We can use $\text{MEDCP}(A^8)$ instead of $(\text{MEDCP}(A^4))^2$.
Better Approach

- New linear layer “chaining” ARX-Boxes.
- We can use MEDCP($A^8$) instead of ($MEDCP(A^4))^2$.
- If left half has zero differences,
**Better Approach**

- New linear layer “chaining” ARX-Boxes.
- We can use $\text{MEDCP}(A^8)$ instead of $(\text{MEDCP}(A^4))^2$.
- If left half has zero differences, we can use $\text{MEDCP}(A^{12})$ instead of $(\text{MEDCP}(A^4))^3$. 

*Cryptolux Team*
The Long Trail Argument (1/2)

### Definition (Long Trail)

A **Long Trail (LT)** is a trail covering several ARX-Boxes without receiving any outside difference. Can be *static* (probability = 1) or *dynamic* (depends on the trail).
The Long Trail Argument (1/2)

**Definition (Long Trail)**

A Long Trail (LT) is a trail covering several ARX-Boxes without receiving any outside difference. Can be static (probability = 1) or dynamic (depends on the trail).

**Definition (Truncated Trail)**

A sequence of values in $\{0, 1\}^4$: 1 if ARX-Box $i$ is active, else 0.
The Long Trail Argument (2/2)

Bounding Differential Probability

For all truncated trails covering $r$ rounds:

1. check if it is coherent with the linear layer,
2. decompose it into long trails (static and dynamic),
3. bound the probability of all trails following the truncated trail.
The Long Trail Argument (2/2)

Bounding Differential Probability

For all truncated trails covering $r$ rounds:

1. check if it is coherent with the linear layer,
2. decompose it into long trails (static and dynamic),
3. bound the probability of all trails following the truncated trail.

$\implies$ Deduce a bound on the probability of all trails.
The Long Trail Argument (2/2)

Bounding Differential Probability

For all truncated trails covering $r$ rounds:

1. check if it is coherent with the linear layer,
2. decompose it into long trails (static and dynamic),
3. bound the probability of all trails following the truncated trail.

$\Rightarrow$ Deduce a bound on the probability of all trails.

Example of a LT bound

After 5 steps, the best trail for four 4-round ARX-Boxes + Feistel linear layer is $< 2^{-128}$.

$5 \ll 12$ steps
The Long Trail Strategy (LTS)

Definition (Design Principle)

When using **large, weak S-Boxes**, it is better to foster Long Trails than diffusion. Thus, the **linear layer must be small**.
The Long Trail Strategy (LTS)

Definition (Design Principle)

When using large, weak S-Boxes, it is better to foster Long Trails than diffusion. Thus, the linear layer must be small.
The Long Trail Strategy (LTS)

Definition (Design Principle)
When using large, weak S-Boxes, it is better to foster Long Trails than diffusion. Thus, the linear layer must be small.

Wide Trail Strategy
- S-Box: Small, cheap.

Long Trail Strategy
- S-Box: Large, expensive.
- Lin. Layer: Cheap, simple.
Plan

1. A New Design Strategy
2. Description of SPARX
   - High Level View
   - Security Analysis
3. Implementation
4. Conclusion
SPARX family of block ciphers

- Designed using a long trail strategy.
- SPARX-$n/k$: $n$-bit block, $k$-bit key ($k \geq 128$).
- Only need 16-bit operations: $i$, $\oplus$. 
High Level View

SPARX family of block ciphers

- Designed using a long trail strategy.
- SPARX-\(n/k\): \(n\)-bit block, \(k\)-bit key \((k \geq 128)\).
- Only need 16-bit operations: \(i, \oplus\).

<table>
<thead>
<tr>
<th>(n/k)</th>
<th>64/128</th>
<th>128/128</th>
<th>128/256</th>
</tr>
</thead>
<tbody>
<tr>
<td># Rounds/Step</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td># Steps</td>
<td>8</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>Best Attack (# rounds)</td>
<td>15/24</td>
<td>22/32</td>
<td>24/40</td>
</tr>
</tbody>
</table>
Notations (reminder)

\[ A \oplus k_0 \oplus L \rightarrow A \]

\[ A_r k_{r-1} \oplus L \rightarrow A_{k_r} \]

\[ k_L^0 \rightarrow A \rightarrow k_R^0 \]

\[ k_L^{r-1} \rightarrow A \rightarrow k_R^{r-1} \]
A New Design Strategy

Description of SPARX

Implementation

Conclusion

High level view

Round function of SPARX.

Key schedule.

SPARX: A Family of ARX-based Lightweight Block Ciphers
SPARX-64/128

A New Design Strategy

Description of SPARX

Implementation

Conclusion

SPARX: A Family of ARX-based Lightweight Block Ciphers
SPARX-128/128 and SPARX-128/256

Step Function.

\[ \ell' \]

Cryptolux Team SPARX: A Family of ARX-based Lightweight Block Ciphers
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: 4-5 steps for \( n = 64-128 \),
- properties of modular addition: +1 round,
- best distinguishers cover 13-21 rounds for \( n = 64-128 \).
Security

Long Trail Argument

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

Integral Attacks

- Todo’s division property: 4-5 steps for \( n = 64-128 \),
- properties of modular addition: +1 round,
- best distinguishers cover 13-21 rounds for \( n = 64-128 \).

<table>
<thead>
<tr>
<th>( n/k )</th>
<th>64/128</th>
<th>128/128</th>
<th>128/256</th>
</tr>
</thead>
<tbody>
<tr>
<td>rounds attacked/total</td>
<td>15/24</td>
<td>22/32</td>
<td>24/40</td>
</tr>
<tr>
<td>security margin</td>
<td>38 %</td>
<td>31 %</td>
<td>40 %</td>
</tr>
</tbody>
</table>
# Plan

1. **A New Design Strategy**
2. **Description of SPARX**
3. **Implementation**
   - Methodology
   - Results
4. **Conclusion**

**SPARX: A Family of ARX-based Lightweight Block Ciphers**

Cryptolux Team
Benchmarking

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

- **Fair Evaluation of Lightweight Cryptographic Systems**
- 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.
Benchmarkeding

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

- **Fair Evaluation of Lightweight Cryptographic Systems**
- 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 across all platforms for the best implementations of one algorithm.
## Efficiency of the SPARX Ciphers

<table>
<thead>
<tr>
<th>Rank</th>
<th>Cipher</th>
<th>Block size</th>
<th>Key size</th>
<th>Scenario 1 FOM</th>
<th>Security margin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Speck</td>
<td>64</td>
<td>128</td>
<td>5.0</td>
<td>27 %</td>
</tr>
<tr>
<td>2</td>
<td>Chaskey-LTS</td>
<td>128</td>
<td>128</td>
<td>5.0</td>
<td>42 %</td>
</tr>
<tr>
<td>3</td>
<td>Simon</td>
<td>64</td>
<td>128</td>
<td>6.9</td>
<td>32 %</td>
</tr>
<tr>
<td>4</td>
<td>RECTANGLE</td>
<td>64</td>
<td>128</td>
<td>7.8</td>
<td>28 %</td>
</tr>
<tr>
<td>5</td>
<td>LEA</td>
<td>128</td>
<td>128</td>
<td>8.0</td>
<td>33 %</td>
</tr>
<tr>
<td>6</td>
<td>SPARX</td>
<td>64</td>
<td>128</td>
<td>8.6</td>
<td>38 %</td>
</tr>
<tr>
<td>7</td>
<td>SPARX</td>
<td>128</td>
<td>128</td>
<td>12.9</td>
<td>31 %</td>
</tr>
<tr>
<td>8</td>
<td>HIGHT</td>
<td>64</td>
<td>128</td>
<td>14.1</td>
<td>19 %</td>
</tr>
<tr>
<td>9</td>
<td>AES</td>
<td>128</td>
<td>128</td>
<td>15.3</td>
<td>30 %</td>
</tr>
<tr>
<td>10</td>
<td>Fantomas</td>
<td>128</td>
<td>128</td>
<td>17.2</td>
<td>?? %</td>
</tr>
</tbody>
</table>
## Efficiency of the SPARX Ciphers

<table>
<thead>
<tr>
<th>Rank</th>
<th>Cipher</th>
<th>Block size</th>
<th>Key size</th>
<th>Scenario 1 FOM</th>
<th>Security margin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RECTANGLE</td>
<td>64</td>
<td>128</td>
<td>7.8</td>
<td>28 %</td>
</tr>
<tr>
<td>2</td>
<td>Sparx</td>
<td>64</td>
<td>128</td>
<td>8.6</td>
<td>38 %</td>
</tr>
<tr>
<td>3</td>
<td>Sparx</td>
<td>128</td>
<td>128</td>
<td>12.9</td>
<td>31 %</td>
</tr>
<tr>
<td>4</td>
<td>AES</td>
<td>128</td>
<td>128</td>
<td>15.3</td>
<td>30 %</td>
</tr>
<tr>
<td>5</td>
<td>Fantomas</td>
<td>128</td>
<td>128</td>
<td>17.2</td>
<td>?? %</td>
</tr>
<tr>
<td>6</td>
<td>Speck</td>
<td>64</td>
<td>128</td>
<td>5.0</td>
<td>27 %</td>
</tr>
<tr>
<td>7</td>
<td>Chaskey-LTS</td>
<td>128</td>
<td>128</td>
<td>5.0</td>
<td>42 %</td>
</tr>
<tr>
<td>8</td>
<td>Simon</td>
<td>64</td>
<td>128</td>
<td>6.9</td>
<td>32 %</td>
</tr>
<tr>
<td>9</td>
<td>LEA</td>
<td>128</td>
<td>128</td>
<td>8.0</td>
<td>33 %</td>
</tr>
<tr>
<td>10</td>
<td>Speck</td>
<td>64</td>
<td>128</td>
<td>5.0</td>
<td>27 %</td>
</tr>
<tr>
<td>11</td>
<td>Speck</td>
<td>64</td>
<td>128</td>
<td>5.0</td>
<td>27 %</td>
</tr>
</tbody>
</table>

Gray: designers did not provide differential/linear bounds.
## Flexibility of the Implementation

<table>
<thead>
<tr>
<th>Implem.</th>
<th>Block size [bits]</th>
<th>AVR</th>
<th>MSP</th>
<th>ARM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-step ro</td>
<td>1789</td>
<td>248</td>
<td>2</td>
<td>1088</td>
</tr>
<tr>
<td>1-step un</td>
<td>1641</td>
<td>424</td>
<td>1</td>
<td>907</td>
</tr>
<tr>
<td>2-steps ro</td>
<td>1677</td>
<td>356</td>
<td>2</td>
<td>1034</td>
</tr>
<tr>
<td>2-steps un</td>
<td>1529</td>
<td>712</td>
<td>1</td>
<td>853</td>
</tr>
<tr>
<td>1-step ro</td>
<td>4553</td>
<td>504</td>
<td>11</td>
<td>2809</td>
</tr>
<tr>
<td>1-step un</td>
<td>4165</td>
<td>1052</td>
<td>10</td>
<td>2353</td>
</tr>
<tr>
<td>2-steps ro</td>
<td>4345</td>
<td>720</td>
<td>11</td>
<td>2593</td>
</tr>
<tr>
<td>2-steps un</td>
<td>3957</td>
<td>1820</td>
<td>10</td>
<td>2157</td>
</tr>
</tbody>
</table>

“ro”: rolled; “un”: unrolled.
Plan

1. A New Design Strategy
2. Description of SPARX
3. Implementation
4. Conclusion
   - Wrapping up!
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.
Visit https://www.cryptolux.org/index.php/SPARX

Check https://eprint.iacr.org/

Study the SPARX ciphers!
Conclusion (2/2)

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

Thank you!