On the Scope of Lightweight Cryptography

Alex Biryukov\textsuperscript{1}, Daniel Dinu\textsuperscript{1}, Léo Perrin\textsuperscript{1}

\textsuperscript{1}SnT, University of Luxembourg

https://www.cryptolux.org

January 16, 2017
Early Symmetric Crypto
Lightweight crypto is whatever you are currently working on.

In this talk

- Lightweight Crypto?
- IoT?
In this talk

- Lightweight Crypto?
- IoT?
- No mention of proprietary algorithms (MIFARE, Keeloq, etc).
Outline

1. In the Literature
2. Lightweight Cryptography in the Wild
3. Two Faces for Lightweight Crypto
4. Conclusion
Plan

1. In the Literature
   - Example: a semi-exhaustive list of LW-BC
   - Trends in LW Design

2. Lightweight Cryptography in the Wild

3. Two Faces for Lightweight Crypto

4. Conclusion
Block ciphers (1/2)

1993  **3-WAY**
1997  **Misty1 (KASUMI)**
1998  **AES, Skipjack**
2000  **Noekeon**
2004  **Iceberg**
2006  **HIGHT, mCrypton, SEA**
2007  **CLEFIA, DESLX, PRESENT**
2009  **KATAN/KTANTAN**

(Soon-to-be?) standards **underlined**.
FELICS FOM under 10 in **red**.
No S-Box (or bit-sliced S-Box) in **bold**.
Block ciphers (2/2)

2010  GOST revisited
2011  LBlock, LED, Piccolo
2012  KLEIN, PRINCE, TWINE, XTEA
2013  ITUbee, LEA, SIMON/SPECK, Zorro
2014  Chaskey Cipher, Fantomas/Robin, PRIDE
2015  Midori, Rectangle, RoadRunneR, SIMECK
2016  FLY, Mantis/SKINNY, SPARX

(Soon-to-be?) standards underlined.
FELICS FOM under 10 in red.
No S-Box (or bit-sliced S-Box) in bold.
**Algorithms**

*Number of lightweight symmetric primitives (LWSP) published*
Algorithms

Number of LWSP published/two years
Non-Linearity Source

Number of LWSP with given non-linear operations
Non-Linearity Source

Number of LWSP with given non-linear operations/two years
Number of LWSP with given linear operations
In the Literature

Lightweight Cryptography in the Wild

Two Faces for Lightweight Crypto

Conclusion

Linearity Source

Number of LWSP with given linear operations/two years

Biryukov, Dinu, Perrin
On the Scope of Lightweight Cryptography

11 / 24
Plan

1. In the Literature

2. Lightweight Cryptography in the Wild
   - What is used
   - How it fails

3. Two Faces for Lightweight Crypto

4. Conclusion
Communication Protocols

**GSM**  A5/1, A5/2, A5/3 (= KASUMI ≈ Misty1)

**3GPP**  SNOW 3G, ZUC

**Bluetooth**  E0

**Bluetooth Smart**  $^1$ AES

**WPA**  RC4

**WPA2**  AES

$^1$Low energy variant of Bluetooth
ISO Standards

29167 (Air interface) Targets RFID devices:
ISO Standards

29167 *(Air interface)* Targets RFID devices: AES-128, PRESENT-80, Grain-128A

29192 *(Lightweight Crypto)*:

- **Block ciphers**: PRESENT, CLEFIA, SIMON/SPECK (soon?);
- **Stream ciphers**: Trivium, Enocoro;
- **Hash functions**: PHOTON, Spongent, Lesamnta-LW.
IoT Oriented Protocols/Libraries

- **Lora Alliance** AES

- **IEEE 802.15.4** (common protocol for wireless IoT devices), AES

---

\(^2\)Was used by tinyOS.
IOT Oriented Protocols/Libraries

Lora Alliance  AES

IEEE 802.15.4  (common protocol for wireless IoT devices), AES

Tinysec ² Skipjack (CBC)

Minisec  (successor of tinysec)  Skipjack (OCB)

TinyOS  At the same time, can use the AES and Trivium

²Was used by tinyOS.
NIST Standardization

- Still at an early stage.
- Possible at all?
  - vagueness of scope statement
  - IP issues
  - Reducing number of algorithms even possible?
NIST Standardization

- Still at an early stage.
- Possible at all?
  - vagueness of scope statement
  - IP issues
  - Reducing number of algorithms even possible?

Source: wikimedia commons
Side-Channel Attacks

Table 1. Power analysis attacks against commercially available hardware cryptographic implementations. Entries marked with † indicate firmware-based implementations, but still being commercially available.

<table>
<thead>
<tr>
<th>Target</th>
<th>Cipher</th>
<th>Attack</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptoMemory</td>
<td>proprietary</td>
<td>CPA</td>
<td>17</td>
</tr>
<tr>
<td>DESFire MF3ICD40</td>
<td>3DES</td>
<td>CPA</td>
<td>18</td>
</tr>
<tr>
<td>DS2432, DS28E01</td>
<td>SHA-1</td>
<td>CPA</td>
<td>19</td>
</tr>
<tr>
<td>Microchip HCSXXX</td>
<td>KeeLoQ</td>
<td>CPA</td>
<td>20</td>
</tr>
<tr>
<td>ProASIC3</td>
<td>AES</td>
<td>PEA</td>
<td>21</td>
</tr>
<tr>
<td>SimonsVoss†</td>
<td>proprietary</td>
<td>CPA</td>
<td>22</td>
</tr>
<tr>
<td>Spartan-6</td>
<td>AES</td>
<td>CPA</td>
<td>23</td>
</tr>
<tr>
<td>Stratix II</td>
<td>AES</td>
<td>CPA</td>
<td>24</td>
</tr>
<tr>
<td>Stratix III</td>
<td>AES</td>
<td>CPA</td>
<td>25</td>
</tr>
<tr>
<td>Virtex-II</td>
<td>3DES</td>
<td>CPA</td>
<td>26</td>
</tr>
<tr>
<td>Virtex-4, Virtex-5</td>
<td>AES</td>
<td>CPA</td>
<td>27</td>
</tr>
<tr>
<td>XMEGA</td>
<td>AES</td>
<td>CPA</td>
<td>8</td>
</tr>
<tr>
<td>Yubikey 2†</td>
<td>AES</td>
<td>CPA</td>
<td>28</td>
</tr>
</tbody>
</table>

# Plan

1. In the Literature

2. Lightweight Cryptography in the Wild

3. Two Faces for Lightweight Crypto
   - Separation
   - Ultra-Lightweight Crypto
   - Pervasive Crypto

4. Conclusion
LWC is Spread Thin

One algo to rule them all?
LWC is Spread Thin

One algo to rule them all? I am skeptical...

- IoT and lightweight constraints were lumped together...
- ... yet even lightbulbs run the AES!
  (https://eprint.iacr.org/2016/1047.pdf)
- Still, need something specific to address IoT constraints.
LWC is Spread Thin

One algo to rule them all? I am skeptical...

- IoT and lightweight constraints were lumped together...

- ... yet even lightbulbs run the AES!
  (https://eprint.iacr.org/2016/1047.pdf)

- Still, need something specific to address IoT constraints.

Ultra-Lightweight Crypto ≠ Pervasive crypto
RFID tags

Robshaw’s talk at NIST workshop on RAIN RFID:

- It is arguable whether an algorithm with a 128-bit key and “poor” side-channel profile is necessarily better than an algorithm with a 80- or 96-bit key and “good” side-channel profile.
- There is no demand for very short block lengths (e.g. 48 bits)
- 64-bit block sizes can be both useful and appropriate for RAIN RFID (implementation/volume of data transmitted)
- It is very hard to come up with a scenario that gets anywhere close to $2^{32}$ uses of a 64-bit block cipher
- Small/low power implementations are vital
Ultra-Lightweight Crypto

- Only for most constrained devices (RFID, etc).
- Hardware only.
- Focus on performance: gate area, latency...
- Bold trade-offs make sense (little data encrypted, etc).
- \( \approx \) “old” lightweight cryptography definition.
- Niche use cases (RFID, memory encryption,...)
Ultra-Lightweight Crypto

- Only for most constrained devices (RFID, etc).
- Hardware only.
- Focus on performance: gate area, latency...
- Bold trade-offs make sense (little data encrypted, etc).
- \( \approx \) “old” lightweight cryptography definition.
- Niche use cases (RFID, memory encryption,...)

Algos that already fit this bill: KATAN, PRESENT, Grain, Ketje...
Ultra-Lightweight Crypto

- Only for most constrained devices (RFID, etc).
- Hardware only.
- Focus on performance: gate area, latency...
- Bold trade-offs make sense (little data encrypted, etc).
- \( \approx \) “old” lightweight cryptography definition.
- Niche use cases (RFID, memory encryption,...)

Algos that already fit this bill: KATAN, PRESENT, Grain, Ketje...
BC have smaller state \( \Rightarrow \) better choice?
8-bit AVR

FELICS results for CTR encryption (balanced implementation)\(^3\)

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Block</th>
<th>key</th>
<th>Code</th>
<th>RAM</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chaskey-LTS</td>
<td>128</td>
<td>128</td>
<td>770</td>
<td>84</td>
<td>2413</td>
</tr>
<tr>
<td>Speck</td>
<td>64</td>
<td>128</td>
<td>452</td>
<td>53</td>
<td>2917</td>
</tr>
<tr>
<td>AES</td>
<td>128</td>
<td>128</td>
<td>1246</td>
<td>81</td>
<td>3408</td>
</tr>
<tr>
<td>LEA</td>
<td>128</td>
<td>128</td>
<td>906</td>
<td>80</td>
<td>4023</td>
</tr>
<tr>
<td>RECTANGLE</td>
<td>64</td>
<td>128</td>
<td>602</td>
<td>56</td>
<td>4381</td>
</tr>
<tr>
<td>SPARX</td>
<td>64</td>
<td>128</td>
<td>662</td>
<td>51</td>
<td>4397</td>
</tr>
</tbody>
</table>

\(^3\)Sorted by speed; only ciphers with key \(\geq 128\).
FELICS results for CTR encryption (balanced implementation)\(^4\)

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Block</th>
<th>key</th>
<th>Code</th>
<th>RAM</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speck</td>
<td>64</td>
<td>128</td>
<td>332</td>
<td>48</td>
<td>2013</td>
</tr>
<tr>
<td>Chaskey-LTS</td>
<td>128</td>
<td>128</td>
<td>492</td>
<td>86</td>
<td>2064</td>
</tr>
<tr>
<td>SPARX</td>
<td>64</td>
<td>128</td>
<td>580</td>
<td>52</td>
<td>2261</td>
</tr>
<tr>
<td>RECTANGLE</td>
<td>64</td>
<td>128</td>
<td>480</td>
<td>54</td>
<td>2651</td>
</tr>
<tr>
<td>LEA</td>
<td>128</td>
<td>128</td>
<td>722</td>
<td>78</td>
<td>2814</td>
</tr>
<tr>
<td>AES</td>
<td>128</td>
<td>128</td>
<td>1170</td>
<td>80</td>
<td>4497</td>
</tr>
</tbody>
</table>

\(^4\)Sorted by speed; only ciphers with key \(\geq 128\). Simon-64/128, SPARX-128/128 and Fantomas are between LEA and AES.
32-bit ARM

FELICS results for CTR encryption (balanced implementation)\(^5\)

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Block</th>
<th>key</th>
<th>Code</th>
<th>RAM</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chaskey-LTS</td>
<td>128</td>
<td>128</td>
<td>178</td>
<td>80</td>
<td>790</td>
</tr>
<tr>
<td>Speck</td>
<td>64</td>
<td>128</td>
<td>276</td>
<td>60</td>
<td>972</td>
</tr>
<tr>
<td>LEA</td>
<td>128</td>
<td>128</td>
<td>520</td>
<td>112</td>
<td>1171</td>
</tr>
<tr>
<td>SIMON</td>
<td>64</td>
<td>128</td>
<td>388</td>
<td>64</td>
<td>1453</td>
</tr>
<tr>
<td>RC5-20</td>
<td>64</td>
<td>128</td>
<td>372</td>
<td>64</td>
<td>1919</td>
</tr>
<tr>
<td>AES</td>
<td>128</td>
<td>128</td>
<td>1348</td>
<td>124</td>
<td>4044</td>
</tr>
</tbody>
</table>

\(^5\)Sorted by speed; only ciphers with key $\geq 128$. SPARX-64/128, RECTANGLE and SPARX-128/128 are between the AES and RC5-20.
Pervasive Crypto

- Software (micro-processors) oriented.
- Performance should be better than the AES on all $\mu$-proc.
- Conservative security claims (need RK security, large amounts of data may be available).
- Focus on SCA resistance.
Pervasive Crypto

- Software (micro-processors) oriented.
- Performance should be better than the AES on all $\mu$-proc.
- Conservative security claims (need RK security, large amounts of data may be available).
- Focus on SCA resistance.

Algos that already fit this bill: LS-designs, Noekeon, RECTANGLE, SPARX...
Pervasive Crypto

- Software (micro-processors) oriented.
- Performance should be better than the AES on all $\mu$-proc.
- Conservative security claims (need RK security, large amounts of data may be available).
- Focus on SCA resistance.

Algos that already fit this bill: LS-designs, Noekeon, RECTANGLE, SPARX...
The key has to be loaded in the registers anyway... Why not use corresponding space? $\implies$ Sponge better choice?
Plan

1. In the Literature
2. Lightweight Cryptography in the Wild
3. Two Faces for Lightweight Crypto
4. Conclusion
   - Wrapping up!
Conclusion

Ultra-Lightweight Crypto

- Hardware (RFID...)
- huge implementation constraints
- bold security trade-offs
- 1 niche = 1 algo?
## Conclusion

### Ultra-Lightweight Crypto
- Hardware (RFID...)
- huge implementation constraints
- bold security trade-offs
- 1 niche = 1 algo?

### Pervasive Crypto
- $\mu$-controllers
- Less implementation constraints
- Conservative security
- 1 size fits all
- SCA resistance

Thank you!

Biryukov, Dinu, Perrin
Ultra-Lightweight Crypto

- Hardware (RFID...)
- huge implementation constraints
- bold security trade-offs
- 1 niche = 1 algo?

Pervasive Crypto

- \( \mu \)-controllers
- Less implementation constraints
- Conservative security
- 1 size fits all
- SCA resistance

Thank you!