Low-Latency Encryption

- Is "Lightweight = Light + Wait?" -

Miroslav Knežević, Ventzislav Nikov, Peter Rombouts
Digital Continuum

Low-Latency Encryption
Is “Lightweight = Light + Wait?”

Slide credit: Ingrid Verbauwhede
Digital Continuum

Is "Lightweight = Light + Wait?"

Low-Latency Encryption

~kb/s, μW

~Gb/s, MW

Slide credit: Ingrid Verbauwhede
Digital Continuum

Low-Latency Encryption

Is “Lightweight = Light + Wait?”

~kb/s, µW

~Gb/s, MW

Slide credit: Ingrid Verbauwhede
Latency vs Throughput

Low-Latency Encryption

Is "Lightweight = Light + Wait?"
Latency vs Throughput

Is “Lightweight = Light + Wait?”
Latency vs Throughput

Latency = 15 s
Throughput = 0.067 beer/s
Latency vs Throughput

Ad Fundum

Is “Lightweight = Light + Wait?”
Latency vs Throughput

Latency = 5 s
Throughput = 0.2 beer/s
Latency vs Throughput

Is "Lightweight = Light + Wait?"
Latency vs Throughput

Latency = 15 s
Throughput = 0.2 beer/s
Latency vs Throughput

Latency = 15 s
Throughput = 0.2 beer/s
Latency vs Throughput

Is "Lightweight = Light + Wait?"
Latency vs Throughput

Latency = 15 s
Throughput = 0.2 beer/s

Pipelining
Typical Trade-offs in Crypto

Is "Lightweight = Light + Wait?"

Low-Latency Encryption

Diagram showing the trade-offs between Security, Speed, and Area Power.
Typical Trade-offs in Crypto

Is “Lightweight = Light + Wait?”

Low-Latency Encryption

Diagram:
- Security
- Speed
- Area Power

- Arrows indicate trade-offs between Security, Speed, and Area Power.
Typical Trade-offs in Crypto

AES

3DES

Square

Groestl

SHA-256

Skein

Blake

Keccak

Twofish

NOEKEON

JH

Serpent

IDEA

“Lightweight = Light + Wait?”

Low-Latency Encryption

AES

NOEKEON

JH

Skein

Blake

Keccak

Twofish

Serpent

IDEA

3DES

Square

Groestl

SHA-256

Conventional

Speed

Area

Power

Security
Typical Trade-offs in Crypto

Is “Lightweight = Light + Wait?”

Low-Latency Encryption

Security

Conventional

Lightweight

Area

Power

Speed
Typical Trade-offs in Crypto

Low-Latency Encryption

Is “Lightweight = Light + Wait?”
Typical Trade-offs in Crypto

Is “Lightweight = Light + Wait?”

Low-Latency Encryption

AES
Keccak
Groestl
Blake
Keccak
Twofish
SHA-256

NOEKEON

AES

Conventional

Low Latency

Lightweight

Area

Power

Speed

?
A kid in a Toy store
A kid in a Toy store

Low-Latency Encryption
Is "Lightweight = Light + Wait?"
A kid in a Toy store

Low-Latency Encryption

Is “Lightweight = Light + Wait?”
A kid in a Toy store

Low-Latency Encryption

Is “Lightweight = Light + Wait?”
A kid in a Toy store

Is "Lightweight = Light + Wait?"
A kid in a Toy store

Low-Latency Encryption
Is “Lightweight = Light + Wait?”
A kid in a Toy store

Low-Latency Encryption
Is “Lightweight = Light + Wait?”

- KLEIN
- PRESENT
- MCCRYPTON
- AES
- LED
- NOEKEON
- MINI-AES
- MINI-AES
## Variety of Choices

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>BLOCK-SIZE</th>
<th>KEY-SIZE</th>
<th>S-BOX</th>
<th>P-LAYER</th>
<th>KEY SCHEDULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>128</td>
<td>128</td>
<td>8</td>
<td>MDS</td>
<td>LIGHT</td>
</tr>
<tr>
<td>NOEKEON</td>
<td>128</td>
<td>128</td>
<td>4</td>
<td>BINARY</td>
<td>NO</td>
</tr>
<tr>
<td>MINI-AES</td>
<td>64</td>
<td>64</td>
<td>4</td>
<td>MDS</td>
<td>LIGHT</td>
</tr>
<tr>
<td>MCCRYPTON</td>
<td>64</td>
<td>64, 96, 128</td>
<td>4</td>
<td>BINARY</td>
<td>LIGHT</td>
</tr>
<tr>
<td>PRESENT</td>
<td>64</td>
<td>80, 128</td>
<td>4</td>
<td>BIT PERMUTATION</td>
<td>LIGHT</td>
</tr>
<tr>
<td>KLEIN</td>
<td>64</td>
<td>64, 80, 96</td>
<td>4</td>
<td>MDS</td>
<td>LIGHT</td>
</tr>
<tr>
<td>LED</td>
<td>64</td>
<td>64, 128</td>
<td>4</td>
<td>MDS</td>
<td>NO</td>
</tr>
</tbody>
</table>
Low-Latency Encryption

Is “Lightweight = Light + Wait?”

Number of Rounds

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Number of Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-128</td>
<td>10</td>
</tr>
<tr>
<td>KLEIN-64</td>
<td>10</td>
</tr>
<tr>
<td>KLEIN-80</td>
<td>10</td>
</tr>
<tr>
<td>KLEIN-96</td>
<td>10</td>
</tr>
<tr>
<td>LED-64</td>
<td>10</td>
</tr>
<tr>
<td>LED-128</td>
<td>50</td>
</tr>
<tr>
<td>MCrypton-64</td>
<td>20</td>
</tr>
<tr>
<td>MCrypton-96</td>
<td>20</td>
</tr>
<tr>
<td>Mini-AES-64</td>
<td>20</td>
</tr>
<tr>
<td>Nokeon-128</td>
<td>30</td>
</tr>
<tr>
<td>Present-80</td>
<td>30</td>
</tr>
<tr>
<td>Present-128</td>
<td>30</td>
</tr>
</tbody>
</table>
Six Architectures

Is “Lightweight = Light + Wait?”
Results - Latency

Is “Lightweight = Light + Wait?”
**Results - Latency**

Is “Lightweight = Light + Wait?”

![Bar chart showing latency comparison between different encryption algorithms.](chart)

- **AES-128**: 1-cycle: 7.8, 2-cycle: 20.2
- **KLEIN-64**: 1-cycle: 15.3, 2-cycle: 6.4
- **KLEIN-96**: 1-cycle: 20.1, 2-cycle: 14.4
- **KLEIN-128**: 1-cycle: 25.3, 2-cycle: 26.4
- **LED-64**: 1-cycle: 31.2, 2-cycle: 48.2
- **LED-128**: 1-cycle: 46.6, 2-cycle: 48.2
- **MCRYPTON-64**: 1-cycle: 9.8, 2-cycle: 10.8
- **MCRYPTON-96**: 1-cycle: 10.8, 2-cycle: 10.8
- **MCRYPTON-128**: 1-cycle: 9.8, 2-cycle: 11.2
- **MINI-AES-64**: 1-cycle: 9.9, 2-cycle: 12
- **NOEKEON-128**: 1-cycle: 14.8, 2-cycle: 17
- **NOEKEONs-128**: 1-cycle: 15.5, 2-cycle: 17.4
- **PRESENT-80**: 1-cycle: 14.8, 2-cycle: 16.4
- **PRESENT-128**: 1-cycle: 14.7, 2-cycle: 16.6

*ENC/DEC; Max Time-Constrained*
Results - Area

1-cycle  2-cycle

*ENC/DEC, Max Time-Constrained
### Results - Area

#### Low-Latency Encryption

Is “Lightweight = Light + Wait?”

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>1-cycle</th>
<th>2-cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-128</td>
<td>366.6</td>
<td>191.8</td>
</tr>
<tr>
<td>KLEIN-64</td>
<td>48.2</td>
<td>24.9</td>
</tr>
<tr>
<td>KLEIN-96</td>
<td>63.7</td>
<td>32.6</td>
</tr>
<tr>
<td>KLEIN-128</td>
<td>9.9</td>
<td>41.3</td>
</tr>
<tr>
<td>LED-64</td>
<td>28.7</td>
<td>41.3</td>
</tr>
<tr>
<td>LED-128</td>
<td>96</td>
<td>96</td>
</tr>
<tr>
<td>MCRYPTON-64</td>
<td>41.3</td>
<td>20.9</td>
</tr>
<tr>
<td>MCRYPTON-96</td>
<td>20.9</td>
<td>21.1</td>
</tr>
<tr>
<td>MCRYPTON-128</td>
<td>21.1</td>
<td>21.1</td>
</tr>
<tr>
<td>MINI-AES-64</td>
<td>21</td>
<td>40</td>
</tr>
<tr>
<td>MINI-AES-128</td>
<td>40</td>
<td>40.4</td>
</tr>
<tr>
<td>NOEKEON-128</td>
<td>40</td>
<td>41.4</td>
</tr>
<tr>
<td>NOEKEON-6-128</td>
<td>41.4</td>
<td>22</td>
</tr>
<tr>
<td>NOEKOEN-6-80</td>
<td>41.4</td>
<td>22</td>
</tr>
<tr>
<td>PRESENT-80</td>
<td>102.5</td>
<td>49.6</td>
</tr>
<tr>
<td>PRESENT-128</td>
<td>72.3</td>
<td>73.8</td>
</tr>
</tbody>
</table>

*ENC/DEC; Max Time-Constrained
Results - Average Latency per Round
Low-Latency Encryption

Is “Lightweight = Light + Wait?”

Results - Average Latency per Round

ENC/DEC  ENC

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>ENC/DEC</th>
<th>ENC</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-128</td>
<td>1.78</td>
<td>1.48</td>
</tr>
<tr>
<td>KLEIN-64</td>
<td>1.28</td>
<td>0.93</td>
</tr>
<tr>
<td>KLEIN-96</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>KLEIN-128</td>
<td>0.92</td>
<td>0.92</td>
</tr>
<tr>
<td>LED-64</td>
<td>0.96</td>
<td>0.96</td>
</tr>
<tr>
<td>LED-128</td>
<td>0.97</td>
<td>0.97</td>
</tr>
<tr>
<td>MCRYPTON-64</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>MCRYPTON-96</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>MCRYPTON-128</td>
<td>0.97</td>
<td>0.97</td>
</tr>
<tr>
<td>MINI-AES-64</td>
<td>0.48</td>
<td>0.48</td>
</tr>
<tr>
<td>MINI-AES-96</td>
<td>0.46</td>
<td>0.46</td>
</tr>
<tr>
<td>NOEKEON-128</td>
<td>0.97</td>
<td>0.97</td>
</tr>
<tr>
<td>NOEKEONs-128</td>
<td>0.46</td>
<td>0.46</td>
</tr>
<tr>
<td>PRESENT-80</td>
<td>0.48</td>
<td>0.48</td>
</tr>
<tr>
<td>PRESENT-128</td>
<td>0.46</td>
<td>0.46</td>
</tr>
</tbody>
</table>

*1-cycle Architecture; Max Time-Constrained
Is "Lightweight = Light + Wait?"

Results - Area per Round Distribution
PRESENT-80, ENC only
Hardware Recommendations

We provide hardware recommendations for designing low-latency primitives.

Evaluated ciphers are designed with low-area and low-power in mind and not to satisfy new low-latency requirements.

Still, we can learn quite a lot from their constructions.
Use small Sboxes (4-bit or even 3-bit ones).

Even among them there are significant differences in latency and area [24].

These differences are library dependent.

Hardware Recommendations

-Number of Rounds-

Minimize!
Hardware Recommendations

-Round Complexity-

Not too low complexity.

Reduce the number of rounds at the cost of (slightly) heavier round.
Hardware Recommendations

-Key Schedule-

Number of rounds should be independent of the key schedule.

Use constant addition instead of a key schedule (if possible).
Hardware Recommendations
-Heterogeneous Constructions-

- Last few rounds of the cipher are smaller than the middle ones.
- Make those few rounds more computationally complex.
- Not very good for compact implementations.
Hardware Recommendations

-Encryption vs Decryption-

Use involution: \( f(f(x)) = x \).

Make Encryption and Decryption procedures similar.

BUT: Think “application oriented” - sometimes is beneficial to have “asymmetric” constructions.
Conclusions

meet PRINCE

Low-Latency Encryption

Is “Lightweight = Light + Wait?”

Latency [ns]

Area [kGE]

AES

PRESENT

PRINCE

Thank you!