FIDES:
Lightweight Authentication Cipher
with Side-Channel Resistance
for Constrained Hardware

Begül Bilgin, Andrey Bogdanov, Miroslav Knežević, Florian Mendel, and Qingju Wang
Side Channel Resistance
Side Channel Resistance

The Game...
Side Channel Resistance

The Game...

- Mathematically secure crypto algorithms
Side Channel Resistance

The Game...

- Mathematically secure crypto algorithms
  - AES, RSA, Keccak, OCB, …
Side Channel Resistance

The Game...

- Mathematically secure crypto algorithms
  - AES, RSA, Keccak, OCB, …

- Weak implementation
Side Channel Resistance

The Game...

- Mathematically secure crypto algorithms
  - AES, RSA, Keccak, OCB, …
- Weak implementation
Side Channel Resistance

The Game...

- Mathematically secure crypto algorithms
  - AES, RSA, Keccak, OCB, …
- Weak implementation

Dependency between power consumption and intermediate value (depends on the key)
Side Channel Resistance
Side Channel Resistance

- Change the key frequently
Side Channel Resistance

- Change the key frequently
- Equalize power consumption
Side Channel Resistance

- Change the key frequently
- Equalize power consumption
- Randomize power consumption
Side Channel Resistance

- Change the key frequently
- Equalize power consumption
- Randomize power consumption
  - Boolean masking
Side Channel Resistance

- Change the key frequently
- Equalize power consumption
  - Randomize power consumption
    - Boolean masking
Side Channel Resistance

- Change the key frequently
- Equalize power consumption
- Randomize power consumption
  - Boolean masking
Side Channel Resistance

- Change the key frequently
- Equalize power consumption
- Randomize power consumption
  - Boolean masking
Side Channel Resistance

- Change the key frequently
- Equalize power consumption
- Randomize power consumption
  - Boolean masking
  - Multiplicative masking
Side Channel Resistance

- Change the key frequently
- Equalize power consumption
- Randomize power consumption
  - Boolean masking
  - Multiplicative masking
Side Channel Resistance

- Change the key frequently
- Equalize power consumption
- Randomize power consumption
  - Boolean masking
  - Multiplicative masking
  - Secret sharing e.g. Threshold Implementations [Nikova’11]
Side Channel Resistance

- Change the key frequently
- Equalize power consumption

✓ Randomize power consumption
  - Boolean masking
  - Multiplicative masking
  - Secret sharing e.g. Threshold Implementations [Nikova’11]
Side Channel Resistance
Side Channel Resistance

Have the design
Side Channel Resistance

- Have the design
- Need efficient impl.
Side Channel Resistance

Have the design

Need efficient impl.

Need secure impl.
Side Channel Resistance

Have the design

Need efficient impl.

Need secure impl.

1\textsuperscript{st} Order

2\textsuperscript{nd} Order

Boolean Mask

Multipl. Mask

TI

SW

HW

?? Still efficient ??
Side Channel Resistance

Have the design

Need efficient impl.

Need secure impl.

Boolean Mask Multipl. Mask

1st Order 2nd Order

Still efficient

TI SW HW
Design - Structure

\[ K || N \]

\[ K || 0 \]
Design - Structure

- Similar to duplex sponge
Design - Structure

- Similar to duplex sponge
- Rounds are not keyed
Design - Structure

- Similar to duplex sponge
- Rounds are not keyed
✓ Online
Design - Structure

- Similar to duplex sponge
- Rounds are not keyed
  ✓ Online
  ✓ Single pass
Design - Structure

- Similar to duplex sponge
- Rounds are not keyed
✓ Online
✓ Single pass

FIDES-80
FIDES-96
Design - Structure

- Similar to duplex sponge
- Rounds are not keyed
✓ Online
✓ Single pass

FIDES-80  160
FIDES-96  192
Design - Structure

- Similar to duplex sponge
- Rounds are not keyed
✓ Online
✓ Single pass

<table>
<thead>
<tr>
<th></th>
<th>b</th>
<th>k/n/t</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIDES-80</td>
<td>160</td>
<td>80</td>
</tr>
<tr>
<td>FIDES-96</td>
<td>192</td>
<td>96</td>
</tr>
</tbody>
</table>
Design - Structure

- Similar to duplex sponge
- Rounds are not keyed
✓ Online
✓ Single pass

<table>
<thead>
<tr>
<th></th>
<th>b</th>
<th>k/n/t</th>
<th>r</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIDES-80</td>
<td>160</td>
<td>80</td>
<td>10</td>
</tr>
<tr>
<td>FIDES-96</td>
<td>192</td>
<td>96</td>
<td>12</td>
</tr>
</tbody>
</table>
Design - Structure

1R

State

\[
\begin{array}{cccccccc}
  a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} & a_{0,4} & a_{0,5} & a_{0,6} & a_{0,7} \\
  a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} \\
  a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} \\
  a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} \\
\end{array}
\]
Design - Structure

1R

State

SubBytes

\[ \begin{array}{cccccccc}
  a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} & a_{0,4} & a_{0,5} & a_{0,6} & a_{0,7} \\
  a_{1,0} & a_{1,1} & a_{i,j} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} \\
  a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} \\
  a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} \\
\end{array} \]
Design - Structure

1R

State

SubBytes

ShiftRows
Design - Structure

1R

State

SubBytes

ShiftRows

MixColumns

Almost MDS branch number is 4
Design - Structure

1R

State

SubBytes

ShiftRows

MixColumns

ConstantAddition
Design - S-boxes

- FIDES-80: 5-bit Almost Bent (AB)
  - optimal resistance against differential & linear cryptanalysis

- FIDES-96: 6-bit Almost Perfect Nonlinear (APN)
  - optimal resistance against differential cryptanalysis
Design - S-boxes

- FIDES-80: 5-bit Almost Bent (AB)
  - optimal resistance against differential & linear cryptanalysis

- FIDES-96: 6-bit Almost Perfect Nonlinear (APN)
  - optimal resistance against differential cryptanalysis

++Low latency++
Design - S-boxes

- FIDES-80: 5-bit Almost Bent (AB)
  - optimal resistance against differential & linear cryptanalysis
  - degree 2 (two), 3(one), 4(one)

- FIDES-96: 6-bit Almost Perfect Nonlinear (APN)
  - optimal resistance against differential cryptanalysis
  - degree 4

++Low latency++
Design - S-boxes

- FIDES-80: 5-bit Almost Bent (AB)
  - optimal resistance against differential & linear cryptanalysis
  - degree 2 (two), 3(one), 4(one)

- FIDES-96: 6-bit Almost Perfect Nonlinear (APN)
  - optimal resistance against differential cryptanalysis
  - degree 4

++Low latency++
Design - S-boxes
Design - S-boxes

Affine Equivalent to AB permutation with degree 2
Design - S-boxes

Affine Equivalent to AB permutation with degree 2

Unshared S-box

Shared S-box
Design - S-boxes

Affine Equivalent to AB permutation with degree 2

Unshared S-box

Shared S-box

# of S-boxes

# of GE (UMC 180nm)
Design - S-boxes

Affine Equivalent to AB permutation with degree 2

Unshared S-box

Shared S-box

Similar for APN
## Security Analysis

<table>
<thead>
<tr>
<th># rnd.</th>
<th># Active S-box</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>any diff.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>32</td>
</tr>
<tr>
<td>7</td>
<td>42</td>
</tr>
<tr>
<td>8</td>
<td>48</td>
</tr>
</tbody>
</table>
## Security Analysis

<table>
<thead>
<tr>
<th># rnd.</th>
<th># Active S-box</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>any diff.</td>
<td>zero diff.</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>22</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>32</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>42</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>48</td>
<td>48</td>
<td></td>
</tr>
</tbody>
</table>

- Differential & Linear Cryptanalysis
Security Analysis

<table>
<thead>
<tr>
<th># rnd.</th>
<th># Active S-box</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>any diff.</td>
<td>zero diff.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>22</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>32</td>
<td>52</td>
</tr>
<tr>
<td>7</td>
<td>42</td>
<td>49</td>
</tr>
<tr>
<td>8</td>
<td>48</td>
<td>48</td>
</tr>
</tbody>
</table>

• Differential & Linear Cryptanalysis
16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$
Security Analysis

<table>
<thead>
<tr>
<th># rnd.</th>
<th># Active S-box</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>any diff.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>32</td>
</tr>
<tr>
<td>7</td>
<td>42</td>
</tr>
<tr>
<td>8</td>
<td>48</td>
</tr>
</tbody>
</table>

- Differential & Linear Cryptanalysis
  16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$
- Collision Trails
Security Analysis

<table>
<thead>
<tr>
<th># rnd.</th>
<th># Active S-box</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>any diff.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>32</td>
</tr>
<tr>
<td>7</td>
<td>42</td>
</tr>
<tr>
<td>8</td>
<td>48</td>
</tr>
</tbody>
</table>

• Differential & Linear Cryptanalysis
  16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$

• Collision Trails
  16 rounds: $2^{-4 \times (48 + 48)} = 2^{-384}$
Security Analysis

<table>
<thead>
<tr>
<th># rnd.</th>
<th># Active S-box</th>
<th>any diff.</th>
<th>zero diff.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>22</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>32</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>42</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>48</td>
<td>48</td>
<td></td>
</tr>
</tbody>
</table>

- **Differential & Linear Cryptanalysis**
  - 16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$
- **Collision Trails**
  - 16 rounds: $2^{-4 \times (48+48)} = 2^{-384}$
- **Impossible Differential**
Security Analysis

<table>
<thead>
<tr>
<th># rnd.</th>
<th># Active S-box</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>any diff.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>32</td>
</tr>
<tr>
<td>7</td>
<td>42</td>
</tr>
<tr>
<td>8</td>
<td>48</td>
</tr>
</tbody>
</table>

- **Differential & Linear Cryptanalysis**
  16 rounds: $2^{-4 \times 48 \times 2} = 2^{-384}$
- **Collision Trails**
  16 rounds: $2^{-4 \times (48 + 48)} = 2^{-384}$
- **Impossible Differential**
  9 rounds
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- **FIDES-S**
- **FIDES-4S**
- **FIDES-R**
- **FIDES-T**
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- **FIDES-S**
- **FIDES-4S**
- **FIDES-R**
- **FIDES-T**
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Implementation

- FIDES-S
- FIDES-4S
- FIDES-R
- FIDES-T
Performance

FIDES on Different Technologies

Area in GE

FIDES-80-S  FIDES-80-4S  FIDES-80-R  FIDES-80-T  FIDES-96-S  FIDES-96-4S  FIDES-96-R  FIDES-96-T

NXP 90nm  NANGATE 45nm  UMC 130nm
Performance

Throughput (kb/s) vs. Area (GE)

- FIDES-80
- FIDES-96
- ALE
- AES-CCM
- ASC-1 A
- ASC-1 B
- c-QUARK
- KECCAK-200-MD
- Hummingbird2
Conclusion

FIDES
Conclusion

- Lightweight AE
  - less than 1500GE
  - online, single-pass

FIDES
Conclusion

- Lightweight AE
  - less than 1500GE
  - online, single-pass
- with Side Channel Resistance
  - TI less than 5000 GE

FIDES
Conclusion

- Lightweight AE
  - less than 1500GE
  - online, single-pass
- with Side Channel Resistance
  - TI less than 5000 GE
- and 80-bit or 90-bit security
  - AB and APN permutations
  - almost MDS
THANK YOU!