Side-Channel Analysis of MAC-Keccak

Mostafa Taha and Patrick Schaumont
Virginia Tech
HOST-2013

This research was supported in part by the VT-MENA program of Egypt, and by NSF grant no. 1115839.
Side-Channel Analysis

Classical Cryptanalysis

Algorithm

Input

Key

Output

Side-Channel Analysis

Algorithm

Input

Key

Output

Execution Time

Power Consumption

Electromagnetic Radiation

Acoustic Waves

Photonic Emission
Keccak

- Keccak is a hash function; a one-way function that converts arbitrary length messages into fixed-length digests

- SHA-0, SHA-1, SHA-2 → SHA-3

- Competition started in Nov. 2007 and ended in Oct. 2012 with Keccak as the winner.
- Chosen for having a Sponge construction.
Keccak

- SHA-3 Evaluation at CESCA-VT with an ASIC implementation of the final round algorithms
MAC-Keccak

- Message Authentication Code

\[ H((K \oplus opad) || H((K \oplus ipad) || M)) \]

- HMAC

- MAC-Keccak

\[ H(K || M) \]
The Addressed Challenge

- Key-length is variable
- Intermediate variables are deep inside the algorithm
Previous Work

• Zohner et al. "SCA of the SHA-3 finalists" DATE 2012
  – Acknowledged the effect of changing the key-length, but they did not study the problem in details.

• Bertoni et al. "Keccak implementation overview" 2012
  – SCA countermeasure based on Masking

• Bertoni et al. "Power analysis of Keccak protected with Masking" ePrint IACR 2013
  – Studied the effect of changing the state-size, not the key-length

None have studied the effect of changing the key-length
Our Contribution

• The effect of key-length on the attack difficulty.
• Analysis of Keccak operations.
• Complete attack scenarios.
• Results of a practical attack.
Effect of Key-Length

- Key-Length
- MESSAGE
- Rate
- State-Size
- Optimum key-length

Graph showing attack difficulty vs. key-length in multiples of the rate.
Analysis of Keccak Operations

24 Rounds of

\[ \text{Output} = \iota \circ \chi \circ \pi \circ \rho \circ \theta(\text{Input}) \]
Analysis of Keccak Operations

24 Rounds of

\[ \text{Output} = \iota \circ \chi \circ \pi \circ \rho \circ \theta(\text{Input}) \]

- Keccak operations that leak information for SCA
Effect of the Key-Length

Key-Length = 1 Plane

1st of $\theta$

Key-Length = 2 Planes

1st of $\theta$
2nd of $\theta$

2 bits of $\theta_{\text{plane}}$
Attack Scenarios

MAC-Keccak

\( l_k \leq r \) Rate

\begin{align*}
\begin{array}{|c|c|c|}
\hline
l_k & < r & \geq r \\
\hline
l_k \leq p & 1^{st} \text{ of } \theta & 1^{st} \text{ of } \theta \\
1^{st} \text{ of } \theta & 2^{nd} \text{ of } \theta & 1^{st} \text{ of } \theta \\
2^{nd} \text{ of } \theta & & 2^{nd} \text{ of } \theta \\
\hline
\end{array}
\end{align*}

\( l_k > r - p \)
### Attack Scenarios

#### MAC-Keccak

<table>
<thead>
<tr>
<th>Condition</th>
<th>State XOR</th>
<th>State XOR</th>
<th>State XOR</th>
<th>State XOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>$l_k \leq r$</td>
<td>$1^{st}$</td>
<td>$2^{nd}$</td>
<td>$1^{st}$</td>
<td>$1^{st}$</td>
</tr>
<tr>
<td>$1^{st}$ of $\theta$</td>
<td></td>
<td></td>
<td>$1^{st}$</td>
<td></td>
</tr>
<tr>
<td>$2^{nd}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$p &lt; l_k \leq r - p$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1^{st}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2^{nd}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$l_k &gt; r - p$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1^{st}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2^{nd}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$l_k \equiv r$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1^{st}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2^{nd}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$l_k \equiv p$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1^{st}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2^{nd}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$p &lt; l_k \equiv r - p$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1^{st}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2^{nd}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$l_k \equiv r - p$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$1^{st}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2^{nd}$ of $\theta$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Diagram

- **KEY**
- **MSG**
- **F**
- **X**
- **y**
- **0 1 2 3 4 64**
- **0 1 2 3 4 → X**

---

- Virginia Tech
- Invent the Future
- Page 14
Practical Attack

• The reference software implementation.
• 32-bit Microblaze processor.
• On top of a Xilinx Spartan-3e FPGA.
• We used
  – Tektronix CT-2 current probe
  – Hamming Weight model.
Results
Why this research is useful?

• Keccak is the new SHA-3 standard.
• Keccak provides modes of operation for:
  – Hashing, stream encryption, MAC computation.
  – Reseable pseudo-random bit generator.
  – Authenticated encryption.
• Key-length is a new dimension in SCA.
  – In Keccak, DPA complexity increases faster than linear.
  – and, there is an optimum length.
• An almost-free DPA protection for MAC-Keccak.
Future Work

• Develop a systematic analysis for MAC-Keccak at any key-length.
• DPA protection of other Keccak modes of operation.
• Move the new concept to other cryptographic primitives.
Thank You