MK-3: Customizable Sponge-Based Authenticated Encryption

Professors P. Bajorski (COS), A. Kaminsky (GCCIS), M. Łukowiak (KGCOE), S. Radziszowski (GCCIS), RIT
Students M. Kelly (KGCOE), S. Soldavini (KGCOE), D. Stafford (KGCOE), G. Werner (GCCIS), C. Wood (GCCIS), RIT
Sponsors M. Kurdziel, S. Farris, Harris Corporation

Abstract. We introduce MK-3, a novel authenticated encryption algorithm based on the duplex sponge construction that is targeted for hardware implementation. We provide explicit customization guidelines for users who desire unique authenticated encryption solutions within our security margins. Our substitution step uses 16×16 AES-like S-boxes, which are novel because they are the largest bijective S-boxes to be used by an encryption scheme in the literature and are still efficiently implementable in both hardware and software. Several alternative hardware implementations of the algorithm using a field programmable gate array (FPGA) have been designed and analyzed, yielding encryption throughputs of 415 to 626 megabits per second. Statistical tests show that the algorithm’s core bijective function produces random outputs, as is necessary for a cryptographic algorithm.

Algorithm Design [3]

Goals
• Support authenticated encryption as well as encryption-only
• Support 128-bit and 256-bit key sizes
• Utilize state-of-the-art cryptographic design
• One pass over the plaintext
• Customizable
• Security analysis applicable to all customized versions
• FPGA implementation

Duplex Sponge Construction [9]

<table>
<thead>
<tr>
<th>Key/IV</th>
<th>AAD</th>
<th>PT1</th>
<th>PT2</th>
<th>PT3</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>C bits</td>
<td>R bits</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>Tag</td>
</tr>
</tbody>
</table>

Ni = initialization vector
AAD = Additional authenticated data
PT = Plaintext blocks
CT = Ciphertext blocks
Tag = Authentication tag
Generic security level = min (2^128, 2^128, 2^K), where K = key size [10]

Bijective Function F

Round Function

<table>
<thead>
<tr>
<th>Round Function</th>
<th>16 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 bits Layer</td>
<td>Substitution Layer</td>
</tr>
<tr>
<td>S = 16-bit substitution box (S-box)</td>
<td>M = Mixer</td>
</tr>
<tr>
<td>Each layer can be customized to give a different encryption algorithm with the same security as the original</td>
<td></td>
</tr>
</tbody>
</table>

FPGA Implementation [2]

S-box Implementation

S-box formula: S(ω) = A·ω^4 + b using GF(2^16) arithmetic

Recursive circuit for GF(2^4) inversion

GF(2^4) inversion circuit

GF(2^4) multiplication circuit

Bijective Function Throughput (Mbps)

<table>
<thead>
<tr>
<th>S-box Circuit</th>
<th>Mult. LUT</th>
<th>Inv. LUT</th>
<th>Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>GF(2^16)^2</td>
<td>None</td>
<td>None</td>
<td>527.7</td>
</tr>
<tr>
<td>GF(2^16)^2</td>
<td>None</td>
<td>GF(2^4)</td>
<td>626.0</td>
</tr>
<tr>
<td>GF(2^16)^2</td>
<td>GF(2^4)</td>
<td>GF(2^4)</td>
<td>525.2</td>
</tr>
<tr>
<td>GF(2^16)^2</td>
<td>GF(2^4)</td>
<td>GF(2^4)</td>
<td>414.6</td>
</tr>
<tr>
<td>GF(2^4)^2</td>
<td>None</td>
<td>GF(2^4)</td>
<td>528.3</td>
</tr>
<tr>
<td>GF(2^4)^2</td>
<td>GF(2^4)</td>
<td>GF(2^4)</td>
<td>626.0</td>
</tr>
<tr>
<td>GF(2^4)^2</td>
<td>GF(2^4)</td>
<td>GF(2^4)</td>
<td>525.2</td>
</tr>
</tbody>
</table>

Statistical Analysis

Methodology
• Feed a series of input values into the bijective function
• Each input differs from the previous input in one bit position
• Examine the frequency of 1 bits in the 512 output bit positions
• Examine output of round 1, round 2, . . . round 10
• Frequency should be close to 0.5

Results

• Nonrandom behavior = one or more frequencies too far from 0.5
• Nonrandom behavior detected in rounds 1 and 2
• No nonrandom behavior detected in rounds 3 and higher

Patents, Publications, Grants, References