Encryption algorithm Rocca-S
draft-nakano-rocca-s

Yuto Nakano, Kazuhide Fukushima, Takanori Isobe

CRFG@IETF115
Backgrounds

• Increase of throughput:
  • Peak data rate of the Internet is increasing
  • Consideration of new services (e.g. holography, digital twin) requiring higher (100+ Gbps) data rate

• High (256-bit) security encryption algorithm with 100+ Gbps throughput is required
Rocca-S

• Design
  • Sponge-based construction
  • 256-bit key and 256-bit tag
  • three modes: AEAD, encryption only and keystream generation

• Security (in the nonce respecting setting)
  • 256-bit security against key-recovery and forgery attacks

• Performance
  • First algorithm to exceed 200Gbps in software environment
    • 230Gbps (0.122 cycles/bytes) in an encryption only mode
    • 205Gbps in an AEAD mode
Design: Round function

- Seven 128-bit blocks are updated as $s^{\text{new}} = R(S, X_0, X_1)$ with AES round function $A$ and XOR $\oplus$
Design: Procedure

- Four phases: initialization, processing associated data, encryption and finalization
Design: Modes

- Rocca-S supports three modes:
  - AEAD mode
    - encryption + message authentication for plaintext and associated data
  - Encryption only mode
    - Message input to the internal state
    - Decryption will fail with a single bit error
  - Keystream generation mode
    - No message input to the internal state
    - Plaintext can be recovered even when ciphertext bits are flipped, except those flipped ones
Security claim

- 256-bit security against following attacks in the nonce-respecting setting:
  - key-recovery attacks
  - forgery attacks

- The lower bound of the number of active S-box (AS) in the initialization phase in single key setting

<table>
<thead>
<tr>
<th>Rounds</th>
<th>1R</th>
<th>2R</th>
<th>3R</th>
<th>4R</th>
<th>5R</th>
<th>6R</th>
<th>7R</th>
<th>8R</th>
<th>9R</th>
<th>10R</th>
<th>11R</th>
<th>12R</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>2</td>
<td>7</td>
<td>22</td>
<td>40</td>
<td>68</td>
<td>94</td>
<td>113</td>
<td>122</td>
<td>134</td>
<td>152</td>
<td>159</td>
<td>159</td>
</tr>
</tbody>
</table>

- The lower bound of the number of AS is 46 for forgery attack
Performance

- Performance evaluation of AEAD mode with “openssl -speed” on Intel® Core™ i9-12900K

![Graph showing throughput vs. message size for Rocca-S and AES-256-GCM]
Conclusion

• Encryption algorithm: Rocca-S
  • 256-bit security including forgery
  • 200+ Gbps on PC
  • AEAD, encryption only and keystream generation

• We do not claim any intellectual property rights and restrictions to use
• We plan to provide Rocca-S for OpenSSL on GitHub