Classification of the CAESAR Candidates

Farzaneh Abed  Christian Forler  Stefan Luck

Bauhaus-Universität Weimar

ESC 2015, Luxembourg

Jan, 2015
What is CAESAR?

- Competition for Authenticated Encryption: Security, Applicability, and Robustness
- Goal?
CAESAR

What is CAESAR?

- Competition for Authenticated Encryption: Security, Applicability, and Robustness
- Goal?
- New authenticated encryption schemes which:
What is CAESAR?

- Competition for Authenticated Encryption: Security, Applicability, and Robustness
- Goal?
- New authenticated encryption schemes which:
  - Offer advantages over AES-GCM
What is CAESAR?

- Competition for Authenticated Encryption: Security, Applicability, and Robustness
- Goal?
- New authenticated encryption schemes which:
  - Offer advantages over AES-GCM
  - Suitable for widespread adoption
Time Schedule

- Announced at ESC 2013
- Co-funded by US NIST?!
Time Schedule

- Announced at ESC 2013
- Co-funded by US NIST?! 
- First round submission: March 2014
- Reference software implementation: May 2014
Time Schedule

- Announcement of second round candidates: Jan 2015
- Second round tweak, software and hardware implementation: Feb, March, April 2015
Time Schedule

- Announcement of second round candidates: Jan 2015
- Second round tweak, software and hardware implementation: Feb, March, April 2015
- Announcement of third round candidates: Dec 2015
- Third round tweak, software and hardware implementation: Jan, Feb, March 2016
Time Schedule

- Announcement of second round candidates: Jan 2015
- Second round tweak, software and hardware implementation: Feb, March, April 2015
- Announcement of third round candidates: Dec 2015
- Third round tweak, software and hardware implementation: Jan, Feb, March 2016
- Announcement of finalist: Dec 2016
- Final tweak, software and hardware implementation: Jan, Feb, March 2017
Time Schedule

- Announcement of second round candidates: Jan 2015
- Second round tweak, software and hardware implementation: Feb, March, April 2015
- Announcement of third round candidates: Dec 2015
- Third round tweak, software and hardware implementation: Jan, Feb, March 2016
- Announcement of finalist: Dec 2016
- Final tweak, software and hardware implementation: Jan, Feb, March 2017
- Announcement of final portfolio: Dec 2017
Classification

Candidates

- 57 candidates for the first round!
- 8 candidates are broken
Classification of the CAESAR Candidates

Candidates

- 57 candidates for the first round!
- 8 candidates are broken
- What to compare:
  - Design approach
  - Functional features
  - Security
Design Approach

Block Cipher

Keyed family of permutation to encrypt message under a secret key.

- Full AES
- Round reduced AES
- New block cipher: KIASU, Deoxys, Joltik
Design Approach

Block Cipher

Keyed family of permutation to encrypt message under a secret key.

- Full AES
- Round reduced AES
- New block cipher: KIASU, Deoxys, Joltik

### Design

<table>
<thead>
<tr>
<th>Design</th>
<th>#Candidates</th>
<th>#Attacked</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES Blockcipher-based</td>
<td>17</td>
<td>7</td>
</tr>
<tr>
<td>Round reduced/Modified AES</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>New block cipher</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>
### Candidates

<table>
<thead>
<tr>
<th>AES-based</th>
<th>COPA, CFPB, CLOC, ELmD, iFeed, OCB, SILC, SHELL, YAES ++AE, CMCC, AVALANCHE JAMBU, CBA, POET, Julius</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-reduced-AES</td>
<td>AEZ, Silver</td>
</tr>
<tr>
<td>New BC</td>
<td>Deoxys, Joltik, KIASU, SCREAM, L-Block</td>
</tr>
</tbody>
</table>
Design Approach

Stream Cipher

Symmetric pseudo-random bit generator: takes fixed key and generates keystream of variable length.
Design Approach

Stream Cipher

Symmetric pseudo-random bit generator: takes fixed key and generates keystream of variable length.

Number of candidates: 8
Number of attacked candidates: 5
Design Approach

Stream Cipher

Symmetric pseudo-random bit generator: takes fixed key and generates keystream of variable length.

Number of candidates: 8
Number of attacked candidates: 5
Candidates:
Enchilada, HS1-SIV, Raviyoyla
Acorn, Sablier, Calico, Trivia-ck, Wheesht
**Permutation**

Bijective mapping on fixed-length string.

- Number of candidates: 3
- Number of attacked candidates: 1
Design Approach

Permutation

Bijective mapping on fixed-length string.

Number of candidates: 3
Number of attacked candidates: 1
Candidates:
Minalpher, PAEQ, Prøst
Design Approach

Sponge

Iterated function with variable length input/output from a permutation which operates on fixed length state.
Design Approach

**Sponge**

Iterated function with variable length input/output from a permutation which operates on fixed length state.

- Number of candidates: 9
- Number of attacked candidates: 3
Design Approach

**Sponge**

Iterated function with variable length input/output from a permutation which operates on fixed length state.

Number of candidates: 9
Number of attacked candidates: 3
Candidates:
Artemia, Ascon, Ketje, Keyak, NORX, STRIBOB, PRIMATE, ICEPOLE, \(\pi\)-Cipher
Compressor function

Compresses two fixed-length inputs to a single fixed-length output.

- Number of candidates: 1
- Number of attacked candidates: 0
Design Approach

Compression function

Compresses two fixed-length inputs to a single fixed-length output.

Number of candidates: 1
Number of attacked candidates: 0
Candidates: OMD
Design Approach

Dedicated

Message is used to update the state of the cipher and message authentication can be achieved for free.

Number of candidates: 3
Number of attacked candidates: 0
Design Approach

Dedicated

Message is used to update the state of the cipher and message authentication can be achieved for free.

Number of candidates: 3
Number of attacked candidates: 0
Candidates: AEGIS, MORUS, Tiaoxin
Overview

<table>
<thead>
<tr>
<th>Attribute</th>
<th>#Candidates/56</th>
<th>#Attacked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Cipher</td>
<td>30</td>
<td>14 (46.66%)</td>
</tr>
<tr>
<td>Sponge</td>
<td>10</td>
<td>4 (40%)</td>
</tr>
<tr>
<td>Stream Cipher</td>
<td>9</td>
<td>6 (66.66%)</td>
</tr>
<tr>
<td>Permutation</td>
<td>3</td>
<td>1 (33.33%)</td>
</tr>
<tr>
<td>Dedicated</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Compression Function</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

We don’t consider POLAWIS because of its complicated structure.
Functional Feature

Parallelizeable

Processing of $i$-th input block does not depend on the output of processing the $j$-th block.

Number of candidates: Encryption/Decryption 3/2
Number of candidates: Both Enc & Dec 30
Number of attacked candidates: 12
Functional Feature

Parallelizeable

Processing of $i$-th input block does not depend on the output of processing the $j$-th block.

Number of candidates: Encryption/Decryption $3/2$
Number of candidates: Both Enc & Dec $30$
Number of attacked candidates: $12$
### Candidates

<table>
<thead>
<tr>
<th>Only Encryption</th>
<th>AES-CPFB, iFeed, AEGIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only Decryption</td>
<td>AES-CMCC, SILC</td>
</tr>
<tr>
<td>Both Enc/DEC</td>
<td>AES-COPA, AES-OTR, AEZ, Deoxy, ELmD, Enchilada Joltik, Keyak, KIASU, Minalpher, NORX, OCB, PAEQ, SHELL, Silver, Tiaoxin, YAES ++AE, Acorn, AVALANCHE, CBA ICEPOLE, Julius, LAC, π-cipher Prøst, Sablier, SCREAM, Trivia-ck</td>
</tr>
</tbody>
</table>
Online

Encryption of the $i$-th input block $M_i$ depends only on the $M_1, \ldots, M_{i-1}$ blocks.

Number of candidates: 44
Number of attacked candidates: 15
<table>
<thead>
<tr>
<th>Not Online</th>
<th>AEZ, HS1-SIV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AES-CMCC, Julius, Trivia-ck</td>
</tr>
<tr>
<td>Attacked online candidates</td>
<td>++AE, AES-JAMBU, AVALANCHE</td>
</tr>
<tr>
<td></td>
<td>Calico, CBA, Julius, LAC, POET</td>
</tr>
<tr>
<td></td>
<td>Acorn, Sablier, Wheesht, ICEPOLE</td>
</tr>
<tr>
<td></td>
<td>PRIMATE, $\pi$-cipher, Prøst</td>
</tr>
</tbody>
</table>
Inverse-Free
Scheme requires only decryption or encryption function of underlying primitive.

Number of candidates: 37
Number of attacked candidates: 15
### Candidates

| COPA, CPFB, AEZ, OTR, CLOC, iFeed, SILC, YAES, AEGIS, MORUS, Tiaoxin, Enchilada, HS1-SIV, Raviyoyla, OMD PAEQ, Artemia, Ascon, Ketje, Keyak, NORX, STRIBOB, Calico, JAMBU, AVALANCHE, CBA, Julius, POET, Acorn, SCREAM, Sablier, Trivia-ck, Wheesht, ICEPOLE, PRIMATE, \( \pi \)-cipher, Prøst |
Functional Feature

Incremental Associated Data/AE

Given a previous authenticated (C,T) for message $M$, encrypting and authenticating message $M'$ which differ from $M$ with fraction, is computed only for changed block. Means, only the changed blocks and a finalization step need re-computation.

- Number of candidates: AD/AE 11/0
- Number of candidates: AD&AE 1
- Number of attacked candidates: 4
## Candidates

<table>
<thead>
<tr>
<th>Only Associated Data</th>
<th>AES-COPA, AES-OTR, AEZ</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enchilada, iFeed, OMD, YAES</td>
</tr>
<tr>
<td></td>
<td>CBA, POET, Sablier, Prøst</td>
</tr>
<tr>
<td>Both AD/AE</td>
<td>PAEQ</td>
</tr>
</tbody>
</table>
Functional Feature

Fixed-Associated Data Reuse

Using the same or slightly modified associated data for subsequent messages.

Number of candidates: 14
Number of attacked candidates: 5
Fixed-Associated Data Reuse
Using the same or slightly modified associated data for subsequent messages.

Number of candidates: 14
Number of attacked candidates: 5
Candidates:
Fixed-Associated Data Reuse

Using the same or slightly modified associated data for subsequent messages.

Number of candidates: 14
Number of attacked candidates: 5
Candidates:
AES-COPA, AES-OTR, AEZ, CLOC, Enchilada, iFeed, OMD, PAEQ, YAES
Functional Feature

Fixed-Associated Data Reuse

Using the same or slightly modified associated data for subsequent messages.

Number of candidates: 14
Number of attacked candidates: 5
Candidates:
AES-COPA, AES-OTR, AEZ, CLOC, Enchilada, iFeed, OMD, PAEQ, YAES, CBA, POET, PRIMATE, Prøst, Sablier
Intermediate Tags

Receiver detects early if parts of decrypted message are invalid.

Number of candidates: 7
Number of attacked candidates: 3
Intermediate Tags

Receiver detects early if parts of decrypted message are invalid.

Number of candidates: 7
Number of attacked candidates: 3
Candidates:
Intermediate Tags

Receiver detects early if parts of decrypted message are invalid.

Number of candidates: 7
Number of attacked candidates: 3
Candidates:
Ketje, Keyak, ELMd, iFeed, Trivia-ck, ICEPOLE, POET
## Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>#Candidates</th>
<th>#Attacked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parallelizeable</td>
<td>30</td>
<td>12</td>
</tr>
<tr>
<td>Online</td>
<td>44</td>
<td>15</td>
</tr>
<tr>
<td>Inverse-Free</td>
<td>37</td>
<td>15</td>
</tr>
<tr>
<td>Incremental AD/AE</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>Fixed AD reuse</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>Intermediate tag</td>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>
Input Masking Methods

- AX: Addition and XOR
- Doubling: XOR with a key dependent variable doubled in Galois Field
- GFM: Multiplication in Galois Field
- AES: XORing AES-processed chaining value
Input Masking Methods

- AX: Addition and XOR
- Doubling: XOR with a key dependent variable doubled in Galois Field
- GFM: Multiplication in Galois Field
- AES: XORing AES-processed chaining value

<table>
<thead>
<tr>
<th>Method</th>
<th>#Candidates</th>
<th>Candidates</th>
</tr>
</thead>
<tbody>
<tr>
<td>AX</td>
<td>1</td>
<td>++AE</td>
</tr>
<tr>
<td>Doubling</td>
<td>7</td>
<td>AES-COPA, AES-OTR, CBA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ELMd, iFeed, OCB, SHELL</td>
</tr>
<tr>
<td>GFM</td>
<td>1</td>
<td>Julius</td>
</tr>
<tr>
<td>AES</td>
<td>1</td>
<td>POET</td>
</tr>
</tbody>
</table>
Security

Privacy

- IND-CPA-Security
Security

Privacy
- IND-CPA-Security

Integrity
- INT-CTXT-Security
Provably Secure Candidates

Number of candidates: 33
Number of attacked candidates: 8
### Provably Secure Candidates

Number of candidates: 33  
Number of attacked candidates: 8

<table>
<thead>
<tr>
<th>Candidates</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-COPA, AES-CPFB, AES-OTR, AEZ</td>
</tr>
<tr>
<td>Artemia, Ascon, CLOC, Deoxy, ELmD, iFeed, Joltik, KIASU, OCB, SILC, SHELL</td>
</tr>
<tr>
<td>Silver, Enchilada, HS1-SIV, OMD, Minalpher, PAEQ, Ketje, Keyak, NORX, STRIBOB</td>
</tr>
<tr>
<td>AES-CMCC, AVALANCHE, ICEPOLE, Julius, POET, Trivia-ck, PRIMATE, Prøst</td>
</tr>
</tbody>
</table>

**Classification of the CAESAR Candidates**

Farzaneh Abed, Christian Forler, Stefan Luck
Robustness

- **Nonce-misuse:**
  - Offline scheme: PRP-CPA and INT-CTXT
  - Online scheme: OPRP-CPA and INT-CTXT
Robustness

- **Nonce-misuse**:  
  - Offline scheme: PRP-CPA and INT-CTX
  - Online scheme: OPRP-CPA and INT-CTX

- **Decryption-misuse**:  
  - Offline scheme: PRP-CCA
  - Online scheme: OPRP-CCA

<table>
<thead>
<tr>
<th>Robustness #</th>
<th>Candidates</th>
<th>Attacked Candidates</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMR</td>
<td>21</td>
<td>8</td>
</tr>
<tr>
<td>DMR</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>
Robustness

- Nonce-misuse:
  - Offline scheme: PRP-CPA and INT-CTXT
  - Online scheme: OPRP-CPA and INT-CTXT
- Decryption-misuse:
  - Offline scheme: PRP-CCA
  - Online scheme: OPRP-CCA

<table>
<thead>
<tr>
<th>Robustness</th>
<th>#Candidates</th>
<th>#Attacked Candidates</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMR</td>
<td>21</td>
<td>8</td>
</tr>
<tr>
<td>DMR</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Candidates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td><strong>NMR</strong></td>
<td>AES-COPA, AEZ, Deoxy, ELmD, iFeed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Joltik, KIASU, SHELL, HS1-SIV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minalpher, PAEQ, Artemia, Ascon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>++AE, AES-CMCC, AES-JAMBU</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICEPOLE, Julius, POET, PRIMATE, Prøst</td>
<td></td>
</tr>
<tr>
<td><strong>DMR</strong></td>
<td>AEZ, Minalpher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>POET, PRIMATE, Prøst</td>
<td></td>
</tr>
</tbody>
</table>
## Overview

### Statistic

<table>
<thead>
<tr>
<th>Candidates</th>
<th>#Unharmed</th>
<th>#Harmed</th>
<th>Conceded Broken</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>32 (56.14%)</td>
<td>18 (29.82%)</td>
<td>8 (14.03%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Broken Candidates</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBRA, CBEAM, FASER, HKC, McMambo, PAES, PANDA, Marble</td>
</tr>
</tbody>
</table>
Overview

Statistic

<table>
<thead>
<tr>
<th>Candidates</th>
<th>#Unharmed</th>
<th>#Harmed</th>
<th>Conceded Broken</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>32 (56.14%)</td>
<td>18 (29.82%)</td>
<td>8 (14.03%)</td>
</tr>
</tbody>
</table>

Broken Candidates

- COBRA
- CBEAM
- FASER
- HKC
- McMambo
- PAES
- PANDA
- Marble
### Attacks

<table>
<thead>
<tr>
<th>Forgery</th>
<th>Distinguish</th>
<th>Key/State Recovery</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>5</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Classification</td>
<td>Candidates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forgery</td>
<td>++AE, Calico, COBRA, JAMBU, Julius-ECB, LAC, AVALANCHE, CMCC, HKC, Marble, McMambo, Screa, Wheesht, POET, PAES, PANDA, CBEAM, (\pi)-cipher, Prøst-OTR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key/State Recovery</td>
<td>PRIMATE, ICEPOLE, Sablier, Wheesht, Trivia-ck, Acorn, PANDA, FASER, Calico, Marble, Prøst-OTR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distinguish</td>
<td>CBA, CMCC, FASER, ICEPOLE, Wheesht</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Pi-Cipher, PRIMATE, POET</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Thank you for your attention!