Announcement of the CAESAR finalists

Daniel J. Bernstein

CAESAR timeline planned in 2012

2013.01: Announce “tentative schedule”.
2014.01: Deadline for first-round submissions.
2015.01: Announce second-round candidates.
2016.01: Announce third-round candidates.
2017.01: Announce finalists.
2018.01: Announce final portfolio.

CAESAR timeline planned in 2012

2013.01: Announce “tentative schedule”.
2014.01: Deadline for first-round submissions.
2015.01: Announce second-round candidates.
2016.01: Announce third-round candidates.
2017.01: Announce finalists.
2018.01: Announce final portfolio.

. . . but all sides requested extra time.

. . . and all sides requested an extra feedback loop between submitters and committee members.

Actual CAESAR timeline

2013.01:	Announce “tentative schedule”.
2014.03:	Deadline for first-round submissions.
2015.07:	Announce second-round candidates.
2016.08:	Announce third-round candidates.
2018.03:	Announce finalists.
Later:	Announce final portfolio.

Use Case 1: Lightweight applications (resource constrained environments)

- critical: fits into small hardware area and/or small code for 8-bit CPUs
- desirable: natural ability to protect against side-channel attacks
- desirable: hardware performance, especially energy/bit
- desirable: speed on 8-bit CPUs
- message sizes: usually short (can be under 16 bytes), sometimes longer

Use Case 2: High-performance applications

- critical: efficiency on 64-bit CPUs (servers) and/or dedicated hardware
- desirable: efficiency on 32-bit CPUs (small smartphones)
- desirable: constant time when the message length is constant
- message sizes: usually long (more than 1024 bytes), sometimes shorter

Use case 3: Defense in depth

- critical: authenticity despite nonce misuse
- desirable: limited privacy damage from nonce misuse
- desirable: authenticity despite release of unverified plaintexts
- desirable: limited privacy damage from release of unverified plaintexts
- desirable: robustness in more scenarios; e.g., huge amounts of data

An important caveat

"The submitter/submitters understand
that the selection of some algorithms is not
a negative comment regarding other algorithms,
and that an excellent algorithm might fail to be
selected simply because not enough analysis was
available at the time of the committee decision."

The CAESAR finalists

The CAESAR finalists

- ACORN for use case 1.
- AEGIS for use case 2. However, if AEGIS is selected for the final portfolio, one of AEGIS-128 and AEGIS-128L will be dropped, by default AEGIS-128L.
- Ascon for use case 1.
- COLM for use case 3.
- Deoxys-II for use case 3.
- MORUS for use case 2.
- OCB for use case 2.

Last chance for analysis before the final portfolio!