Changelog – Ascon v1.2

Updates on 31 May 2021

`asconv12.pdf`:

- Fix typo in Section 2.5.1: Remove excessive and incorrect zeros in 64-bit IV of Ascon-Hash and Ascon-Hasha.

Updates on 17 May 2021 (NIST LWC Final Round)

`Algorithms`:

- The specifications and test vectors of Ascon-128, Ascon-128a, Ascon-80pq, Ascon-Xof, and Ascon-Hash remain unchanged.
- Added a new hash function Ascon-Hasha and extendable output function Ascon-Xofa to the Ascon familiy.

  Compared to Ascon-Hash and Ascon-Xof, Ascon-Hasha and Ascon-Xofa use 8 rounds during absorbing and most of the squeezing instead of 12, while the transition between absorbing and squeezing still uses 12 rounds. We have reduced the number of rounds where the current analysis shows a very large security margin in order to get a less conservative and faster variant that pairs nicely with Ascon-128a. Moreover, we hope that these less conservative variants Ascon-Hasha and Ascon-Xofa encourage more cryptanalysis of the hash function in the last round of the standardization process.

`asconv12.pdf`:

- Updated Chapter 1 to introduce also the new variants Ascon-Hasha and Ascon-Xofa
- Replaced the algorithm $\mathcal{X}_{h,r,a}$ with $\mathcal{X}_{h,r,a,b}$ in order to define new variants Ascon-Hasha and Ascon-Xofa in Chapter 2. $\mathcal{X}_{h,r,a,b}$ is identical to $\mathcal{X}_{h,r,a}$ if $a = b$ and so $\mathcal{X}_{h,r,a,a} = \mathcal{X}_{h,r,a}$.
- Added Ascon-Hasha to the recommended parameter sets at second place for hash function in Section 2.2.
- Added Ascon-128a and Ascon-Hasha as recommended pairing for authenticated encryption and hashing in Section 2.2.

- Updated description of algorithms for hashing and extendable output functions in Section 2.5. They now allow to instantiate Ascon-Hasha and Ascon-Xofa. Please note that the changes in description do not influence Ascon-Hash and Ascon-Xof. Hence, Ascon-Hash and Ascon-Xof remain identical to the previous rounds with the test vectors still the same.
- Added security claims for Ascon-Hasha and Ascon-Xofa in Chapter 3.
- Small updates of features in Chapter 4.
- Added design rationale for Ascon-Hasha and Ascon-Xofa in Chapter 5.
- Updated the security analysis of Chapter 6 with recently published insights into the security of Ascon.
- Added section on size-optimized Ascon implementations in Chapter 7.
- Added recently published papers covering implementation aspects to Chapter 7.
- Fixed typos.

`asconv12.tar.gz`:

- Add implementations for Ascon-Hasha and Ascon-Xofa
- Add combined software implementations supporting AEAD and hashing:
  - Ascon-128 and Ascon-Hash in `crypto_aead_hash/asconv12`
  - Ascon-128a and Ascon-Hasha in `crypto_aead_hash/asconav12`
- Add size-optimized implementations
- Add AVX-512 implementations
- Generalize code base

Updates on 27 September 2019 (NIST LWC Round 2)

`asconv12.pdf`:

- Update title page (date, layout)
- Add new references to Section 7.4 on implementation security and robustness.

`asconv12.tar.gz`:

- Use constant-time comparison.