Changelog – ISAP v2.0

Updates on 17 May 2021 (NIST LWC Final Round)

`isapv20.pdf`:

- Changed ordering of recommended parameters sets in Section 2.5 as announced at the NIST Lightweight Cryptography Workshop (October 2020).

  This change is motivated by (1) the better performance of Ascon's permutation on 32-bit devices, (2) the noticeably lower area requirements of Ascon-based Isap instances in hardware. Note that the specification of the individual Isap instances remains the same.
- Adaption in Section 1 to reflect the change of ordering.
- Added reference to Ascon design document and NIST FIPS PUB 202 for pairings with already specified hash functions in Section 2.6.
- Changed ordering of instances in the table of Section 3.
- Changed text in Section 4.6 to reflect the changed ordering of recommended parameter sets.
- Changed ordering of instances in the tables of Section 4.6.1.
- Added reference to Isap v2.0 ToSC publication in Section 5.1.
- Updated list of published analysis in Section 5.
- Cite new insights into the security of the tag comparison in Section 6.1.4.
- Updated implementation results in Section 6.
- Fixed typos throughout document.

`isapv20.tar.gz`:

- In `crypto_aead`: Added plattform optimized implementations for 64-bit CPUs (`opt_64`, `avx512`) and 32-bit CPUs (`opt_32`, `opt_32_arm`)
- In `crypto_aead_hash`: Added combined implementations for Isap-A-128a and AsconHash.

Updates on 27 September 2019 (NIST LWC Round 2)

`isapv20.pdf`:

- Updated titlepage (date, website link, layout)
- Added brief discussion of recent papers on the leakage resilience of ISAP to Section 5.1.
- Added new references to Section 5.2 on the security of Keccak.
- Added reference to website in Table 6.1 and Table 6.2.
- Converted "Runtime per block" into "Runtime per byte" in Table 6.2.
- Added statement about runtime of masked versions of ISAP in Section 6.1.1.
- Mentioned data complexity in Section 6.1.3.

`isapv20.tar.gz`:

- No changes