Variants

Notation:

Number of Blocks

Symbols *Na*, *Nm*, *Nc*, *Nh* represent the number of complete blocks of associated data, plaintext, ciphertext, and hash message, respectively.

Incomplete Blocks

Symbols *Ina*, *Inm*, *Inc*, *Inh* represent the completeness of a block of of associated data, plaintext, ciphertext, and hash message, respectively. These are binary variables equal to 1 if the last block is incomplete and 0 if it is complete.

Valid Bytes

Symbols *Bla*, *Blm*, *Blc*, *Blh* represent the number of valid bytes in an incomplete block of associated data, plaintext, ciphertext, and hash message, respectively.

1. v1

aceae128v1 & acehash256v1

A. Design goal.

Support for authenticated encryption, decryption, and hashing. Balance throughput and area use by unfolding SB-64 function loop, but maintaining ACE-permutation folded.

Resource Use

```
< 2000 LUTs
< 4000 FFs
No BRAMs
No DSP units
```

B. Supported maximum sizes of inputs.

Authenticated Encryption

No limit.

Authenticated Decryption

No limit.

Hashing

No limit.

C. Reference software implementation.

A copy of the original authors' reference implementation can be found in:

```
src_sw/crypto_aead/aceae128v1/ref/
src_sw/crypto_hash/acehash256v1/ref/
```

For all their code and documents, see their team website.

D. Non-default values of generics and constants.

No changes to generics and constants of synthesizable sources.

Changed LWC testbench KAT file paths to absolute paths:

```
G_FNAME_PDI
G_FNAME_SDI
G_FNAME_DO
```

E. Block Sizes

```
AD block size:                    64 bits
Plaintext/Ciphertext block size:  64 bits
Hash block size:                  64 bits
```

F. Execution times (in clock cycles)

Authenticated Encryption

With no incomplete last blocks:

= 60 + 18*Na* + *16* + *18Nm* + 16 + 36

= 18*Na* + *18Nm* + 128

With incomplete last blocks:

= 60 + 18*Na* + *18Nm* + 36

= 18*Na* + *18Nm* + 96

Authenticated Decryption

With no incomplete last blocks:

= 60 + 18*Na* + *16* + *18Nc* + 16 + 37

= 18*Na* + *18Nc* + 129

With incomplete last blocks:

= 60 + 18*Na* + *18Nc* + 37

= 18*Na* + *18Nc* + 97

Hashing

With no incomplete last blocks:

= 1 + 16 + 18**Nh* + 16 + 2 + 16 + 2 + 16 + 2 + 16 + 2

= 18**Nh* + 89

With incomplete last blocks:

= 1 + 16 + 18**Nh* + 2 + 16 + 2 + 16 + 2 + 16 + 2

= 18**Nh* + 81

G. Latencies

Authenticated Encryption

No clock cycle latency.

Authenticated Decryption

No clock cycle latency.

H. Difference between execution times for a new key and the same key.

Authenticated Encryption

Key reuse saves four cycles key read cycles plus one idle cycle, for a total of five saved cycles.

Authenticated Decryption

Key reuse saves four cycles key read cycles plus one idle cycle, for a total of five saved cycles.