Haraka

Efficient Short-Input Hashing for Post-Quantum Applications

Stefan Kölbl[1] Martin M. Lauridsen[1] Florian Mendel[2] Christian Rechberger[1,2]

March 22, 2015

[1]DTU Compute, Technical University of Denmark, Denmark

[2]IAIK, Graz University of Technology, Austria

Haraka

Hash-based Signature Schemes

- XMSS (IETF Draft), SPHINCS
- Post-Quantum secure with minimal assumptions

Haraka

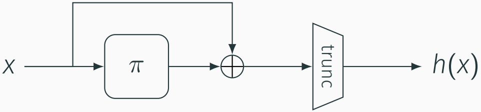
Hash-based Signature Schemes

- XMSS (IETF Draft), SPHINCS
- Post-Quantum secure with minimal assumptions
- Require many calls to a hash function but...
- ...only need to hash short inputs.
- ...do not require collision resistance.

Haraka

Haraka

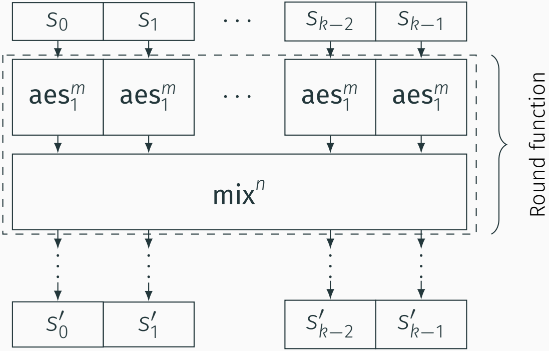
- Designed specifically for short inputs.
- Very efficient permutation π utilizing AES-NI.



Haraka

Internal permutation π

- Use k AES states $s_0, \ldots, s_{k-1}$
- Round function: $\mathsf{mix} \circ \mathsf{aes}^m$



Haraka

Performance for single inputs

	Haswell	Skylake
Haraka-512/256	1.77 cpb	0.95 cpb
Haraka-256/256	0.97 cpb	0.66 cpb

- Latency $\approx$ 60 cycles for Haraka-512/256

Haraka

Paper on e-print:

`https://eprint.iacr.org/2016/098`

Reference Implementation and Cryptanalysis:

`https://github.com/kste/haraka`