HARAKA V2

Efficient Short-Input Hashing for Post-Quantum Applications

Stefan Kölbl[1] Martin M. Lauridsen[2] Florian Mendel[3] Christian Rechberger[1,3]

March 7th, 2017

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

[2]InfoSec Global Ltd., Switzerland

[3]IAIK, Graz University of Technology, Austria

Impact of Quantum Computers

- Public-key
    - Diffie-Hellman
    - RSA
    - Elliptic Curves
- Symmetric-key
    - Block Ciphers
    - Hash Functions

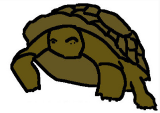
Impact of Quantum Computers

- Public-key
  - ~~Diffie-Hellman~~
  - ~~RSA~~
  - ~~Elliptic Curves~~
- Symmetric-key
  - Block Ciphers (Larger key)
  - Hash Functions (Longer output)

POST-QUANTUM CRYPTOGRAPHY

NIST-call[1]

- Digital Signature Scheme
- Encryption / Key Establishment



PQCrypto Project[2]

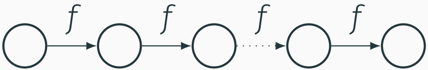
[1] http://csrc.nist.gov/groups/ST/post-quantum-crypto/
[2] https://pqcrypto.eu.org/

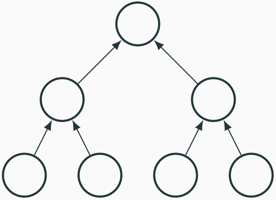
Hash-based Signature Schemes

- Post-quantum secure
- Minimal Assumptions
- Lamport [Lam79], Merkle Tree [Mer89], XMSS [BDH11], SPHINCS [BHH+15], ...

Performance of hash-based signature schemes

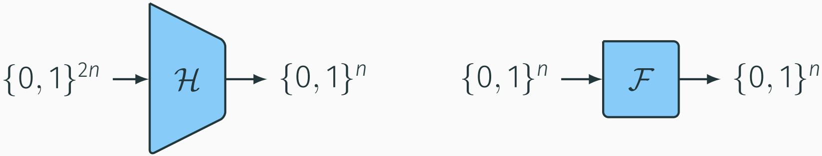
- Many calls to the hash function…
- …but using short input only.
- …no collision resistance required.

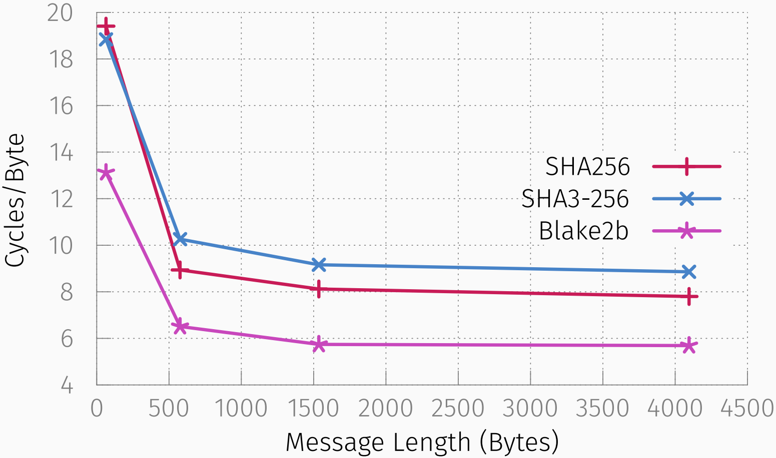




Example SPHINCS:

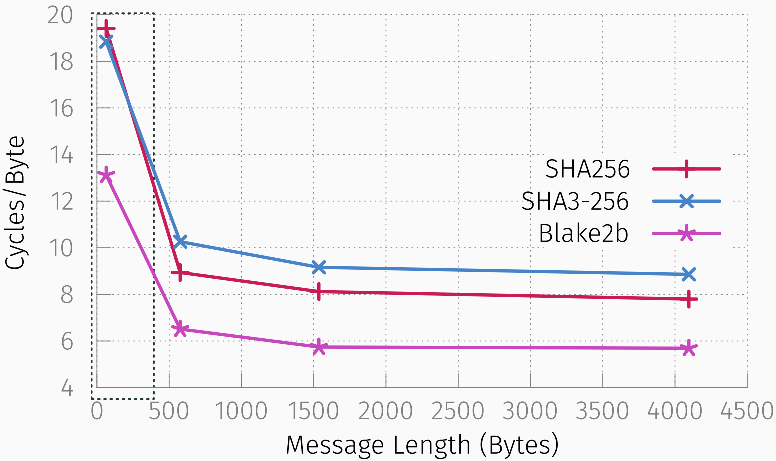
- Provides 128-bit post-quantum security.
- Signing takes roughly 500.000 hash function evaluations.





[2] Benchmarks from SUPERCOP on Intel Core i5-6600

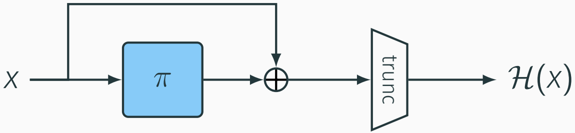
HARAKA



[2] Benchmarks from SUPERCOP on Intel Core i5-6600

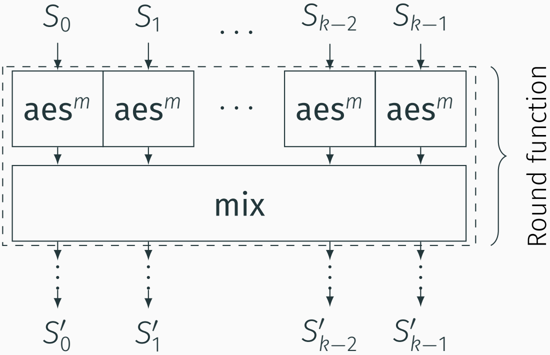
A short-input hash function

- AES-based.
- 256- and 512-bit permutation.
- Using Davies-Meyer with 0 key.

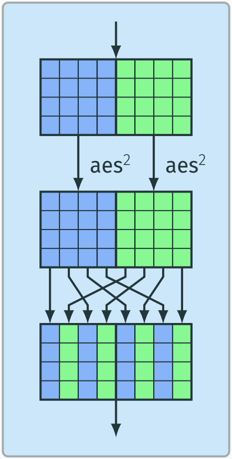


Internal permutation of Haraka v2

- Substitution Permutation Network
- Round function: $\mathsf{mix} \circ \mathsf{aes}^m$



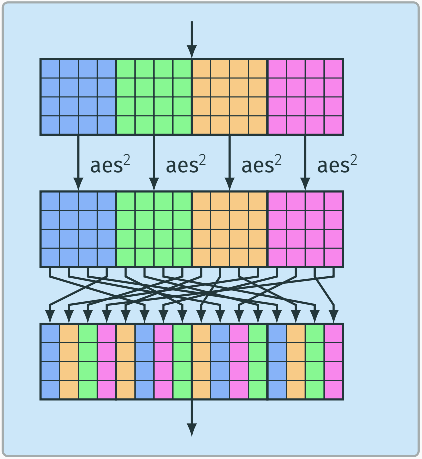
Haraka-256 v2



Requires only 6 instructions per round

- $4 \times$ `vaesenc`
- `vpunpckldq`, `vpunpckhdq`

Haraka-512 v2



Requires only 16 instructions per round

- 8 × **vaesenc**
- 8 for **mix**

Security Analysis

- Active S-boxes
    - 80 for Haraka-256 v2
    - 130 for Haraka-512 v2
- Truncated Differentials
- Meet-in-the-Middle attacks
- Round Constants [Jea16]

HARAKA

Performance

- AES instructions have high latency.
- Costs for mixing can be hidden.
- Often multiple independent blocks available.

Single Input

	Haswell Cycles/Byte	Skylake Cycles/Byte
Haraka-256 v2	**1.25**	**0.72**
Simpirav2[$b = 2$]	1.91	1.09
SPHINCS-256-F	11.31	11.12
Haraka-512 v2	**1.75**	**0.97**
Simpirav2[$b = 4$]	4.5	2.12
SPHINCS-256-H	11.16	10.92

Multiple Inputs

	Haswell Cycles/Byte	Skylake Cycles/Byte
Haraka-256 v2	**1.14**	**0.63**
Simpirav2[$b = 2$]	0.96	0.94
SPHINCS-256-F	2.11	1.71
Haraka-512 v2	**1.43**	**0.72**
Simpirav2[$b = 4$]	0.94	0.94
SPHINCS-256-H	1.99	1.62

SPHINCS on Intel Skylake

	ChaCha12 Cycles	Haraka v2[3] Cycles
Key generation	2,839,018	1,340,338 (×2.12)
Signing	43,517,538	20,782,894 (×2.09)
Verification	1,291,980	415,586 (×3.11)

[3] Updated numbers from `https://github.com/kste/haraka`.

CONCLUSION

Summary

- AES-based SPN for Short-Input Hash.
- Low Latency
- Can speed up SPHINCS significantly.

Future Work

- ARMv8 platform
- Collision vs. Preimage

Implementation of Haraka and SPHINCS-256-Haraka

https://github.com/kste/haraka

Questions?

REFERENCES I

- Johannes A. Buchmann, Erik Dahmen, and Andreas Hülsing, *XMSS - A practical forward secure signature scheme based on minimal security assumptions*, Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, 2011, pp. 117–129.
- Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn, *SPHINCS: practical stateless hash-based signatures*, Advances in Cryptology - EUROCRYPT 2015, 2015, pp. 368–397.

REFERENCES II

- Jérémy Jean, *Cryptanalysis of haraka*, IACR Trans. Symmetric Cryptol. **2016** (2016), no. 1, 1–12.
- Leslie Lamport, *Constructing digital signatures from a one-way function*, Tech. report, Technical Report CSL-98, SRI International Palo Alto, 1979.
- Ralph C. Merkle, *A certified digital signature*, Advances in Cryptology - CRYPTO '89, 1989, pp. 218–238.