Putting Wings on SPHINCS

PQCRYPTO 2017 - Recent Results

Stefan Kölbl

June 26th, 2017

DTU Compute, Technical University of Denmark

Putting Wings on SPHINCS

SPHINCS

- Hash-based Signature Scheme
- **Stateless**
- 128-bit post-quantum security
- Sizes:
  - Public Key: 1kb
  - Secret Key: 1kb
  - Signature: 41kB

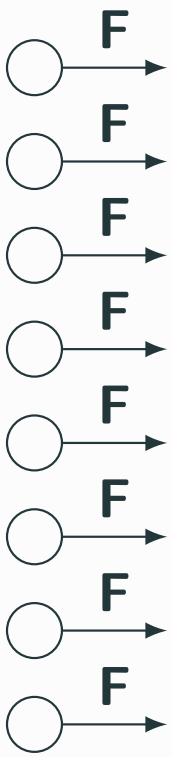
`https://sphincs.cr.yp.to/`

Putting Wings on SPHINCS

For one signature

- 450.000 times $\mathbf{F} : \{0,1\}^{256} \rightarrow \{0,1\}^{256}$
- 90.000 times $\mathbf{H} : \{0,1\}^{512} \rightarrow \{0,1\}^{256}$

Many calls in parallel:

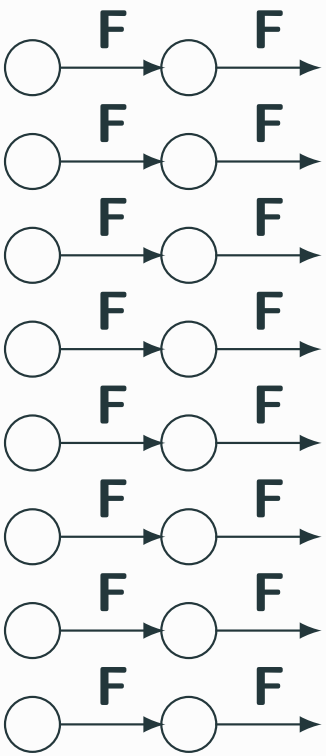


Putting Wings on SPHINCS

For one signature

- 450.000 times $\mathbf{F} : \{0,1\}^{256} \rightarrow \{0,1\}^{256}$
- 90.000 times $\mathbf{H} : \{0,1\}^{512} \rightarrow \{0,1\}^{256}$

Many calls in parallel:

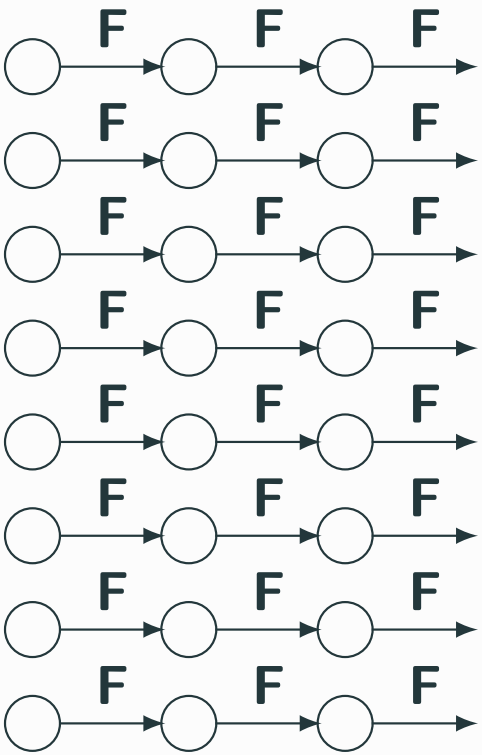


Putting Wings on SPHINCS

For one signature

- 450.000 times $\mathbf{F} : \{0,1\}^{256} \rightarrow \{0,1\}^{256}$
- 90.000 times $\mathbf{H} : \{0,1\}^{512} \rightarrow \{0,1\}^{256}$

Many calls in parallel:

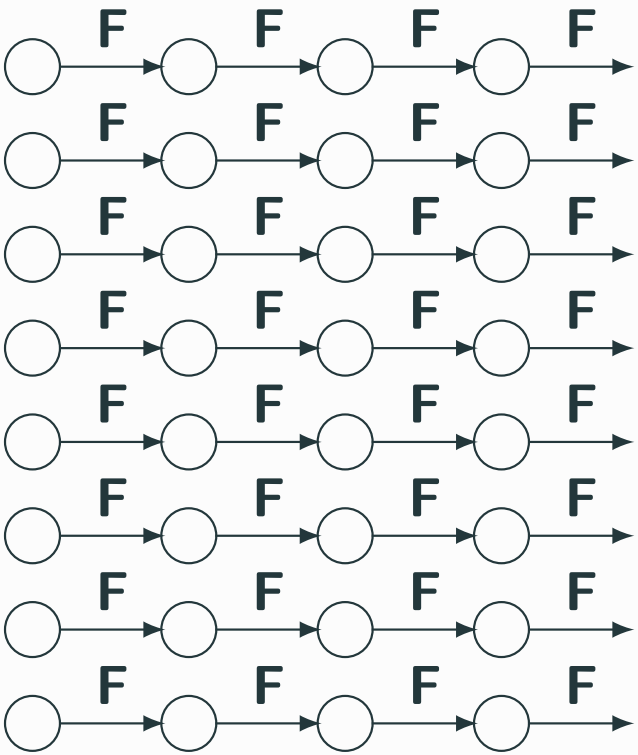


Putting Wings on SPHINCS

For one signature

- 450.000 times $\mathbf{F} : \{0,1\}^{256} \rightarrow \{0,1\}^{256}$
- 90.000 times $\mathbf{H} : \{0,1\}^{512} \rightarrow \{0,1\}^{256}$

Many calls in parallel:

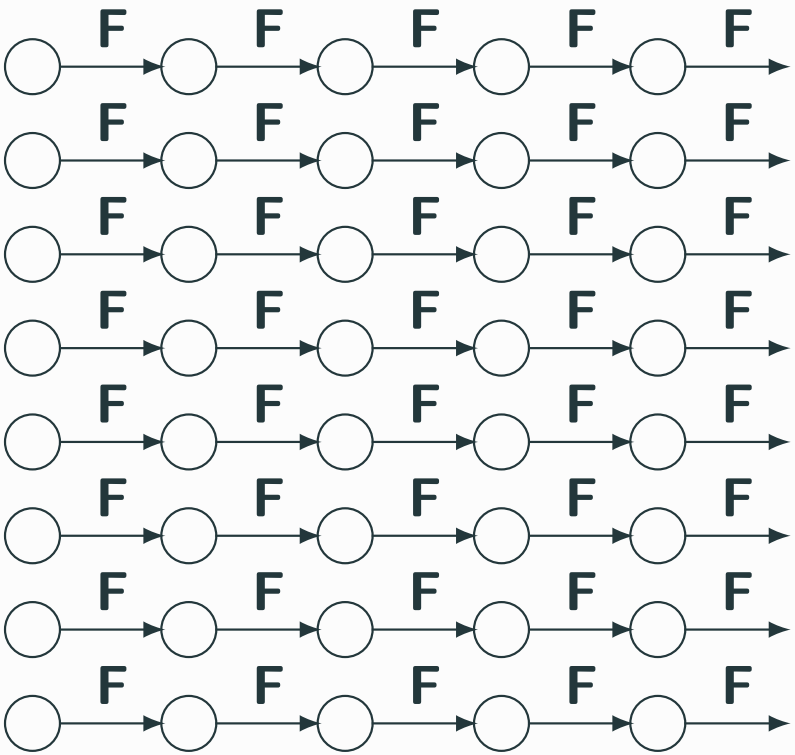


Putting Wings on SPHINCS

For one signature

- 450.000 times $\mathbf{F} : \{0,1\}^{256} \rightarrow \{0,1\}^{256}$
- 90.000 times $\mathbf{H} : \{0,1\}^{512} \rightarrow \{0,1\}^{256}$

Many calls in parallel:

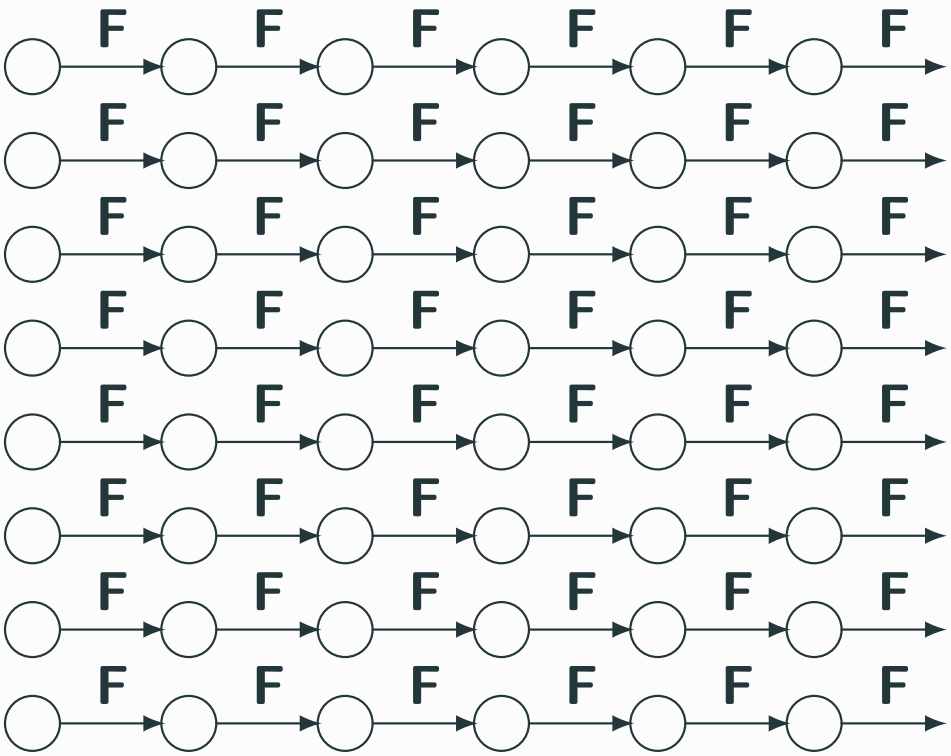


Putting Wings on SPHINCS

For one signature

- 450.000 times $\mathbf{F} : \{0,1\}^{256} \rightarrow \{0,1\}^{256}$
- 90.000 times $\mathbf{H} : \{0,1\}^{512} \rightarrow \{0,1\}^{256}$

Many calls in parallel:

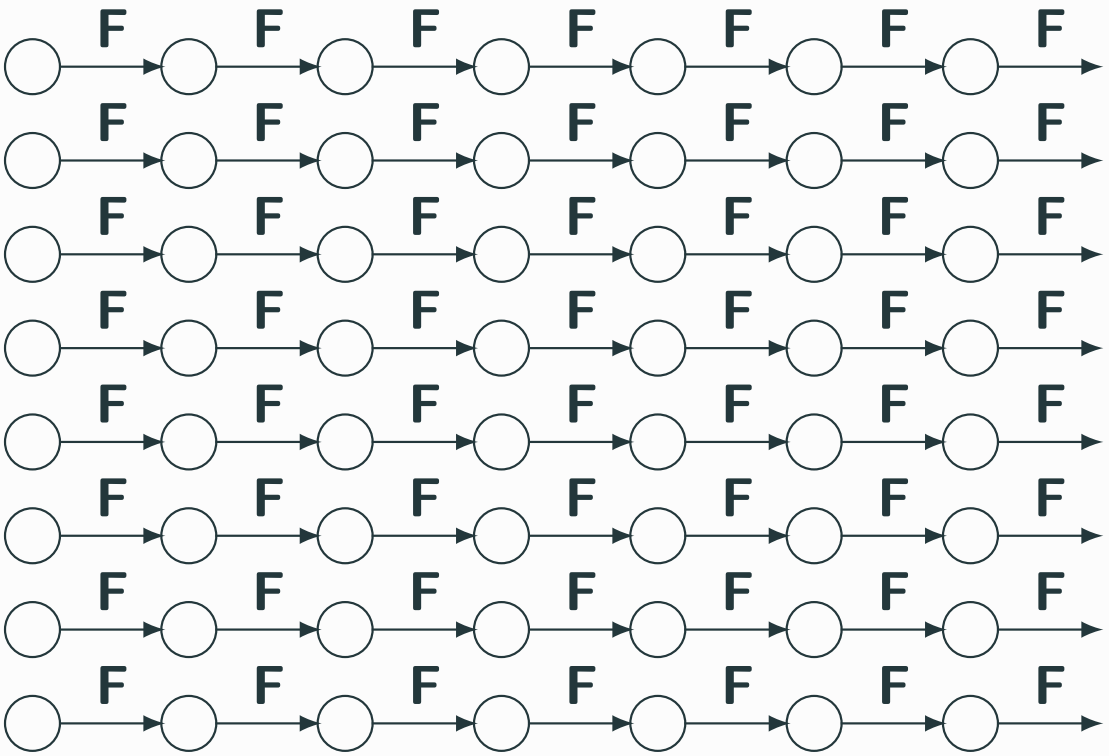


Putting Wings on SPHINCS

For one signature

- 450.000 times $\mathbf{F} : \{0,1\}^{256} \rightarrow \{0,1\}^{256}$
- 90.000 times $\mathbf{H} : \{0,1\}^{512} \rightarrow \{0,1\}^{256}$

Many calls in parallel:

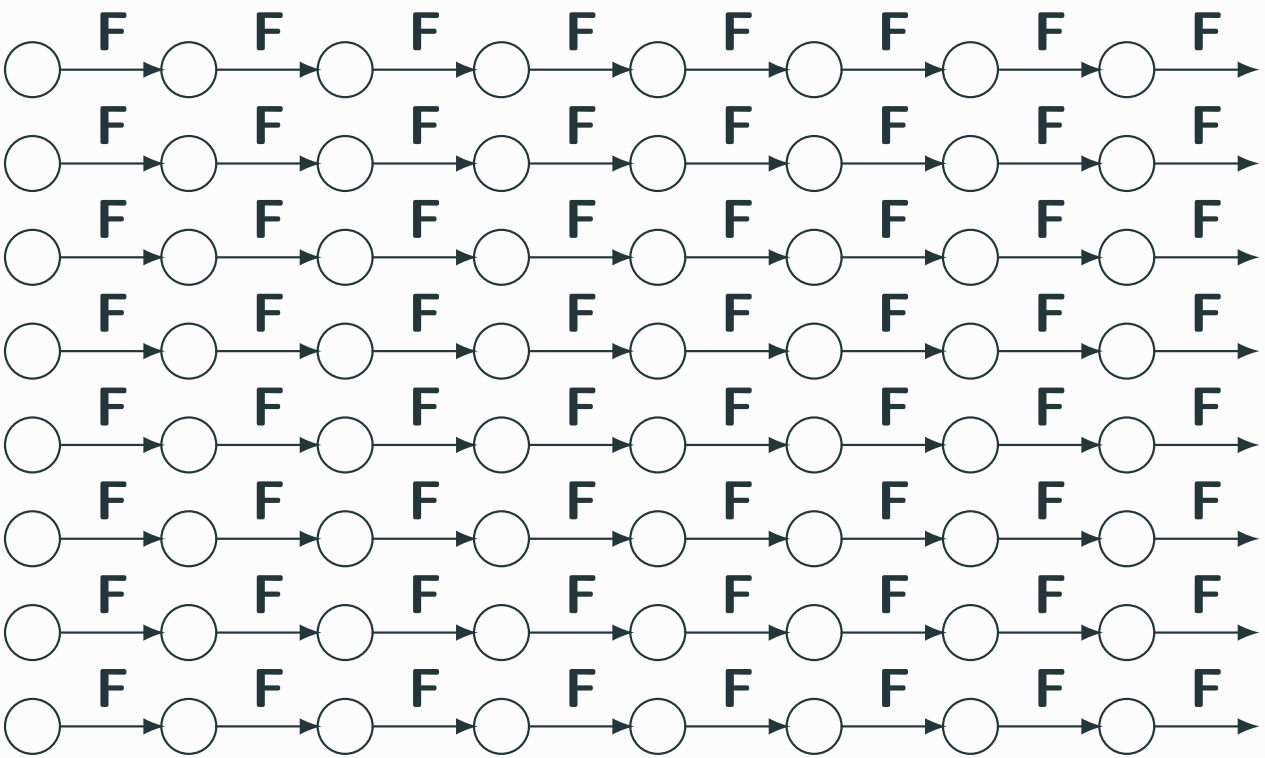


Putting Wings on SPHINCS

For one signature

- 450.000 times **F** : $\{0,1\}^{256} \rightarrow \{0,1\}^{256}$
- 90.000 times **H** : $\{0,1\}^{512} \rightarrow \{0,1\}^{256}$

Many calls in parallel:

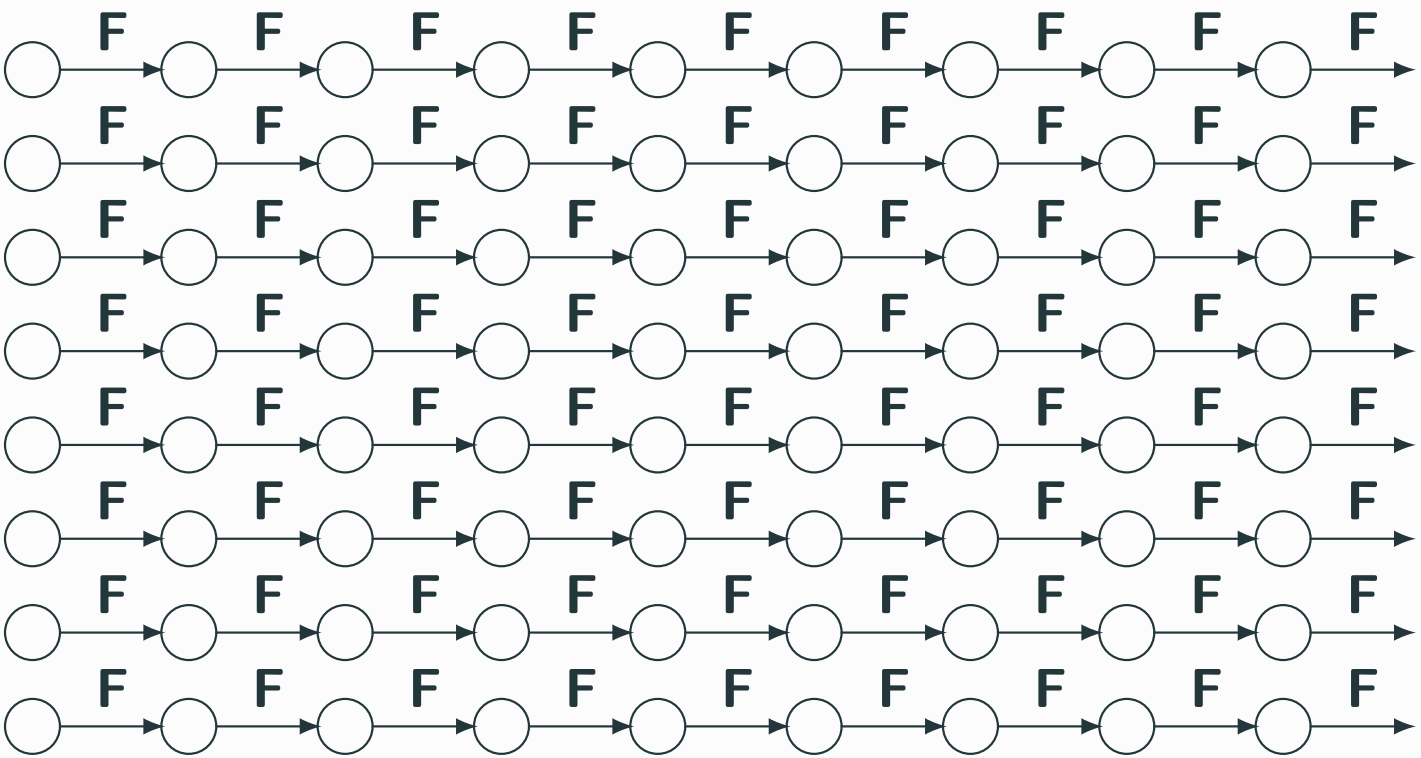


Putting Wings on SPHINCS

For one signature

- 450.000 times **F** : $\{0,1\}^{256} \rightarrow \{0,1\}^{256}$
- 90.000 times **H** : $\{0,1\}^{512} \rightarrow \{0,1\}^{256}$

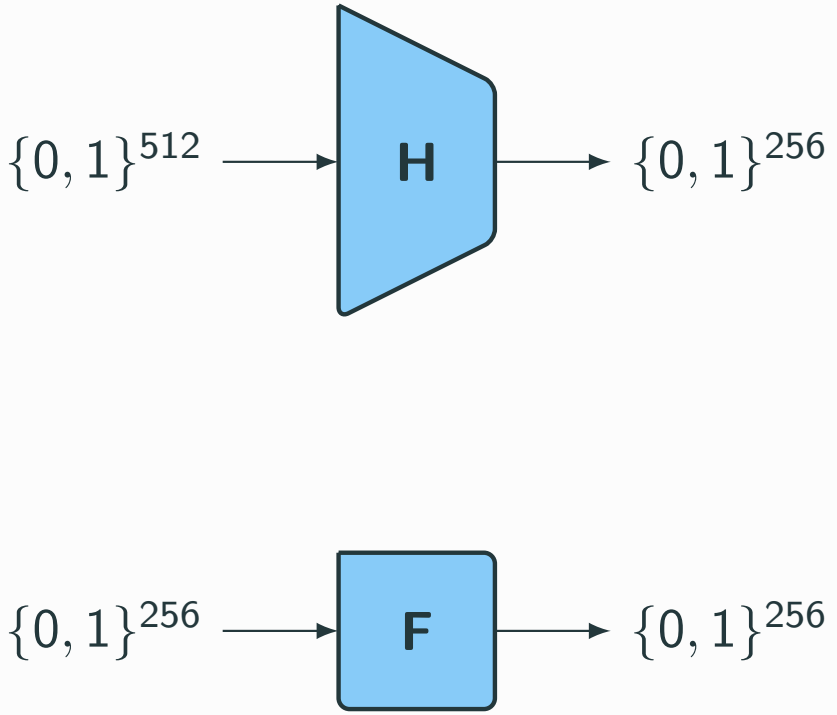
Many calls in parallel:



Putting Wings on SPHINCS

How to instantiate?

- SHA-3 / Keccak
- SHA256
- ChaCha
- Haraka (AES-based)
- Simpira (AES-based)



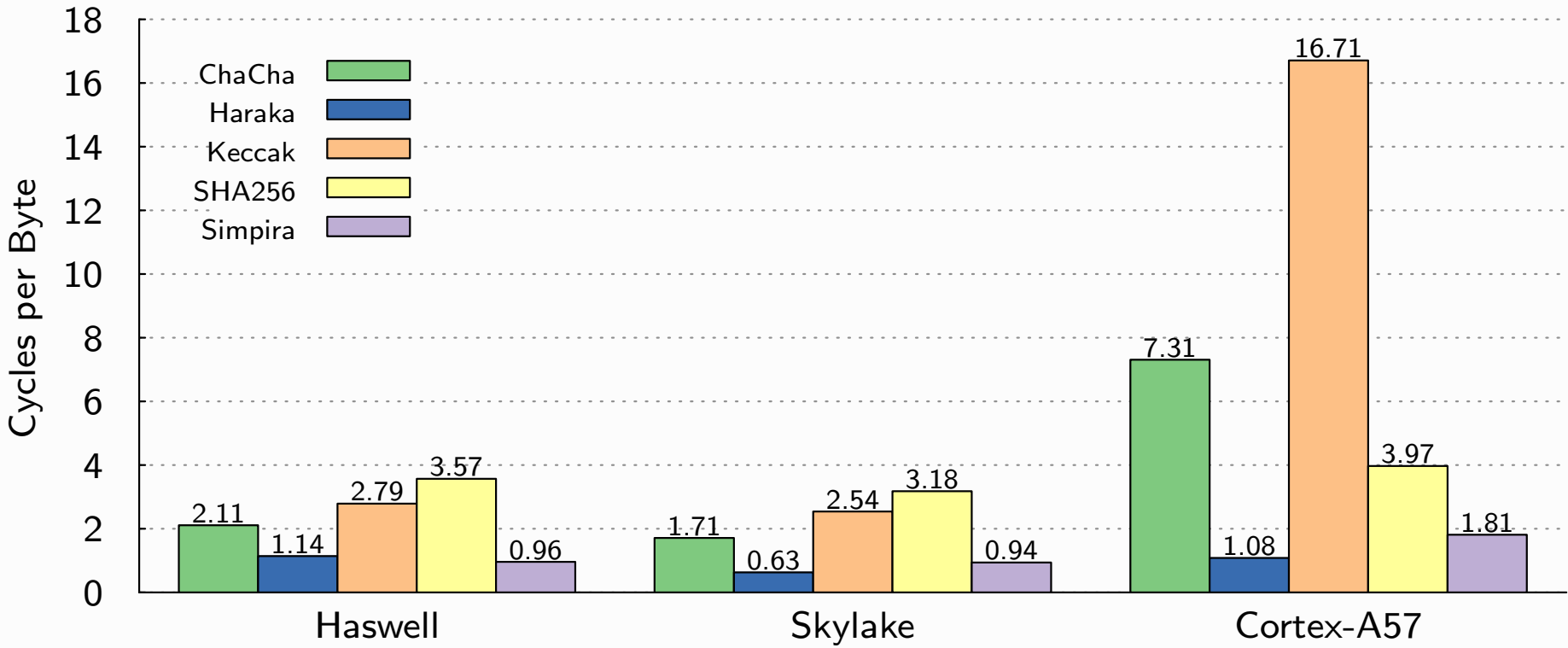
Putting Wings on SPHINCS

How to get fast implementation?

- Vectorization (AVX2, NEON)
- Hardware Support (AES, SHA-2)
- Parallelization trivial for SPHINCS

Putting Wings on SPHINCS

Performance of $\mathbf{F} : \{0,1\}^{256} \rightarrow \{0,1\}^{256}$



[0]Keccak with $b = 800$ and 12 rounds.

Putting Wings on SPHINCS

Architecture	Primitive	KeyGen	Sign	Verify
Intel Skylake	ChaCha	2.839.018	43.495.454	1.291.980
	Haraka	1.340.338	20.782.894	415.586
	Keccak	6.589.798	108.629.952	2.152.066
	SHA256	8.724.516	142.063.840	2.812.466
	Simpira	1.808.830	28.408.658	520.832
ARM Cortex A57	ChaCha	10.361.344	191.782.400	3.488.256
	Haraka	2.223.616	46.241.792	750.080
	Keccak	22.006.272	376.908.288	7.358.464
	SHA256	5.292.032	94.082.048	1.679.872
	Simpira	3.044.864	60.507.136	928.256