# SPHINCS$^{+}$

Jean-Philippe Aumasson, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, **Andreas Hülsing**, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe

# Hash-based signatures

Boring crypto:

- Dates back to beginning of public key cryptography
- No fancy new mathematical assumption:
  Only requires a secure hash function
  („minimal security assumptions“)
- Stateful schemes already in standardization

# SPHINCS

Joint work with Daniel J. Bernstein, Daira Hopwood, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O’Hearn

# Stateless hash-based signatures

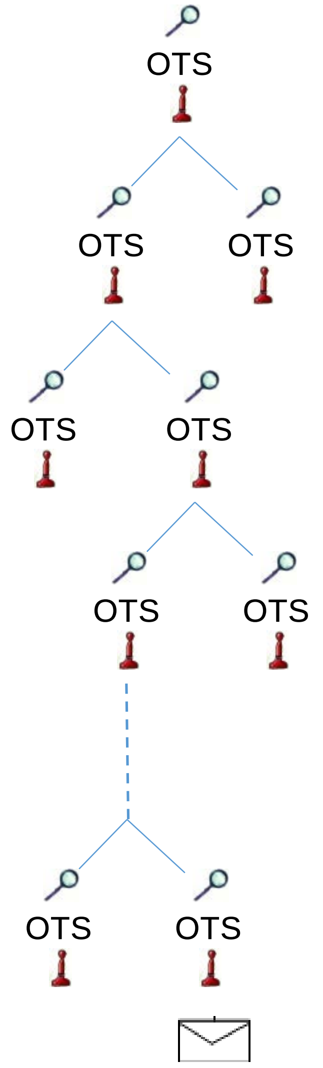
[NY89,Gol87,Gol04]

Goldreich's approach [Gol04]:

Security parameter $\lambda = 128$

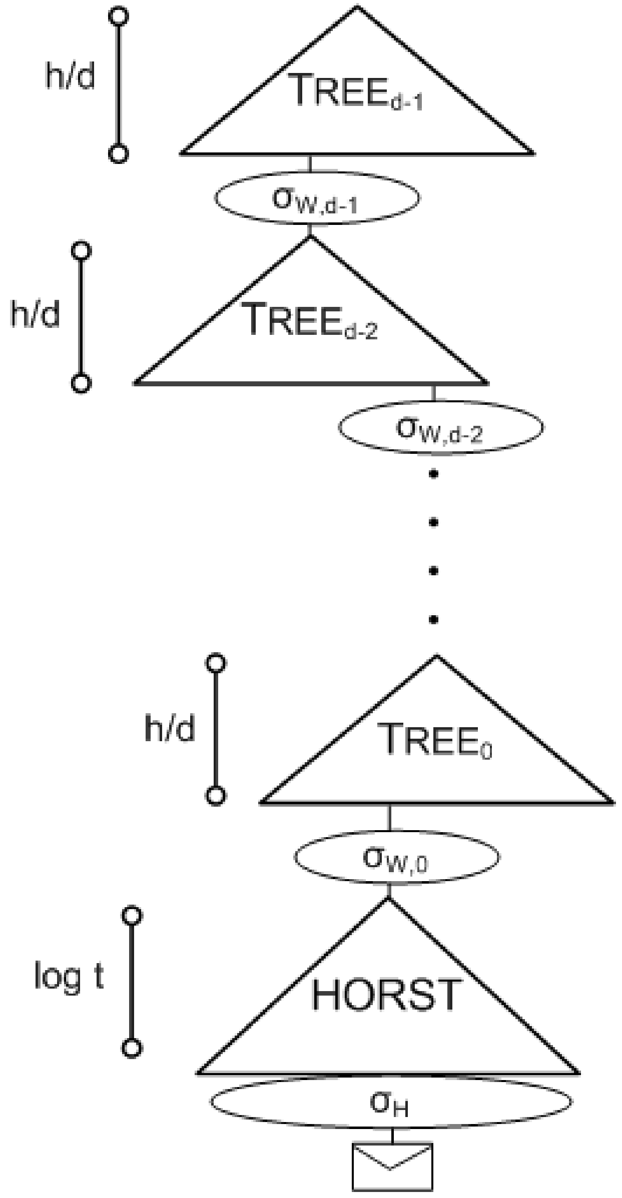
Use binary tree as in Merkle, but...

- ...for security
  - pick index i at random;
  - requires huge tree to avoid index collisions (e.g., height $\mathrm{h} = 2\lambda = 256$).
- ...for efficiency:
  - use binary certification tree of OTS key pairs (= Hypertree with $d = h$),
  - all OTS secret keys are generated pseudorandomly.



# SPHINCS [BHH+15]

- Select index pseudorandomly
- Use a few-time signature key-pair on leaves to sign messages
  - Few index collisions allowed
  - Allows to reduce tree height
- Use hypertree: Use d << h.



# SPHINCS$^+$ in 1st Round

Joint work with Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe

# SPHINCS$^+$ vs SPHINCS

- Allow for $2^{64}$ instead of $2^{50}$ signatures per key pair
- Add multi-target attack mitigation (Tweakable hash functions)
- New few-time signature scheme FORS
- Verifiable index selection
- Optional non-deterministic signatures

# SPHINCS$^+$ in 2nd Round

Joint work with Jean-Philippe Aumasson, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe

# 2nd Round changes

- One new team member: 1/2 Gravity-SPHINCS (J.-P. Aumasson)
- “Simple”-instantiations (of tweakable hash functions)
- Performance optimization for SHA-256 instantiations
- Fixed tight security reduction

# Instantiations

- SPHINCS$^+$-SHAKE256-robust
- SPHINCS$^+$-SHAKE256-simple NEW!
- SPHINCS$^+$-SHA-256-robust
- SPHINCS$^+$-SHA-256-simple NEW!
- SPHINCS$^+$-Haraka-robust
- SPHINCS$^+$-Haraka-simple NEW!

Simple instantiations inspired by LMS: All security reasoning in (Q)ROM

# Instantiations (cycles for SHA2)

| Scheme | | Cycles | | | Bytes | | |
|---|---|---|---|---|---|---|---|
| | sec | keypair | sign | verify | sig | pk | sk |
| SPHINCS$^+$-SHA-256-128s-simple | L1 | 49 078 104 | 835 272 076 | 2 348 916 | 8 080 | 32 | 64 |
| SPHINCS$^+$-SHA-256-128s-robust | L1 | 94 988 100 | 1 624 566 118 | 4 700 588 | 8 080 | 32 | 64 |
| SPHINCS$^+$-SHA-256-128f-simple | L1 | 1 602 368 | 51 805 308 | 5 676 578 | 16 976 | 32 | 64 |
| SPHINCS$^+$-SHA-256-128f-robust | L1 | 2 978 018 | 96 974 576 | 11 401 188 | 16 976 | 32 | 64 |
| SPHINCS$^+$-SHA-256-192s-simple | L3 | 69 860 954 | 1 737 629 602 | 3 662 790 | 17 064 | 48 | 96 |
| SPHINCS$^+$-SHA-256-192s-robust | L3 | 134 664 612 | 3 024 929 742 | 7 784 118 | 17 064 | 48 | 96 |
| SPHINCS$^+$-SHA-256-192f-simple | L3 | 2 116 010 | 66 380 214 | 9 611 814 | 35 664 | 48 | 96 |
| SPHINCS$^+$-SHA-256-192f-robust | L3 | 4 390 738 | 133 192 018 | 19 219 918 | 35 664 | 48 | 96 |
| SPHINCS$^+$-SHA-256-256s-simple | L5 | 85 946 882 | 1 121 074 298 | 4 903 926 | 29 792 | 64 | 128 |
| SPHINCS$^+$-SHA-256-256s-robust | L5 | 350 260 762 | 4 064 645 574 | 13 790 402 | 29 792 | 64 | 128 |
| SPHINCS$^+$-SHA-256-256f-simple | L5 | 5 298 662 | 133 374 038 | 9 408 596 | 49 216 | 64 | 128 |
| SPHINCS$^+$-SHA-256-256f-robust | L5 | 21 672 826 | 495 051 104 | 26 825 462 | 49 216 | 64 | 128 |

# SHA-256 optimization

$$\mathrm{F}(\mathrm{PK}.seed, \mathrm{ADRS}, M_1) = \mathrm{SHA{-}256}(\mathrm{PK}.seed \mid\mid \mathrm{toByte}(0, 64 - n) \mid\mid \mathrm{ADRS}^c \mid\mid M_1^{\oplus})$$

**Ensure that key dependent input fills first block (precompute & reuse state)**

**Compress ADRS to fit padding in second block**

**Only 1 compression function call per F call!**

**Table 2: Performance comparison of different symmetric-crypto-based signature schemes on the Intel Haswell microarchitecture. All software is optimized using architecture-specific optimizations such as AESNI or AVX2 instructions.**

| Scheme | Cycles | | | Bytes | | |
|---|---|---|---|---|---|---|
| | keypair | sign | verify | sig | pk | sk |
| **Comparison to SPHINCS-256** | | | | | | |
| SPHINCS-256 [8] | 2 868 464[a] | 50 462 856[a] | 1 672 652[a] | 41 000 | 1 056 | 1 088 |
| SPHINCS$^+$ (Haraka, robust) ($n = 192, h = 51, d = 17, b = 7, k = 45, w = 16$) | 1 254 968[b] | 29 015 002[b] | 2 739 770[b] | 30 696 | 48 | 96 |
| **Comparison to Gravity-SPHINCS** | | | | | | |
| Gravity-SPHINCS [5] (parameter-set L) | 30 729 044 392[a] | 32 564 796[a] | 625 752[a] | max: 35 168 avg: ?[c] | 32 | 1 048 608 |
| SPHINCS$^+$ (Haraka, robust) ($n = 192, h = 66, d = 22, b = 8, k = 33, w = 16$) | 1 257 826[b] | 38 840 268[b] | 3 467 192[b] | 35 664 | 48 | 96 |
| SPHINCS$^+$ (Haraka, simple) ($n = 192, h = 64, d = 16, b = 7, k = 49, w = 16$) | 1 892 462[b] | 35 029 380[b] | 1 460 204[b] | 30 552 | 48 | 96 |
| **Comparison to Picnic** | | | | | | |
| Picnic2-L5-FS [16] | 18 244[c] | 904 189 188[c] | 268 485 212[c] | max: 54 732 avg: 46 282 | 65 | 97 |
| SPHINCS$^+$ (SHA-256, simple) ($n = 256, h = 63, d = 9, b = 12, k = 29, w = 16$) | 43 317 320[b] | 527 413 100[b] | 5 463 884[b] | 33 408 | 64 | 128 |

[a] As reported by SUPERCOP [10] from 3.5GHz Intel Xeon E3-1275 V3 (Haswell)
[b] Median of 100 runs on 3.5GHz Intel Xeon E3-1275 V3 (Haswell), compiled with `gcc-5.4 -O3 -march=native -fomit-frame-pointer -flto`
[c] As reported by SUPERCOP [10] from 3.1GHz Intel Xeon E3-1220 V3 (Haswell)
[d] Neither [5] nor [6] report the average size of signatures; the analysis in [4] suggests that it is about 1KB smaller than the worst-case size.

# Tight security reduction

“2. This claim is incorrect, because the theorem apparently does not apply to the proposed instantiations: it requires the component function F to have a structural property that it almost certainly does not have. (Indeed, it seems hard to find *any* suitable instantiation having the property.)”

Chris Peikert, May 24, 2018

# Ugly fixes:

a) Rely on loose security reduction

b) Build artificial hash with property

$$F = \mathrm{SHA2{-}256}(K, \mathrm{SHA2{-}256}(K, M)_{0\ldots248})$$

Cost of factor 2 speed penalty and slightly decreased security

# More elegant fix

Replace statistical property by new computational assumption:

Decisional second-preimage resistance (DSPR) [BH19]

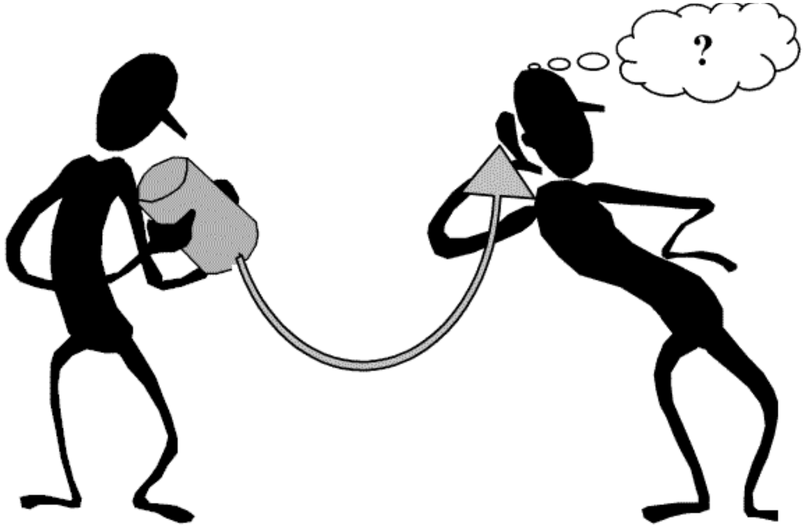
Intuition:

Given domain element it is hard to decide if second-preimage exists (with probability better than guessing)

# Conclusion

- SPHINCS$^+$ beats performance of other symmetric crypto based signatures for comparable parameters.
- Possible synergies with standardizing stateful hash-based signatures
- New *simple* instantiations integrate well with an LMS-like stateful scheme.
- Re-established tight security proof.
- *The* most conservative submission in the competition.

# Thank you!
# Questions?



# Structural property

- “Every n bit string has at least one colliding n bit string under $F_K$“

Use in proof:

We can turn preimage finder $A$ for $F_K$ into second-preimage finder $B$ for $F_K$.

- $B(x)$: On input $x$ return $A(F_K(x))$
- If property holds,

$$\Pr\left[A\left(F_K(x)\right) \neq x\right] \geq \frac{1}{2}$$