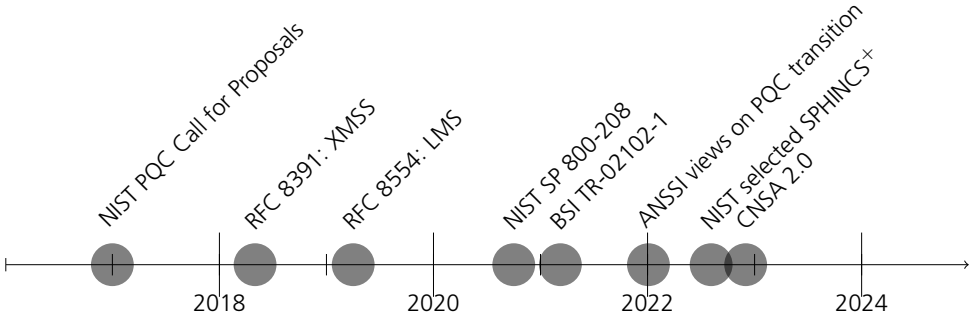
Faulting Winternitz One-Time Signatures to forge LMS, XMSS, or SPHINCS$^+$ signatures

Alexander Wagner, Vera Wesselkamp, Felix Oberhansl, Marc Schink, Emanuele Strieder,
August 18, 2023

Hash-based signatures

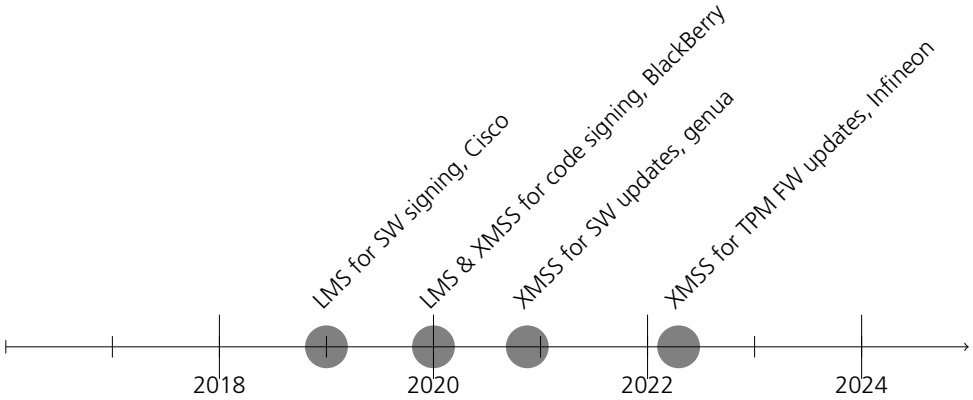
Standardisations and regulations



Fraunhofer AISEC

Hash-based signatures

Exemplary real-world applications



Hash-based signatures

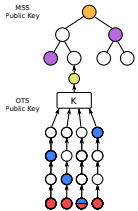
Implementation security

- Side-channel analysis by Kannwischer et al.
  - Timing or SPA not promising
  - DPA targets the underlying hash function
- Fault attacks
  - *Grafting Trees* attack by Castelnovi et al.
  - Very powerful
  - Not applicable to all HBS schemes
  - No other attacks are publicly known

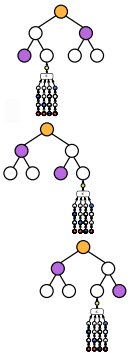
Research question: How resilient are HBS schemes against fault attacks?

Background

Tree structure



single-tree

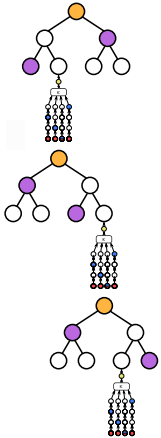


multi-tree

Fraunhofer AISEC

Background

Grafting Trees attack



Background

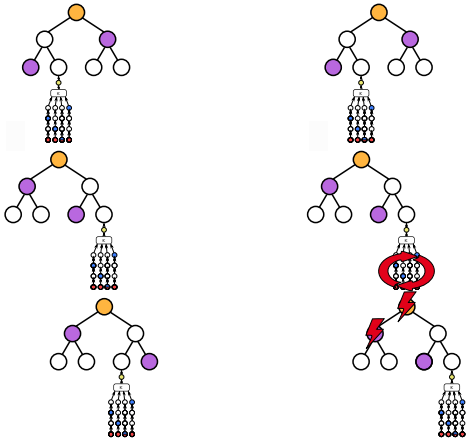
Grafting Trees attack

- Fault introduces errors into a root node

→ Reuse of a WOTS instance

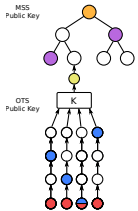
- Single reuse compromises security

	single-tree	multi-tree
signing	✗	✓
verifying	✗	✗

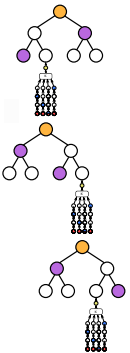


Background

Tree structure



single-tree



multi-tree

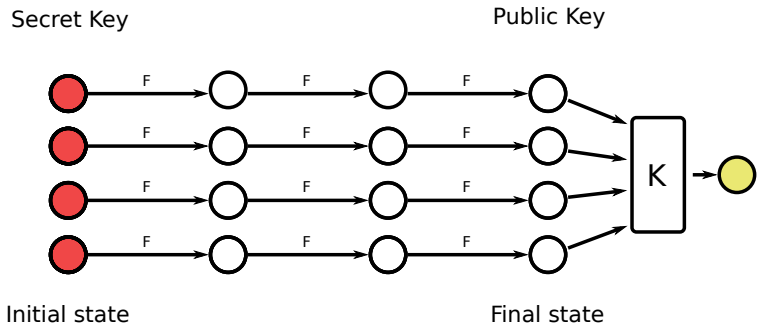
Fraunhofer AISEC

Background

Winternitz one-time signatures

- Winternitz parameter $w = 4$

→ hash chain length: $w - 1 = 3$



private key public key

Fraunhofer AISEC

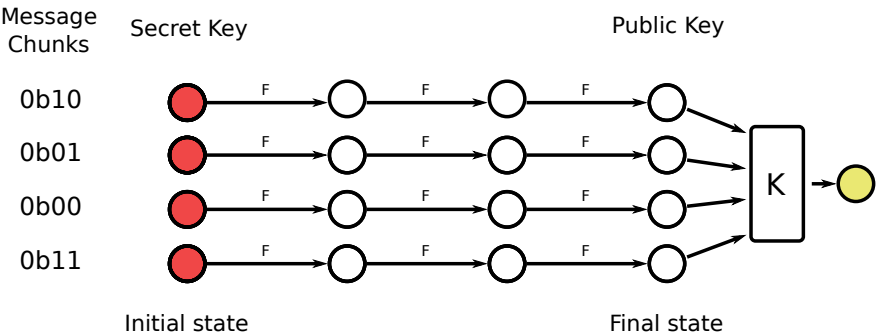
Background

Winternitz one-time signatures

- Winternitz parameter $w = 4$

→ hash chain length: $w - 1 = 3$

→ chunk bitsize: $log_2(w) = 2$



private key public key

Fraunhofer AISEC

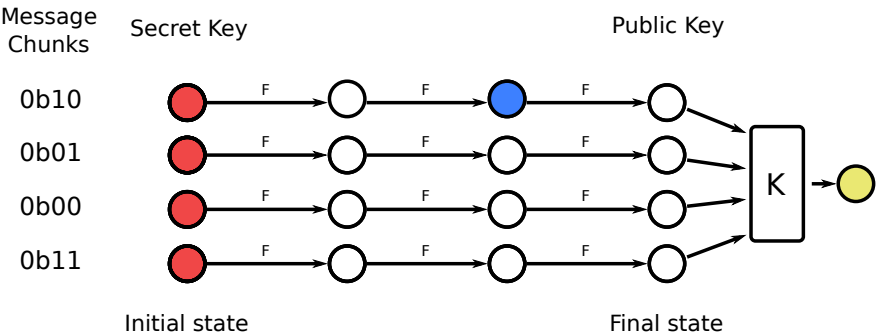
Background

Winternitz one-time signatures

- Winternitz parameter $w = 4$

→ hash chain length: $w - 1 = 3$

→ chunk bitsize: $log_2(w) = 2$



private key public key signature

Fraunhofer AISEC

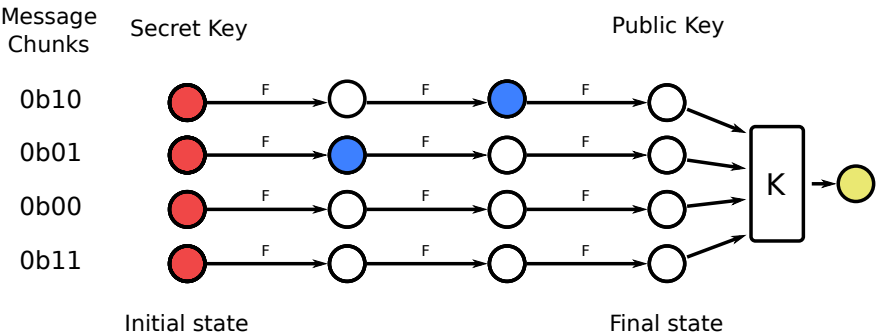
Background

Winternitz one-time signatures

- Winternitz parameter $w = 4$

→ hash chain length: $w - 1 = 3$

→ chunk bitsize: $log_2(w) = 2$



private key public key signature

Fraunhofer AISEC

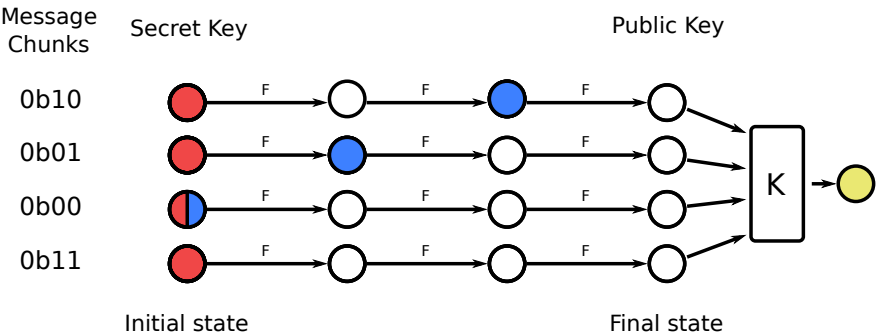
Background

Winternitz one-time signatures

- Winternitz parameter $w = 4$

→ hash chain length: $w - 1 = 3$

→ chunk bitsize: $log_2(w) = 2$



private key public key signature

Fraunhofer AISEC

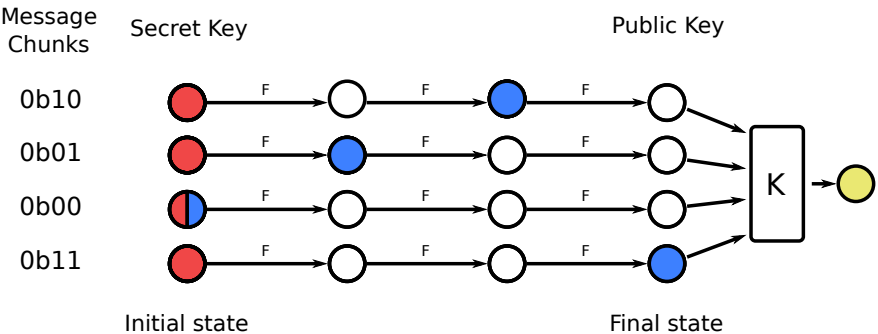
Background

Winternitz one-time signatures

- Winternitz parameter $w = 4$

→ hash chain length: $w - 1 = 3$

→ chunk bitsize: $log_2(w) = 2$



private key public key signature

Fraunhofer AISEC

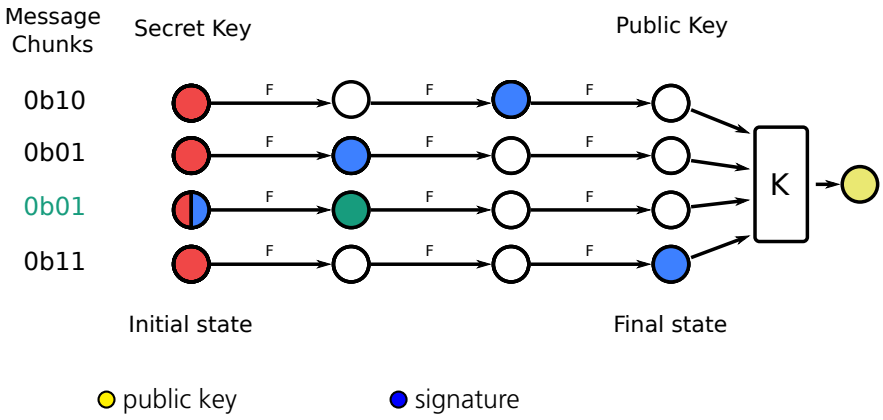
Background

Winternitz one-time signatures

- Winternitz parameter $w = 4$

→ hash chain length: $w - 1 = 3$

→ chunk bitsize: $log_2(w) = 2$



Fraunhofer AISEC

Background

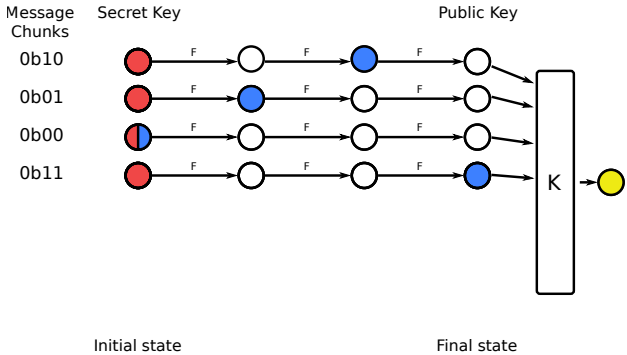
Winternitz one-time signatures

Checksum mechanism:

$$c = \mathcal{C}(m) = \sum_{i=0}^{l_1-1} (w - 1 - m_i)$$

$$c = 1 + 2 + 3 + 0$$

$$c = 6 = 0b0110$$



Background

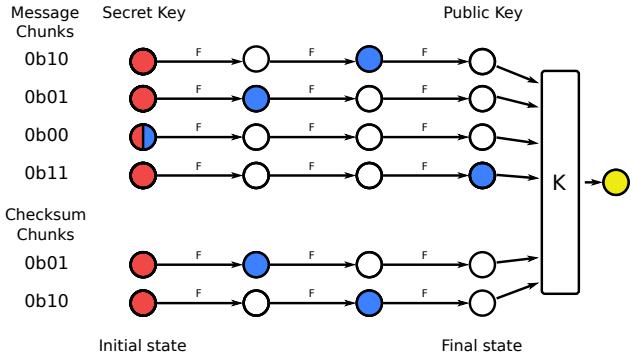
Winternitz one-time signatures

Checksum mechanism:

$$c = \mathcal{C}(m) = \sum_{i=0}^{l_1-1} (w - 1 - m_i)$$

$$c = 1 + 2 + 3 + 0$$

$$c = 6 = 0b0110$$



Background

Winternitz one-time signatures

Checksum mechanism:

$$c = \mathcal{C}(m) = \sum_{i=0}^{l_1-1} (w - 1 - m_i)$$

$$c = 1 + 2 + 3 + 0$$

$$c = 6 = 0b0110$$

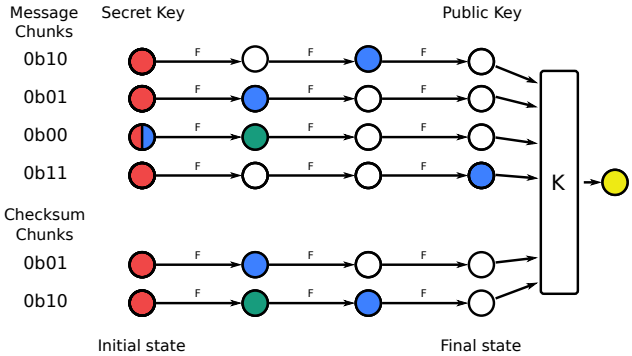
Tampered signature from before:

$$c = 1 + 2 + 2 + 0$$

$$c = 5 = 0b0101$$

F is a one-way function

$\rightarrow$ Last checksum node unknown



Background

Winternitz one-time signatures

Checksum mechanism:

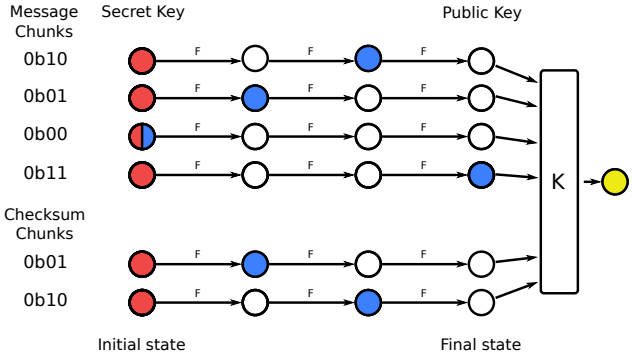
$$c = \mathcal{C}(m) = \sum_{i=0}^{l_1-1} (w - 1 - m_i)$$

$$c = 1 + 2 + 3 + 0$$

$$c = 6 = 0b0110$$

→ How resilient is this against fault attacks?

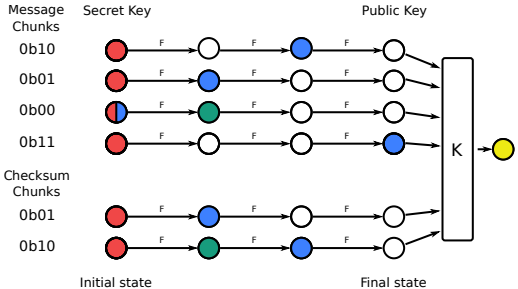
→ Does tampering allow a forgery?

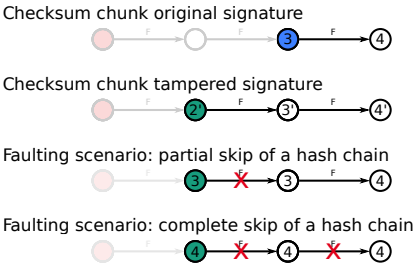


Fraunhofer AISEC

Attack

Exemplary attack scenarios





Attack

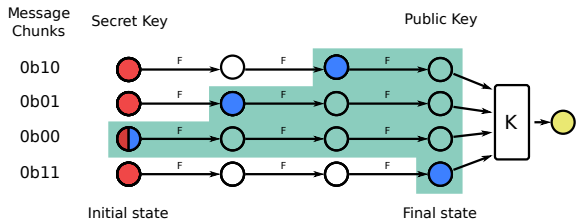
Brute-forcing

- Forge signature for a given message
- Any forgery chunk must be greater or equal

- Brute-forcing requires different input for same message
- Details in the paper, but in short:

  LMS & XMSS vary randomised hashing

  SPHINCS$^+$ vary authentication path



Attack

Attacking an ARM Cortex-M4

- Analysis of reference implementations with ARCHIE: github.com/Fraunhofer-AISEC/archie
- Fault model: single instruction skip
- Number of vulnerable instructions:

	Invalid signature	Our attack
XMSS	0	8

- Similar results for LMS and SPHINCS$^+$
- Results shown for -Os, similar results for -O2

Attack

Countermeasure design

Details in the paper, in short:

- Redundant computation of inexpensive operations

→ memcmp of public key and its candidate or hash chain length calculations

- Loop iteration hardening of hash chain traversal
- Call hardening within hash chain traversal

Attack

Countermeasure effectiveness

	CMs	Invalid signature	Our attack
XMSS	No	0	8
	Yes	0	0

- Similar results for LMS and SPHINCS$^+$
- Results shown for -Os, similar results for -O2

Attack

Countermeasure efficiency

	Code size	Code size increase by CMs
XMSS	3870 Bytes	+3.5 % / +134 Bytes

	Cycle count	Cycle count increase by CMs
XMSS	32.3M	+0.01 % / +4.27k

- Similar results for LMS and SPHINCS$^+$
- Results shown for -Os, similar results for -O2

Conclusion

- Fault attack targeting WOTS feasible

	single-tree	multi-tree
signing	✓	✓
verifying	✓	✓

- Allows for existential or universal forgery
- Effective and efficient countermeasures proposed

Contact Information

Alexander Wagner, Vera Wesselkamp, Felix Oberhansl, Marc Schink, Emanuele Strieder

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Lichtenbergstraße 11
85748 Garching (near Munich)
Germany
Internet: https://www.aisec.fraunhofer.de

Phone: +49 89 3229986-149
Fax: +49 89 3229986-299
E-Mail: alexander.wagner@aisec.fraunhofer.de