# Hash-based signatures III

## Stateful signatures

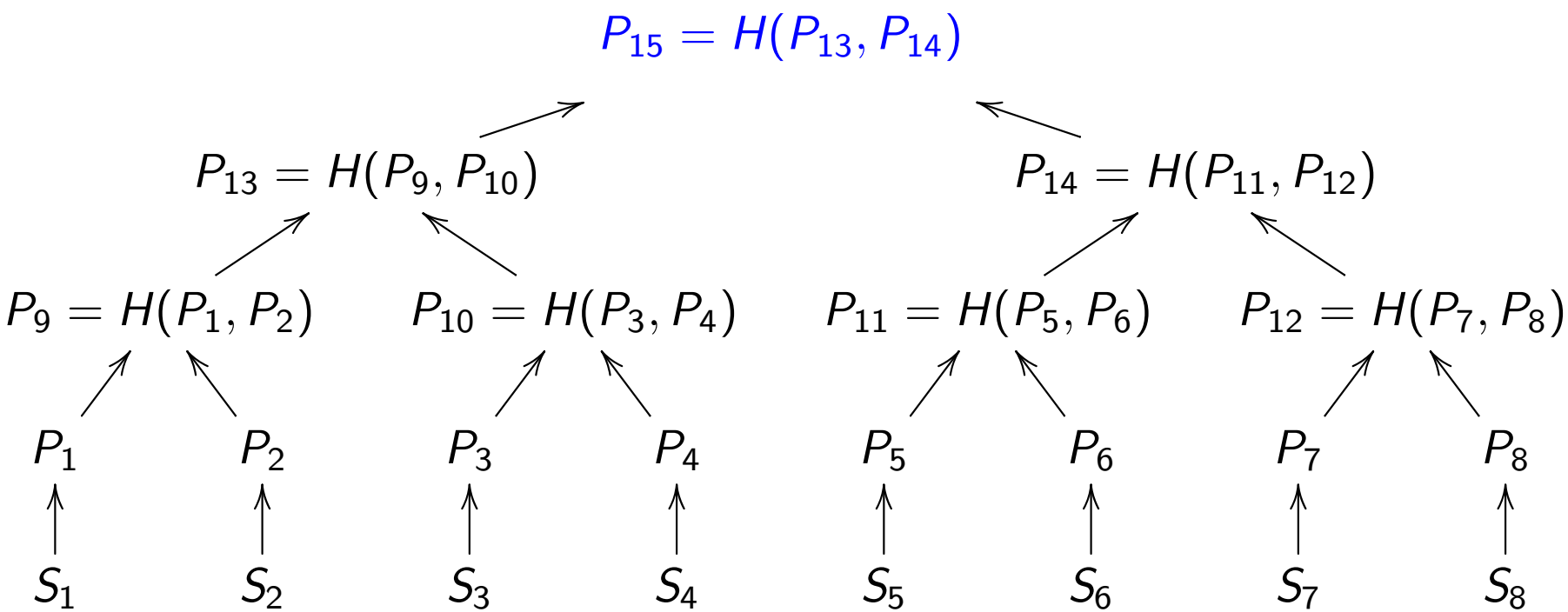
Tanja Lange
(with some slides by Daniel J. Bernstein)

Eindhoven University of Technology

SAC – Post-quantum cryptography

# Merkle's (e.g.) 8-time signature system

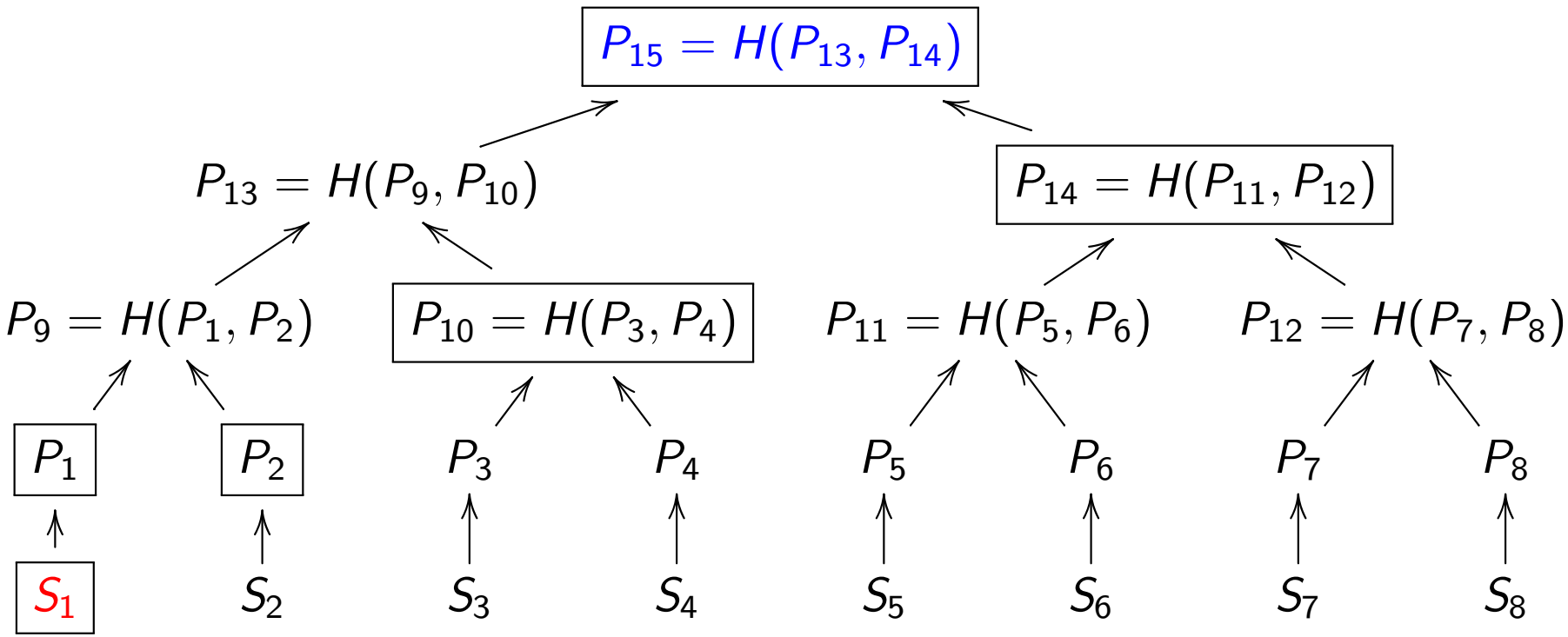
Hash 8 one-time public keys into a single Merkle public key $P_{15}$.




$S_i \to P_i$ can be Lamport or Winternitz one-time signature system.
Each such pair $(S_i, P_i)$ may be used only once.

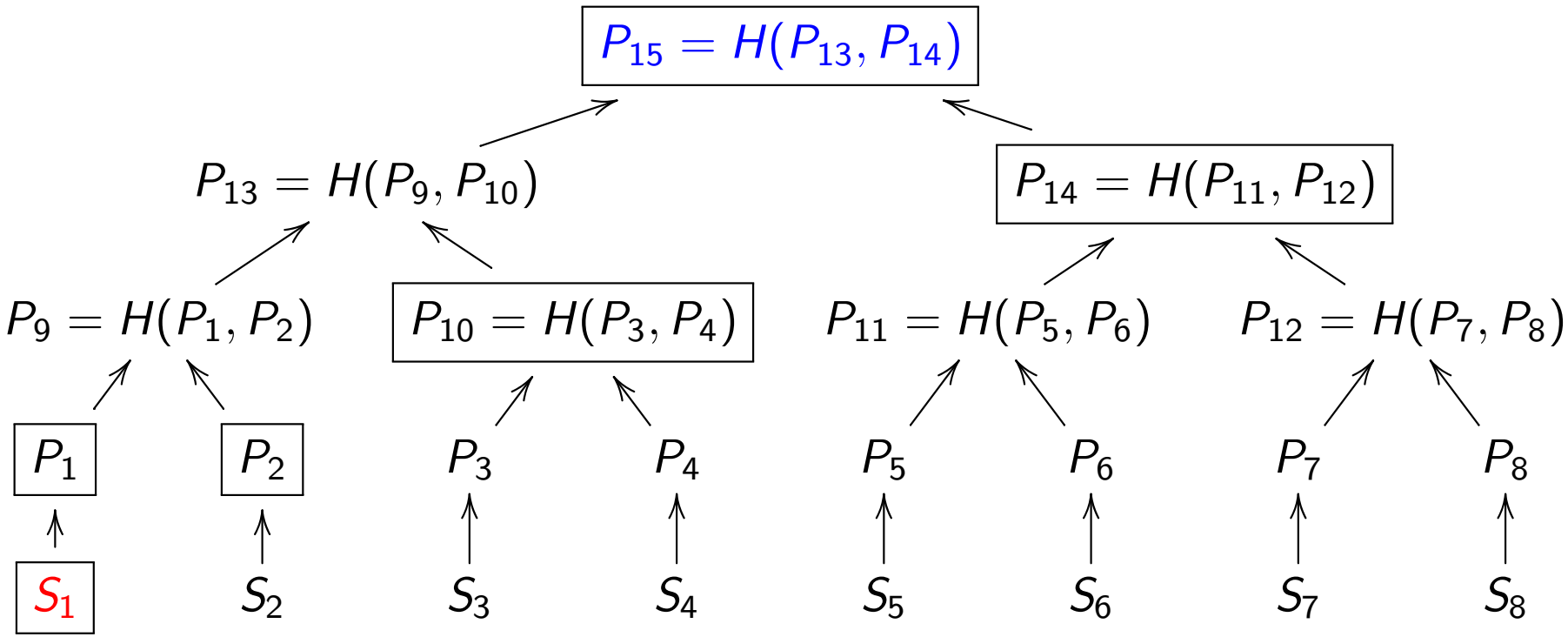
# Signature in 8-time Merkle hash tree

Signature of first message: $(\texttt{sign}(m, S_1), P_1, P_2, P_{10}, P_{14})$.



# Signature in 8-time Merkle hash tree

Signature of first message: $(\texttt{sign}(m, S_1), P_1, P_2, P_{10}, P_{14})$.




Verify signature $\texttt{sign}(m, S_1)$ with public key $P_1$ (provided in signature).
Link $P_1$ against public key $P_{15}$ by computing $P'_9 = H(P_1, P_2)$,
$P'_{13} = H(P'_9, P_{10})$, and comparing $H(P'_{13}, P_{14})$ with $P_{15}$.
Reject if $H(P'_{13}, P_{14}) \neq P_{15}$ of if the signature verification failed.

# Improvements to Merkle's scheme

- Each key is good only for fixed number of messages, typically $2^n$.
- The public key is very short: just one hash output.
  But each signature contains $n$ public keys along with the one-time signature.
- Computing the public key requires computing and storing $2^n$ one-time signature keys.

# Improvements to Merkle's scheme

- Each key is good only for fixed number of messages, typically $2^n$.
- The public key is very short: just one hash output.
  But each signature contains $n$ public keys along with the one-time signature.
- Computing the public key requires computing and storing $2^n$ one-time signature keys.
- Can trade time for space by computing the secret keys $S_i$ deterministically from a short secret seed.
  Very little storage for the seed but more time in signature generation.

# Improvements to Merkle's scheme

- Each key is good only for fixed number of messages, typically $2^n$.
- The public key is very short: just one hash output.
  But each signature contains $n$ public keys along with the one-time signature.
- Computing the public key requires computing and storing $2^n$ one-time signature keys.
- Can trade time for space by computing the secret keys $S_i$ deterministically from a short secret seed.
  Very little storage for the seed but more time in signature generation.
- Can build trees of trees where each leaf of the top tree signs the root of a tree below it. Only the top tree is needed in key generation.
  This increases the signature length (one one-time signature per tree) and signing time. See PhD thesis of Andreas Hülsing for an optimized schedule of what to store and when to precompute.

# Stateful hash-based signatures

- Only one prerequisite: a good hash function, e.g. SHA3-512.
  Hash functions map long strings to fixed-length strings.
  Signature schemes use hash functions in handling plaintext.
- Old idea: 1979 Lamport one-time signatures.
- 1979 Merkle extends to more signatures.

Pros:

- Post quantum
- Only need secure hash function
- Security well understood
- Fast

Cons:

- Biggish signature
  though some tradeoffs possible
- Stateful, i.e., ever reusing a subkey breaks security.
  Adam Langley "for most environments it's a huge foot-cannon."

# Stateful hash-based signatures

- Only one prerequisite: a good hash function, e.g. SHA3-512.
  Hash functions map long strings to fixed-length strings.
  Signature schemes use hash functions in handling plaintext.
- Old idea: 1979 Lamport one-time signatures.
- 1979 Merkle extends to more signatures.

Pros:

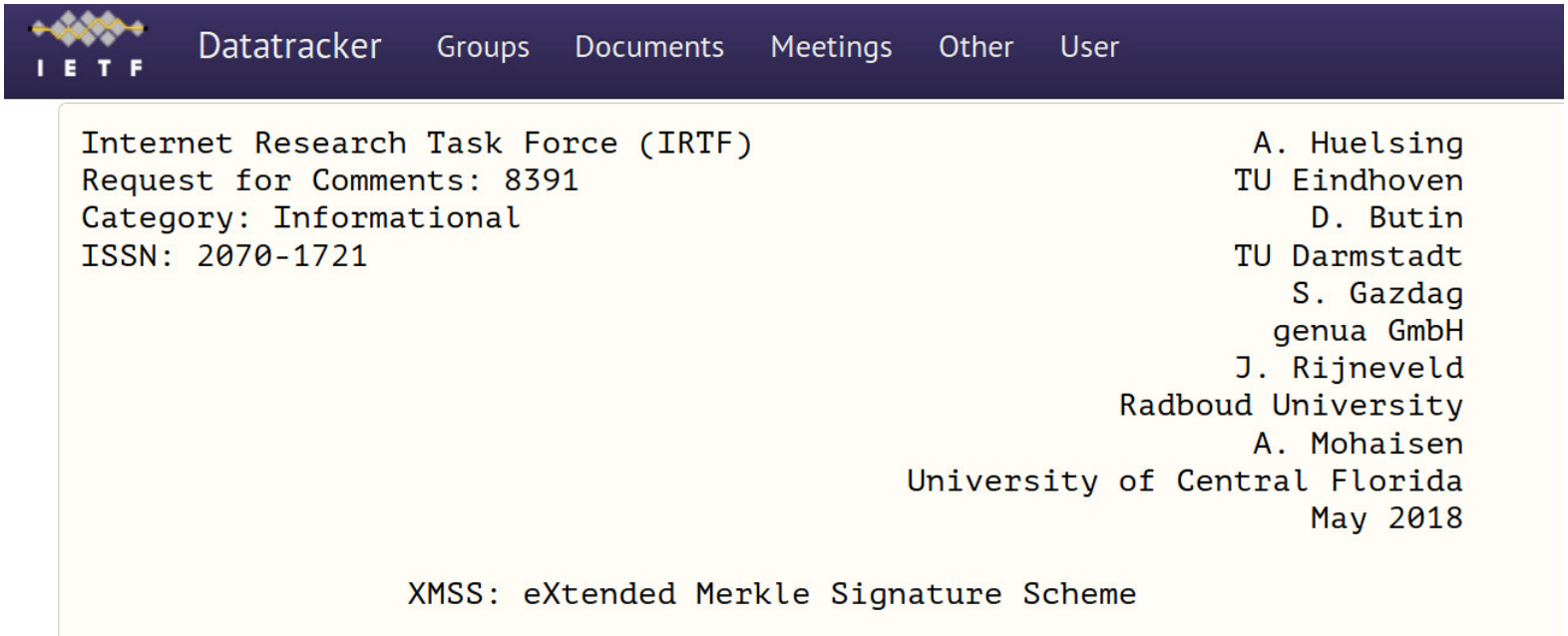
- Post quantum
- Only need secure hash function
- Security well understood
- Fast
- We can count: OS update, code signing, . . . naturally keep state.

Cons:

- Biggish signature
  though some tradeoffs possible
- Stateful, i.e., ever reusing a subkey breaks security.
  Adam Langley "for most environments it's a huge foot-cannon."

# Standardization progress

- CFRG has published 2 RFCs: RFC 8391 and RFC 8554



IETF Datatracker Groups Documents Meetings Other User

Internet Research Task Force (IRTF) — A. Huelsing, TU Eindhoven; D. Butin, TU Darmstadt; S. Gazdag, genua GmbH; J. Rijneveld, Radboud University; A. Mohaisen, University of Central Florida

Request for Comments: 8391
Category: Informational
ISSN: 2070-1721

May 2018

XMSS: eXtended Merkle Signature Scheme

IETF Datatracker Groups Documents Meetings Other User

Internet Research Task Force (IRTF) — D. McGrew, M. Curcio, S. Fluhrer, Cisco Systems

Request for Comments: 8554
Category: Informational
ISSN: 2070-1721

April 2019

Leighton-Micali Hash-Based Signatures

# Standardization progress

- CFRG has published 2 RFCs: RFC 8391 and RFC 8554
- NIST has gone through two rounds of requests for public input, most are positive and recommend standardizing XMSS and LMS. Only concern is about statefulness in general.

# Standardization progress

- CFRG has published 2 RFCs: RFC 8391 and RFC 8554
- NIST has gone through two rounds of requests for public input, most are positive and recommend standardizing XMSS and LMS. Only concern is about statefulness in general.


- ISO SC27 JTC1 WG2 has started a study period on stateful hash-based signatures.