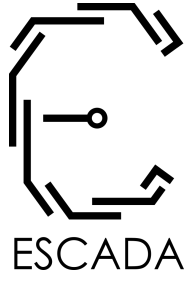
Subterranean 2.0

Joan Daemen, Pedro Maat Costa Massolino, Yann Rotella

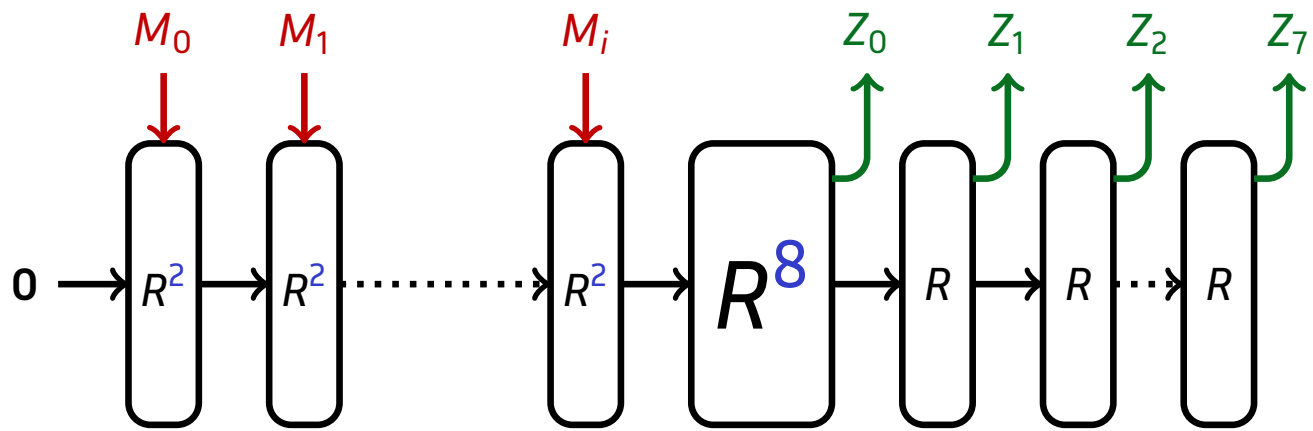
March 27, 2019
FSE 2019 rump session



Radboud
Universiteit
Nijmegen

Subterranean 2.0 Hash function

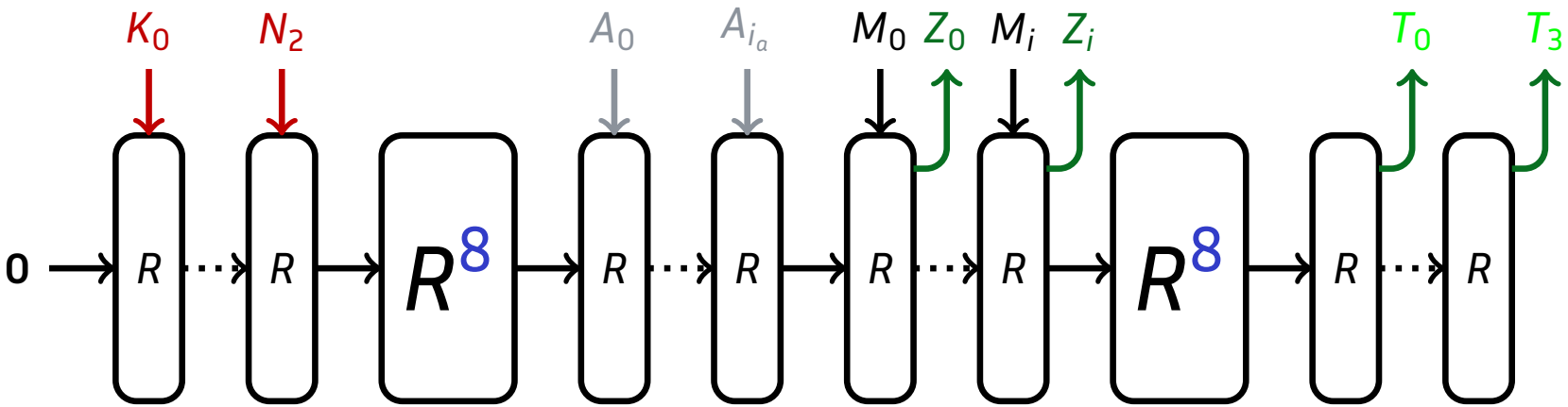
- $|Z| = 256$



- $|M_j| = 9 = 8 + 1$, 8 bits of message, 1 padding;
- $|Z_j| = 32$, NIST: 8 output blocks.

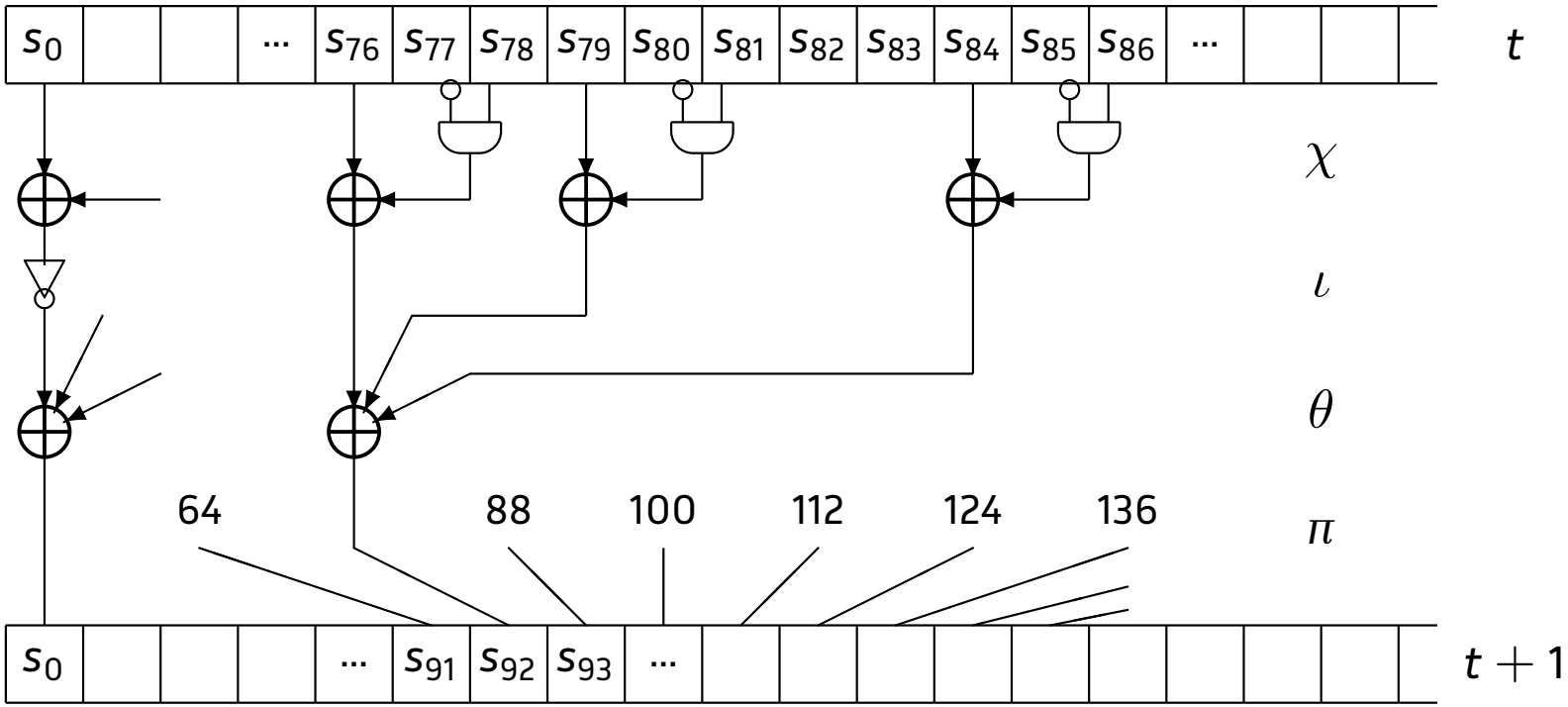
Subterranean 2.0 Authenticated Encryption

- $|T| = |K| = 128$



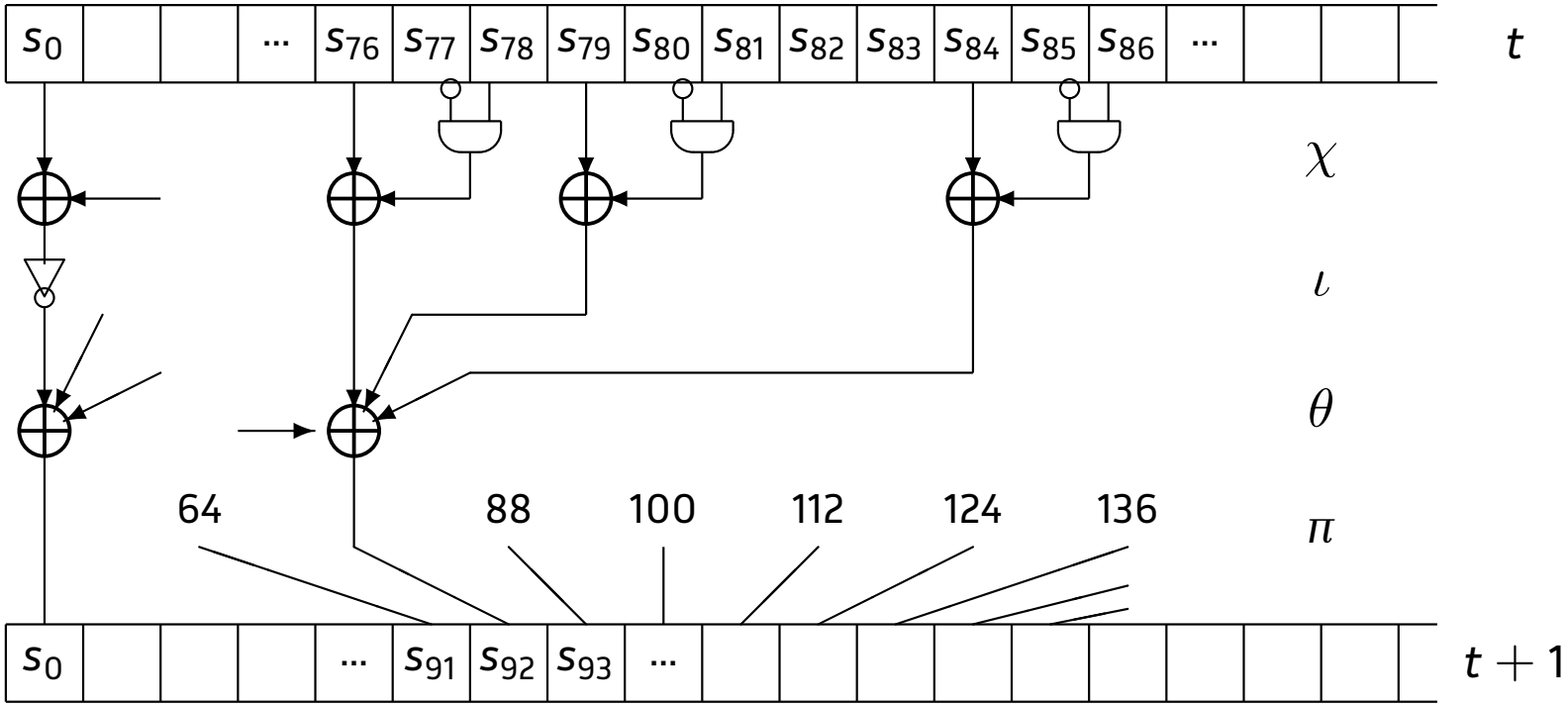
- $|K_j| = |N_j| = |A_j| = |M_j| = 33 = 32 + 1$: 32 bits of message, 1 bit for padding.
- $|Z_j| = |T_j| = 32$

The Round function



$$
\begin{aligned}
\chi: \quad & s_i \leftarrow s_i + (s_{i+1} + 1)s_{i+2}\,, \\
\iota: \quad & s_i \leftarrow s_i + \delta_i\,, \\
\theta: \quad & s_i \leftarrow s_i + s_{i+3} + s_{i+8}\,, \\
\pi: \quad & s_i \leftarrow s_{12i}\,.
\end{aligned}
$$

Absorb and Squeeze



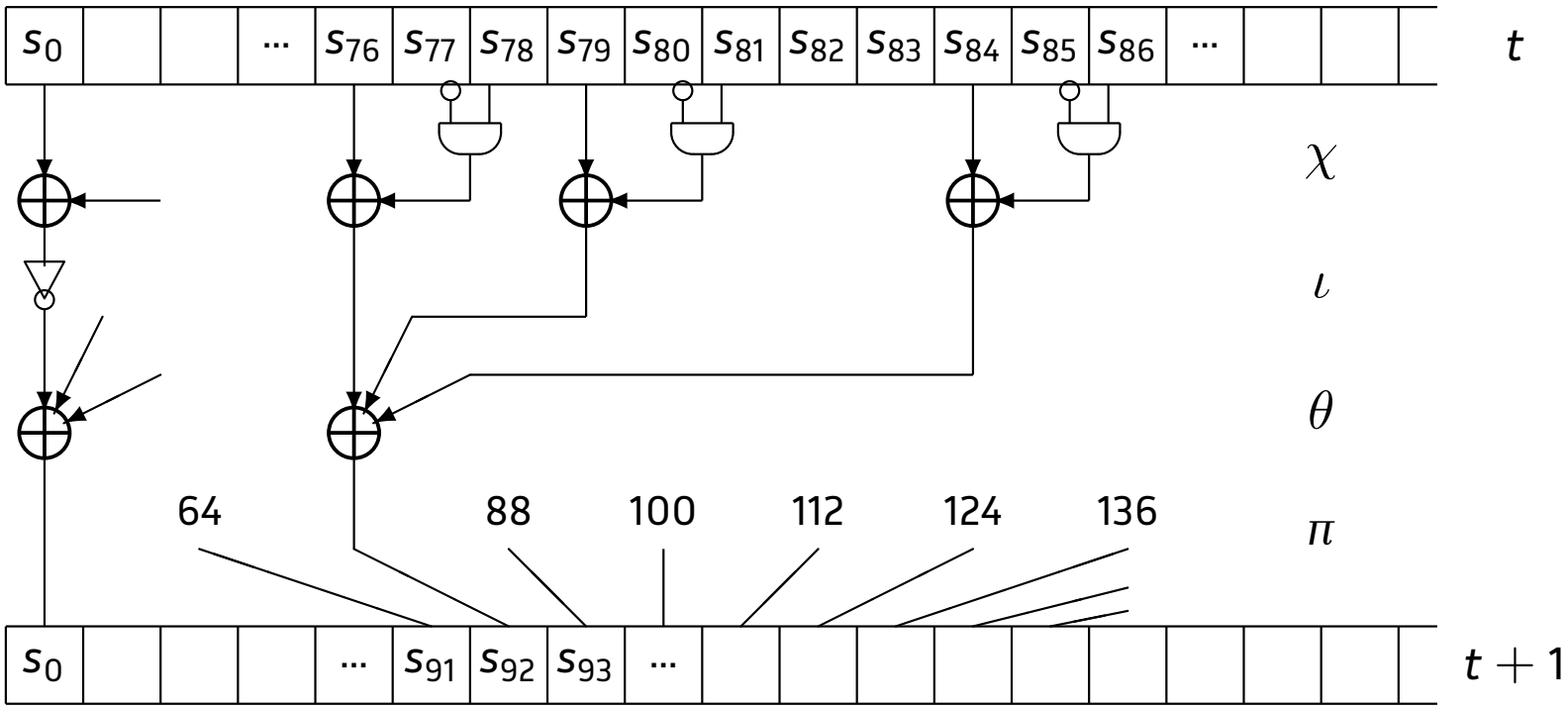
$$12^4 = 176$$

$$\mathcal{G}_{64} = \{1, 176, 136, 35, 249, \ldots, 92\}$$

$$z_i = s_{176^i} + s_{176^{-i}}$$

$$s_i = s_i + m_i, i \in \{1,176,136,35,249,134,197,234,64, 213, \ldots, 165, 256\}$$

Software Implementation



$$
\begin{aligned}
\chi: \quad & s_i \leftarrow s_i + (s_{i+12^j})s_{i+2*12^j} \,, \\
\iota: \quad & s_i \leftarrow s_i + \delta_i \,, \\
\theta: \quad & s_i \leftarrow s_i + s_{i+3*12^j} + s_{i+8*12^j} \,, \\
\pi: \quad & s_i \leftarrow s_{12i} \text{ not anymore} \,.
\end{aligned}
$$