TU Graz

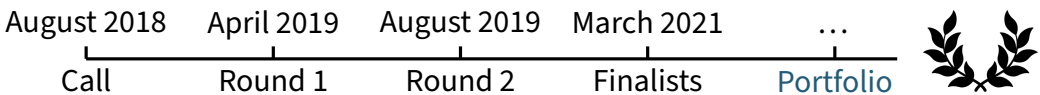
SCIENCE
PASSION
TECHNOLOGY

Finding Collisions for Round-Reduced Romulus-H

Marcel Nageler, Felix Pallua, Maria Eichlseder

FrisiaCrypt 2022

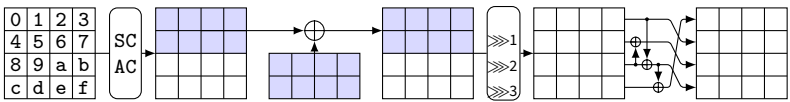
The **NIST LWC** Competition



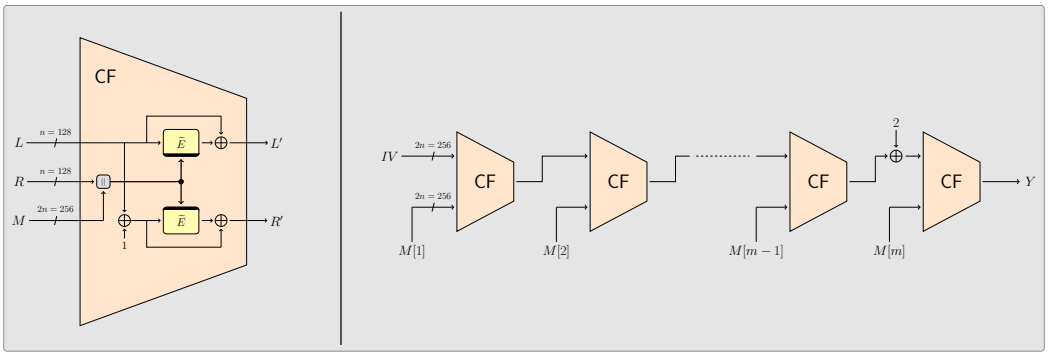
- 10 Finalists including `Romulus`
  - **Romulus-H** hash function

Skinny Specification [GIK+18]

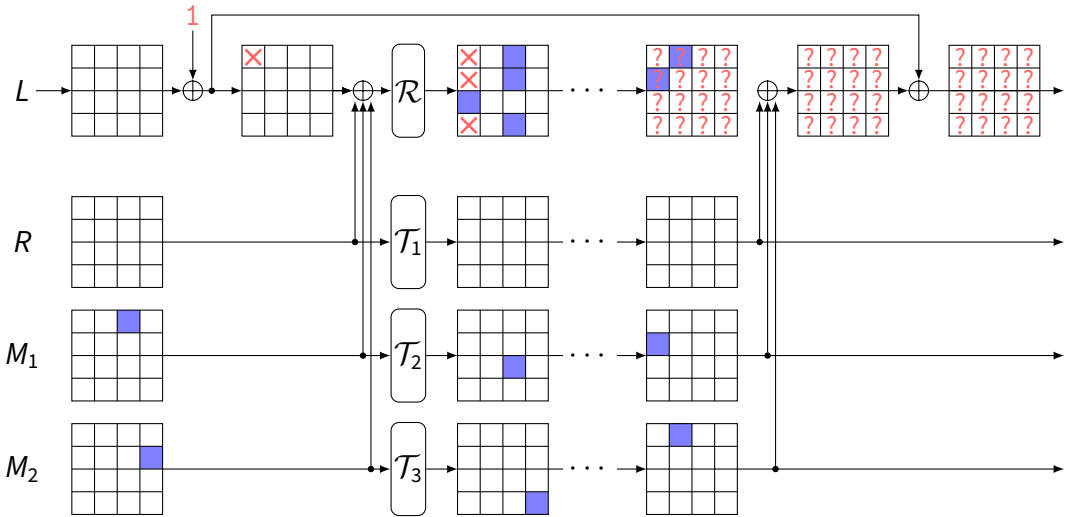
- `Romulus` uses `Skinny-128-384` with 40 rounds (instead of 56)
  - 128-bit blocks
  - 384-bit tweakey



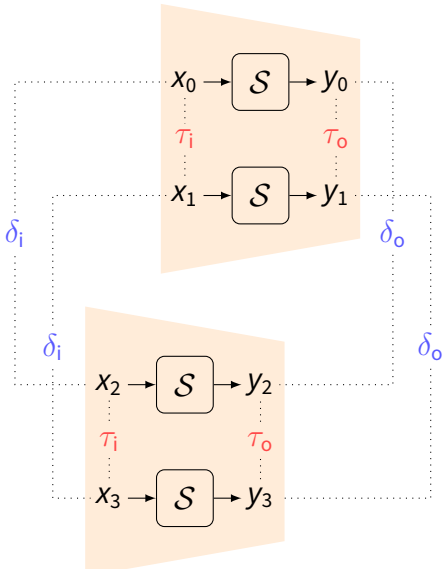
Romulus-H Specification [GIK+18]



Differential Analysis

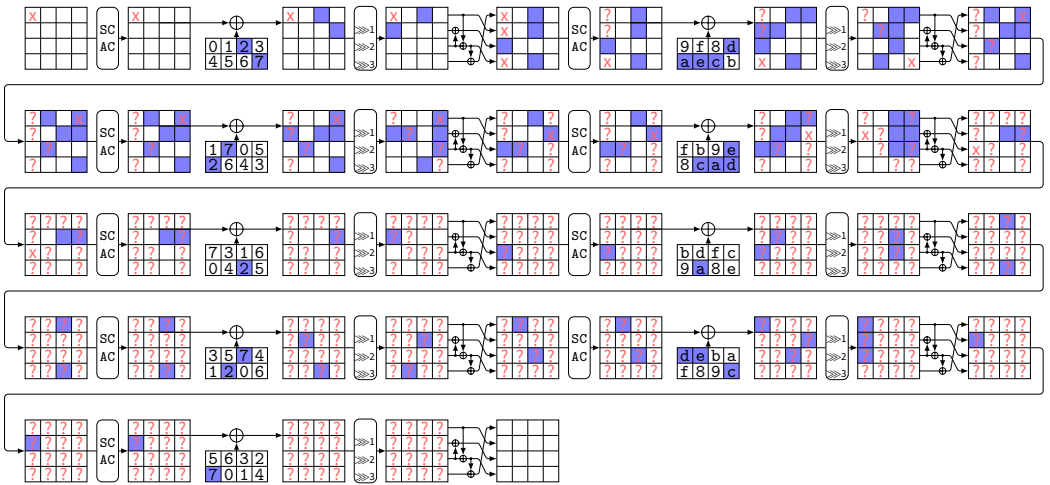


Boomerang-style setup



- $\delta = \times, \tau = 0 \rightarrow \text{cost} = 1$
- $\delta = 0, \tau_o = \times \rightarrow \text{cost} = 1$
- $\delta = \times, \tau_o = \times \rightarrow \text{cost} = 1 \text{ or } 2$
- $\delta = \times, \tau = ? \rightarrow \text{cost} = 2$

Truncated Characteristic for 9 Rounds



Finding Bitwise Characteristics

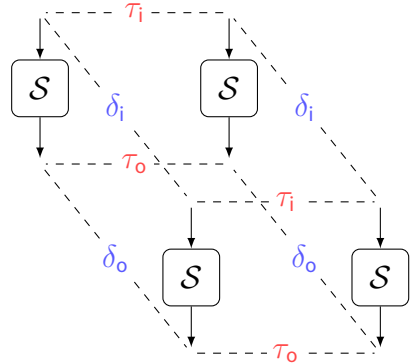
- model CNF of DDT $\geq x$

- what to do when $\delta = \times$ and $\tau = \times$

a) define DDT4($\delta_i, \delta_o, \tau_i, \tau_o$)
   - model CNF of DDT4 $\geq x$

   $\rightarrow$ very expensive

b) use MILP model where this does not happen

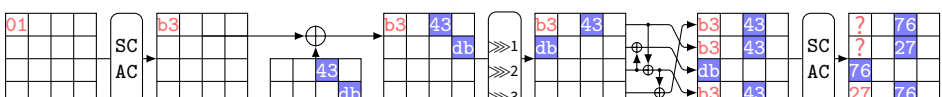


Finding Assignment for Characteristic (Semi-Free-Start Collision)

- Encode linear layer using Xor constraints of cryptominisat/Z3
- Encode S-box as minified CNF of solution set (XDDT)
- If $\tau = ?$ use 2 variables instead of 1

Finding Full Collision

- Randomly choose an initial block
- Verify the characteristic in the first 2 rounds is satisfiable (in C++)
  - $p \approx 2^{-15}$ for the characteristic below
- Collision can be found in a few minutes on a laptop



9-Round Collision

$$P = \texttt{55554654434b555559495a41504a4c414c415452474144524a4447515247594c}$$
$$M_1 = \texttt{b63a14a596b5216e97e6d7cc7b0b014d1d533b4f882a207504dd06463e1f98ed}$$
$$M_2 = \texttt{b63aa4a596b5211697e620cc50202a4d1d534a4f882a20fc04dd2d46dffe79ed}$$

$$H_9(P \| M_1) = H_9(P \| M_2)$$

Collisions without Bitwise Characteristic

- Basic SAT model based only on truncated characteristic
- Model `Romulus-H` 2 times
  - Output must be equal
  - Inactive cells must be equal
  - Active cells must be different

12-Round Semi-Free-Start Collision

$$LR = \texttt{5c8b5917f91ef90cd4d43db01fabad9ee8eacb53d56e94cb7e2583855002f641}$$
$$M_1 = \texttt{84f5295203b834903954a45bd2e1ea5eca7d5417431e6320a1376ecebdb3b76f}$$
$$M_2 = \texttt{2af529ea15b834903954a45bd2e1eada937d54010c1e6320a1376ecebdb3b7f9}$$

$$h_{12}(LR, M_1) = h_{12}(LR, M_2)$$

Conclusion

- Differential model for `Romulus-H`
  - Based on differences δ and τ
- Collisions for 9 rounds of `Romulus-H`
- Collisions for 12 rounds of the compression function

Bibliography I

[GIK+18] Chun Guo, Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thmoas Peyrin. **Romulus**. Submission to NIST Lightweight Cryptography. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/romulus-spec-final.pdf. Aug. 2018.