

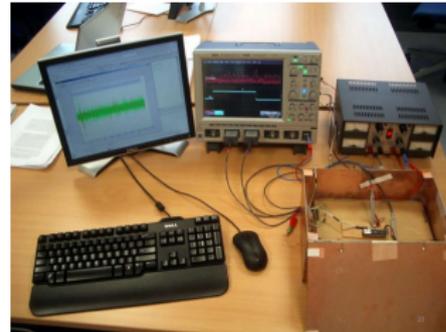
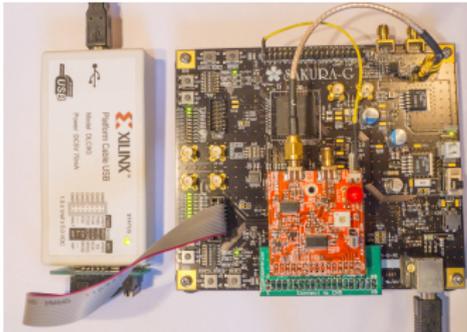
Threshold Implementations of PRINCE: Cost of Physical Security

Dušan Božilov

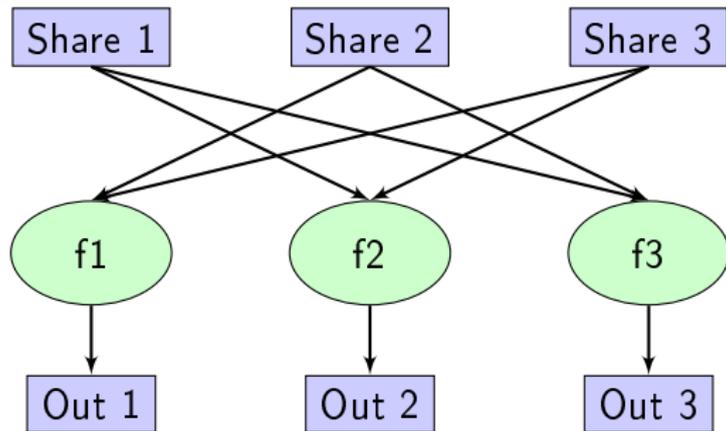
October 2016, Gaithersburg, USA



- Gray-box model of cryptographic algorithms
- Passive attackers (SCA)
 - Simple visual trace inspection or statistical methods used to extract most probable key
- Protection against attackers
 - Make auxiliary information indistinguishable from random



- Boolean masking scheme
- Properties
 - Correctness
 - Non-completeness
 - Uniformity
- Arbitrary order of security d
- Registers needed to separate nonlinear operations



- Used to ensure uniformity of the shared output x_1, \dots, x_n by introducing fresh random masks r_1, \dots, r_n
- Higher order TI can use ring refreshing method

$$y_1 = x_1 \oplus r_1 \oplus r_n \quad y_i = x_i \oplus r_{i-1} \oplus r_i, \quad i \in \{2, \dots, n\}$$

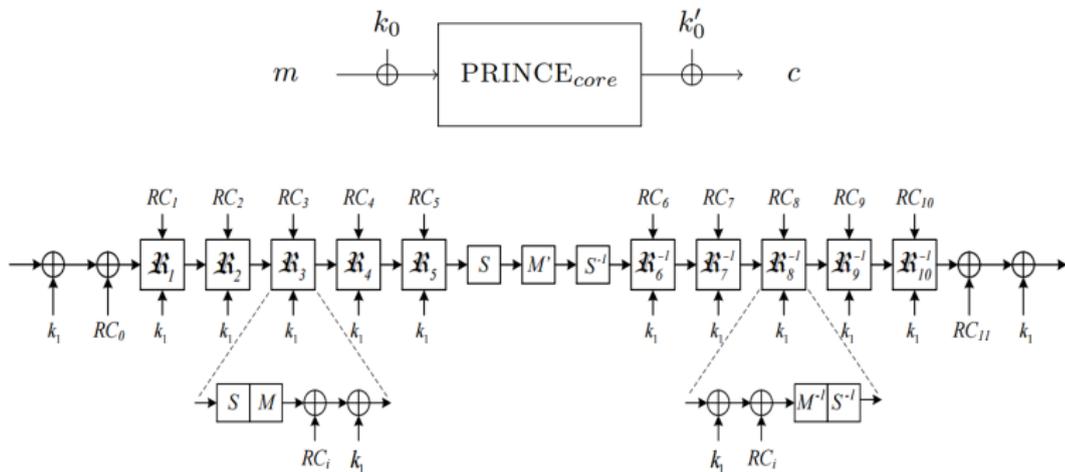
- First order implementations can use optimized method

$$y_i = x_i \oplus r_i, \quad i \in \{1, \dots, n-1\}, \quad y_n = x_n \oplus r_1 \oplus \dots \oplus r_{n-1}$$

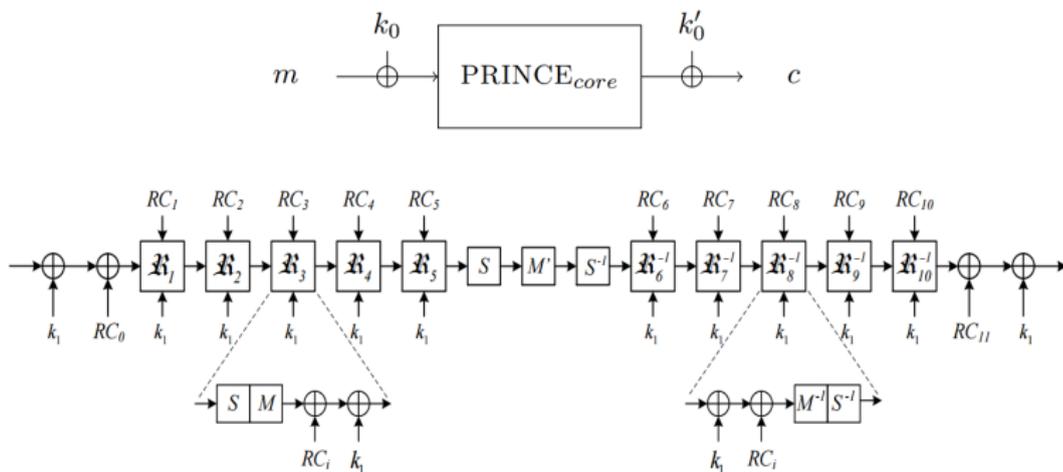
Two different flavors of TI

- $td + 1$ approach
 - Number of input and output shares dependant on security order d and algebraic degree t of nonlinear function
 - Uniformity can be achieved in some cases without re-masking
 - Larger area
- $d + 1$ approach
 - Number of input shares always equal to $d + 1$.
 - More output shares needed
 - Re-masking is necessary

- Low-latency/energy cipher
- 12 rounds, extremely efficient in hardware
- Very efficient bit-sliced software implementations
- Decryption operation is the same as encryption using a different key

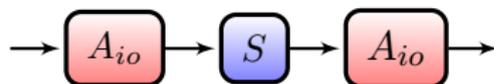


- 64-bit data path
- 4-bit S-box of algebraic degree three
- Last rounds use inverse S-box
- Diffusion achieved using matrices M , M' and M^{-1} that transform entire state
 - M can be obtained from M' by applying nibble shuffling SR .



- S-box and its inverse belong to the same affine equivalence class

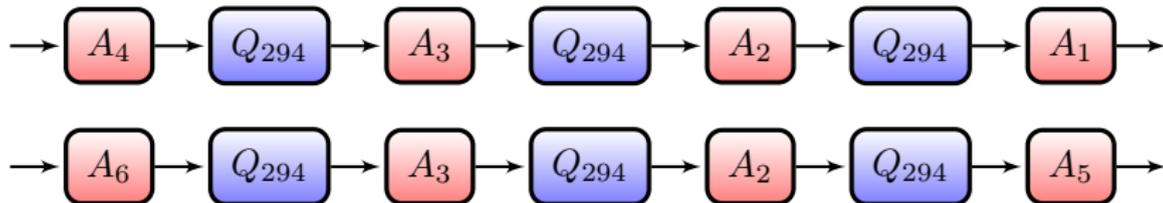
$$S^{-1} = A_{io} \circ S \circ A_{io}$$



- S-box decomposition

$$S = A_1 \circ Q_{294} \circ A_2 \circ Q_{294} \circ A_3 \circ Q_{294} \circ A_4$$

$$S^{-1} = A_5 \circ Q_{294} \circ A_2 \circ Q_{294} \circ A_3 \circ Q_{294} \circ A_6$$



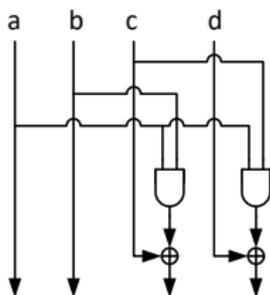
ANF of $Q_{294}(x, y, z, t) = F(a, b, c, d)$ is given with

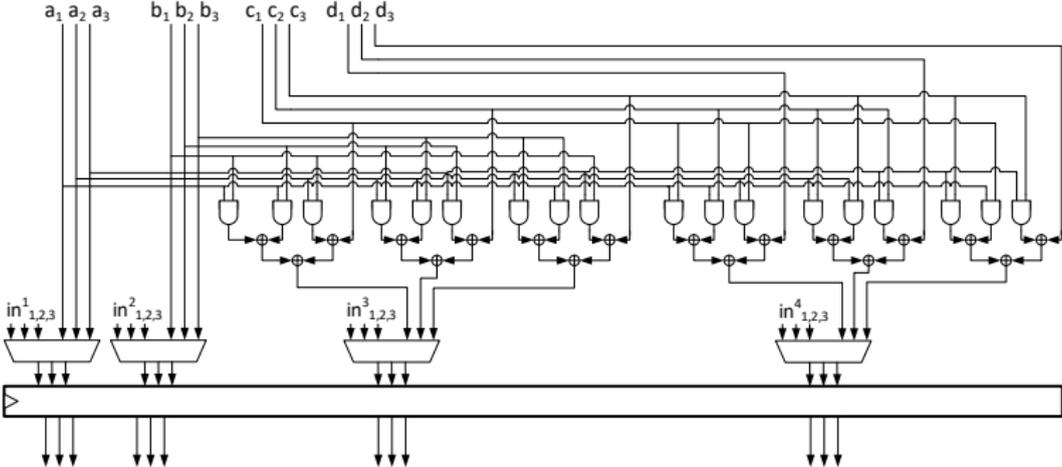
$$x = a$$

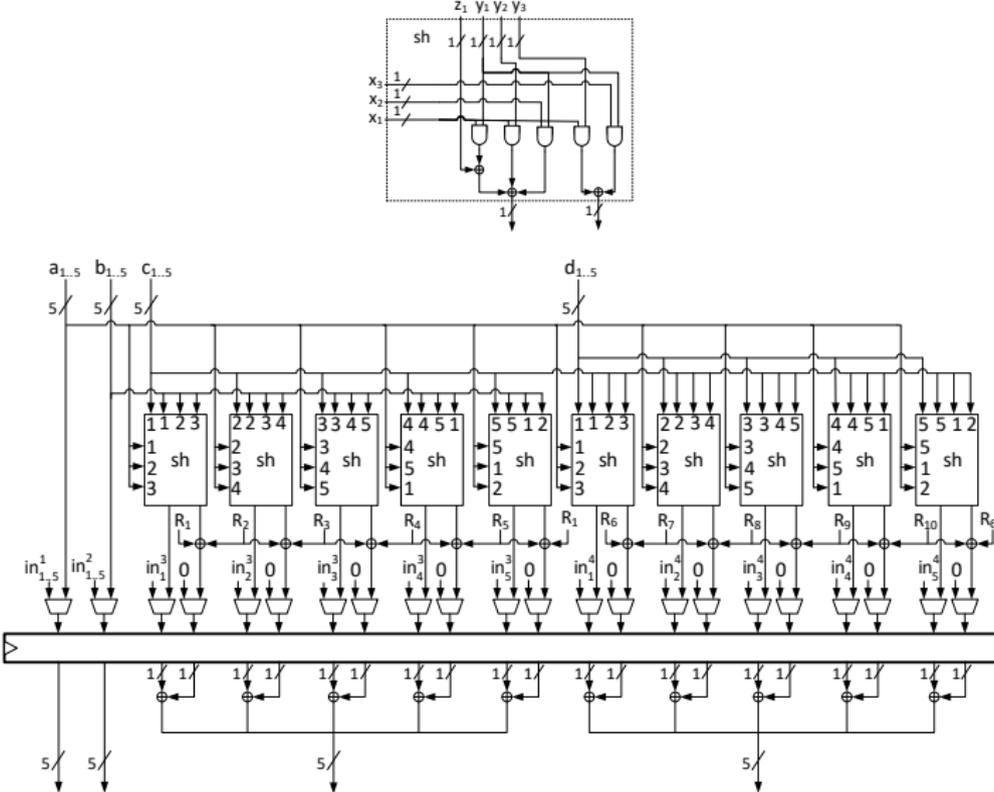
$$y = b$$

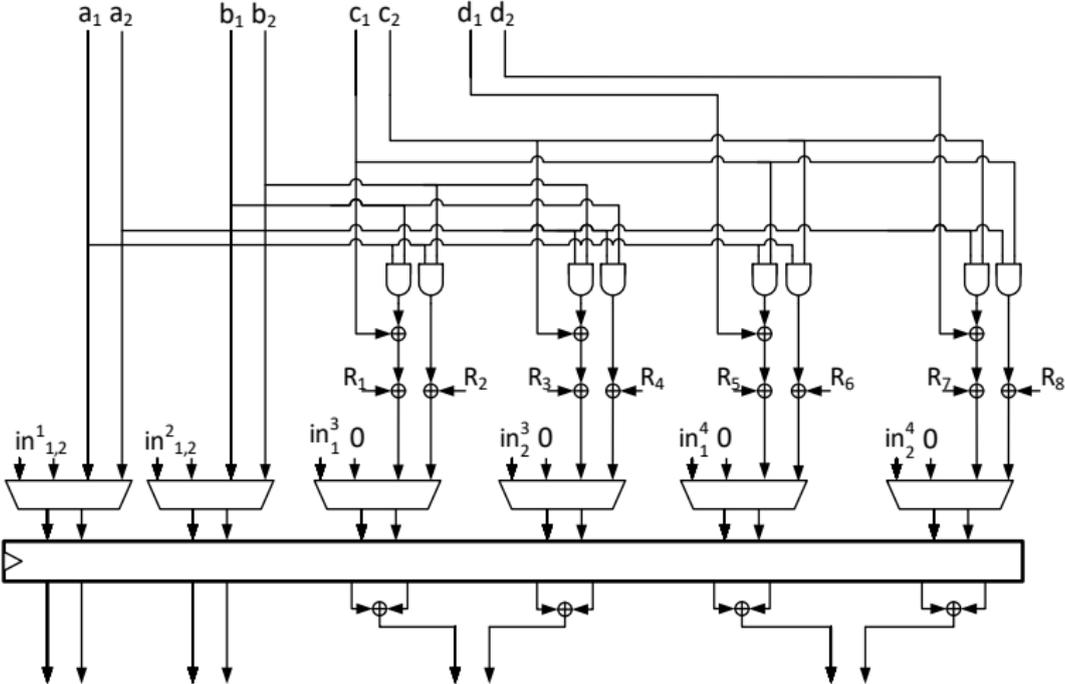
$$z = ab \oplus c$$

$$t = ac \oplus d$$

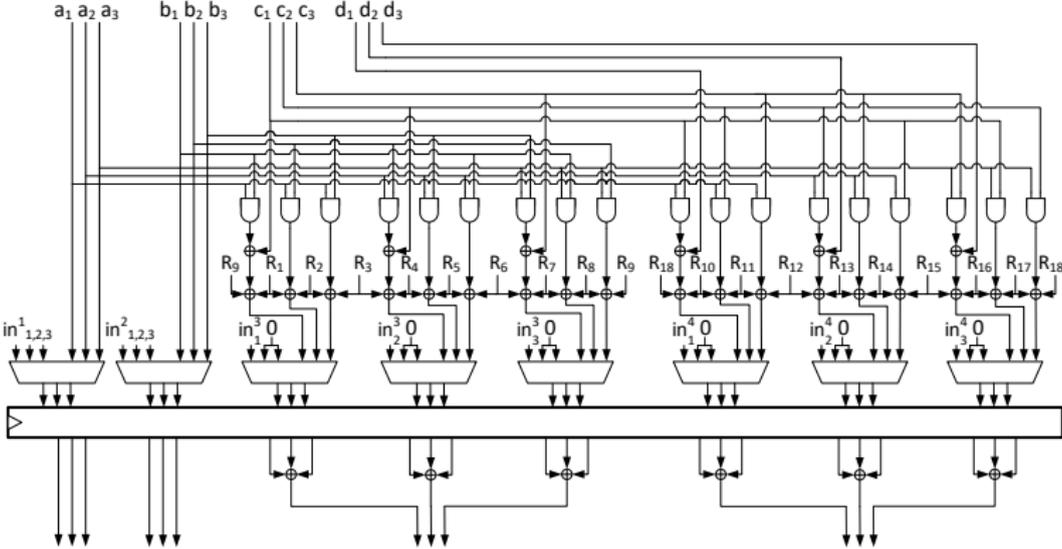


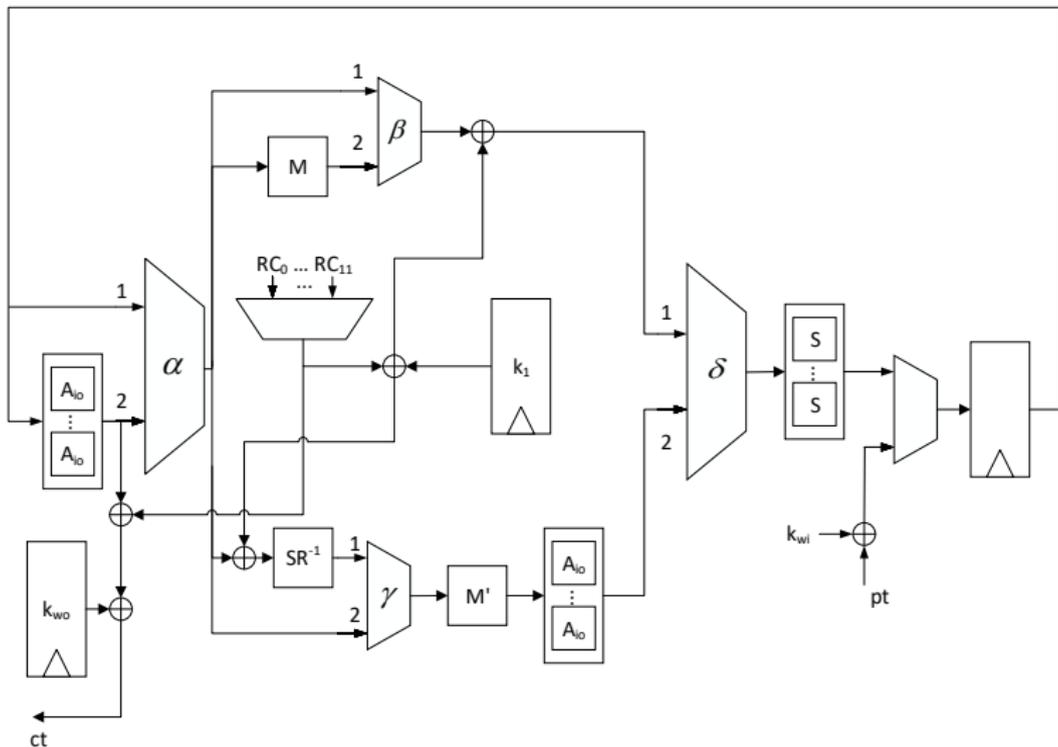


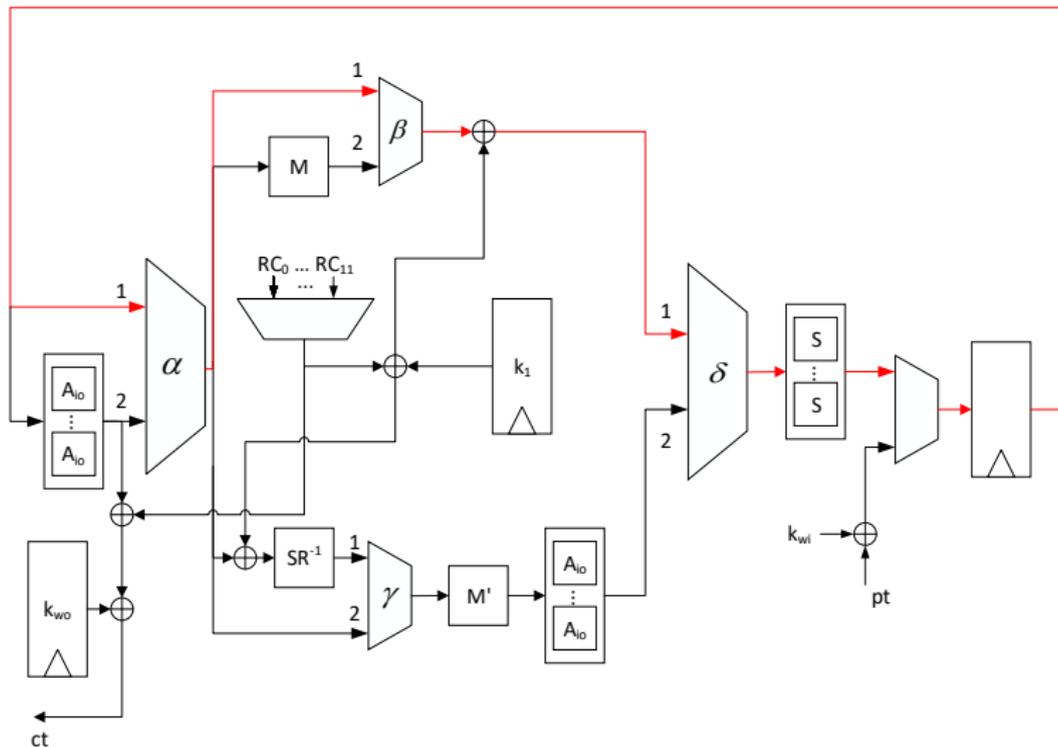


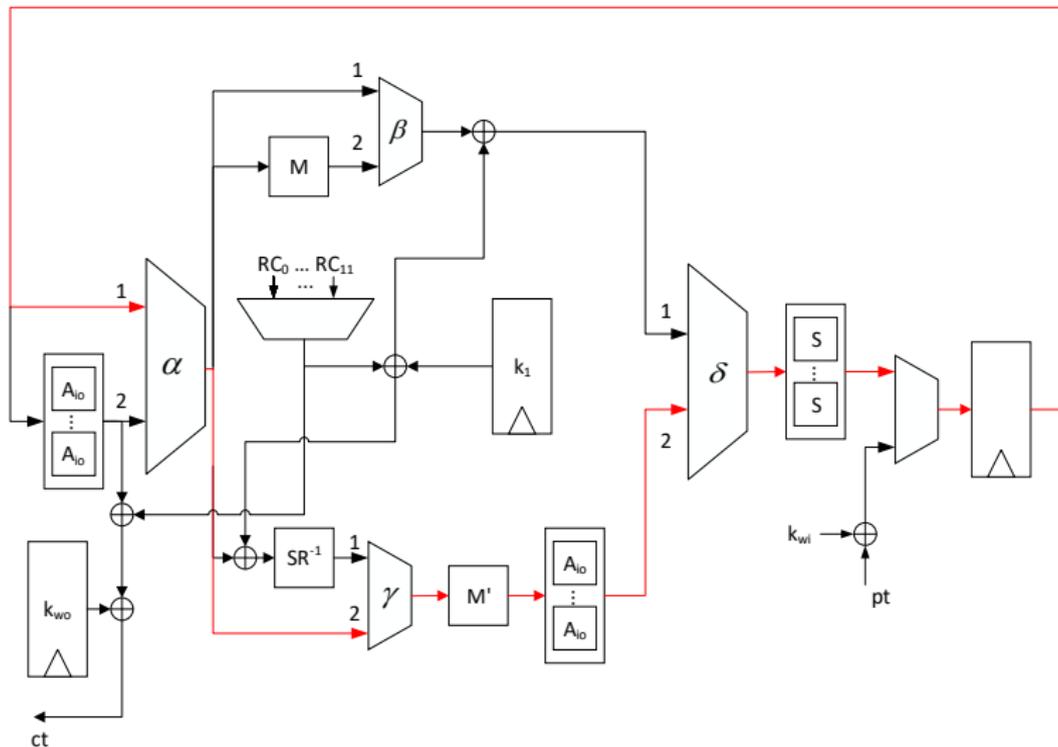
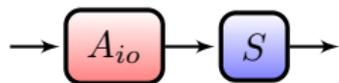


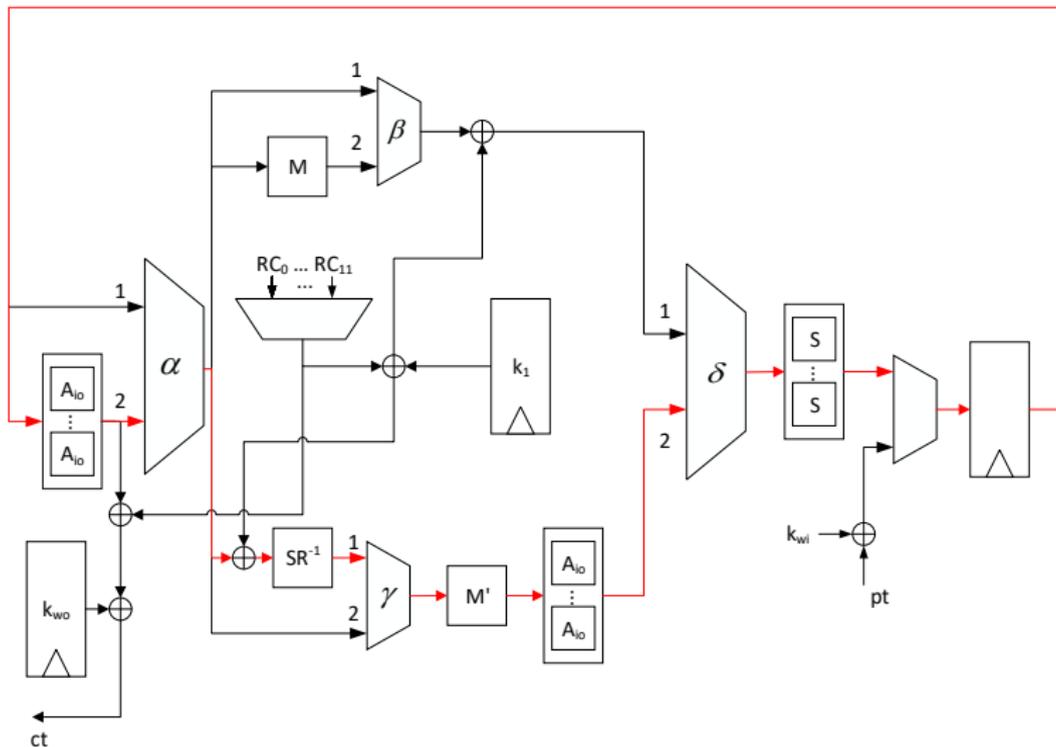
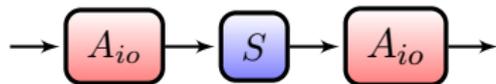
$d + 1$ second order secure masking of Q_{294}

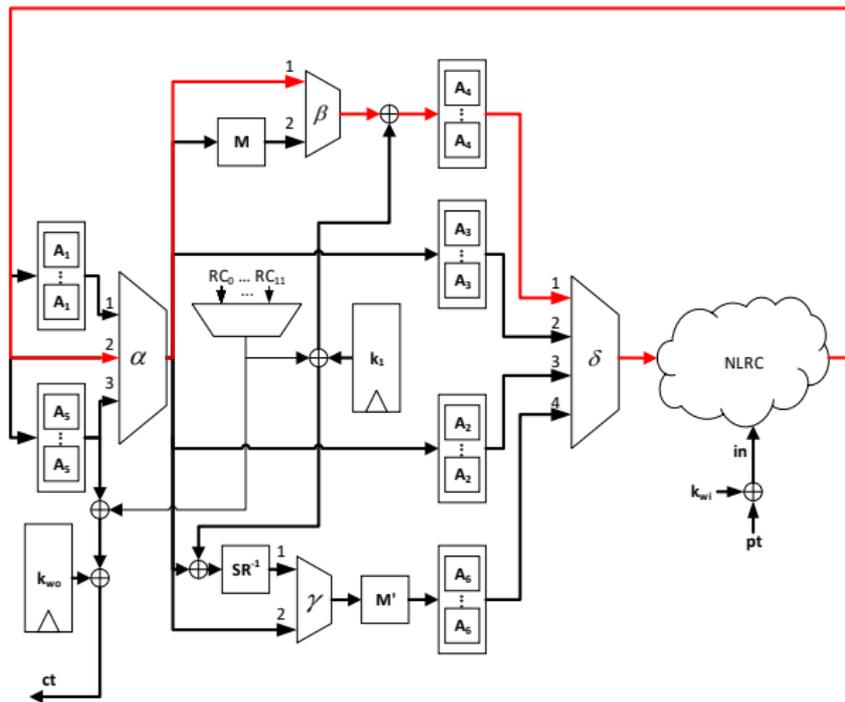
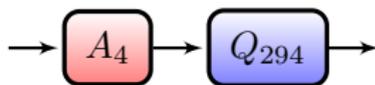


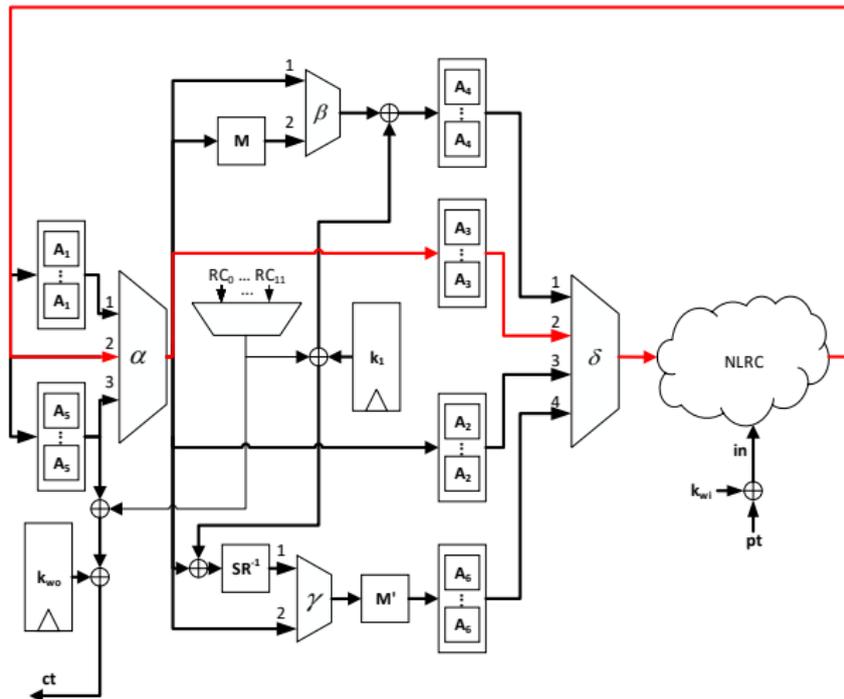
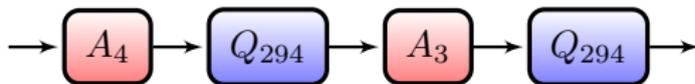


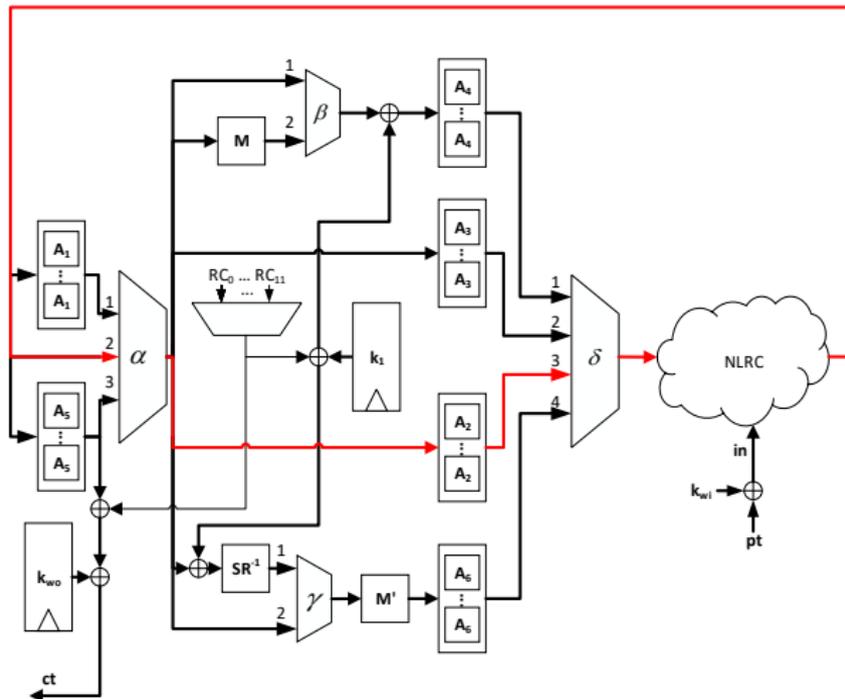
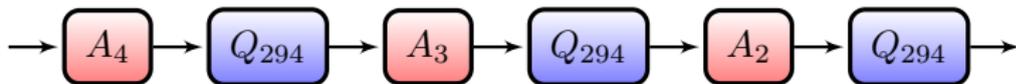


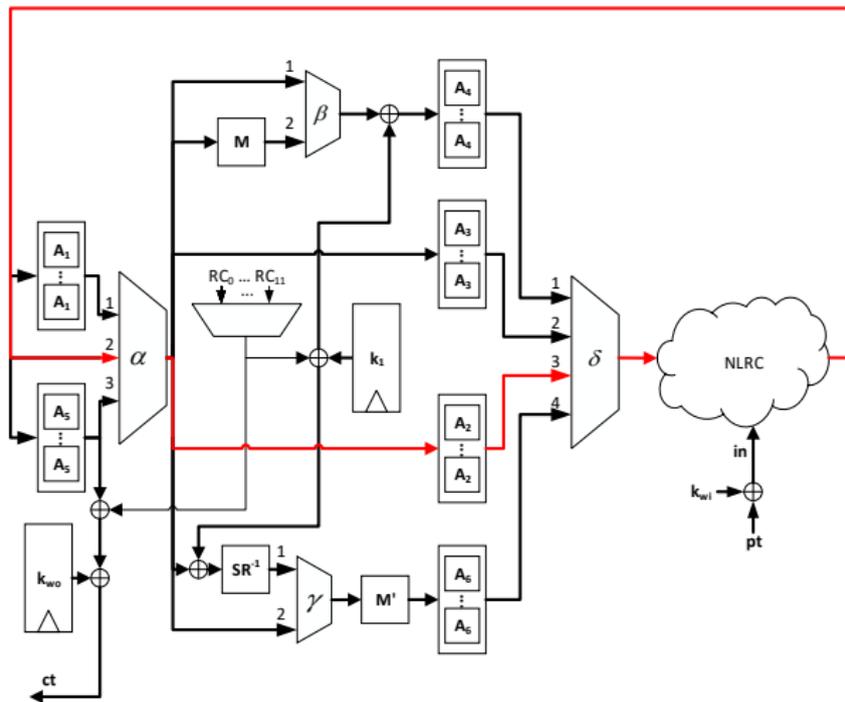
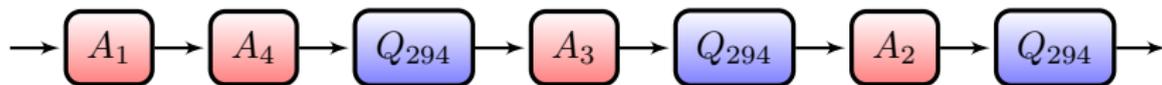


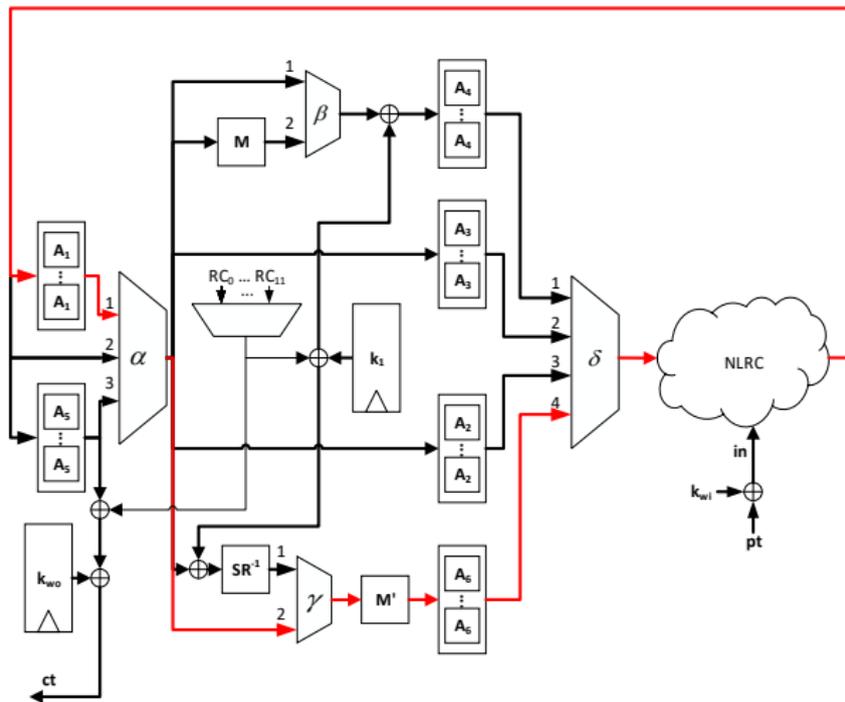
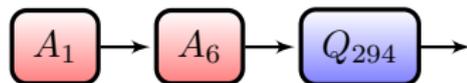


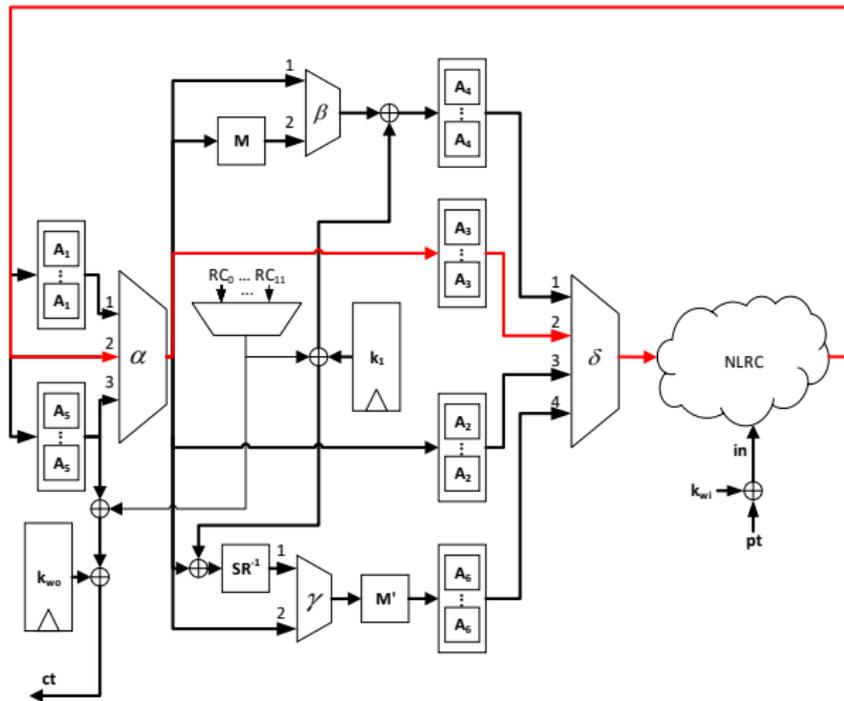
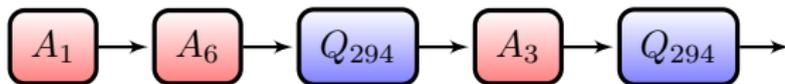


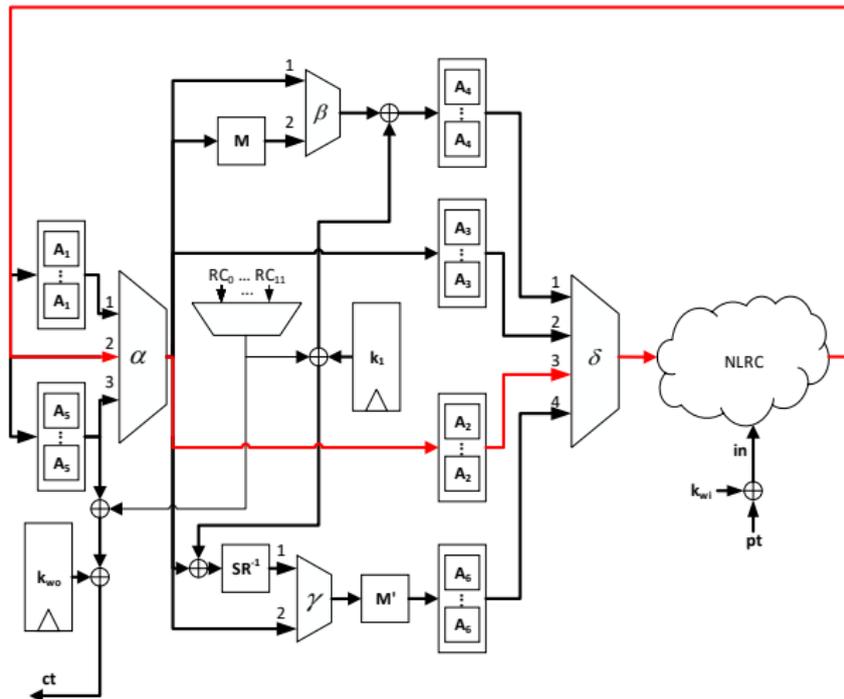
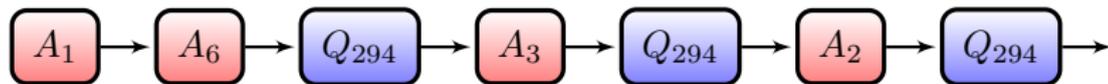


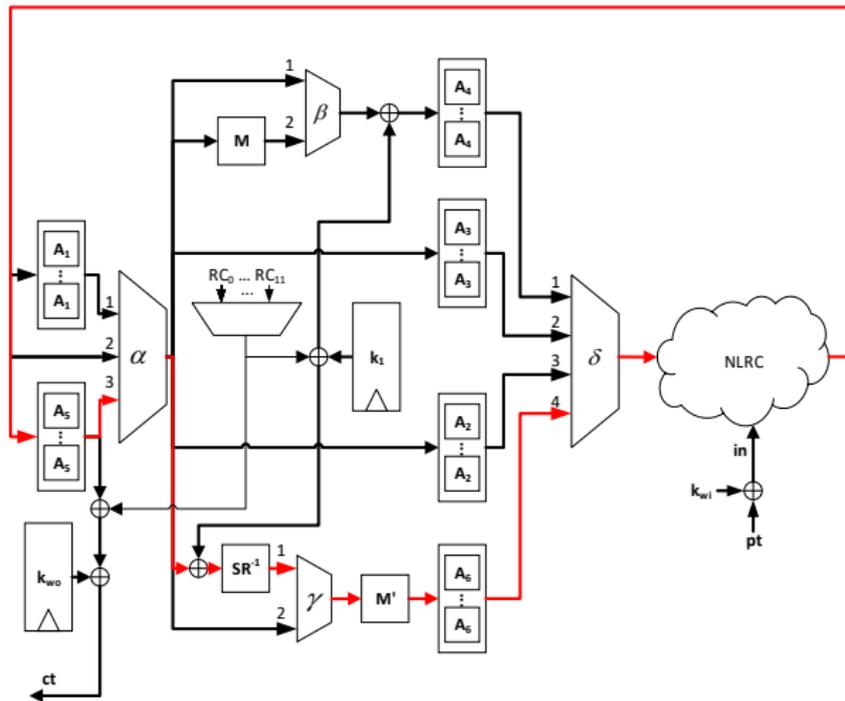
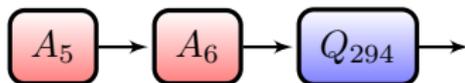


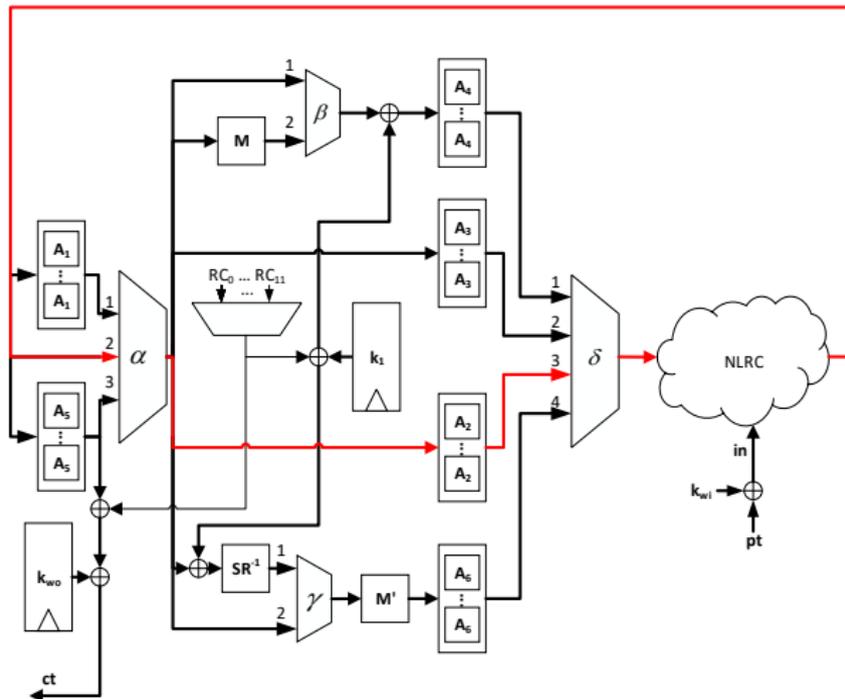
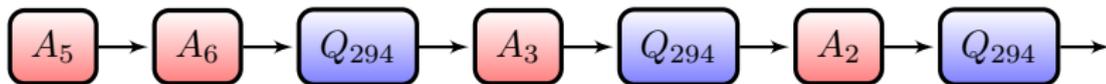




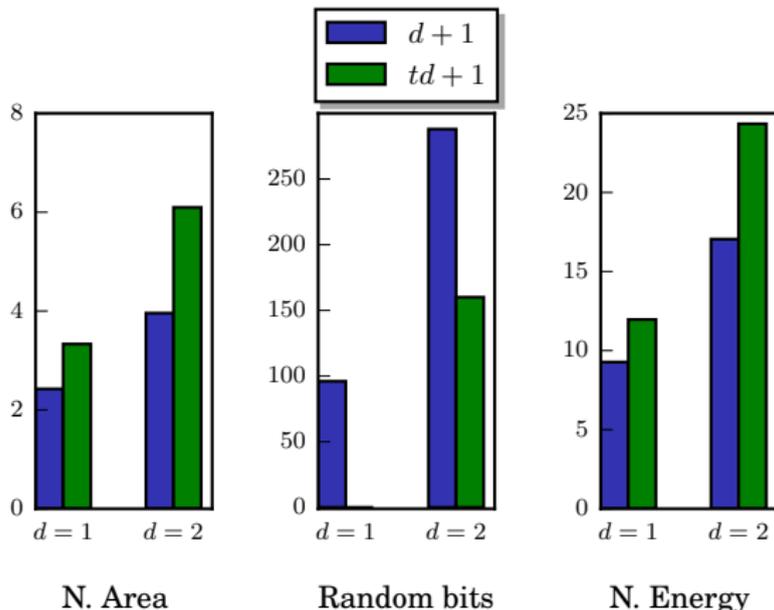








	Unprotected	1 st ($d + 1$)	1 st ($td + 1$)	2 nd ($d + 1$)	2 nd ($td + 1$)
Area (GE)	3589	8701	11958	14205	21879
Power (μ W)	59.21	183.06	236.05	336.4	480.31
Energy (pJ)	71.1	659	849.8	1211	1729.1
Randomness/cycle (bits)	0	96	0	288	160
Latency (cycles)	12	36	36	36	36



- Round based PRINCE implementations
 - 4 side-channel resistant implementations, 2 first order TI masking, 2 second order TI masking
 - 1 unprotected implementation as a reference
- Quantification of area, randomness, power, energy and latency penalties
 - Smallest masked implementation requires 2.5 times more area compared to the unprotected version
 - Power consumption increase of at least 3 times for smallest TI design
 - Latency increased by a factor of 3
- Low latency side-channel countermeasures still remain an open problem!
- Next steps
 - Security evaluation

Thank you! Questions?