Design Exploration of the NIST LWC Competition Lilliput-AE

Gaëtan LEPLUS, Julien FRANCQ

24/06/2019

NIST Call Requirements

- Current authenticated encryption recommendations: AES with an authenticated mode (e.g., Galois Counter Mode – GCM)
- Probably not optimal for IoT since designed 20 years ago
  - Question: can we do better?
- 2015: 1st NIST Lightweight Crypto workshop, 2017: NISTIR 8114 Report
- NIST Call for Authenticated Encryption with Associated Data (AEAD) algorithms submissions published at the end of 2018
- Submissions: March 2019, probably a 4-year competition, probably not a unique winner (portfolio).
- Key lengths: at least 128 bits (2^{112} computations security in single-key setting). If larger, 256-bit key recommended (2^{224} computations security)
- Nonce length: at least 96 bits. Tag length: at least 64 bits.
- Input size limit: no less than $2^{50} - 1$ bytes.

Algorithm Design Requirements

- Better performance in constrained environments (hardware and software) compared to current NIST standards
  - Compact hardware implementations and embedded software implementations with low RAM and ROM usage
  - Wide range of standard cell libraries considered for ASIC and FPGA performance. Wide range of 8-bit, 16-bit and 32-bit architectures considered for microcontrollers performance.
  - Flexible to support various implementation strategies (low energy, low power, low latency)
- Efficient preprocessing of a key (computation time and memory footprint)
- Countermeasures against various Side-Channel Attacks

LILLIPUT-AE Quick Presentation

- LILLIPUT-AE [FLM19] uses a (strenghthened) Tweakable Block Cipher (TBC) [JNP14] as internal primitive and has an authenticated encryption mode built on top of it: nonce-respecting mode ΘCB3 [KR11] LILLIPUT-I or nonce-misuse resistant mode SCT-2 [JNP14] LILLIPUT-II
  - Each tweak T gives a different permutation, T is public
- Based on the block cipher LILLIPUT [BFM+15]
- LILLIPUT-TBC is composed of 6 variants

Name	k	t	Nb. of Rounds r
LILLIPUT-TBC-I-128	128	192	32
LILLIPUT-TBC-I-192	192	192	36
LILLIPUT-TBC-I-256	256	192	42
LILLIPUT-TBC-II-128	128	128	32
LILLIPUT-TBC-II-192	192	128	36
LILLIPUT-TBC-II-256	256	128	42

Table: Recommended Parameter Sets for LILLIPUT-TBC

LILLIPUT-TBC: Encryption Process (f Function)

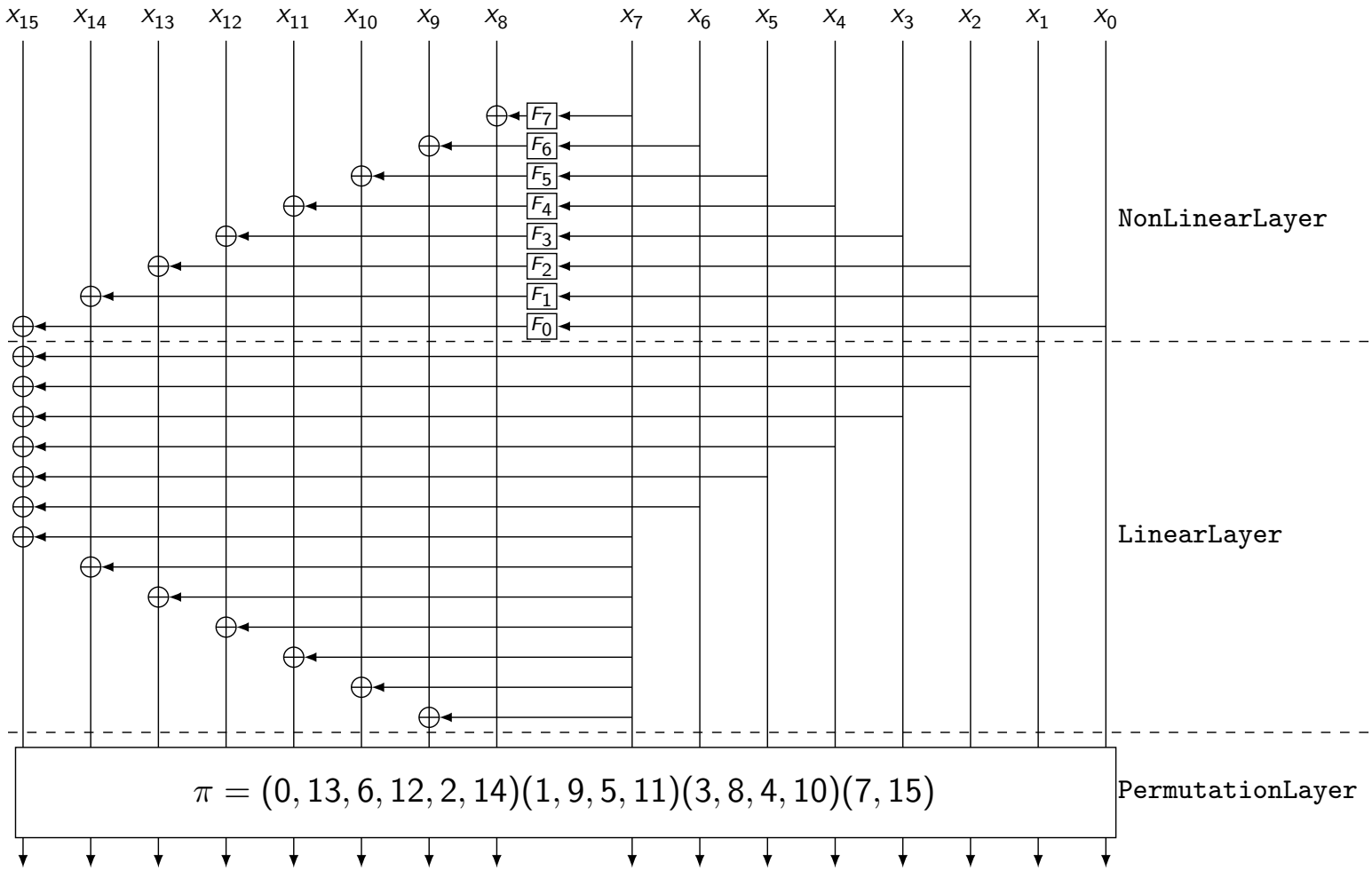
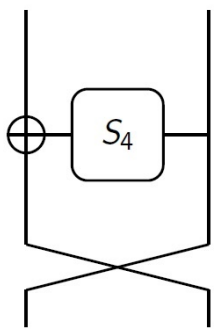


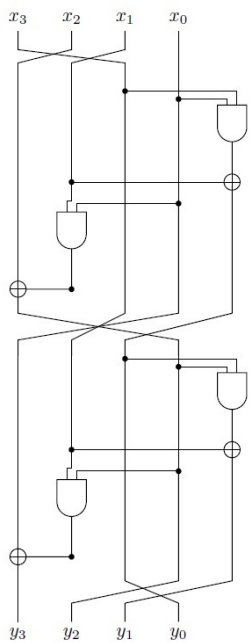
Figure: The Extended Generalized Feistel Network (EGFN) used in LILLIPUT-TBC with $F_j = S(X_j \oplus RTK_j^i)$

Design Rationale: The S-Box

- Chosen for its good cryptographic properties (resistance against linear/differential cryptanalysis, high algebraic degree, etc.)
- Based on a 3-round Feistel scheme with two Almost Perfect Nonlinear (APN) functions and a 4-bit S-box in the middle round
- Chosen for its low cost in terms of both hardware and Threshold implementations



(a) One Feistel round.



(b) $\bar{S}_4^2 = Q \circ Q =$ 081f4c792b36e5da

Tweakey Schedule: Parameters

- An adapted version of the TWEAKEY framework [JNP14]: The key and the tweak inputs are handled almost the same way
- It ensures that the number of cancellations on $(r+1)$ subtweakeys is at most $(p-1)$
- The Tweakey Schedule produces the 64-bit subtweakeys RTK^0 to RTK^{r-1} from the master key K and the tweak T divided into $p = (t+k)/64$ lanes that we denote TK^i_j

Name	k	t	p	r
LILLIPUT-TBC-I-128	128	192	5	32
LILLIPUT-TBC-I-192	192	192	6	36
LILLIPUT-TBC-I-256	256	192	7	42
LILLIPUT-TBC-II-128	128	128	4	32
LILLIPUT-TBC-II-192	192	128	5	36
LILLIPUT-TBC-II-256	256	128	6	42

Table: Recommended Parameter Sets for LILLIPUT-TBC

Tweakey Schedule: Overview

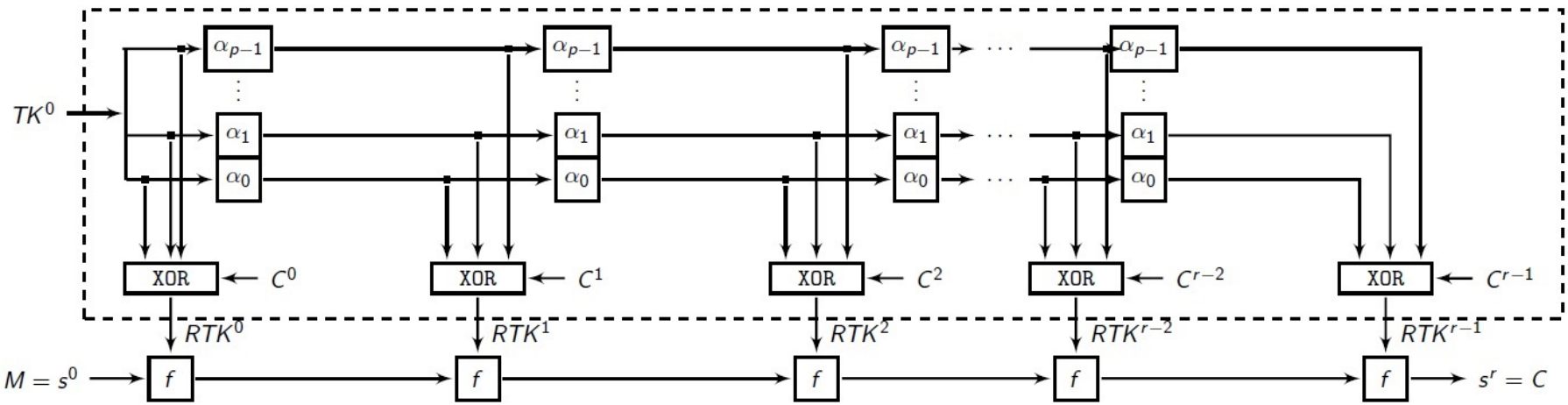


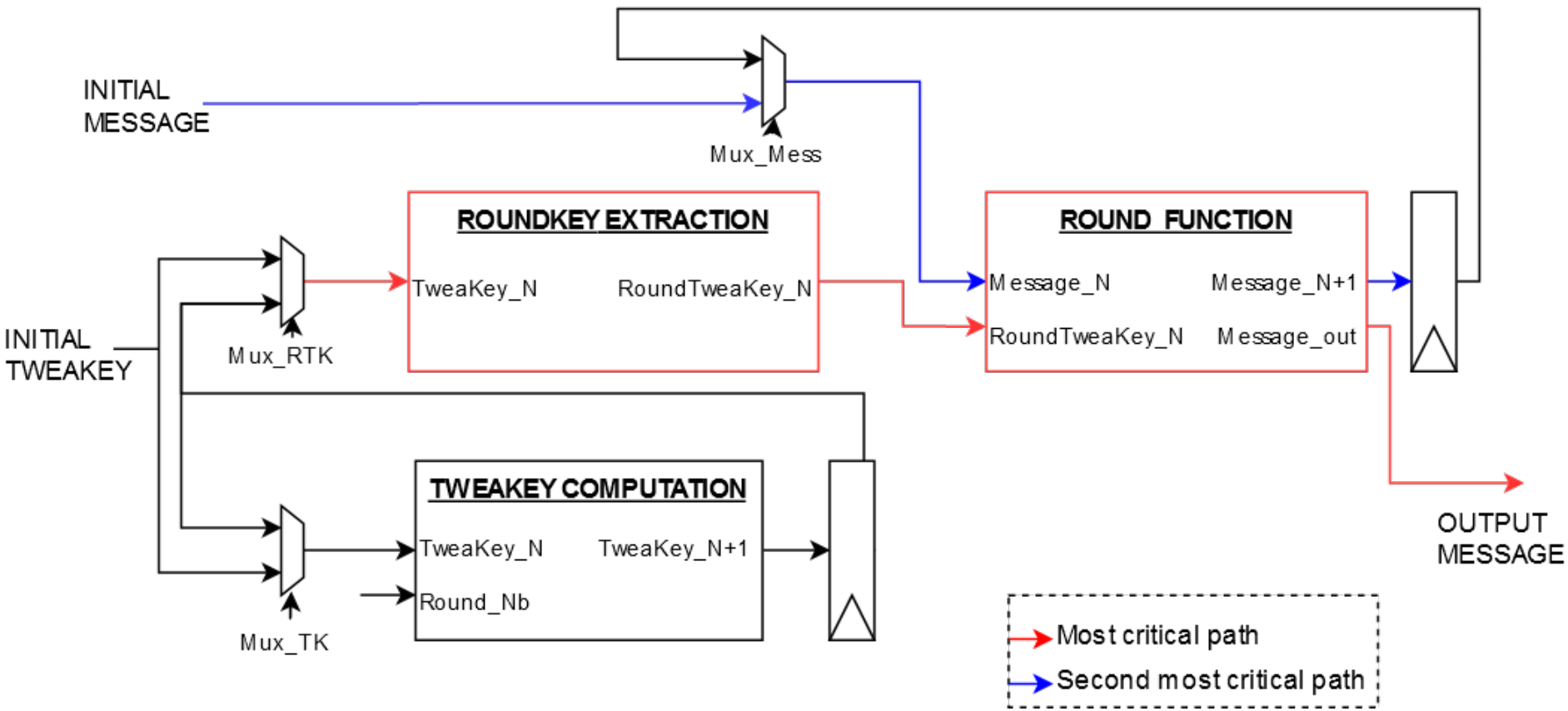
Figure: The Tweakey Schedule. f represents the round function `OneRoundEGFN`.

- $\alpha_0, \cdots, \alpha_{p-1}$ have been chosen as produced by word-ring LFSRs to improve software and hardware performances

Benchmark Conditions

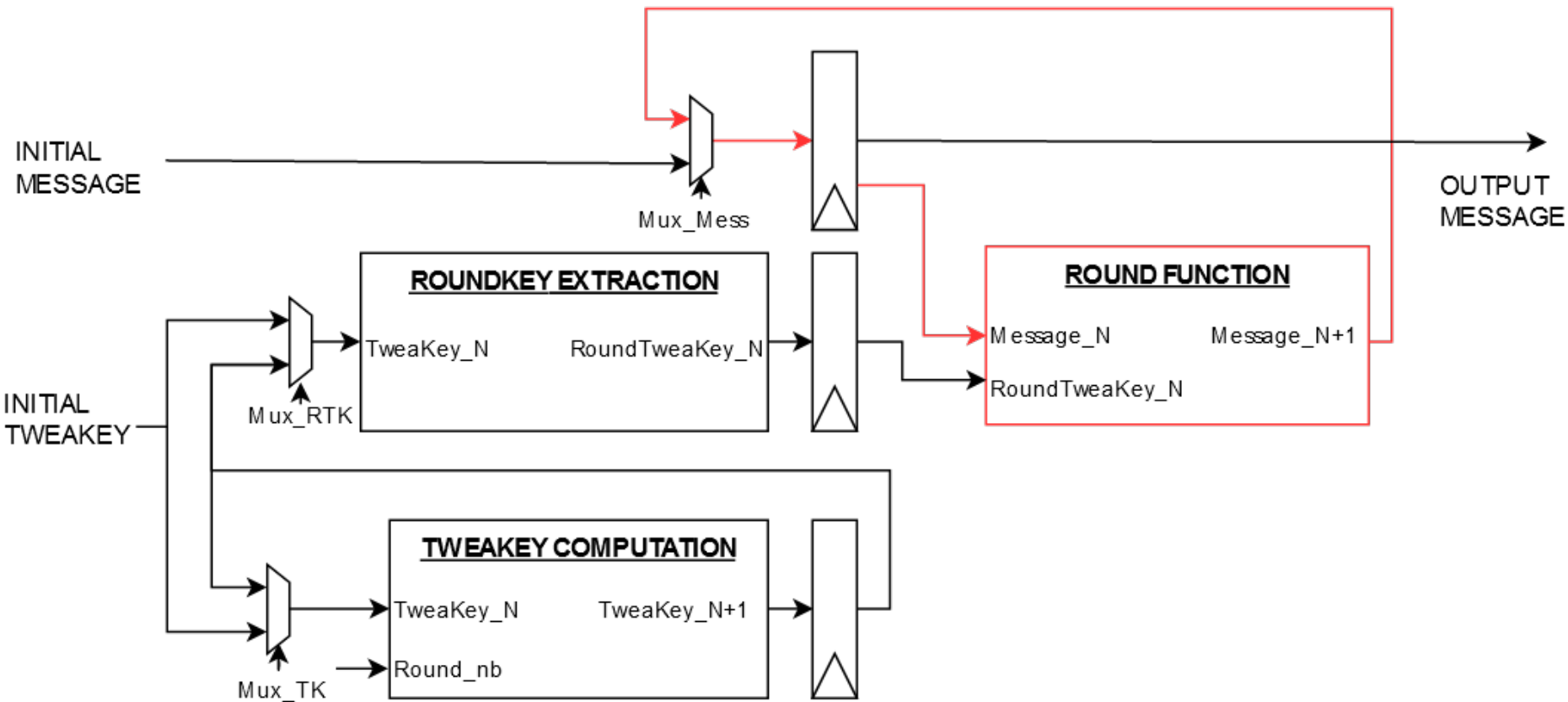
- Design exploration of LILLIPUT-TBC: straightforward, serial, unfolded, threshold.
- VHDL implementations, ISE 14.4, post-place-and-route results
- Xilinx Virtex-6 XC6VLX75T-FF484 FPGA
- Optimization priority: area reduction for straightforward, serial, and threshold/timing performance for unfolded.
- Comparisons with ASCON-128 (portfolio of CAESAR competition): source code provided in the submission package
- Results given by ATHENa v.0.6.5 benchmark
  - Difficult to make a "fair" comparison with ACORN
- Comparisons with AES: Wolkerstorfer *et al.*'s combinatorial S-Box [WOL02]

LILLIPUT-TBC Straightforward Implementation



LILLIPUT-TBC "Pipelined" Implementation

- Goal: decrease the critical path and then accelerate the throughput (TP) by putting additional registers on the datapath



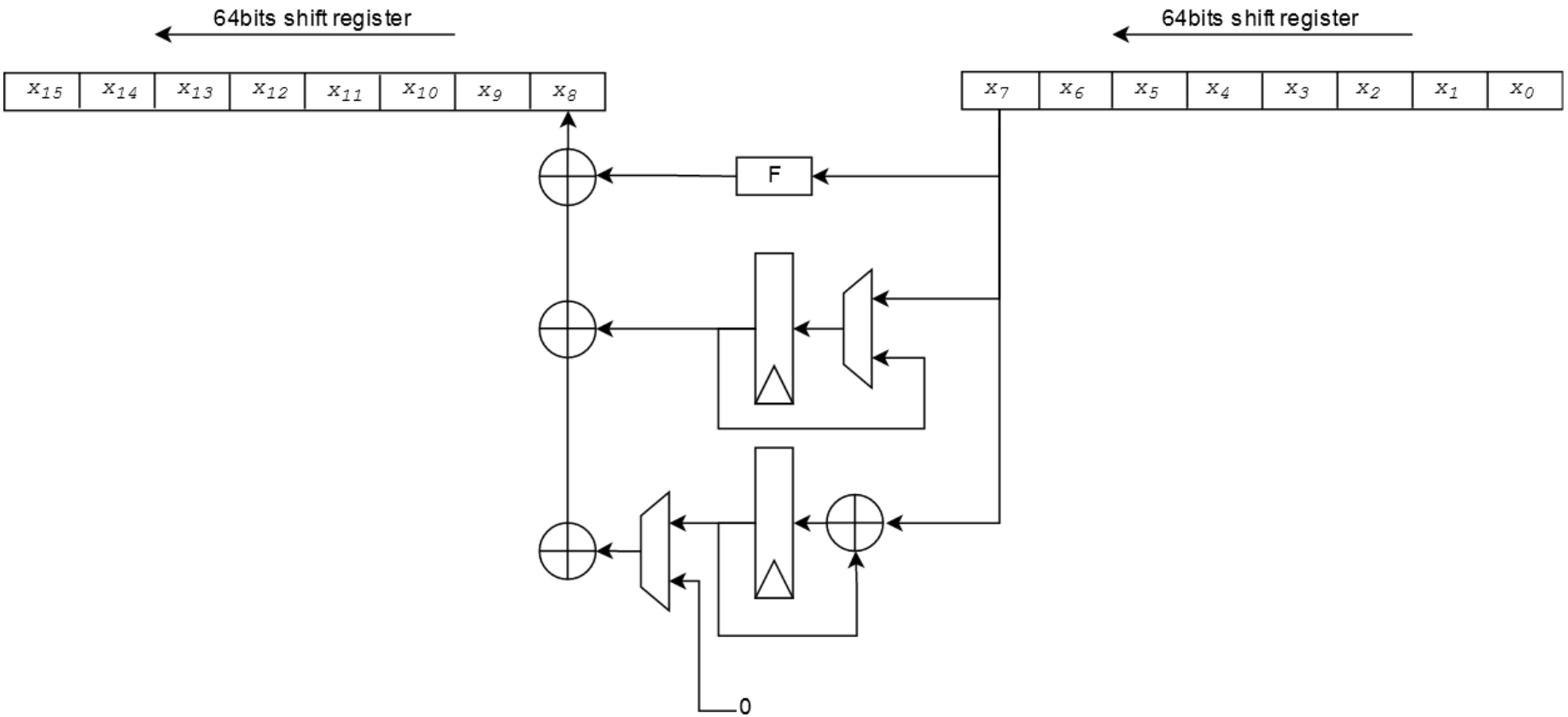
LILLIPUT-TBC "Pipelined" Implementation: Results

	ASCON128	ASCON128A	TBC-I-128	TBC-II-128	AES
LUTs	1318	1422	1304	946	1615
slices	357	387	373	289	437
registers	933	997	1114	975	661
Freq (MHz)	372	357	289	367	170
Throughput(Mbit/sec)	3402	5084	1088	1349	2181

- Compared to ASCON, LILLIPUT-TBC is competitive in terms of area occupation
- But not from a throughput point of view (32 rounds is a lot)
- Version -II more compact than -I
  - You have to implement both encryption and decryption in Version -I
- LILLIPUT-TBC is competitive compared to AES since it provides both encryption and authentication

Lilliput-TBC Serial Implementation

- Goal: only a fraction of one round is processed in a clock cycle. Up to a certain point, this strategy can significantly decrease the area (and the power consumption)



Serial Implementation Results

Table: Results for LILLIPUT-TBC serial implementations, optimized for area reduction.

LILLIPUT-TBC	I-128	I-192	I-256	II-128	II-192	II-256
LUTs	1391	1633	1828	1101	1340	1496
slices	398	471	505	311	349	397
registers	1135	1263	1395	995	1127	1255
Freq (MHz)	316	308	314	342	346	335
TP (Mbps)	157	135	119	170	153	126

- On Xilinx FPGAs, serial implementations of LILLIPUT-TBC do not seem to be a suitable implementation strategy since the savings are canceled by the overheads in additional control logic [MBG17]
- But significant savings in ASIC (like initially stated in [BFM+15]): around 15% gain on a CMOS 28nm technology.

Serial Implementation Results: Comparisons

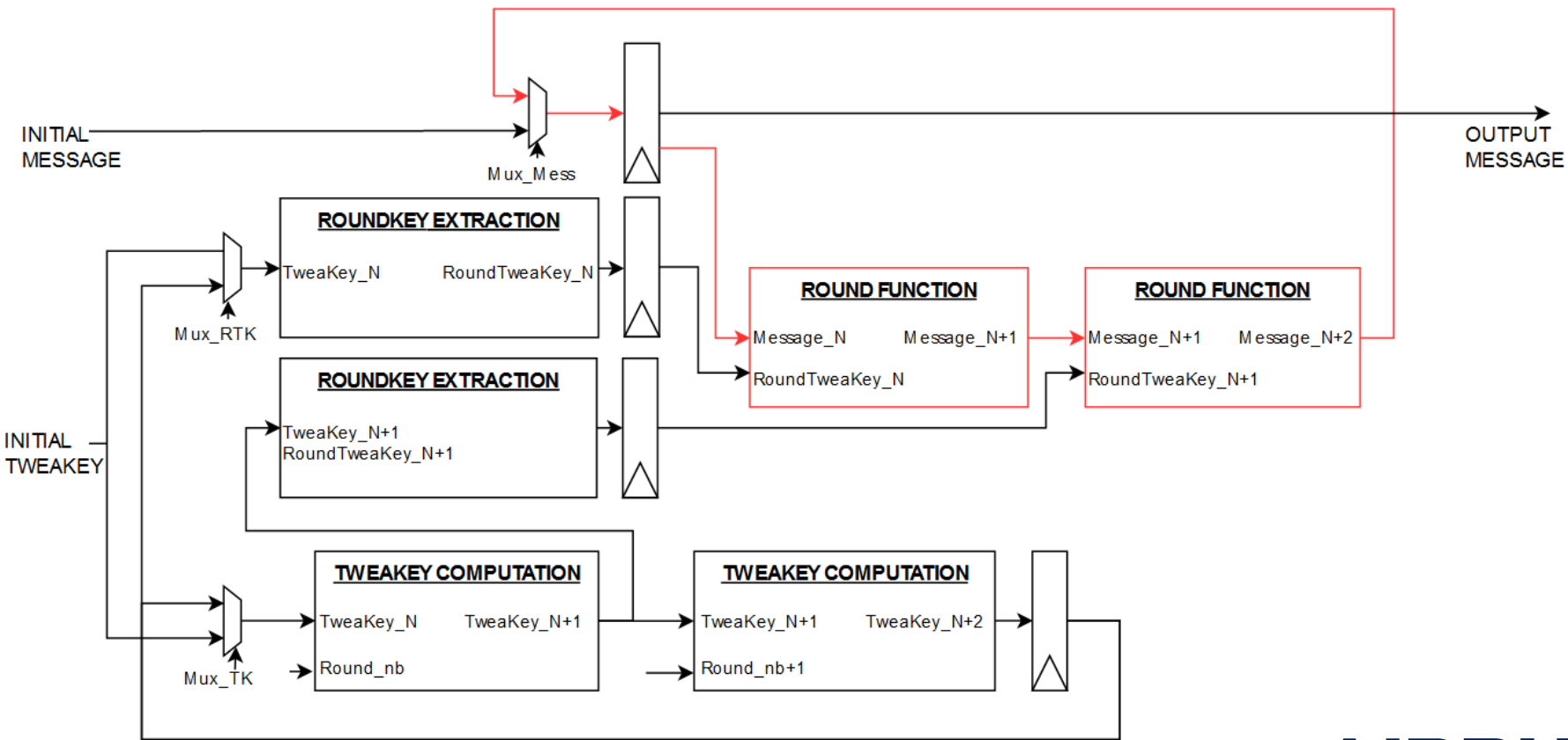
Table: Comparison of LILLIPUT-TBC-128 and ASCON serial implementations optimized for area reduction.

	ASCON128	ASCON128A	TBC-I-128	TBC-II-128
LUTs	1532	1737	1391	1101
slices	434	477	398	311
registers	944	1007	1135	995
Freq (MHz)	309	326	316	346
TP (Mbps)	360	572	157	170

- Serial implementation of LILLIPUT-TBC-128 are more compact than the ones of the existing most compact lightweight authenticated encryption algorithm

LILLIPUT-TBC Unfolded Implementation

- Definition: An unfolded (i.e. loop unrolled) implementation performs several round operations of the encryption/decryption process within one clock cycle
- Goal: Find the optimal unfolding factor from the TP point-of-view



LILLIPUT-TBC-II-128 Unfolded Implementation: Results

Table: Comparison of LILLIPUT-TBC-II-128 unfolding implementations optimized for timing performance.

LILLIPUT-TBC-128	II	uf2x-II	uf4x-II	uf8x-II
LUTs	1128	1487	2142	3983
slices	336	463	645	1125
registers	975	1043	1167	1428
Freq (MHz)	405	242	143	68
TP (Mbps)	1526	1722	1839	1466
TP/area ((Mbps)/slice)	4.54	3.72	2.85	1.26

- Optimal unfolding factor for Version -II is 4 (2 for Version -I)
- The TP is increased up to 20% with optimal unfolding factor

Unfolded ASCON

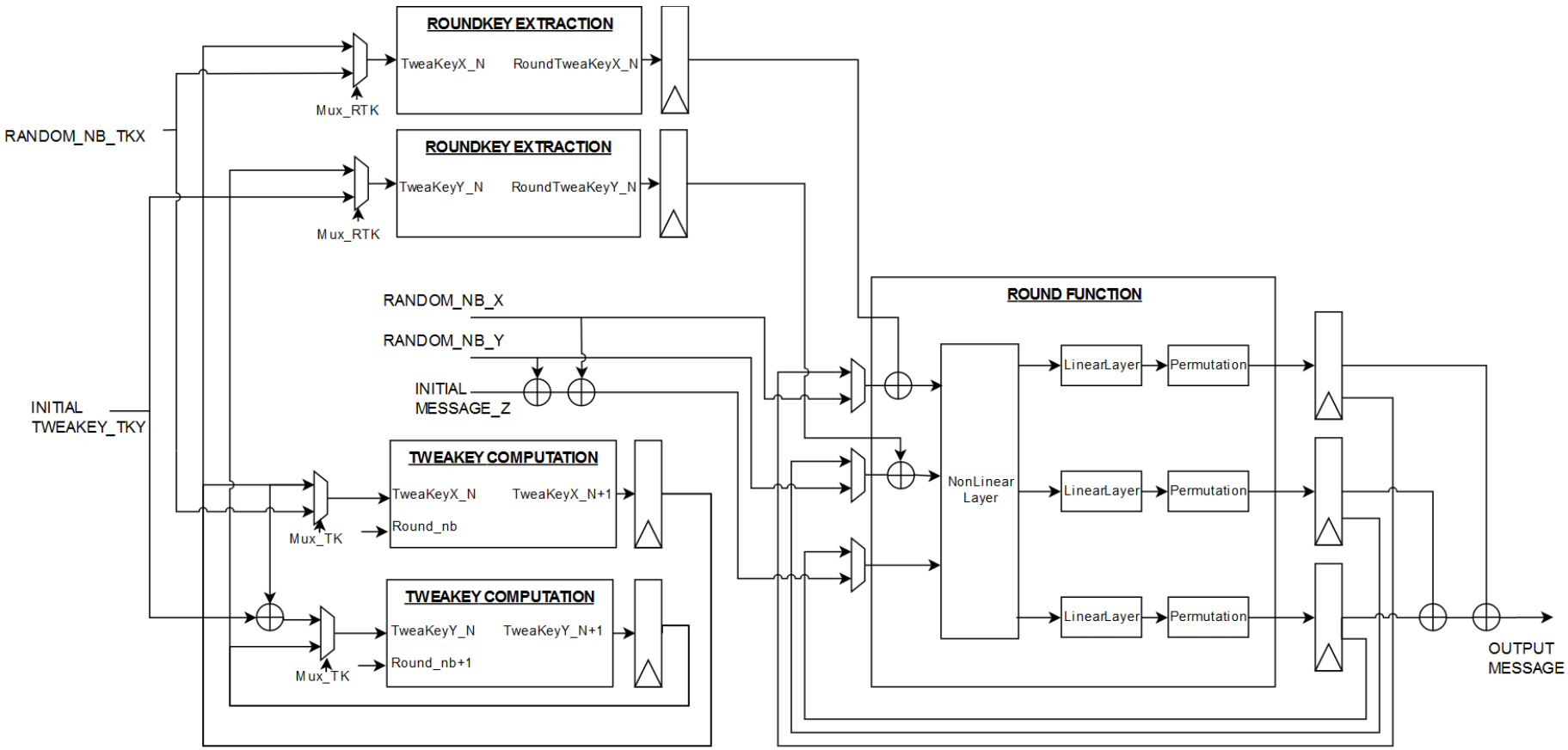
Table: Comparison of ASCON128 unfolding implementations optimized for timing performance.

	Basic	-2x	-3x	-6x
LUTs	1370	2122	2709	4611
slices	392	603	768	1304
registers	933	931	933	928
Freq (MHz)	432	246	161	72
TP (Mbps)	3951	3945	4127	3110
TP/area ((Mbps)/slice)	10.07	6.54	5.37	2.38

- Optimal unfolding factor for ASCON128 is 3
- The TP is increased (only) up to 4% with optimal unfolding factor

LILLIPUT-TBC Threshold Implementation (TI)

- The only tricky part is the round function, especially the F_i function: 3 shares are needed for a theoretical 1st order protection
- Other operations are linear



COMPUTATION

AIRBUS

LILLIPUT-TBC TI: Results

Table: Results for LILLIPUT-TBC threshold implementations, optimized for area reduction.

LILLIPUT-TBC	I-128	I-192	I-256	II-128	II-192	II-256
LUTs	2899	3291	3703	2257	2542	2804
slices	879	966	1013	645	777	951
registers	1941	2197	2457	1808	2068	2324
Freq (MHz)	191	190	191	219	214	211
TP (Mbps)	721	642	556	825	722	614

Summary

- First implementations of LILLIPUT-AE provided
- Good news: LILLIPUT-TBC-128 has comparable Xilinx FPGA slices usage with ASCON-128
- Other good news:
  LILLIPUT-TBC is also competitive with ASCON and ACORN on ATMega 128 (8-bit) and MSP430 (16-bit) software IoT platforms in terms of execution time
  - LILLIPUT-TBC also optimized for threshold implementations
  - Only 7 rounds to protect against Differential Fault Attacks
- Bottlenecks: throughput on FPGAs, 32-bit software implementations (tbc)
- On-going/Future works: LILLIPUT-AE complete benchmarks, straightforward boolean masking implementations, ASIC implementations.
- Let's wish LILLIPUT-AE good luck in the process!

References

- [FLM19] A. Adomnicai, T. P. Berger, C. Clavier, J. Francq, P. Huynh, V. Lallemand, K. Le Gouguec, M. Minier, L. Reynaud, G. Thomas. "Lilliput-AE: a new Lightweight Tweakable Block Cipher for Authenticated Encryption with Associated Data", Submission to NIST LWC Standardization Process, 2019.
- [JNP14] J. Jean, I. Nikolic, and T. Peyrin. "Tweaks and Keys for Block Ciphers: the TWEAKEY Framework". ASIACRYPT, 2014.
- [KR11] T. Krovetz and P. Rogaway. "The Software Performance of Authenticated-Encryption Modes". FSE, 2011.
- [BFM+15] T. Berger, J. Francq, M. Minier and G. Thomas. "Extended Generalized Feistel Networks using Matrix Representation to Propose a New Lightweight Block Cipher: Lilliput". IEEE TC, 2015.
- [MBG17] C. Marchand, L. Bossuet, K. Gaj. "Area-Oriented Comparison of Lightweight Block Ciphers Implemented in Hardware for the Activation Mechanism in the Anti-Counterfeiting Schemes", IJCTA, 2017.
- [WOL02] J. Wolkerstorfer, E. Oswald, M. Lamberger. "An ASIC Implementation of the AES SBoxes", CT-RSA, 2002.

PACLIDO Project

- Fonds Unique Interministériel (FUI) 23, 2017−2020, budget: 5.2M€, funding: 2.0M€
- Label by: Systematic, SCS, Minalogic, ELOPSYS
- Goal: Protect IoT networks with:
  - New lightweight cryptographic primitives, area and energy efficient on most of IoT platforms, and standardized by the NIST
  - New anomaly (attack) detection methods using Machine Learning with high detection rate and low false positives rate
- 4 use cases: Smart City, Home Automation, Avionics, ICS/SCADA
- Let's stay tuned: `paclido.fr`