sLiSCP: Simeck-based Permutations for Lightweight Sponge Cryptographic Primitives

Riham AlTawy, Raghvendra Rohit, Morgan He, Kalikinkar Mandal, Gangqiang Yang, and Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, ON, N2L 3G1, CANADA

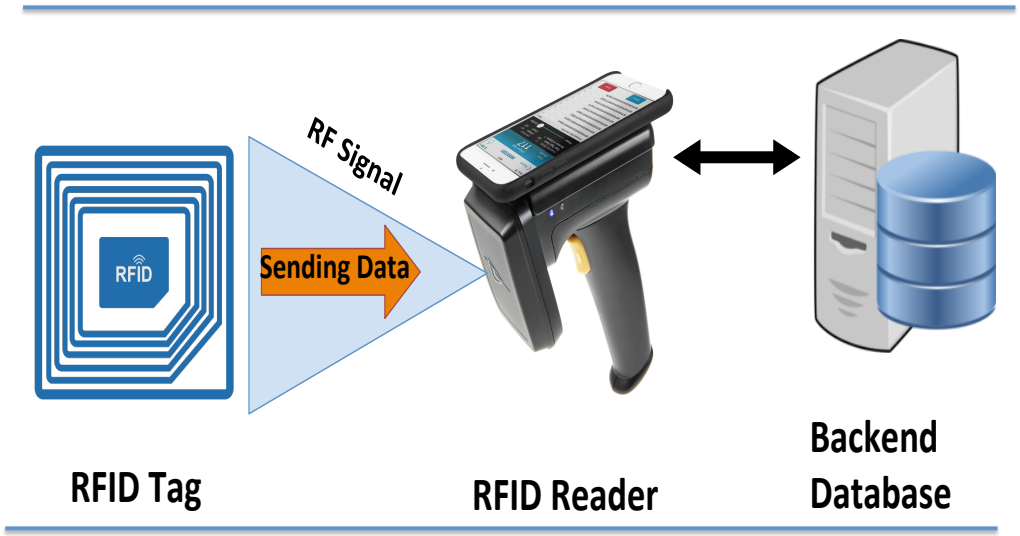
SAC 2017, Ottawa, CANADA
August 17, 2017

UNIVERSITY OF WATERLOO

Outline

Motivation

- Lightweight applications such as RFID and sensor networks are resource-constrained in computational and storage aspects.



- Threats to the RFID systems
  - Leaking info about product details
  - Tracking buyers
  - Identifying information of tags

Motivation (2)

- Multiple security services are needed for securing such applications.
  - Privacy
  - Device authentication
  - Privacy-preserving authentication protocol
- For a passive RFID tag (est. 1k - 10k GE), a maximum of 20% of its area (2k GE) can be used for all security functionalities.

Motivation (3)

- Over the last few years, numerous lightweight symmetric-key primitives such as block ciphers, stream ciphers and hash functions have been proposed.
  - Block ciphers:
    - PRESENT
    - PRINCE
    - SIMON and SPECK
    - SIMECK
    - PRIDE
    - SKINNY
  - Stream ciphers: Grain-80/128, Trivium and WG (WG-5,7,8)
  - Hash functions:
    - PHOTON
    - QUARK
    - SPONGENT
    - LHash
- Various authenticated encryption (AE) schemes have been developed.
  - NORX-16 and Ketje-JR; Grain-128a

Need for a design with multiple crypto-functionalities!

Objectives

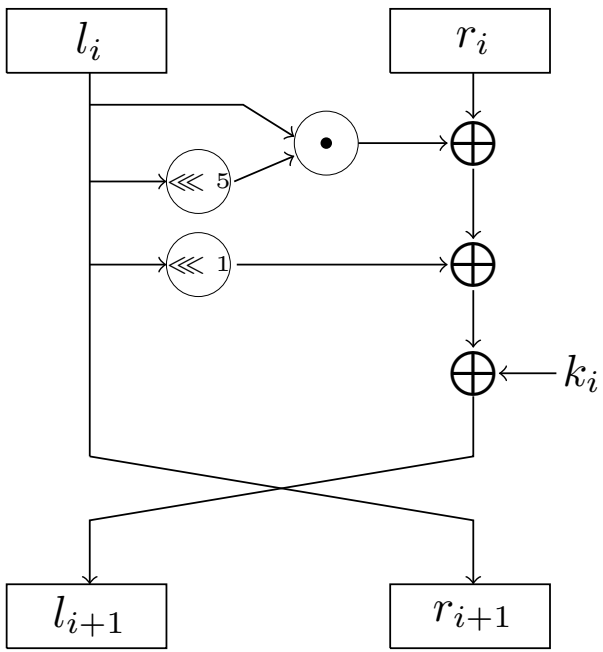
- Providing multiple cryptographic functions with low overhead for lightweight applications
  - Encryption
  - Authentication
  - Hash computation
  - Pseudorandom bit generation
- Efficient hardware implementations
- Providing security guarantees

Contributions

- We design the sLiSCP family of lightweight cryptographic permutations to be used in a unified sponge duplex construction in order to provide (authenticated) encryption and hashing functionalities.
- We implement sLiSCP in CMOS 65 nm ASIC and the area of the parallel architecture is competitive with existing primitives.

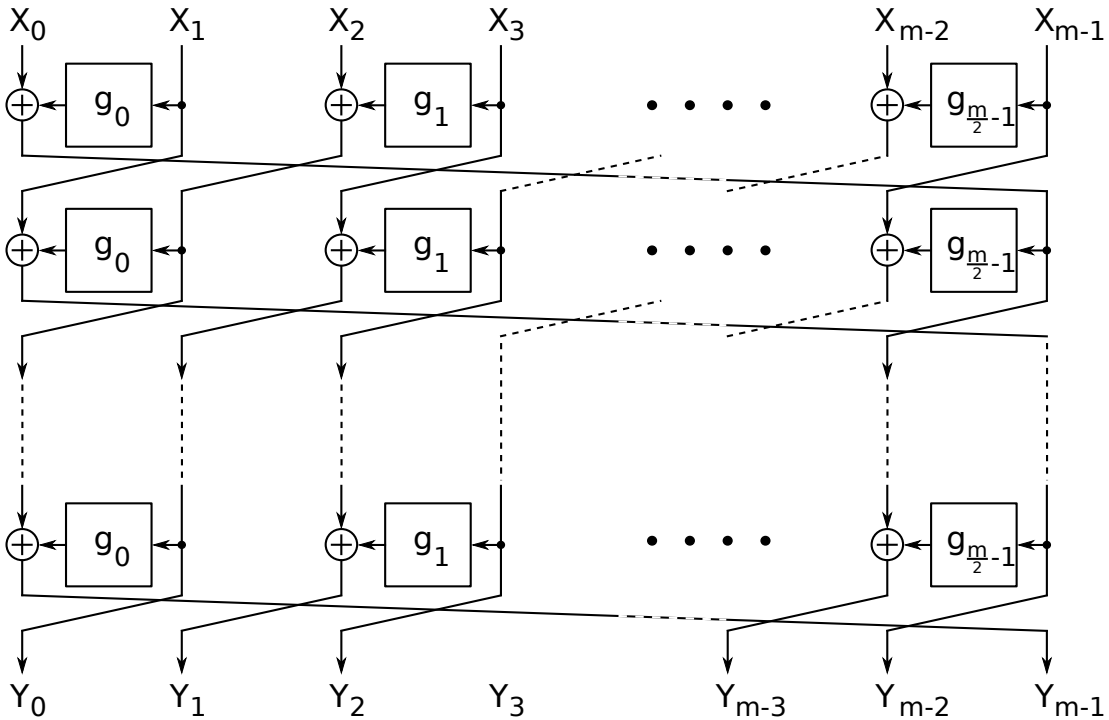
Background: Simeck

- Simeck is a family of block ciphers designed in ComSec lab [Yang et al., CHES 2015]. Its design is based on Simon [Beaulieu et al., eprint 2013/404].
  - Three lightweight instances: Simeck32/64, 48/96, 64/128
  - The Simeck block cipher family is more hardware efficient than the Simon family.

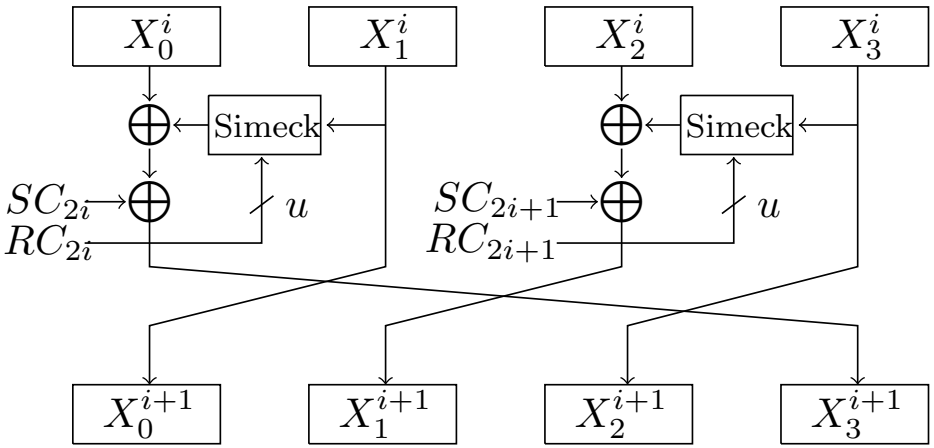


Background: Type 2 GFS

- A Type 2 Generalized Feistel Structure (GFS) [Nyberg, ASIACRYPT'96] is a Feistel network consists of
  - m (even) branches and $\frac{m}{2}$ functions $g_0, g_1, \cdots, g_{\frac{m}{2}-1}$
  - the functions $g_i : \{0,1\}^n \to \{0,1\}^n$



The sLiSCP Family of Permutations



- The sLiSCP is an iterative permutation constructed by combining the Type 2 GFS and round-reduced Simeck cipher.
- Round-reduced Simeck, with no key schedule but round constants added, is used to construct the round function of the GFS.
- Same LFSR is used to generate Simeck^u-m and Feistel round constants.

The sLiSCP Family of Permutations (2)

- Let $h_t^u(\cdot)$ denote the u-round Simeck^u-m box.
- The round function $f : \mathbb{F}_2^{4m} \to \mathbb{F}_2^{4m}$ of sLiSCP is given by

$$
\begin{aligned}
&(X_0^{i+1}, X_1^{i+1}, X_2^{i+1}, X_3^{i+1}) = f(X_0^i, X_1^i, X_2^i, X_3^i) \text{ where} \\
&X_0^{i+1} = X_1^i \\
&X_1^{i+1} = h_t^u(X_3^i) + X_2^i + SC_{2i}, t = RC_{2i} \\
&X_2^{i+1} = X_3^i \\
&X_3^{i+1} = h_t^u(X_1^i) + X_0^i + SC_{2i+1}, t = RC_{2i+1}
\end{aligned}
$$

- On input $(X_0^0, X_1^0, X_2^0, X_3^0)$, the output of an s-step sLiSCP permutation F is given by

$$(X_0^s, X_1^s, X_2^s, X_3^s) = F(X_0^0, X_1^0, X_2^0, X_3^0) = f^s(X_0^0, X_1^0, X_2^0, X_3^0).$$

- An LFSR is employed to generate step constants and round constants.
  - Simeck constants are called *round* constants RC_j
  - Feistel structure constants are called *step* constants SC_j

Two sLiSCP Instances

- There are two lightweight instances of sLiSCP.
- sLiSCP-192: $(\mathbb{F}_2^{48})^4 \rightarrow (\mathbb{F}_2^{48})^4$
  - Internal state size $= 192$
  - Simeck-48 is employed (i.e., $m = 48$)
  - # of Simeck rounds $= 6$
  - # of Feistel steps $= 18$
  - An LFSR of degree 6 is used: $x^6 + x + 1$.
- sLiSCP-256: $(\mathbb{F}_2^{64})^4 \rightarrow (\mathbb{F}_2^{64})^4$
  - Internal state size $= 256$
  - Simeck-64 is employed (i.e., $m = 64$)
  - # of Simeck rounds $= 8$
  - # of Feistel steps $= 18$
  - An LFSR of degree 7 is used: $x^7 + x + 1$.

Permutation (b-bit)	Subblock width m	Rounds u	Steps s	Total # rounds ($u \cdot s$)
sLiSCP-192	48	6	18	108
sLiSCP-256	64	8	18	144

Security Analysis: sLiSCP Design Security Goals

- Bounds against differential and linear cryptanalysis
  - Consider the u-round Simeck round function as an Sbox and use SAT/SMT and MILP tools to provide bounds based on the minimum number of active Sboxes.
- Resistance against diffusion-based attacks
  - Choosing the number of steps equals three times the number of rounds required for the full bit diffusion.
- Resistance against algebraic attacks
  - Choosing the number of rounds that provides an adequate growth of algebraic degree.

Security Analysis: Differential and Linear Cryptanalysis

- Employing an SAT/SMT tool, tightly bound the estimated maximum differential probability (MEDP) of the Simeck boxes

Rounds (u)	1	2	3	4	5	6	7	8	9
MEDP (Simeck^u-48)	0	-2	-4	-6	-8	-11.299	-13.298	-16.597	-18.595

- Develop a MILP model to bound the minimum number of active Simeck boxes h_t^u.

Step	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Min. # of active h_t^u	0	1	2	3	4	6	6	7	8	9	10	12	12	13	14	15	16	18

- Then the MEDCP of sLiSCP-192, and sLiSCP-256 are:

$$\text{MEDCP} = \text{MEDP}(\text{Simeck}^6\text{-}48)^{18} = (2^{-11.299})^{18} = 2^{-203.382}$$
$$\text{MEDCP} = \text{MEDP}(\text{Simeck}^8\text{-}64)^{18} = (2^{-16.597})^{18} = 2^{-298.746}$$

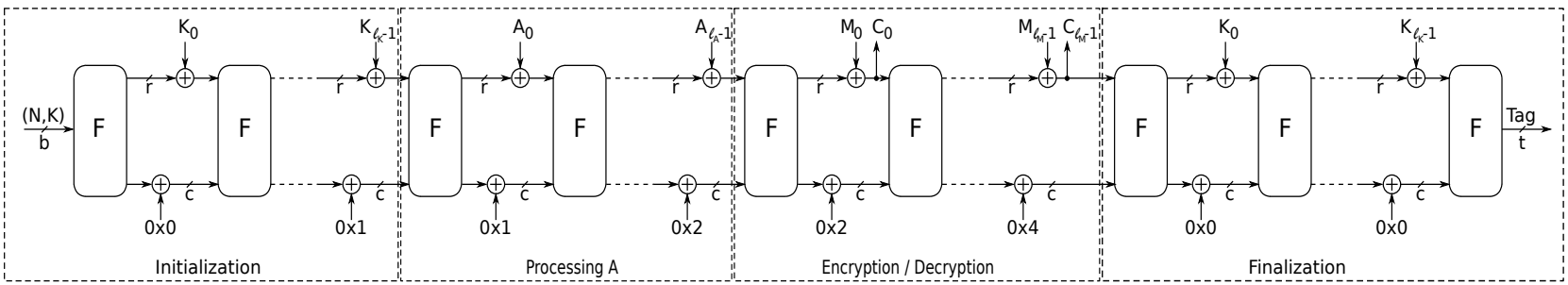
- The maximum expected linear characteristic correlation (MELCC) can be computed analogously.

A Summary of the Distinguishing Complexities

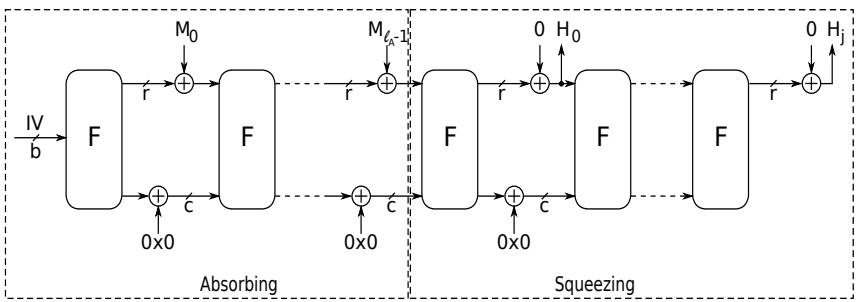
Attacks	Complexity	# steps	Remark
	sLiSCP-**192**		
Differential cryptanalysis	$2^{203.382}$	18	
Linear cryptanalysis	$2^{203.382}$	18	
Integral Distinguishers	2^{188}	9	Division property
Zero-sum Distinguishers	2^{111}	6 (7)	Basic zero-sum (1 extra step)
	2^{158}	8 (9)	Basic zero-sum (1 extra step)
	2^{190}	17	Partial zero-sum (Div. prop.)
	sLiSCP-**256**		
Differential cryptanalysis	$2^{298.746}$	18	
Linear cryptanalysis	$2^{295.2}$	18	
Integral Distinguishers	2^{255}	9	Division property
Zero-sum Distinguishers	2^{178}	6	Basic zero-sum (1 extra step)
	2^{241}	8	Basic zero-sum (1 extra step)
	2^{255}	17	Partial zero-sum (Div. prop.)

Constructing AE and Hash from sLiSCP

- Our goal is to provide as many cryptographic functionalities as possible such as authenticated encryption, stream cipher, MAC and hash function.
- We use the sLiSCP permutation as a unified round function in the sponge construction to design multiple crypto-functionalities.



(a) Authenticated Encryption Mode



(b) Hash Mode

AE and Hash Instances

- There are three instances of authenticated encryption schemes of sLiSCP, denoted by sLiSCP-b/k, with different key and tag sizes.

Algorithm	Key	Nonce	Tag	Block size r	Capacity c	Usage exponent a	Security claim
sLiSCP-192/80	80	80	80	32	160	72	80
sLiSCP-192/112	112	80	112	32	160	40	112
sLiSCP-256/128	128	128	128	64	192	56	128

- There are three instances of hash functions, constructed from sLiSCP, with different hash sizes.

Algorithm	IV	h	r	r'	c	collision	Sec. preimage	Primage
sLiSCP-192	$0x502020$	160	32	32	160	80	80	128
sLiSCP-256	$0x604040$	192	64	64	192	96	96	128
sLiSCP-256	$0x604020$	192	64	32	192	96	96	160

Hardware Implementation Results

- We implemented the sLiSCP instances in the CMOS 65 nm technology.
- The areas for sLiSCP-192 and sLiSCP-256 are given below.

Permutation F	**Process** (nm)	**Area** (GEs)
sLiSCP-192	65	2153
sLiSCP-256	65	2833

- The AE and hash modes consume more XOR gates. The areas for sLiSCP-192 and sLiSCP-256 modes are given below.

Hash	**Process** (nm)	**Area** (GEs)	**AE**	**Process** (nm)	**Area** (GEs)
sLiSCP-192 ($r' = 32$)	65	2271	sLiSCP-192/80	65	2289
sLiSCP-256 ($r' = 64$)	65	3019	sLiSCP-192/112	65	2289
sLiSCP-256 ($r' = 32$)	65	3019	sLiSCP-256/128	65	3039

Hardware implementation results on 130 nm tech. are available in the full paper.

Comparisons with Other Primitives

Hash function	**Parameters**				**Security (bits)**			**Process**	**Latency**	**Area**	**Throughput**
	r	c	r'	h	Pre	2nd Pre.	Coll.	(nm)	(Cycles)	(GEs)	(kbps)
sLiSCP-**192**	32	160	32	160	128	80	80	65	108	**2271**	29.62
Photon-160/36/36	36	160	36	160	124	80	80	180	180	2117	20.00
D-Quark	16	160	16	176	160	80	80	180	88	2819	18.18
Spongent-160/160/16	16	160	16	160	144	80	80	130	90	2190	17.78
Keccak-f[40,160]	40	160	40	200	160	160	80	130	18	4900	222.22
Keccak-f[72,128]	72	128	72	200	128	128	64	130	18	4900	400.00
sLiSCP-**256**	64	192	64	192	128	96	96	65	144	**3019**	44.44
sLiSCP-**256**	64	192	32	192	160	96	96	65	144	**3019**	22.22
Photon-224/32/32	32	224	32	224	192	112	112	180	204	2786	15.69
Spongent-160/160/80	80	160	80	160	80	80	80	130	120	3139	66.67
Spongent-224/224/16	16	224	16	224	208	112	112	130	120	2903	13.33
Spongent-256/256/16	16	256	16	256	240	128	128	130	140	3281	11.43
S-Quark	32	224	32	256	224	112	112	180	64	4640	50
AE algorithm				t	Con.	Int.					
sLiSCP-**192/80**	32	160	32	80	80	80	-	65	108	**2289**	29.62
sLiSCP-**192/112**	32	160	32	112	112	112	-	65	108	**2289**	29.62
sLiSCP-**256/128**	64	192	64	128	128	128	-	65	144	**3039**	44.44
Ketje-Jr	16	184	16	96	96	96	-	-	-	4900	-
NORX-16	128	128	128	96	96	96	-	-	-	2880	-

Conclusions

In this paper:

- we proposed a family of lightweight permutations based on Simeck and Type 2 GFS structure.
- two instances of the permutation are presented and their security has been analyzed against known distinguishing attacks.
- we proposed total six instances of authenticated encryption and hash modes of sLiSCP using the sponge function.
- we implemented all the instances in ASICs with 65 nm technology.

  - sLiSCP-192: 2271 (rate 32)
  - sLiSCP-256: 3019 (rate 64)
  - sLiSCP-256: 3019 (rate 32)
  - sLiSCP-192/80: 2289
  - sLiSCP-192/112: 2289
  - sLiSCP-256/128: 3039

- Full paper can be found at:
  https://eprint.iacr.org/2017/747.pdf
  http://cacr.uwaterloo.ca/techreports/2017/cacr2017-04.pdf

Thank you for your attention!

Communication Security (ComSec) Lab
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, ON, N2L 3G1, CANADA
www.comsec.uwaterloo.ca/