LowMC v3: a security update

Martin Albrecht[1] Christian Rechberger[2,4] Thomas Schneider[3] **Tyge Tiessen**[2] Michael Zohner[3]

FewMul 2017

[1]Royal Holloway, University of London, UK

[2]DTU Compute, Technical University of Denmark, Denmark

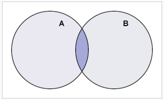
[3]TU Darmstadt, Darmstadt, Germany

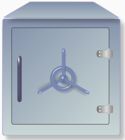
[4]TU Graz, Graz, Austria

Introduction

MPC applications using block ciphers

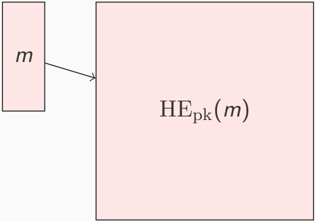
Block ciphers have various applications in MPC



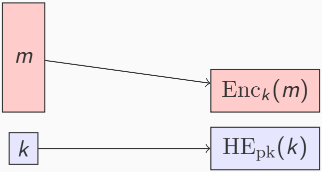


- Oblivious Pseudorandom Functions (OPRFs) for **privacy-preserving keyword search**, **private set intersection**, **secure database join**, etc.
- **Secure storage**: store symmetrically encrypted intermediate MPC values in untrusted storage

FHE Motivation: Avoid ciphertext expansion



FHE schemes typically come with a ciphertext expansion in the order of **1000s** to **1000000s**.



Solution:
Encrypt message symmetrically,
transfer key homomorphically.
Cloud decrypts homomorphically then.

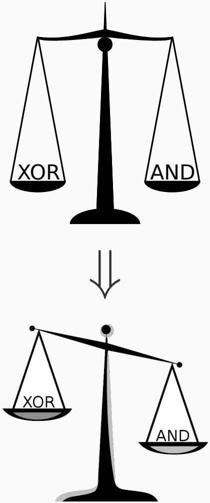
Usage in PQ signature schemes

Zero-knowledge based post-quantum signature schemes can be build by only relying on the security of a hash function.

Bottleneck: Number of multiplications in the hash function.

`http://eprint.iacr.org/2017/279`

New computational models require new designs



- Cost of XOR gate is (almost) negligible compared to AND gate in MPC or FHE setting
- But since 1970s: balance between linear and non-linear operations
- Idea: Explore **extreme** trade-offs

Question

What would an efficient cipher look like if linear operations were for free?

Possible metrics for optimisation

There are three possible metrics to minimise:

1. ANDs per bit of encrypted text (**ANDs/bit**)
2. multiplicative depth of the encryption circuit (**ANDdepth**)
3. total number of ANDs per encryption (**ANDs**)

Question

Can we design a cipher that can be optimized with regard to any combination of these metrics?

Related work

Minimization of multiplicative complexity also relevant in side-channel countermeasures. Designs much less extreme though:

- Noekeon
- Fantomas
- Robin

Joan Daemen, Michaël Peeters, Gilles Van Assche, and Vincent Rijmen. Nessie proposal: Noekeon. In *First Open NESSIE Workshop*, 2000.

Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici. LS-designs: Bitslice encryption for efficient masked software implementations. In *Fast Software Encryption (FSE 2014)*, LNCS. Springer.

There are follow-up designs now

- Kreyvium
- Flip

Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, Renaud SirdeySirdey. Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression. In *FSE 2016*, LNCS, Springer.

Pierrick Méaux, Anthony Journault, François-Xavier Standaert, Claude Carlet. Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. In *EUROCRYPT 2016*, LNCS, Springer.

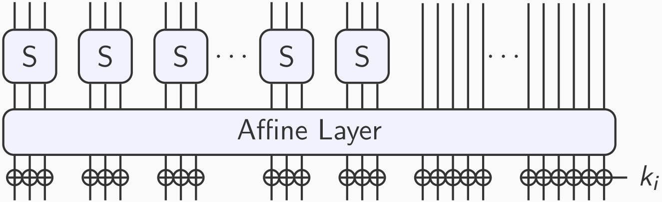
Design Strategy

Design Ideas

Minimise ANDs needed for confusion, maximise diffusion.

- Use an SPN
- Use small S-boxes with low multiplicative complexity
- Maximize diffusion in affine layer
- Utilize a partial substitution layer

The LowMC round function and parameters



Size parameters

- **block size** n bits
- **number** m **of S-boxes** in substitution layer

Security parameters

- **key size** k
- allowed **data complexity** d

Number of **rounds** r is then calculated as a function of the above.

Choice of the S-box

Properties of S-box

- Maximum differential probability 2^{-2}
- Maximum squared correlation 2^{-2}
- Circuit needs only 3 AND gates and has ANDdepth 1
- Any combination of output bits has algebraic degree 2

Algebraic Normal Form of S-box:

$$S_0(A, B, C) = A \oplus BC$$
$$S_1(A, B, C) = A \oplus B \oplus AC$$
$$S_2(A, B, C) = A \oplus B \oplus C \oplus AB$$

Maximise diffusion in affine layer

How do we maximise diffusion in affine layer?

- **Choose most general affine layer**: multiplication with quadratic $n \times n$ matrix over $\mathbb{F}_2$ and addition of constant $\mathbb{F}_2$ vector of length n.

How do we choose good matrices and vectors?

- Unfortunately, determining branch number of a binary matrix is hard in practice and theory.

We thus choose to

- **Choose random matrix** uniformly from all invertible $n \times n$ matrices over $\mathbb{F}_2$.
- **Choose random constant vector** uniformly from $\mathbb{F}_2^n$.

Bonus: This allows novel security arguments.

Instantiation of affine layers and round key matrices

Problem: How do you accountably instantiate the random matrices and vectors?

- instance of cipher cannot use "random" matrices but must use fixed ones
- how choose them in an accountable way ("nothing up the sleeve")?

Our solution:

- **Use Grain LFSR as self-shrinking generator** to produce random bit string
- Then use this string to generate the matrices.

Security Analysis

Determine number of rounds needed for security

The traditional approach of combining some dedicated cryptanalysis with ad-hoc security margins fails due to the variety of parameter combinations and the explicit goal of minimizing multiplicative complexity.

Round number determination

1. Determine the length of elemental distinguishers,
2. determine the length of valid combinations of these,
3. take the maximum of those values.

To determine round number cryptanalysis necessary

Considered elemental distinguishers

- Statistical distinguishers: linear and differential characteristics
- Higher-order derivatives
- Interpolation
- Key-guessing
- Boomerangs
- Impossible differentials

Resistance Against Differential attacks

Standard method to determine probability of best differential characteristic:

1. Determine minimal number of active S-boxes.
2. Combine with maximal differential probability of S-box to determine lower bound on best possible characteristic.

To determine the minimal number of active S-boxes the branch number would be helpful.

Problem

We do not know the branch number of the randomly chosen matrix.

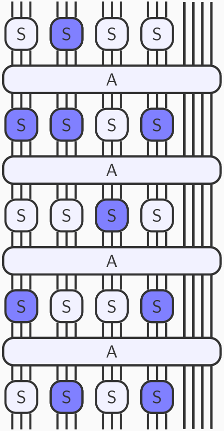
Determining probability of best differential characteristics

Idea

Calculate for each possible good differential characteristic probability that it is realized in instantiation of LowMC. Sum all these probabilities to get upper bound for probability that at least one is realized.

C set of possible good characteristics.

$$\sum_{c \in C} \Pr(c \text{ exists in cipher}) \geq \Pr(\text{good characteristic exists})$$



Question: What is the minimal number of rounds needed to reach a given algebraic degree?

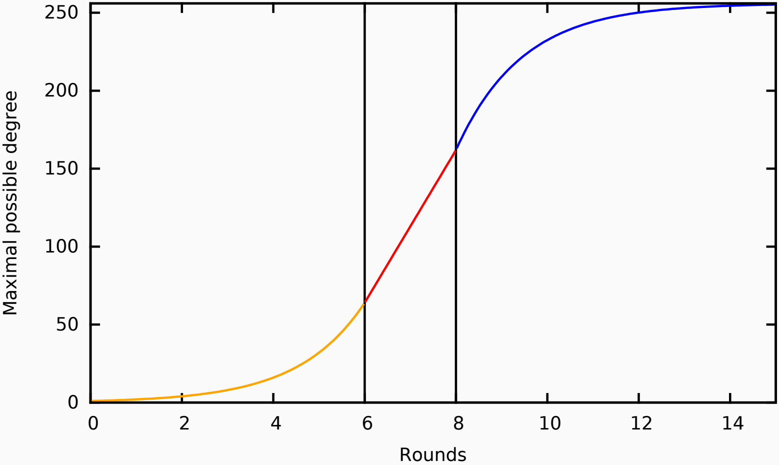
Lemma

If algebraic degree is d_r after r rounds, max. degree in round $r+1$ is

$$\min\left(2d_r, m + d_r, \frac{n}{2} + \frac{d_r}{2}\right).$$

- The first bound is trivial.
- Third bound was proven by Boura, Canteaut, and De Cannière [1]
- Second bound is new.

Growth of the degree



Update for LowMC: v3

The attacks that we considered for version 2 were not enough to guarantee security of LowMC in the entire parameter space.

LowMC with few S-boxes

When LowMC uses only very few S-boxes per non-linear layer, attacks based on difference enumeration could successfully break the security claims.

Parameter space for AES-like security

blocksize n	sboxes m	keysize k	data d	rounds r	# of ANDs	ANDs per bit
256	49	80	64	**12**	1764	6.89
128	31	80	64	**12**	1116	8.72
64	1	80	64	164	**492**	7.69
1024	20	80	64	45	2700	2.64
1024	10	80	64	85	2550	**2.49**
256	63	128	128	**14**	2646	10.34
196	63	128	128	**14**	2646	13.50
128	3	128	128	88	792	6.19
128	2	128	128	128	768	6.00
128	1	128	128	252	**756**	5.91
1024	20	128	128	49	2940	2.87
1024	10	128	128	92	2760	**2.70**
512	66	256	256	**18**	3564	6.96
256	10	256	256	52	1560	6.09
256	1	256	256	458	**1374**	5.37
1024	10	256	256	103	3090	**3.02**

Comparison with most competitive other ciphers

AES-like security

Cipher	Key size	Block size	Data sec.	ANDdepth	ANDs/bit
AES-128	128	128	128	40 (60)	43 (40)
Simon	128	128	128	68	34
Noekeon	128	128	128	32	16
Robin	128	128	128	96	24
Fantomas	128	128	128	48	16.5
LowMC	128	256	128	16	11.8

Comparison with most competitive other ciphers

Lightweight security

Cipher	Key size	Block size	Data sec.	ANDdepth	ANDs/bit
PrintCipher-96	160	96	96	96	96
PrintCipher-48	80	48	48	48	48
Present	80 or 128	64	64	62 (93)	62 (31)
Simon	96	64	64	42	21
Simon	64	32	32	32	16
Prince	128	64	64	24	30
KATAN64	80	64	64	74	36
KATAN32	80	32	32	64	24
DES	56	64	56	261	284
LowMC	80	256	64	14	8.04

Benchmark results

Benchmark results for multiple blocks of total size 12.8 Mbit in GMW

Lightweight Security

Cipher	Present		Simon		LowMC	
Comm. [GB]	7.4		5.0		**2.5**	
	LAN	WAN	LAN	WAN	LAN	WAN
Total [s]	216.88	488.24	272.22	605.41	**45.36**	**155.75**

Long-Term Security

Cipher	AES		Simon		LowMC	
Comm. [GB]	16		13		**3.5**	
	LAN	WAN	LAN	WAN	LAN	WAN
Total [s]	555.91	947.79	447.27	761.90	**64.37**	**215.01**

Benchmark results FHE using HELib by Halevi & Shoup

d	n	ANDdepth	t_{block}	t_{bit}	Cipher	Ref.	Key Sched.
128	128	40	1.5s	0.0119s	AES-128	[2]	excluded
128	128	40	55s	0.2580s	AES-128	[3]	excluded
128	128	40	22m	10.313s	AES-128	[4]	excluded
128	128	40	14m	6.562s	AES-128	[4]	excluded
128	256	12	0.8s	0.0033s	LowMC	this work	included
64	size	24	3.3s	0.0520s	PRINCE	[5]	excluded
64	256	11	0.64s	0.0025s	LowMC	this work	included

Cryptanalysis Challenge

Set of cryptanalytic challenges for LowMC

To raise the trust in LowMC and to increase our understanding of the security of designs like LowMC, we propose a cryptanalytic challenge.

Attack targets

Versions of LowMC tailored for differens settings:

- Signature schemes
- Fully-homomorphic encryption
- Multi-party computation

For each target, there are two attack categories: Fast attack on reduced rounds, and breaking (or getting close to breaking) security claims.

Cryptanalysis Challenge

Check it out at:

`lowmc.github.io/challenge`

Conclusion

Conclusion

- Proposed **flexible block cipher** design of **extremely low** number of **ANDs/bit** and **extremely low ANDdepth**
- Provided experimental and theoretical cryptanalysis to ensure soundness of design
- Demonstrate that symmetric design and cryptanalysis can significantly contribute to make applications of MPC and FHE more practical
- Measured **speed-up** factors between 2 and 25

Open problems

- Can the cost of LowMC in the traditional setting be reduced by using a more efficient affine layer without reducing security claims?
- Improve implementations of LowMC in MPC and FHE settings
- Further refinement of round calculation

Appendix

References

- C. Boura, A. Canteaut, and C. D. Cannière, "Higher-order differential properties of Keccak and Luffa", in *Fast Software Encryption (FSE)*, ser. LNCS, vol. 6733, Springer, 2011, pp. 252–269.
- C. Gentry, S. Halevi, and N. P. Smart, *Homomorphic evaluation of the aes circuit*, Cryptology ePrint Archive, Report 2012/099, `http://eprint.iacr.org/`, 2012.
- Y. Doröz, Y. Hu, and B. Sunar, *Homomorphic AES evaluation using NTRU*, Cryptology ePrint Archive, Report 2014/039, `http://eprint.iacr.org/2014/039`, 2014.

S. Mella and R. Susella, "On the homomorphic computation of symmetric cryptographic primitives", in *Cryptography and Coding*, ser. LNCS, M. Stam, Ed., vol. 8308, Springer Berlin Heidelberg, 2013, pp. 28–44.

Y. Doröz, A. Shahverdi, T. Eisenbarth, and B. Sunar, *Toward practical homomorphic evaluation of block ciphers using Prince*, Cryptology ePrint Archive, Report 2014/233, `http://eprint.iacr.org/2014/233`, presented at Workshop on Applied Homomorphic Cryptography and Encrypted Computing (WAHC'14), 2014.

Key schedule

Reuse random matrix approach for key schedule:

- Derive round keys from general key by multiplication with $n \times k$ binary matrix.
- Choose matrices uniformly at random from all binary $n \times k$ matrices of rank $\min(n, k)$.

Benchmark results for single block in GMW

Lightweight Security						
Cipher	Present		Simon		LowMC	
Communication [kB]	39		**26**		51	
Runtime	LAN	WAN	LAN	WAN	LAN	WAN
Setup [s]	0.003	0.21	**0.002**	0.21	**0.002**	**0.14**
Online [s]	**0.05**	13.86	**0.05**	5.34	0.06	**1.46**
Total [s]	**0.05**	14.07	**0.05**	5.45	0.06	**1.61**

Long-Term Security						
Cipher	AES		Simon		LowMC	
Communication [kB]	170		136		**72**	
Runtime	LAN	WAN	LAN	WAN	LAN	WAN
Setup [s]	0.01	0.27	0.009	0.23	**0.002**	**0.15**
Online [s]	**0.04**	4.08	0.05	6.95	0.07	**1.87**
Total [s]	**0.05**	4.35	0.06	7.18	0.07	**2.02**

Boomerang attacks

- Use good differentials that meet halfway from both sides
- Partial non-linear layers allow probability 1 differentials for a few rounds
- The individual differentials must have higher probability though

Solution

- Calculate length at which no differential is usable for boomerang attacks
- Double this length