New Ciphers for MPC and FHE

Christian Rechberger, DTU

Joint work with Martin Albrecht (RHUL), Thomas Schneider (TUD), Michael Zohner (TUD) and Tyge Tiessen (DTU)

AES circuit is used a lot

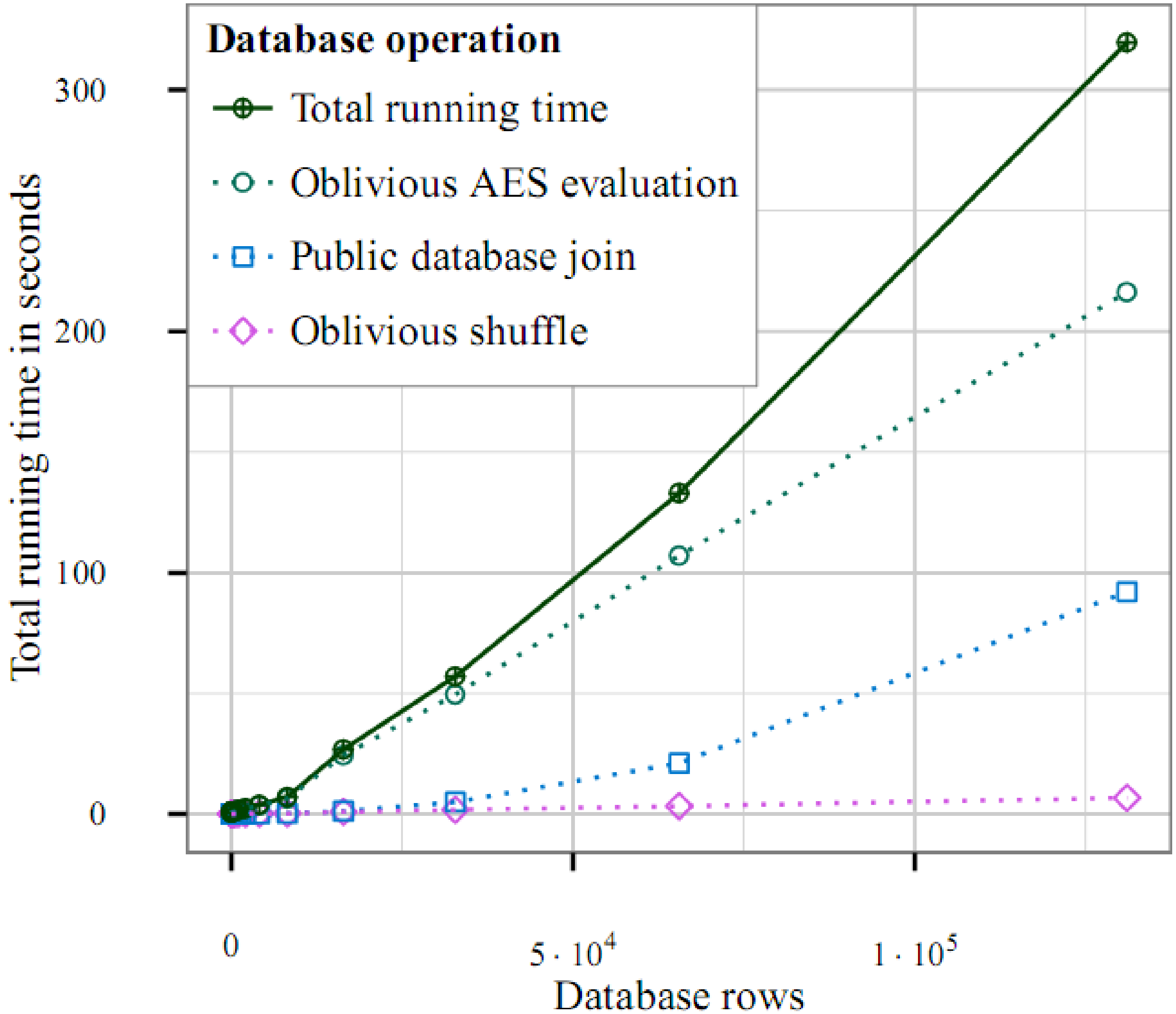
- Often protocols need PRF evaluations
- AES is the standard choice for that
- Designed in 1997, standardized in 2001
- Novel security arguments (proofs) against powerful classes of attacks

Application: Secure database join, three parties

Way to combine several data sources in privacy preserving manner

Source: Cybernetica

Application:
- Merging databases from two different ministries in Estonia, while obeying various data-protection laws.



More MPC applications

- Server-side one-time passwords
  - Shared-evaluation of AES-encryption to derive one-time passwords
- Password encryption with shared key

https://www.dyadicsec.com/media/1080/dyadic whitepaper.pdf

Avoid ciphertext expansion in FHE

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

Proposed solution: encrypt with AES first!

Cloud homomorphically decrypts them (FHE AES needed).

New designs for new computational models

- Since 1970s: balance between linear and non-linear operations
- Idea: Explore ***extreme*** trade-offs

How would a PRF/cipher or a hash function look like if linear operations were for free?

Towards LowMC

- Metrics to optimize: AND-depth, #AND/bit

- Since DES in the 1970s, design was always about trade-off between linear and non-linear operations
- Extreme points of design space where never explored

Related work

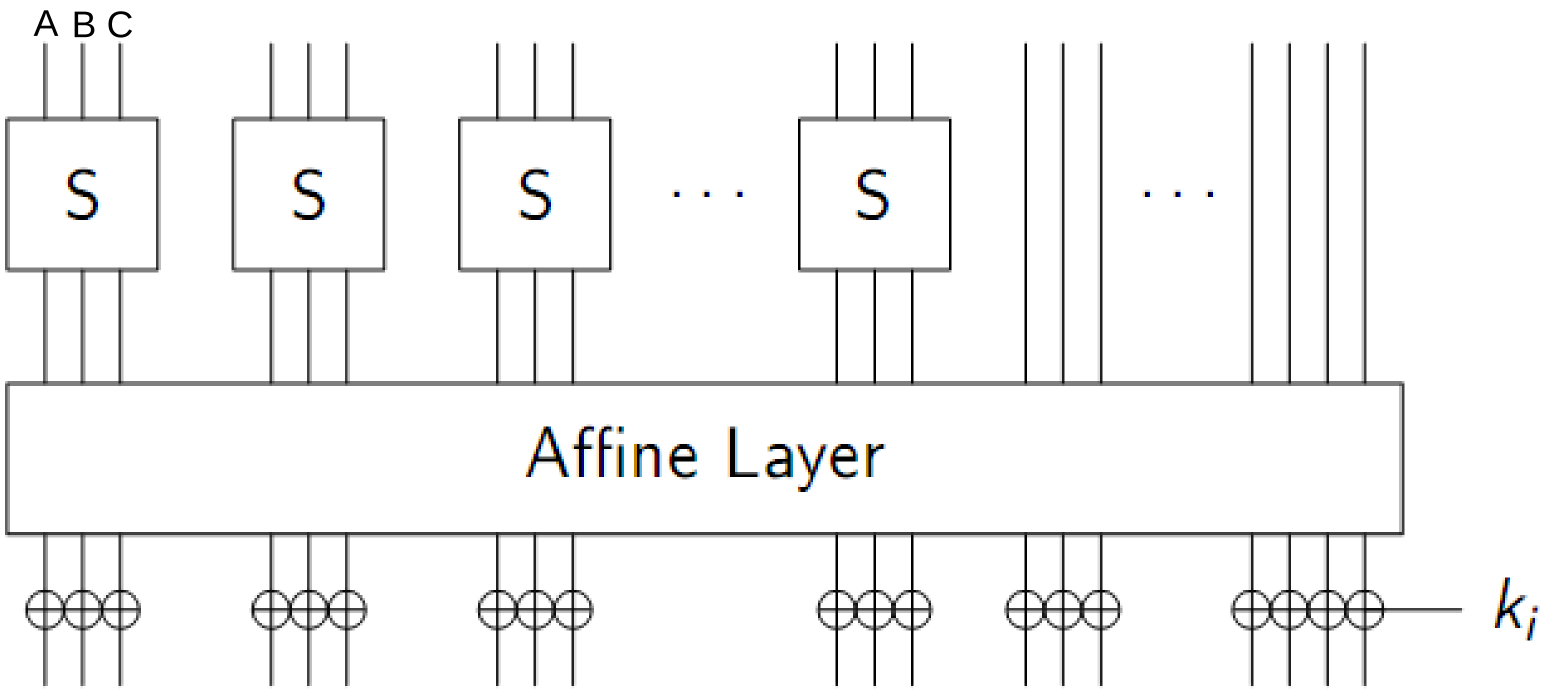
Ciphers that try to minimizing cost of side-channel attack countermeasures

- Noekeon
- LS-designs (Robin, Fantomas)

LowMC

- Joint work with Martin Albrecht (RHUL), Thomas Schneider (TUD), Michael Zohner (TUD) and Tyge Tiessen (DTU)

Round transformation



$$S_0(A, B, C) = A \oplus BC$$

$$S_1(A, B, C) = A \oplus B \oplus AC$$

$$S_2(A, B, C) = A \oplus B \oplus C \oplus AB$$

Affine layer

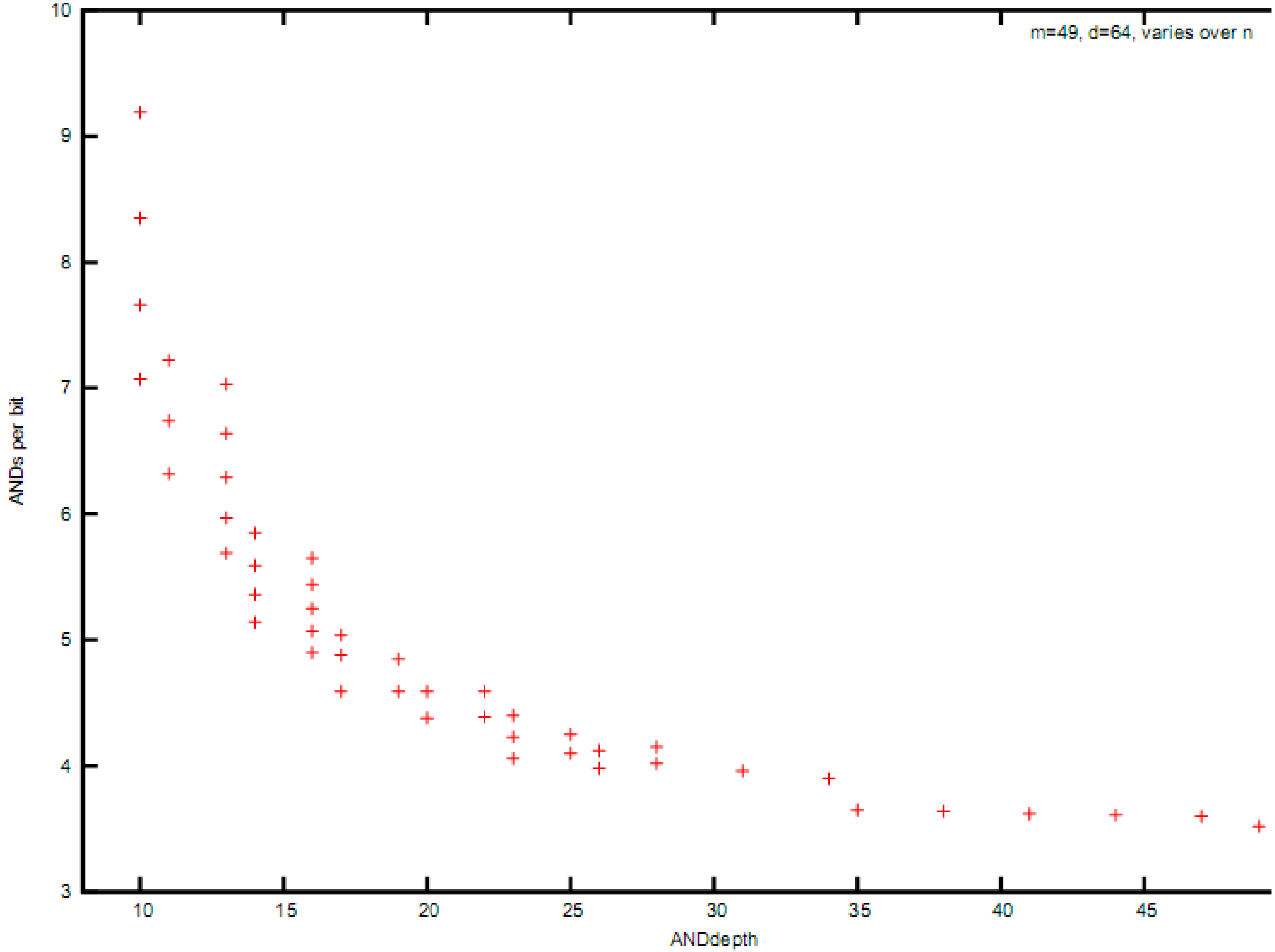
Let block-size be n

Multiplication of internal state with randomly chosen invertible matrix in GF(2) with n rows/columns

Add randomly chosen n-bit vector

Distinct for every rounds

Visualizing the design space



Concrete instances

blocksize n	sboxes m	keysize k	data d	rounds r	ANDdepth	ANDs per bit
256	49	80	64	11	11	6.3
256	63	128	128	12	12	8.86

Comparison with other designs AES-like security

Cipher	Key size	Block size	Data sec.	ANDdepth	ANDs/bit
		AES-like security			
AES-128	128	128	128	40 (60)	43 (40)
AES-192	192	128	128	48 (72)	51 (48)
AES-256	256	128	128	56 (84)	60 (56)
Simon	128	128	128	68	34
Simon	192	128	128	69	35
Simon	256	128	128	72	36
Noekeon	128	128	128	32	16
Robin	128	128	128	96	24
Fantomas	128	128	128	48	16.5
Threefish	512	512	512	936 (4 536)	306 (36)
Threefish	512	1 024	1024	1 040 (5 040)	340 (40)
LowMC	128	256	128	**12**	8.85

Comparison with other designs „lightweight“ security

Cipher	Key size	Block size	Data sec.	ANDdepth	ANDs/bit
Lightweight security					
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
KATAN48	80	48	48	74	32
KATAN32	80	32	32	64	24
DES	56	64	56	261	284
LowMC	80	256	64	11	**6.31**

Properties and Advantages

- Low ANDDepth and ANDs/encrypted bit
- Block size and security(data-complexity) de-coupled
- Differential and linear attacks will *provably* not work, except for extremely unlucky choices of linear layers

GMW benchmarks – long message

Lightweight Security						
Cipher	Present		Simon		LowMC	
Comm. [GB]	7.4		5.0		**2.5**	
Runtime	LAN	WAN	LAN	WAN	LAN	WAN
Setup [s]	214.17	453.89	268.93	568.35	**43.33**	**138.63**
Online [s]	2.71	34.35	3.29	37.06	**2.02**	**17.12**
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**	
Runtime	LAN	WAN	LAN	WAN	LAN	WAN
Setup [s]	553.41	914.27	444.30	727.48	**62.01**	**193.90**
Online [s]	2.50	33.52	2.97	34.42	**2.36**	**21.11**
Total [s]	555.91	947.79	447.27	761.90	**64.37**	**215.01**

GMW benchmarks – single block

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**

FHE implementation benchmarks

d	ANDdepth	#blocks	t_{eval}	t_{block}	t_{bit}	Cipher	Reference	Key Schedule
128	40	120	3m	1.5s	0.0119s	AES-128	[GHS12b]	excluded
128	40	2048	31h	55s	0.2580s	AES-128	[DHS14]	excluded
128	40	1	22m	22m	10.313s	AES-128	[MS13]	excluded
128	40	12	2h47m	14m	6.562s	AES-128	[MS13]	excluded
128	12	600	8m	0.8s	0.0033s	LowMC	this work	included
64	24	1024	57m	3.3s	0.0520s	PRINCE	[DSES14]	excluded
64	11	600	6.4m	0.64s	0.0025s	LowMC	this work	included

Caveat: implementations/underlying techniques improve over time

Conclusions

- Explored extreme corner of cipher design space, motivated by new set of applications
- PRF with ANDdepth 11/12 with 128-bit security, balanced with low number of ANDs/bit

- One order of magnitude speed-gain
- Is this the limit?

Open Problems

- Cryptanalysis
- Design
- Implementation

Open Problems: Cryptanalysis

- Analysis of concrete LowMC instances against other attack vectors
  - Algebraic attacks
    - extremely simple structure
    - more information available per PT/CT pair
  - ?
- (Asymptotic) behavior of attacks vectors when blocksize increases
  - Largely solved for differential/linear attacks
  - MITM/Imposs. Differential/Integral/… attacks?

Open Problems: Design

- Application for even more extreme concrete parameterizations for LowMC?
- Larger S-Boxes with low ANDdepth?
- Hash functions using the same design strategy
- Something that is fast, both in the classical as well as in the new MPC/FHE world.
- LowMC design mainly optimizes for ANDdepth and GF(2) multiplication. What about other settings?

Open Problems: Implementations

Improved implementations of LowMC in

- GMW
- Yao
- SPDZ
- …

Other protocols / applications

- Interested in MPC protocols that are slower but have some desirable property
  - More advantages of choosing LowMC over AES
  - Example: SPDZ with larger #players (cost of multiplication grows quadratic with number of players)
  - Others?
- Applications in other areas
  - SNARKS
  - Obfuscation

Addendum

- Reference implementations, FHE implementations, MPC implementations will be put online soon.
- Paper also (Eurocrypt, eprint)

New Ciphers for MPC and FHE

Q&A

Christian Rechberger, DTU

Joint work with Martin Albrecht (RHUL), Thomas Schneider (TUD), Michael Zohner (TUD) and Tyge Tiessen (DTU)

Bounds against differential attacks

Rounds	[redacted]	p_{stat}
2	[redacted]	-
3	[redacted]	-
4	[redacted]	-
5	[redacted]	-
6	[redacted]	-
7	[redacted]	-
8	[redacted]	-
10	[redacted]	$2^{-5.91}$
11	[redacted]	$2^{-16.00}$
12	[redacted]	$2^{-26.28}$
19	[redacted]	$2^{-101.5}$

Bounds against differential attacks

Rounds	[redacted]	p_{stat}
2		-
3		-
4		-
5		-
6		-
7		-
8		-
10		$2^{-5.91}$
11		$2^{-16.00}$
12		$2^{-26.28}$
19		$2^{-101.5}$

[redacted]

Rounds	[redacted]	p_{stat}
4		-
5		-
6		-
7		-
8		-
9		-
10		-
11		-
12		-
20		$2^{-5.91}$
21		$2^{-10.93}$
22		$2^{-16.00}$
38		$2^{-101.5}$

[redacted]

Bounds + concrete security against differential attacks

Rounds	p_{best}	p_{worst}	n_{imposs}	deg_{exp}	deg_{theor}	p_{stat}
2	$2^{-8.64}$	0	$2^{28.58}$	4	4	-
3	$2^{-12.64}$	0	$2^{28.00}$	8	8	-
4	$2^{-14.64}$	0	$2^{4.25}$	12	12	-
5	$2^{-18.60}$	$2^{-26.06}$	0	16	16	-
6	$2^{-20.49}$	$2^{-25.84}$	0	20	20	-
7	$2^{-23.03}$	$2^{-25.74}$	0	22	22	-
8	$2^{-23.06}$	$2^{-25.74}$	0	23	23	-
10	-	-	-	-	-	$2^{-5.91}$
11	-	-	-	-	-	$2^{-16.00}$
12	-	-	-	-	-	$2^{-26.28}$
19	-	-	-	-	-	$2^{-101.5}$

(a) $n = 24$, $m = 4$, $k = 12$, $d = 12$

Rounds	p_{best}	p_{worst}	n_{imposs}	deg_{exp}	deg_{theor}	p_{stat}
4	$2^{-8.64}$	0	$2^{28.55}$	6	8	-
5	$2^{-12.62}$	0	$2^{28.17}$	10	10	-
6	$2^{-12.64}$	0	$2^{24.93}$	10	12	-
7	$2^{-14.64}$	0	$2^{4.75}$	14	14	-
8	$2^{-16.63}$	$2^{-26.47}$	0	14	16	-
9	$2^{-16.64}$	$2^{-26.06}$	0	16	18	-
10	$2^{-20.34}$	$2^{-25.84}$	0	18	20	-
11	$2^{-20.50}$	$2^{-25.84}$	0	22	22	-
12	$2^{-22.94}$	$2^{-26.06}$	0	22	23	-
20	-	-	-	-	-	$2^{-5.91}$
21	-	-	-	-	-	$2^{-10.93}$
22	-	-	-	-	-	$2^{-16.00}$
38	-	-	-	-	-	$2^{-101.5}$

(b) $n = 24$, $m = 2$, $k = 12$, $d = 12$

Table 5: For two different sets of parameters, experimental results of full codebook encryption over 100 random keys are given. p_{best} and p_{worst} are the best and the worst approximate differential probability of any differential with one active bit in the input difference. n_{imposs} is the number of impossible differentials with one active bit in the input difference. deg_{exp} is the minimal algebraic degree in any of the output bits. deg_{theor} is the upper bound for the algebraic degree as determined from equation 5. p_{stat} is the probability that a differential or linear characteristic of probability at least 2^{-12} exists (see eq. 4).