1. Florian Mendel, FSE 2018 statistics and ToSC info
2. Anton Naumenko, 2R MEDP and MELP for Kuznyechik
3. Dragos Rotaru, Adz for cryptographers
4. Anne Canteaut, FSE and our new publication model
5. Gregor Leander: The workflow of ToSC
6. Aleksei Udovenko, New Directions in White-Box Crypto
7. Yann Rotella, attacking the LILLE cipher
8. Michael Peeters, Ketje Cryptanalysis Prizes
9. Thomas Peyrin, Result of the 2nd Skinny competition
10. Jeremy Jean, FSE 2019 Announcement
11. Shivam Bhasin, COSADE 2018
12. Carlos Cid, SAC 2018 in Calgary
13. Yuhei Watanabe, Extending FELICS for Automotive PKES
14. Gaëtan Leurent, Cryptanalysis records
15. Maria Naya Plasencia, FSE 2018 Best Paper Award
16. Dan Bernstein, CAESAR update
An announcement from the CAESAR committee

The final portfolio of CAESAR algorithms will be revealed on Dec. 26 MMXIX
FSE 2018

Florian Mendel (Infineon Technologies)
María Naya-Plasencia (Inria)
program co-chairs
Since 2016: publication model conference/journal hybrid
IACR Transactions Symmetric Cryptology (ToSC)

- 4 submission deadlines per year
- Rebuttal phase
- Decision after 2 months
  - ACCEPT
  - MINOR REVISION
  - MAJOR REVISION
  - REJECT
- Long papers
- SoK papers
- Hope to get included in Thomson ISI in 2020
Statistics: 174 submissions (148 new)
Acceptance rate: 28% (or 32%)
Resubmissions after major revision

- 2017-2: 9
- 2017-3: 2
- 2017-4: 4
- 2018-1: 11

- 2017-2: 27%
- 2017-3: 6%
- 2017-4: 8%
- 2018-1: 18%
New Publication Model

• Cite ToSC from other ISI Journals (DCC, JoC, LNCS)
• Everything published has been reviewed: if you need more than 20 pages, go for a long paper
• Want also SoK (systematization of knowledge)
• High work load for revisions
• Style file may need some minor improvements but please don’t hack the LaTeX
• Camera ready means camera ready
• Use standard bib file: DBLP or https://cryptobib.di.ens.fr/
Program Committee

Elena Andreeva
Frederik Armknecht
Alex Biryukov
Celine Blondeau
Andrey Bogdanov
Christina Boura
Anne Canteaut
Carlos Cid
Joan Daemen
Patrick Derbez
Itai Dinur
Maria Eichlseder
Pierre-Alain Fouque
Jian Guo
Deukjo Hong
Tetsu Iwata

Jérémy Jean
Pierre Karpman
Nathan Keller
John Kelsey
Stefan Kölbl
Virginie Lallemand
Gregor Leander
Gaëtan Leurent
Subhamoy Maitra
Willi Meier
Bart Mennink
Kazuhiko Minematsu
Shiho Moriai
Ivica Nikolić
Kaisa Nyberg
Léo Perrin

Bart Preneel
Yu Sasaki
Martin Schläffer
Yannick Seurin
Hadi Soleimany
Martijn Stam
François-Xavier Standaert
John Steinberger
Marc Stevens
Bing Sun
Yosuke Todo
Gilles Van Assche
Meiqin Wang
Lei Wang
Thank you

General chair: Elena Andreeva
Invited speaker: Marc Stevens
Rump session chairs: Joan Daemen and Pierre Karpman
Sponsors:

embracing a better life
Thank you

Managing Editor ToSC: Gregor Leander
Technical support: Shai Halevi, Friedrich Wiemer

FSE Steering Committee:
• Anne Canteaut, chair
• Orr Dunkelman
• Tetsu Iwata
• Gregor Leander
• Florian Mendel
• Thomas Peyrin
• María Naya-Plasencia
• Bart Preneel
Thank you!
An announcement from the CAESAR committee

The previous date was mistakenly given in the Julian calendar. The corrected date is Jan. 8 2020
Exact maximum expected differential and linear probability for 2-round Kuznyechik

Vitaly Kiryukhin, Anton Naumenko

JSC «InfoTeCS»

Fast Software Encryption – March 5, 2018
GOST 34.12-2015 – «Kuznyechik»

Kuznyechik is an LSX block cipher
Block size – 128 bit (16 byte)
Key size – 256 bit
It contains 9 full rounds
Round transformations

\( X \) – modulo 2 addition of an input block with an iterative key

\( S \) – parallel application of a fixed bijective byte substitution

\( L \) – linear transformation – matrix of MDS\((32, 16, 17)\), optimal diffusion operation, branch number \( B_d = 17 \)
2-round Kuznyechik

\[ \Delta_1 = \text{L}(\Delta_1) \]

\[ \Delta_2 = \text{L}(\Delta_1) \]

\[ \Delta_y \]
2-round Kuznyechik

\[ \Delta x \]

2-round trail and differential

\[ \Omega = \Delta x \xrightarrow{S} \Delta_1 \xrightarrow{L} \Delta_2 \xrightarrow{S} \Delta y - \text{2-round differential trail} \]

\[ EDCP(\Omega) = \prod_{i=1}^{n} DP(\Delta x[i] \to \Delta_1[i]) \cdot \prod_{i=1}^{n} DP(\Delta_2[i] \to \Delta y[i]) \]

\[ DIFF(\Delta x, \Delta y) = \{ \Omega : \Omega = \Delta x \to \ldots \to \Delta y \} \]

\[ EDP(\Delta x, \Delta y) = \sum_{\Omega \in DIFF(\Delta x, \Delta y)} EDCP(\Omega) \]

\[ MEDP = \max_{DIFF(\Delta x, \Delta y)} \sum_{\Omega \in DIFF(\Delta x, \Delta y)} EDCP(\Omega) \]
Algorithm for finding codewords with the smallest byte weight

- Fix locations of active S-boxes of first and second layers
- Let’s present the linear transformation as a system of equations $\Delta_1 \mathbb{L} = \Delta_2$
- Select and solve the subsystem $\mathbb{S}$ in $\Delta_1 \mathbb{L} = \Delta_2$
- If number of active S-boxes is equal to $B_d$ then we have the set solutions $\Delta_1^{(i)} \mathbb{L} = \Delta_2^{(i)}$, $i = 1, 255$
Algorithm for finding the best differential

- Let number of active S-boxes is equal to $B_d$
- Let’s consider all sets of solutions $\Delta_1^{(i)} \mathbb{L} = \Delta_2^{(i)}$
- We perform the algorithm to construct a differential for each of these sets
- It is based on the «pruning» of the branches of the search tree by using the constructed upper bounds

The result is all the best differentials of 2-round Kuznyechik

\[
\begin{align*}
MEDP &= \left( \frac{8}{256} \right)^{13} \left( \frac{6}{256} \right)^4 = 2^{-86.66...} \\
MELP &= \left( \frac{56}{256} \right)^{2.8} \left( \frac{52}{256} \right)^{2.7} \left( \frac{48}{256} \right)^{2.2} + 2^{-134.601} = 2^{-76.936...}
\end{align*}
\]
Estimate of differential with 18 active S-boxes

Theorem

Let $\Delta x \rightarrow \Delta y$ is the differential in 2-round Kuznyechik. Let $EDP(\Delta x, \Delta y) = MEDP$. Then the number of active S-boxes in $\Delta x \rightarrow \Delta y$ is equal to $B_d = 17$

The main idea of the proof is to construct an upper bound for the differential $\Delta x \rightarrow \Delta y$ containing $B_d + 1 = 18$ active S-boxes.

The upper bound is built by using:

- the greedy principle

- the MDS code property (byte weight of the sum of codewords is not less than $B_d = n + 1$)

- the rearrangement inequality
Conclusion

We presented algorithms:

- for finding codewords with the small byte weight in MDS-codes
- for finding all the best differential trails (linear characteristics) and differentials (linear hulls) in 2-round Kuznyechik

It was shown that in 2-round Kuznyechik:

- the best differential contains one differential trail
- the best linear hull contains 48 linear characteristics.
Thank you for attention!
Questions?
An announcement from the revolutionary CAESAR committee

Power to the people!
In order to accommodate the current political situation, the release date of the final CAESAR portfolio has been postponed to the décadi of the first décade of Thermidor, year CCXXX
You won’t believe what this talk is going to be about!

Click next to see what happens

Dragoș Rotaru

KU Leuven / University of Bristol
Cryptographers see Obfuscation for the first time. Can you believe what they do?
Cryptographer tried to implement a program with 1000000000 lines of code using FHE.

You won’t believe what happened next!
Are you stuck in an infinite loop?

NO

YES
Renowned cryptographer shares secret to achieve fame and glory and eternal life.
This paper is not a joke. You may laugh, but you shouldn’t.

It’s quite horrifying.
One joke study from 2007 on the energy expenditure of adolescents playing video games has been cited about 500 times since then, according to a Google Scholar estimate.
When you read these 19 shocking paper facts:

You’ll change the way you review papers forever!
Try to be kind and helpful
Try to be kind and helpful
Try to be kind and helpful
….  
Try to be kind and helpful
Here’s a paycheck for a McDonald’s researcher. And here’s my jaw dropping to the floor.
What This Ugly Little Bird Can Do To Survive Is Actually Pretty Genius
Best talk you will ever witness:

Modes of operation for computing on encrypted data

You won’t believe who approves!

Tomorrow
"Had anyone subjected Mme. de Gallardon's conversation to that form of analysis which by noting the relative frequency of its several terms would furnish him with the key to a ciphered message, he would at once have remarked that no expression, not even the commonest forms of speech, occurred in it nearly so often as ‘at my cousins the Guermantes’s,’ ‘at my aunt Guermantes’s,’ ‘Elzéar de Guermantes's health,’ ‘my cousin Guermantes's box.’"

This excerpt of Swann's way, by Marcel Proust, was brought to you by BlockLit, the smart Blockchain publisher, and your best choice for putting your next book inside the Blockchain.

Prices starting from 1 cent the iso-latin character

*10% discount for Nobel prize laureates!*
FSE and our new publication model

Anne Canteaut (FSE steering committee)

FSE 2018 rump session, March 2018
Transactions on the kind of Cryptology
that is Symmetric
Motivation

We are not happy with the current publication model

- The *Journal of Craptology* is in open-access only after 4 years.
Journal of Craptology

What is it?

The Journal of Craptology is an electronic journal on cryptologic issues. Papers accepted for publication in the Journal of Craptology relate to cryptology and fall into one or several of the following categories.

1. It is funny.
2. It is controversial.
3. It is crap.

In particular the paper must make us laugh and essentially be aimed at making fun of academic cryptography.

Submission Guidelines

Send either of us an email containing your document, preferably in PostScript, PDF, HTML, or LaTeX. Our call for papers.

Editorial Board

- Tom Berson (Editor Emeritus) : berson at anagram.com
- Nigel Smart (Editor in Cheek): nigel at cs.bris.ac.uk
- Raphael C.-W. Phan : raphaelphan.crypt at gmail.com
- Orr Dunkelman : orrd at cs.technion.ac.il
- Dan Page : page at cs.bris.ac.uk

Reviews

"A seminal journal in its field", Moti Yung.
"If I wanted to know anything about Craptology, this is the place I would turn to first", Chris Mitchell.

Similar Journals You May Wish To Check Out

Journal of Universal Rejection

News

As of Summer 2006 we have decided to relaunch the Journal of Craptology.

The main reason is to encourage people to be more silly, and to help encourage the funnier talks in Rump Sessions at Crypto, EuroCrypt etc.

Indeed we aim to invite the funniest talks at Rump Sessions as invited papers to be published here, and vice versa to have invited talk sessions at Rump Sessions for the funniest papers published here.

Issues

Volume 0, No. 0, December 1998
Volume 0, No. 1, April 1999
Volume 1, December 2000
Volume 2, July 2006
Volume 3, November 2006
Volume 4, May 2007
Volume 5, April 2008
Volume 6, March 2009
Volume 7, Feb 2010
Volume 8, Nov 2011
Volume 9, Feb 2014

NB. If you take offense of some things on this page, be it controversial, funny or crap, please do not email us. The intention of this page is to have fun, not to hurt. If you are hurt, please do not send us emails, you will only hurt us. Just delete your bookmark of this page and forget about it.

The Journal of Craptology was started in 1998 by Lars Knudsen, Keith Martin, and Vincent Rijmen.
Motivation

We are not happy with the current publication model

- The *Journal of Craptology* is in open-access only after 4 years.
- The publication delay is unacceptable
Secure Cloud Computing for Medical Data
by D.J. Bernstein, C. Ellison, T. Lange, K. Lauter, V. Miller, M. Naehrig, and E. Tromer

- presented at Crypto 2009 rump session
- published in November 2011
A better model

ToSC:
Authors of all papers published in the journal within Year $N$ are required to present their work at FSE ($N + 1$)
A better model

ToSC:
Authors of all papers published in the journal within Year $N$ are required to present their work at FSE $(N + 1)$

ToCS:
Authors of all papers presented at the rump session of FSE $N$ are required to submit their work to ToCS within Year $2N$
Impact factor

Make sure that references to ToSC/ToCS papers are standardized and clean.

Don’t refer to Eprint versions.
Special thanks to

Our two Editors-in-Chief:

- Florian Mendel
- María Naya Plasencia
Special thanks to

**Our two Editors-in-Chief:**
- Florian Mendel
- María Naya Plasencia

**Our Managing Editor:**
- Gregor Leander
- Friedrich Wiemer
- Kathrin Lucht-Roussel
Special thanks to

Our two Editors-in-Chief:

- Florian Mendel
- María Naya Plasencia

Our Managing Editor:

- Gregor Leander
- Friedrich Wiemer
- Kathrin Lucht-Roussel

Our General Chair:

- Elena Andreeva
An announcement from the real CAESAR committee

The CAESAR committee wishes to apologize for the previous announcement. The legitimate committee has now been reinstated and has decided on a new date for announcing the portfolio. This will be done on Julian day 2460000, which is a distinguished day.
Author → Editors → Us → RUB LIB

tosc.iacr.org

“First hit in google: namibian-studies.com”
“We send it in two mails, due to size constraints”

“First hit in google: namibian-studies.com”
“We send it in two mails, due to size constraints”

“The author did not send the source files”

“First hit in google: namibian-studies.com”
"We send it in two mails, due to size constraints"
“The author did not send the source files”

“We send it in two mails, due to size constraints”

“First hit in google: namibian-studies.com”
“We send it in two mails, due to size constraints”

“style was hacked using \noindent and increased margins”

“The author did not send the source files”

“First hit in google: namibian-studies.com”
We send it in two mails, due to size constraints.

"First hit in google: namibian-studies.com"

"style was hacked using \noindents and increased margins"

"The author did not send the source files"

"same bibtex label twice for two different works"
“It says (Long Paper) in the title”

“We send it in two mails, due to size constraints”

“style was hacked using \noindents and increased margins”

“The author did not send the source files”

“First hit in google: namibian-studies.com”

“same bibtex label twice for two different works”
“my name was wrongly spelt. Could you please correct it?”

“It says (Long Paper) in the title”

“We send it in two mails, due to size constraints”

“style was hacked using \noindent and increased margins”

“The author did not send the source files”

“First hit in google: namibian-studies.com”

“same biblatex label twice for two different works”
“There is a typo in the preface (cryptoogy, instead of cryptology)”

“my name was wrongly spelt. Could you please correct it?”

“It says (Long Paper) in the title”

“We send it in two mails, due to size constraints”

“style was hacked using \noindent and increased margins”

“The author did not send the source files”

“same bibtex label twice for two different works”

“First hit in google: namibian-studies.com”
null
I, SpongeBob Squarepants, hereby declare that I have nothing to do with this whole sponge function thing. In particular, the Keccak team has used my name for their shameless propaganda without contacting me. And anyway, I find all this permutation-based crypto overrated and think tweakable block ciphers are the way to go for keyed crypto. And what is wrong about HAIFA for hashing?
New Directions in White-box Cryptography

Alex Biryukov, Aleksei Udovenko  
University of Luxembourg, SnT

March 5, 2018
White-box
White-box
White-Box: Industry vs Academia

**Industry**

- Many applications
- Strong need for practical white-box
- Academia does WB: hidden designs

**Theory:** possible using iO/FE, currently impractical

**Practical WB:** few attempts (2002-2011), all broken

**Powerful DCA attack**
White-Box: Industry vs Academia

1. many applications
2. strong need for *practical* white-box
3. industry *does* WB: hidden designs
White-Box: Industry vs Academia

1. many applications
2. strong need for practical white-box
3. industry does WB: hidden designs

1. theory: possible using iO/FE, currently impractical
2. practical WB: few attempts (2002-2011), all broken
3. powerful DCA attack
Our Framework: Two Components

Value Hiding

Structure Hiding

001010101110100100101011101001
1010101010101010010001010101011
...
1000001001100000010101010001001
01100011100000100101011101110

1 Bos et al. CHES 2016
Our Framework: Two Components

Value Hiding

Structure Hiding

1 DCA side-channel attack\(^1\)
2 (new) linear algebra attack\(^2\)

\(^1\)Bos et al. CHES 2016
\(^3\)Goubin et al.: https://eprint.iacr.org/2018/098
Our Framework: Two Components

Value Hiding

1. DCA side-channel attack
2. (new) linear algebra attack

Structure Hiding

1. circuit analysis / simplification
2. fault injections
3. pseudorandomness removal

---

1. Bos et al. CHES 2016
Our Framework: Two Components

Value Hiding

1. DCA side-channel attack\(^1\)
2. (new) linear algebra attack\(^{2,3}\)

Structure Hiding

1. circuit analysis / simplification
2. fault injections
3. pseudorandomness removal

Easier to solve independently

\(^1\)Bos et al. CHES 2016
\(^3\)Goubin et al.: https://eprint.iacr.org/2018/098
Value Hiding

Our solution for value hiding:

1. non-linear masking (vs linear algebra attack)
2. classic linear masking (vs DCA correlation attack)
3. provable security
Our solution for value hiding:

1. **non-linear** masking (vs linear algebra attack)
2. classic **linear** masking (vs DCA correlation attack)
3. provable security

Requires easy-to-obfuscate PRNG!

(easier than generic obfuscation)
Conclusions

- new directions for research in white-box cryptography!
Conclusions

- new *directions* for research in *white-box* cryptography!
- check our paper:
  
  ePrint 2018/049

- an update soon: *provable security* and more *attacks*

Thank you!
An announcement from the CAESAR committee

The CAESAR committee realizes that it greatly overestimated the importance of distinguished days. Accordingly, the release of the final portfolio is postponed to UNIX time $2^{31} - 2^{29} + 2^{27} - 7$, which is a prime number with efficient arithmetic.
PSG VS LOSC : 3 - 0, 3/2/2018

Yann Rotella

Inria - SECRET, Paris, France
\( K = K_1 \parallel K_2 \), of size 80.
\( P \) consists of 120 clocks of \( S_{t+1} = S_t[1] \| S_t[2] \| \cdots \| S_t[39] \| y_t, \) with

\[
y_t = s_t[0] \oplus s_t[5] \oplus s_t[8] \oplus s_t[12] \oplus s_t[16] \oplus s_t[19] \oplus s_t[22] \oplus s_t[26] \oplus s_t[29] \\
\oplus s_t[31] \oplus s_t[32] \oplus s_t[35] \oplus s_t[19] \cdot s_t[22] \oplus s_t[5] \cdot s_t[9] \oplus s_t[26] \\
\cdot s_t[12] \cdot s_t[16] \cdot s_t[19] \oplus s_t[5] \cdot s_t[16] \cdot s_t[26] \cdot s_t[35] \\
\oplus s_t[19] \cdot s_t[22] \cdot s_t[31] \cdot s_t[32] \oplus s_t[9] \cdot s_t[12] \cdot s_t[32] \cdot s_t[35] \oplus s_t[22] \cdot s_t[26] \\
\cdot s_t[31] \cdot s_t[32] \cdot s_t[35] \oplus s_t[5] \cdot s_t[9] \cdot s_t[12] \cdot s_t[16] \cdot s_t[19] \oplus s_t[12] \\
\cdot s_t[16] \cdot s_t[19] \cdot s_t[22] \cdot s_t[26] \cdot s_t[31] \oplus IV[t] \oplus C_i[t]
\]
Hence,

$S_t[1], S_t[2], S_t[3], S_t[4]$ do not intervene in $y_t$. So, for all $K = K_1 || K_2$, $IV$ and $\delta = \cdots \cdots 00...00$,

$$ENC_{K_1,K_2,IV}(X) = \delta \oplus ENC_{K_1 \oplus \delta, K_2 \oplus \delta}(X), \forall X$$

Asking for all 32 $IV$s of the form $\delta$, we recover the key with an exhaustive search of $2^{75}$ (and not $2^{80}$).
Hence,

\( S_t[1], S_t[2], S_t[3], S_t[4] \) do not intervene in \( y_t \). So, for all \( K = K_1 \parallel K_2 \), \( IV \) and \( \delta = \ast \ast \ast \ast \ast 00 \ldots 00 \),

\[
ENC_{K_1,K_2,IV}(X) = \delta \oplus ENC_{K_1 \oplus \delta,K_2 \oplus \delta}(X), \forall X
\]

Asking for all 32 \( IV \)s of the form \( \delta \), we recover the key with an exhaustive search of \( 2^{75} \) (and not \( 2^{80} \)).
An announcement from the CAESAR committee

Do not wait anymore! The final portfolio might be announced today, for YOU!

The CAESAR committee is offering free tickets for a space trip around the solar system at relativistic speed. Waiting for a distant event has never been simpler! The committee will start collecting applications at the end of the rump session.
Outcome of the Ketje Cryptanalysis Prize

Keccak Team

March 5, 2018
KETJE contest as announced March 7, 2017 at FSE

Wanted! Cryptanalysis of:

**Ketje Jr, Ketje Sr, Ketje Minor, Ketje Major**

...possibly weakened, e.g., with increased rates

Reward will be a selection of Belgian beers

mailto: crypto-competitions@googlegroups.com
cc: ketje@noekeon.org
before January 31, 2018

See [https://keccak.team/ketje_contest.html](https://keccak.team/ketje_contest.html)
The submissions are:

<table>
<thead>
<tr>
<th>Submission</th>
<th>Authors</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cube-like 7-round key-recovery on Ketje Sr</td>
<td>Xiaoyang Dong, Zheng Li, Xiaoyun Wang and Ling Qin</td>
<td>March 16 2017</td>
</tr>
<tr>
<td>Conditional cube attacks on round-reduced Ketje</td>
<td>Ling Song, Jian Guo and Danping Shi</td>
<td>October 29 2017</td>
</tr>
<tr>
<td>State-recovery attacks on Ketje Jr</td>
<td>Thomas Fuhr, Yann Rotella and Maria Naya-Plasencia</td>
<td>January 31 2018</td>
</tr>
</tbody>
</table>
And the winners are:

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Names</th>
<th>Prize</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cube-like 7-round key-recovery on Ketje Sr</td>
<td>Xiaoyang Dong, Zheng Li, Xiaoyun Wang and Ling Qin</td>
<td>win Great chocolate!</td>
</tr>
<tr>
<td>Conditional cube attacks on round-reduced Ketje</td>
<td>Ling Song, Jian Guo and Danping Shi</td>
<td>win Great chocolate!</td>
</tr>
<tr>
<td>State-recovery attacks on Ketje Jr</td>
<td>Thomas Fuhr, Yann Rotella and Maria Naya-Plasencia</td>
<td>win Great Beer!</td>
</tr>
</tbody>
</table>
Result of the 2nd Skinny competition

C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich and S.M. Sim

NTU - Singapore

FSE 2018 rump session
Bruges, Belgium - March 5, 2018

Paper, Specifications, Results and Updates available at: https://sites.google.com/site/skinnycipher/

Any new cryptanalysis of SKINNY is welcome!
SKINNY goals and results

Goals
- Provide an alternative to NSA-designed SIMON block cipher
- Construct a lightweight (tweakable) block cipher
- Achieve scalable security
- Suitable for most lightweight applications
- Perform and share full security analysis
- Efficient software/hardware implementations in many scenarios

Results
- SKINNY family of (tweakable) block ciphers
- 64 or 128-bit block, various tweakkey sizes: $n$, $2n$, and $3n$ bits
- Security guarantees for differential/linear cryptanalysis (both single and related-key)
- Efficient and competitive software/hardware implementations
  - Round-based SKINNY-64-128: 1539 GE (SIMON: 1751 GE)
  - on Skylake (avx2): 2.78 c/B (SIMON: 1.81 c/B) for fixed-key
The 2nd **SKINNY** cryptanalysis competition

<table>
<thead>
<tr>
<th>Block size $n$</th>
<th>Tweakey size $t$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$n$</td>
</tr>
<tr>
<td>64</td>
<td>32 rounds</td>
</tr>
<tr>
<td>128</td>
<td>40 rounds</td>
</tr>
</tbody>
</table>

**SKINNY has several versions**:  
- **SKINNY-64-128** has **36** rounds  
- **SKINNY-128-128** has **40** rounds

To motivate further cryptanalysis on **SKINNY**, we proposed several (very) reduced versions for a cryptanalysis competition.
We proposed 5 categories, best cryptanalysis for:

1. 32 rounds of SKINNY-64-128 or 30 rounds of SKINNY-128-128
2. 30 rounds of SKINNY-64-128 or 28 rounds of SKINNY-128-128
3. 28 rounds of SKINNY-64-128 or 26 rounds of SKINNY-128-128
4. 26 rounds of SKINNY-64-128 or 24 rounds of SKINNY-128-128
5. 24 rounds of SKINNY-64-128 or 22 rounds of SKINNY-128-128
The **SKINNY** competition categories

We proposed 5 *categories*, best cryptanalysis for:

- **Cryptanalysis of Reduced round SKINNY Block Cipher**
  by S. Sadeghi, T. Mohammadi and N. Bagheri
  *(very slight improvement of the complexity of the best attack)*

![Bar chart showing SKINNY-64-128 and SKINNY-128-128 categories]
The **SKINNY competition categories**

We proposed **5 categories**, best cryptanalysis for:

- **Cryptanalysis of Reduced round SKINNY Block Cipher**
  by S. Sadeghi, T. Mohammadi and N. Bagheri
  (very slight improvement of the complexity of the best attack)

- **MILP Modeling for (Large) S-boxes to Optimize Probability of Differential Characteristics**
  by A. Abdelkhalek, Y. Sasaki, Y. Todo, M. Tolba and A. M. Youssef
  (improvement of the differential bounds for Skinny)
### Ratio of rounds required for Diff/Lin resistance

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Single Key (SK)</th>
<th>Related Key (RK)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SKINNY-64-128</strong></td>
<td>8/36 = 22%</td>
<td>15/36 = 42%</td>
</tr>
<tr>
<td><strong>SIMON-64-128</strong></td>
<td>19/44 = 43%</td>
<td>no bound known</td>
</tr>
<tr>
<td><strong>SKINNY-128-128</strong></td>
<td>14/40 = 35%</td>
<td>19/40 = 47%</td>
</tr>
<tr>
<td><strong>SIMON-128-128</strong></td>
<td>37/68 = 54%</td>
<td>no bound known</td>
</tr>
<tr>
<td><strong>AES-128</strong></td>
<td>4/10 = 40%</td>
<td>6/10 = 60%</td>
</tr>
</tbody>
</table>

### Ratio of attacked rounds

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Single Key (SK)</th>
<th>Related Key (RK)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SKINNY-64-128</strong></td>
<td>20/36 = 55%</td>
<td>23/36 = 64%</td>
</tr>
<tr>
<td><strong>SIMON-64-128</strong></td>
<td>31/44 = 70%</td>
<td>? ≥ 70%</td>
</tr>
<tr>
<td><strong>SKINNY-128-128</strong></td>
<td>18/40 = 45%</td>
<td>19/40 = 48%</td>
</tr>
<tr>
<td><strong>SIMON-128-128</strong></td>
<td>49/68 = 72%</td>
<td>? ≥ 72%</td>
</tr>
<tr>
<td><strong>AES-128</strong></td>
<td>7/10 = 70%</td>
<td>7/10 = 70%</td>
</tr>
</tbody>
</table>
Comparing Simon and Skinny (single-key)

Ratio of attacked rounds (single-key)

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>36</th>
<th>44</th>
<th>40</th>
<th>68</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKINNY-64-128</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIMON-64-128</td>
<td>20</td>
<td>31</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>SKINNY-128-128</td>
<td></td>
<td></td>
<td></td>
<td>49</td>
</tr>
<tr>
<td>SIMON-128-128</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Comparing Simon and Skinny (related-key)

Ratio of attacked rounds (related-key)

- **SKINNY-64-128**: Ratio 36, Attacked rounds 23
- **SIMON-64-128**: Ratio 44, Attacked rounds 31
- **SKINNY-128-128**: Ratio 40, Attacked rounds 19
- **SIMON-128-128**: Ratio 68, Attacked rounds 49
Thank you!
An announcement from the USA (United Secret Agencies)

Dear cryptographers,
Given the obvious benefit that effective cryptography brings to terrorists and criminals of all sort, we kindly ask you to voluntarily help us in our work.

Please submit the backdoors that we know you have been inserting in your papers (omitted proofs, hidden assumptions, missing security analysis) to backdoors@usa.mil

Cooperation will be rewarded.
FSE 2019 Announcement

Jérémy Jean

ANSSI, France

FSE 2018 Rump Session
March 5, 2018
FSE 2019
Paris, France
March 25-28
Organization

- **Dates**: March 25–28
- **Program Chairs**: Florian Mendel and Yu Sasaki
- **General Chair**: Jérémy Jean
Details

- 3 days and a half!
- Conference will end on Thursday 28 around noon
- FSE/ToSC submission deadlines similar to this year
- Website already online: https://fse.iacr.org/2019/
Submission Deadlines

- Submission: 1 March 2018 (passed)
- Submission: 1 June 2018
- Submission: 1 September 2018
- Submission: 23 November 2018
Conference Venue

- FIAP Jean Monnet Conference Center
- Localisation: Paris 14th
- Easily accessible from both airports (CDG and ORY)
- Some rooms are available in the building
Tentative Conference Fees

- Regular Fee (without IACR fee) .................... 550 USD
- Student Fee (without IACR fee) .................... 275 USD
- Late registration surcharge ......................... 100 USD
Call for Sponsors

We are currently looking for sponsorship!
If you would like to contribute, please come and talk to me or send me an email.

Jeremy.Jean@ssi.gouv.fr
See you in Paris in March 2019!
FSE 2018
FSE 2018

Keywords:
FSE 2018

Keywords:

Symmetries
FSE 2018

Keywords:

Symmetries
Differentials
Can for Once Symmetries And Differentials Ease?
Can for Once Symmetries And Differentials Ease?
COSADE 2018: Facts and Figures

• Since 2010
• 9th event in the series
• Previously located in Darmstadt, Paris, Berlin, Graz
• First time in Asia (Singapore)
• 14 Accepted Papers
• 2 Invited Talks
• Co-located event: Emertech
  • Invited talks on security aspects of emerging technologies
An announcement from the CAESAR committee

Due to a clerical error, the committee has realized that the cost of fast space travel is beyond its current means. It decided that the only acceptable solution to ensure that at least some of you could learn the composition of the final portfolio today was to drastically advance the date of its announcement.

Stay tuned for more exciting information!
Selected Areas in Cryptography – SAC 2018

15-17 August 2018
Calgary, Alberta, Canada
SAC 2018

• to be held at Calgary University on 15-17 Aug 2018
• 25th edition of SAC
• four themes:
  • Design and analysis of symmetric key primitives and cryptosystem.
  • Efficient implementations of symmetric and public key algorithms.
  • Mathematical and algorithmic aspects of applied cryptology.
  • Cryptography for the Internet of Things
• SAC Summer School (S3) on 13-14 August
• Organisers: Mike Jacobson (local co-chair) and Carlos Cid (external/program co-chair)
Calgary

- largest city in the Canadian province of Alberta
  - population ~ 1.2M (third largest in Canada)
- first Canadian city to host the Winter Olympic Games (1988)
- ranked as the 5th most livable city in the world in 2017 (according to the Economist Intelligence Unit)

Calgary

• direct flights from LHR, FRA, AMS, NRT, PEK, several US/Canada cities
  • a little over 3 hours to LAX (if you plan to go to CRYPTO in the following week)

• Calgary is also the home of the CAESAR cocktail
  • made with 2 shots of vodka, a pinch of horseradish, 5 dashes of tabasco, 10 dashes of Worcestershire, over ice, and in a celery salt and spice rimmed glass with Clamato juice. Finished with three turns from a pepper mill on top of the ungarnished product. Garnished with a stick of crisp celery flanked by two cocktail olives, and a lime wedge on the rim

  (the cocktail is popular as a hangover "cure", though its effectiveness has been questioned)

Source: also Wikipedia!
SAC 2018

Important Dates

• Submission deadline: 9 May 2018 (Wed)
• Notifications: 27 June 2018
• Pre-proceedings version deadline: 18 July 2018
• SAC Summer School: 13-14 August 2018
• Conference: 15-17 August 2018

See you in Calgary!
Extending FELICS for Automotive PKES Systems

Yuhei Watanabe$^{1,3}$ Hideki Yamamoto$^{1,2}$
Hirotaka Yoshida$^{1,3}$

$^{1}$SEI-AIST Cyber Security Cooperative Research Laboratory
$^{2}$Sumitomo Electric Industries, Ltd. (SEI)
$^{3}$National Institute of Advanced Industrial Science and Technology (AIST)

FSE 2018, Rump session, 5 March 2018
PKES system

PKES (Passive Keyless Entry and Start) system

1. Cryptographic protocol is used on communication between a key fob and a vehicle ECU
2. Cryptography should offer PKES-software/hardware-flexibility meaning compact in both of software and hardware
3. Public protocol employing AES [GPHM10, TW12]
4. CheckUID-protocol [TW12] using a tweakable block cipher
Tillich et al. proposed
Countermeasure against a tracking threat of the key fob
Tweakable block cipher: \( C = E_k(\text{Nonce} \oplus E_k(P)) \)
Lightweight cryptographic primitives in our evaluation

1. Grain-128a
   - Generate different ciphertexts by initialization vectors

2. SKINNY
   - Lightweight tweakable block cipher
   - Realize a same function as \( C = E_k(Nonce \oplus E_k(P)) \)

3. Chaskey-12
   - Lightweight software-optimized MAC
   - Consider Chaskey-12 as a block cipher and use it as \( E_k \)
Problems and Methods for Evaluation on FELICS

- **Problems**
  1. Evaluate primitives and modes
  2. Flexibility of data length

- **Methods**
  1. Extend primitives and scenarios on FELICS
     - Target primitives
     - Processes of CheckUID-protocol in vehicle
  2. Evaluate short-message performance of stream ciphers
  3. Evaluation value includes following value
     - Key-schedule process on block ciphers
     - Key initialization process on stream cipher
Results on implementation in C on ARM Cortex-M3

1. Primitives (16-byte data)

<table>
<thead>
<tr>
<th>Name</th>
<th>Code (Data) [byte]</th>
<th>RAM (Data) [byte]</th>
<th>RAM (Stack) [byte]</th>
<th># cycles @84MHz</th>
<th>Time [µs]</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>948</td>
<td>208</td>
<td>92</td>
<td>42235</td>
<td>502</td>
<td>FELICS, v01, -O1</td>
</tr>
<tr>
<td>Chaskey-12</td>
<td>108</td>
<td>32</td>
<td>12</td>
<td>302</td>
<td>3.6</td>
<td>Ours, v01, -O1 Based on Chaskey-8 impl. v01 on FELICS.</td>
</tr>
<tr>
<td>SKINNY-128-128</td>
<td>588</td>
<td>48</td>
<td>64</td>
<td>47323</td>
<td>563</td>
<td>Ours, v01, -O1</td>
</tr>
<tr>
<td>Grain-128a</td>
<td>1596</td>
<td>76</td>
<td>88</td>
<td>32361</td>
<td>385</td>
<td>Ours, v04, -O1</td>
</tr>
</tbody>
</table>

2. CheckUID-protocol employing the above primitives
Conclusion

1. Our methods: extending FELICS for protocol evaluation
2. Our results: RAM-cost reduction of CheckUID-protocol by replacing the employed AES with the lightweight primitives:
   - Grain-128a: 53%
   - SKINNY-128-128: 59%
   - Chaskey-12: 74%
3. The implication of our results:
   - Grain-128a and SKINNY fulfill PKES-software/hardware-flexibility meaning:
     - Small amount of RAM on Cortex-M3 for the vehicle ECUs
     - Small area of circuit for the Key-fob (Known results)

Table: Known results on Hardware Implementations

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Area [kgate]</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block cipher</td>
<td>AES</td>
<td>5.4</td>
<td>[SMTM01]</td>
</tr>
<tr>
<td></td>
<td>SKINNY-128-128</td>
<td>2.4</td>
<td>[BJKL16]</td>
</tr>
<tr>
<td>Stream cipher</td>
<td>Grain-128a</td>
<td>2.8</td>
<td>[AHJM11]</td>
</tr>
</tbody>
</table>

- We do not know hardware impl. results of Chaskey-12, though it requires the smallest RAM that we evaluated.
An announcement from the International Association of Crypto

To all IACR members, this is to let you know that We, the IAC, as the prime learned scholarly association about Crypto, have successfully trademarked the name CRYPTO. Consequently, you are hereby required to choose another name for your annual beach party. We kindly propose CRYPTO-NOT-CURRENCY or CRYPTONONO as suggestions.

Sincerely,
The IAC board
Cryptanalysis records

Gaëtan Leurent
Inria, France
FSE 2018 Rump Session
The 3XOR problem

3XOR problem

Given a $n$-bit hash function $H$, find $x, y, z$ such that:

$$H(x) \oplus H(y) \oplus H(z) = 0$$

Best known algorithmics

- 2XOR: Complexity $2^{n/2}$ from the birthday paradox
- 3XOR: Complexity $2^{n/2}$ (slightly less)
- 4XOR: Complexity $2^{2n/3}$ using generalized birthday

[Wagner, Crypto’02]
Recent Results

- Recent results (next wednesday): **3XOR for 96-bit SHA-256**
  - 10,000 CPU hours, 384 MB of RAM
  - *The reader can readily check ...*

- New result (last friday): **3XOR for 119-bit SHA-256**
  - 5 CPU minutes, 20 MB of RAM
  - (reversed endianness)

\[
x = \text{"F00-0x0000B70947f064A1"}
\]
\[
y = \text{"BAR-0x000013f9e450df0b"}
\]
\[
z = \text{"FOOBAR-0x0000e9b2cf21d70a"}
\]

\[
\text{SHA-256}(x) = \text{aa620d4e abb51899 2fbdefb3 63b4774f 88e0f6ec 16d63cf2 6ed00121 c8409e75}
\]

\[
\oplus \text{SHA-256}(y) = 23f9822f 921cddb0 8579b083 8046cb5c 8274ca78 c6eb7991 bde2b5f5 8761b7b4
\]

\[
\oplus \text{SHA-256}(z) = 0f17a88c 455ec6c1 24a252cc 996fbb20 f7de735c 80e8a949 964545fc d9a73226
\]

\[
= 868c27ed 7cf703e8 8e660dfc 7a9d0733 fd4a4fc8 50d5ec2a 4577f128 96861be7
\]
Recent Results

- Recent results (next wednesday): **3XOR for 96-bit SHA-256**
  - 10 000 CPU hours, 384 MB of RAM
  - *The reader can readily check...*  

- New result (last friday): **3XOR for 119-bit SHA-256**
  - 5 CPU minutes, 20 MB of RAM
  - (reversed endianness)

\[
\begin{align*}
x &= "\text{FOO-0x0000B70947f064A1}" \\
y &= "\text{BAR-0x000013f9e450df0b}" \\
z &= "\text{FOOBAR-0x0000e9b2cf21d70a}" \\
\text{SHA-256}(x) &= \text{aa620d4e, abb51899, 2fbdefb3, 63b4774f, 88e0f6ec, 16d63cf2, 6ed00121, c8409e75} \\
\oplus \text{SHA-256}(y) &= 23f9822f, 921cdd0b, 8579b083, 8046cb5c, 8274ca78, c6eb7991, bde2b5f5, 8761b7b4 \\
\oplus \text{SHA-256}(z) &= 0f17a88c, 455ec6c1, 24a252cc, 996fbb20, f7de735c, 80e8a949, 964545fc, d9a73226 \\
\text{= } &= 868c27ed, 7cf703e8, 8e660dfc, 7a9d0733, fd4a4fc8, 50d5ec2a, 4577f128, 96861be7
\end{align*}
\]
Recent Results

- **Recent results (next wednesday):** 3XOR for 96-bit SHA-256
  - 10,000 CPU hours, 384 MB of RAM
  - *The reader can readily check ...*

- **New result (last friday):** 3XOR for 119-bit SHA-256
  - 5 CPU minutes, 20 MB of RAM
  - (reversed endianness)

\[
x = "\text{FOO}-0x0000B70947f064A1"
\]
\[
y = "\text{BAR}-0x000013f9e450df0b"
\]
\[
z = "\text{FOOBAR}-0x0000e9b2cf21d70a"
\]

\[
\text{SHA-256}(x) = \begin{array}{c}
\text{aa620d4e}
\text{abb51899}
\text{2fbdefb3}
\text{63b4774f}
\text{88e0f6ec}
\text{16d63cf2}
\text{6ed00121}
\text{c8409e75}
\end{array}
\]
\[
\oplus \text{SHA-256}(y) = \begin{array}{c}
\text{23f9822f}
\text{921cddb0}
\text{8579b083}
\text{8046cb5c}
\text{8274ca78}
\text{c6eb7991}
\text{bde2b5f5}
\text{87617b4}
\end{array}
\]
\[
\oplus \text{SHA-256}(z) = \begin{array}{c}
\text{0f17a88c}
\text{455ec6c1}
\text{24a252cc}
\text{996fbb20}
\text{f7de735c}
\text{80e8a949}
\text{964545fc}
\text{d9a73226}
\end{array}
\]
\[
= \text{868c27ed}
\text{7cf703e8}
\text{8e660dfc}
\text{7a9d0733}
\text{fd4a4fc8}
\text{50d5ec2a}
\text{4577f128}
\text{96861be7}
\]
Recent Results

- Recent results (next wednesday): 3XOR for 96-bit SHA-256
  - 10 000 CPU hours, 384 MB of RAM
  - *The reader can readily check ...*

- New result (last friday): 3XOR for 119-bit SHA-256
  - 5 CPU minutes, 20 MB of RAM
  - (reversed endianness)

\[
x = "F00-0x0000B70947F064A1"
y = "BAR-0x000013F9E450DF0B"
z = "F00BAR-0x0000E9B2CF21D70A"
\]

\[
\text{SHA-256}(x) = 000000a9 4fc67b35 beedd47fc addb8253 911bb4fa ecaee2d9 f46f7f10 5c7ba78c
\]
\[
\oplus \text{SHA-256}(y) = 00000017 d29b29eb a0ef2522 db22d0cc 5d48d2f9 36149197 6430685b 1266ee76
\]
\[
\oplus \text{SHA-256}(z) = 000000be 9d5d52de 1e0262de e51c1119 edff081d 868fe419 879932ab bbcfe66e
\]
\[
= 00000000 00000000 00000000 93e54386 21ac6e1e 5c359757 17c625e0 f5d2af94
\]
Recent Results

- Recent results (next Wednesday): 3XOR for 96-bit SHA-256
  - 10 000 CPU hours, 384 MB of RAM
  - *The reader can readily check* ...

- New result (last Friday): 3XOR for 119-bit SHA-256
  - 5 CPU minutes, 20 MB of RAM
  - (reversed endianness)

\[
\begin{align*}
x &= G80hI1Uwk1yHTFeMAAIuaN9/zpdoInwPsYUBj9Z+/p0=b64 \\
y &= ProWYdocsPEQXxgSNHl0Wh3S8MZe4WQH2AFDj5qtf9o=b64 \\
z &= i/dqm4xNB2uJyDf07zqv4lz4YtKYIyAFd4DpdsnbfM=b64 \\
\end{align*}
\]

SHA-256(x) = 00000000 00000000 024388d4 d89fc0d6 f15e504b 85f2ebe4 12b75a27 a9581285

⊕ SHA-256(y) = 00000000 00000000 056fd7db a401e927 8b4929a7 d9aa17a2 eb19ab56 be56929c

⊕ SHA-256(z) = 00000000 00000000 072c5f0f 7c9e28c8 a51781c6 3e4bafe3 73281e9d 82b9aaef

= 00000000 00000000 00000000 00000139 df00f82a 621356f5 8a86efec 95b72af6
How did I do it?
How did I do it?

I cheated!

- With pre-computation
- That someone else was doing anyway
Distributed computing

Gaëtan Leurent (Inria, France) Cryptanalysis records FSE 2018 Rump Session
Distributed computing

Pre-computation

- A few years
- Using more than 1GW of power
- Distributed across the globe
Miners are trying very hard to find small hashes

To run an inefficient payment network (4 transactions per second)

- Bitcoin: $2^{17.5}$ SHA-256 hashes with 64 leading zeros
- Ethereum: $2^{20}$ Keccak hashes with 50 leading zeros
- Run 3XOR on this list!
Miners are trying very hard to find small hashes
To run an inefficient payment network (4 transactions per second)
- Bitcoin: $2^{17.5}$ SHA-256 hashes with 64 leading zeros
- Ethereum: $2^{20}$ Keccak hashes with 50 leading zeros
- Run 3XOR on this list!
Attacks demonstration

- We like to demonstrate second-preimage attacks with a preimage of zero
  - 3XOR for 96-bit SHA-256
  - 64-bit preimage of MD4 compression function

- Brute-force can provide the same kind of results
  - 87-bit SHA-256 preimage (from Bitcoin)
  - 70-bit? Keccak preimage (from Ethereum)

\[
x = 2b\text{NETgFgklnMBeeiMgCsqfT6QuVvwCBHF89t0TbfnI} = \text{b64}
\]

\[
\text{SHA-256}(x) = 00000000 \ 00000000 \ 00001124 \ 6f99d9 \ 4f91628d \ 71c9d75a \ d2f9a06e \ 2beb7e92
\]
Attacks demonstration

- We like to demonstrate second-preimage attacks with a preimage of zero
  - 3XOR for 96-bit SHA-256  \[\text{[BDF, FSE’18]}\]
  - 64-bit preimage of MD4 compression function  \[\text{[L, FSE’08]}\]

- Brute-force can provide the same kind of results
  - 87-bit SHA-256 preimage (from Bitcoin)
  - 70-bit? Keccak preimage (from Ethereum)

\[
x = 2\text{bNETgFgklnMBeeiMgCsqfT6QulVvwCBHF89t0TbfnI}_b_{64}
\]

\[
\text{SHA-256}(x) = 00000000 00000000 0000112 46f099d9 4f91628d 71c9d75a d2f9a06e 2beb7e92
\]
Attacks demonstration

- We like to demonstrate second-preimage attacks with a preimage of zero
  - 3XOR for 96-bit SHA-256
  - 64-bit preimage of MD4 compression function
  - [BDF, FSE’18]
  - [L, FSE’08]

- Brute-force can provide the same kind of results
  - 87-bit SHA-256 preimage (from Bitcoin)
  - 70-bit? Keccak preimage (from Ethereum)

Cryptanalysis records

- SHA-1 collision [SBKAM, Crypto’17] 2^{63} SHA-1
- RSA-768 factorization [KOFLTBGKMTZ, Crypto’10] 2^{67} instructions
- Bitcoin network 2^{74} SHA-256/hr
Blockchain is stealing crypto

A look at how cryptocurrencies and blockchain are reshaping our world from Bloomberg @business

The era of cryptocurrency "anarchy" must come to an end, Bank of England's Mark Carney says bloom.bg/2GVekUq
Blockchain is stealing crypto

Gaëtan Leurent (Inria, France)
Cryptanalysis records FSE 2018 Rump Session

Cryptoanalyst
@Bitthereumcoin

Technical analyzer of cryptocurrencies. Tweets, retweets and more. Only views, no advice.

The Netherlands
Gaëtan Leurent (Inria, France)

2018 Crypto Valley Conference on Blockchain Technology 20-22 June, Switz
via Blockfolio: goo.gl/Lqzhjr

Cryptanalysis records
Cryptocurrencies are getting all the attention, and stealing the crypto name...

What can we do?

- Become cryptoanalysts?
- Use this computation for science?
  - Verify that SHA-256 is not biased?
  - Create new coin based on SHA-1 collisions?
- Rebrand symmetric cryptography as Pre-shared-key two-party blockchain?
Cryptocurrencies are getting all the attention, and stealing the crypto name...

What can we do?

 Become cryptoanalysts?

 Use this computation for science?
  - Verify that SHA-256 is not biased?
  - Create new coin based on SHA-1 collisions?

 Rebrand symmetric cryptography as Pre-shared-key two-party blockchain?
Cryptocurrencies are getting all the attention, and stealing the crypto name...

What can we do?

Become cryptoanalysts?

Use this computation for science?
  ▶ Verify that SHA-256 is not biased?
  ▶ Create new coin based on SHA-1 collisions?

Rebrand symmetric cryptography as Pre-shared-key two-party blockchain?
Taking crypto back

- Cryptocurrencies are getting all the attention, and stealing the crypto name...
- What can we do?
- Become cryptoanalysts?
- Use this computation for science?
  - Verify that SHA-256 is not biased?
  - Create new coin based on SHA-1 collisions?
- Rebrand symmetric cryptography as Pre-shared-key two-party blockchain?
Best Paper Award

Key-Recovery Attacks on Full Kravatte

Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jian Guo, Jérémy Jean, Jean-René Reinhard and Ling Song
Announcement of the CAESAR finalists

Daniel J. Bernstein
CAESAR timeline planned in 2012

2013.01: Announce “tentative schedule”.
2014.01: Deadline for first-round submissions.
2015.01: Announce second-round candidates.
2016.01: Announce third-round candidates.
2017.01: Announce finalists.
2018.01: Announce final portfolio.

...but all sides requested extra time.
...and all sides requested an extra feedback loop between submitters and committee members.

Announcement of the CAESAR finalists Daniel J. Bernstein
CAESAR timeline planned in 2012

2013.01: Announce “tentative schedule”.
2014.01: Deadline for first-round submissions.
2015.01: Announce second-round candidates.
2016.01: Announce third-round candidates.
2017.01: Announce finalists.
2018.01: Announce final portfolio.

... but all sides requested extra time.
... and all sides requested an extra feedback loop between submitters and committee members.
Actual CAESAR timeline

2013.01: Announce “tentative schedule”.
2014.03: Deadline for first-round submissions.
2015.07: Announce second-round candidates.
2016.08: Announce third-round candidates.
2018.03: Announce finalists.
Later: Announce final portfolio.
Use Case 1: Lightweight applications (resource constrained environments)

- **critical**: fits into small hardware area and/or small code for 8-bit CPUs
- **desirable**: natural ability to protect against side-channel attacks
- **desirable**: hardware performance, especially energy/bit
- **desirable**: speed on 8-bit CPUs
- **message sizes**: usually short (can be under 16 bytes), sometimes longer
Use Case 2: High-performance applications

- critical: efficiency on 64-bit CPUs (servers) and/or dedicated hardware
- desirable: efficiency on 32-bit CPUs (small smartphones)
- desirable: constant time when the message length is constant
- message sizes: usually long (more than 1024 bytes), sometimes shorter
Use case 3: Defense in depth

- critical: authenticity despite nonce misuse
- desirable: limited privacy damage from nonce misuse
- desirable: authenticity despite release of unverified plaintexts
- desirable: limited privacy damage from release of unverified plaintexts
- desirable: robustness in more scenarios; e.g., huge amounts of data
An important caveat

“The submitter/submitters understand that the selection of some algorithms is not a negative comment regarding other algorithms, and that an excellent algorithm might fail to be selected simply because not enough analysis was available at the time of the committee decision.”
The CAESAR finalists

Announcement of the CAESAR finalists

Daniel J. Bernstein
The CAESAR finalists

- ACORN for use case 1.
- AEGIS for use case 2. However, if AEGIS is selected for the final portfolio, one of AEGIS-128 and AEGIS-128L will be dropped, by default AEGIS-128L.
- Ascon for use case 1.
- COLM for use case 3.
- Deoxys-II for use case 3.
- MORUS for use case 2.
- OCB for use case 2.

Last chance for analysis before the final portfolio!
The Rump Session PC report

Joan Daemen & Pierre Karpman
Submission statistics

- Received **327** submissions
- A new record for a rump session?
- All reviewed looked-at by at least one chair
- We selected **14** papers, plus two invited talks
Submissions by country

100%

Belgium
Accepted papers by country

100 %

Belgium
Accepted papers by country

Well done!
(Much better than the Winter Olympics)
Now time for the prizes!

Brought to you by the Prize Committee:

Christina Boura, Shiho Moriai, Yu Sasaki & Martijn Stam
Now time for the prizes!

• Grand ToCS Prize for the most entertaining talk, awarded to Anne Canteaut

• De Cannière/Mendel Award for the fanciest slides, including Tikz pictures and special effects, awarded to Gregor Leander

• Intel Prize for the presentation revealing the weakness that requires most urgent immediate real-world intervention, not awarded this year :( 

• Desmedt Trophy for the best dance moves/fancy footwork/X factor, awarded to Aleksei Udovenko

• ToCS Rump Recognition Memorial for the presentation-that-everyone-thought-would-be-boring-but-you-managed-to-make-it-funny,-well-done!, awarded to Carlos Cid