Welcome to the FSE 2024 Rump Session

Gaëtan Leurent and Bart Mennink

Fast Software Encryption 2024

March 26, 2024

Start of the Rump Session

Rules

- We allowed boring talks of 1-4 minutes, funny talks of 1-5 minutes
- Bonus minute if the MD5 or SHA-1 of the PDF ends with "`f5e2024`"
- Presenters exceeding their time may face annoying interruption by us
- Program is online: `https://fse.iacr.org/2024/rumpsession.php`

Start of the Rump Session

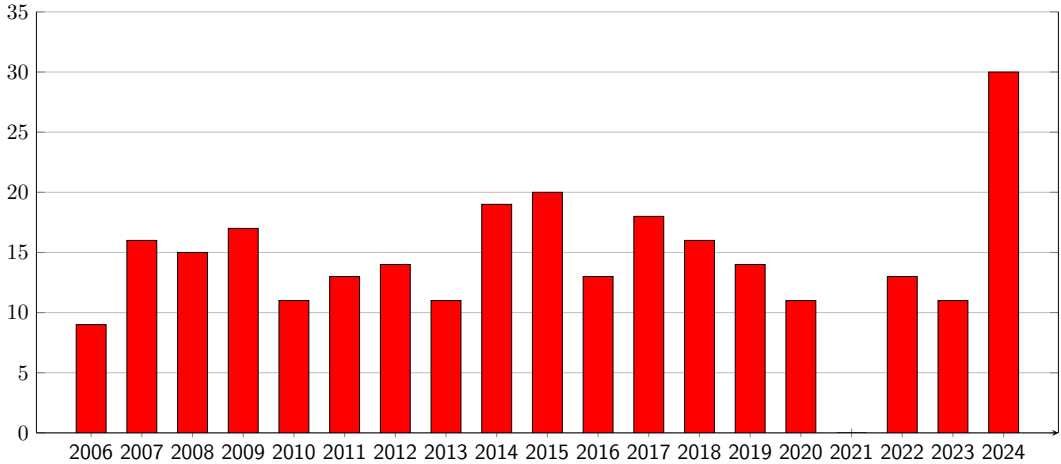
Rules

- We allowed boring talks of 1-4 minutes, funny talks of 1-5 minutes
- Bonus minute if the MD5 or SHA-1 of the PDF ends with "`f5e2024`"
- Presenters exceeding their time may face annoying interruption by us
- Program is online: `https://fse.iacr.org/2024/rumpsession.php`

Prizes

- Best rump talk award!
- Double "`f5e2024`" preimage award!

Statistics


35
30
25
20
15
10
5
0
2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024

There Will Be a Quizzzzzz

- Each rump talk will be preceded by a quiz question
- Everyone can participate!
- You can enter your solutions here:
  `https://u1.survey.science.ru.nl/index.php/233224?lang=en`
- Time you get for each question? Depends on the time the speaker needs to get on stage!
- Last question in survey:
  vote for best rump session talk!

Prize for the best participant!

Useful Information for the Quiz

Capital and largest city	Brussels 50°51′N 4°21′E
Official languages	Dutch • French • German
Ethnic groups (2022[1])	66.6% Belgians 33.4% other
Religion (2020[2])	63.7% Christianity ├ 60.6% Catholicism └ 3.1% other Christian 28.0% no religion 7.4% Islam 0.9% other
Demonym(s)	Belgian
Government	Federal parliamentary constitutional monarchy[3]
• Monarch	Philippe
• Prime Minister	Alexander De Croo
Legislature	Federal Parliament
• Upper house	Senate
• Lower house	Chamber of Representatives
Independence from the Netherlands	
• Declared	4 October 1830
• Recognized	19 April 1839
Area	
• Total	30,689[4][5] km^2 (11,849 sq mi) (136th)
• Water (%)	0.71 (2015)[6]
Population	
• 2023 estimate	▲ 11,697,557[7] (82nd)
• Density	376/km^2 (973.8/sq mi) (22nd)

Useful Information for the Quiz

- Belgium is obviously a ChatGPT hallucination of an average European country.
  - Known for comics and chocolate

Useful Information for the Quiz

- Belgium is obviously a ChatGPT hallucination of an average European country.
  - Known for comics and chocolate
  - Standard European coat of arms

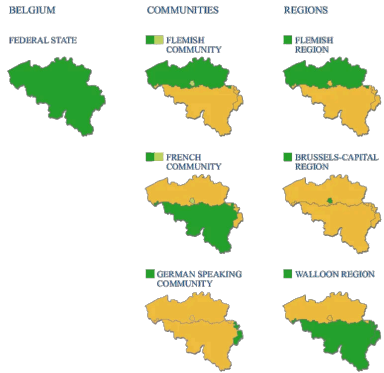
Useful Information for the Quiz

- Belgium is obviously a ChatGPT hallucination of an average European country.
  - Known for comics and chocolate
  - Standard European coat of arms
  - Motto: "Unity makes strength"

Useful Information for the Quiz

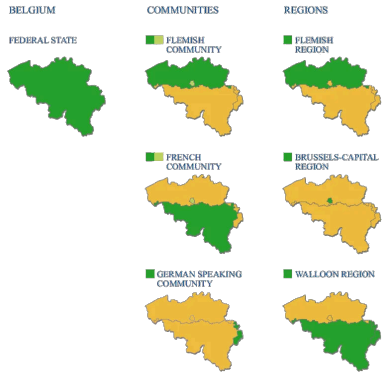
- Belgium is obviously a ChatGPT hallucination of an average European country.
  - Known for comics and chocolate
  - Standard European coat of arms
  - Motto: "Unity makes strength"
  - Speaks French, Dutch and German

Useful Information for the Quiz



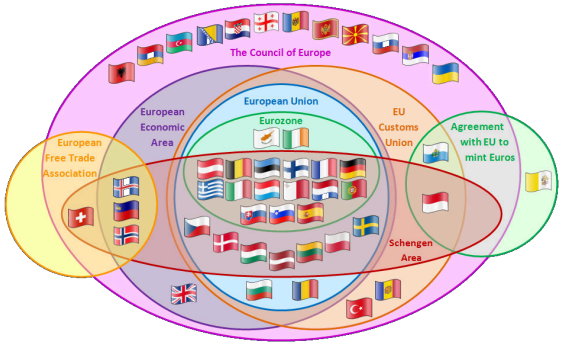
- Belgium is obviously a ChatGPT hallucination of an average European country.
  - Known for comics and chocolate
  - Standard European coat of arms
  - Motto: "Unity makes strength"
  - Speaks French, Dutch and German
  - 3 communities, 3 regions, 7 governments?

Useful Information for the Quiz



- Belgium is obviously a ChatGPT hallucination of an average European country.
  - Known for comics and chocolate
  - Standard European coat of arms
  - Motto: "Unity makes strength"
  - Speaks French, Dutch and German
  - 3 communities, 3 regions, 7 governments?
  - 541 days without government?

Useful Information for the Quiz



- Belgium is obviously a ChatGPT hallucination of an average European country.
  - Known for comics and chocolate
  - Standard European coat of arms
  - Motto: "Unity makes strength"
  - Speaks French, Dutch and German
  - 3 communities, 3 regions, 7 governments?
  - 541 days without government?
  - Brussels capital of Europe?

More Useful Information for the Quiz

- Leuven is a beautiful medieval city
- In 1969 they started building a cheap copy: *Louvain-la-Neuve*
- Both cities have their own *Catholic University of Leuven*

Quiz Question 1

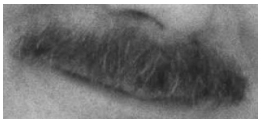
Which of these is *not* Belgian?

A

B

C

D



Next Talk:
Program Chair Report

Program Chair Report

Christina Boura, **Kazuhiko Minematsu**
ToSC Co-Editors-in-Chief

IACR Transactions on Symmetric Cryptology

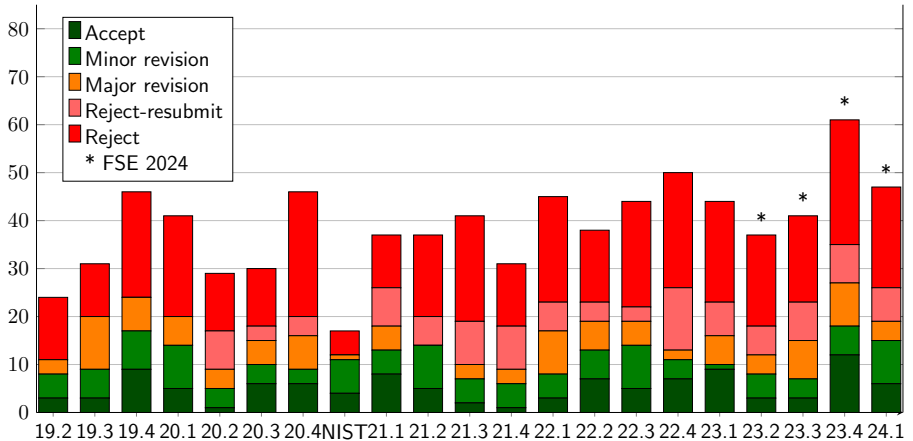
- **FSE follows a hybrid journal/conference model since 2016**
  - Open access journal: IACR ToSC
  - Published by Ruhr University Bochum
  - Indexed by Scopus, DOAJ
  - Selected for inclusion in the Web of Science
- **4 issues per year**
  - Deadline every 3 months
  - Decision after 2 months (for regular papers)
- **Rebuttal phase**
- **Journal-style decisions**
  - Accept
  - Minor revision (conditional accept with shepherd)
  - Major revision (can resubmit to the next two cycles)
  - Reject-and-resubmit (can resubmit after two cycles)
  - Reject (cannot resubmit in the next two cycles)
- Also: Systematization of Knowledge (SoK), addendum, and corrigendum papers

FSE 2024 Program

- 48 papers from ToSC 2023(2-4), and 2024(1)
- 2 Invited talks: Maria Eichlseder and Gaëtan Leurent


- Rump Session Chairs: Gaëtan Leurent and Bart Mennink

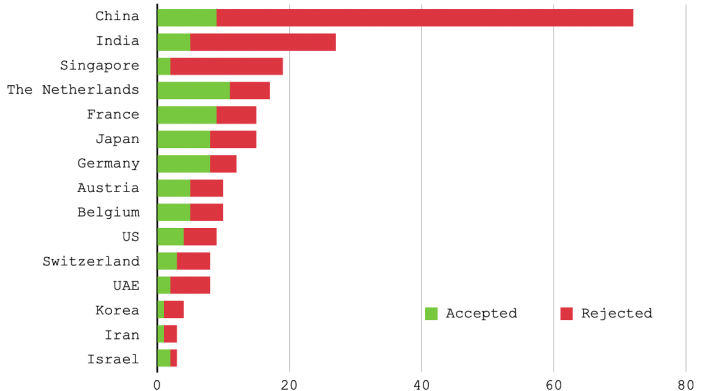

Decision Statistics



Decision Statistics for ToSC 2023(2-4), and 2024(1)

- 175 regular submissions
  - **27.4%** accepted (48 papers)
  - Previous years: 2023 (26%), 2022 (27%)
- Major revision papers often return to ToSC.
  - 25 major revision decisions given
  - 25 major revisions resubmitted (among them **16** were accepted)
- Around 1/2 of reject-and-resubmit (R&R) papers **return** to ToSC, but . . . **rarely get accepted**.
  - 29 R&R decisions given
  - 16 R&R resubmitted (among them **2** were accepted and **2** received a major revision decision)
- SoK/addendum/corrigendum: only 1/0/0 submissions (1/0/0 accepted)

Statistics Per Country



- Submissions from **29** countries (accepted papers from **19** countries).

A Novelty for FSE 2024

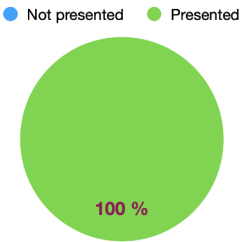
From the FSE 2024 Call for Papers

Presentation of accepted papers is **only possible in person for authors physically attending FSE 2024**. Presentation of accepted papers is highly encouraged.

A Novelty for FSE 2024

From the FSE 2024 Call for Papers

Presentation of accepted papers is **only possible in person for authors physically attending FSE 2024**. Presentation of accepted papers is highly encouraged.



- 100% of the papers will be presented in person at FSE 2024!

Program Committee (2023)

- Nasour Bagheri
- Zhenzhen Bao
- Xavier Bonnetain
- Anne Canteaut
- Wonseok Choi
- Carlos Cid
- Benoît Cogliati
- Patrick Derbez
- Itai Dinur
- Orr Dunkelman
- Avijit Dutta
- Maria Eichlseder
- Patrick Felke
- Antonio Flórez-Gutiérrez
- Lorenzo Grassi
- Chun Guo
- Akinori Hosoyamada
- Ryoma Ito
- Tetsu Iwata
- Ashwin Jha
- Thomas Johansson
- Mustafa Khairallah
- Virginie Lallemand
- Fukang Liu
- Yunwen Liu
- Kalikinkar Mandal
- Silvia Mella
- Florian Mendel
- Bart Mennink
- Yusuke Naito
- Thomas Peyrin
- Shahram Rasoolzadeh
- Francesco Regazzoni
- Raghvendra Rohit
- Yann Rotella
- Dhiman Saha
- Santanu Sarkar
- Yu Sasaki
- André Schrottenloher
- Yannick Seurin
- Meltem Sönmez Turan
- François-Xavier Standaert
- Ling Sun
- Siwei Sun
- Tyge Tiessen
- Yosuke Todo
- Aleksei Udovenko
- Damian Vizár
- Lei Wang
- Qingju Wang

Thank You

- **Managing co-editors**: Gregor Leander, Christof Beierle
- **Technical support**: Linda Groß
- **Submission system**: Kevin McCurley

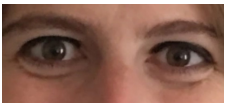
- **General co-chairs** : Svetla Petkova-Nikova, Siemen Dhooghe
- **Virtual conference organizers**: Kevin McCurley, Kay McKelly
- **FSE steering committee**:
  - Christina Boura
  - Christoph Dobraunig
  - Orr Dunkelman (chair)
  - Maria Eichlseder
  - Gregor Leander (IACR Board representative)
  - Gaëtan Leurent
  - Bart Mennink
  - Kazuhiko Minematsu
  - Bart Preneel
  - Yu Sasaki
  - Ling Song
  - Siwei Sun

Quiz Question 2

Who of the following four persons has served as both general chair and program chair of FSE?

A

B



C

D

Next Talk:
Award Ceremony

FSE 2024
Best Paper Award

Gregor Leander, Shahram Rasoolzadeh, and Lukas Stennes

Cryptanalysis of HALFLOOP Block Ciphers: Destroying HALFLOOP-24

Christina Boura and Kazuhiko Minematsu
Program Co-Chairs

FSE 2024
Best Paper Award

Aurélien Boeuf, Anne Canteaut, and Léo Perrin

Propagation of Subspaces in Primitives with Monomial Sboxes: Applications to Rescue and Variants of the AES

Christina Boura and Kazuhiko Minematsu
Program Co-Chairs

FSE 2024
Test of Time Award

Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen

The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl

Published at FSE 2009

Gaëtan Leurent, chair of the Test-of-Time award committee

The International Association For Cryptologic Research Gratefully Acknowledges

Christina Boura

For her contribution to the worldwide cryptologic community through her role as Editor-in-Chief of the IACR Transactions on Symmetric Cryptology in 2024.

Orr Dunkelman, chair of the FSE steering committee

The International Association For Cryptologic Research Gratefully Acknowledges

Kazuhiko Minematsu

For his contribution to the worldwide cryptologic community through his role as Editor-in-Chief of the IACR Transactions on Symmetric Cryptology in 2024.

Orr Dunkelman, chair of the FSE steering committee

The International Association For Cryptologic Research Gratefully Acknowledges

Svetla Petkova-Nikova

For her contribution to the worldwide cryptologic community through her role as General Chair of FSE 2024

Orr Dunkelman, chair of the FSE steering committee

The International Association For Cryptologic Research Gratefully Acknowledges

Siemen Dhooghe

For his contribution to the worldwide cryptologic community through his role as General Chair of FSE 2024

Orr Dunkelman, chair of the FSE steering committee

Call for Proposals

- Ever wanted to give back to the community?

Call for Proposals

- Ever wanted to give back to the community?
- Do you want to show everyone how great is country/city/university?

Call for Proposals

- Ever wanted to give back to the community?
- Do you want to show everyone how great is country/city/university?
- Are you envy of the General Chairs for their cool plaques?

Call for Proposals

- Ever wanted to give back to the community?
- Do you want to show everyone how great is country/city/university?
- Are you envy of the General Chairs for their cool plaques?
- Want to find out new cool acronyms like GC, PC, SC?

Call for Proposals

- Ever wanted to give back to the community?
- Do you want to show everyone how great is country/city/university?
- Are you envy of the General Chairs for their cool plaques?
- Want to find out new cool acronyms like GC, PC, SC?
- Do you feel you sleep too much and work too little?

FSE 2026 Proposals

- The FSE steering committee would like to encourage you to consider organizing FSE 2026!
- More info:
  - IACR website (rules for GC)
  - Talk with any FSE SC member

Quiz Question 3

Which Wang has most publications at FSE?

A

Meiqin

B

Lei

C

Wei

D

Xiaoyun

Next Talk:
ROME for FSE 2025

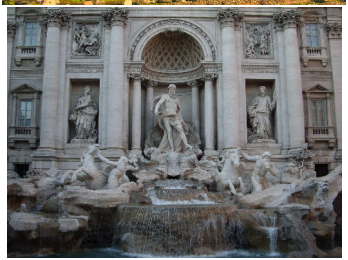
ROME for FSE 2025

General Co-Chairs: Marco Pedicini & Lorenzo Grassi
Program Co-Chairs: Kazuhiko Minematsu & Christoph Dobraunig

https://fse.iacr.org/2025/

17 - 21 March 2025 (Tentative)

About Rome



- *13 UNESCO World Heritage Sites*:

  Colosseum, Pantheon, Roman Forum and Palatine Hill, Trevi Fountain, Navona Square, and many others!

- *Vatican City*:

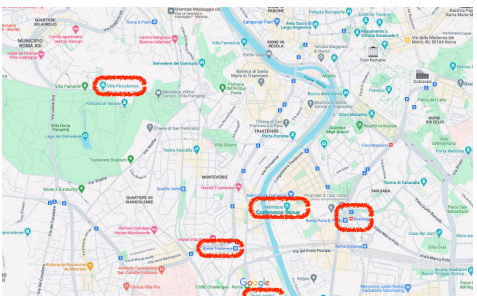
  St. Peter's Basilica, Vatican Museum, Sistine Chapel, and more!

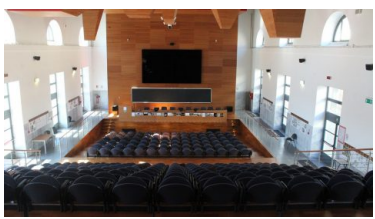
About Rome

- Thousand-year history
- Many accommodation options
- Modern infrastructure
- Amazing food!

Conference Venue

- Roma Tre University (architecture department): Plenary room for 200 - 250 participants
- Close to city center
- Excellent facilities for coffee breaks and lunches





Conference Dinner (Tentative)

- *Conference dinner* at **Villa Piccolomini**, with amazing view on the Vatican city.
- Great opportunity to taste Italian food!

See You in Rome in 2025!

Important: **JUBILEE 2025!**

Do **not** wait until the last to book your hotel!

Quiz Question 4

Which cryptographic competition ran for the longest time?

A The AES competition

B The SHA-3 competition

C The CAESAR competition

D The Snake Oil Crypto competition

Next Talk:
Freewheeling to FSE

Radboud University

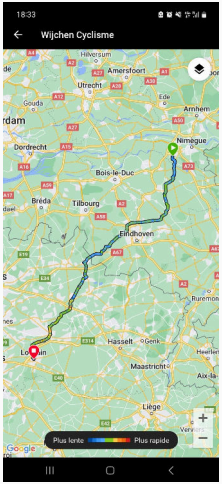
Freewheeling to FSE

Yanis Belkheyar, Charlotte Lefevre
Radboud University (The Netherlands)

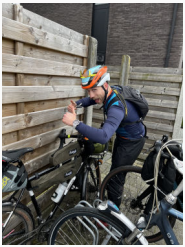
FSE rump session

26 March 2024

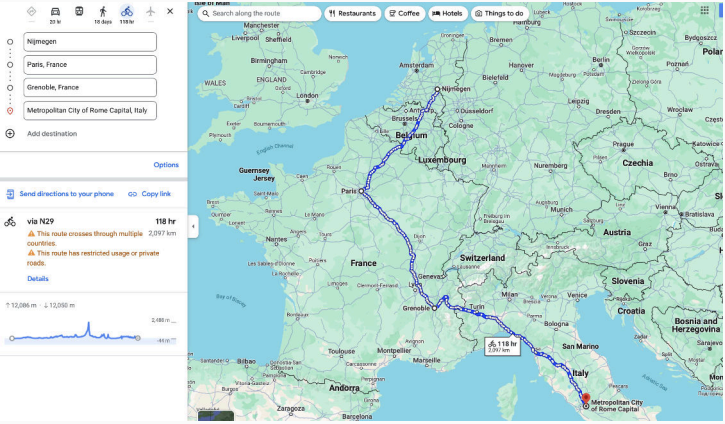
From Nijmegen to Leuven



Local wildlife



Hopefully next year



Hope to see many of you![1]

[1] non-contractual itinerary, total km may vary ($\pm$ 500 km)

Quiz Question 5

Which Big Bang Theory Actor is born in Belgium?

A 

B 

C 

D 

Next Talk:
It Takes Me 8 Years to Attend a Full FSE

Xiamen University

It Takes Me 8 Years to Attend a Full FSE

Yaobin Shen

March 26, FSE 2024 Rump Session @Leuven

The Beginning of My Career

- Phd student at SJTU(2016-2021)
  - 2016 -> no paper
  - 2017 -> no paper
  - 2018 -> no paper
  - 2019 -> one paper at ToSC 2019 (2)
  - 2020 -> one paper at ToSC 2020 (1)
  - 2021 -> no paper (no FSE 2021 neither)

virtual FSE 2020

During my Post-doc at Belgium

- Post-doc at UCLouvain (what’ s the difference between UC Louvain and KU Leuven?)
  - 2022 -> no paper (FSE 2022 was a hybrid event)
  - 2023 -> one paper (but FSE 2023 was separated in two locations…)
  - 2024 -> one paper (the first full FSE I attend in person!)

Thanks

Quiz Question 6

Who was occupied at the time of receiving their best paper award?

A Bart Mennink

B Colin Chaigneau

C Orr Dunkelman

D Colin Chataigneau

Next Talk:
Optimizing Quantum Search-based Cryptanalysis through Quantum State Preparation

KOREA UNIVERSITY

Cryptographic Algorithm Laboratory

Optimizing Quantum Search-based Cryptanalysis through Quantum State Preparation

Dongjae Lee[1], Hanbeom Shin, Insung Kim, Seokhie Hong

[1]ldj0676@korea.ac.kr

26 March

FSE 2024 - Rump session

Grover Search / Quantum Amplitude Amplification

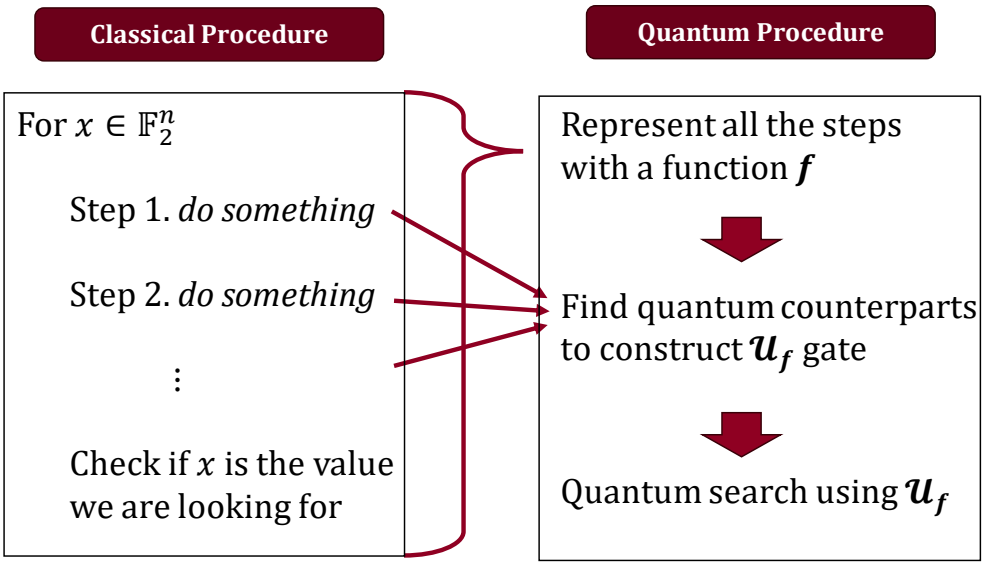
Given $f: \{0,1\}^n \rightarrow \{0,1\}$,

find x such that $f(x) = 1$

Classical	Quantum
$O(2^n)$	$O(2^{n/2})$

Quadratic Speedup !

A Structure in Quantum Cryptanalysis



A Slightly More Complex Structure

For $x \in \mathbb{F}_2^{\boldsymbol{n}}$
  If $g(x) = 0$
    then continue
  For $y \in \mathbb{F}_2^{\boldsymbol{m}}$
    do something
      ⋮
    check x, y

$$p \coloneqq \Pr[g(x) \neq 0]$$

Classical	Quantum
$O(p2^{n+m})$	$O(2^{(n+m)/2})$

Illustrative Example

For $(\Delta x, \Delta y)$

Solve S-box diff. eq.

If no such solution

then continue

⋮

For $i = 1,2, \ldots$

do something with i-th solution

⋮

Recovering the Quadratic Speedup

For $x \in X \coloneqq \{x : g(x) \neq 0\}$

  For $y \in \mathbb{F}_2^{\boldsymbol{m}}$

    do something

    $\vdots$

    check x, y

Classical	Quantum
$O(p2^{n+m})$	$O(\sqrt{p}2^{(n+m)/2})$

The only remaining task is..

Constructing Quantum State

$$|\psi\rangle = \sum_{x \in X} \frac{1}{\sqrt{|X|}} |x\rangle$$

at negligible cost
compared to $|\boldsymbol{U_f}|$

=

A method to construct
an arbitrary quantum state

Q&A

Thanks

KOREA UNIVERSITY

Cryptographic Algorithm Laboratory

Quiz Question 7

In which city has FSE *not* taken place?

A

B

C

D

Next Talk:
The 19th International Workshop on Security

IWSEC 2024

- Kyoto International Conference Center, Japan

Important Dates

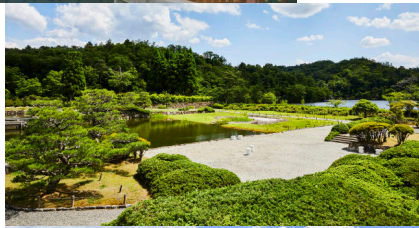
- Submission: April 16, 2024 (23:59 UTC)
- Notification: June 20, 2024
- Conference: September 17-19, 2024

Access

Kyoto Sta. (京都駅) → 20 min. → ICC Sta. (国際会館駅) → 5 min.

Other Important Notices

- PCCs: Kazuhiko Minematsu, Mamoru Mimura
- 3 keynote talks (to be announced soon)
- An excursion (to be announced soon)



https://www.icckyoto.or.jp/brochures-media/image-gallery/

Quiz Question 8

Which painting is *not* Belgian?

A

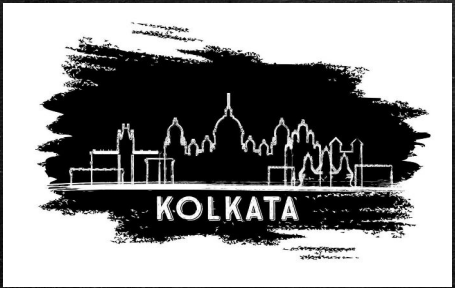
B

C

Next Talk:
ASK 2024

ASK 2024

The 11th Asian-workshop on Symmetric Key Cryptography



- Date: Dec 14 – Dec 17, 2024 (tentative)
- Venue: Kolkata, India

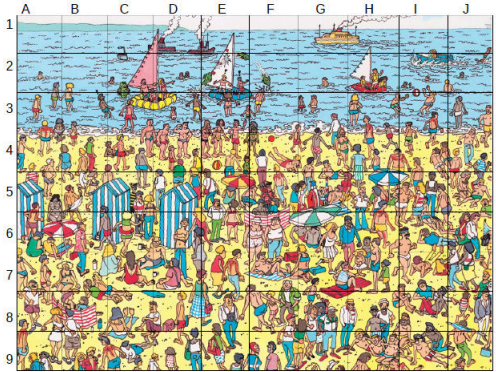
Associated Events	Date	Venue
ASIACRYPT 2024	Dec 09 – Dec 13	Kolkata, India
INDOCRYPT 2024	Dec 18 – Dec 21	Chennai, India

Contact: Mridul Nandi, ISI Kolkata (mridul.nandi@gmail.com)

Somitra Sanadhya, IIT Jodhpur (somitra@iitj.ac.in)

Quiz Question 9

Where is Waldo?



A Row 2

B Row 5

C Row 7

D Row 8

Next Talk (after the break):
A Practical Colliding Message Pair for 31-Step SHA-256

A Practical Colliding Message Pair for 31-Step SHA-256

Yingxin Li[1], Fukang Liu[2], Gaoli Wang[1], Xiaoyang Dong[3], Siwei Sun[4]

[1]East China Normal University, Shanghai, China
[2]Tokyo Institute of Technology, Tokyo, Japan
[3]Tsinghua University, Beijing, China
[4]University of Chinese Academy of Sciences, Beijing, China

FSE 2024, Rump Session

SHA-256

- A well-known hash function standardized by NIST
- Widely deployed in real-world applications
- A famous application: Bitcoin

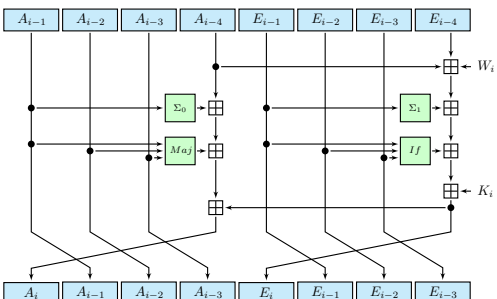


Figure: The round function of SHA-256

Progress on the Analysis of SHA-256

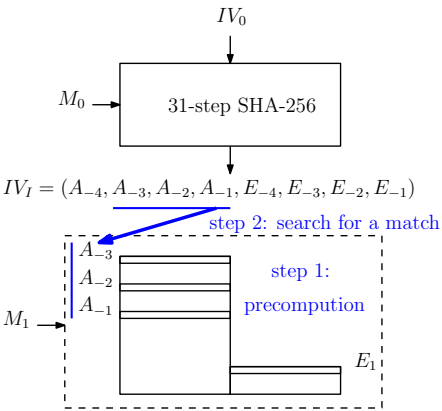
Progress on collision attacks on SHA-256:

- FSE 2006: 18 steps (practical)
- FSE 2008: 21 steps (practical)
- SAC 2008: 23 & 24 steps (practical)
- Asiacrypt 2011: 27 steps (practical)
- Eurocrypt 2013: 28 steps (practical)
- Eurocrypt 2013: 31 steps (time: $2^{65.5}$, memory: 2^{34})
- Eurocrypt 2024: 31 steps (time: $2^{49.8}$, memory: 2^{48})

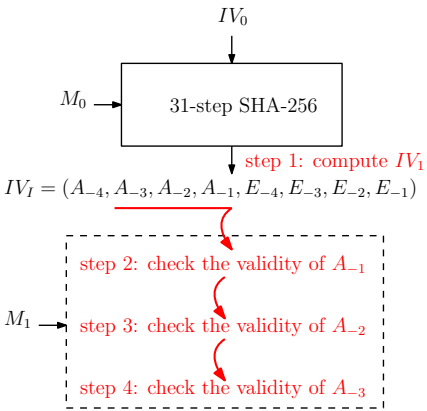
We are close to a practical collision attack on 31-step SHA-256 and the current bottleneck is the memory complexity!!!

New Results

- Find a memory-efficient collision attack on 31-step SHA-256



Mendel et al.'s MITM technique



Our new technique

New Results

- Obtain a colliding message pair in about 43 hours with 560 threads (negligible memory)

Table: The first colliding message pair (M_0, M_1) and (M_0, M_1') for 31-step SHA-256

M_0	c32aef52	512294ba	9db5ed8c	8c8c88ed	b2de2765	63a2d14e	ec7619cc	93b21182
	e5050f50	f0839b60	7b1ee176	aaa06d68	c462343c	67898962	9558f495	04281f2c
M_1	5d0f5ae6	05e98311	8fa3c73a	9af8c49d	a2bf31f7	de547b67	5baecee3	da0d8c94
	e4c19564	f682d45c	f7c57698	f871f9b5	f14469b7	fc28eb0c	2d76db75	043fe071
M_1'	5d0f5ae6	05e98311	8fa3c73a	9af8c49d	a2bf31f7	de548b61	5b8e46f2	8a1dd69a
	bcc08464	f6825458	f7c57698	f871f9b5	f14469b7	fc28eb0c	2d76db75	043fe071
hash	8557667d	6515fe6d	f8323458	015998c3	32bbd7cc	0c9e12b8	c1fcfb7a	1a81a47a

More details will be soon published on eprint.

Quiz Question 10

Who is the true Itai Dinur?

A

B

C

Next Talk:
Algebraic Hashes Initiative

Algebraic Hashes Initiative

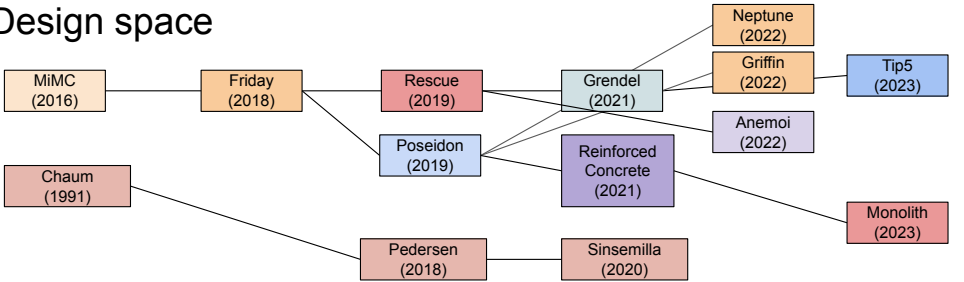
Dmitry Khovratovich, Ethereum Foundation

New hash designs

With development of Incrementally Verifable Computation (IVC), we need hash functions that are efficient in circuits (have good arithmetization):

- Merkle tree opening proofs
- Fiat-Shamir-transformed protocols
- Compression in recursive SNARKs
- Provenance proofs

Design space



We need more confidence in these functions

Algebraic Hashes Initiative: step 1

Bounties:

- Build on 2021-22 bounty program
- Craft reduced versions of most interesting schemes
- Award growing with target strength and supplementary material

Feedback needed:

- Give us weakened versions
- Any fairness issue
- Comments on rules

Algebraic Hashes Initiative: step 2

Research wishlist:

- Interest in a wide class of papers (Groebner basis, heavily modified variants, incremental results) that are often rejected from conferences due to (somewhat) low contribution.

Feedback needed:

- Suggestions

Other steps

Special Journal Editions?

Extra entries in calls for papers?

Quiz Question 11

Which comic figure is *not* born in Belgium?

A 

B 

C 

D 

Next Talk:
A N00b's take on presenting

A N00b’s take on prezzz….

Erik Takke

1 – 3 – 5

$$x = 5$$

1 – 3 – 5

$f(x) = x^3 + 7x + 99$

$P \neq NP$

$F(x) = d/dx\ r*m/g + 2*m*a$

One more random formula!

$C_{u,v} = \sum_i C_{u,i} * C_{i,v}$

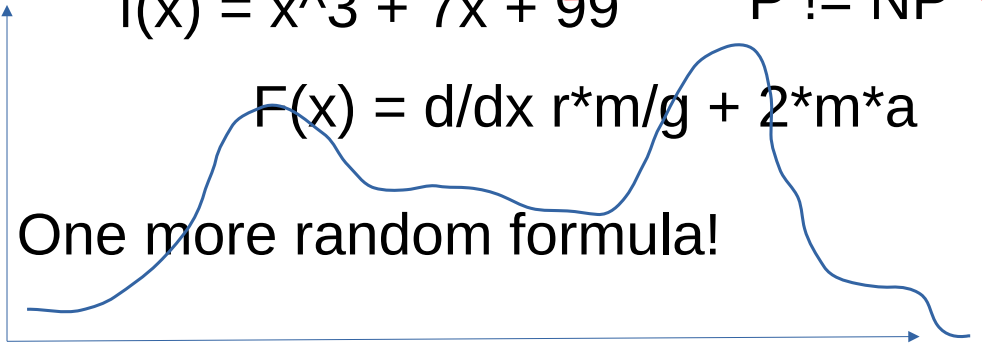
$P = NP$

$f(x) = x^3 + 7x + 99$

$P \neq NP$

$F(x) = d/dx\ r*m/g + 2*m*a$

One more random formula!

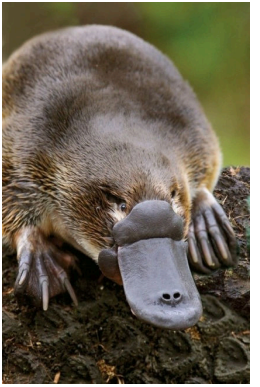


$C_{u,v} = \sum_i C_{u,i} * C_{i,v}$

$P = NP$

1] Takke, E, On the sleeping patterns of PhD's, 2023
2] Ali, M. How to knock oneself out. 2017

My favorite animal

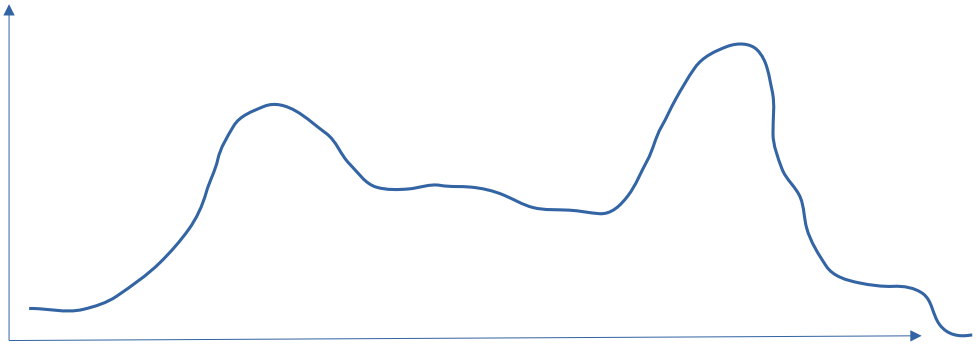


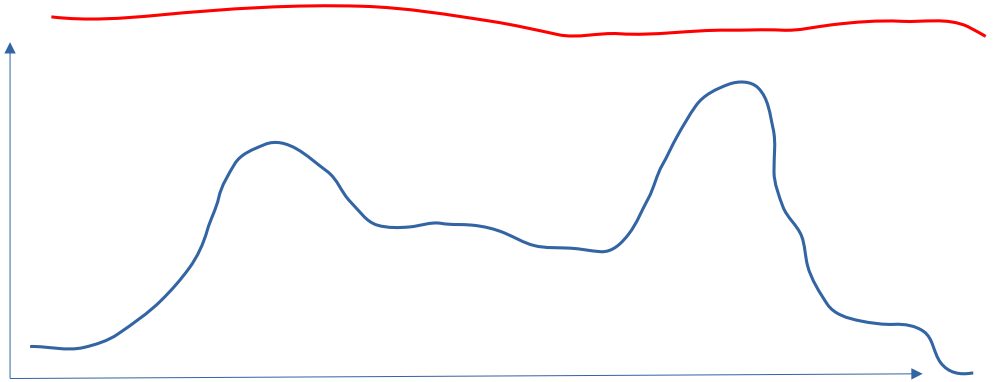
I love Platypuses!

1 – 3 – 5

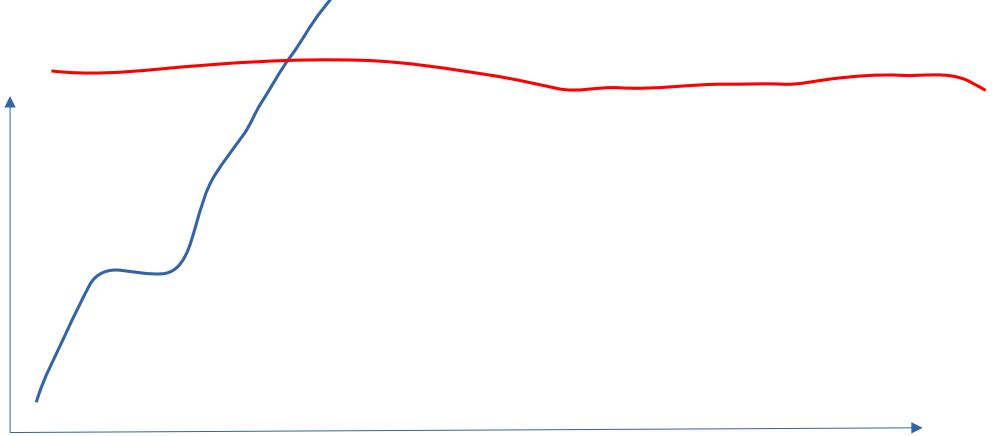
My favorite animals

- Platypuses
  - Are super awesome!
  - Have webbed feet
- Armadillos
  - Slightly less awesome
  - Much more scaly
    - Tough as nails!
- Hippopotamus!
  - Veggie eaters
- Rhino
  - Big horn
  - Looks so funny!
- Elephants
  - Sounds really cool



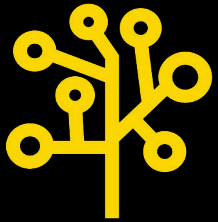


1 – 3 – 5



1 – 3 – 5

Good luck!



3MI LABS

Quiz Question 12

Suppose I eat Américain préparé with French fries and Brussels sprouts, with a glass of La Trappe trappist beer on the side. Which of these four is *not* Belgian?

A 

B 

C 

D 

Next Talk:
On the DC/LC Equivalence Classes of BOGI based Ciphers

KOREA UNIVERSITY

Cryptographic Algorithm Laboratory

On the DC/LC- Equivalence Classes of BOGI-based Ciphers
(work in progress)

Insung Kim, Seonggyeom Kim, Hanbeom Shin, Dongjae Lee, Seokhie Hong

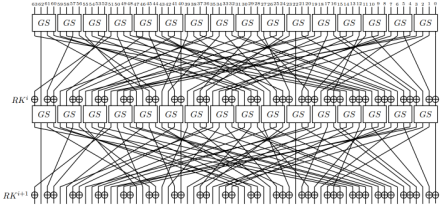
FSE 2024-Rump Session

2024.03.26

Introduction

BOGI-based Ciphers

- Bad Output must go to Good Input
- Well-known as a `GIFT`-variant
- In 2022, Kim et al. discovered the most resistant BOGI-64 against statistical attacks



[GIFT-64]

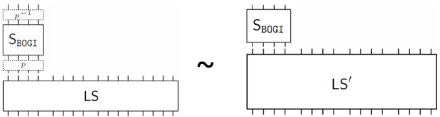
Our contributions

- The proof of the existence of a larger DC/LC-equivalence class for BOGI-based ciphers than previously known
- Ongoing work : Searching of the most resistant BOGI-based cipher against statistical attacks

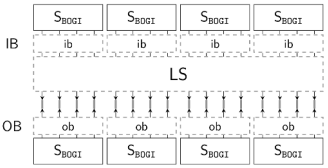
DC/LC-equivalence classes of BOGI-based ciphers

The state-of-the-art DC/LC-equivalence classes of BOGI-based ciphers are as follows

- **The number of 4-bit optimal BOGI-applicable S-boxes : 2,654,208**
  - Reduction through DDT/absLAT-Equivalence : 2,654,208 → 10,368
- **The number of Latin Square : 576**



  - Reduction through LS-equivalence : 576 → 24
- **The number of considered {S, (ib, ob)} combinations : 10,368 × 96**
  - For optimal BOGI-applicable S-boxes, there exist 96 (ib, ob) pairs for each S-box
  - {S, (ib, ob)} is linearly equivalent to {S, (id, id)} : 10,368 × 96 → 1,728



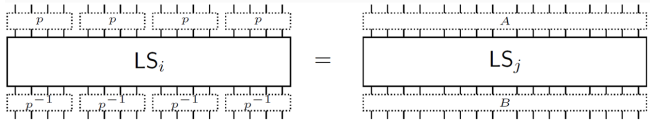
[Decomposition of the Mixing Layer in BOGI Logic]

→ The final number of combinations of {S, (id, id)} that must to be considered is 1,728 × 24 = **41,472**

Basic Properties for Proof

Let p be a 4-bit permutation and let A and B be word-wise permutations.

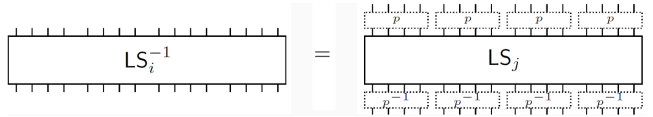
- **[Property 1] :** Each (LS_i, p) can be represented by 24 $(\mathrm{LS}_j, \mathrm{A}, \mathrm{B})$ such that $(p^{-1}||p^{-1}||p^{-1}||p^{-1}) \circ \mathrm{LS}_i \circ (p||p||p||p) = \mathrm{B} \circ \mathrm{LS}_j \circ \mathrm{A}$



- **[Property 2] :** Each $(\mathrm{LS}_j, \mathrm{A}, \mathrm{B})$ can be represented by only one (LS_i, p) such that

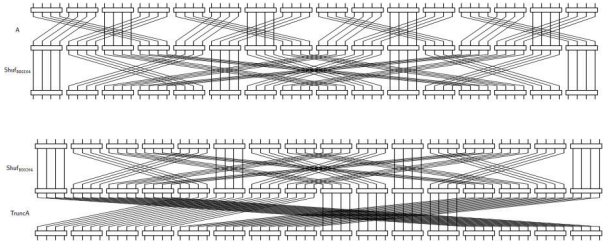
$$\mathrm{B} \circ \mathrm{LS}_j \circ \mathrm{A} = (p^{-1}||p^{-1}||p^{-1}||p^{-1}) \circ \mathrm{LS}_i \circ (p||p||p||p)$$

- **[Property 3] :** Each LS_i^{-1} can be represented by only one (LS_j, p) such that $(p^{-1}||p^{-1}||p^{-1}||p^{-1}) \circ \mathrm{LS}_j \circ (p||p||p||p) = \mathrm{LS}_i^{-1}$



Basic Properties for Proof

- **[Property 4] :** $\mathrm{Shuf}_{64} \circ (\mathrm{A}||\mathrm{A}||\mathrm{A}||\mathrm{A}) = \mathrm{Trunc}(\mathrm{A}, 4) \circ \mathrm{Shuf}_{64}$ and $(\mathrm{A}||\mathrm{A}||\mathrm{A}||\mathrm{A}) \circ \mathrm{Shuf}_{64} = \mathrm{Shuf}_{64} \circ \mathrm{Trunc}(\mathrm{A}, 4)$



- **[Property 5] :** $\mathrm{LS} \circ \mathrm{Trunc}(\mathrm{A}, 4) = \mathrm{Trunc}(\mathrm{A}, 4) \circ \mathrm{LS}$

- **[Property 6] :** For each LS, there exist word-wise permutations C_i such that satisfy the following conditions
  - $\mathrm{LS} \circ \mathrm{C}_i = \mathrm{C}_{i+1} \circ \mathrm{LS}, \quad i = 0,1, \ldots n-1$
  - $\mathrm{C}_0 \circ \mathrm{LS} = \mathrm{LS} \circ \mathrm{C}_n$

Our Main Idea

- The best trail search result for LS, $A^{-1} \circ A \circ LS$ is the same ➔ Reducible by a multiple of 24
  - $\{S, LS, Shuf_{64}\} \sim_{eq} \{S, LS \circ C, Shuf_{64}\} \sim_{eq} \{S, A^{-1} \circ A \circ LS \circ C, Shuf_{64}\} \sim_{eq} \{S, A \circ LS \circ C \circ A^{-1}, Shuf_{64}\} \sim_{eq} \{S', LS', Shuf_{64}\}$

Our Approach

In the case of BOGI-64,

1. Obtaining C included in the LS's Iterative Permutation Characteristic
2. Obtaining $A \circ LS \circ C \circ A^{-1}$
3. Applying Property-2 to obtain p, p^{-1}, LS'
4. Obtaining S' corresponding to $p \circ S \circ p^{-1}$
5. $\{S, LS, Shuf_{64}\} \sim_{eq} \{S', LS', Shuf_{64}\}$

41,472 ➔ 864

- Final reduction by a factor 48 : 41,472 ➔ 864
- For BOGI-128, it is similarly provable and reducible by a multiple of 8 : 41,472 ➔ 5,184

➔ We can obtain the most resistant BOGI-128 against statistical attacks

Thank you for your attention!

Quiz Question 13

Which of these is the Liège waffle?

A

B

C

D

Next Talk:
CiC Area Chair

CiC Area Chair

Yu Sasaki

Communications in Cryptology (CiC)

IACR's new journal started from January 2024.

General positioning is not competing with existing general/area conferences and is complementary to them.

- To accommodate the growing community, increase the publication venue.
- Provide equal opportunities for researchers who have issues with travel budgets.
- Spotlight on research results that do not belong to TCC/PKC/FSE/CHES.

Some issues were also pointed out, mainly by the FSE community

- a new journal will make the publication landscape too complex,
- might lead to more reviews overall and make it harder to find good reviewers.

(*MINUTES IACR BOARD MEETING VIRTUAL-2 '22*
https://www.iacr.org/docs/minutes/virtual-2_2022bod.pdf)

Vote at IACR 2022 election; **Yes: 491, No: 128**

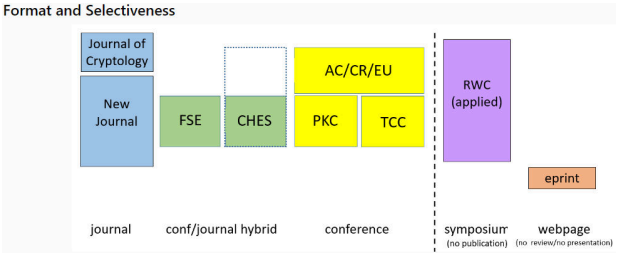
Relationship with ToSC

Q: What is the relationship of CiC and ToSC/TCHES?

A: ToSC/TCHES are considered the prime venues for publishing major results in their respective areas. (*Q&A of CiC*, https://cic.iacr.org/faq)

Q: Does the target level of papers in CiC include those rejected by ToSC?

A: … yes, the CiC is (also) for scientifically sound papers which have been rejected from ToSC. (*personal communication*)



Principles, Scope, Organization and FAQ for the IACR Journal : https://iacr.org/cic-proposal/

Quick Look on Volume 1, Issue 1

Submission: January 8
Notification: March 5

100 submissions in total, and 17 of them are in the symmetric-key area.

Accept	4
Minor revision	1
Major revision	5
Reject & Resubmit	1
Reject	3
Decision postponed (long papers)	3

Final Remarks

CiC started.

Personal thoughts on issues that may appear in future:

- high review workload
- fairness among different fields (position of CiC is different for different fields)

"almost 80 percent of the members voted for the new journal, however this means that we have work to do to talk and understand the concerns of the other 20 percent."

(*MINUTES IACR BOARD MEETING VIRTUAL-11 '22*, https://www.iacr.org/docs/minutes/virtual-11_2022bod.pdf)

Useful links to understand CiC.

- *FAQ of CiC*: https://cic.iacr.org/faq
- *Principles, Scope, Organization and FAQ for the IACR Journal*: https://iacr.org/cic-proposal/

Quiz Question 14

Which statue stands *closest* to the conference venue?

A

B

C

D

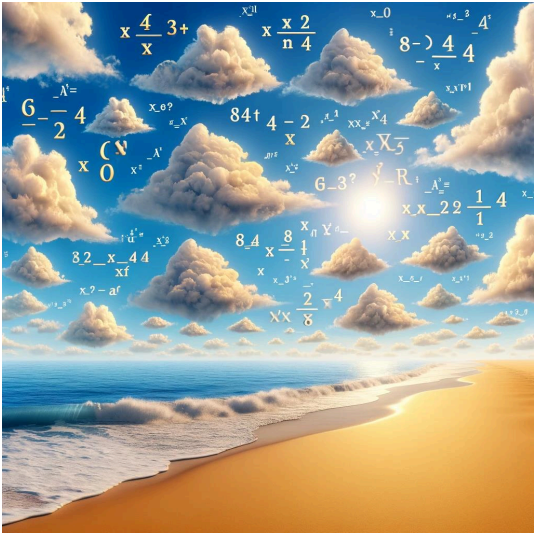
Next Talk:
Tropical Issue


Welcome to FSE 2024
Porto de Galinhas, Brazil

Tropical Issue on Boolean functions

Tropical Issue on Boolean functions

Tropical Issue on Boolean functions



Tropical Issue on Boolean functions


30th Fast Software Encryption Conference
March 25-29, 2024
Leuven, Belgium

~~Tropical~~ Topical Issue on Boolean functions

JoC: Topical Collection on Advances in Boolean Functions with Applications in Cryptography

Topics include (but not limited to):

•Design and analysis of cryptographically significant (vectorial) Boolean functions;
•Applications of (vectorial) Boolean functions in cryptography;
•Applications of (vectorial) Boolean functions in protecting secure implementations against physical attacks.

Submissions will be opened from **April 1st, 2024 to July 1st, 2024**

Questions? Contact Svetla Nikova and Gregor Leander

Quiz Question 15

Which famous cryptographic algorithm was *not* (co-)designed by a Belgian cryptographer?

A Mister Monster Burrito

B Hasty Pudding Cipher

C BaseKing

D Donkey Sponge

Next Talk:
Means of Communication

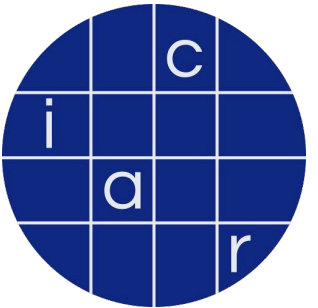
Means of communication

Dmitry Khovratovich, Ethereum Foundation

There were many ideas how we could discuss papers and new results online…

Not “at which location”

But how

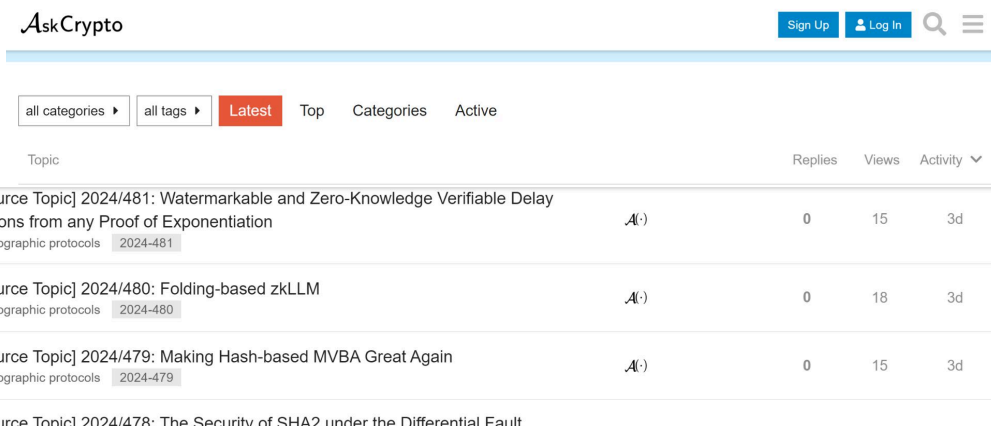


Not particularly successful

Goto: ·

Forums	Threads	Posts	Last Post
2017 Reports Discussion forum for Cryptology ePrint Archive reports posted in 2017. Please put the report number in the subject.	1	2	24 May 2017 16:10

Not particularly successful



At the same time in Telegram…

Group Info

ZK Study Club

250 members

Group Info

ZeroKnowledgePodcast

2,539 members

At the same time in Telegram…

Dozens of fresh, active, hot chats on cryptography every day.

related to this week's zk hack puzzle, I'm working through an explainer of the puzzle and I'm somewhat confused by the zcash spec Lemma 5.4.7 proof, demonstrating that:

Lemma 5.4.7. Let $P=(u,v) \in \mathbb J^{(r)}.$ Then $(u,-v) \not \in \mathbb J^{(r)}$ (subgroup of Jubjub of order r).

if anyone here might be more familiar, I'd appreciate any comments or direction.

Hi folks. Does anybody have any pointers on where I should look to get up to speed on the state of the art when it comes to the GKR protocol? Are the techniques from Libra still the best approach?

At the same time in Telegram…

Dozens of fresh, active, hot chats on cryptography every day.

But not on symmetric crypto yet…

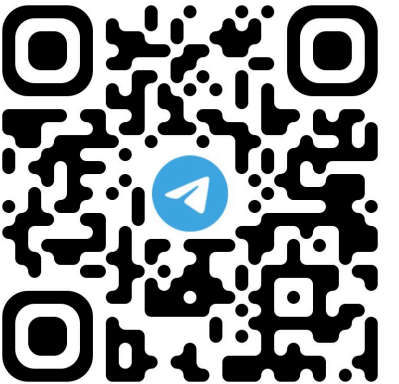
Join Symmetric Cryptography Chat!

Already there:

- Groebner basis attacks
- Algebraic hash discussions

No hate speech
No spam
Respond at your convenience

Scan QR code or ask
@khovratovich for a link



Quiz Question 16

How is Manneken Pis currently dressed?

A

B

C

D

Next Talk:
Partial Sums Meet FHT

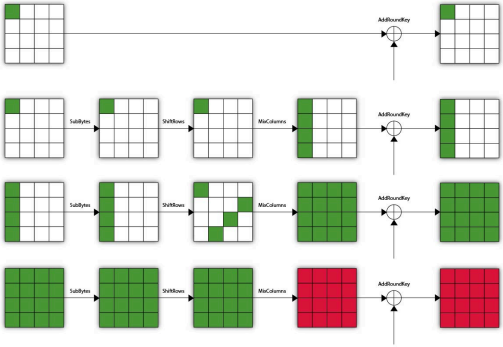
Partial Sums Meet FHT

FSE 2024

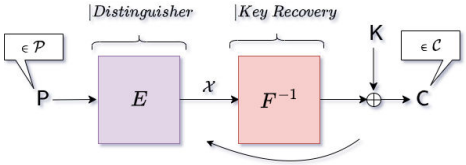
Orr Dunkelman Shibam Ghosh Nathan Keller
Gaëtan Leurent Avichai Marmor Victor Mollimard

March 26, 2024

Zero-Sum/Integral/Square Property Of 3-Round AES

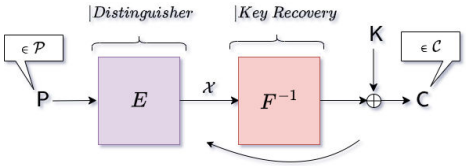


Key Recovery



$$\bigoplus_{X \in \mathcal{X}} X = \bigoplus_{P \in \mathcal{P}} E(P) = 0 = \bigoplus_{C \in \mathcal{C}} F(C \oplus K), \text{ For the right key } K$$

Key Recovery

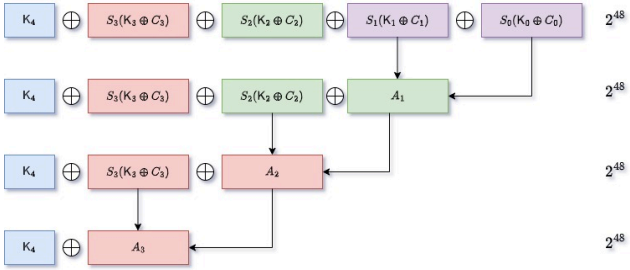


$$\bigoplus_{X \in \mathcal{X}} X = \bigoplus_{P \in \mathcal{P}} E(P) = 0 = \bigoplus_{C \in \mathcal{C}} F(C \oplus K), \text{ For the right key } K$$

$$F(K \oplus C) = S(K_4 \oplus S_3(K_3 \oplus C_3) \oplus S_2(K_2 \oplus C_2) \oplus S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0))$$

Partial Sum Technique, Ferguson et al.

Partial Sum Technique, Ferguson et al.



Another View Of F, Todo et al.

$$\begin{bmatrix} F(0\oplus 0) & F(0\oplus 1) & F(0\oplus 2) & F(0\oplus 3) & F(0\oplus 4) & F(0\oplus 5) & F(0\oplus 6) & F(0\oplus 7) \\ F(1\oplus 0) & F(1\oplus 1) & F(1\oplus 2) & F(1\oplus 3) & F(1\oplus 4) & F(1\oplus 5) & F(1\oplus 6) & F(1\oplus 7) \\ F(2\oplus 0) & F(2\oplus 1) & F(2\oplus 2) & F(2\oplus 3) & F(2\oplus 4) & F(2\oplus 5) & F(2\oplus 6) & F(2\oplus 7) \\ F(3\oplus 0) & F(3\oplus 1) & F(3\oplus 2) & F(3\oplus 3) & F(3\oplus 4) & F(3\oplus 5) & F(3\oplus 6) & F(3\oplus 7) \\ F(4\oplus 0) & F(4\oplus 1) & F(4\oplus 2) & F(4\oplus 3) & F(4\oplus 4) & F(4\oplus 5) & F(4\oplus 6) & F(4\oplus 7) \\ F(5\oplus 0) & F(5\oplus 1) & F(5\oplus 2) & F(5\oplus 3) & F(5\oplus 4) & F(5\oplus 5) & F(5\oplus 6) & F(5\oplus 7) \\ F(6\oplus 0) & F(6\oplus 1) & F(6\oplus 2) & F(6\oplus 3) & F(6\oplus 4) & F(6\oplus 5) & F(6\oplus 6) & F(6\oplus 7) \\ F(7\oplus 0) & F(7\oplus 1) & F(7\oplus 2) & F(7\oplus 3) & F(7\oplus 4) & F(7\oplus 5) & F(7\oplus 6) & F(7\oplus 7) \end{bmatrix}_{8\times 8}$$

Why Not Both?

The 6-Round AES Duel(s)

	FFT+Part. Sums	FFT	Part. Sums
AWS Instance	m6i.32xlarge	r6i.32xlarge	m6i.32xlarge
Time Complexity	$2^{44.1}$ Additions	$2^{50.8}$ Additions	2^{50} Sbox
Running Time(m)	48	3120	4859
Total Cost (USD)	5	418	497

In Conclusion: Our attack is 65 times faster and 83 times cheaper

Full Presentation at

Quiz Question 17

Welcher Patrick ist kein Deutscher?

A

B

C

D

Next Talk:
NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

June 20–21, 2024, Rockville, Maryland

NIST plans to develop an accordion cipher mode

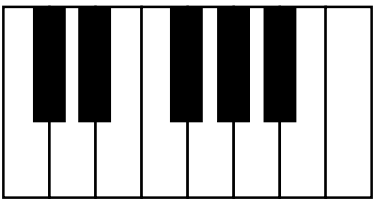
keys

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

June 20–21, 2024, Rockville, Maryland

NIST plans to develop an accordion cipher mode

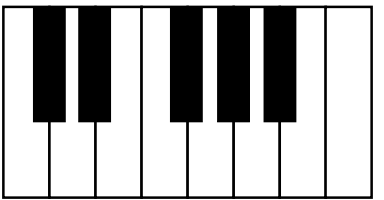
keys



NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

June 20–21, 2024, Rockville, Maryland

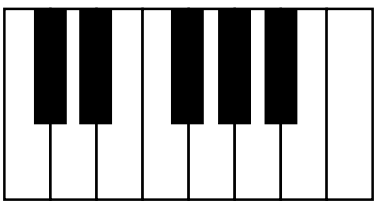
NIST plans to develop an accordion cipher mode



NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

June 20–21, 2024, Rockville, Maryland

NIST plans to develop an accordion cipher mode



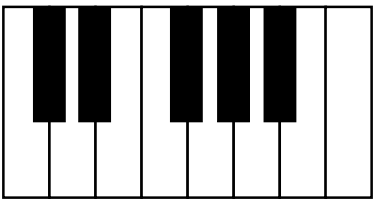
not required to be format preserving

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

June 20–21, 2024, Rockville, Maryland

NIST plans to develop an accordion cipher mode

Piano instrument mode



not required to be format preserving

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

June 20–21, 2024, Rockville, Maryland

NIST plans to develop an accordion cipher mode

Piano instrument mode

Drum instrument mode

keys

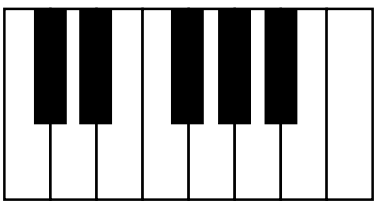
plaintext	C	D	E	F	G	A	B	C
ciphertext	¶	◸	dž dž	♨	ǂǂ ǂǂ	☹	⅞	☎

not required to be format preserving

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

June 20–21, 2024, Rockville, Maryland

NIST plans to develop an accordion cipher mode



not required to be format preserving

Piano instrument mode

Drum instrument mode

Weapon mode

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

June 20–21, 2024, Rockville, Maryland

NIST plans to develop a new mode of the **AES** that is a **tweakable**, variable-input-length-strong pseudorandom permutation (**VIL-SPRP**) with a **reduction proof** to the security of the underlying block cipher.

Accordion mode

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

Purpose

To solicit public input on the design requirements and use of an accordion mode.

- Parameter lengths: keys, tweaks, data input
- Potential support of an underlying block cipher with 256-bit blocks
- Formal security goals
- Requirements and features for the main use cases (e.g., AEAD)
- Design strategies
- Performance targets and implementation considerations
- Development and standardization process

Workshop Form

- Attendees may submit extended abstracts or slides (up to 10 minutes) for any number of the sessions.
- Sessions are expected to include a panel discussion or extensive open discussion.
- “lightning talks” — brief presentations of recent results without slides.

NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

Rockville, Maryland
National Cybersecurity Center of Excellence (NCCoE)

Important dates

- Workshop: June 20–21, 2024
- Submission deadline: May 1, 2024
- Notification date: May 17, 2024
- Registration deadline: June 13, 2024

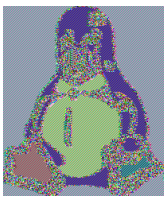
Links

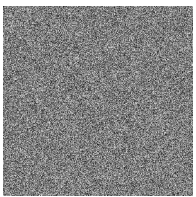
- Event: https://csrc.nist.gov/Events/2024/accordion-cipher-mode-workshop-2024
- Forum: https://csrc.nist.gov/Projects/block-cipher-techniques/email-list-ciphermodes-forum
- Contact e-mail: ciphermodes@nist.gov

Quiz Question 18

A penguin  **has been encrypted three times: with AES, with Lolcipher, and with chaos-based image encryption. Which one is done with AES?**

A 

B 

C 

Next Talk:
A Collaborative Automated Cryptanalysis Initiative

A Collaborative Automated Cryptanalysis Initiative

Emanuele Bellini (UAE), Christina Boura (France), Patrick Derbez (France),
Maria Eichlseder (Austria), Juan Grados (UAE), Kai Hu (China),
María Naya-Plasencia (France), Thomas Peyrin (Singapore), Thomas Pornin (Canada),
Danping Shi (China), Ling Song (China), Siwei Sun (China), Meiqin Wang (China)

Automatic cryptanalysis field is becoming quite mature, maybe now is a good time to start consolidating

- Free and Open Source
- Easy to use / contribute
- Start simple (differential/linear)
- **Future ?** Moar attacks, key recovery, graphical interface, parallelisation, implementations, testing on reduced rounds, a pre-existing library of ciphers and attacks, path drawings, …
- **Goal:** become the **go-to platform** for creating / testing / benchmarking cryptanalysis
- Establishing governance to put proper development processes into place, regular meetings

We are just starting (not even a name) … a lot of work to be done.
Interested to use / to provide feedback / to contribute / propose a name ?
For questions, contact thomas.peyrin@ntu.edu.sg
Or register to the mailing list: automated-cryptanalysis@googlegroups.com
(click on this link: https://groups.google.com/g/automated-cryptanalysis)

WE WANT YOU!

Quiz Question 19

Is RadioGatún a sponge?

A Yes

B No

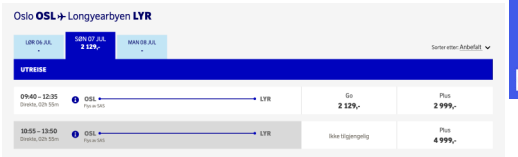
C Yes, but no

D No, but yes

Next Talk:
Make Crypto Cool Again - ArcticCrypt Returns!

Make Crypto Cool Again
ArcticCrypt Returns!

Longyearbyen, Svalbard
July 6th – 11th 2025



In cooperation with CiC

Papers submitted to CiC's issue 2 & 3 can opt to be automatically considered for ArcticCrypt

We also accept submissions directly to ArcticCrypt, deadline September 13th

https://simula-uib.com/arcticcrypt2025/

Quiz Question 20

What is the correct spelling of the name of  **?**

A María Naya-Plasencia

B María Playa-Nasencia

C María Naya-Placensia

D María Eichlseder

Next Talk (after the break):
Update on the QARMAGEDDON: The Competition

QARMAGEDDON: The Competition

Roberto Avanzi, Subhadeep Banik, Light Darkman, Maria Eichlseder,
Shibam Ghosh, Marcel Nageler, and Francesco Regazzoni

Arm, CRI, Universities of Amsterdam, Graz, Haifa, Lugano

arm

A competition to analyze the Tweakable Block Cipher QARMAv2...

... a redesign of the TBC QARMA (FSE 2017)
for better security and longer tweaks.

Details will be given at FSE 2024. If you, by any chance, are planning to attend that conference, you will know.

Like QARMA, it is in the public domain!

A competition to analyze the Tweakable Block Cipher QARMAv2...

... a redesign of the TBC QARMA (FSE 2017)
for better security and longer tweaks.

Details will be given at FSE 2024. If you, by any chance, are planning to attend that conference, you will know.

Like QARMA, it is in the public domain!

A competition to analyze the Tweakable Block Cipher QARMAv2...

... a redesign of the TBC QARMA (FSE 2017)
for better security and longer tweaks.

Details will be given at FSE 2024. If you, by any chance, are planning to attend that conference, you will know.

Like QARMA, it is in the public domain!

The competition

- Categories: Block $n = 64$ or 128 bits ($2n$ bit tweak and key, S-Box = קּ).
- A single submission may apply to one or both categories.
- **Break as many rounds as possible!**
  Then, minimize Time * max (Data, Mem)!
- Other attacks may be considered at the sole discretion of the Jury.
- Mathematical, classical cryptanalysis only. (No quantum computers.)
- **No extra credits if you are from Belgium.**

The competition

- Categories: Block $n = 64$ or 128 bits ($2n$ bit tweak and key, S-Box = קּ).
- A single submission may apply to one or both categories.
- **Break as many rounds as possible!**
  Then, minimize Time * max (Data, Mem)!
- Other attacks may be considered at the sole discretion of the Jury.
- Mathematical, classical cryptanalysis only. (No quantum computers.)
- **No extra credits if you are from Belgium.**

The competition

- Categories: Block $n = 64$ or 128 bits ($2n$ bit tweak and key, S-Box = קּ).
- A single submission may apply to one or both categories.
- **Break as many rounds as possible!**
  Then, minimize Time * max (Data, Mem)!
- Other attacks may be considered at the sole discretion of the Jury.
- Mathematical, classical cryptanalysis only. (No quantum computers.)
- **No extra credits if you are from Belgium.**

The competition

- Categories: Block $n = 64$ or 128 bits ($2n$ bit tweak and key, S-Box = קּ).
- A single submission may apply to one or both categories.
- **Break as many rounds as possible!**
  Then, minimize Time * max (Data, Mem)!
- Other attacks may be considered at the sole discretion of the Jury.
- Mathematical, classical cryptanalysis only. (No quantum computers.)
- **No extra credits if you are from Belgium.**

The competition

- Important Dates:
  - We need to reschedule because ~~shit~~ bad luck happens (Arm has made the role of cryptographer “redundant” so I am busy with other stuff).
  - Arm committed to competitition.
  - Deadline: One month before Asiacrypt in India.
  - **No extra time if you are from Belgium.**
  - HotCRP instance (or equivalent) ASAP.

The Jury

- Roberto Avanzi (Chair)
- Orr Dunkelman
- Maria Eichlseder
- Francesco Regazzoni
- Hugo Vincent (Arm representative)

Submission and Prizes

- **Jackpot: 10K (ten thousand) USD sponsored by Arm.**
- We pay first author, they must share with other authors.

  We strongly encourage the professors to exclude themselves from the money sharing.


Especially the professors from Belgium.

You can participate if ...

- You do not reside in a US embargoed country (Cuba, Iran, North Korea, Russia, Sudan, Syria).
  Neither is your bank account.
  For some unexplainable reasons, Belgium is fine, though.
- Government officials — with the exception of professors and other academics — need authorization from their gov.
- If you are a student, collaborator, or close relative of one of the Jury members, the latter will recuse themselves.

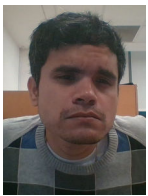
BELGIUM!

Have fun with the QARMAGEDDON Competition!!!

arm

Quiz Question 21

The saxophone is a Belgian invention. It was invented in the 1840s. Something else that happened in the 1840s was the Mexican-American war. The colors in the Mexican flags are green, white, and red. The Japanese word for green is "midori". Who was a co-designer of the Midori block cipher?

A 

B 

C 

D 

Next Talk:
On Overidealizing Ideal Worlds: Xor of Two Permutations and its Applications

On Overidealizing Ideal Worlds: Xor of Two Permutations and its Applications

Wonseok Choi[1] Minki Hhan[2] Yu Wei[1] Vassilis Zikas[1]

[1]Purdue University, West Lafayette, IN, USA

[2]Korea Institute for Advanced Study, Seoul, Korea

March 26th, 2024

Motivation

- My colleagues asked me to give a short talk about our work
- I had no idea how to make this talk fun
- I asked one of rump session chairs, but he couldn't give me a clear answer
- But then I realized that a new research topic is always fun! So it is probably okay

Motivation

- My colleagues asked me to give a short talk about our work
- I had no idea how to make this talk fun
- I asked one of rump session chairs, but he couldn't give me a clear answer
- But then I realized that a new research topic is always fun! So it is probably okay

Motivation

- My colleagues asked me to give a short talk about our work
- I had no idea how to make this talk fun
- I asked one of rump session chairs, but he couldn't give me a clear answer
- But then I realized that a new research topic is always fun! So it is probably okay

Motivation

- My colleagues asked me to give a short talk about our work
- I had no idea how to make this talk fun
- I asked one of rump session chairs, but he couldn't give me a clear answer
- But then I realized that a new research topic is always fun! So it is probably okay

Game Reduction

- It is common to introduce an *ideal world* to prove security notion; the ideal world is the ultimate goal of a given construction wants to be
- E.g. Unforgeability $\Leftrightarrow \left|\Pr\left[\mathcal{A}^{(Mac, Ver)}\right] - \Pr\left[\mathcal{A}^{(Mac, \perp)}\right]\right|$

Game Reduction

- It is common to introduce an *ideal world* to prove security notion; the ideal world is the ultimate goal of a given construction wants to be
- E.g. Unforgeability $\Leftrightarrow \left|\Pr\left[\mathcal{A}^{(Mac, Ver)}\right] - \Pr\left[\mathcal{A}^{(Mac, \perp)}\right]\right|$

Idealized Ideal World

- It is common to idealize the ideal world
- What does this mean?
- $\left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(\$,\perp)}\right]\right| \Rightarrow \left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(Mac,\perp)}\right]\right|$
- Why do this?
- There is (almost) no way to analyze the behavior of hash functions in the real world,
- i.e., JUST FOR CONVENIENCE

Idealized Ideal World

- It is common to idealize the ideal world
- What does this mean?
- $\left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(\$,\perp)}\right]\right| \Rightarrow \left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(Mac,\perp)}\right]\right|$
- Why do this?
- There is (almost) no way to analyze the behavior of hash functions in the real world,
- i.e., JUST FOR CONVENIENCE

Idealized Ideal World

- It is common to idealize the ideal world
- What does this mean?
- $\left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(\$,\perp)}\right]\right| \Rightarrow \left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(Mac,\perp)}\right]\right|$
- Why do this?
- There is (almost) no way to analyze the behavior of hash functions in the real world,
- i.e., JUST FOR CONVENIENCE

Idealized Ideal World

- It is common to idealize the ideal world
- What does this mean?
- $\left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(\$,\perp)}\right]\right| \Rightarrow \left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(Mac,\perp)}\right]\right|$
- Why do this?
- There is (almost) no way to analyze the behavior of hash functions in the real world,
- i.e., JUST FOR CONVENIENCE

Idealized Ideal World

- It is common to idealize the ideal world
- What does this mean?
- $\left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(\$,\perp)}\right]\right| \Rightarrow \left|\Pr\left[\mathcal{A}^{(Mac,Ver)}\right] - \Pr\left[\mathcal{A}^{(Mac,\perp)}\right]\right|$
- Why do this?
- There is (almost) no way to analyze the behavior of hash functions in the real world,
- i.e., JUST FOR CONVENIENCE

Overidealized Ideal World

- Somewhat not surprisingly, this harms security analysis
- How can we do better?

Quiz Question 22

This FSE is the 30th FSE conference.
In which year was the first FSE?

A 1993
B 1994
C 1995
D 1996

Next Talk:
Targets You've Never Heard Of!

Targets You've Never Heard Of!

Léo Perrin

Inria
leo.perrin@inria.fr

FSE 2024 (rump session)

Sacred vs. Heretical Symmetric Primitives

In the holy land of Leuven, the two prophets convened, and together built the prophecized block cipher: **Rijndael**.

Sacred vs. Heretical Symmetric Primitives

In the holy land of Leuven, the two prophets convened, and together built the prophecized block cipher: **Rijndael**.

And cryptographers throughout the world rejoiced,

Sacred vs. Heretical Symmetric Primitives

In the holy land of Leuven, the two prophets convened, and together built the prophecized block cipher: **Rijndael**.

And cryptographers throughout the world rejoiced,for its rounds were plentiful,

Sacred vs. Heretical Symmetric Primitives

In the holy land of Leuven, the two prophets convened, and together built the prophecized block cipher: **Rijndael**.

And cryptographers throughout the world rejoiced,for its rounds were plentiful, and its S-box of high degree,

Sacred vs. Heretical Symmetric Primitives

In the holy land of Leuven, the two prophets convened, and together built the prophecized block cipher: **Rijndael**.

And cryptographers throughout the world rejoiced,for its rounds were plentiful, and its S-box of high degree, and it feared no adversaries, not even adaptatively chosen ciphertext queries.

Sacred vs. Heretical Symmetric Primitives

In the holy land of Leuven, the two prophets convened, and together built the prophecized block cipher: **Rijndael**.

And cryptographers throughout the world rejoiced,for its rounds were plentiful, and its S-box of high degree, and it feared no adversaries, not even adaptatively chosen ciphertext queries.

What ~~Heretics~~MPC people build

- 1 round
- multiplicative depth $= 1$
- only random queries

Mod 6 ?

The Candidates

Name:	**BIPSW**
Introduced when?	2018
Introduced where?	(Boneh, Ishai, Passelègue, Sahai, Wu, TCC'18)
Known cryptanalysis:	(CCKK, PKC'21), (JMN, ISIT'23)
Applications:	OPRF, OT extension, PCF, signature, side channel…

Construction

$k \leftarrow_r \{0,1\}^n, \; x \leftarrow_r \{0,1\}^n$

$F_k(x) = \lceil \langle k, x \rangle \bmod 6 \rfloor_2$, where

- $\lceil u \rfloor_2 = 0$ if $u \in \{0,1,2\}$
- $\lceil u \rfloor_2 = 1$ if $u \in \{3,4,5\}$

Parameter set ($\lambda = 128$)

$n = 770^*$
$N = 2^{44.5}$

Rationale: $6 = 2 \times 3 \rightarrow$ resists (?) to basic algebraic attack, provides high non-linearity over both $\mathbb{F}_2$ and $\mathbb{F}_3$

“predicate” ??!

The Candidates

Name:	**GAR**
Introduced when?	2000
Introduced where?	(Goldreich, 2000) and (Applebaum and Raykov, TCC’16)
Known cryptanalysis:	Way too much to list (but see next slide)
Applications:	OT extension, PCF, constant-overhead MPC, iO…

Construction	**Parameter set ($\lambda = 128$)**
$k \leftarrow_r \{0,1\}^n$, x is parsed as a subset S_x of $[1,n]$ of size $\lvert S_x \rvert = \ell$ $F_k(x) = P(k[S_x])$, where $P : \{0,1\}^\ell \to \{0,1\}$ is a suitable predicate	$n = 256$, $N = 2^{40}$ $\ell = \ell_1 + \ell_2$ with $\ell_1 = 10$ and $\ell_2 = 64$ $P = \mathsf{XOR}_{\ell_1}\text{-}\mathsf{MAJ}_{\ell_2}$: $P(u) = \mathsf{XOR}(u_1, \cdots, u_{\ell_1}) \oplus \mathsf{MAJ}(u_{\ell_1+1}, \cdots, u_\ell)$

FOCS conference ??!?!

The Candidates

Name:	**(Aggressive)-VDLPN**
Introduced when?	2020
Introduced where?	(Boyle, Couteau, Gilboa, Ishai, Kohl, Scholl, FOCS'20
Known cryptanalysis:	(BCGIKS, FOCS'20), (CD, PKC'23)
Applications:	PCF, learning theory

Construction

$k \leftarrow_r \{0,1\}^{w \cdot D}$ is viewed as $(k_{j,\ell})_{j \le w, \ell \le D}$,
$x \leftarrow_r \{0,1\}^{w \cdot D}$ is viewed as $(x_{j,\ell})_{j \le w, \ell \le D}$

$$F_k(x) = \bigoplus_{i=1}^{D} \bigoplus_{j=1}^{w} \bigwedge_{\ell=1}^{i} (x_{j,\ell} \oplus k_{j,\ell})$$

$$= \bigoplus_{j=1}^{w} T(x_j \oplus k_j) \text{ where } T \text{ is a « fake »}$$

triangular function

Parameter set ($\lambda = 80$)

$w = 120, D = \log N = 30$

Note: $T(x) = x_1 \oplus x_1x_2 \oplus x_1x_2x_3 \oplus \cdots$
If T was a *true* triangular function, we'd get the real VDLPN candidate, below:

$$F_K(x) = \bigoplus_{i=1}^{d} \bigoplus_{j=1}^{t} \bigwedge_{\ell=1}^{i} \left(x_{i,j,\ell} \oplus K_{i,j,\ell} \right) = F(x \oplus K)$$

This one has a fair bunch of security arguments*, but the aggressive variant has none!

COMPARISONS ??!?!111?!1

The Candidates

Name:	**EA-LPN**
Introduced when?	2022
Introduced where?	(Boyle, Couteau, Gilboa, Ishai, Kohl, Resch, Scholl, CRYPTO'22)
Known cryptanalysis:	(BCGIKRS, CRYPTO'22), (RRT, CRYPTO'23)
Applications:	PCF (state of the art)

Construction

$k = (k_1, \cdots, k_\ell)$ where $k_i = (k_{i,1}, \cdots, k_{i,t/\ell}) \in [1{,}5N/t]$

$x = (j_1, x_1), \cdots, (j_\ell, x_\ell)$,
where $j_i \leftarrow_r [1{,}t/\ell]$ and $x_i \leftarrow_r [1{,}5N/t]$

$$F_k(x) = \sum_{i=1}^{\ell} \mathsf{GT}(x_i, k_{i,j_i}),$$

where $\mathsf{GT}(a, b) = 1$ iff $a > b$

Parameter set ($\lambda = 128$)

Standard: $t = 85$, $\ell = 3\ln(5N)$, $N = 2^{45}$
Aggressive: $t = 660$, $\ell = 11$, $N = 2^{45}$

The Heroes We Need!

They should have expected the Symmetric Inquisition!

The Heroes We Need!

They should have expected the **Symmetric** Inquisition!

The Heroes We Need!

They should have expected the **Symmetric** Inquisition!

- BIPSW https://ia.cr/2018/1218
- GAR https://ia.cr/2000/063
- VDLPN https://ia.cr/2020/1417
- EA-LPN https://ia.cr/2022/1035

The Heroes We Need!

They should have expected the **Symmetric** Inquisition!

- BIPSW `https://ia.cr/2018/1218`
- GAR `https://ia.cr/2000/063`
- VDLPN `https://ia.cr/2020/1417`
- EA-LPN `https://ia.cr/2022/1035`

Thanks to Geoffroy Couteau for his slides/help, and

The Heroes We Need!

They should have expected the **Symmetric** Inquisition!

- BIPSW https://ia.cr/2018/1218
- GAR https://ia.cr/2000/063
- VDLPN https://ia.cr/2020/1417
- EA-LPN https://ia.cr/2022/1035

Thanks to Geoffroy Couteau for his slides/help, and

Thank you!

Quiz Question 23

How many times has FSE been organized in Leuven?

A 2

B 3

C 4

D 5

Next Talk:
Mistakes made by cryptographers

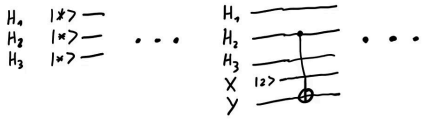
Radboud University

Mistakes cryptographers makes

March 26, 2024

The “standard oracle”, StO

- **Keep function in superposition** $|*\rangle := \sum_x |x\rangle$
- **Register H_x – contains the output $H(x)$.**
- **Initial state:** $|*\rangle|*\rangle \ldots |*\rangle$
- **Query:** $|h_1\rangle|h_2\rangle \ldots |h_N\rangle |x\rangle|y\rangle \longmapsto \cdots |y \oplus h_x\rangle$



- **Indistinguishable from random function**

Did you miss it?

Titel der Präsentation | Name des Vortragenden | Organisationseinheit | 00.00.2000 | Die Fußzeile bietet Platz für einen Text über 3 Zeilen | Die Fußzeile bietet Platz für einen Text über 3 Zeilen | Die Fußzeile bietet Platz für 3 Zeilen

Mistake: Buy dinosaur suit

Where is the cryptograher?

Mistake: Run a children's race

When you do... Smile!

Hiring this guy...

Hiring this guy...

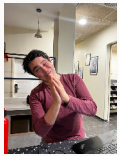
Encouraging students to do rump sessions...

Hiring this guy...

Encouraging students to do rump sessions...

Making this presentation!

Seriously, don't fire me



But, he did do some things right!

Alphabet: Always leave some future work!

- **A**: Andreeva Aly Ashur Athanasopoulos Aumasson
- **B**: Berendsen Beyne Bhaumik Bilgin Bogdanov Boura Beato
- **C**: Chang, Chen
- **D**: Daemen Dai Datta Dinur Dobraunig Dodis Dutta Dhooghe
- **E**: Eichlseder Erkin
- **F**: Fehr
- **G**: Granger Grassi Gunsing Guajardo
- **H**: Halunen Hermans
- **I**: Iwata
- **J**: Jha Jovanovic
- **K**: Karpman Khovratovich
- **L**: Lambooij Lee Lefevre Luykx Leander
- **M**: Mangard Marhuenda Mendel Mouha Matusiewicz Maulany Minematsu Mustafa
- **N**: Nandi Neves Nateghizad Naya-Plasencia Nyberg
- **P**: Paterson Preneel Primas Papadimitratos
- **Q**: Quine
- **R**: Reyhanitabar Rechberger Rijmen Rotaru
- **S**: Sanadhya Sasaki Shen Sibleyras Steinberger Schoenmakers Schroé Skrobot Symeonidis Szepieniec
- **T**: Tischhauser Tereschenko
- **U**: Unterluggauer
- **V**: Van Assche Vizár Van Herrewege Verbauwhede
- **W**: Watanabe Winnen
- **Y**: Yasuda

No O ,X, Z

But seriously, he's cool...

Temporary page!

LaTeX was unable to guess the total number of pages correctly. As there was some unprocessed data that should have been added to the final page this extra page has been added to receive it.

If you rerun the document (without altering it) this surplus page will go away, because LaTeX now knows how many pages to expect for this document.

Quiz Question 24

Which of the following is *not* an official language of Belgium?

A Dutch

B French

C Brusselian

D German

Next Talk:
How to add a quiz question

How to add a quiz question

Jules Baudrin[1], Rachelle Heim Boissier[2]

[1]Inria Paris, [2]UVSQ

26 March 2024

Outline

Context

- Quiz at FSE 2024 rump session.
- As many quiz questions as there are presentations. [LeuMen24]

Our motivation

- We love quizzes.
- This motivated us to try to find a way to add an extra question.

Our heuristic

- We think if we make an extra presentation then there will be an extra question.

Methodology

- We used LaTeX beamer class.

Experiments

- Currently ongoing.
- Expected result : extra quiz question.

Conclusion

Thank you very much for your attention.

Feel free to ask any question.

especially if it is a quiz question

Quiz Question 25

Which journal is *not* the leading journal in its field?

A The Journal of Cryptology

B The IACR Transactions on Symmetric Cryptology

C The Journal of Craptology

D The IACR Communications in Cryptology

Next Talk:
How to add two quiz questions

How to add two quiz questions

Jules Baudrin[1], Rachelle Heim Boissier[2]

[1]Inria Paris, [2]UVSQ

26 March 2024

Plan

Previous work

Extracted from [BauHei24a]:

“

- Quiz at FSE 2024 rump session.
- As many quiz questions as there are presentations. [MenLeu24]
- We love quizzes.
- This motivated us to try to find a way to add extra questions.
- We think if we make an extra presentation then there will be an extra question.
- Expected result : extra quiz question.

”

Plan

Our incredible results !

Attack	Number of quiz questions	Reference
DDoS	1	[BauHei24a]
DDoS	2	This paper: [BauHei24b]

Plan

Our methodology

Detailed Instructions

- The rump session will be entirely physical, we do not accept remote contributions.
- The rump session will be recorded.
- Please submit a single PDF. We require the speakers to submit at least a title slide even if they are not planning to prepare slides for the talk.
- Submissions should be made to this HotCRP instance.

Rump Session Chairs

- Gaëtan Leurent, Inria, France
- Bart Mennink, Radboud University, The Netherlands

Source : `https://fse.iacr.org/2024/rumpsession.php`

Our methodology

Detailed Instructions

- The rump session will be entirely physical, we do not accept remote contributions.
- The rump session will be recorded.
- Please submit a single PDF. We require the speakers to submit at least a title slide even if they are not planning to prepare slides for the talk.
- Submissions should be made to this HotCRP instance.

Rump Session Chairs

- Gaëtan Leurent, Inria, France
- Bart Mennink, Radboud University, The Netherlands

Source : `https://fse.iacr.org/2024/rumpsession.php`

Our methodology

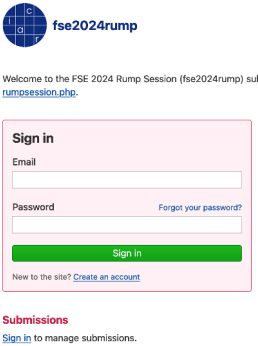
Detailed Instructions

- The rump session will be entirely physical, we do not accept remote contributions.
- The rump session will be recorded.
- Please submit a single PDF. We require the speakers to submit at least a title slide even if they are not planning to prepare slides for the talk.
- Submissions should be made to this HotCRP instance.

Rump Session Chairs

- Gaëtan Leurent, Inria, France
- Bart Mennink, Radboud University, The Netherlands

Source : `https://fse.iacr.org/2024/rumpsession.php`



Our methodology

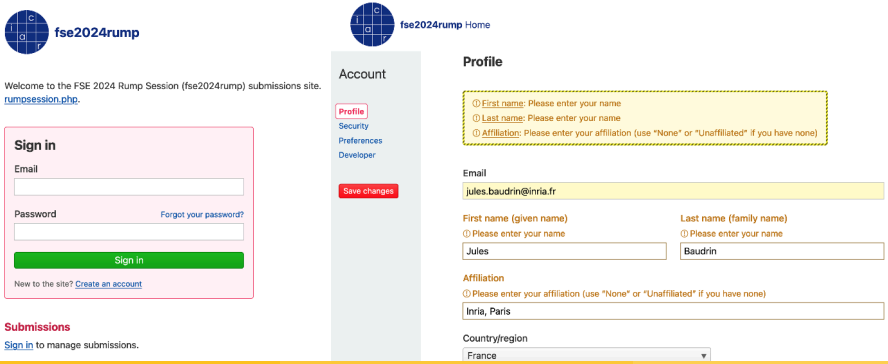
Detailed Instructions

- The rump session will be entirely physical, we do not accept remote contributions.
- The rump session will be recorded.
- Please submit a single PDF. We require the speakers to submit at least a title slide even if they are not planning to prepare slides for the talk.
- Submissions should be made to this HotCRP instance.

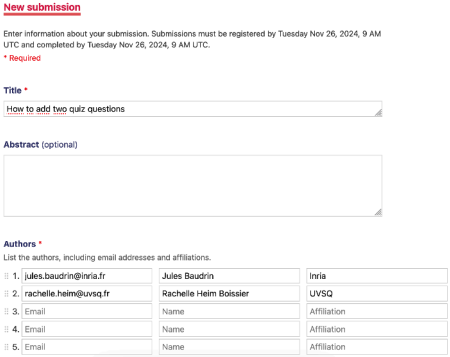
Rump Session Chairs

- Gaëtan Leurent, Inria, France
- Bart Mennink, Radboud University, The Netherlands

Source : `https://fse.iacr.org/2024/rumpsession.php`



Our methodology



New submission

Enter information about your submission. Submissions must be registered by Tuesday Nov 26, 2024, 9 AM UTC and completed by Tuesday Nov 26, 2024, 9 AM UTC.

* Required

Title *

How to add two quiz questions

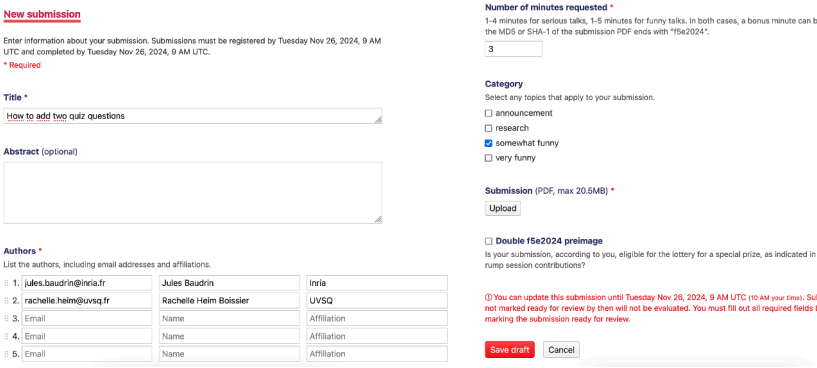
Abstract (optional)

Authors *

List the authors, including email addresses and affiliations.

1.	jules.baudrin@inria.fr	Jules Baudrin	Inria
2.	rachelle.heim@uvsq.fr	Rachelle Heim Boissier	UVSQ
3.	Email	Name	Affiliation
4.	Email	Name	Affiliation
5.	Email	Name	Affiliation

Our methodology



New submission

Enter information about your submission. Submissions must be registered by Tuesday Nov 26, 2024, 9 AM UTC and completed by Tuesday Nov 26, 2024, 9 AM UTC.

* Required

Title *

How to add two quiz questions

Abstract (optional)

Authors *

List the authors, including email addresses and affiliations.

1.	jules.baudrin@inria.fr	Jules Baudrin	Inria
2.	rachelle.heim@uvsq.fr	Rachelle Heim Boissier	UVSQ
3.	Email	Name	Affiliation
4.	Email	Name	Affiliation
5.	Email	Name	Affiliation

Number of minutes requested *

1-4 minutes for serious talks, 1-5 minutes for funny talks. In both cases, a bonus minute can be earned if the MD5 or SHA-1 of the submission PDF ends with "f5e2024".

3

Category

Select any topics that apply to your submission.

- ☐ announcement
- ☐ research
- ☑ somewhat funny
- ☐ very funny

Submission (PDF, max 20.5MB) *

Upload

☐ **Double f5e2024 preimage**

Is your submission, according to you, eligible for the lottery for a special prize, as indicated in the call for rump session contributions?

ⓘ You can update this submission until Tuesday Nov 26, 2024, 9 AM UTC (10 AM your time). Submissions not marked ready for review by then will not be evaluated. You must fill out all required fields before marking the submission ready for review.

Save draft Cancel

Plan

Conclusion

- Not an easy task
- Definitely room for improvements

Thank you very much for your attention.

Feel free to ask any question.

Quiz Question 26

Whose father won a nobel prize?

A

John Steinberger

B

Nicky Mouha

C

Adi Shamir

D

Michaël Quisquater

Next Talk:
Exploring the Six Worlds of Gröbner Basis Cryptanalysis: Application to Anemoi

SCIENCE
PASSION
TECHNOLOGY

Rump Session Talk

Exploring the Six Worlds of Gröbner Basis Cryptanalysis: Application to Anemoi

Katharina Koschatko, Reinhard Lüftenegger, Christian Rechberger

FSE 2024, Leuven

The waffle motivation

Some may say algebraic equations are as elegant as a fine Belgian waffle ...

The waffle motivation

Some may say algebraic equations are as elegant as a fine Belgian waffle ... complex yet satisfying.*

*A hilarious ice breaker, created by ChatGPT.

What we did: hugely simplified

No big surprise: Gröbner Basis attack

- High impact of variable ordering

What we did: hugely simplified

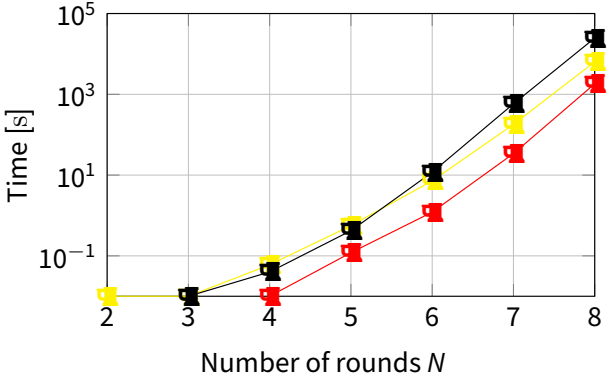
No big surprise: Gröbner Basis attack

- High impact of variable ordering

What we did: hugely simplified

No big surprise: Gröbner Basis attack

- High impact of variable ordering



What we did: hugely simplified

No big surprise: Gröbner Basis attack

- High impact of variable ordering

Moreover:

(GB) Tighter complexity formula

(FGLM) Multihomogeneous Bézout bound

What we did: hugely simplified

No big surprise: Gröbner Basis attack

- High impact of variable ordering

Moreover:

(GB) Tighter complexity formula

(FGLM) Multihomogeneous Bézout bound

What we did: hugely simplified

No big surprise: Gröbner Basis attack

- High impact of variable ordering

Moreover:

(GB) Tighter complexity formula

(FGLM) Multihomogeneous Bézout bound

Result: more rounds needed for Anemoi

"The Six Worlds of Gröbner Basis Cryptanalysis"

Result: more rounds needed for Anemoi

"The Six Worlds of Gröbner Basis Cryptanalysis"
What you want to read: https://eprint.iacr.org/2024/250

Result: more rounds needed for Anemoi

"The Six Worlds of Gröbner Basis Cryptanalysis"
What you want to read: https://eprint.iacr.org/2024/250

		New					
		Experimental approach			**Theoretical approach**		
s	Old [1]	GB	*FGLM*	*FAC*	*GB*	*FGLM*	*FAC*
128	21	23	27	31	?	23	26
256	37	45	54	61	?	45	51

[1]: Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov, and Willems: "New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode." CRYPTO 2023.

Result: more rounds needed for Anemoi

"The Six Worlds of Gröbner Basis Cryptanalysis"
What you want to read: https://eprint.iacr.org/2024/250

		New					
		Experimental approach			**Theoretical approach**		
s	Old [1]	GB	*FGLM*	*FAC*	*GB*	*FGLM*	*FAC*
128	21	23	27	31	?	23	26
256	37	45	54	61	?	45	51

[1]: Bouvier, Briaud, Chaidos, Perrin, Salen, Velichkov, and Willems: "New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode." CRYPTO 2023.

TU Graz

SCIENCE
PASSION
TECHNOLOGY

Rump Session Talk

Exploring the Six Worlds of Gröbner Basis Cryptanalysis: Application to Anemoi

Katharina Koschatko, Reinhard Lüftenegger, Christian Rechberger

FSE 2024, Leuven

Quiz Question 27

Name one symmetric cryptographer that has spent significant time in jail.

Next Talk:
Key Recovery Attack on 5-round AES using the Multiple-of-8 Property

KOREA UNIVERSITY

Cryptographic Algorithm Laboratory

Key Recovery Attack on 5-round AES using the Multiple-of-8 Property

(work in progress)

FSE 2024 Rump Session

Hanbeom Shin, **newonetiger@korea.ac.kr**

Insung Kim, cmcom35@korea.ac.kr

Dongjae Lee, ldj0676@korea.ac.kr

Seokhie Hong, shhong@korea.ac.kr

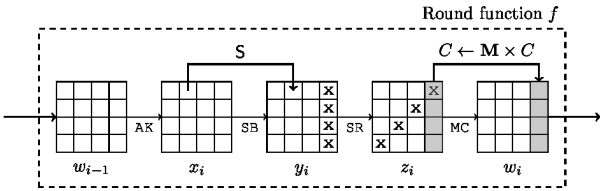
26.03.2024

Introduction

- **Our contribution**
  - The first key recovery attack on 5-round AES **using the multiple-of-8 property** : the overall complexity of recovering 32-bit partial key $\approx 2^{31.6}$
  - Not the best attack on 5-round AES, but it has the advantage of being **easily applicable** to other AES-like ciphers
  - Ongoing work : experimental results

The multiple-of-8 property for 5-round AES

- **AES**
  - Round function : AK∘MC∘SR∘SB
  - Additional AK on 0 round
  - No MC on last round



- **The multiple-of-8 property for 5-round AES**
  - Proposed at EUROCRYPT 2017 by Grassi, Rechberger and Rønjom [GRR17]
  - For the active diagonal structure, the number of inverse diagonal right pairs is always a multiple of 8
  - Key recovery attack has not been presented
  - Modified for key recovery attack to 4-round mixture differential cryptanalysis

Key recovery attack

- **Proposition**
  - If **exactly 8 pairs are found**, then for the 8 right pairs, **the difference is the same from after 1 round SB to before the 4 round SB**. (the value is the same from after 2 round SB to before 3 round SB) : can be proved by yoyo tricks or equations

- **Attack scenario**

1. **Find exactly 8 pairs** : 1 active diagonal structure and 2 inverse diagonal right pairs
   => The expected value is $2^{63} \cdot (2^{-32})^2 = 2^{-1}$ pairs
   - Due to the multiple-of-8 property, the probability of finding exactly 8 pairs is approximately 2^{-4}
   - For 1 active diagonal structure, it is possible to check $\binom{4}{2} = 6$ number of 2 inverse diagonal right pairs => need 3 structures
2. **Guess 0 round key 1 byte** : for the 8 right pairs, after 0 round ARK, there is only one key that makes all differences equal
   - 2 pairs are sufficient => $2^{32} \cdot 2^{-2} = 2^{30}$ elements of the structure are sufficient
   - Overall complexity $\approx 3 \cdot 2^{30} = 2^{31.6}$

Comparison with mixture differential cryptanalysis

- **Grassi's attack [Gra18] (using mixture differential cryptanalysis)**
  - Guess 0 round key, then **make mixture**
  - With made mixture, check guessed key is correct
  - The overall complexity of recovering **32-bit** partial key ≈ 2^{32}
- **Bar-On's attack [BDK+18] (using mixture differential cryptanalysis)**
  - **Find mixture** by using statistical analysis (**disadvantage to apply it to other ciphers**)
  - Find mixture, then find key
  - The overall complexity of recovering **24-bit** partial key ≈ 2^{22}
- **Our attack (using multiple-of-8 property)**
  - **Exactly 8 pairs are mixture** (**advantage to apply it to other ciphers**)
  - **Find mixture**, then find key
  - The overall complexity of recovering **32-bit** partial key ≈ $2^{31.6}$

Q&A

Thanks

KOREA UNIVERSITY

Cryptographic Algorithm Laboratory

Quiz Question 28

What was the issue with Wang *et al.*'s first MD5 collision?

A It required too much computation power

B They forgot the padding

C The endianness was wrong

D They forgot the feed-forward

Next Talk:
f5e2024 Lottery Ticket

f5e2024 Lottery Entry

Vukašin Karadžić
Technische Universität Darmstadt, Germany

f5e2024 Lottery Entry

Vukašin Karadžić
Technische Universität Darmstadt, Germany

```
00004e10: 6f20 3330 2030 2052 0a2f 4944 205b 3c43  o 30 0 R./ID [<C
00004e20: 4132 3332 3136 3431 3845 3733 3539 3141  A23216418E73591A
00004e30: 3146 3844 3641 4232 3643 3342 3033 393e  1F8D6AB26C3B039>
```

~~f5e2024 Lottery Entry~~

Vukašin Karadžić
Technische Universität Darmstadt, Germany

Rugged Pseudorandom Permutation (RPRP)

Rugged Pseudorandom Permutation (RPRP)

security notion for VIL tweakable ciphers

Rugged Pseudorandom Permutation (RPRP)

security notion for VIL tweakable ciphers

$$\text{PRP} \;<\; \textbf{RPRP} \;<\; \text{SPRP}$$

Rugged Pseudorandom Permutation (RPRP)

security notion for VIL tweakable ciphers

$$\text{PRP} < \textbf{RPRP} < \text{SPRP}$$

RPRP ciphers are more **efficient** than SPRP ciphers

Rugged Pseudorandom Permutation (RPRP)

security notion for VIL tweakable ciphers

$$\text{PRP} < \textbf{RPRP} < \text{SPRP}$$

RPRP ciphers are more **efficient** than SPRP ciphers

and

can do many things one can do with an SPRP-secure cipher:

AEAD + secure channels, onion encryption, ...?

ia.cr/2022/817 ia.cr/2023/1432

Quiz Question 29

Which ciphers do *not* have a backdoor?

A Skipjack

B Simon & Speck

C Dual_EC

D Streebog

Next Talk:
I want to win a prize

I want to win a prize

Michiel Verbauwhede

- I want to thank Tim Beyne and Addie Neyt for the 5 min discussion on this topic.
- I also want to thank the FSE2024 rump session program committee for my lack of sleep (and the of course fun challenge).
- And I can't forget to thank Marc Stevens. I don't know who you are, but without your `hashclash` tool this would have never been possible.

Quiz Question 30

What was the best talk in this rump session?

(Then, enter your name and submit your answers.)

Next Talk:
I want to win a prize

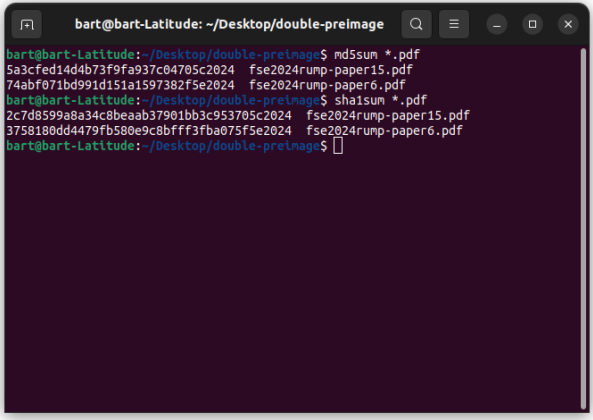
I want to win a prize

Michiel Verbauwhede

- I want to thank Tim Beyne and Addie Neyt for the 5 min discussion on this topic.
- I also want to thank the FSE2024 rump session program committee for my lack of sleep (and the of course fun challenge).
- And I can't forget to thank Marc Stevens. I don't know who you are, but without your `hashclash` tool this would have never been possible.

Rump Session Award Ceremony

Double “f5e2024” preimage award



Double “f5e2024” preimage award

- 1 double partial preimage of f5e2024
  Michiel Verbauwhede

Double "f5e2024" preimage award

- 1 double partial preimage of f5e2024
  Michiel Verbauwhede
- 1 double partial preimage of 705c2024
  Tim Beyne

Rump Session Award Ceremony

Double "f5e2024" preimage award

- 1 double partial preimage of f5e2024
  Michiel Verbauwhede
- 1 double partial preimage of 705c2024
  Tim Beyne
- 1 full SHA-1 preimage of
  f2f4f49a36044c35a65c15721ec1148dccc2b412

Rump Session Award Ceremony

Winner of the quiz

Rump Session Award Ceremony

Winner of the quiz

Best rump talk award