Welcome to the FSE 2023 Rump Session

Tetsu Iwata and Ling Song

March 22, 2023

The Rules

- Authors were allowed to submit talks of 1 up to 5 minutes in length
- Three categories: serious; serious-but-funny; joke
- Remote presentations are allowed
- Please respect the time
  - If your time is over, we will use …

The Prizes

- We will reward the best talk(s) according to the following metric: entertaining, informative, and musical

Statistics

- 10 submissions: 3 talks in Beijing; 7 talks in Kobe

1	Program Chair Report, Christina Boura, Bart Mennink, Kobe
2	News from the FSE steering committee, Anne Canteaut, Kobe
3	God save the Queen : Cryptanalysis of Elisabeth-4 - (work in progress), Henri Gilbert, Rachelle Heim Boissier, Jérémy Jean, Jean-René Reinhard, Kobe
4	AES-level secure PRF, Antonio Flórez-Gutiérrez, Gregor Leander, Ferdinand Sibleyras, Yosuke Todo, Kobe
5	CCA Security with Short Tags, Mustafa Khairallah, Kobe
6	STAP: Symmetric Techniques for Advanced Protocols, Léo Perrin, Kobe
7	The Third NIST Workshop on Block Cipher Modes of Operation 2023, Nicky Mouha, Kobe
8	New Records for RIPEMD-160 and SHA-256, Yingxin Li, Fukang Liu, Gaoli Wang, Beijing
9	British Tea Workshop, Andrew William Roscoe, Lei Wang, Beijing
10	The 10th Asian Workshop on Symmetric Key Cryptography (ASK 2023), Yaobin Shen and Ling Song, Beijing

Program Chair Report

Christina Boura, Bart Mennink

ToSC co-editors-in-chief

FSE 2023

IACR Transactions on Symmetric Cryptology (ToSC)

- **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 (evaluated at the next cycle)
  - Reject-and-resubmit (can resubmit after two cycles)
  - Reject (cannot resubmit in the next two cycles)
- **Regular, systematization of knowledge, addendum, and corrigendum papers**

ToSC Schedule

Submission:	ToSC Issue	Conference
...		
November $y-2$:	ToSC $y-1$ issue 1	
March $y-1$:	ToSC $y-1$ issue 2	FSE y (March y)
June $y-1$:	ToSC $y-1$ issue 3	
September $y-1$:	ToSC $y-1$ issue 4	
November $y-1$:	ToSC y issue 1	
March y:	ToSC y issue 2	FSE $y+1$ (March $y+1$)
June y:	ToSC y issue 3	
September y:	ToSC y issue 4	
November y:	ToSC $y+1$ issue 1	
March $y+1$:	ToSC $y+1$ issue 2	FSE $y+2$ (March $y+2$)
June $y+1$:	ToSC $y+1$ issue 3	
September $y+1$:	ToSC $y+1$ issue 4	
...		

ToSC Schedule

Submission:	ToSC Issue	Conference
...		
November 2020:	ToSC 2021 issue 1	
March 2021:	ToSC 2021 issue 2	FSE 2022 (March 2022)
June 2021:	ToSC 2021 issue 3	
September 2021:	ToSC 2021 issue 4	
November 2021:	ToSC 2022 issue 1	
March 2022:	ToSC 2022 issue 2	FSE 2023 (March 2023)
June 2022:	ToSC 2022 issue 3	
September 2022:	ToSC 2022 issue 4	
November 2022:	ToSC 2023 issue 1	
March 2023:	ToSC 2023 issue 2	FSE 2024 (March 2024)
June 2023:	ToSC 2023 issue 3	
September 2023:	ToSC 2023 issue 4	
...		

ToSC Schedule with COVID

Submission:	ToSC Issue	Conference
...		
November 2020:	ToSC 2021 issue 1	
March 2021:	ToSC 2021 issue 2	FSE 2022 (March 2022)
June 2021:	ToSC 2021 issue 3	FSE 2022 (March 2022)
September 2021:	ToSC 2021 issue 4	
November 2021:	ToSC 2022 issue 1	
March 2022:	ToSC 2022 issue 2	FSE 2023 (March 2023)
June 2022:	ToSC 2022 issue 3	
September 2022:	ToSC 2022 issue 4	
November 2022:	ToSC 2023 issue 1	
March 2023:	ToSC 2023 issue 2	FSE 2024 (March 2024)
June 2023:	ToSC 2023 issue 3	
September 2023:	ToSC 2023 issue 4	
...		

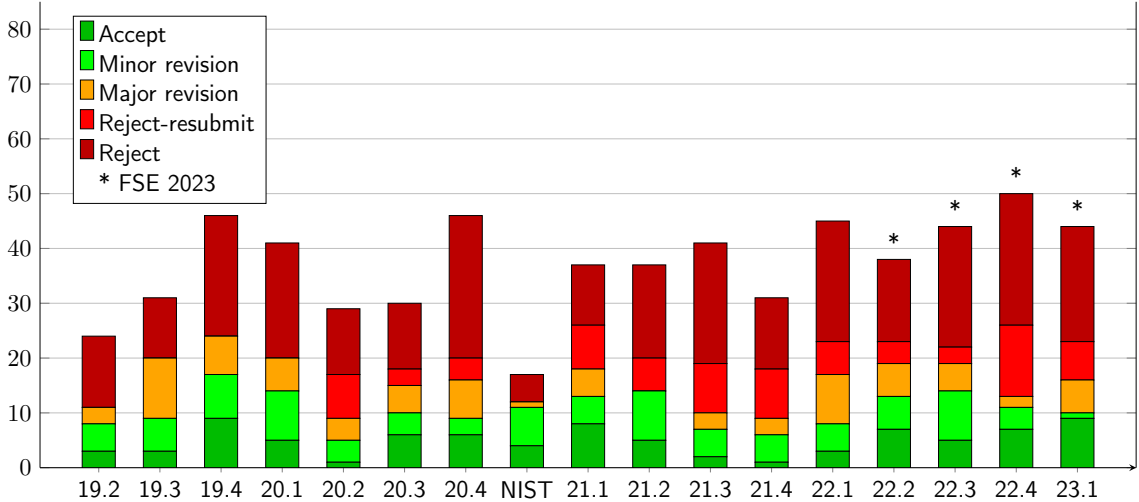
ToSC Schedule with COVID but Going Back to Normal

Submission:	ToSC Issue	Conference
...		
November 2020:	ToSC 2021 issue 1	
March 2021:	ToSC 2021 issue 2	FSE 2022 (March 2022)
June 2021:	ToSC 2021 issue 3	FSE 2022 (March 2022)
September 2021:	ToSC 2021 issue 4	
November 2021:	ToSC 2022 issue 1	
March 2022:	ToSC 2022 issue 2	FSE 2023 (March 2023)
June 2022:	ToSC 2022 issue 3	
September 2022:	ToSC 2022 issue 4	
November 2022:	ToSC 2023 issue 1	
March 2023:	ToSC 2023 issue 2	FSE 2024 (March 2024)
June 2023:	ToSC 2023 issue 3	
September 2023:	ToSC 2023 issue 4	
...		

FSE 2023 Program

- 48 papers from ToSC 2022(2-4), and 2023(1)
- 2 Invited talks
  - Siwei Sun
  - Yosuke Todo
- Rump Session
  - Chairs: Tetsu Iwata and Ling Song

Decision Statistics



Decision Statistics

- 184 regular submissions for ToSC 2022(2-4), and 2023(1)
  - 26% accepted (48 papers)

- Major revision papers often return to ToSC
- For last 4 issues:
  - 21 major revisions resubmitted
  - 19 major revision decisions

- Around 50% of reject-and-resubmit papers return to ToSC
- For last 4 issues:
  - 13 reject-and-resubmits resubmitted
  - 27 reject-and-resubmit decisions

- SoK/addendum/corrigendum: only 2/0/0 submissions (1/0/0 accepted)

Program Committee (2022)

- Tomer Ashur
- Subhadeep Banik
- Zhenzhen Bao
- Xavier Bonnetain
- Itai Dinur
- Christoph Dobraunig
- Avijit Dutta
- Henri Gilbert
- Lorenzo Grassi
- Vincent Grosso
- Jian Guo
- Akinori Hosoyamada
- Takanori Isobe
- Ryoma Ito
- Tetsu Iwata
- Ashwin Jha
- Jooyoung Lee
- Gaëtan Leurent
- Yunwen Liu
- Stefan Lucks
- Cuauhtemoc Mancillas-López
- Silvia Mella
- Florian Mendel
- Kazuhiko Minematsu
- Nicky Mouha
- Léo Perrin
- Thomas Peyrin
- Yann Rotella
- Dhiman Saha
- Yu Sasaki
- André Schrottenloher
- Yannick Seurin
- Leonie Simpson
- Hadi Soleimany
- Ling Song
- Meltem Sönmez Turan
- Siwei Sun
- Tyge Tiessen
- Aleksei Udovenko
- Gilles Van Assche
- Damian Vizár
- Qingju Wang
- Friedrich Wiemer

Thank You

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

- General chairs (Beijing): Bin Zhang, Meiqin Wang
- General chairs (Kobe): Takanori Isobe, Fukang Liu
- Virtual conference organizers: Kevin McCurley, Kay McKelly
- FSE steering committee:
  - Anne Canteaut, chair
  - Itai Dinur
  - Orr Dunkelman
  - Tetsu Iwata
  - Gregor Leander
  - Florian Mendel
  - María Naya-Plasencia
  - Thomas Peyrin
  - Bart Preneel
  - Yu Sasaki

Best Paper Award

- Elected two best papers for ToSC 2022(2-4) and 2023(1)

FSE 2023
Best Paper Award

Yosuke Todo and Takanori Isobe

Hybrid Code Lifting on Space-Hard Block Ciphers – Application to Yoroi and SPNbox

Christina Boura and Bart Mennink
Program Co-Chairs

FSE 2023
Best Paper Award

Thomas Peyrin and Quan Quan Tan

Mind Your Path: on (Key) Dependencies in Differential Characteristics

Christina Boura and Bart Mennink
Program Co-Chairs

News from the FSE steering committee

Anne Canteaut

Inria, Paris, France

March 22, 2023

Test-of-Time Awards

FSE Test-of-Time Awards

The FSE Test-of-Time Award is given in year X to honor a paper presented at FSE in year X-15 which has had a lasting impact on the field.

Eligible papers.

Nominations are possible but not mandatory.

This year.

3 awards corresponding to papers presented at FSE 2006, FSE 2007 and FSE 2008.

FSE 2021 Test-of-Time Award

Papers from FSE 2006

Committee.

- Orr Dunkelman, chair
- Matt Robshaw (chair of FSE 2006)
- Gaëtan Leurent (chair of FSE 2021)
- María Naya Plasencia
- Thomas Peyrin

FSE 2021
Test of Time Award

Tetsu Iwata

New Blockcipher Modes of Operation with Beyond the Birthday Bound Security

Published at FSE 2006

Orr Dunkelman, chair of the Test-of-Time award committee

FSE 2022 Test-of-Time Award

Papers from FSE 2007

Committee.

- Bart Mennink, chair
- Alex Biryukov (chair of FSE 2007)
- Itai Dinur (chair of FSE 2022)
- Yu Sasaki
- Florian Mendel

FSE 2022
Test of Time Award

Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, Tetsu Iwata

The 128-bit Blockcipher CLEFIA

Published at FSE 2007

Bart Mennink, chair of the Test-of-Time award committee

FSE 2023 Test-of-Time Award

Papers from FSE 2008

Committee.

- Tetsu Iwata, chair
- Kaisa Nyberg (chair of FSE 2008)
- Christina Boura (chair of FSE 2023)
- Gregor Leander
- Bart Preneel

FSE 2023
Test of Time Award

Huseyin Demirci and Ali Aydin Selçuk

A Meet-in-the-Middle Attack on 8-Round AES

Published at FSE 2008

Tetsu Iwata, chair of the Test-of-Time award committee

Thanks to our General Chairs
and Program Chairs

Many thanks to Bin Zhang and Meiqin Wang

The International Association For Cryptologic Research Gratefully Acknowledges

Bin Zhang

For his contribution to the worldwide cryptologic community through his role as General Chair of FSE 2023

Anne Canteaut, chair of the steering committee

Many thanks to Bin Zhang and Meiqin Wang

The International Association For Cryptologic Research Gratefully Acknowledges

Meiqin Wang

For her contribution to the worldwide cryptologic community through her role as General Chair of FSE 2023

Anne Canteaut, chair of the steering committee

Many thanks to Takanori Isobe and Fukang Liu

The International Association For Cryptologic Research Gratefully Acknowledges

Takanori Isobe

For his contribution to the worldwide cryptologic community through his role as General Chair of FSE 2023

Anne Canteaut, chair of the steering committee

Many thanks to Takanori Isobe and Fukang Liu

The International Association For Cryptologic Research Gratefully Acknowledges

Fukang Liu

For his contribution to the worldwide cryptologic community through his role as General Chair of FSE 2023

Anne Canteaut, chair of the steering committee

Many thanks to Christina Boura and Bart Mennink

Renewal of the FSE Steering Committee

FSE Steering Committee

- Anne Canteaut, France, chair
- Bart Preneel, Belgium, IACR Board representative
- Christina Boura, France, EiC ToSC 22/23
- Itai Dinur, Israel, EiC ToSC 21/22
- Orr Dunkelman, Israel
- Tetsu Iwata, Japan
- Gregor Leander, Germany
- Gaëtan Leurent, France
- Florian Mendel, Austria
- Bart Mennink, NL, EiC ToSC 21/22
- Kazuhiko Minematsu, Japan, EiC ToSC 23/24
- Maria Naya Plasencia, France
- Thomas Peyrin, Singapore
- Yu Sasaki, Japan

Send nominations for new members by May 31 to Anne.Canteaut@inria.fr

FSE 2024

25-29.03.2024

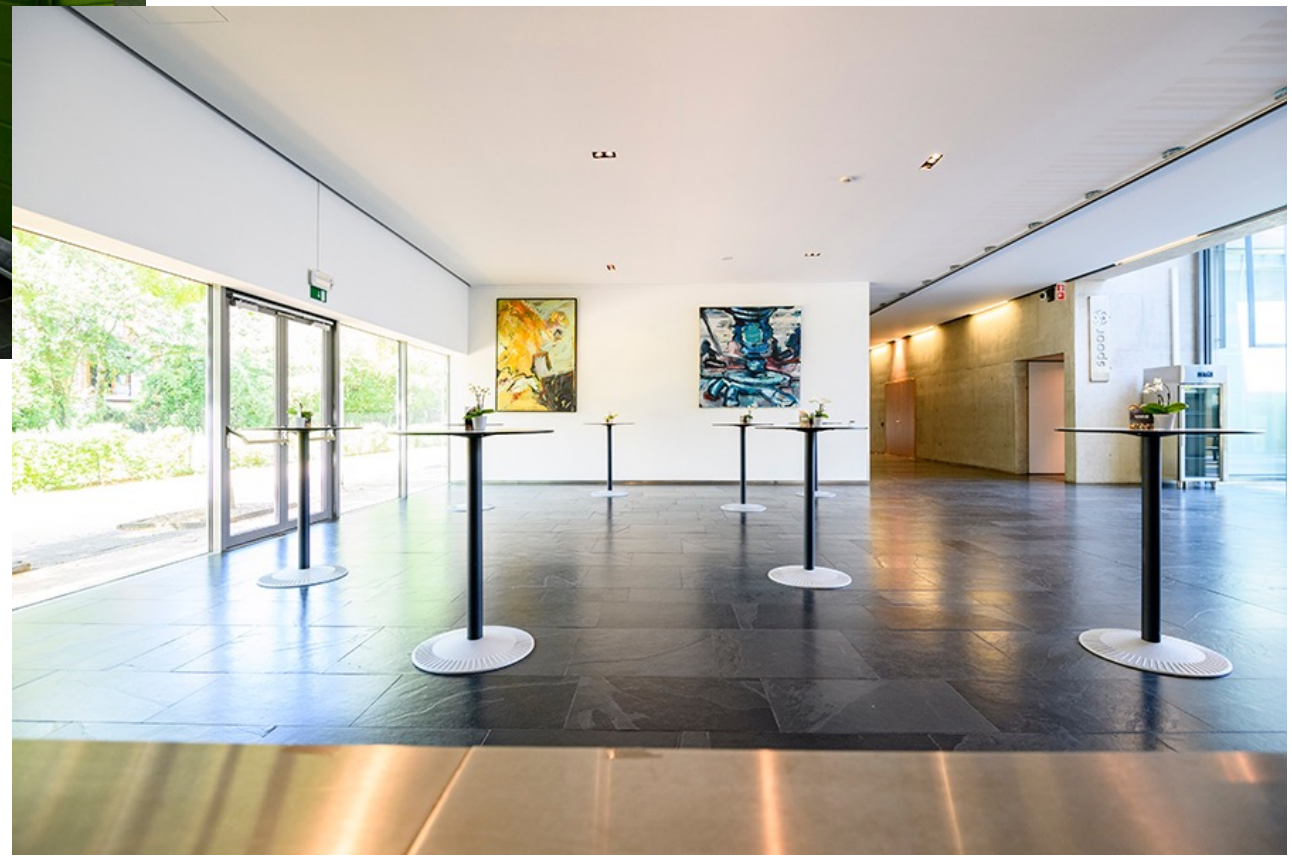
Leuven, Belgium

General chairs: Svetla Nikova and Siemen Dhooghe

COSIC, KU Leuven

FSE 2024 in Leuven

- Venue: Province house in Leuven – at Leuven Station
  https://www.vlaamsbrabant.be/nl/over-de-provincie/provinciehuis



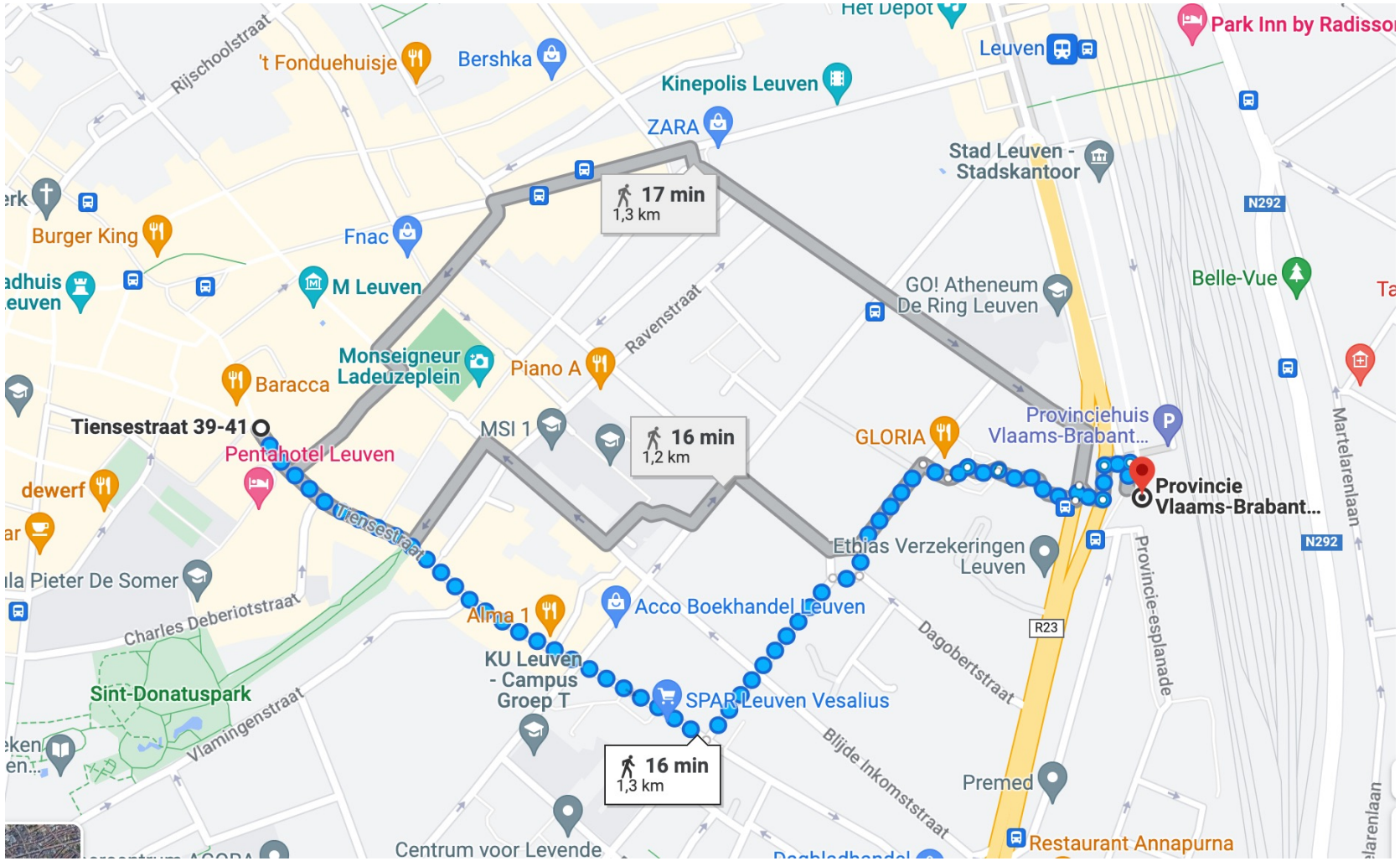
FSE venue - about 10-15 min from center of Leuven

Hotels close to the venue and in the center of Leuven

Leuven is easy to access by train from the main train stations in Europe

Flights to Brussels airport from all continents.

Leuven easy accessible by train from Brussels airport (20 min)



FSE 2025?

Looking for volunteers for FSE 2025

Thank you!

God save the Queen : Cryptanalysis of `Elisabeth-4`

(work in progress)

Henri Gilbert, Rachelle Heim Boissier, Jérémy Jean, Jean-René Reinhard

ANSSI, UVSQ

FSE 2023 - Rump session

Introduction

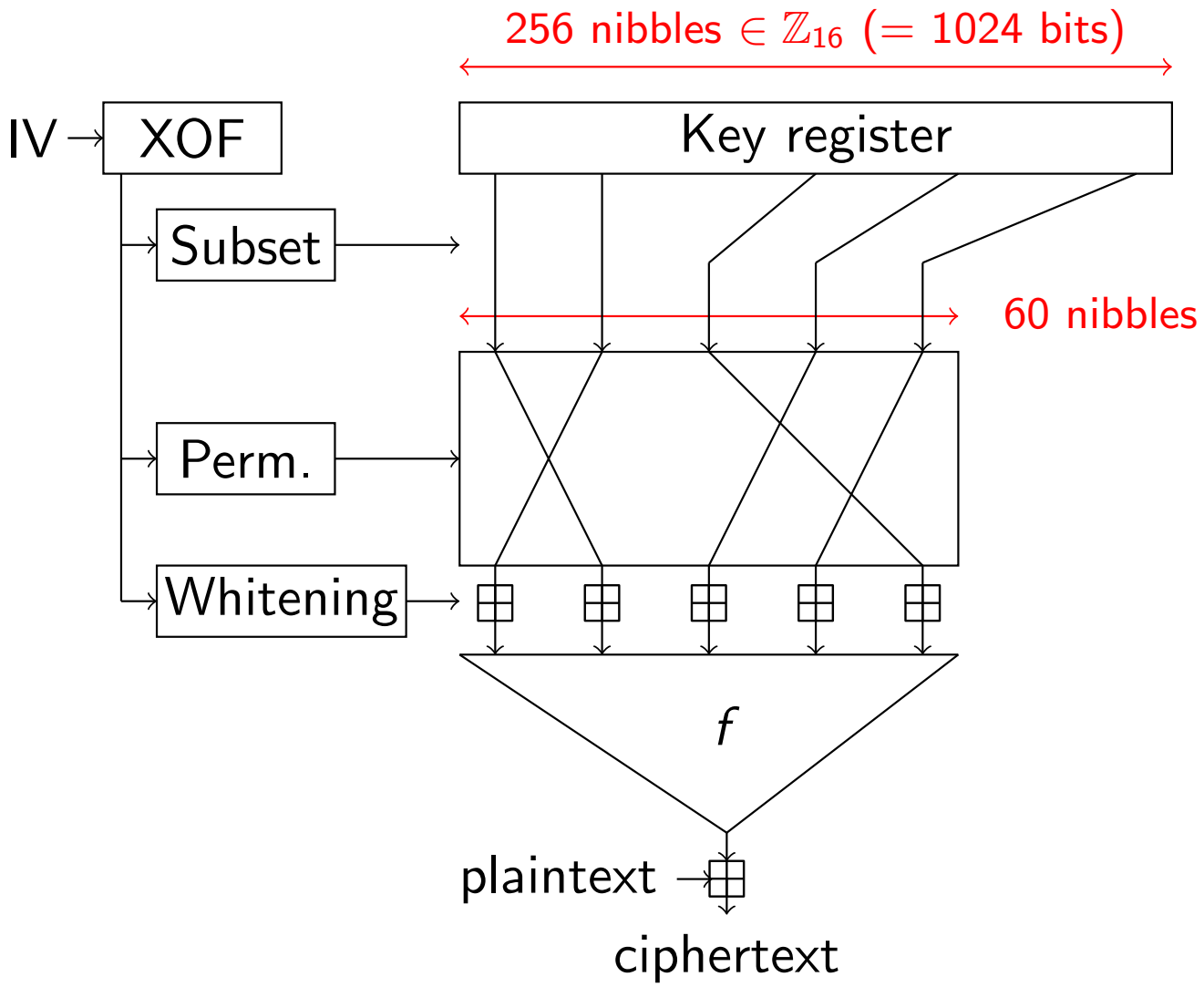
About `Elisabeth-4`

- Stream cipher published at ASIACRYPT 2022
- Designed by Cosseron, Hoffman, Méaux, Standaert
- Optimised for Hybrid Homomorphic Encryption (HHE) use cases
- 128-bit security claim

Our contribution

- Full break of `Elisabeth-4`: an optimised linearisation attack of complexity $\approx 2^{90}$
- Ongoing work: analysis of HHE-dedicated features

Overall construction of Elisabeth-4

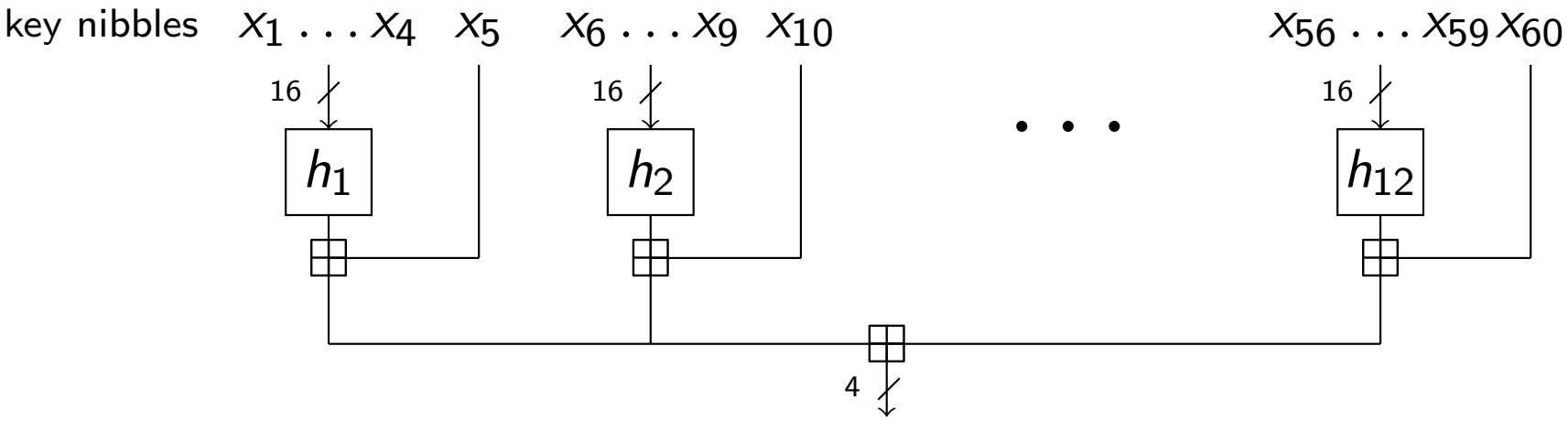


Basic linearisation attack in $\mathbb{F}_2$

Linearisation

- collect linear equations, the variables are monomials in the key bits
- solve the linear system

Overall structure of one application of the masked filter

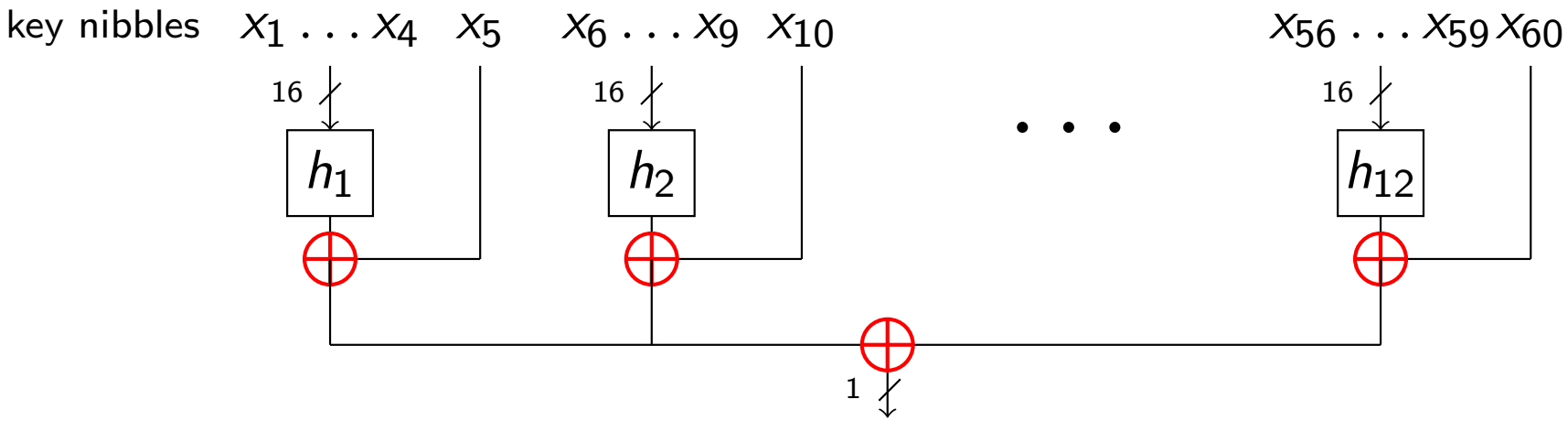


Basic linearisation attack in $\mathbb{F}_2$

Linearisation

- collect linear equations, the variables are monomials in the key bits
- solve the linear system

Overall structure of one application of the masked filter



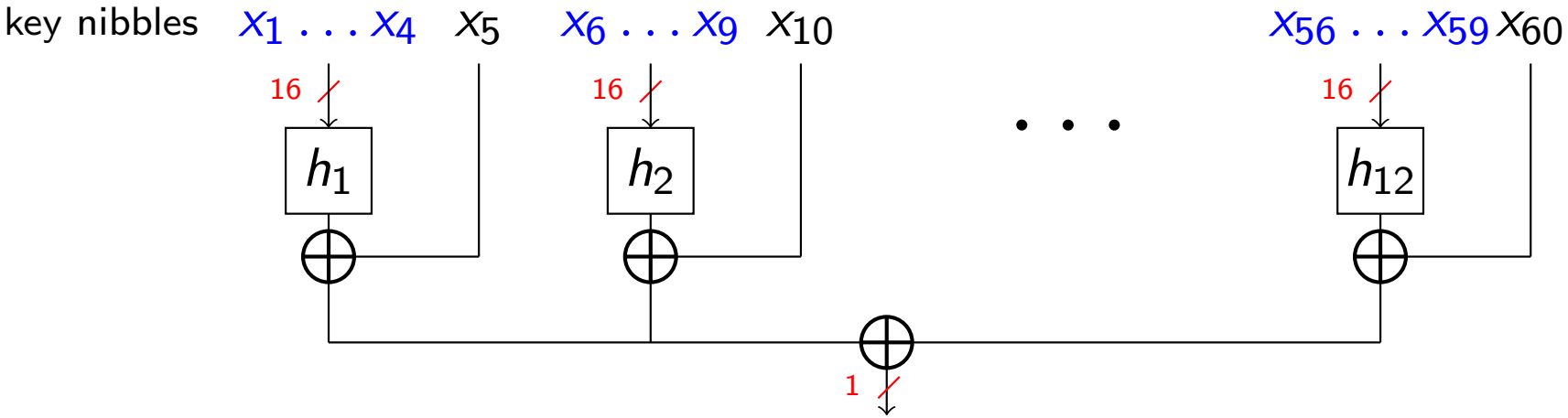
We focus on the **LSB of the output nibble**
$\rightarrow$ On the LSB, the addition in $\mathbb{Z}_{16}$ is a XOR

Basic linearisation attack in $\mathbb{F}_2$

Linearisation

- collect linear equations, the variables are monomials in the key bits
- solve the linear system

Overall structure of one application of the masked filter



Total number of monomials in the system

$$\text{At most } \mu = \binom{256}{4} 2^{16} \quad \longrightarrow \quad \mathrm{T} = \mu^3 \approx 2^{131}$$

A handful of improvements

Exploiting the sparsity of the linear system

- Using Block Wiedemann

Impact of HHE-dedicated features

- Two main ingredients in h:
  - Additions over $\mathbb{Z}_{16}$
  - *Negacyclic* S-boxes: $S[x+8] = -S[x]$
- Their interaction causes rank defects

Precomputation-based trade-offs

- Example: filtering IVs so that all (quartets of) nibbles are taken from the first half of the key

Rough complexity estimates

Precomputation phase:

- Time: $\approx 2^{85}$ operations
- Memory complexity: $\approx 2^{53}$ bits

Linearisation phase:

- Time: $\approx 2^{90}$ operations
- Data complexity: $\approx 2^{37}$ bits

Rough complexity estimates

Precomputation phase:

- Time: $\approx 2^{85}$ operations
- Memory complexity: $\approx 2^{53}$ bits

Linearisation phase:

- Time: $\approx 2^{90}$ operations
- Data complexity: $\approx 2^{37}$ bits

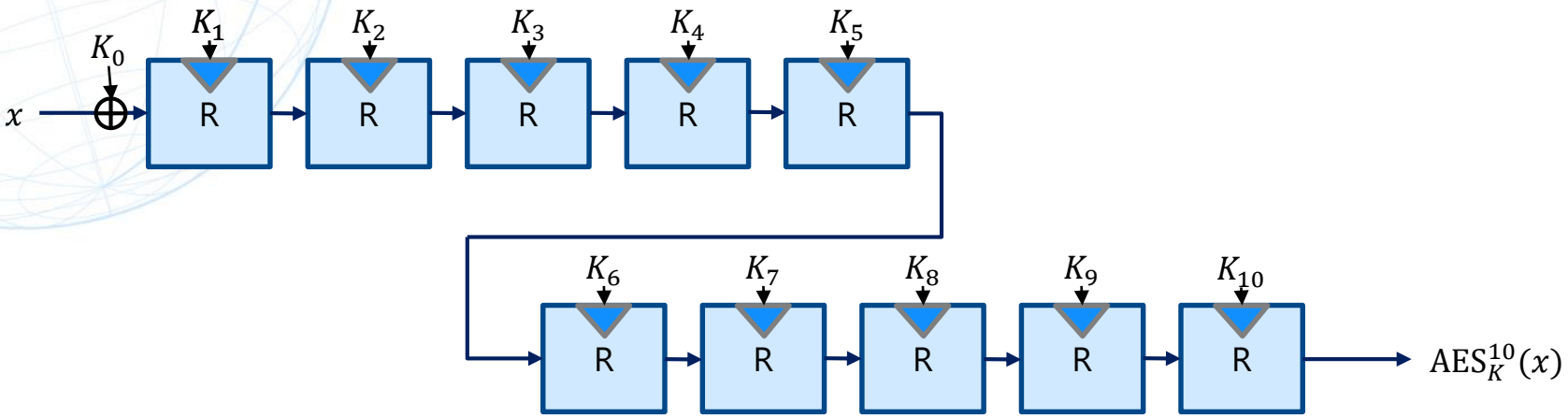
Thank you for your attention!

AES-level secure PRF

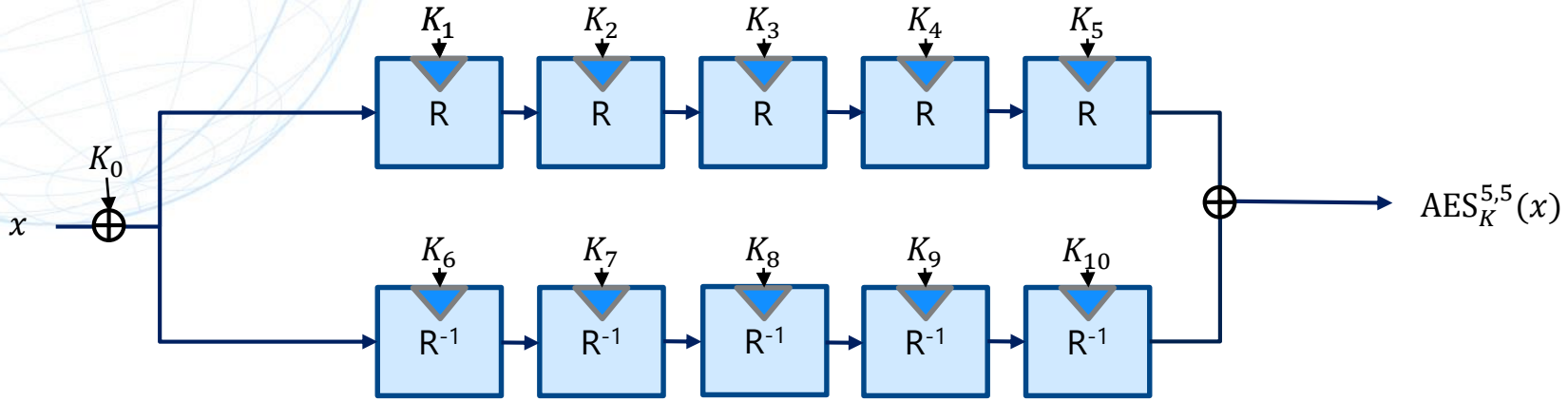
Antonio Flórez-Gutiérrez, Gregor Leander, Ferdinand Sibleyras, Yosuke Todo

March 22, FSE 2023

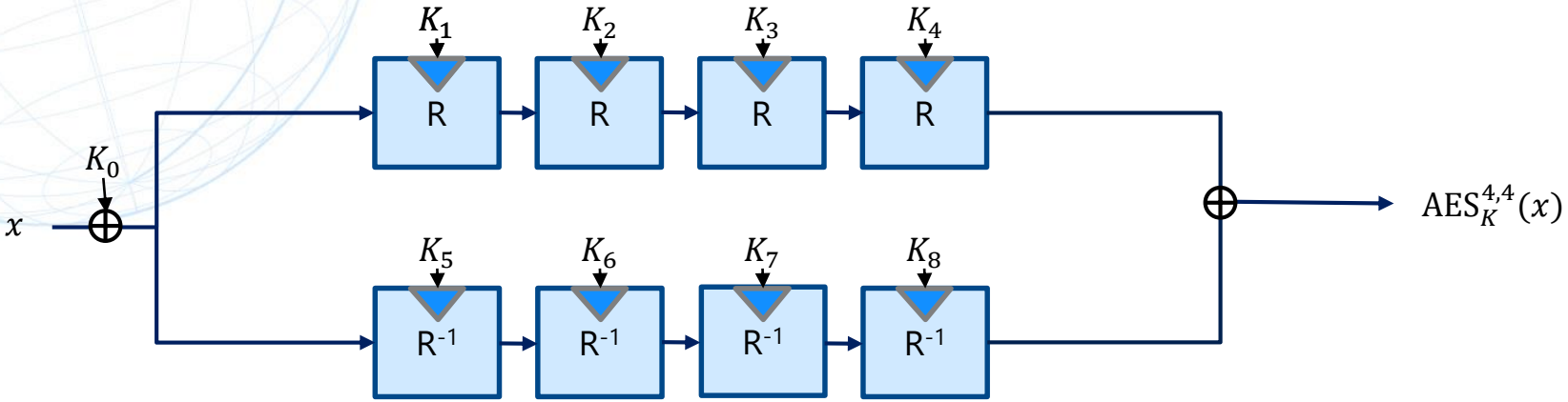
10 rounds of AES

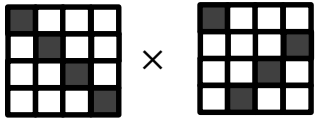


$5 + 5 = 10$!!!


K_1
K_2
K_3
K_4
K_5
R
R
R
R
R
K_0
x
K_6
K_7
K_8
K_9
K_{10}
R-1
R-1
R-1
R-1
R-1
$\mathrm{AES}_K^{5,5}(x)$

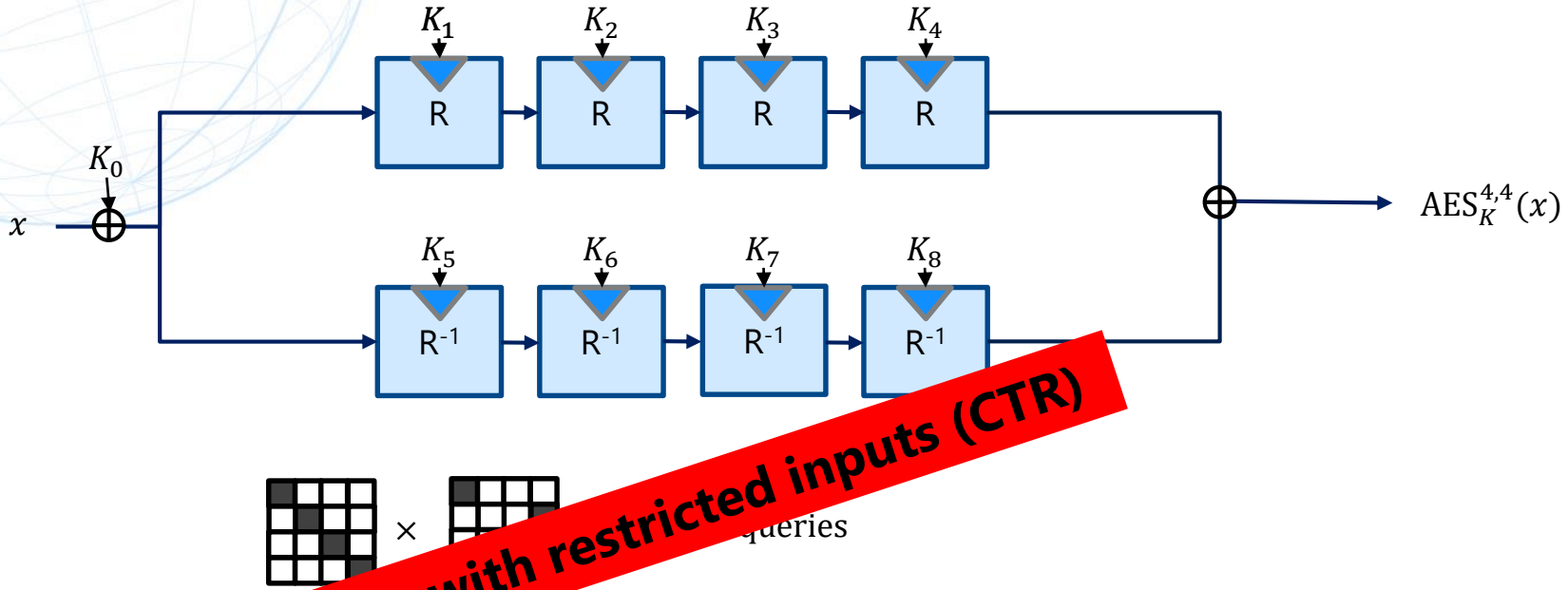
$4 + 4 \neq 8$ rounds => Integral²





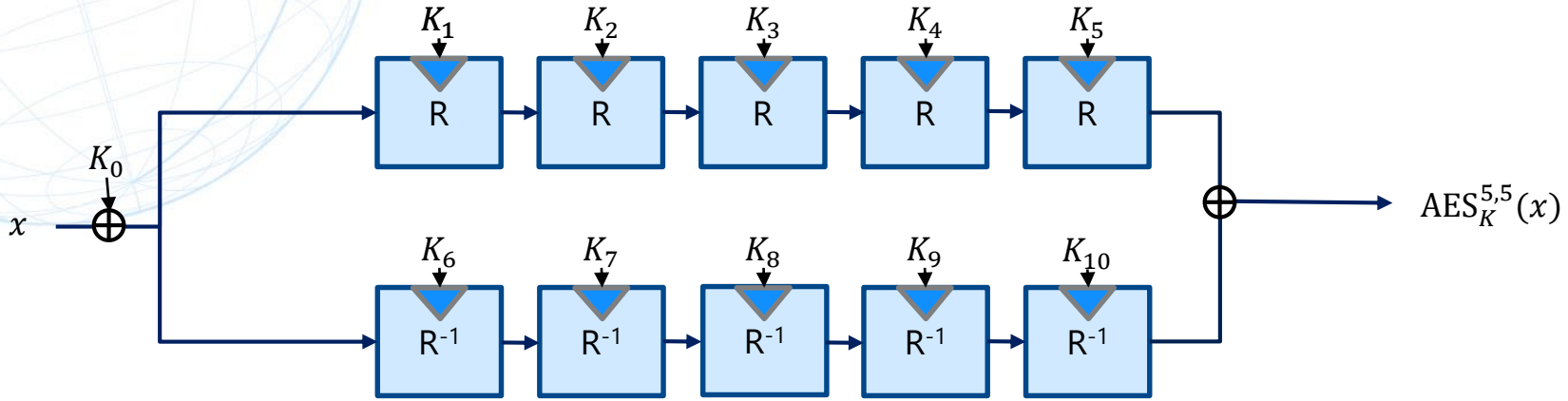
$\Rightarrow 2^{48}$ queries

$4 + 4 \neq 8$ rounds => Integral²

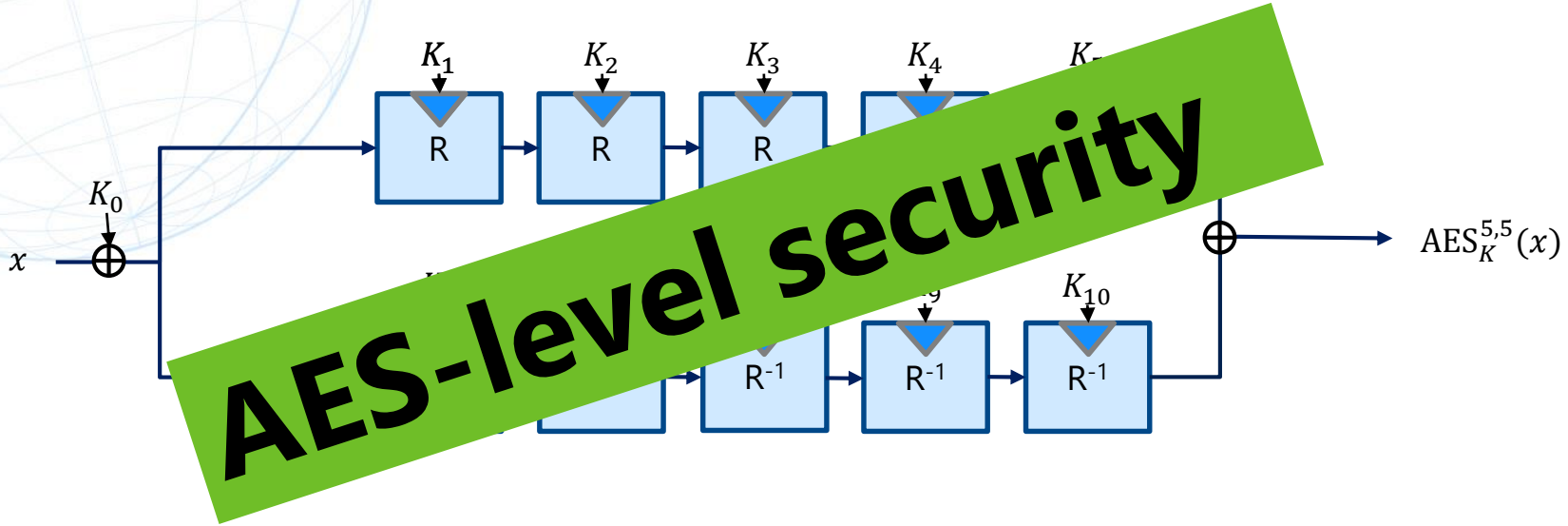


Not applicable with restricted inputs (CTR)

$5 + 5 = 10$!!!


K_1
K_2
K_3
K_4
K_5
R
R
R
R
R
K_0
x
K_6
K_7
K_8
K_9
K_{10}
R-1
R-1
R-1
R-1
R-1
$\mathrm{AES}_K^{5,5}(x)$

$5 + 5 = 10$!!!


K_1
K_2
K_3
K_4
K_{10}
K_0
x
R
R
R
R-1
R-1
R-1
$\mathrm{AES}_K^{5,5}(x)$
AES-level security

CCA Security with Short Tags

Mustafa Khairallah

March 21, 2023

IND-CCA with Short Tags

- This is not a new problem.
- Bellare and Nemprempre, 2000, showed that given a CCA adversary $\mathbf{A}$, we can build two adversaries $\mathbf{B}$ and $\mathbf{C}$ such that,

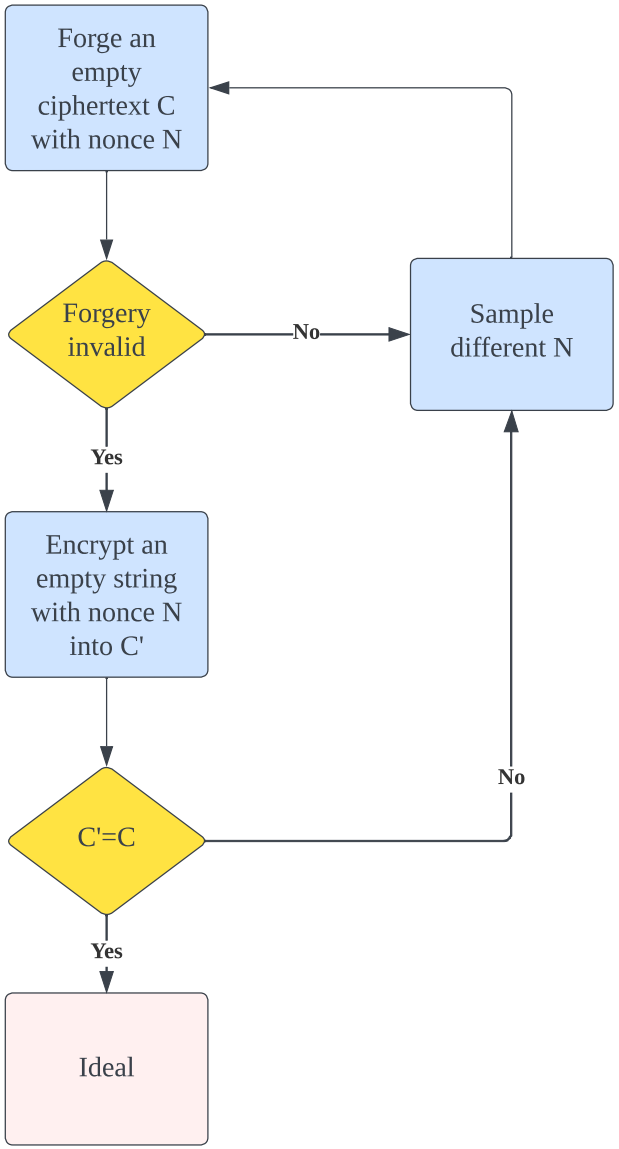
$$\mathbf{Adv}_{\Pi}^{\mathtt{cca}}(\mathbf{A}) \leq \mathbf{Adv}_{\Pi}^{\mathtt{cpa}}(\mathbf{B}) + 2\mathbf{Adv}_{\Pi}^{\mathtt{int-ctxt}}(\mathbf{C})$$

- The topic was revived in discussions during the NIST LWC project, through an attack on schemes with short tags proposed by Alexandre Mège.
- Khairallah 2022 analyzed this attack on online AE schemes, showing that indeed the second term of the bound above is almost tight, then he also showed it is almost tight (up to a log factor) for COFB, which uses 128-bit tag and has 58-bit INT-CTXT security, with a CCA attack with 2^{64} forgery attempts.

IND-CCA with Short Tags II

- Hosoyamada et al, 2022, showed a similar attack on online AE, they also showed an IND-CCA attack on Rocca with 2^{128} complexity. (IND-CPA security is 256 bits).
- They also showed that it is possible to design a scheme with 128-bit INT-CTXT security and 256-bit IND-CCA security.
- The scheme uses Encode-then-Encipher (EtE):
  - The plaintext is restricted to 128-bit strings and the ciphertext length is 256 bits.
  - The message is encoded as $M||0^{128}$ and encrypted using a 256-bit TBC, where the nonce is used as tweak.
- To generalize this scheme, we require an expensive variable length enciphering scheme.

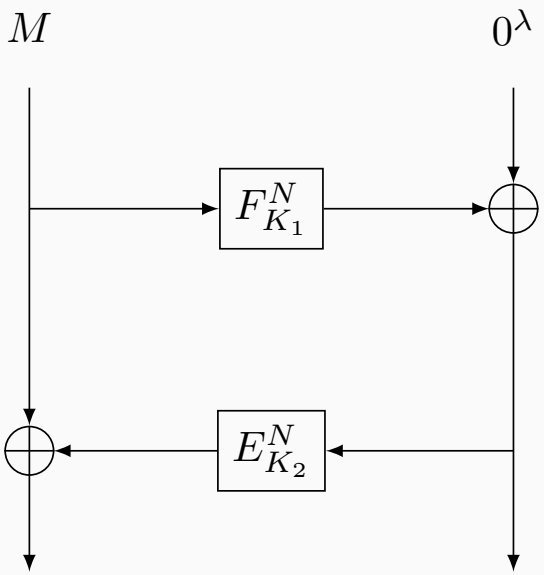
Generalizing with arbitrary messages is infeasible

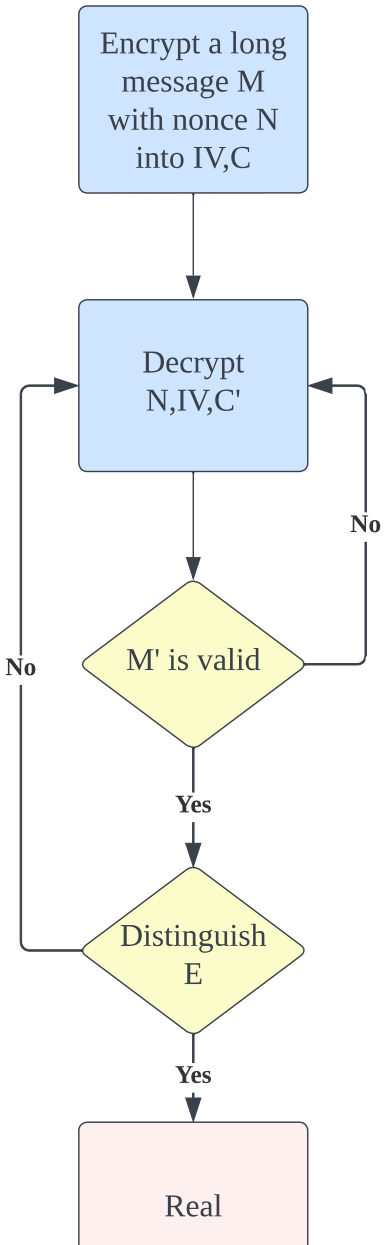


- We expect such collision inthe ideal world after roughly 2^{λ}.
- In general, we can show that any Pseudo-Random Injection (PRI) is IND-CCA secure up to at most $2^{s+\lambda}$ forgeries, where s is the minimum plaintext length.
- Similar bound was found by Rogaway and Shrimpton when comparing PRI to Deterministic AE (DAE).

What is the tightness of offline encryption schemes?

- SIV was proposed by Rogaway and Shrimpton in 2006.
- If E is online, the decryption is partially online.





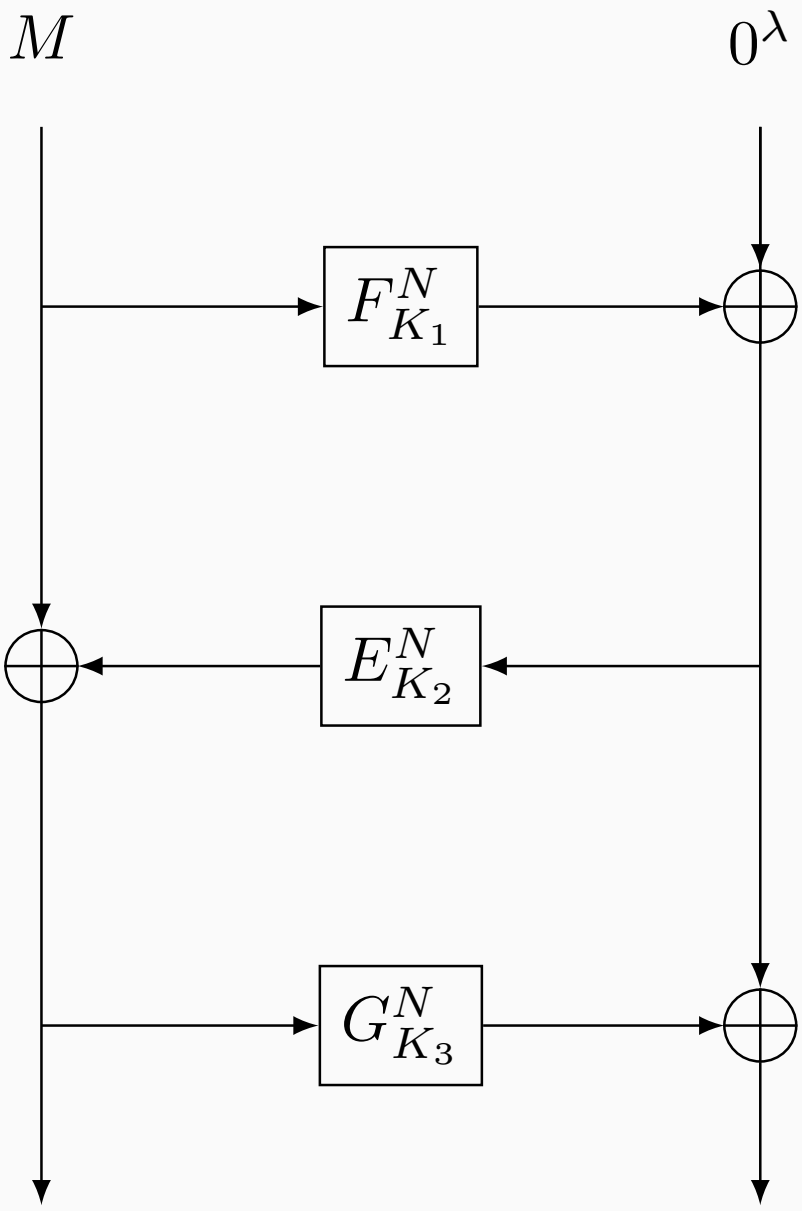
Lessons

1. If the tag size is fixed and small, the plaintext must have a minimum length.
2. If IV-based IND-CCA-insecure encryption is used, IV cannot be controllable by the adversary during decryption.

RIV

- Proposed by Farzaneh Abed, Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel in 2016.
- Its goal is to provide security with release of unverified plaintext.
- Its nonce-respecting variant should remain IND-CCA secure with short tags, up to double the tag size.

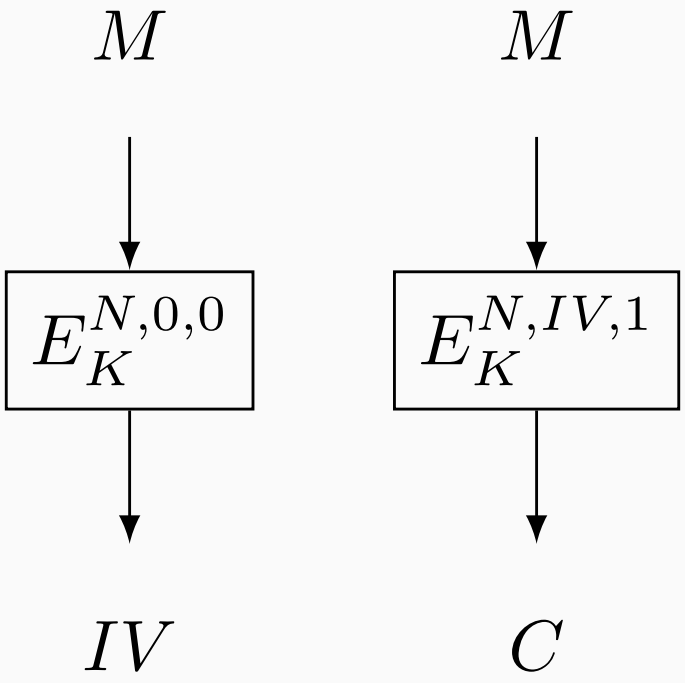
RIV



- The idea is that the attacker needs to satisfy two conditions on two λ bit values simultaneously to be able to break PRI security of the underlying encryption scheme:
  1. The adversary needs a collision on the nonce-IV pair during the decryption.
  2. If such collision occurs, the MAC of the unverified plaintext must collide with the MAC of the plaintext in the colliding encryption query.
- Optimal case is $s = \lambda$, with 2λ IND-CCA security.

Optimizing Hosoyamada et al.'s scheme with large tweaks

- The scheme uses a single call to a 256-bit TBC with t-bit tweak.
- This is a potential idea to use 128-bit TBC with $t + 129$-bit tweak.



May also use t-bit tweak but the construction is more complex with more calls.

Thanks

STAP

Symmetric Techniques for Advanced Protocols

Léo Perrin[1]

[1]Inria, France

leo.perrin@inria.fr

Financed by the ERC StG ReSCALE

FSE 2023

Why would anyone want symmetric primitives over $\mathbb{F}_p$?
What do we need to know when working on this?

https://who.paris.inria.fr/Leo.Perrin/rescale/stap-23.html

Why would anyone want symmetric primitives over $\mathbb{F}_p$?
What do we need to know when working on this?

Answers, and more, will be given at **STAP'23**!

https://who.paris.inria.fr/Leo.Perrin/rescale/stap-23.html

Why would anyone want symmetric primitives over $\mathbb{F}_p$?
What do we need to know when working on this?

Answers, and more, will be given at **STAP'23**!

Where? Lyon, France

When? 22nd and 23rd of April (before EC'23)

How? Sign up when registering for EC

https://who.paris.inria.fr/Leo.Perrin/rescale/stap-23.html

Why would anyone want symmetric primitives over $\mathbb{F}_p$?
What do we need to know when working on this?

Answers, and more, will be given at **STAP'23**!

Where? Lyon, France

When? 22nd and 23rd of April (before EC'23)

How? Sign up when registering for EC

Invited talks/discussions on:

Algebraic attacks, STARKs, permutations over $\mathbb{F}_p$, arithmetization, side-channel resilience, FHE, symmetric design, standardization...

`https://who.paris.inria.fr/Leo.Perrin/rescale/stap-23.html`

The Third NIST Workshop on Block Cipher Modes of Operation 2023

October 3-4, 2023, at National Cybersecurity Center of Excellence (Rockville, Maryland)

Purpose:

- Address limitations of NIST block cipher modes of operation (See NIST SP 800-38 series and NISTIR 8459)
- Discuss possibility of standardizing a tweakable wide encryption technique

Topics include:

- Security and efficiency of current modes
- Additional security features (e.g., misuse resistance, key commitment) desirable in new encryption technique
- Case studies for specific uses, such as storage and key wrapping
- Security and efficiency of tweakable encryption techniques

The Third NIST Workshop on Block Cipher Modes of Operation 2023

Important dates:

- Submission deadline: July 1, 2023
- Notification: July 30, 2023
- Workshop: October 3-4, 2023

Links:

- Event: https://csrc.nist.gov/Events/2023/third-workshop-on-block-cipher-modes-of-operation
- Forum: ciphermodes-forum@list.nist.gov (https://groups.google.com/a/list.nist.gov/g/ciphermodes-forum)
- Contact e-mail: ciphermodes@nist.gov

New Records in Collision Attacks on RIPEMD-160 and SHA-256

Yingxin Li[1],Fukang Liu[2,3], Gaoli Wang[1]

[1]East China Normal University
[2]Tokyo Institute of Technology
[3]University of Hyogo

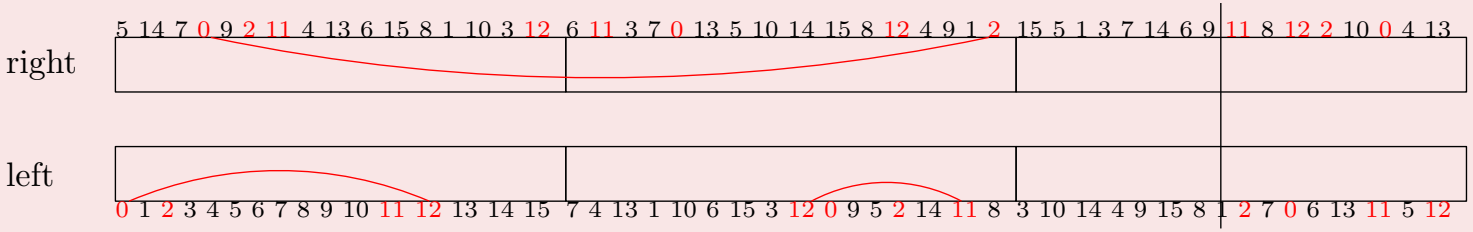
March 2023

Our results on RIPEMD-160 and SHA-256

- The first practical collision for $\{40/80\}$ steps of RIPEMD-160.
- The first practical SFS collision for $\{39/64\}$ steps of SHA-256.

Local collisions for 40-step RIPEMD-160

Injecting differences in the new message words $(m_0, m_2, m_{11}, m_{12})$



The differential trail for 40-step RIPEMD-160

i	ΔX_i	m_l^i	i	ΔY_i	m_r^i
−5	==========		−5	==========	
−4	==========		−4	==========	
−3	==========		−3	==========	
−2	==========		−2	==========	
−1	==========		−1	==========	
0	unnn==========	0	0	==========	5
1	==========nuuuu=n==========	1	1	==========	14
2	u=uun=u==========n==u====un=nnnn	2	2	==========0==========	7
3	=====nnn===unun==u==u====nn=====	3	3	0==u==========	0
4	u=u==uu==u==========n=nu	4	4	0====1==========0==1=n==1===010	9
5	==========nuuu=n======u=n=====	5	5	101====u==0=00=1===0000=100u0000	2
6	==u====nuu==========	6	6	0110=1===nnuu1nuuuuuuuuu10100=0	11
7	==========unnnnnnnnnn=====	7	7	1unnnnn11000unn00unn10nunn11=110	4
8	==========	8	8	=1011nu001nu111nuu=unnn0101nuuuu	13
9	==========	9	9	00u==nu00u010===1000101u=0101n0=	6
10	==========	10	10	111====0==u=n10=0u01=1n01=010==1	15
11	==========	11	11	0=0=n1=0=10n0===u====n1=1===0===	8
12	==========	12	12	11u===10=0=1u=0======1==0=1u===0	1
13	==========	13	13	==0======1==0=n=10=0====1=10===n	10
14	==========	14	14	==1====0========u1=1==========u	3
15	==========	15	15	=======1=n==========n=======	12
16	==========	7	16	==========u==	6
17	==========	4	17	==========	11
18	==========	13	18	==========	3
19	==========	1	19	==========0==========	7
20	==========	10	20	==========1==========	0
21	==========	6	21	==========u==========	13
22	==========	15	22	==========	5
23	==========	3	23	==========1==========	10
24	=========n==========	12	24	==========1==========010000=	14
25	==u======0==========	0	25	=u==========111111=	15
26	==0==========1	9	26	==========nuuuuu==========	8
27	==========1=======	5	27	======1==========	12
28	==========	2	28	======0==========	4
29	==========	14	29	==========	9
30	==========	11	30	==========	1
31	==========	8	31	==========	2
32	==========	3	32	==========	15
33	==========	10	33	==========	5
34	==========	14	34	==========	1
35	==========	4	35	==========	3
36	==========	9	36	==========	7
37	==========	15	37	==========	14
38	==========	8	38	==========	6
39	==========	1	39	==========	9

$Y_{15}[10] = Y_{14}[10]$, $Y_{15}[27] = Y_{14}[27]$, $Y_{16}[10] = Y_{15}[10]$, $Y_{16}[25] = Y_{15}[25]$
$Y_{17}[0] = Y_{16}[0]$, $Y_{17}[17] = Y_{16}[17]$, $Y_{18}[12] = Y_{17}[12]$, $Y_{23}[30] = Y_{22}[30]$,
$Y_{27}[8] = Y_{26}[8]$, $Y_{28}[i] = Y_{27}[i] (i \in \{21, 22, 23, 24, 26\})$
$X_{23}[22] = X_{22}[12]$, $X_{24}[29] = X_{23}[19]$

The colliding message pair for 40-step RIPEMD-160

The colliding message pair $(M_0||M_1, M_0||M_1')$

M_0	4b1de304	f52a5a3e	bbd7d814	6454a1d6
	a5571007	6c4151f5	8970f768	32c48fd1
	54c428ea	113b00cf	3db1bb85	1d2b2de6
	89157118	89157118	d22f990b	6db9f321
M_1	0a179ed0	582e9fee	8c68cd3d	0d120a6e
	de43af57	df2e7a6f	2b40967e	df302947
	ee7f066f	d7b7707d	9f1cc8a9	eaecfcb8
	0b449f1a	ec058b69	996ee0d2	994ef6b1
M_1'	0a159ed0	582e9fee	8c48cd3d	0d120a6e
	de43af57	df2e7a6f	2b40967e	df302947
	ee7f066f	d7b7707d	9f1cc8a9	eaecfd38
	0b451f1a	ec058b69	996ee0d2	994ef6b1
hash	a76b7982	e39826f9	52eb6b63	6b48ecdd
	4ddca6c5			

The first differential trail for 39-step SHA-256

i	ΔA_i	ΔE_i	ΔW_i
−4	==========	==========	
−3	==========	==========	
−2	==========	==========	
−1	==========	==========	
0	==========	==========	==========
1	==========	==========	==========
2	==========	==========	==========
3	==========	==========	==========
4	==========	==========	==========
5	==========	==========	==========
6	==========	===0==========	==========
7	==========	===1========1======11======0===	==========
8	===u==========	unnn1=1110=0=0101==000====1110=	===u==========
9	==========n=u====u======n===	010n0n0111010nu01001un011n10n=10	======n===u==========u==========
10	==========	0101u1n=1n0n010=u0=11nuu=1u00=n1	===n==========
11	==========	=100010==0=0101=0===0010=10=1=0=	=======nn=======n===n===nn==uu=n
12	==========	=unn010000=1000011=00011==0=101=	==========u=======nn=========
13	==========	10110nuuuuuuuu0u101un000010n111	==========
14	==========	=111=0000000000=0=1=001111111=1=	==========
15	==========n===	1100110110100000001nuuuuuuuu001	==========
16	=======u=u=======u==========	010100unu000001001u1000110unn=n1	======n===u==========u==========
17	==========	11=0111u00nn=100110=u1u00unn000n	===n==========
18	===n==========	uuu1uuuu01000=110n000111101=0101	==========
19	==========	000u0n1000101=0un01=1100=u11n000	==========
20	==========	011100un0u001unnnn11000000001111	==========
21	==========	=110=111=0===000=1=======1==1===	==========
22	==========	=nuu==0110===00101=0110====110=	==========
23	==========	=000==========	==========
24	==========	=111==========	=======n=n=======n==========
25	==========	==========	==========
26	==========	==========	===u==========
27	==========	==========	==========
28	==========	==========	==========
29	==========	==========	==========
30	==========	==========	==========
31	==========	==========	==========
32	==========	==========	==========
33	==========	==========	==========
34	==========	==========	==========
35	==========	==========	==========
36	==========	==========	==========
37	==========	==========	==========
38	==========	==========	==========

The SFS colliding message pair for 39-step SHA-256

CV	02b19d5a	88e1df04	5ea3c7b7	f2f7d1a4
	86cb1b1f	c8ee51a5	1b4d0541	651b92e7
M	c61d6de7	755336e8	5e61d618	18036de6
	a79f2f1d	f2b44c7b	4c0ef36b	a85d45cf
	f72b8c2f	0def947c	a0eab159	8021370c
	4b0d8011	7aad07f6	33cd6902	3bad5d64
M'	c61d6de7	755336e8	5e61d618	18036de6
	a79f2f1d	f2b44c7b	4c0ef36b	a85d45cf
	e72b8c2f	0fcf907c	b0eab159	81a1bfc1
	4b098611	7aad07f6	33cd6902	3bad5d64
hash	431cadcd	ce6893bb	d6c9689a	334854e8
	3baae1ab	038a195a	ccf54a19	1c40606d

Our results on RIPEMD-160 and SHA-256

- The first practical collision for $\{40/80\}$ steps of RIPEMD-160.
- The first practical SFS collision for $\{39/64\}$ steps of SHA-256.

British TEA Workshop

Andrew William Roscoe, Lei Wang

International Workshop on Timed-release Encryption and its Applications

held in Oxford, United Kingdom

Sponsor: Crypto.com

TEA Workshop

- **Date:** June 26-27, 2023
- **Venue:** Oxford, United Kingdom
- **Host:** Department of Computer Science, Oxford University
- **Co-organizer:** Blockchain Research Centre, Shanghai Jiao Tong University
- **Website:** http://treow.cs.ox.ac.uk

Sponsored by Crypto.com

TEA Workshop

- **Promote the research in the field of Timed-Release Encryption and its Applications**
  - timed-release encryption

    Make Software Encryption Slow Again
  - similar primitives: timed commitments, timed puzzles, etc
  - applications to protocols, blockchain, etc
  - design, analysis and implementation

TEA Workshop

- **Expect to bring together researchers from around the world**
    - speakers are invited
    - open to individuals with exceptional research ideas
    - attendees are open to general public
    - contact us to reserve a spot

TEA Workshop

- **Date:** **June 26-27, 2023**
- **Venue:** **Oxford, United Kingdom**
- **Web:** **http://treow.cs.ox.ac.uk**
- **Contact:**

  - Ivo Maffei (ivo.Maffei@cs.ox.ac.uk)

ASK 2023

The 10th Asian Workshop on Symmetric Key Cryptography

Yaobin Shen and Ling Song

FSE 2023 Rump Session

The 10th Asian Workshop on Symmetric Key Cryptography

- Date: December 9-11, 2023
  Saturday-Monday, just after Asiacrypt 2023 (December 4-8)
- Venue: Jinan University, Guangzhou, China
- Contact: Yaobin Shen, yaobins180 [at] gmail.com
  Ling Song, songling.qs [at] gmail.com
- Web: https://askworkshop.github.io/ask2023/ (update soon)

ASK 2023

- To promote research on symmetric key cryptography in Asia
  - block ciphers, stream ciphers, hash functions, modes of operations,…
  - analysis, designs, proofs, implementations,…
- Any researcher (even not based in Asia) is welcome for participance
- Limited number of stipend for PhD students who have difficulty obtaining funding

ASK Format

- Invited talk sessions in the morning
  - respectable speakers
  - advanced results
  - survey on popular topics
- Working group sessions in the afternoon
  - small discussion group
  - particular research topic
  - facilitate cooperation

Previous ASK

- ASK 2011: Singapore, Jian Guo and Thomas Peyrin
- ASK 2012: Japan, Tetsu Iwata and Lei Wang
- ASK 2013: China, Meiqin Wang and Hongbo Yu
- ASK 2014: India, Nalla Anandakumar and Somitra Sanadhya
- ASK 2015: Singapore, Jérémy Jean and Lei Wang
- ASK 2016: Japan, Tetsu Iwata and Yu Sasaki
- ASK 2017: China, Meicheng Liu and Bing Sun
- ASK 2018: India, Subhamoy Maitra and Mridul Nandi
- ASK 2019: Japan,Takanori Isobe and Yu Sasaki
- 2020-2022 are cancelled due to covid

Some Publications Related to ASK

- ASIACRYPT 2012, ASIACRYPT 2013, Eurocrypt 2018
- FSE 2012, FSE 2014 (2), FSE 2015, FSE 2016 (2), FSE 2018, FSE 2019 (2), FSE 2020, FSE 2021
- ACISP 2012, ACISP 2013, ACISP 2016, ACNS 2016 (2), ACNS 2017, LatinCrypt 2017, SAC 2018, ACNS 2019, ACNS 2020, Indocrypt 2020
- IEICE 2015, Designs Codes and Cryptography 2017

Some Statistics Regarding Venue Guangzhou

Delicious Food

- more than 1,000 dim sum
- thousands of desserts

Tourist Attractions

- 223+ million visitors each year
- Canton tower, museum, paradise

Welcome to ASK 2023 @ Guangzhou!
Date: December 9-11

The End of the Rump Session

The Best Rump Session Award

- Will be rewarded to ..