



CHAE:

Challenges in Authenticated Encryption

White paper available:
<https://chae.cr.jp.to>

Contributors to the white paper

Jean-Philippe Aumasson

Steve Babbage

Daniel J. Bernstein

Carlos Cid

Joan Daemen

Orr Dunkelman

Kris Gaj

Shay Gueron

Pascal Junod

Adam Langley

David McGrew

Kenny Paterson

Bart Preneel

Christian Rechberger

Vincent Rijmen

Matt Robshaw

Palash Sarkar

Patrick Schaumont

Adi Shamir

Ingrid Verbauwhede

Challenges in the white paper

The security target is wrong:

- Side-channel attacks
- Birthday attacks
- Data limits
- Attack economics
- Quantum computers

The performance target is wrong:

- Denial-of-service attacks
- Very short inputs
- Higher-level protocols
- Flexibility
- CPU evolution

The interface is wrong:

- Streams
- Files
- Noisy channels
- Software engineering and hardware engineering

Mistakes and malice:

- Error-prone designs
- Unverifiability
- Miscommunication of security prerequisites
- Incorrect proofs
- Malicious software and hardware

Challenges in Authenticated Encryption

1. Introduction

2. Challenges in Authenticated Encryption

3. Summary

4. Bibliography

Contents

1. Introduction

2. Challenges in Authenticated Encryption

3. Summary

4. Bibliography

Executive summary

1. Introduction

2. Challenges in Authenticated Encryption

3. Summary

4. Bibliography

Chapter 1

The security target is wrong

1.1. Introduction

1.2. The security target is wrong

1.3. Summary

1.4. Bibliography

Chapter 2

A brief introduction to authenticated encryption

2.1. Introduction

2.2. A brief introduction to authenticated encryption

2.3. Summary

2.4. Bibliography

Chapter 3

The performance target is wrong

3.1. Introduction

3.2. The performance target is wrong

3.3. Summary

3.4. Bibliography

Chapter 4

Mistake and make

4.1. Introduction

4.2. Mistake and make

4.3. Summary

4.4. Bibliography

Chapter 5

The interface is wrong

5.1. Introduction

5.2. The interface is wrong

5.3. Summary

5.4. Bibliography

Chapter 6

Robustness

6.1. Introduction

6.2. Robustness

6.3. Summary

6.4. Bibliography

Chapter 7

Adaptive adversary model

7.1. Introduction

7.2. Adaptive adversary model

7.3. Summary

7.4. Bibliography

Chapter 8

Adaptive adversary model

8.1. Introduction

8.2. Adaptive adversary model

8.3. Summary

8.4. Bibliography

Chapter 9

Adaptive adversary model

9.1. Introduction

9.2. Adaptive adversary model

9.3. Summary

9.4. Bibliography

Chapter 10

Adaptive adversary model

10.1. Introduction

10.2. Adaptive adversary model

10.3. Summary

10.4. Bibliography

Chapter 11

Adaptive adversary model

11.1. Introduction

11.2. Adaptive adversary model

11.3. Summary

11.4. Bibliography

Chapter 12

Adaptive adversary model

12.1. Introduction

12.2. Adaptive adversary model

12.3. Summary

12.4. Bibliography

Chapter 13

Adaptive adversary model

13.1. Introduction

13.2. Adaptive adversary model

13.3. Summary

13.4. Bibliography

Chapter 14

Adaptive adversary model

14.1. Introduction

14.2. Adaptive adversary model

14.3. Summary

14.4. Bibliography

Chapter 15

Adaptive adversary model

15.1. Introduction

15.2. Adaptive adversary model

15.3. Summary

15.4. Bibliography

Chapter 16

Adaptive adversary model

16.1. Introduction

16.2. Adaptive adversary model

16.3. Summary

16.4. Bibliography

Chapter 17

Adaptive adversary model

17.1. Introduction

17.2. Adaptive adversary model

17.3. Summary

17.4. Bibliography

Chapter 18

Adaptive adversary model

18.1. Introduction

18.2. Adaptive adversary model

18.3. Summary

18.4. Bibliography

Chapter 19

Adaptive adversary model

19.1. Introduction

19.2. Adaptive adversary model

19.3. Summary

19.4. Bibliography

Chapter 20

Adaptive adversary model

20.1. Introduction

20.2. Adaptive adversary model

20.3. Summary

20.4. Bibliography