



CHAE:

Challenges in Authenticated Encryption

White paper available:
<https://chae.cr.yp.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



Chapter 1

The security target is wrong

The security target is wrong. The security target is too high. The security target is too low. The security target is too complex. The security target is too simple. The security target is too expensive. The security target is too cheap. The security target is too difficult. The security target is too easy. The security target is too hard. The security target is too soft. The security target is too strong. The security target is too weak. The security target is too fast. The security target is too slow. The security target is too big. The security target is too small. The security target is too long. The security target is too short. The security target is too wide. The security target is too narrow. The security target is too deep. The security target is too shallow. The security target is too high. The security target is too low. The security target is too complex. The security target is too simple. The security target is too expensive. The security target is too cheap. The security target is too difficult. The security target is too easy. The security target is too hard. The security target is too soft. The security target is too strong. The security target is too weak. The security target is too fast. The security target is too slow. The security target is too big. The security target is too small. The security target is too long. The security target is too short. The security target is too wide. The security target is too narrow. The security target is too deep. The security target is too shallow.

Chapter 2

The interface is wrong

The interface is wrong. The interface is too high. The interface is too low. The interface is too complex. The interface is too simple. The interface is too expensive. The interface is too cheap. The interface is too difficult. The interface is too easy. The interface is too hard. The interface is too soft. The interface is too strong. The interface is too weak. The interface is too fast. The interface is too slow. The interface is too big. The interface is too small. The interface is too long. The interface is too short. The interface is too wide. The interface is too narrow. The interface is too deep. The interface is too shallow. The interface is too high. The interface is too low. The interface is too complex. The interface is too simple. The interface is too expensive. The interface is too cheap. The interface is too difficult. The interface is too easy. The interface is too hard. The interface is too soft. The interface is too strong. The interface is too weak. The interface is too fast. The interface is too slow. The interface is too big. The interface is too small. The interface is too long. The interface is too short. The interface is too wide. The interface is too narrow. The interface is too deep. The interface is too shallow.

Chapter 3

The performance target is wrong

The performance target is wrong. The performance target is too high. The performance target is too low. The performance target is too complex. The performance target is too simple. The performance target is too expensive. The performance target is too cheap. The performance target is too difficult. The performance target is too easy. The performance target is too hard. The performance target is too soft. The performance target is too strong. The performance target is too weak. The performance target is too fast. The performance target is too slow. The performance target is too big. The performance target is too small. The performance target is too long. The performance target is too short. The performance target is too wide. The performance target is too narrow. The performance target is too deep. The performance target is too shallow. The performance target is too high. The performance target is too low. The performance target is too complex. The performance target is too simple. The performance target is too expensive. The performance target is too cheap. The performance target is too difficult. The performance target is too easy. The performance target is too hard. The performance target is too soft. The performance target is too strong. The performance target is too weak. The performance target is too fast. The performance target is too slow. The performance target is too big. The performance target is too small. The performance target is too long. The performance target is too short. The performance target is too wide. The performance target is too narrow. The performance target is too deep. The performance target is too shallow.