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

CHAE: Challenges in Authenticated Encryption https://chae.cr.yp.to