ECRYPT

DIAC - Directions in Authenticated Ciphers

July 05 & 06, 2012

Want to protect messages against espionage **and** against forgery; have shared secret key.

This should be faster and/or more secure than with current approaches, so let's have a competition for authenticated ciphers.

Purpose of this workshop is to evaluate the state of the art in authenticated encryption and to gather community input regarding desired future directions.

Scope and function similar to SASC 2004 and the ECRYPT Hash Workshop 2007.

http://hyperelliptic.org/DIAC

ECRYPT

Topics I

Components and combinations

- block ciphers
- dedicated stream ciphers
- stream ciphers based on block ciphers
- dedicated hash functions, sponges, etc.
- hash functions based on block ciphers
- dedicated MACs
- MACs based on hash functions
- MACs based on block ciphers

http://hyperelliptic.org/DIAC

ECRYPT

Topics II

- authenticated encryption based on any of the above
- dedicated ciphers with built-in authentication

Implementations

- APIs
- software
- FPGAs
- ASICs
- comparisons

http://hyperelliptic.org/DIAC

ECRYPT

Topics III

Attacks

- Cryptanalysis of symmetric systems
- side-channel attacks on symmetric systems
- real-world costs of attacks

Requirements

- quantitative security: e.g., is 80 bits enough?
- qualitative security: e.g., MAC vs. PRF, INT-PTXT vs. INT-CTXT
- robustness: e.g., security under nonce reuse, security against idiots

http://hyperelliptic.org/DIAC

ECRYPT

Topics IV - Requirements

- handling of limited randomness; key agility
- safety of using a key for many messages: 2^32? 2^64?
- throughput in software, FPGA, ASIC
- parallelizability, incrementality, etc.
- ASIC area budgets, FPGA slice budgets, etc.
- power limits, energy limits, etc.
- bandwidth: short plaintexts, ciphertexts, authenticators
- flexibility: e.g., variable authenticator lengths
- convenience: e.g., one-pass, intermediate tags
- use cases http://hyperelliptic.org/DIAC

ECRYPT

DIAC - Directions in Authenticated Ciphers

July 05 & 06, 2012

Practical stuff:

Location: most likely Stockholm (long days to have discussions around the clock); in any case somewhere northern with an international airport.

Deadline: May 7, 2012

Notification: June 4, 2012

Other events: July 1-3 is RFIDsec in Nijmegen, enough time to travel between events

http://hyperelliptic.org/DIAC

ECRYPT

Program committee (tbc)

- Daniel J. Bernstein
- Carlos Cid
- Tetsu Iwata
- Tanja Lange
- Stefan Lucks
- Kaisa Nyberg
- Elisabeth Oswald
- Bart Preneel
- Vincent Rijmen
- Phillip Rogaway
- François-Xavier Standaert
- Ingrid Verbauwhede

http://hyperelliptic.org/DIAC