EasyCrypt and Family

Yves Bertot (pour B. Grégoire)

Language Based Cryptography

EasyCrypt

1. Formal methods applied to Cryptography
2. Cryptographic processes as probabilistic programs
3. Game-based cryptographic proofs viewed as program transformations
4. Specific proof assistant (lessons from Coq)
5. Integration of automatic proof (SMT through Why)

EasyCrypt applications

- Symetric and asymetric encryption

  (OAEP, Cramer-Shoup, XCBC)

- Hash functions

  (Merkle-Damgård, Keccak)

- Signature

- (Protocoles -- AKE)

Fault attacks

- Making RSA-PSS secure against non-random faults (CHES'14)
- Model adversaries with powerful fault injection
- Computer-verified proof verified with EasyCrypt (6 games)

Higher-Order Masking

- Verified Proofs of Higher-Order Masking (Eurocrypt 2015)
- Split a secret among t+1 shares
- Model of adversary access to t internal registers
- Useful information when proof failure

Certified synthesis of batch verifiers

- Signature can be verified efficiently in batch mode
- Gains of efficiency at the cost of failing to reject with negligible probability
- Used for pairing-based cryptography
- Connecting EasyCrypt as a certifying back-end to Autobatch
- Generic proof of screening assuming the initial verifier is robust against chosen-message attacks
- Paper accepted at CSF'14