Short signatures in the random oracle model

Louis Granboulan

École Normale Supérieure

Louis.Granboulan@ens.fr

Overview of the talk

1. Short signatures

2. Paddings for trapdoor one-way functions

3. OPSSR

4. Conclusion

Digital signature scheme

- Parameter generation
  returns the common parameters (e.g. choice of an ell. curve)

- Key generation
  returns the private and public keys of a user

- Signing
  takes a message and returns a valid signed message

- Verification
  takes a signed message and returns either "invalid" or the message

Concrete security

- (t, ε, q_S)-forger
  attacks a given public key; makes q_S signing queries; runs in time t; success probability ε

- k bits of concrete security
  no (t, ε, q_S)-forger with $\log_2(t/\varepsilon) < k$

- Security proof
  assumption: no (t', ε')-solver for some problem
  reduction: existence of (t, ε, q_S)-forger implies (t', ε')-solver
  efficiency: comparison of $k = t/\varepsilon$ and $k' = t'/\varepsilon'$

Security proofs in idealized worlds

- Proofs based of a reduction algorithm
  builds a (t', ε')-solver from a (t, ε, q_S)-forger
  needs to make valid answers to signature queries: simulator

- Idealized components
  oracle property: the simulator knows the queries
  programmability: the simulator chooses the answers

- Examples
  random oracle, for hash functions
  ideal cipher, for families of random permutations
  generic group, for group operations

Appendix or message recovery

- Signature scheme with appendix
  a signed message is the concatenation of the message and of an appendix (of fixed length)

- Signature scheme with full message recovery
  the message is completely hidden in a signed message

- Signature scheme with partial message recovery
  a signed message is the concatenation of part of the message and of an appendix (of fixed length) that contains the rest

Message expansion

- Definition

  Length of the signed message, minus the length of the message
  Usually it is a constant
  We use the notation λ

  For a signature scheme with appendix, it is the length of the appendix

- Our goal

  "Short signatures" will mean "small message expansion"

Lower bound

Let $\#r$ be the number of random bits effectively used by the signing algorithm (e.g. $2^{\#r}$ is the number of distinct outputs for fixed key and message)

- Validity of a random signed message
  probability at least $1/2^{\lambda-\#r}$

- Conclusion
  security level k is at most $\lambda - \#r$
  message expansion is at least $k + \#r$
  minimal message expansion implies unique signature

Our OPSSR scheme has k bits of message expansion

Lower bound for signature schemes with appendix

- Coron's result (Eurocrypt'02)
  $k' \geq k + \log_2 q_S - \#r$ (and also $k' \geq k$)

- Length of the appendix
  exhaustive search to solve the underlying problem proves that $\lambda \geq k'$

- Conclusion
  $\lambda - k \geq \#r$ and $\lambda - k \geq \log_2 q_S - \#r$, therefore $\lambda \geq k + \frac{1}{2}\log_2 q_S$

We don't know if this lower bound can be reached

Trapdoor one-way functions

- Definition
  bijective mapping $f : \mathcal{S} \rightarrow \mathcal{L}$; the 2^l elements of $\mathcal{L}$ are l'-bit strings
  computing f is easy; computing f^{-1} with the trapdoor is easy
  computing f^{-1} without the trapdoor has intractability k'
  exhaustive search $\Rightarrow k' \leq l'$

- Random self-reducibility
  randomized $\mathsf{R} : \mathcal{L} \rightarrow \mathcal{L}$ with uniform output,
  such that $f^{-1}(y)$ is easy to compute from $f^{-1}(\mathsf{R}(y))$
  birthday paradox $\Rightarrow k' \leq l/2$

FDH and PFDH

(schemes with appendix)

- Components

  a hash function H, a trapdoor one-way bijection f

- FDH (full domain hash)

  verification of signed message $\sigma = m \| s$: tests $\mathsf{H}(m) \stackrel{?}{=} f(s)$

  signing of m: returns $m \| f^{-1}(\mathsf{H}(m))$

- PFDH (probabilistic)

  verification of signed message $\sigma = m \| r \| s$: tests $\mathsf{H}(m \| r) \stackrel{?}{=} f(s)$

  signing of m: returns $m \| r \| f^{-1}(\mathsf{H}(m \| r))$, for a random r

Security of FDH and PFDH

- For generic trapdoor one-way functions
  random oracle model for H, with at most $q_H \leq 2^k$ queries
  proof shows that $k' - k \simeq \log_2(q_S + q_H)$ (Bellare & Rogaway)

- For random self reducible trapdoor one-way functions
  random seed r can take $2^{\#r}$ values; random oracle model for H
  proof shows that $k' - k \simeq \max(\log_2 q_S - \#r, 0)$ (Coron)
  NB: generalizes to claw-free permutations (Dodis & Reyzin)

PSS and PSSR

(schemes with message recovery)

two hash functions H, G, a trapdoor one-way bijection f

PSS0: verification of signed message $\sigma = \widehat{m} \| s$:

  computes $a \| h = f(s)$ and $\bar{m} = a \oplus \mathsf{G}(h)$

  recovers message with $m = \widehat{m} \| \bar{m}$: tests $\mathsf{H}(m) \stackrel{?}{=} f(s)$

signing of m: sets $\widehat{m} \| \bar{m} = m$

  computes $h = \mathsf{H}(m)$ and $a = \bar{m} \oplus \mathsf{G}(h)$;

  returns $\widehat{m} \| f^{-1}(a \| h)$

PSSR: randomized variant: $m \| r$ used in place of m

PSS: only the random seed is recovered: $\bar{m} = r$

Security of PSSR

- Security result

  random oracle model for H and G

  same security as PFDH, if the output of H has no collision

  $k' - k \simeq \log_2(q_S + q_H)$ in general

  $k' - k \simeq \max(\log_2 q_S - \#r, 0)$ when random self reducible

- Message expansion

  No collision $\Rightarrow h$ is at least $2k$-bit long

  Message expansion is at least $2k + \#r$

Basic OPSSR

- Design principles
  improve PSSR to increase the amount of message recovered
  random oracle can generate collisions: use random permutation
  Basic OPSSR: fixed message length, full message recovery

- Description
  a generic permutation E, a trapdoor one-way bijection f
  a fixed value κ of k bits
  – verification computes $m\|v = \mathsf{E}(f(\sigma))$ and tests if $v \stackrel{?}{=} \kappa$
  – signing computes $\sigma = f^{-1}(\mathsf{E}^{-1}(m\|\kappa))$
  randomized variant: $m\|r$ used in place of m

Security proof for Basic OPSSR

Security reduction to the computation of $f^{-1}(y)$ for some $y \in \mathcal{L}$
number of oracle calls $q_S + q_E + q_{E^{-1}} \leq 2^k$

- Generation of elements $y' \in \mathcal{L}$
  one (with probability 2^{-k}) is the challenge to solve
  others are $f(x')$ for random x'

- Simulation of signature oracle
  signature query for m: generates y', sets $y' \overset{\mathsf{E}}{\mapsto} m \| \kappa$; answers x'
  - fails if $\mathsf{E}(y')$ was defined (probability $1/2^{l-k}$)
  - fails if y is the challenge (probability $1/2^k$)

Security proof for Basic OPSSR (cont.)

- Simulation of E^{-1} oracle

  query for $m\|\kappa$: does a signature query for m; answers y'

  fails if $\mathsf{E}(y')$ was defined (probability $1/2^{l-k}$)

  query for $m\|v$: generates random y'', sets $y'' \overset{\mathsf{E}}{\mapsto} m\|v$; answers y''

  fails if $\mathsf{E}(y'')$ was defined (probability $1/2^{l-k}$)

- Simulation of E oracle

  query for y'': random m and v, sets $y'' \overset{\mathsf{E}}{\mapsto} m\|v$; answers $m\|v$

  fails if $v \overset{?}{\neq} \kappa$ (probability $1/2^k$)

Security proof for Basic OPSSR (end)

- Total success probability

  if recovered message length more than k, then $l > 2k$ and each oracle simulation fails with probability at most $1/2^k$

  at most 2^k oracle calls $\Rightarrow$ probability of non failure more than $1/e$

  forgery is $f^{-1}(y)$ with probability 2^{-k}

  $\Rightarrow$ total success probability $2^{-k}/e$, i.e. $k' - k \simeq k$

- Random self-reducible f

  as for PFDH and PSSR, randomized scheme

  security $k' - k \simeq \max(\log_2 q_S - \#r, 0)$

  message expansion $k + \#r$

OPSSR

- Design principles

  signature of messages of arbitrary lengths

  use a collision-resistant hash function H

- Description

  an ideal cipher E, a trapdoor one-way bijection f

  a fixed value κ of k bits

  – verification of $\widehat{m}\|s$ computes $\bar{m}\|v = \mathsf{E}_{\mathsf{H}(\widehat{m})}(f(s))$ tests if $v \stackrel{?}{=} \kappa$

  – signing computes $s = f^{-1}(\mathsf{E}^{-1}_{\mathsf{H}(\widehat{m})}(\bar{m}\|\kappa))$ returns $\widehat{m}\|s$

  randomized variant: $m\|r$ used in place of m

Security proof for OPSSR

- Proof for Basic OPSSR applies
  oracle calls are dependent on the value of $\widehat{m}$
  E ideal cipher $\Rightarrow$ all permutations E_h are independent oracles

- Multi-key setting: dependence on the public key
  if attacker has signing oracle access for many keys
  proof still holds if all components are independent
  public key should be input to E
  proposal: use $\mathsf{E}_{\mathsf{H}(\widehat{m},\mathsf{pk})}$

Application to RSA

- RSA trapdoor one-way bijection
  parameter e; private key p, q; public key $n = pq$, $(l+1)$-bit long
  $f(x) = x^e$ in $\mathbb{Z}_n$; $\mathcal{L} =$ integers smaller than 2^l; $\mathcal{S} = f^{-1}(\mathcal{L})$
  Intractability of f^{-1}:

k'	80	128	160
l	1536	4096	8192

- 80-bit secure RSA-OPSSR
  security parameters are $k = 80$, $\log_2 q_S = 48$
  security proof gives $k' - k \simeq \max(\log_2 q_S - \#r, 0)$
  deterministic $\Rightarrow$ 4096-bit modulus and 80-bit expansion
  randomized $\Rightarrow$ 1536-bit modulus and 128-bit expansion

Conclusion

- Our main result

  minimal message expansion can be achieved

  an idealized world is needed for the security proof

  ideal cipher rather than random oracle

- Practical use

  application to RSA needs a large block cipher

  1536-bit or 4096-bit block with 160-bit key

Open problems

- Signature schemes with appendix

  needs a k'-bit trapdoor one-way permutation with security k' bits

  NB: no random self-reducibility

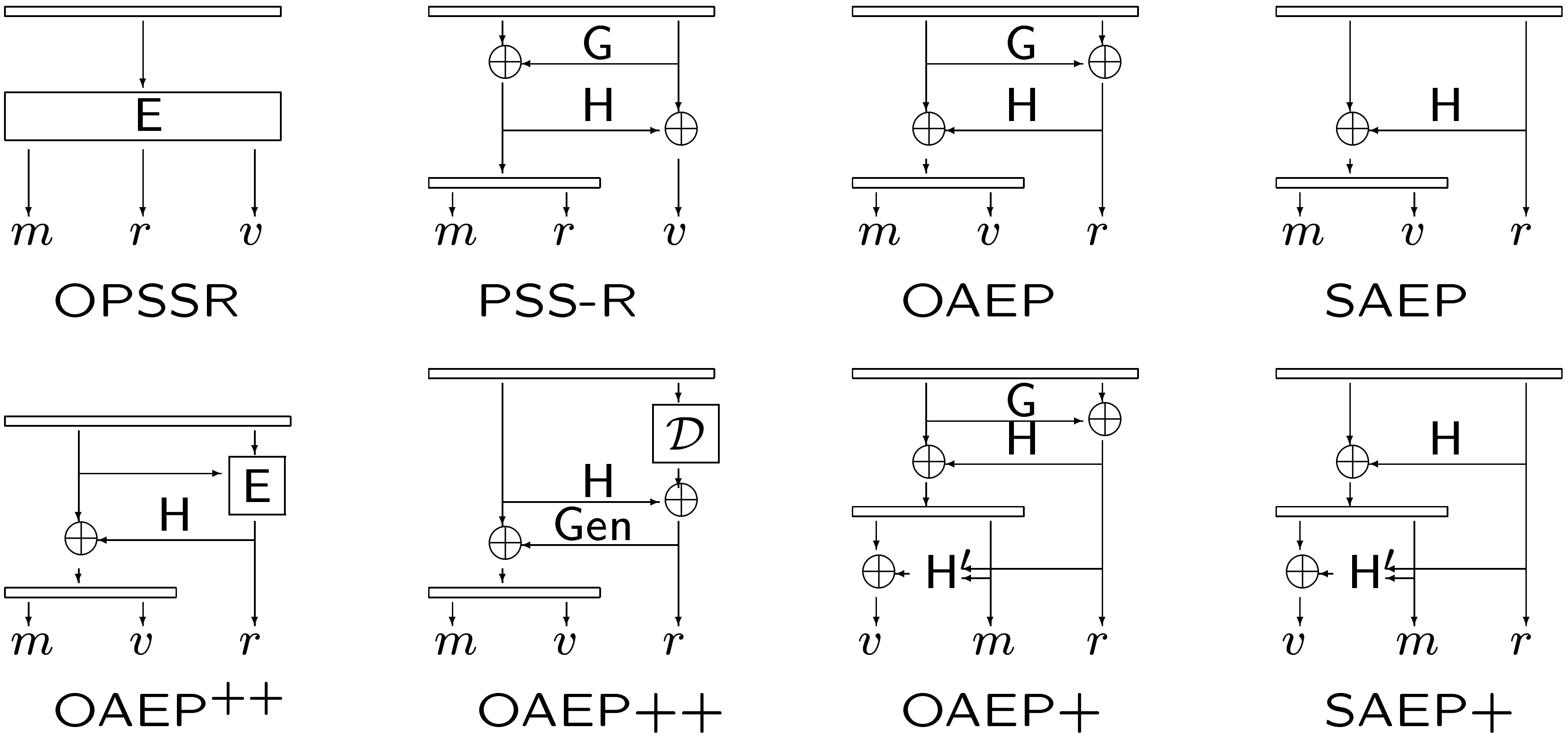
  needs an appropriate padding

  NB: FDH not appropriate if $\log_2 q_S < k$

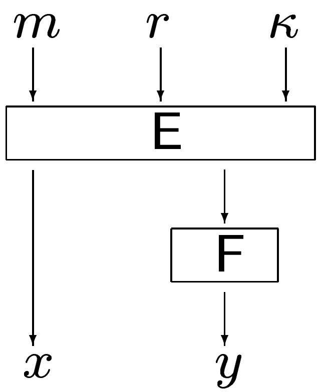
- Real world security proof

  what is the lower bound for message expansion?

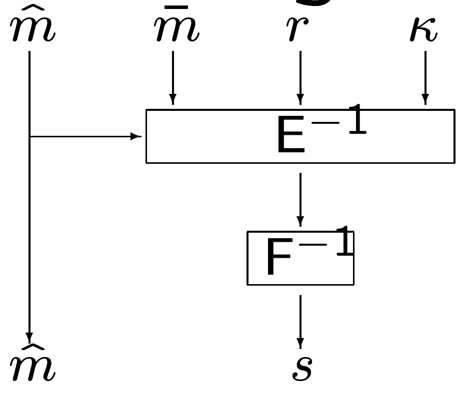
Comparison with other paddings



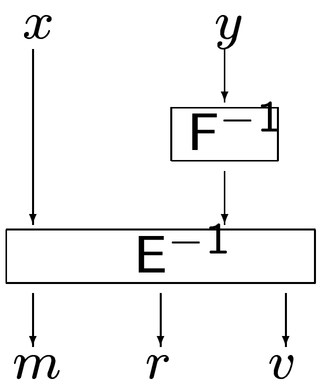
OPSSR: universal padding scheme



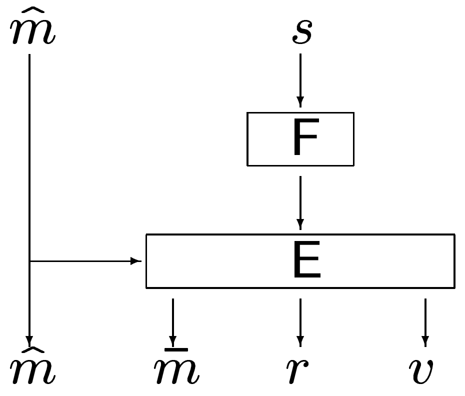
for encryption



for signature



for decryption



for verification