CS 4803
Computer and Network Security

Alexandra (Sasha) Boldyreva

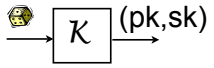
Digital signatures.

Digital signature schemes

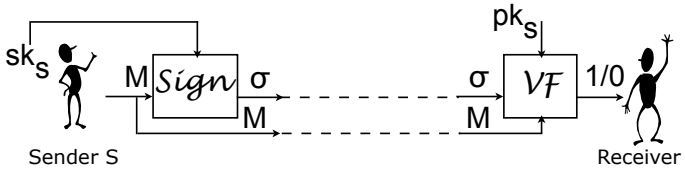
- Let's study the problem of data authentication and integrity in the asymmetric (public-key) setting.
- A sender needs to be assured that a message came from the legitimate sender and was not modified on the way.
- MACs solved this problem but for the symmetric-key setting.
- A digital signature scheme primitive is the solution to the goal of authenticity in the asymmetric setting.

Digital signature schemes

$\mathcal{DS}=(\mathcal{K},\mathcal{Sign},\mathcal{VF})$



MsgSp(pk)-message space



It is required that for every M∈MsgSp, every (pk,sk) that can be output by $\mathcal{K}$, if σ is output by $\mathcal{Sign}$, then $\mathcal{VF}$(pk,M,σ)=1

Digital signature schemes

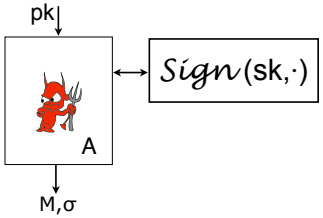
- The signing algorithm can be randomized or stateful (but it does not have to be).
- The MsgSp is often $\{0,1\}^*$ for every pk.
- Note that the key usage in a digital signature scheme is reverse compared to an asymmetric encryption scheme:
  - in a digital signature scheme the holder of the secret key is a sender, and anyone can verify
  - in an asymmetric encryption scheme the holder of the secret key is a receiver and anyone can encrypt

Security definition for digital signatures

Fix DS=(*K*,Sign,VF)

Run *K* to get (pk,sk)

For an adversary A consider an experiment $\mathbf{Exp}^{\text{uf-cma}}_{\mathcal{DS}}(A)$



Return 1 iff VF(pk,M,σ)=1 and M∈MsgSp(pk) that was was not queried to the signing oracle

The uf-cma advantage of A is defined as $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{DS}}(A) = \Pr\left[\mathbf{Exp}^{\text{uf-cma}}_{\mathcal{DS}}(A) = 1\right]$

A signature scheme is uf-cma secure if no efficient adversary has non-negligible uf-cma advantage.

Plain RSA signature scheme

Algorithm $K(k)$
$((N,e)(N,p,q,d)) \xleftarrow{\$} K^{\$}_{rsa}(k)$
Return $((N,e)(N,p,q,d))$

Algorithm $\text{Sign}_{N,p,q,d}(M)$
If $M \notin \mathbf{Z}^*_N$ then return $\perp$
$x \leftarrow M^d \bmod N$
Return x

Algorithm $\text{VF}_{N,e}(M,x)$
If ($M \notin \mathbf{Z}^*_N$ or $x \notin \mathbf{Z}^*_N$) then return 0
If $M = x^e \bmod N$ then return 1 else return 0

- Is Plain RSA signature scheme secure?

Plain RSA is not secure

Forger $F_1^{\text{Sign}_{N,p,q,d}(\cdot)}(N,e)$
Return $(1,1)$

Forger $F_2^{\text{Sign}_{N,p,q,d}(\cdot)}(N,e)$
$x \xleftarrow{\$} Z^*_N$; $M \leftarrow x^e \bmod N$
Return (M,x)

Forger $F_3^{\text{Sign}_{N,e}(\cdot)}(N,e)$
$M_1 \xleftarrow{\$} Z^*_N - \{1,M\}$; $M_2 \leftarrow MM_1^{-1} \bmod N$
$x_1 \leftarrow \text{Sign}_{N,e}(M_1)$; $x_2 \leftarrow \text{Sign}_{N,e}(M_2)$
$x \leftarrow x_1 x_2 \bmod N$
Return (M,x)

All adversaries (forgers) have uf-cma advantages 1 and are efficient.

Hash-then-invert paradigm

- We want to have an RSA-based signature scheme
  - that resists the attacks above
  - has a more flexible message space
  - provably secure
- An idea: let's hash the message first

Full-Domain-Hash (FDH) RSA signature scheme

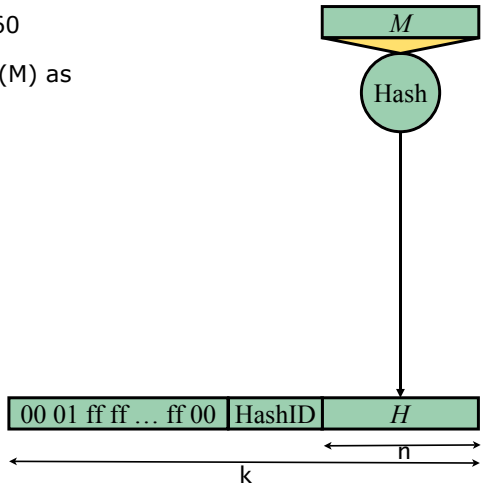
- Let H: $\{0,1\}^* \to Z_N^*$ be a hash function.
- FDH-RSA is a signature scheme $\mathcal{DS} = (\mathcal{K}_{\text{rsa}}, \text{Sign}, \text{VF})$

Algorithm $\text{Sign}^{H(\cdot)}_{N,p,q,d}(M)$	Algorithm $\text{VF}^{H(\cdot)}_{N,e}(M,x)$
$y \leftarrow H(M)$	$y \leftarrow H(M)$
$x \leftarrow y^d \bmod N$	$y' \leftarrow x^e \bmod N$
Return x	If $y = y'$ then return 1 else return 0

- What properties of the hash function do we need?
- If we have hash that "destroys" the algebraic structure and is collision resistant the obvious attacks do not apply.
- However, to prove security we need more:
  - we need to assume that the hash function is a random function
  - this is not a very realistic assumption
- Theorem. Under the RSA assumption the FDH-RSA signature scheme is uf-cma secure in the random oracle (RO) model.

In practice: RSA PKSC#1

- Fix a function $\text{Hash}:\{0,1\}^* \to \{0,1\}^n$ where $n \geq 128$
- E.g. for SHA1 n=160
- Define PKCS-HASH(M) as



- If Hash is collision resistant, so is PKCS-HASH.
- But hardness of computing the inverse of the RSA function on a random point in Z_N^* does not imply that on a point in $S=\{\text{PKCS-HASH}(M): M \in \{0,1\}^*\}$
- The are no attacks known, but it does not mean we should not be concerned.

Other signature schemes

- Let's consider several signature schemes whose security relies on the hardness of the DL problem.
  - Schnorr signature scheme

Algoritm K(k)
pick a k-bit prime p s.t. p=2q+1
pick $g \in Z_p^*$ of order q
$x \xleftarrow{\$} Z_q$
$X \leftarrow g^x$
Pick a hash function $H:\{0,1\}^* \rightarrow Z_q$
Return ((H,g,p,q,X),(H,g,p,q,x))

Algoritm $Sign_{sk}(M)$
$y \xleftarrow{\$} Z_q$
$Y \leftarrow g^y \bmod p$
$c \leftarrow H(M||Y)$
$s \leftarrow y+cx \bmod q$
Return (Y,s)

Algoritm $VF_{pk}(M,(Y,s))$
$c \leftarrow H(M||Y)$
If $g^s = YX^c \pmod p$ then return 1 else return 0

Other signature schemes

- ElGamal signature scheme

Algoritm K(k)
pick a k-bit prime p
pick a generator g of Z_p^*
$x \xleftarrow{\$} Z_{p-1}$
$X \leftarrow g^x$
Pick a hash function $H:\{0,1\}^* \rightarrow Z_{p-1}$
Return ((H,g,p,q,X),(H,g,p,q,x))

Algoritm $Sign_{sk}(M)$
$y \xleftarrow{\$} Z_{p-1}^*$
$Y \leftarrow g^y \bmod p$
$s \leftarrow y^{-1} (H(M||Y)-xY) \bmod (p-1)$
Return (Y,s)

Algoritm $VF_{pk}(M,(Y,s))$
If $X^Y Y^s = g^{H(M||Y)} \pmod p$ then return 1 else return 0

Security of Schnorr and ElGamal signatures

- The Schnorr and ElGamal signature schemes are uf-cma secure in the random oracle (RO) model in groups where the discrete logarithm (DL) problem is hard.

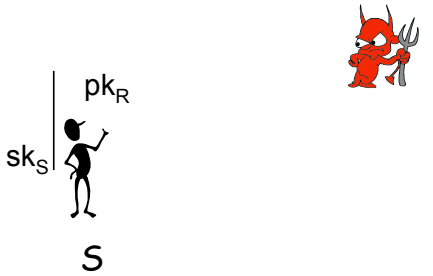
Signature schemes variations

- Multisignatures: several signers create a signature on a single message, that is shorter and faster to verify than when a standard signature scheme is used in a straightforward way.
- Aggregate signatures: similar to multisignatures, but the signers sign different messages.
- Threshold signatures: a group of n users holds a single public key. Each user holds a share of the secret key. At least t users need to cooperate to produce a valid signature on a message.
- Proxy signatures: a signer delegates its signing capabilities to a proxy.

- Group signatures: a group of users holds a single public key. Each user can sign on behalf of the group and remain anonymous, except from the manager of the group, who manages the group (joining and revocations of users).
- Ring signatures: similar to group signatures, but there is no group manager.
- Blind signatures: any user can obtain a signature on a message of its choice from a signer, such that the signer does not know what it signed.
- ....

Signcryption

- It is often desirable to achieve both privacy and authenticity in the public key setting.
- Signcryption is a public key primitive that assures privacy and authenticity of transmitted data
- Signcryption must be considered in the two-user or multi-user setting.



Security of signcryption

- As before an interesting question is how to properly compose an asymmetric encryption scheme and a digital signature scheme in order to get a secure signcryption
- If an encryption scheme is IND-CPA secure and a signature scheme is UF-CMA secure and is deterministic then Encrypt-then-Sign signcryption scheme provides privacy (in the IND-CCA sense) and authenticity.
- To insure security against "identity fraude" attacks one needs to
  - whenever encrypting something, add the public key of the sender to a message to encrypt
  - whenever signing something, add the public key of the receiver to a message to sign