Course: Modern Cryptography

Digital Signature Schemes

Shashank Singh

IISER Bhopal

Oct 31, 2025

Hurrah! We got to share a secret key!! (using public key paradigm)
We will be able to send a message secretly!!

What is the guarantee that it is the (original) Alice, he has exchanged the key with, not a fake one (some body may be pretending to be a Alice, an adversary).

Hurrah! We got to share a secret key!! (using public key paradigm)
We will be able to send a message secretly!!

What is the guarantee that it is the (original) Alice, he has exchanged the key with, not a fake one (some body may be pretending to be a Alice, an adversary).

Digital Signature/Certificate crypto schemes come as a saviour.

Digital Signature

- What is digital signature? What is meant by signing a digital file?

Elliptic and modular curves over finite fields
and related computational issues
Noam D. Elkies
March 1997

Introduction

msg.txt/msg.pdf

DIGITAL SIGNATURE

- What is digital signature? What is meant by signing a digital file?

Elliptic and modular curves over finite fields and related computational issues

Noam D. Elkies

March 1997

msg.txt/msg.pdf

Digital Signature

- What is digital signature? What is meant by signing a digital file?

Elliptic and modular curves over finite fields and related computational issues

Noam D. Elkies

March 1997

Based on a talk given at the conference Computational Perspectives on Number Theory in honor of A.O.L. Atkin held September 1995 in Chicago

Introduction

[illegible]

msg.txt/msg.pdf

- Alice want to digitally sign a digital file, say "msg.pdf" in this case.
- How is she digitally identified? Ans: By her public key.

Digital Signature

- The digital signature of a digital file (message) is another digital file (signature), created using the secret key of the signer, which when valid, guarantees the authenticity/approval of the message.

msg.txt.sig

msg.txt/msg.pdf

- Alice want to digitally sign a digital file, say "msg.pdf" in this case.
- How is she digitally identified? Ans: By her public key.

Digital Signature

- The digital signature of a digital file (message) is another digital file (signature), created using the secret key of the signer, which when valid, guarantees the authenticity/approval of the message.

msg.txt.sig

- It is of very very small size and often is embedded into the original file itself.
- Nobody, other than the owner of secret key, can produce it, however everybody can verify the signature.

Definition

A (digital) signature scheme consists of three PPT algorithms $(\texttt{GEN}, \texttt{SIGN}, \texttt{VRFY})$ such that:

- **GEN:** $(pk, sk) \leftarrow \texttt{GEN}(n)$. We assume that pk and sk each has length at least n, and that n can be determined from pk or sk.
- **SIGN:** It outputs the signature $\sigma \leftarrow \texttt{SIGN}_{sk}(m)$, where sk is a secret key and m is a message.
- **VRFY:** It takes as input a pk, a message m, and a signature σ and outputs a bit b, with $b = 1$ meaning valid and $b = 0$ meaning invalid. $n := \texttt{VRFY}_{pk}(m, \sigma)$.

It is required that except with negligible probability over (pk, sk) output by $\texttt{GEN}(1^n)$, it holds that $\texttt{VRFY}_{pk}(m, \texttt{SIGN}_{sk}(m)) = 1$ for every (legal) message m.

Security of signature schemes

Let $\Pi = (\texttt{GEN}, \texttt{SIGN}, \texttt{VRFY})$ be a signature scheme, and consider the following experiment for an adversary $\mathcal{A}$ and parameter n:

The signature experiment $\mathrm{SigForge}_{\mathcal{A},\Pi}(n)$**:**

- $(pk, sk) \leftarrow \texttt{GEN}(n)$.
- $\mathcal{A}$ is given pk and access to an oracle $\texttt{SIGN}_{sk}(\cdot)$. $\mathcal{A}$ then outputs (m, σ). Let $\mathcal{Q}$ denote the set of all oracle queries that A has made.
- A succeeds if and only if $\texttt{VRFY}_{pk}(m, \sigma) = 1$ and $m \notin \mathcal{Q}$. In this case the output of the experiment is defined to be 1.

Definition

A signature scheme $\Pi = (\mathtt{GEN}, \mathtt{SIGN}, \mathtt{VRFY})$ is existentially unforgeable under an adaptive chosen-message attack, or just secure, if for all PPT adversaries $\mathcal{A}$, there is a negligible function ε such that:

$$\Pr\left[\mathrm{SigForge}_{\mathcal{A},\Pi}(n) = 1\right] \leq \varepsilon(n).$$

☞ Informally a signature scheme is secure if nobody, other than the owner of secret key, can produce a valid signature of a (new) message(may be gibberish), which gets validated by the corresponding public key.

RSA SIGNATURES

The RSA-FDH signature scheme

Construct a signature scheme as follows:

- GEN: $(N, e, d) \leftarrow \texttt{genRSA}(n)$, return a public key $pk := \langle N, e\rangle$ and a private key $sk := \langle N, d\rangle$ and a function $H : \{0,1\}^* \mapsto \mathbb{Z}/N\mathbb{Z}$
- SIGN: On input $sk := \langle N, d\rangle$ and a message $m \in \mathbb{Z}/N\mathbb{Z}$, compute the signature

$$\sigma = \left[H(m)^d \bmod N\right]$$

- VRFY: On input $pk := \langle N, d\rangle$, a message $m \in \mathbb{Z}/N\mathbb{Z}$ and a signature $\sigma \in \mathbb{Z}/N\mathbb{Z}$, output 1 iff

$$H(m) \overset{?}{=} [\sigma^e \bmod N]$$

Theorem

If the RSA problem is hard relative to `genRSA` *and H is modeled as a random oracle, then RSA-FDH signature is secure*

Theorem

If the RSA problem is hard relative to `genRSA` *and H is modeled as a random oracle, then RSA-FDH signature is secure*

☞ In the RSA-FDH signature scheme, if we do not use hash function H and generate the signature using $\sigma = m^d \pmod N$ and do the verification using $m \overset{?}{=} [e^d \pmod N]$, will it result a secure signature scheme? Justify your answer.

DLP BASED SIGNATURES

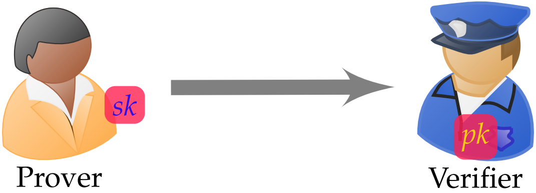
- We can construct digital signature schemes based on DLP as well but they ar not as straight forward as the one based on RSA problem.

- We now describe a DLP based signature scheme introduced by Claus Schnorr which is secure in the random-oracle model.

- Schnorr signature scheme is based on Schnorr identification scheme. The identification scheme when clubbed with the Fiat-Shamir transform gives the required signature scheme.

IDENTIFICATION SCHEMES

- An identification scheme is an interactive protocol that allows one party (prover) to prove its identity (i.e., to authenticate itself) to another (verifier).

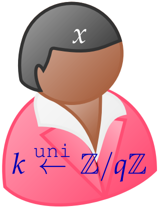


- the prover and verifier do not share any secret information (such as a password) in advance; instead, the verifier only knows the public key of the prover.

The Schnorr Identification Scheme

$$(G, q, g) \leftarrow \mathcal{G}(1^n)$$

$$x \overset{\texttt{uni}}{\leftarrow} \mathbb{Z}/q\mathbb{Z}; \;\; y := g^x$$



x

$k \overset{\texttt{uni}}{\leftarrow} \mathbb{Z}/q\mathbb{Z}$

Prover

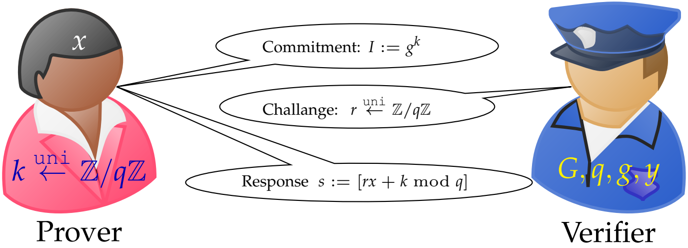
G, q, g, y

Verifier

The Schnorr Identification Scheme

$$(G, q, g) \leftarrow \mathcal{G}(1^n)$$

$$x \overset{\texttt{uni}}{\leftarrow} \mathbb{Z}/q\mathbb{Z}; \;\; y := g^x$$


x
$k \overset{\texttt{uni}}{\leftarrow} \mathbb{Z}/q\mathbb{Z}$
G, q, g, y

Commitment: $I := g^k$

Challange: $r \overset{\texttt{uni}}{\leftarrow} \mathbb{Z}/q\mathbb{Z}$

Response $s := [rx + k \bmod q]$

Prover

Verifier

If $g^s \cdot y^{-r} \overset{?}{=} I$,
Welcome!

Formally the above identification protocols is specified by three algorithms; $\mathcal{P}_1, \mathcal{P}_2$ on prover side and $\mathcal{V}$ on verifier side, such that

- The prover runs $\mathcal{P}_1(sk)$ using its private key sk to obtain an initial message I along with some state $\mathtt{st}$, and initiates the protocol by sending I to the verifier.
- In response, the verifier sends a challenge r chosen uniformly from some set Ω_{pk} defined by the prover's public key pk.
- Next, the prover runs $\mathcal{P}_2(sk, \mathtt{st}, r)$ to compute a response s that it sends back to the verifier.
- Finally, the verifier computes $\mathcal{V}(pk, r, s)$ and accepts if and only if this results in the initial message I.

For correctness, we require that if the legitimate prover executes the protocol correctly then the verifier should always accept.

SECURITY OF IDENTIFICATION SCHEME

- Nobody other than the owner of secret key should be unable to fool the verifier into accepting.
- This should be the case even the attacker is allowed to passively eavesdrop on multiple (honest) executions of the protocol between the prover and verifier.
- Let Trans_{sk} be an oracle, which when called without any input, runs an honest execution of the protocol and returns to the adversary the entire transcript (I, r, s) of the interaction.

Let $\Pi = (\texttt{GEN}, \mathcal{P}_1, \mathcal{P}_2, \mathcal{V})$ be an identification scheme, and consider the following experiment for an adversary $\mathcal{A}$ and parameter n:

The identification experiment $\text{Ident}_{\mathcal{A},\Pi}(n)$:

- $(pk, sk) \leftarrow \texttt{GEN}(1^n)$.
- $\mathcal{A}$ is given pk and access to an oracle Trans_{sk} that it can query as often as it likes.
- At any point during the experiment, $\mathcal{A}$ outputs a message I. A uniform challenge $r \in \Omega_{pk}$ is chosen and given to $\mathcal{A}$, who responds with some s. (A may continue to query Trans_{sk} even after receiving r.)
- The experiment outputs 1 if and only if $\mathcal{V}(pk, r, s) = I$.

Definition

An identification scheme $\Pi = (\texttt{GEN}, \mathcal{P}_1, \mathcal{P}_2, \mathcal{V})$ is secure against a passive attack, or just secure, if for all PPT adversaries $\mathcal{A}$, there exists a negligible function ε such that:

$$\Pr\left[\mathrm{Ident}_{\mathcal{A},\Pi}(n) = 1\right] \leq \varepsilon(n)$$

From Identification Schemes to Signatures

- We can turn an identification scheme into a signature scheme using the Fiat-Shamir transform.

Schnorr signature scheme:

- `GEN`: $(G, q, g) \leftarrow \mathcal{G}(1^n)$. $x \overset{\texttt{uni}}{\leftarrow} \mathbb{Z}/q\mathbb{Z}$ and let $y := g^x$. Set $sk := x$ and $pk := (G, q, g, y)$. Also a function $H : \{0,1\}^* \mapsto \mathbb{Z}/q\mathbb{Z}$ is specified, but we leave this implicit.

- `SIGN`: on input x and $m \in \{0,1\}^*$, choose a uniform $k \in \mathbb{Z}/q\mathbb{Z}$ and set $I := g^k$. Compute $r := H(I, m)$ followed by $s = [(rx + k) \bmod q]$, output the signature (r, s).

- `VRFY`: on input (G, q, g, y), m and (r, s), compute $I := g^s \cdot y^{-r}$ and output 1 if $H(I, m) \overset{?}{=} r$.

Theorem

If the discrete-logarithm problem is hard relative to G, then the Schnorr identification scheme is secure.

THE FIAT–SHAMIR TRANSFORM, GENERIC CONSTRUCTION

Let $(\mathtt{GEN}_{\mathtt{id}}, \mathcal{P}_1, \mathcal{P}_2, \mathcal{V})$ be an identification scheme, we construct a signature scheme as follows:

- GEN: $(pk, sk) \leftarrow \mathtt{GEN}_{\mathtt{id}}(1^n)$. pk specifies a set of challenges Ω_{pk}. Also, a function $H : \{0,1\}^* \mapsto \Omega_{pk}$ is specified, but we leave this implicit.
- SIGN: on input sk and $m \in \{0,1\}^*$, Compute $(I, \mathtt{st}) \leftarrow \mathcal{P}_1(sk)$, $r := H(I, m)$ and $s = \mathcal{P}_2(sk, \mathtt{st}, r)$. Output the signature (r, s).
- VRFY: on input pk, m and (r, s), compute $I := \mathcal{V}(pk, r, s)$ and output 1 if $H(I, m) \overset{?}{=} r$.

Theorem

Let Π be an identification scheme, and let Π' be the signature scheme obtained by applying the Fiat-Shamir transform to Π. If Π is secure and H is modeled as a random oracle, then Π' is secure.

DSA/ECDSA

- Though the Fiat-Shamir transform based Schnorr Signature Algorithm is very elegant and simple, it did not get the required popularity. One possible reason could be due to its patent, which expired in 2008.
- Another digital signature scheme is DSA. It can also be viewed as derived from identification scheme.
- It is very popular and widely used in practice. It is also based on the discrete logarithm problem.
- The Elliptic Curve Digital Signature Algorithm (ECDSA) is a DSA, which is based on the discrete-logarithm problem in the group of points on Elliptic Curve.