DD2520 Applied Cryptography
Lecture 6

Douglas Wikström
KTH Royal Institute of Technology
dog@kth.se

February 3, 2022

Signature Schemes

Digital Signature

- A digital signature is the **public-key** equivalent of a MAC; the receiver verifies the integrity and authenticity of a message.
- Does a digital signature replace a real handwritten one?
- How do you verify a written signature?

Textbook RSA Signature (1/2)

- Generate RSA keys $((N, e), (N, d))$.
- To sign a message $m \in \mathbb{Z}_N$, compute $\sigma = m^d \bmod N$.
- To verify a signature σ of a message m, verify that $\sigma^e = m \bmod N$.

Textbook RSA Signature (2/2)

- Are Textbook RSA Signatures any good?

Textbook RSA Signature (2/2)

- Are Textbook RSA Signatures any good?
- If σ is a signature of m, then $\sigma^2 \bmod N$ is a signature of $m^2 \bmod N$.

Textbook RSA Signature (2/2)

- Are Textbook RSA Signatures any good?
- If σ is a signature of m, then $\sigma^2 \bmod N$ is a signature of $m^2 \bmod N$.
- If σ_1 and σ_2 are signatures of m_1 and m_2, then $\sigma_1\sigma_2 \bmod N$ is a signature of $m_1 m_2 \bmod N$

Textbook RSA Signature (2/2)

- Are Textbook RSA Signatures any good?
- If σ is a signature of m, then $\sigma^2 \bmod N$ is a signature of $m^2 \bmod N$.
- If σ_1 and σ_2 are signatures of m_1 and m_2, then $\sigma_1\sigma_2 \bmod N$ is a signature of $m_1 m_2 \bmod N$
- We can also pick a signature σ and compute the message it is a signature of by $m = \sigma^e \bmod N$.

Textbook RSA Signature (2/2)

- Are Textbook RSA Signatures any good?
- If σ is a signature of m, then $\sigma^2 \bmod N$ is a signature of $m^2 \bmod N$.
- If σ_1 and σ_2 are signatures of m_1 and m_2, then $\sigma_1\sigma_2 \bmod N$ is a signature of $m_1 m_2 \bmod N$
- We can also pick a signature σ and compute the message it is a signature of by $m = \sigma^e \bmod N$.

We must be more careful!

RSA with Full Domain Hash (1/2)

Let $H_N : \{0,1\}^* \to \mathbb{Z}_N^*$ be a random oracle for every N.

- Generate RSA keys $((N, e), (N, d))$.
- To sign a message $m \in \{0,1\}^*$, compute $\sigma = H_N(m)^d \bmod N$.
- To verify a signature σ of a message m, verify that $\sigma^e = H_N(m) \bmod N$.

RSA with Full Domain Hash (2/2)

Theorem. RSA-FDH is provably secure in the random oracle model under the RSA assumption.

Problems.

- The hash function H_N has an inconvenient range.
- Our analysis is in the random oracle model, **which is unsound!**.

RSA with Full Domain Hash (2/2)

Theorem. RSA-FDH is provably secure in the random oracle model under the RSA assumption.

Problems.

- The hash function H_N has an inconvenient range.
- Our analysis is in the random oracle model, **which is unsound!**.

Solutions.

- The hash function can be replaced by a standard one or theoretical results can avoid it.

RSA with Full Domain Hash (2/2)

Theorem. RSA-FDH is provably secure in the random oracle model under the RSA assumption.

Problems.

- The hash function H_N has an inconvenient range.
- Our analysis is in the random oracle model, **which is unsound!**.

Solutions.

- The hash function can be replaced by a standard one or theoretical results can avoid it.
- Using the strong RSA assumption a signature scheme without random oracles or other additional assumptions can be constructed.

PKIs

Problem

- We have constructed public-key cryptosystems and signature schemes.
- Only the holder of the secret key can decrypt ciphertexts and sign messages.
- How do we **know** who holds the secret key corresponding to a public key?

Signing Public Keys of Others

- Suppose that Alice computes a signature $\sigma_{A,B} = \mathsf{Sig}_{\mathsf{sk}_A}(\mathsf{pk}_B, \mathit{Bob})$ of Bob's public key pk_B and his identity and hands it to Bob.

- Suppose that Eve holds Alice's public key pk_A.

- Then **anybody** can hand $(\mathsf{pk}_B, \sigma_{A,B})$ **directly** to Eve, and Eve will be convinced that pk_B is Bob's key (assuming she trusts Alice).

Certificate

- A **certificate** is a signature of a public key along with some information on how the key may be used, e.g., it may allow the holder to issue certificates.
- A certificate is valid for a given setting if the signature is valid and the usage information in the certificate matches that of the setting.
- Some parties must be trusted to issue certificates. These parties are called Certificate Authorities (CA).

Certificate Chains

A CA may be "distributed" using in certificate chains.

- Suppose that Bob holds valid certificates

$$\sigma_{0,1}, \sigma_{1,2}, \ldots, \sigma_{n-1,n}$$

  where $\sigma_{i-1,i}$ is a certificate of pk_{P_i} by P_{i-1}.

- Who does Bob trust?

Zero-Knowledge Proofs

Interaction

- A student claims to know the content of a course.

  Why does passing the written exam lead to passing the course?

- A new friend claims that they are a snowboarder like you.

  How can they convince you outside the slope?

- An attentative suspect claims watching the news as an alibi.

  How can the suspect convince the Police quickly?

- You use a VPN and Amazon is unhappy about that. They require you to unlock your account.

  How do they authenticate you?

Real-world Properties

- **Completeness.** Honest parties mostly agree on any claims after interacting.
- **Knowledge extraction.** Claims of knowledge are accepted only if the prover actually do know most of what is claimed.
- **Soundness.** Truth claims are accepted only if they are likely to be true.
- **Zero knowledge.** Interactions do not leak too much of the evidence.

What is a claim?

Consider NP relations of the form $\mathcal{R} \subset \{0,1\}^* \times \{0,1\}^*$ and corresponding languages

$$\mathcal{L} = \{x \mid (x, w) \in \mathcal{R}\} \ .$$

Let $x \in \{0,1\}^*$ be a string and $\mathcal{R}$ a relation.

Knowledge claim about x:

- I know w such that $(x, w) \in \mathcal{R}$.

Truth claim about x:

- $x \in \mathcal{L}$, or equivalently
- there exists a w such that $(x, w) \in \mathcal{R}$.

Examples

Example. RSA moduli and their factorizations

$$\mathcal{R}_{RSA} = \big\{ \big(N, (p, q)\big) \mid p \text{ and } q \text{ are distinct primes and } N = pq \big\}$$

- We can efficiently determine that N is a composite integer!
- Proving knowledge of (p, q) such that $N = pq$ still make sense.

Examples

Example. Let G by a cyclic group of order q with generator g

$$\mathcal{R}_{DL} = \left\{(y, x) \mid x \in \mathcal{Z}_q \text{ and } y = g^x\right\}$$

- For every $y \in G$ there exists an $x \in \mathcal{Z}_q$ such that $y = g^x$.
- Proving knowledge of x such that $y = g^x$ still make sense.

Examples

Example. Let G by a cyclic group of order q with generators g and h

$$\mathcal{R}_{DL} = \left\{ \big((y,z), x \big) \mid x \in \mathcal{Z}_{\boldsymbol{q}} \text{ and } (y,z) = (g^x, h^x) \right\}$$

- Most pairs (y, z) do not have this property and it is infeasible to check!
- Proving that there exists an x such that $(y, z) = (g^x, h^x)$ makes sense.
- Proving knowledge of x such that $(y, z) = (g^x, h^x)$ makes sense.

Properties

- **Knowledge extraction.** If Alice convinces Bob, then we could extract w from Alice: "Alice knows w".
- **Soundness.** If $x \notin \mathcal{L}$, then Alice convinces Bob with small probability no matter what she does: "Alice cannot lie".
- **Completeness.** If Alice and Bob are honest, then Bob accepts Alice's claim: "it works".
- **Zero knowledge.** Bob can simulate an interaction with Alice on his own: "Bob does not learn anything".

Example: Written Exam

Example: Written Exam

- Some **knowledge extraction.** If Alice passes the course, then we could rewind time and ask different questions until we have extracted everything that Alice knows.

Example: Written Exam

- Some **knowledge extraction.** If Alice passes the course, then we could rewind time and ask different questions until we have extracted everything that Alice knows.
- Decent **soundness.** If Alice committed to everything she knows in a bunch of envelopes, she could prove that the content of her commitment corresponded to a given grade by opening a few. (Proof claim.)

Example: Written Exam

- Some **knowledge extraction.** If Alice passes the course, then we could rewind time and ask different questions until we have extracted everything that Alice knows.
- Decent **soundness.** If Alice committed to everything she knows in a bunch of envelopes, she could prove that the content of her commitment corresponded to a given grade by opening a few. (Proof claim.)
- Resonable **completeness.** If Alice knows the course content and the teacher is honest, then she will most likely pass the course.

Example: Written Exam

- Some **knowledge extraction.** If Alice passes the course, then we could rewind time and ask different questions until we have extracted everything that Alice knows.
- Decent **soundness.** If Alice committed to everything she knows in a bunch of envelopes, she could prove that the content of her commitment corresponded to a given grade by opening a few. (Proof claim.)
- Resonable **completeness.** If Alice knows the course content and the teacher is honest, then she will most likely pass the course.
- Almost **zero knowledge.** Bob could look up some random answers and prepare an exam for the corresponding questions.

Example: Written Exam

The teacher must be experienced to write a good exam, but they need to know very little of the content of the course to assess knowledge precisely.

Teaching is much harder than assessing!

Example: Written Exam

The teacher must be experienced to write a good exam, but they need to know very little of the content of the course to assess knowledge precisely.

Teaching is much harder than assessing!

Computing is much harder than verifying!

Prove knowledge of pre-image

Let q be a prime and let G be a group of order q. Let $\phi : \mathbb{Z}_q \to G$ be a homomorphism, i.e., $\phi(a)\phi(b) = \phi(ab)$ for any $a, b \in \mathbb{Z}_q$.

Alice holds a such that $A = \phi(a)$ and Bob holds A.

1. Alice chooses $r \in \mathbb{Z}_q$ randomly and hands $R = \phi(r)$ to Bob.
2. Bob chooses $c \in \mathbb{Z}_q$ randomly and hands c to Alice.
3. Alice computes $d = ca + r \bmod q$ and hands d to Bob.
4. Bob accepts if and only if $A^c R = \phi(d)$.

Completeness

If Alice and Bob are honest, then Bob is convinced since

$$\phi(d) = \phi(ca + r) = \phi(a)^c \phi(r) = A^c R \ .$$

Knowledge Extraction

Given **two related accepting** executions (R, c, d) and (R, c', d') such that

$$c \neq c'$$
$$A^c R = \phi(d)$$
$$A^{c'} R = \phi(d')$$

Knowledge Extraction

Given **two related accepting** executions (R, c, d) and (R, c', d') such that

$$c \neq c'$$
$$A^c R = \phi(d)$$
$$A^{c'} R = \phi(d')$$

we have

$$\frac{A^c R}{A^{c'} R} = \frac{\phi(d)}{\phi(d')}$$

Knowledge Extraction

Given **two related accepting** executions (R, c, d) and (R, c', d') such that

$$c \neq c'$$
$$A^c R = \phi(d)$$
$$A^{c'} R = \phi(d')$$

we have

$$A^{c-c'} = \frac{A^c R}{A^{c'} R} = \frac{\phi(d)}{\phi(d')} = \phi(d - d')$$

Knowledge Extraction

Given **two related accepting** executions (R, c, d) and (R, c', d') such that

$$c \neq c'$$
$$A^c R = \phi(d)$$
$$A^{c'} R = \phi(d')$$

we have

$$A^{c-c'} = \frac{A^c R}{A^{c'} R} = \frac{\phi(d)}{\phi(d')} = \phi(d - d')$$

from which we can derive a preimage

$$x = (d - d')(c - c')^{-1}$$

such that $A = \phi(x)$.

Zero Knowledge

Bob can choose $c, d \in \mathbb{Z}_q$ randomly and compute

$$R = \phi(d)A^{-c}$$

to form a transcript (R, c, d) such that $A^c R = \phi(d)$.

This type of protocol is very common in practice. It is an **honest** verifier zero knowledge protocol, more precisely a Sigma protocol, or even more precisely a Schnorr protocol.

Fiat-Shamir Transform

Interaction is incredibly powerful, but also impractical.

Note that the verifier only flips coins in the protocol.

How do we reduce the protocol to a single message from Alice to Bob, which Bob verifies?

If we manage to do this, then anybody can post a their (only) message online and prove whatever they like!!!

Fiat-Shamir Transform

$H : \{0,1\}^* \to \mathbb{Z}_q$ is tweaked-SHA-3 and $m \in \{0,1\}^*$.

1. Alice picks $r \in \mathbb{Z}_q$ and computes $R = \phi(r)$ ~~and hands R to Bob~~.
2. Alice computes $c = H(A, R, m)$.
3. Alice computes $d = ca + r \bmod q$ and hands (R, d) to Bob.
4. Bob accepts if and only if $A^{H(A,R,m)}R = \phi(d)$.

Fiat-Shamir Transform

$H : \{0,1\}^* \to \mathbb{Z}_q$ is tweaked-SHA-3 and $m \in \{0,1\}^*$.

1. Alice picks $r \in \mathbb{Z}_q$ and computes $R = \phi(r)$ ~~and hands R to Bob~~.
2. Alice computes $c = H(A, R, m)$.
3. Alice computes $d = ca + r \bmod q$ and hands (R, d) to Bob.
4. Bob accepts if and only if $A^{H(A,R,m)} R = \phi(d)$.

Non-interactive!

Alice has signed m using the public key A :-)

Real-world Multiparty Computation

- Multiple keys held by different people needed to open a safe.
- Multiple persons partition a set $x_1, \ldots, x_N$, sum the integers in their part, and add the results.
- Counting votes in an election.

Average Height

Your height is h_i. We wish to compute $\frac{1}{N}\sum_{i\in[N]} h_i$.

Choose a random integer $r_i \in [0, 1000]$ and compute $a_i = h_i + r_i$.

Set $s_0 = 0$.

For $i = 1, \ldots, N$: compute $s_i = s_{i-1} + a_i$.

Set $t_0 = s_N$.

For $i = 1, \ldots, N$: compute $t_i = t_{i-1} - r_i$.

Average Height

Your height is h_i. We wish to compute $\frac{1}{N}\sum_{i\in[N]} h_i$.

Choose a random integer $r_i \in [0, 1000]$ and compute $a_i = h_i + r_i$.

Set $s_0 = 0$.

For $i = 1, \ldots, N$: compute $s_i = s_{i-1} + a_i$.

Set $t_0 = s_N$.

For $i = 1, \ldots, N$: compute $t_i = t_{i-1} - r_i$.

Who learns what?