III. Authentication - identification protocols

Definition 3.1 A cryptographic protocol is a distributed algorithm describing precisely the interaction between two or more parties, achieving certain security objectives.

Definition 3.2 A cryptographic scheme is a suite of cryptographic algorithms and protocols, achieving certain security objectives.

Identification schemes and protocols

Definition 3.3 An identification scheme consists of two cryptographic protocols, called registration and identification, between two parties, called the prover and the verifier.

In a symmetric identification scheme, registrations ends with both parties sharing a secret key. In an asymmetric identification scheme, registration will end with both parties sharing a public key, for which only the prover knows the secret key.

In the identification the verifier is assured of the identity of the prover.

Objective of identification protocols

1. If the prover P and the verifier V are honest, V will accept P's identity.
2. V cannot reuse an identification exchange to impersonate P to a third party C.
3. Only with negligible probability a party C distinct from P is able to cause V to accept C as P's identity.
4. The previous points remain true even if
   - a large number of authentications between P and V have been observed;
   - C has participated in previous executions of the protocol (either as P or V).

Identification - overview

- formalize security requirements for identification schemes
  - proofs of knowledge (simplified)
  - zero-knowledge proofs
- mostly ignore registration
- consider simplified but most important form of identification protocols, i.e. $\sum$-protocols
- indicate more general context
- see important examples
  - Schnorr protocol
  - Fiat-Shamir protocol

Identification - overview

- introduced witness hiding as relaxation of zero-knowledge property
- present Okamoto-Schnorr protocol as an example

Challenge-response protocols

In a challenge-response protocol P proves its identity to V by answering a challenge posed by V. Only by knowing the secret key should P be able to respond to the challenge correctly.

Structure

- challenge
- response

Simple identification based on signatures

$\Pi = (\text{Gen}, \text{Sign}, \text{Vrfy})$ signature scheme with message length n, (pk_P, sk_P) P's key pair.

P		V
		$c \leftarrow \{0,1\}^n$
	$\xleftarrow{\;c\;}$ challenge	
$r \leftarrow \text{Sign}_{sk_P}(c)$		
	$\xrightarrow{\;r\;}$ response	
		return 1 iff $\text{Vrfy}_{pk_P}(c, r)$

c is called nonce. Chosen for each execution. Guarantees time dependence.

Relations

- $R \subseteq \{0,1\}^* \times \{0,1\}^*$ binary relation, $(x,y) \in R :\Leftrightarrow R(x,y) = 1$
- $x \in \{0,1\}^* : W(x) := \{w \in \{0,1\}^* : R(x,w) = 1\}, w \in W(x)$ called called **witnesses** for x.
- $L_R := \{x \in \{0,1\}^* : W(x) \neq \varnothing\}$ language corresponding to R
- R **polynomially bounded** $:\Leftrightarrow$ there is a $c \in \mathbb{N}$ such that for all $x \in \{0,1\}^*$ and all $w \in W(x) : |w| \leq |x|^c$
- R **polynomially verifiable** $:\Leftrightarrow R(\cdot,\cdot)$ can be computed in polynomial time
- R **NP-relation** $:\Leftrightarrow$ R polynomially bounded and polynomially verifiable

Relations and the class NP

Observation

- If R is an NP-relation, then $L_R \in NP$.
- If $L \in NP$, then there is an NP-relation R with $L = L_R$.

Relations and languages - SAT

Example $L = SAT$

- $x = \phi$ Boolean formula, w assignment to varaibles
- $R_{SAT}(x, w) = 1 :\Leftrightarrow \phi(w) = \text{true}.$

Quadratic residues

Definition 3.4 Let $N \in \mathbb{N}$, then

$QR(N) := \left\{ v \in \mathbb{Z}_N^* \,\middle|\, \exists s \in \mathbb{Z}_N^* \;\; s^2 = v \bmod N \right\}$ is called the set of quadratic residues modulo N.

$QNR(N) := \mathbb{Z}_N^* \setminus QR(N)$ is called the set of quadratic non-residues modulo N.

$$QR \quad := \quad \left\{ (N,v) \,\middle|\, v \in QR(N) \right\}$$

$$QNR \quad := \quad \left\{ (N,v) \,\middle|\, v \notin QR(N) \right\}$$

Relations and languages – Quadratic residues

Example $L = QR$

- $x = (N, v), N \in \mathbb{N}, v \in \mathbb{Z}_N^*, w \in \mathbb{Z}_N^*$
- $R_{QR}(x, w) = 1 :\Leftrightarrow w^2 = x \bmod N.$

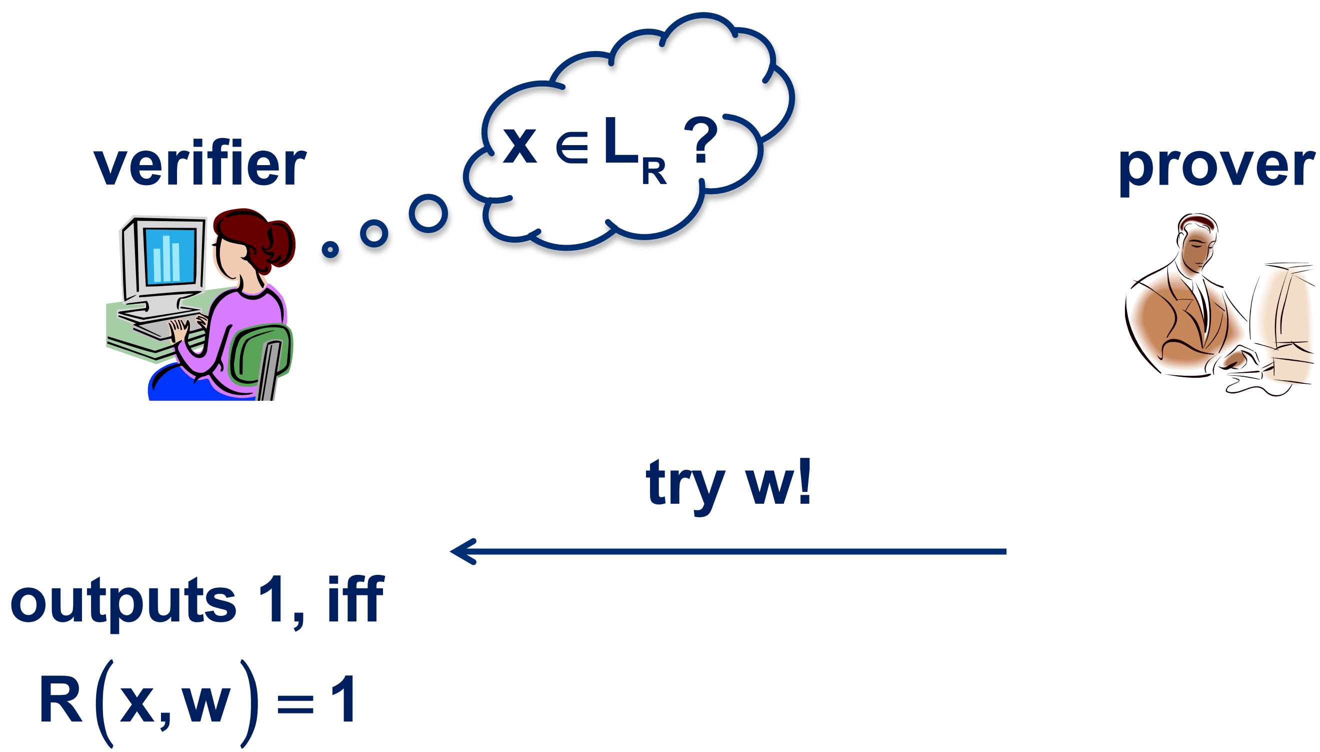
Relations and languages – Discrete logarithms

Example $L = DL$

- $x = (p, g, v)$, $p \in \mathbb{N}$ prime, $g, v \in \mathbb{Z}^*_p$, $w \in \mathbb{Z}_{p-1}$
- $R_{DL}(x, w) = 1 :\Leftrightarrow g^w = v \bmod p$

Relations and identification

- Given binary relation $R \subseteq \{0,1\}^* \times \{0,1\}$, in registration P and V agree on $x \in L_R$, for which P knows $w \in W(x)$.
- In identification, P convinces V that he knows $w \in W(x)$.



SAT and identification

SAT:= $\{\varphi \mid \varphi$ is a satisfiable Boolean formula$\}$

$\varphi \in \mathrm{SAT}$?

verifier

prover

try assignment c!

outputs 1, iff

$$\varphi(c) = 1$$

Identfciation reveals secret key!

QR and identification

$QR(N) := \{v \in \mathbb{Z}_N^* \mid \exists s \in \mathbb{Z}_N^* \;\; s^2 = v \bmod N\}$ is called the set of quadratic residues modulo N.

verifier

$(N, v) \in \mathbb{N} \times \mathbb{Z}_N^*$

prover

try s!

$\longleftarrow$

outputs 1, iff

$s^2 = v \bmod N$

Identfciation reveals secret key!

Three round protocols

Let C a finite set, let α,ρ be ppts, and let φ be a polynomial time computable predicate. Consider a three round protocol as below.

P with input (x, w)		V with input x
$a \leftarrow \alpha(x,w;k)$		
	$\xrightarrow{\ a\ }$	
	$\xleftarrow{\ c\ }$	$c \leftarrow C$
$r \leftarrow \rho(x,w,k,c)$		
	$\xrightarrow{\ r\ }$	
		$\varphi(x,a,c,r)$?

Three round protocols

P with input (x, w)		V with input x
$a \leftarrow \alpha(x, w; k)$		
	$\xrightarrow{a}$	
		$c \leftarrow C$
	$\xleftarrow{c}$	
$r \leftarrow \rho(x, w, k, c)$		
	$\xrightarrow{r}$	
		$\varphi(x, a, c, r)$?

- a is called announcement.
- c is called challenge and C is called challenge space.
- r is called response.
- (a,c,r) is called a conversation or transcript.
- (a,c,r) is called accepting, if $\varphi(x,a,c,r) = 1$.
- In this case, we say that V accepts .

Three round protocols

P with input (x,w)		V with input x
$a \leftarrow \alpha(x,w;k)$		
	$\xrightarrow{\quad a \quad}$	
	$\xleftarrow{\quad c \quad}$	$c \leftarrow C$
$r \leftarrow \rho(x,w,k,c)$	$\xrightarrow{\quad r \quad}$	
		$\varphi(x,a,c,r)$?

- Let R be a binary relation.
- The protocol is called complete for R, or simply a protocol for R, if for $(x,w) \in R$ verifier V always accepts.

Fiat-Shamir protocol

P on input (N,v,w)		V on input (N,v)
$k \leftarrow \mathbb{Z}_N^*, a := k^2 \bmod N$	$\xrightarrow{\quad a \quad}$	
		$c \leftarrow \{0,1\}$
	$\xleftarrow{\quad c \quad}$	
$r := k \cdot w^c \bmod N$		
	$\xrightarrow{\quad r \quad}$	
		accepts iff $r^2 = a \cdot v^c \bmod N$

The Fiat-Shamir protocol is a complete protocol for the relation R_{QR}.

Example L = QR

- $x = (N, v), N \in \mathbb{N}, v \in \mathbb{Z}_N^*, w \in \mathbb{Z}_N^*$
- $R_{QR}(x, w) = 1 :\Leftrightarrow w^2 = v \bmod N.$

Schnorr protocol

P on input (p,g,v,w)		V on input (p,g,v)
$k \leftarrow \mathbb{Z}_{p-1}, a := g^k \bmod p$	$\xrightarrow{\quad a \quad}$	
		$c \leftarrow \{1,\ldots,2^l\}, 2^l < p$
	$\xleftarrow{\quad c \quad}$	
$r := k - w \cdot c \bmod p-1$		
	$\xrightarrow{\quad r \quad}$	
		accepts iff $a = g^r \cdot v^c \bmod p$

The Schnorr protocol is a complete protocol for the relation R_{DL}.

Example $L = DL$

- $x = (p,g,v), p \in \mathbb{N}$ prime, $g,v \in \mathbb{Z}_p^*, w \in \mathbb{Z}_{p-1}$
- $R_{DL}(x,w) = 1 :\Leftrightarrow g^w = v \bmod p$

Soundness and zero-knowledge

Definition 3.5 A three round protocol for relation R has special soundness if there exists a ppt algorithm E (extractor) which given $x \in L_R$ and any two accepting transcripts (a,c,r) and (a,c',r') with $c \neq c'$ computes a witness w satisfying $(x,w) \in R$.

Definition 3.6 A three round protocol for relation R is a special honest verifier zero-knowledge protocol if there exists a ppt algorithm S (simulator) which given any $x \in L_R$ and any challenge c produces transcripts (a,c,r) with the same distribution as in the real protocol.

∑- protocols

Definition 3.7 A three round protocol is a ∑- protocol for relation R if

1. it is complete for relation R,
2. it has special soundness,
3. it is a special honest verifier zero-knowledge protocol for R.

Theorem 3.8 The Fiat-Shamir protocol is a Σ- protocol for relation R_{QR}. The Schnorr protocol is a Σ- protocol for relation R_{DL} restricted to triples (p,g,v), where the order of g is a known prime.

Soundness for Schnorr and Fiat-Shamir

Lemma 3.9 **The Fiat-Shamir protocol and the Schnorr protocol are sound. In the later case, we need that for triples (p,g,v) the order of g is a known prime.**

Schnorr protocol in prime order groups

Let G be a group with $|G| = p$, p prime, and let $g \in G \setminus \{1\}$.

P on input (G,g,v,w)		V on input (G,g,v)
$k \leftarrow \mathbb{Z}_p, a := g^k$ (in G)	$\xrightarrow{\;a\;}$	
	$\xleftarrow{\;c\;}$	$c \leftarrow \{1,\ldots,2^l\}, 2^l < p$
$r := k - w \cdot c \bmod p$	$\xrightarrow{\;r\;}$	
		accepts iff $a = g^r \cdot v^c$ (in G)

Observation The Schnorr protocol is a Σ-protocol for the relation

$R_{GDL} : \forall (v,w) \in G \times \mathbb{Z}_p : R_{GDL}(v,w) = 1 \Leftrightarrow g^w = v$ (in G).

Zero-knowledge for Schnorr and Fiat-Shamir

Lemma 3.10 The Fiat-Shamir protocol is a special honest verifier zero-knowledge protocol.

Lemma 3.11 The Schnorr protocol is a special honest verifier zero-knowledge protocol.

Soundness and security against cheating provers

Theorem 3.12 Let R be a binary relation and V/P a three round protocol for R with special soundness and challenge space C. Then for any $\varepsilon > 0$ and any algorithm A there exists an algorithm A' with the following properties:

1. If on input $x \in L_R$ algorithm A impersonates P with probability $1/|C| + \varepsilon, \varepsilon > 0,$ then A' on input x and with probability $\varepsilon/16$ computes a witness $w \in W(x)$.

2. If A runs in time T, then A' runs in time $\mathcal{O}\left(T/\varepsilon + T'\right)$, where T' is the runnig time of the extractor E for P/V.

Three round protocols

P with input (x,w)		V with input x
$a \leftarrow \alpha(x,w;k)$	$\xrightarrow{\quad a \quad}$	
	$\xleftarrow{\quad c \quad}$	$c \leftarrow C$
$r \leftarrow \rho(x,w,k,c)$	$\xrightarrow{\quad r \quad}$	
		$\varphi(x,a,c,r)$?

From A to A‘

A′ on input x

1. repeat at most $1/\epsilon$ – times
   a) $R \leftarrow \{0,1\}^L, c \leftarrow C$
   b) simulate A with random bits R and challenge c
   c) if A succeeds set $c^{(1)} := c$ and goto 2)
2. repeat at most $2/\epsilon$ – times
   a) $c \leftarrow C$
   b) simulate A with random bits R and challenge c
   c) if A succeeds set $c^{(2)} := c$ and goto 3)
3. Let a be the announcement that A computes with . random bits R. Use extractor E with input a, $c^{(1)}, c^{(2)}$ to compute a witness w.

Soundness and security against cheating provers – the main claim

– A uses bit strings in $\{0,1\}^L$ as its source of randomness.

– With $R \in \{0,1\}^L$ and $c \in C$ fixed, the bevaiour of A is fixed.

– (R,c) called accepting if A, by using randomness R and upon receiving challenge c, makes V accept.

– $R \in \{0,1\}^*$ called heavy if for at least a $\left(1/|C| + \epsilon/2\right)$-fraction of all $c \in C$ the pair (R,c) is accepting. Otherwise R is light.

– (R,c) called heavy if (R,c) is accepting and R is heavy .

Claim If A is as in Theorem 3.12 then for at least an ε/2-fraction of accepting pairs (R,c) the element R is heavy.

Proof of the main claim

- Let p be the fraction of accepting pairs (R,c) with a light R.
- Hence the number of accepting pairs with light R is
  $p \cdot (1/|C|+\epsilon) \cdot 2^L \cdot |C|$.
- Since each light R appears in at most $(1/|C|+\epsilon) \cdot |C|$ such pairs, the number of light R's is at least
  $$\frac{p \cdot (1/|C|+\epsilon) \cdot 2^L \cdot |C|}{(1/|C|+\epsilon/2) \cdot |C|} = \frac{p \cdot (1/|C|+\epsilon)}{(1/|C|+\epsilon/2)} \cdot 2^L.$$
- Hence $\frac{p \cdot (1/|C|+\epsilon)}{(1/|C|+\epsilon/2)} \leq 1$ or $p \leq \frac{1/|C|+\epsilon/2}{1/|C|+\epsilon}$.
- For $1/|C|+\epsilon \leq 1$ we have $\frac{1/|C|+\epsilon/2}{1/|C|+\epsilon} < 1-\epsilon/2$.
- Hence $p < 1-\epsilon/2$.

What does it mean?

- Cheating provers succeed with probability at most $1/|C|$, if computing witnesses for elements in L_R is a hard problem.
- Easy to see that cheating provers can always succeed with probability $1/|C|$.
- For Schnorr computing witnesses means computing discrete logorithms.
- Which, currenty, seems to be a hard problem, provided the prime p is chosen carefully.
- Schnorr can easily be generalized to other groups, where computation of discrete logarithm is even harder than in $\mathbb{Z}_p$.
- $|C|=2^l$ and can make l suffciently large.
- What about Fiat-Shamir?

Security of Fiat-Shamir - factoring and modular square root

Theorem 3.13 For any $\delta > 0$ and any algorithm A there exists an algorithm A′ with the following properties:

1. If on input $N = p \cdot q$, p,q prime, and $a \leftarrow \mathbb{Z}_N^*$, A finds $b \in \mathbb{Z}_N$ satisfying $b^2 = a \bmod N$ with probability δ, then A′ on input N computes p,q with probability $\delta/2$;

2. If A runs in time T, then A′ runs in time $\mathcal{O}\left(T + \log^2(N)\right)$.

Chinese Remainder Theorem

Chinese Remainder Theorem Let $m_1,\ldots,m_r \in \mathbb{N}$ be pairwise relatively prime, i.e. $\gcd\left(m_i,m_j\right) = 1$ for $i \neq j$. Let $b_1,\ldots,b_r \in \mathbb{N}$ be arbitrary integers. Then the system of congruences

$$\begin{aligned} x &= b_1 \bmod m_1 \\ &\vdots \\ x &= b_r \bmod m_r \end{aligned}$$

has a unique solution modulo $M = m_1 \cdots m_r$.

Corollary 3.14 Let $N = p \cdot q$ be the product of two distinct odd primes. For every $a \in \mathbb{Z}_N^*$ the equation $x^2 = a \bmod N$ has either 0 or 4 solutions. In case of 4 solutions, these solutions are of the form $\pm s_1, \pm s_2, s_2 \not\pm s_1$.

From A to A´

A′ on input N

1. choose $b \leftarrow \mathbb{Z}_N$
2. if $d = \gcd(b,N) \neq 1,$ output $d, N/d$
3. $a := b^2 \bmod N$
4. simulate A with input N,a to obtain $w \in \mathbb{Z}_N^*$
5. if $w^2 = a \bmod N$ and $w \neq \pm b \bmod N,$ compute $d = \gcd(w-b,N)$ and output $d, N/d$

Parallel Fiat-Shamir protocol

P on input (N,v,w)

V on input (N,v)

$k_i \leftarrow \mathbb{Z}_N^*, a_i := k_i^2 \bmod N,$
$i = 1,\ldots,l$

$\xrightarrow{(a_1,\ldots,a_l)}$

$c \leftarrow \{0,1\}^l$
$c = (c_1,\ldots,c_l)$

$\xleftarrow{c}$

$r_i := k_i \cdot w^{c_i} \bmod N,$
$i = 1,\ldots,l$

$\xrightarrow{(a_1,\ldots,a_l)}$

accepts, iff for all i

$r_i^2 = a_i \cdot v^{c_i} \bmod N$

Parallel Fiat-Shamir protocol

Theorem 3.15 The parallel Fiat-Shamir protocol is a Σ- protocol for relation R_{QR}.