IV. Interactive & zero-knowledge protocols

- interactive protocols formalize what can be recognized by polynomial time restricted verifiers in arbitrary protocols
- generalize NP
- generalize three round protocols
- zero-knowledge formalizes that verifiers learn nothing beyond recognizing language
- generalizes special honest verifier zero-knowledge protocols
- leads to better understanding of special honest verifier zero-knowledge protocols
- leads to four round identification protocols with all desirable security properties

Class NP and verifiers

Definition 4.1 A verifier V for language $L \subseteq \Sigma^*$ is a computable function $V : \Sigma^* \times \{0,1\}^* \to \{0,1\}$ such that

$$L = \left\{ x \in \Sigma^* \middle| \exists w \in \{0,1\}^* : V(x,w) = 1 \right\}.$$

Definition 4.2 V is a polynomial verifier for language $L \subseteq \Sigma^*$ if V is a verifier for L and

1. the running time of V on input (x,w) is polynomial in $|v|$,
2. there is a polynomial p:$\mathbb{N} \to \mathbb{N}$ such that for all $x \in L$ there is a $x \in \{0,1\}^{p(|x|)}$ with $V(x,w) = 1$.

If language L has a polynomial verifier we call it polynomially verifiable.

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.
- $L_R := \{x \in \{0,1\}^* : W(x) \neq \emptyset\}$ 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 $L = L_R$.

Class NP and verifiers

Theorem 4.3 A language L is in NP if and only if there is a polynomial verifier for L.

verifier

$x \in L$?

prover

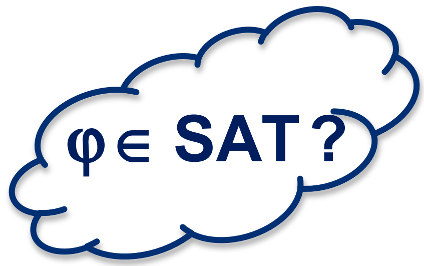
try w!

outputs 1, iff

$$V(x, w) = 1$$

SAT and NP

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



verifier

prover

try assignment w!

outputs 1, iff

$$\varphi(w) = 1$$

SAT ∈ NP.

Quadratic residues

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

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

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

$$QR := \{ (N,v) \mid v \in QR(N) \}$$
$$QNR := \{ (N,v) \mid v \notin QR(N) \}$$

Property If $v \in QR(N)$ and $u \in QNR(N)$, then $v \cdot u \in QNR(N)$.

QR is in NP

Observation QR $\in$ NP.

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

verifier

prover

try w!

$\longleftarrow$

outputs 1, iff

$w^2 = v \bmod N$

Quadratic non-residues and protocols

What about QNR and NP?

Don't know, but ….

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

verifier

prover

$b \leftarrow \{0,1\}, r \leftarrow \mathbb{Z}_N^*,$

$y := r^2 \cdot v^b \bmod N$

$\xrightarrow{\quad y \quad}$

b'

$\xleftarrow{\quad b' \quad}$

outputs 1 iff $b = b'$

Quadratic non-residues and protocols

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

verifier

prover

$b \leftarrow \{0,1\}, r \leftarrow \mathbb{Z}_N^*,$

$y := r^2 \cdot v^b \bmod N$ $\xrightarrow{\quad y \quad}$

$\xleftarrow{\quad b' \quad}$ b'

outputs 1 iff $b = b'$

Properties

- If $(N, v) \in QNR$, then P can make V accept with prob. 1.
- If $(N, v) \in QR$, then no matter what P does, V accepts only with prob. $1/2$.

Interactive protocols

Interactive protocols

- use randomness
- use communication
- allow error in acceptance/rejection

Definition 4.4 A language L is in the class IP, if there are V,P and a protocol V/P with

1. for all $x \in L$ the verifier V outputs 1 with probability $\geq 2/3$ after execution of V/P with input w,
2. for all $x \notin L$ and all provers P' the verifier outputs 1 with probability $\leq 1/3$ after execution of V/P' with P' and input x,
3. the overall running time of V is polynomial.

Interactive protocols

Definition 4.4 A language L is in the class IP, if there are V,P and a protocol V/P with

1. for all $x \in L$ the verifier V outputs 1 with probability $\geq 2/3$ after execution of V/P with input w,
2. for all $x \notin L$ and all provers P' the verifier outputs 1 with probability $\leq 1/3$ after execution of V/P' with P' and input x,
3. the overall running time of V is polynomial.

Remarks

- In protocol V/P' V behaves as in V/P, but P' may behave differently from P.
- May assume that format of message of P' is as in V/P.
- Constants $2/3$ and $1/3$ are arbitrary are arbitrary, $(1/2+\varepsilon)$ & $(1/2-\varepsilon)$ suffice.

QR,QNR and IP

Observation QR and QNR are in IP.

Theorem 4.5 NP $\subseteq$ IP.

QR is in NP

Observation **QR $\in$ NP.**

verifier $(\mathbf{N}, \mathbf{v}) \in \mathbb{N} \times \mathbb{Z}_{\mathbf{N}}^{*}$ **prover**

try w!

outputs 1, iff

$\mathbf{w}^2 = \mathbf{v} \bmod \mathbf{N}$

Fiat-Shamir revisited

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

Properties

- If $(N,v) \in QR$, then P can make V accept with prob. 1.
- If $(N,v) \in QNR$, then no matter what P' does, V accepts only with prob. $1/2$.

Transcripts

Definition 4.6 Let L be a language, $v \in L$ and V/P be an interactive protocol for L. A transcript or communication $\tau \in \{0,1\}^*$ of V/P on input v consists of all messages exchanged between V and P. By $T_{V,P}(x)$ we denote the random variable corresponding to these transcripts, i.e. $\Pr\left[T_{V,P}(x) = \tau\right]$ denotes the probability that the transcript of V/P on input x is τ.

Remark Similarly for a probabilistic algorithm S we denote by $S(x)$ the random variable corresponding to the output of S on input x, i.e. by $\Pr\left[S(x) = \tau\right]$ we denote the probability that S on input x outputs τ.

Zero-knowledge protocols

Definition 4.7 Let L be a language and V/P be an interactive protocol for L. Protocol V/P is called a (honest verifier) zero-knowledge protocol, if there is a ppt S such that for all $x \in L$ and all $\tau \in \{0,1\}^*$

$$\Pr\left[T_{V,P}(x) = \tau\right] = \Pr\left[S(x) = \tau\right].$$

Remarks

– Definition only says something about $x \in L$.

– ppt verifier V learn nothing from execution of V/P since all it learns (=transcript) it can compute alone (via S).

Zero-knowledge protocols and Fiat-Shamir

Theorem 4.8 The Fiat-Shamir protocol is a zero-knowledge protocol for the language QR.

Zero-knowledge protocols and Fiat-Shamir

Theorem 4.8 The Fiat-Shamir protocol is a zero-knowledge protocol for the language QR.

Zero-knowledge protocols and Fiat-Shamir

Theorem 4.8 The Fiat-Shamir protocol is a zero-knowledge protocol for the language QR.

Why is zero-knowledge possible?

- Protocol and simulator compute same transcripts, but in different order.
- In Fiat-Shamir, first compute square, then square root.
- In simulator, first compute root, then square it.
- Squaring is easy, taking square roots modulo N (probably) not.

Perfect zero-knowledge protocols

Definition 4.9 Let L be a language and V/P be an interactive protocol for L. Protocol V/P is called a perfect zero-knowledge protocol, if for all ppt verifiers V^* there is a ppt S^* such that for all $x \in L$ and all $\tau \in \{0,1\}^*$

1. with probability $\leq 1/2$ S^* output a special symbol $\perp$,
2. $\Pr\left[T_{V^*,P}(x) = \tau\right] = \Pr\left[S^*(x) = \tau \mid S^*(x) \neq \perp\right]$.

Remarks

- In protocol V^*/P P behaves as in V/P, but V^* may behave differently from V.
- May assume that format of message of V^* is as in V/P.

Zero-knowledge protocols and Fiat-Shamir

Theorem 4.10 The Fiat-Shamir protocol is a perfect zero-knowledge protocol for the language QR.

S^* on input $v \in \mathbb{Z}_N^*$

- $c \leftarrow \{0,1\}, r \leftarrow \mathbb{Z}_N^*, a := r^2 \cdot v^{-c} \bmod N$
- simulate V^* with input (v,N,a), until V^* outputs a bit b'.
- if $b \neq b'$, output $\perp$, else output (a,c,r)

Parallel Fiat-Shamir protocol

P on input (N,v,w)

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

$i = 1,\ldots,l$

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

V on input (N,v)

$c \leftarrow \{0,1\}^l$

$c = (c_1,\ldots,c_l)$

$\xleftarrow{c}$

$r_i := k_i \cdot w^{c_i} \bmod N,$

$i = 1,\ldots,l$

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

accepts, iff for all i

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

Oberservation The parallel Fiat-Shamir protocol is not known to be perfect zero-knowledge

Schnorr identification protocol

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

Zero-knowledge protocols and Schnorr

Theorem 4.11 The Schnorr protocol is a zero-knowledge protocol.

Observations

- The Schnorr protocol is not known to be perfect zero-knowledge unless 2^l is small.
- No attacks against Schnorr protocol are known.

Sequential Fiat-Shamir

1. For i=1 to l P and V do:

P | **V**

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

$\xrightarrow{a_i}$

$c_i \leftarrow \{0,1\}$

$\xleftarrow{c_i}$

$r_i := k_i \cdot w^{c_i} \bmod N$

$\xrightarrow{r_i}$

rejects if $k_i^2 \neq a_i \cdot v^{c_i} \bmod N$

2. V accepts.

Sequential Fiat-Shamir

Observations

- The sequential Fiat-Shamir protocol is perfect zero-knowledge.
- Cheating provers succeed only with probability $\approx 1/2^l$.
- Sequential version of Schnorr has similar properties.
- Both protocols are rather inefficient, due to their sequential round structure.

A perfect zero-knowledge variant of the Schnorr protocol

Preliminaries

- Let G be a group with order p, p prime.
- Denote elements in G by $\alpha, \beta, \gamma, \ldots$
- G is a cyclic group.
- Fix $\gamma \in G \setminus \{1\}$.
- γ is a generator of G.

A perfect zero-knowledge variant of the Schnorr protocol

P on input (p,g,v,w,G,γ) | **V on input (p,g,v,G,γ)**

P		V
	$\xleftarrow{\beta}$	$b \leftarrow \mathbb{Z}_p, \beta := \gamma^b$
$k \leftarrow \mathbb{Z}_{p-1}, a := g^k \bmod p,$ $d \leftarrow \mathbb{Z}_p, \alpha := \gamma^a \beta^d$ (in G)		
	$\xrightarrow{\alpha}$	
		$c \leftarrow \{1,\ldots,2^l\}, 2^l < p$
	$\xleftarrow{c}$	
$r := k - w \cdot c \bmod p-1$		
	$\xrightarrow{a,d,r}$	
		accepts if $\alpha := \gamma^a \beta^d \wedge a = g^r \cdot v^c \bmod p$

Security for the modified Schnorr protocol

Theorem 4.12 The modified Schnorr protocol is a perfect zero-knowledge protocol (assuming b is fixed and known to the simulator).

Theorem 4.13 For any $\varepsilon > 0$ and any algorithm A that there exists an algorithm A' with the following properties:

1. If on input (p, g, v, G, γ) A makes V accept with probability $1/|C| + \varepsilon$, then A' on input x and with probability $\geq \varepsilon/16$ computes a witness $w \in W(x)$ or it can used to compute the discrete logarithm of elements in G to base γ with success probability $\geq \varepsilon/16$.

2. If A runs in time T, then A' runs in time $\mathcal{O}\left(T/\varepsilon + \log(p)^2\right)$.