Interactive protocols & zero-knowledge

- interactive protocols formalize what can be recognized by polynomial time restricted verifiers in arbitrary protocols

- generalizes NP

- zero-knowledge formalizes that verifiers learn nothing beyond recognizing language.

Class NP and verifiers

Definition 3.6 A verifier V for language $L \subseteq \Sigma^*$ is a computable function $V : \Sigma^* \times \{0,1\}^* \to \{0,1\}$ such that

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

Definition 3.7 V is a polynomial verifier for language $L \subseteq \Sigma^*$ if V is a verifier for L and

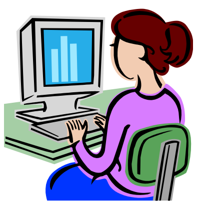
1. the running time of V on input (w,c) is polynomial in $|w|$,
2. there is a polynomial $p : \mathbb{N} \to \mathbb{N}$ such that for all $w \in L$ there is a $c \in \{0,1\}^{p(|w|)}$ with $V(w,c) = 1$.

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

Class NP and verifiers

Theorem 3.8 A language L is in NP if and only if there is a polynomial verifier for L.

verifier



$w \in L$?

prover

try c!

outputs 1, iff

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

SAT and NP

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

verifier

$\varphi \in \text{SAT}\,?$

prover

try assignment c!

outputs 1, iff

$$\varphi(c) = 1$$

SAT $\in$ NP.

Quadratic residues

Definition 3.9 Let $\mathrm{N} \in \mathbb{N}$, then

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

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

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

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

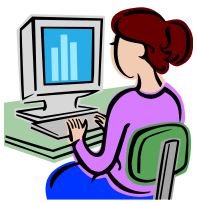
Property If $\mathrm{v} \in \mathrm{QR}(\mathrm{N})$ and $\mathrm{u} \in \mathrm{QNR}(\mathrm{N})$, then $\mathrm{v} \cdot \mathrm{u} \in \mathrm{QNR}(\mathrm{N})$.

QR is in NP

Observation QR $\in$ NP.

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

verifier



prover

try s!

$\longleftarrow$

outputs 1, iff

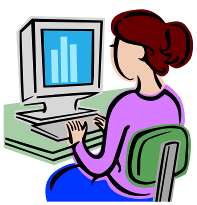
$s^2 = v \bmod N$

Quadratic non-residues and protocols

What about QNR and NP?

Don't know, but ….

verifier



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

prover

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

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

$\xrightarrow{\quad y \quad}$

b'

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

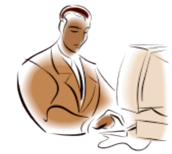
outputs 1 iff $b = b'$

Quadratic non-residues and protocols

verifier

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

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

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

Interactive protocols

Definition 3.10 A language L is in the class IP, if there are V,P and a protocol V/P with

1. for all w $\in$ L the verifier V outputs 1 with probability $\geq 2/3$ after execution of V/P with input w,
2. for all w $\notin$ L and all provers P' the verifier outputs 1 with probability $\leq 1/3$ after execution of V/P' with P' and input w,
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, $(1+\varepsilon)$ & $(1-\varepsilon)$ suffice.

QR,QNR and IP

Observation QR and QNR are in IP.

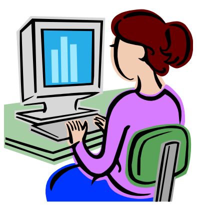
Theorem 3.11 NP $\subseteq$ IP.

QR is in NP

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

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

verifier



prover

try s!

outputs 1, iff

$s^2 = v \bmod N$

Fiat-Shamir revisited

P/A	$(N,v) \in \mathbb{N} \times \mathbb{Z}_N^*$	V/B
$r \leftarrow \mathbb{Z}_N^*, x := r^2 \bmod N$		
	$\xrightarrow{\quad x \quad}$	
		$b \leftarrow \{0,1\}$
	$\xleftarrow{\quad b \quad}$	
$t := r \cdot s_A^b \bmod N$		
	$\xrightarrow{\quad t \quad}$	
		outputs 1, iff $t^2 = x \cdot v_A^b \bmod N$

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. $1/2$.

Fiat-Shamir revisited

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

P/A		V/B
$r_i \leftarrow Z_N^*, x_i := r^2 \bmod N$		
	$\xrightarrow{x_i}$	
		$b_i \leftarrow \{0,1\}$
	$\xleftarrow{b_i}$	
$t_i := r_i \cdot s_A^{b_i} \bmod N$		
	$\xrightarrow{t_i}$	
		rejects if $t_i^2 \neq x_i \cdot v_A^{b_i} \bmod N$

2. V/B accepts.

Transcripts

Definition 3.11 Let L be a language, $v \in L$ and V/P be an interactive protocol for L. A transcript $\tau \in \{0,1\}^*$ of V/P on input v consists of v, the output and all messages exchanged between V and P. By $T_{V,P}(v)$ we denote the random variable corresponding to these transcripts, i.e. $\Pr\left[T_{V,P}(v) = \tau\right]$ denotes the probability that the transcript of V/P on input v is τ.

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

Fiat-Shamir revisited

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

P/A		V/B
$r_i \leftarrow Z_N^*, x_i := r^2 \bmod N$		
	$\xrightarrow{x_i}$	
		$b_i \leftarrow \{0,1\}$
	$\xleftarrow{b_i}$	
$t_i := r_i \cdot s_A^{b_i} \bmod N$		
	$\xrightarrow{t_i}$	
		rejects if $t_i^2 \neq x_i \cdot v_A^{b_i} \bmod N$

2. V/B accepts.

Zero-knowledge protocols

Definition 3.12 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 $v \in L$ and all $\tau \in \{0,1\}^*$

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

Remarks

- Definition only says something about $v \in L$.
- 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 3.13 The Fiat-Shamir protocol is a zero-knowledge protocol for the language QR.

Fact Let $N \in \mathbb{N}$, then every element in $QR(N)$ has the same number of square roots modulo N, namely $|\mathbb{Z}_N^*| / |QR(N)|$.

Fiat-Shamir identification protocol

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

P/A		V/B
$r_i \leftarrow Z_N^*, x_i := r^2 \bmod N$		
	$\xrightarrow{x_i}$	
		$b_i \leftarrow \{0,1\}$
	$\xleftarrow{b_i}$	
$t_i := r_i \cdot s_A^{b_i} \bmod N$		
	$\xrightarrow{t_i}$	
		rejects if $t_i^2 \neq x_i \cdot v_A^{b_i} \bmod N$

2. B accepts.

Zero-knowledge protocols and Fiat-Shamir

Theorem 3.13 **The Fiat-Shamir protocol is a zero-knowledge protocol for the language QR.**

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

- $b \leftarrow \{0,1\}, t \leftarrow \mathbb{Z}_N^*$
- $x := t^2 \cdot v^{-b} \bmod N$
- output $(v,x,b,t,1)$

Zero-knowledge protocols and Fiat-Shamir

Theorem 3.13 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 3.14 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 $v \in L$ and all $\tau \in \{0,1\}^*$

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

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

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

- $b \leftarrow \{0,1\}, t \leftarrow \mathbb{Z}_N^*, x := t^2 \cdot v^{-b} \bmod N$
- simulate V^* with input (v,N,x), until V^* outputs a bit b'.
- if $b \neq b'$, output $\perp$, else output $(v,x,b,t,1)$

Schnorr identification – setup

TA chooses primes p,q such that $q \mid p-1$ and $q > 2^l$,

chooses generator z of $\mathbb{Z}_p^*$ and sets $g := z^{p-1/q}$.

A chooses $a \leftarrow \mathbb{Z}_q$, sets $v_A := g^{-a} \bmod p$.

TA sets $\mathrm{cert}(A) := \left(\mathrm{id}(A), v_A, \mathrm{Sign}_{TA}\left(\mathrm{id}(A), v_A\right)\right)$

Remark g has order q.

Schnorr identification protocol

A

$k \leftarrow \mathbb{Z}_q, x := g^k \bmod p$

$\xrightarrow{\text{cert(A)}, x}$

B

verifies cert(A)

$r \leftarrow \{1,\ldots,2^l\}$

challenge

$\xleftarrow{r}$

$y := k - a \cdot r \bmod q$

$\xrightarrow{y}$

response

accepts iff

$x = g^y \cdot v_A^r \bmod p$

Impersonation in Schnorr protocol

Theorem 3.16 For any $\delta \geq 2^{-l+2}$ and any algorithm C there exists an algorithm C′ with the following properties:

1. If on input p,q,g,v_A C impersonates A with probability $\geq \delta$, then C′ on input p,q,g,v_A computes a discrete logarithm of v_A to base g with probability 0.03;

2. If C runs in time T, then C′ runs in time $\mathcal{O}\left(T/\delta + \log^2(p)\right)$.

From C to C ‘

C′ on input p,q,g,v_A

1. repeat at most $1/\delta$ – times
   a) $z \leftarrow \{0,1\}^R, r \leftarrow \{1,\ldots,2^l\}$
   b) simulate C with random bits z and r
   c) if C succeeds set $r_1 := r$ and goto 2)
2. repeat at most $1/\delta$ – times
   a) $r \leftarrow \{1,\ldots,2^l\}$
   b) simulate C with random bits z and r
   c) if C succeeds set $r_2 := r$ and goto 3)
3. if $r_1 \neq r_2$, output r_1, r_2 and corresponding y_1, y_2.

Zero-knowledge protocols and Schnorr

Theorem 3.17 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.

Okamoto protocol

- efficiency similar to Schnorr
- still not zero-knowledge
- but witness hiding