Fiat-Shamir identification

– offers security against cheating prover:

Theorem 3.5 (restated) For any $\delta \geq 2^{-l+2}$ and any algorithm C there exists an algorithm C′ with the following properties:

1. If on input N, v_A C impersonates A with probability $\geq \delta$, then C′ on input N, v_A computes a square root of $v_A \bmod N$ with probability 0.03;

2. If C runs in time T, then C′ runs in time $\mathcal{O}(T/\delta)$.

– offers security against cheating verifier:

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

Proofs of knowledge - preliminaries

- $R \subseteq \{0,1\}^* \times \{0,1\}^*$ 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

Proofs of knowledge - preliminaries

Observation

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

Definition 3.7 (restated) 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.

Relations and languages - examples

Example $L = SAT$

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

Example $L = QR$

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

Example $L = DL$

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

Fiat-Shamir identification protocol

A		B
$r \leftarrow \mathbb{Z}_N^*, x := r^2 \bmod N$		
	cert(A),x →	
		verifies cert(A)
	challenge b ←	$b \leftarrow \{0,1\}$
$t := r \cdot s_A^b \bmod N$		
	t → response	accepts iff $t^2 = x \cdot v_A^b \bmod N$

Fiat-Shamir identification - security

Theorem 3.4 (restated) For any $\varepsilon > 0$ and any algorithm C thereexists an algorithm C' with the following properties:

1. If on input N,v_A C impersonates A with probability $1/2 + \varepsilon, \varepsilon > 0,$ then C' on input N,v_A computes a square root of v_A mod N with probability 1/2;

2. If C runs in time T, then C' runs in time $\mathcal{O}(T/\varepsilon)$.

Fiat-Shamir proves knowledge of a witness for (N,v_A) in relation R_{QR}!

Schnorr identification protocol

A		B
$k \leftarrow \mathbb{Z}_{p-1}, x := g^k \bmod p$		
	cert(A),x $\longrightarrow$	
		verifies cert(A)
	challenge	$r \leftarrow \{1,\ldots,2^l\}$
	r $\longleftarrow$	
$y := k + a \cdot r \bmod p\text{-}1$		
	y $\longrightarrow$	
	response	accepts iff
		$x = g^y \cdot v_A^r \bmod p$

Impersonation in Schnorr protocol

Theorem 3.16 (restated) 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,g,v_A C impersonates A with probability $\geq \delta$, then C′ on input p,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 $\mathcal{O}\left(T/\delta + \log^2(p)\right)$.

Schnorr proves knowledge of a witness for (p,g,v_A) in relation R_{DL}!

Definition of proofs of knowledge

- V/P interactive protocol for some language L
- R relation with $L_R = L$
- K probabilistic polynomial time algorithm
- P^* (cheating) prover for V/P

K has oracle access to prover P^*, if

1. K can chose randomness r used by P^*.
2. K can fix an initial part x of the communication between V,P^*.
3. K obtains as answer the next message from P^* given r and x.

Definition of proofs of knowledge

K has oracle access to prover P^*, if

1. K can chose randomness r used by P^*.
2. K can fix an initial part x of the communication between V,P^*.
3. K obtains as answer the next message from P^* given r and x.

Oracle access can be used to

- simulate runs of protocol V/P^*
- simulate runs of protocol V/P^*, where randomness of P^* and initial part x is fixed
- initial part may be obtained from previous simulations

Definition of proofs of knowledge

Definition 3.17 Let V/P be an interactive proof for a language $L_R \in NP$, where L_R for relation R. V/P is called a proof of knowledge with knowledge error δ, if there is a ppt K (with oracle access to provers) such that for all provers P^* and every x satisfying

$$\Pr\left[V / P^*(x) = \text{accept}\right] \geq \delta + \epsilon$$

$K^{P^*}(x)$ outputs an element $w \in W(x)$ in time polynomial in $|x|$ and $1/\varepsilon$.

The running time of K is allowed to be expected polynomial time.

Fiat-Shamir and proofs of knowledge

Theorem 3.4 (restated) For any $\varepsilon > 0$ and any algorithm C there exists an algorithm C′ with the following properties:

1. If on input N, v_A C impersonates A with probability $1/2 + \varepsilon, \varepsilon > 0$, then C′ on input N, v_A computes a square root of $v_A \bmod N$ with probability 1/2;

2. If C runs in time T, then C′ runs in time $\mathcal{O}(T/\varepsilon)$.

Corollary 3.18 The Fiat-Shamir protocol is a proof of knowledge with knowledge error 1/2.

From C to C ‘

C' on input N, v_A

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

Impersonation in Schnorr protocol

Theorem 3.16 (restated) 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, g, v_A C impersonates A with probability $\geq \delta$, then C′ on input p, 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 $\mathcal{O}\left(T/\delta + \log^2(p)\right)$.

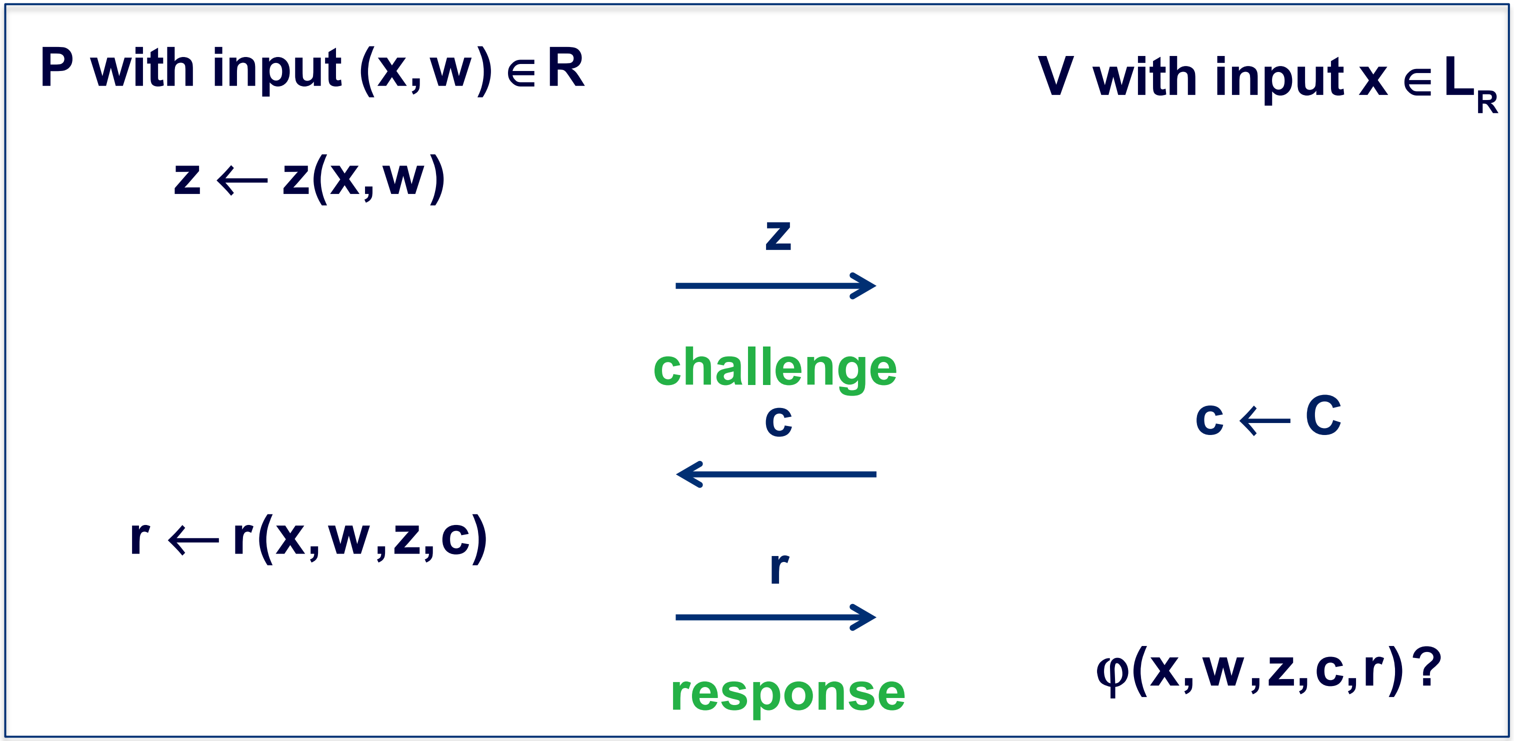
Corollary 3.19 The Schnorr protocol is a proof of knowledge with knowledge error 2^{-l+2}.

Σ- protocols

- R, L_R as before
- C some finite set, often additive group

P		V
P with input $(x,w) \in R$		V with input $x \in L_R$
$z \leftarrow z(x,w)$	z $\longrightarrow$	
	challenge c $\longleftarrow$	$c \leftarrow C$
$r \leftarrow r(x,w,z,c)$	r $\longrightarrow$ response	
		$\varphi(x,w,z,c,r)$?

Σ- protocols



Definition 3.20 A three round protocol as above is called a Σ-protocol if it satisfies the three properties

1. completeness
2. special soundness
3. special honest verifier zero-knowledgeness.

Σ- protocols - properties

completeness If P and V follow the protocol, then V always accepts.

special soundness There exists a ppt algorithm E (extractor) which given $x \in L_R$ and any two accepting transcripts (z,c,r) and (a,c',r') with $c \neq c'$ computes a witness w satisfying $(x,w) \in R$.

special honest verifier zero-knowledgeness There exists a ppt algorithm S (simulator) which given any $x \in L_R$ and any challenge c produces transcripts (z,c,r) with the same distribution as in the real protocol V/P.

Schnorr protocol

P		V
$k \leftarrow \mathbb{Z}_{p-1}, z := g^k \bmod p$	$\xrightarrow{z}$	
	challenge	$c \leftarrow \{1,\ldots,2^l\}$
	$\xleftarrow{c}$	
$r := k - w \cdot c \bmod p\text{-}1$	$\xrightarrow{r}$	
	response	accepts iff $z = g^r \cdot v^c \bmod p$

Lemma 3.21 The Schnorr protocol is a Σ-protocol for the relation R_{DL}.

Example $L = DL$

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

Σ- protocols, proofs of knowledge, extractors

Theorem 3.22 Every Σ-protocol is a proof of knowledge with knowledge error $1/|C|$.

Σ- protocols and zero-knowledgeness

Theorem 3.23 Every Σ-protocol can be transformed into a zero-knowledge protocol.

The tranformed protocol:

P with input $(x,w) \in R$		V with input $x \in L_R$
$z \leftarrow z(x,w), c_P \leftarrow C$	(z,c_P) $\longrightarrow$	
	challenge c_V $\longleftarrow$	$c_V \leftarrow C$
$r \leftarrow r(x,w,z,c_P + c_V)$	r $\longrightarrow$ response	$\varphi(x,w,z,c_P + c_V, r)$?

Composition of $\sum$-protocols - AND

Example $L = AND - DL$

- $p \in \mathbb{N}$ prime, $g, v \in \mathbb{Z}_p^*, x_i = (p, g, v_i), v_i, w_i \in \mathbb{Z}_{p-1}, i = 1,2$
- $R_{DL}(x_1, w_1, x_2, w_2) = 1 :\Leftrightarrow g^{w_i} = v_i \bmod p, i = 1,2$

P | **V**

P: $k_i \leftarrow \mathbb{Z}_{p-1}, z_i := g^{k_i} \bmod p$, $i = 1,2$

P → V: z_1, z_2

challenge

V: $c \leftarrow \{1, \ldots, 2^l\}$

V → P: c

P: $r_i := k_i - w \cdot c \bmod p\text{-}1$, $i = 1,2$

P → V: r_1, r_2

response

V accepts iff

$z_i = g^{r_i} \cdot v_i^c \bmod p, i = 1,2$

Composition of $\sum$-protocols - OR

Example L = OR-DL

- $p \in \mathbb{N}$ prime, $g, v \in \mathbb{Z}_p^*, x_i = (p, g, v_i), v_i, w_i \in \mathbb{Z}_{p-1}, i = 1,2$
- $R_{OR-DL}(x_1, w_1, x_2, w_2) = 1 :\Leftrightarrow \exists i : g^{w_i} = v_i \bmod p$

Assume P knows w_1 with $g^{w_1} = v_1 \bmod p$.

1. P chooses $c_2 \leftarrow C$, and using simulator computes transcript (z_2, c_2, r_2). P also chooses $k_1 \leftarrow \mathbb{Z}_{p-1}$, sets $z_1 := g^{k_1} \bmod p$ and sends (z_1, z_2) to V.
2. V chooses $c \leftarrow C$ and sends it to P.
3. P computes $c_1 := c - c_2$ and $r_1 := k_1 - w_1 c_1 \bmod p-1$. P sends (r_1, r_2) to V.
4. V accepts iff $z_i = g^{r_i} v_i^{c_i} \bmod p$, for $i = 1,2$, and $c_1 + c_2 = c \bmod p-1$.