Schnorr = GQ = Okamoto:

Unifying Zero-knowledge Proofs of Knowledge

Ueli Maurer

ETH Zurich

CRYPTO 2009 Rump Session

Fiat-Shamir protocol

Prover Peggy		**Verifier Vic**
knows $x \in \mathbb{Z}_m^*$		$z = x^2$
$k \in_R \mathbb{Z}_m^*$		
$t = k^2$	$\xrightarrow{t}$	
		$c \in_R \{0, 1\}$
	$\xleftarrow{c}$	
$r = k \cdot x^c$	$\xrightarrow{r}$	$r^2 \stackrel{?}{=} t \cdot z^c$

Guillou-Quisquater protocol

Prover Peggy		Verifier Vic
knows $x \in \mathbb{Z}_m^*$		$z = x^e$
$k \in_R \mathbb{Z}_m^*$		
$t = k^e$	$\xrightarrow{\quad t \quad}$	
	$\xleftarrow{\quad c \quad}$	$c \in_R [1, e-1]$
$r = k \cdot x^c$	$\xrightarrow{\quad r \quad}$	$r^e \stackrel{?}{=} t \cdot z^c$

Schnorr protocol

Prover Peggy		**Verifier Vic**
knows $x \in \mathbb{Z}_q$		$z = h^x$
$k \in_R \mathbb{Z}_q$		
$t = h^k$	$\xrightarrow{t}$	
		$c \in_R [0, q-1]$
	$\xleftarrow{c}$	
$r = k + x^c$		
	$\xrightarrow{r}$	$h^r \stackrel{?}{=} t \cdot z^c$

Group homomorphisms

A group homomorphism from a group $\langle G, \star \rangle$ **to a group** $\langle H, \otimes \rangle$ **is a function** $f : G \rightarrow H$ **such that**

$$f(a \star b) = f(a) \otimes f(b)$$

Group homomorphisms

A group homomorphism from a group $\langle G, \star \rangle$ to a group $\langle H, \otimes \rangle$ is a function $f : G \rightarrow H$ such that

$$f(a \star b) = f(a) \otimes f(b)$$

We write $[a]$ for $f(a)$; hence we have $[a \star b] = [a] \otimes [b]$

Group homomorphisms

A group homomorphism from a group $\langle G, \star \rangle$ to a group $\langle H, \otimes \rangle$ is a function $f : G \rightarrow H$ such that

$$f(a \star b) = f(a) \otimes f(b)$$

We write $[a]$ for $f(a)$; hence we have $[a \star b] = [a] \otimes [b]$

Examples:

- $G = \langle \mathbb{Z}_q, + \rangle$, $H = \langle h \rangle$ **cyclic group gen. by** h
  $[a] = h^a : \quad [a + b] = h^a \cdot h^b = h^{a+b}$

- $G = H = \langle \mathbb{Z}_m, \cdot \rangle$
  $[a] = a^e : \quad [a \cdot b] = (a \cdot b)^e = a^e \cdot b^e$

POK of a pre-image of a group homom.

$$\langle G, \star \rangle \to \langle H, \otimes \rangle : \quad a \mapsto [a]$$

Prover Peggy		Verifier Vic
knows $x \in G$		$z = [x] \in H$
$k \in_R G$		
$t = [k]$	$\xrightarrow{\ t\ }$	
	$\xleftarrow{\ c\ }$	$c \in_R \mathcal{C} \subseteq \mathbb{Z}$
$r = k \star x^c$	$\xrightarrow{\ r\ }$	$[r] \stackrel{?}{=} t \otimes z^c$

Prover Peggy		**Verifier Vic**
knows $x \in G$		$z = [x] \in H$
$k \in_R G$		
$t = [k]$	$\xrightarrow{t}$	
	$\xleftarrow{c}$	$c \in_R \mathcal{C} \subseteq \mathbb{Z}$
$r = k \star x^c$	$\xrightarrow{r}$	$[r] \stackrel{?}{=} t \otimes z^c$

Theorem: **If values** $\ell \in \mathbb{Z}$ **and** $u \in G$ **are known such that**

(1) $\mathrm{gcd}(c - c', \ell) = 1$ **for all** $c, c' \in \mathcal{C}$ **(with** $c \neq c'$**),**

(2) $[u] = z^{\ell}$,

then the protocol round is 2-extractable.

Prover Peggy		Verifier Vic
knows $x \in G$		$z = [x] \in H$
$k \in_R G$		
$t = [k]$	$\xrightarrow{\ t\ }$	
	$\xleftarrow{\ c\ }$	$c \in_R \mathcal{C} \subseteq \mathbb{Z}$
$r = k \star x^c$	$\xrightarrow{\ r\ }$	
		$[r] \stackrel{?}{=} t \otimes z^c$

Theorem: **If values $\ell \in \mathbb{Z}$ and $u \in G$ are known such that**

(1) $\gcd(c - c', \ell) = 1$ **for all $c, c' \in \mathcal{C}$ (with $c \neq c'$),**

(2) $[u] = z^{\ell}$**,**

then the protocol round is 2-extractable.

Theorem: **The protocol consisting of s rounds is a proof of knowledge if $1/|\mathcal{C}|^s$ is negligible, and it is zero-knowledge if $|\mathcal{C}|$ is polynomially bounded.**

Theorem: **If values $\ell \in \mathbb{Z}$ and $u \in G$ are known such that**

(1) $\mathsf{gcd}(c - c', \ell) = 1$ **for all $c, c' \in \mathcal{C}$ (with $c \neq c'$),**

(2) $[u] = z^\ell$,

then the protocol round is 2-extractable.

Example: Schnorr

$$(G, \star) = (\mathbb{Z}_q, +)$$

$H = \langle h \rangle$ **cyclic group, order q**

$$G \to H: \quad x \mapsto [x] = h^x$$

$$\ell = q$$

$$u = 0$$

Theorem: **If values $\ell \in \mathbb{Z}$ and $u \in G$ are known such that**

(1) $\mathsf{gcd}(c - c', \ell) = 1$ **for all $c, c' \in \mathcal{C}$ (with $c \neq c'$),**

(2) $[u] = z^{\ell}$,

then the protocol round is 2-extractable.

Example: Guillou-Quisquater

$$(G, \star) = (\mathbb{Z}_m, \cdot)$$

$$(H, \otimes) = (\mathbb{Z}_m, \cdot)$$

$$G \rightarrow H : \quad x \mapsto [x] = x^e \qquad \textbf{(}e\textbf{ prime)}$$

$$\ell = e$$

$$u = z$$

Theorem: **If values $\ell \in \mathbb{Z}$ and $u \in G$ are known such that**

(1) $\gcd(c - c', \ell) = 1$ **for all $c, c' \in \mathcal{C}$ (with $c \neq c'$),**

(2) $[u] = z^\ell$,

then the protocol round is 2-extractable.

POK of several values:

$$G_i \to H_i : \quad x \mapsto [x]^{(i)}; \qquad [u_i]^{(i)} = z_i^\ell \quad \textbf{(same } \ell\textbf{)}$$

$$(G, \star) = G_1 \times \cdots \times G_n$$

$$(H, \otimes) = H_1 \times \cdots \times H_n$$

$$G \to H : (x_1, \ldots, x_n) \mapsto \left([x_1]^{(1)}, \ldots, [x_n]^{(n)}\right)$$

$$[u_i]^{(i)} = z_i^\ell, \quad i = 1, \ldots, n$$

$$u = (u_1, \ldots, u_n), \quad z = (z_1, \ldots, z_n)$$

Theorem: **If values $\ell \in \mathbb{Z}$ and $u \in G$ are known such that**

(1) $\mathrm{gcd}(c - c', \ell) = 1$ **for all $c, c' \in \mathcal{C}$ (with $c \neq c'$),**

(2) $[u] = z^{\ell}$**,**

then the protocol round is 2-extractable.

Proof of equality of embedded values:

$$G \to H_i : \quad x \mapsto [x]^{(i)};$$

$$[u]^{(i)} = z_i^{\ell} \qquad \text{(same } u, \ell\text{)}$$

$$H = H_1 \times \cdots \times H_n$$

$$G \to H : \; x \mapsto [x] = \left([x]^{(1)}, \ldots, [x]^{(n)}\right)$$

$$z = (z_1, \ldots, z_n)$$

Theorem: **If values $\ell \in \mathbb{Z}$ and $u \in G$ are known such that**

(1) $\mathsf{gcd}(c - c', \ell) = 1$ **for all $c, c' \in \mathcal{C}$ (with $c \neq c'$),**

(2) $[u] = z^{\ell}$**,**

then the protocol round is 2-extractable.

POK of a representation (e.g. Pedersen commitments):

group H with prime order q, generators $h_1, \ldots, h_m$

repr. of $z \in H$: $(x_1, \ldots, x_m)$ with $z = h_1^{x_1} h_2^{x_2} \cdots h_m^{x_m}$

$G = \mathbb{Z}_q^m$

$G \to H : (x_1, \ldots, x_m) \mapsto h_1^{x_1} \cdots h_m^{x_m}$

$\ell = q$

$u = (0, \ldots, 0)$

Theorem: **If values $\ell \in \mathbb{Z}$ and $u \in G$ are known such that**

(1) $\mathrm{gcd}(c - c', \ell) = 1$ **for all $c, c' \in \mathcal{C}$ (with $c \neq c'$),**

(2) $[u] = z^{\ell}$**,**

then the protocol round is 2-extractable.

Correctness proof for a Diffie-Hellman key:

$$A = g^a,\ B = g^b,\ C \stackrel{?}{=} g^{ab}$$

$$\mathbb{Z}_q \to H \times H : \quad x \mapsto [x] = (h^x, B^x)$$

Prove knowledge of preimage of (A, C)