

Schnorr = GQ = Okamoto:
**Unifying Zero-knowledge Proofs
of Knowledge**

Ueli Maurer

ETH Zurich

CRYPTO 2009 Rump Session

Fiat-Shamir protocol

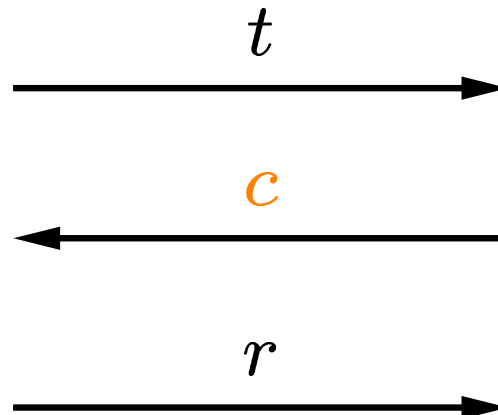
Prover Peggy

knows $x \in \mathbb{Z}_m^*$

$k \in_R \mathbb{Z}_m^*$

$t = k^2$

$r = k \cdot x^c$



Verifier Vic

$z = x^2$

$c \in_R \{0, 1\}$

$r^2 \stackrel{?}{=} t \cdot z^c$

Guillou-Quisquater protocol

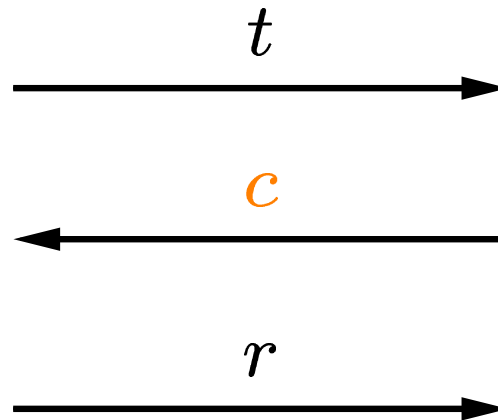
Prover Peggy

knows $x \in \mathbb{Z}_m^*$

$k \in_R \mathbb{Z}_m^*$

$t = k^e$

$r = k \cdot x^c$



Verifier Vic

$z = x^e$

$c \in_R [1, e - 1]$

$r^e \stackrel{?}{=} t \cdot z^c$

Schnorr protocol

Prover Peggy

knows $x \in \mathbb{Z}_q$

$k \in_R \mathbb{Z}_q$

$t = h^k$

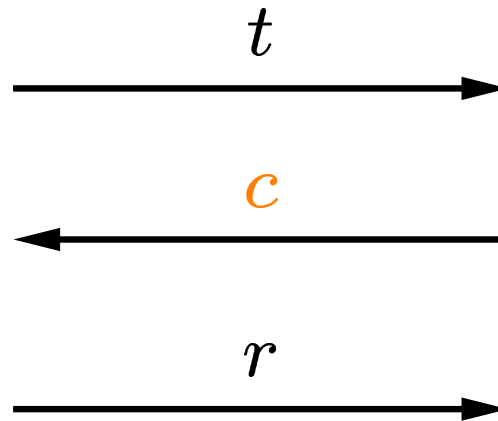
$r = k + x^c$

Verifier Vic

$z = h^x$

$c \in_R [0, q - 1]$

$h^r \stackrel{?}{=} t \cdot z^c$



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

$$[a] = h^a : [a + b] = h^a \cdot h^b = h^{a+b}$$

- $G = H = \langle \mathbb{Z}_m, \cdot \rangle$

$$[a] = a^e : [a \cdot b] = (a \cdot b)^e = a^e \cdot b^e$$

POK of a pre-image of a group homom.

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

Prover Peggy

knows $x \in G$

$k \in_R G$

$t = [k]$

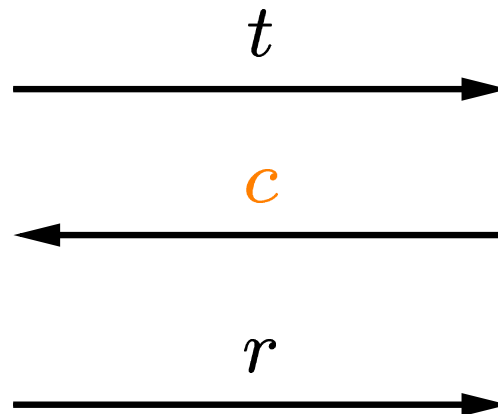
$r = k \star x^c$

Verifier Vic

$z = [x] \in H$

$c \in_R \mathcal{C} \subseteq \mathbb{Z}$

$[r] \stackrel{?}{=} t \otimes z^c$



Prover Peggy

knows $x \in G$

$k \in_R G$

$t = [k]$

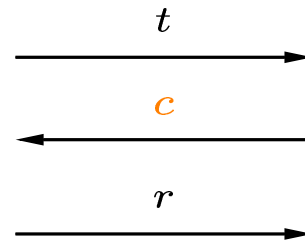
$r = k \star x^c$

Verifier Vic

$z = [x] \in H$

$c \in_R \mathcal{C} \subseteq \mathbb{Z}$

$[r] \stackrel{?}{=} t \otimes z^c$



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.

Prover Peggy

knows $x \in G$

$k \in_R G$

$t = [k]$

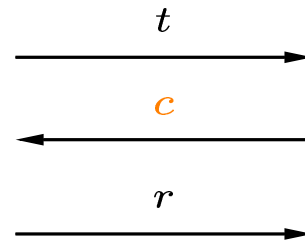
$r = k \star x^c$

Verifier Vic

$z = [x] \in H$

$c \in_R \mathcal{C} \subseteq \mathbb{Z}$

$[r] \stackrel{?}{=} t \otimes z^c$



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

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

then the protocol round is 2-extractable.

Example: Schnorr

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

$$H = \langle h \rangle \quad \text{cyclic group, order } q$$

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

$$\ell = q$$

$$u = 0$$

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

(1) $\gcd(c - c', \ell) = 1$ 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

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

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

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

$$\ell = e$$

$$u = z$$

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:

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

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

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

$$G \rightarrow H : (x_1, \dots, x_n) \mapsto ([x_1]^{(1)}, \dots, [x_n]^{(n)})$$

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

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

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.

Proof of equality of embedded values:

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

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

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

$$G \rightarrow H : x \mapsto [x] = ([x]^{(1)}, \dots, [x]^{(n)})$$

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

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 a representation (e.g. Pedersen commitments):

group H with prime order q , generators h_1, \dots, h_m

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

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

$$G \rightarrow H : (x_1, \dots, x_m) \mapsto h_1^{x_1} \dots h_m^{x_m}$$

$$\ell = q$$

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

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.

Correctness proof for a Diffie-Hellman key:

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

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

Prove knowledge of preimage of (A, C)