Cryptographic Protocols

Spring 2017

Part 4

Guillou-Quisquater – One Round of the Protocol

Setting: m is an RSA-Modulus.
Goal: Prove knowledge of an e-th root of a given $z \in \mathbb{Z}_m^*$.

Peggy		Vic
knows x s.t. $x^e = z \pmod m$		knows $z \in \mathbb{Z}_m^*$
$k \in_R \mathbb{Z}_m^*$, $t = k^e$	$\xrightarrow{t}$	
	$\xleftarrow{c}$	$c \in_R \{0, \ldots, e-1\}$
$r = k \cdot x^c$	$\xrightarrow{r}$	$r^e \stackrel{?}{=} t \cdot z^c$

One-Way Group Homomorphisms (OWGH)

Setting: Groups $\langle G, \star\rangle$ and $\langle H, \otimes\rangle$

Definition: A **group homomorphism** is a function f with:

$$f: \; G \to H, \quad f(a \star b) = f(a) \otimes f(b)$$

Notation: We write $[a]$ for $f(a)$, hence

$$[\,]: \; G \to H, \quad [a \star b] = [a] \otimes [b]$$

Examples

cyclic group gen. by h

- $G = \langle \mathbb{Z}_q, +\rangle$, $H = \langle h\rangle$ with $|H| = q$, $[a] = h^a$:
  $\rightarrow$ $[a+b] = h^{a+b} = h^a \cdot h^b = [a] \cdot [b]$
- $G = H = \langle \mathbb{Z}_m, \cdot\rangle$, $[a] = a^e$:
  $\rightarrow$ $[a \cdot b] = (a \cdot b)^e = a^e \cdot b^e = [a] \cdot [b]$.

PoK of Pre-Image of OWGH – One Round of the Protocol

Setting: Groups G and H, group homomorphism $[\,]: \langle G, \star\rangle \mapsto \langle H, \otimes\rangle$.
Goal: Prove knowledge of pre-image of $z \in H$.

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

Knowledge Extractor of OWGH PoK

Theorem 1.5: Protocol round is 2-extractable if

$\exists \ell \in \mathbb{Z}, u \in G$ s.t. (1) $\forall c_1, c_2 \in \mathcal{C}, c_1 \neq c_2 : \gcd(c_1 - c_2, \ell) = 1$
(2) $[u] = z^\ell$

Proof: Given accepting conversations (t, c_1, r_1), (t, c_2, r_2) with $c_1 \neq c_2$, and ℓ, u as above. Extract pre-image x' with $[x'] = z$ as follows:

1. $$\begin{array}{rcl} [r_1] & = & t \otimes z^{c_1} \\ \hline [r_1 \star r_2^{-1}] & = & z^{c_1 - c_2} \end{array}$$
2. Extended Euclidean Algorithm $\Rightarrow a, b$ s.t. $a\ell + b(c_1 - c_2) = 1$
3. $$\begin{aligned} z &= z^1 = z^{a\ell + b(c_1-c_2)} = z^{a\ell} \otimes z^{b(c_1-c_2)} \\ &= \left(z^\ell\right)^a \otimes \left(z^{c_1-c_2}\right)^b = [u]^a \otimes [r_1 \star r_2^{-1}]^b = [\underbrace{u^a \star (r_1 \star r_2^{-1})^b}_{x'}] \end{aligned}$$

OWGH PoK for Schnorr and Guillou-Quisquater

Schnorr

- $G = \mathbb{Z}_q$, cyclic group $H = \langle h\rangle$, $|H| = q$ prime
- $[\,]: G \to H, \;\; x \mapsto [x] = h^x$.
- Thm 1.5: $\ell = q$, $u = 0$: $z^\ell = 1 = [0]$; q prime $\Rightarrow \gcd(c_1 - c_2, \ell) = 1$.

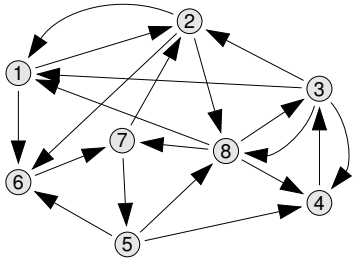
Guillou-Quisquater

- $G = H = \mathbb{Z}_m^*$.
- $[\,]: G \to H, \;\; x \mapsto [x] = x^e$.
- Thm 1.5: $\ell = e$, $u = z$: $z^\ell = z^e = [z]$; e prime $\Rightarrow \gcd(c_1 - c_2, \ell) = 1$.

Further Examples

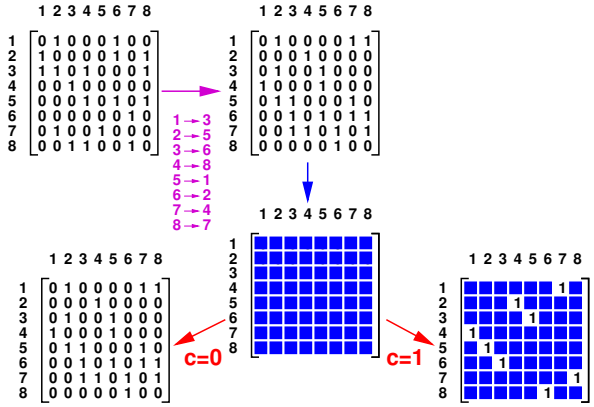
- $\rightarrow$ Script

Hamiltonian Cycles



$$\begin{bmatrix}
0&1&0&0&0&1&0&0\\
1&0&0&0&0&1&0&1\\
1&1&0&1&0&0&0&1\\
0&0&1&0&0&0&0&0\\
0&0&0&1&0&1&0&1\\
0&0&0&0&0&0&1&0\\
0&1&0&0&1&0&0&0\\
0&0&1&1&0&0&1&0
\end{bmatrix}$$

Hamiltonian Cycles — Protocol Idea



Hamiltonian Cycles — One Round of the Protocol

Peggy		Vic
knows HC in $\mathcal{G}$		knows $\mathcal{G}$
π at rand., $\mathcal{H} = \pi\mathcal{G}\pi^{-1}$ Commit $\mathcal{H} \to C_1, .., C_{n^2}$	$\xrightarrow{C_1, .., C_{n^2}}$	
	$\xleftarrow{c}$	$c \in_R \{0, 1\}$
$c = 0$: Decommit $\mathcal{H}$	$\xrightarrow{\pi, d_1, .., d_{n^2}}$	$\mathcal{H} \stackrel{?}{=} \pi\mathcal{G}\pi^{-1}$
$c = 1$: Decommit HC	$\xrightarrow{d_{I_1}, .., d_{I_n}}$	$d_{I_1}, .., d_{I_n} \stackrel{?}{=}$ HC

Commitment Schemes

Name	Setup	Value	Commit	Type	Comments
GI	G_0, G_1 $G_1 = \sigma G_o \sigma^{-1}$	$x \in \{0, 1\}$	$B = \pi G_x \pi^{-1}$	H	Trapdoor: σ
DL	$\|H\| = q$ $H = \langle h \rangle$	$x \in \mathbb{Z}_q$	$b = h^x$	B	OR: LSB(x)
Pedersen	$\|H\| = q$ $H = \langle g \rangle = \langle h \rangle$	$x \in \mathbb{Z}_q$	$b = g^x h^r$	H	Trapdoor DL$_{gh}$
QR B	$m = pq$, $t \in$ QNR, $\left(\frac{t}{m}\right) = 1$	$x \in \{0, 1\}$	$b = r^2 t^x$	B	
QR H	$m = pq$, $t \in$ QR	$x \in \{0, 1\}$	$b = r^2 t^x$	H	Trapdoor $\sqrt{t}$