Cryptographic Protocols

Spring 2018

Part 4

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:

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

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

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

Examples

- $G = \langle \mathbb{Z}_q, + \rangle$, $H = \langle h \rangle$ with $|H| = q$, $[a] = h^a$:

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

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

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

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 a pre-image x of $z \in H$.

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

2-Extractability of OWGH PoK

Theorem 1.5: The 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 ℓ and u as above and triples (t, c_1, r_1) and (t, c_2, r_2) with $c_1 \neq c_2$ satisfying the verification test, extract x' with $[x'] = z$ as follows:

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

OWGH PoK for Schnorr and Guillou-Quisquater

Schnorr

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

Guillou-Quisquater

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

Further Examples

- see paper, lecture, and exercise.