Cryptographic Protocols

Spring 2020

Part 3

2-Extractability

Definition: A three-move protocol (round) with challenge space $C$ is 2-extractable if from any two triples $(t, c, r)$ and $(t', c', r')$ with $c \neq c'$ accepted by $V$ one can efficiently compute $x$ s.t. $Q(z, x) = true$.

Theorem: An interactive protocol consisting of $t$ 2-extractable rounds with uniform challenge from $C$ is a proof of knowledge if $1/|C|^t$ is negligible.

Proof: Knowledge extractor $K$:
1. Choose randomness for $P'$ and execute the protocol between $P'$ and $V$.
2. Execute the protocol again (same randomness for $P'$).
3. Note: $K$ can rewind $P'$ (restart with same randomness).

Proofs of Knowledge

Let $Q(\cdot, \cdot)$ be a binary predicate and let a string $z$ be given. Consider the problem of proving knowledge of a secret $x$ s.t. $Q(z, x) = true$.

Definition: A protocol $(P, V)$ is a proof of knowledge for $Q(\cdot, \cdot)$ if the following holds:
- Completeness: $V$ accepts when $P$ has as input an $x$ with $Q(z, x) = true$.
- Soundness: There exists an efficient program (knowledge extractor) $K$, which can interact with any program $P'$ for which $V$ accepts with noticeable (also called non-negligible) probability, and outputs a valid secret $x$.

Note: $K$ can rewind $P'$ (restart with same randomness).

One-Way Group Homomorphisms (OWGH)

Setting: Groups $(G, \cdot)$ and $(H, \otimes)$

Definition: A group homomorphism is a function $f : (G, \cdot) \rightarrow (H, \otimes)$ with:
- $\forall a, b \in G$ s.t. $[a] = [b]$:
  - $[a \cdot b] = [a] \cdot [b]$;
- $\exists \ell \in \mathbb{Z}, u \in G$ s.t. $(1)$ $\forall c_1, c_2 \in C, c_1 \neq c_2$:
  \[
  [a \cdot b] = [a] \cdot [b] = [u]^{a \cdot b} \cdot [r_2 - r_1]^b
  \]

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

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

Setting: Groups $G$ and $H$, group homomorphism $[] : (G, \cdot) \rightarrow (H, \otimes)$.

Goal: Prove knowledge of a pre-image $x$ of $z \in H$.

Peggy
knows $x \in G$ s.t. $[x] = z$

Vic
knows $z \in H$

$k \in_R G$,
$t = [k]

r = k \cdot x^e

r \rightarrow [r] = t \otimes z^e$

2-Extractability of OWGH PoK

Theorem 3: The protocol round is 2-extractable if
\[
\exists \ell \in \mathbb{Z}, u \in G \text{ s.t. (1) } \forall c_1, c_2 \in C, c_1 \neq c_2 : g\text{cd}(c_1 - c_2, \ell) = 1\]
\[
(2) \ [u] = z^\ell
\]

Proof:
1. $[r_1] = t \otimes z^\ell$
2. $[r_2] = t \otimes z^{\ell^2}$
3. $[r_2^{-1} \cdot r_1] = z^{\ell^2 - c_2}$
4. $\exists : a, b$ with $a \cdot d + b(c_1 - c_2) = 1$
5. $z = z^\ell = z^{ad + b(c_1 - c_2)} = z^{ad} \otimes z^{b(c_1 - c_2)}$

$\therefore (z^a)^b \otimes (z^{c_1-c_2})^b = [u]^b \otimes [r_2^{-1} \cdot r_1]^b = [u^a \cdot (r_2^{-1} \cdot r_1)^b]$
OWGH PoK for Schnorr and Guillou-Quisquater

Schnorr

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

Guillou-Quisquater

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

Further Examples

- see paper, lecture, and exercise.