

Cryptographic Protocols

Spring 2021

Part 4

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 such that $Q(z, x) = \text{true}$.

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 $Q(z, x) = \text{true}$.
- **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).

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 an x with $Q(z, x) = \text{true}$.

Theorem: An interactive protocol consisting of s 2-extractable rounds with uniform challenge from C is a proof of knowledge if $1/|C|^s$ 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').
- 3a. If V accepts in both executions, identify the first round with different challenges c and c' (but same t). Use 2-extractability to compute an x , and output it (and stop).
- 3b. Otherwise, go back to Step 1.

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:

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

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

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

Examples

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

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

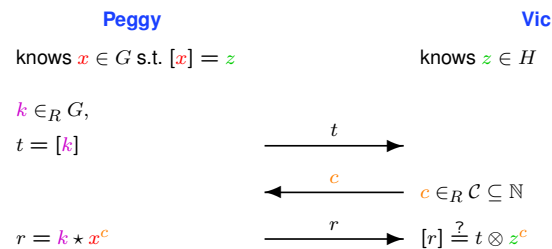
- $G = H = \langle \mathbb{Z}_m^*, \cdot \rangle, [a] = a^e$:

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

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 $z \in H$.



2-Extractability of OWGH PoK

Theorem 3: The protocol round is 2-extractable if

$$\exists \ell \in \mathbb{Z}, u \in G \text{ s.t. } (1) \forall c_1, c_2 \in C, c_1 \neq c_2 : \gcd(c_1 - c_2, \ell) = 1$$

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

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:

$$1. \quad \begin{array}{l} [r_1] = t \otimes z^{c_1} \\ [r_2] = t \otimes z^{c_2} \\ \hline [r_2^{-1} \star r_1] = z^{c_1 - c_2} \end{array}$$

2. Extended Euclidean Algorithm $\Rightarrow a, b$ with $a\ell + b(c_1 - c_2) = 1$

$$3. \quad z = z^1 = z^{a\ell + b(c_1 - c_2)} = z^{a\ell} \otimes z^{b(c_1 - c_2)}$$

$$= (z^\ell)^a \otimes (z^{c_1 - c_2})^b = [u]^a \otimes [r_2^{-1} \star r_1]^b = \underbrace{[u^a \star (r_2^{-1} \star r_1)^b]}_{x'}$$

OWGH PoK for Schnorr and Guillou-Quisquater

Schnorr

- $G = \mathbb{Z}_q$, cyclic group $H = \langle h \rangle$, $|H| = q$ prime
- $[\] : G \rightarrow H$, $x \mapsto [x] = h^x$.
- Thm 3: $\ell = q$, $u = 0$: $z^\ell = 1 = [0]$; q prime $\Rightarrow \gcd(c_1 - c_2, \ell) = 1$.

Guillou-Quisquater

- $G = H = \mathbb{Z}_m^*$.
- $[\] : G \rightarrow H$, $x \mapsto [x] = x^e$.
- Thm 3: $\ell = e$, $u = z$: $z^\ell = z^e = [z]$; e prime $\Rightarrow \gcd(c_1 - c_2, \ell) = 1$.

Further Examples

- see paper, lecture, and exercise.