ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Solution to Exercise 6

6.1 One-Way Homomorphism Zero-Knowledge Proofs of Knowledge

The protocols are instantiations of the proof of knowledge of a pre-image of a one-way group homomorphism. That is, for each scenario, one needs to provide a suitable homomorphism ϕ between two groups, u and ℓ (for each z), as well as a challenge space $\mathcal{C}$ such that the preconditions of the theorem are satisfied.

a) Let $\phi : \mathbb{Z}_m^* \times \mathbb{Z}_m^* \to \mathbb{Z}_m^*, (x, y) \mapsto x^{e_1} y^{e_2}$. Then, ϕ is a homomorphism since

$$\begin{aligned}\phi((x,y)\cdot(x',y')) = \phi((xx',yy')) = (xx')^{e_1}(yy')^{e_2} &= x^{e_1}y^{e_2}x'^{e_1}y'^{e_2}\\ &= \phi(x,y)\cdot\phi(x',y').\end{aligned}$$

Let $\mathcal{C} \subseteq \{0, \ldots, e_1 + e_2 - 1\}$ be polynomially bounded. For $z \in \mathbb{Z}_m^*$, let $u := (z, z)$ and $\ell := e_1 + e_2$. Then,

1. ℓ is prime, and thus $\gcd(c_1 - c_2, \ell) = 1$ for all $c_1, c_2 \in \mathcal{C}$, and
2. $\phi(u) = \phi(z, z) = z^{e_1} z^{e_2} = z^{e_1+e_2} = z^\ell$.

b) Let $\phi : \mathbb{Z}_q^4 \to H^2, (x_1, x_2, x_3, x_4) \mapsto (z_1, z_2) = (h_1^{x_3} h_2^{x_1}, h_1^{x_2} h_2^{x_4} h_3^{x_1})$. Clearly, ϕ is a homomorphism since

$$\begin{aligned}&\phi((x_1,x_2,x_3,x_4)+(x_1',x_2',x_3',x_4'))\\ &= (h_1^{x_3+x_3'}h_2^{x_1+x_1'}, h_1^{x_2+x_2'}h_2^{x_4+x_4'}h_3^{x_1+x_1'})\\ &= (h_1^{x_3}h_2^{x_1}\cdot h_1^{x_3'}h_2^{x_1'}, h_1^{x_2}h_2^{x_4}h_3^{x_1}\cdot h_1^{x_2'}h_2^{x_4'}h_3^{x_1'})\\ &= (h_1^{x_3}h_2^{x_1}, h_1^{x_2}h_2^{x_4}h_3^{x_1})\cdot(h_1^{x_3'}h_2^{x_1'}, h_1^{x_2'}h_2^{x_4'}h_3^{x_1'})\\ &= \phi((x_1,x_2,x_3,x_4))\cdot\phi((x_1',x_2',x_3',x_4')).\end{aligned}$$

Let $\mathcal{C} \subseteq \mathbb{Z}_q$. For $z \in H^2$, let $u := (0, 0, 0, 0)$ and $\ell := q$. Then,

1. ℓ is prime, and thus $\gcd(c_1 - c_2, \ell) = 1$ for all $c_1, c_2 \in \mathcal{C}$, and
2. $\phi(u) = \phi(0, 0, 0, 0) = (1, 1) = z^q = z^\ell$.

6.2 Perfectly Binding/Hiding Commitments

We consider *perfectly correct* commitment schemes with a *non-interactive* Commit *phase*. Such a commitment scheme can be characterized by a function $C : \mathcal{X} \times \mathcal{R} \to \mathcal{B}$ that maps a value $x \in \mathcal{X}$ and a randomness string r from some randomness space $\mathcal{R}$ to a blob $b = C(x, r)$ in some blob space $\mathcal{B}$. The Open phase simply consists of the prover's sending (x, r) to the verifier, who checks that $C(x, r) = b$.

In the following, denote by $\mathcal{B}_x := \operatorname{im} C(x, \cdot)$ for $x \in \mathcal{X}$.

a) Let $x \neq x'$. Perfectly binding means that $\mathcal{B}_x \cap \mathcal{B}_{x'} = \emptyset$, whereas perfectly hiding means that $C(x, R)$ and $C(x', R)$ are identically distributed random variables for $R \in_R \mathcal{R}$. This requires in particular that $\mathcal{B}_x = \mathcal{B}_{x'}$, which contradicts $\mathcal{B}_x \cap \mathcal{B}_{x'} = \emptyset$.

b) Subtasks **b)** and **c)** are discussed simultaneously in **c)**.

c) Note that in all cases, the combined scheme is a string commitment $C(x, (r_1, r_2))$.

1. HIDING: The computational hiding property of C_B cannot be broken by additionally adding the blob of the perfectly hiding scheme C_H.[1]
   BINDING: As C_B is perfectly binding, this is also true for the combined scheme $(C_H(x, r_1), C_B(x, r_2))$, since $C(x, (r_1, r_2) = C(x', (r_1', r_2'))$ implies that $C(x, r_1) = C(x', r_2)$.
2. HIDING: Clearly, the scheme is perfectly hiding as $C_H(C_B(x, r_1), r_2)$ perfectly hides $C_B(x, r_1)$ and thereby x.
   BINDING: Assume for contradiction one could efficiently come up with $x \neq x'$, (r_1, r_2), and (r_1', r_2') such that $C(x, (r_1, r_2)) = C(x', (r_1', r_2'))$. Then, by the fact that C_B is perfectly binding, $y := C_B(x, r_1) \neq C_B(x', r_1') =: y'$, one can efficiently come up with $y \neq y'$, r_2, and r_2' such that $C_H(y, r_2) = C_H(y', r_2')$, which breaks the (computational) binding property of C_H.
3. HIDING: Clearly, the scheme is perfectly hiding as $C_H(x, r_1)$ perfectly hides x.
   BINDING: Assume for contradiction one could efficiently come up with $x \neq x'$, (r_1, r_2), and (r_1', r_2') such that $C(x, (r_1, r_2)) = C(x', (r_1', r_2'))$. Then, by the fact that C_B is perfectly binding, $y := C_H(x, r_1) = C_H(x', r_1') =: y'$, one can efficiently come up with $x \neq x'$, r_1, and r_1' such that $C_H(x, r_1) = y = C_H(x', r_1')$, which breaks the (computational) binding property of C_H.

6.3 Graph Coloring

The protocol is a proof of statement, it shows that $\mathcal{G}$ has a 3-coloring. Let $V = \{1, \ldots, n\}$, and the 3-coloring be defined as a function $f : V \to \{1, 2, 3\}$.

Peggy		**Vic**
knows a 3-coloring f for $\mathcal{G} := (V, E)$		knows $\mathcal{G}$
choose a random permutation of the colors π let $f' = \pi \circ f$ $\forall i \in V$, commit to $f'(i)$ as C_i	$\xrightarrow{C_1, \ldots, C_n}$	
	$\xleftarrow{(i, j)}$	let $(i, j) \in_R E$
open colors of vertices i and j	$\xrightarrow{d_i, d_j}$	check if $f'(i), f'(j) \in \{1, 2, 3\}$ and $f'(i) \neq f'(j)$

COMPLETENESS: It is easily verified that if G has a 3-coloring, then Vic always accepts. Peggy can answer all the Vic's queries correctly such that Vic is convinced as long as the commitment scheme is binding.

SOUNDNESS: The scheme has soundness $\frac{1}{|E|}$: if $\mathcal{G}$ does not have a 3-coloring, a cheating prover must commit to a coloring that has at least one edge whose vertices have the same color, or to colors that are not in $\{1, 2, 3\}$. Hence, with probability $\frac{1}{|E|}$, the verifier catches him, assuming the commitments are perfectly binding. When doing $n|E|$ sequential repetitions of the protocol, the soundness error is down to $(1 - \frac{1}{|E|})^{n|E|} \leq e^{-n}$.

ZERO-KNOWLEDGE: The protocol is c-simulatable: Given (i, j), choose random colors σ_i, σ_j, and compute the commitments C_i, C_j. Since $|E|$ is polynomially large the protocol is zero-knowledge., assuming that the commitments are perfectly hiding.

[1] Formally, this would have to be proved via a reduction.