ETH Zurich, Department of Computer Science — Dr. Jonathan Bootle
HS 2023 — Karen Klein, Varun Maram, Antonio Merino Gallardo

Zero-Knowledge Proofs
Exercise 11

11.1 AFGHO Commitments

Recall the definition of AFGHO commitments [AFG+10] presented in the lectures. Given a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where the groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are of prime order p, we have generators g, h of $\mathbb{G}_2$ to be the commitment keys. Then a commitment to message $m \in \mathbb{G}_1$ using randomness $r \in \mathbb{G}_1$ is computed as $C = e(m, g) + e(r, h) \in \mathbb{G}_T$ (verification recomputes the commitment).

a) Show that the above AFGHO commitment scheme is perfectly hiding and computationally binding under the DPAIR assumption[1].

Consider the following Σ-protocol to prove knowledge of an opening for an AFGHO commitment $C = e(m, g) + e(r, h) \in \mathbb{G}_T$.

$\underline{P}$		$\underline{V}$
$y, s \leftarrow_\$ \mathbb{G}_1$ $D = e(y, g) + e(s, h) \in \mathbb{G}_T$	$\xrightarrow{\quad D \quad}$	
	$\xleftarrow{\quad c \quad}$	$c \leftarrow_\$ \mathbb{Z}_p$
$z = c \cdot m + y$ $t = c \cdot r + s$	$\xrightarrow{\quad z, t \quad}$	Accepts if and only if $e(z, g) + e(t, h) = c \cdot C + D$.

b) Prove that the above protocol is complete, 2-special-sound and special honest-verifier zero-knowledge (SHVZK).

11.2 Sumchecks and Discrete-Logarithm-Based Polynomial Commitments

Let $\mathbb{G}$ be a prime-order group ($p := |G|$) and consider $n = 2^\ell$ group elements $g_0, \ldots, g_{n-1}$. Given a Pedersen commitment $C = \langle \mathbf{a}, \mathbf{g} \rangle = \sum_{i=0}^{n-1} a_i \cdot g_i$, knowledge of an opening can be proved with logarithmic prover communication complexity using split-and-fold techniques as seen in the lectures.

In this exercise, we want to show that similar split-and-fold based proofs of knowledge of Pedersen commitment openings can be abstracted by sumcheck protocols.

a) Given $\mathbf{a} \in \mathbb{Z}_p^n$ and $\mathbf{g} \in \mathbb{G}^n$, define multi-linear extension polynomials $\tilde{\mathbf{a}} : \mathbb{Z}_p^\ell \to \mathbb{Z}_p$ and $\tilde{\mathbf{g}} : \mathbb{Z}_p^\ell \to \mathbb{G}$ corresponding to $\mathbf{a}$ and $\mathbf{g}$ respectively.

---

[1] Roughly speaking, the DPAIR assumption states that given a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ and generators g, h of $\mathbb{G}_2$, it is computationally hard to come up with a non-trivial pair $m, r \in \mathbb{G}_1$ (i.e., $(m, r) \neq (0, 0)$) such that $e(m, g) + e(r, h) = 0 \in \mathbb{G}_T$.

Now consider the polynomial $p : \mathbb{Z}_p^\ell \to \mathbb{G}$ defined as the product of the polynomials $\tilde{\mathbf{a}}$ and $\tilde{\mathbf{g}}$; namely, $p(X_0, \ldots, X_{\ell-1}) = \tilde{\mathbf{a}}(X_0, \ldots, X_{\ell-1}) \cdot \tilde{\mathbf{g}}(X_0, \ldots, X_{\ell-1})$. Note that the statement "$C = \langle \mathbf{a}, \mathbf{g} \rangle = \sum_{i=0}^{n-1} a_i \cdot g_i$" related to the opening of Pedersen commitment C is equivalent to the following instance of the sumcheck protocol with respect to the polynomial p:

$$\sum_{\omega_0, \ldots, \omega_{\ell-1} \in \{0,1\}} p(\omega_0, \ldots, \omega_{\ell-1}) = C$$

b) Consider the following variant of the sumcheck protocol on polynomial p:

$\underline{P}$		$\underline{V}$
	$\xrightarrow{q_0(X_0)}$	
	$\xleftarrow{r_0}$	$r_0 \leftarrow_\$ \mathbb{Z}_p$
	$\xrightarrow{\tilde{\mathbf{a}}(r_0, X_1, \ldots, X_{\ell-1})}$	Accepts if and only if $\sum_{\omega_0 \in \{0,1\}} q_0(\omega_0) = C$, and $\sum_{\omega_1, \ldots, \omega_{\ell-1} \in \{0,1\}} \tilde{\mathbf{a}}(r_0, \omega_1, \ldots, \omega_{\ell-1}) \cdot \tilde{\mathbf{g}}(r_0, \omega_1, \ldots, \omega_{\ell-1}) = q_0(r_0)$.

where the prover computes the polynomial $q_0(X_0) = \sum_{\omega_1, \ldots, \omega_{\ell-1} \in \{0,1\}} p(X_0, \omega_1, \ldots, \omega_{\ell-1})$ in the first round; also note that in the third round, the polynomial $\tilde{\mathbf{g}}$ corresponding to the "key" of Pedersen commitments above is public and known to the verifier beforehand, in contrast to the "opening" polynomial $\tilde{\mathbf{a}}$.

Show that the above protocol satisfies 3-special-soundness.

Hint: You might want to describe the polynomial $q_0(X_0)$ in the $(X_0^2, X_0(1-X_0), (1-X_0)^2)$-basis; i.e., $q_0(X_0) = X_0^2 \cdot C_0 + X_0(1-X_0) \cdot C_1 + (1-X_0)^2 \cdot C_2$ for $C_0, C_1, C_2 \in \mathbb{G}$.

References

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 209–236. Springer, 2010.