Composite ...

No Author Given

No Institute Given

Abstract. abstract

1 Introduction

2 Preliminaries

2.1 Assumptions

The following assumption is the *Bilinear Diffie-Hellman Knowledge Exponent* Assumption presented by Abdomaleki et al. ([1]) adapted to the generated elements belongs to the first source group. We call this assumption *Single Group Bilinear Diffie-Hellman Knowledge Exponent* ($\mathsf{SGBDH\text{-}KE}$).

Assumption 1 (Single Group BDH-KE ($\mathsf{SGBDH\text{-}KE}$) Assumption) *Given $gk = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, $\mathcal{G}_1$, $\mathcal{G}_2$ generators of $\mathbb{G}_1$, $\mathbb{G}_2$, respec., the $\mathsf{SGBDH\text{-}KE}$ Assumption holds if, for all non-uniform polynomial time adversary $\mathcal{A}$ there exists an extractor $\mathcal{X}_{\mathcal{A}}$ such that*

$$Pr\left[\begin{array}{c}([c]_1, [c_0]_1 | x) \leftarrow (\mathcal{A}|\mathcal{X}_{\mathcal{A}})\,(gk, \mathcal{G}_1, \mathcal{G}_2, [\phi]_{1,2}) : \\ e([c]_1, [\phi]_2) = e([c_0]_1, [\mathcal{G}_2]_2), [c]_1 = x\mathcal{G}_1, [c_0]_1 = x[\phi]_1\end{array}\right] \approx 0.$$

3 Succinct proof for knowledge of x s.t. $H(g^x)$

3.1 Intuition

Let C_H be an arithmetic representation of either a hash function H or a combination of several hash functions stitched properly. C_H admits tuples $\{0,1\}^{n_0}$ as input elements. Given $z \in \mathbb{Z}_p$, we present a proof of knowledge of a value $x \in \mathbb{Z}_p$ such that $H(g^x) = z$ in the following.

We want to prove these three statements together in a single and succinct proof:

1. Knowledge of $x \in \mathbb{Z}_p$ such that $y = x\mathcal{G} \in \mathbb{G}$ where $\mathcal{G}$ is the generator of $\mathbb{G}$.
2. Knowledge of $\overline{y} \in \mathbb{G}$ such that $H(\overline{y}) = z$.
3. Finally, that $y = \overline{y}$.

We have to prove all three conditions above by not leaking $[y]$, neither $[\overline{y}]$!! The main ideas to prove them are explained in the following:

1. We can prove knowledge of x by producing a tuple $([y],[\psi],[y_0])$ such that $e([y],[\psi]) = e([y_0],[1])$, i.e. $[y_0] = [y\psi]$, for some given $[\psi] \in \mathbb{G}$ in the CRS. Applying $\mathsf{SGBDH\text{-}KE}$ assumption to this tuple we will have knowledge of x. The verification equation could be proven by a Groth-Sahai proof.
2. SNARK of Groth is composed by these 3 elements [3]:

$$[A]_1 = \left[\alpha + \sum_{i=0}^{m} \overline{a}_i v_i(s) + r_1\delta\right]_1 \qquad [B]_2 = \left[\beta + \sum_{i=0}^{m} \overline{a}_i w_i(s) + r_2\delta\right]_2$$
$$[C]_1 = \left[\frac{\sum_{i=0}^{m} \overline{a}_i \left(\beta v_i(s) + \alpha w_i(s) + y_i(s) + h(s)t(s)\right)}{\delta} + Ar_2 + Br_1 + r_1 r_2 \delta\right]_1$$

where $\{v_i(X), w_i(X), y_i(X)\}$ are the polynomials of the QAP, $s \in \mathbb{Z}_p$ is the secret point used to evaluate the polynomials in the CRS. We will use the same construction for $(\overline{a}_0, \ldots, \overline{a}_{n_0})$, which will correspond with $\overline{y}$, the input on C_H, and the evaluation $(\overline{a}_{n_0+1}, \ldots, \overline{a}_m)$, which includes the result of middle gates and the output of the circuit (if the evaluation is correct then $\overline{a}_m = z$).
3. We can prove that $\overline{y} = y$ by a membership proof that gives us the vector

$$\begin{bmatrix} A - \alpha \\ c_y \end{bmatrix} \in \mathrm{Im} \begin{bmatrix} v_0(s) & \ldots & v_{n_0}(s) & v_{n_0+1}(s) & \ldots & v_m(s) & \delta & 0 & 0 \\ 2^0 \boldsymbol{e}_2 & \ldots & 2^{n_0}\boldsymbol{e}_2 & 0 & \ldots & 0 & 0 & \boldsymbol{u}_1 & \boldsymbol{u}_2 \end{bmatrix},$$

where $[c_y]$ is a Groth-Sahai commitment of the representation of $y \in \mathbb{G}$ in the perfectly binding setting and $[A]$ is the commitment from SNARK with the representation of $\overline{y}$ ($\overline{\boldsymbol{a}} = (\overline{a}_0, \ldots, \overline{a}_{n_0})$) and its evaluation in the circuit $(a_{n_0}, \ldots, a_m)$. This proofs give us both commitments open to same representation because perfectly binding of G-S commitments. Thus, $\boldsymbol{a} = \overline{\boldsymbol{a}}$, which uniquely define respective y and $\overline{y}$, so $y = \overline{y}$.

3.2 Proof

$gk := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathcal{G}_1, \mathcal{G}_2, e)$, where Diffie-Hellman Assumption and $\mathsf{SGBDH\text{-}KE}$ assumption hold.

Setup.

- Algorithm $\mathsf{K}_0(gk)$: Sample $\mathbf{A} \leftarrow \mathcal{D}_1$

- Algorithm $\mathsf{K}_1(gk, \mathbf{A})$: For Groth-Sahai proof sample a vector $\boldsymbol{u}_1 \leftarrow \mathbb{Z}_p^2$, $\phi \leftarrow \mathbb{Z}_p$ uniformly at random and compute a vector $\boldsymbol{u}_2 \in \mathbb{Z}_p^2$ linear independent to $\boldsymbol{u}_1$.
  For SNARK proof compute QAP of the circuit C_H, $\{v_i(X), w_i(X), y_i(X)\}_{i=1}^m$, $t(X)$ of degree n. Sample $s \leftarrow \mathbb{Z}_p$ uniformly at random to compute evaluation of QAP polynomials at point s in $\mathbb{G}_1, \mathbb{G}_2$. Sample also $\alpha, \beta, \delta \in \mathbb{Z}_p$ uniformly at random.

For membership proof sample $\mathbf{\Delta} \leftarrow \mathbb{Z}_p^{2\times 3}$. Compute $[\mathbf{A}_{\mathbf{\Delta}}]_2 = [\mathbf{\Delta}^\top \mathbf{A}]_2 \in \mathbb{G}_2^{3\times 1}$, $[\mathbf{M}_{\mathbf{\Delta}}]_1 = [\mathbf{\Delta}\mathbf{M}]_1 \in \mathbb{G}_1^{3\times(m+3)}$, where

$$\mathbf{M} = \begin{pmatrix} v_0(s) & \dots & v_{n_0}(s) & v_{n_0+1}(s) & \dots & v_m(s) & \delta & 0 & 0 \\ 2^0\boldsymbol{e}_2 & \dots & 2^{n_0}\boldsymbol{e}_2 & 0 & \dots & 0 & 0 & \boldsymbol{u}_1 & \boldsymbol{u}_2 \end{pmatrix} \in \mathbb{Z}_p^{3\times(m+3)}.$$

The CRS includes the elements

$$\left(gk, [\boldsymbol{u}_1]_1, [\boldsymbol{u}_2]_1, [\phi]_{1,2}, [\alpha]_1, [\beta]_{1,2}, [\delta]_{1,2}, [\gamma]_2, [\mathbf{M}_{\mathbf{\Delta}}]_1, [\mathbf{A}]_2, [\mathbf{A}_{\mathbf{\Delta}}]_2, \left\{\left[s^i\right]_{1,2}\right\}_{i\in\{1,\dots,n-1\}}, \right.$$
$$\left. \left\{\left[\frac{s^i t(s)}{\delta}\right]_1\right\}_{i=0}^{n-2}, \left\{\left[\frac{\beta v_i(s) + \alpha w_i(s) + y_i(s)}{\delta}\right]_2\right\}_{i=n_0+1}^{m}\right)$$

The trapdoor: $\tau = (\alpha, \beta, \delta, \mathbf{\Delta})$.

Prover.

– The prover P with input (CRS, x) defines $[y] = x\mathcal{G}_1 \in \mathbb{G}_1$ and computes the following binary representation of $y = (P_x, P_y) \in \mathbb{F}_p$: $(a_0, \dots, a_{n_0}) \in \{0,1\}^{n_0+1}$, where $\sum_{i=0}^{n_0-1} a_i 2^i = P_x \in \mathbb{F}_p$ and $a_{n_0} = sign(P_y)$.
Evaluate $(a_0, \dots, a_{n_0})$ in the circuit $C_H((a_0, \dots, a_{n_0}))$ to obtain the whole assignment $\boldsymbol{a} \in \{0,1\}^m$ (this includes input of the circuit, middle gates and output of the circuit) and compute corresponding SNARK proof $\pi_{\mathsf{SNARK}} := ([A]_1, [B]_2, [C]_1)$ for circuit satisfiability of $C_H((a_0, \dots, a_{n_0})) = z$, where

$$[A]_1 = \left[\alpha + \sum_{i=0}^{m} a_i v_i(s) + r_1\delta\right]_1$$
$$[B]_2 = \left[\beta + \sum_{i=0}^{m} a_i w_i(s) + r_2\delta\right]_2$$
$$[C]_1 = \left[\frac{\sum_{i=0}^{m} a_i\left(\beta v_i(s) + \alpha w_i(s) + y_i(s) + h(s)t(s)\right)}{\delta} + Ar_2 + Br_1 + r_1 r_2\delta\right]_1,$$

for some $r_1, r_2 \leftarrow \mathbb{Z}_p$ chosen uniformly at random.
Compute $[y_0]_1 = x[\phi]_1 \in \mathbb{G}_1$ and a Groth-Sahai proof for the pairing equation

$$e([y]_1, [\phi]_2) = e([y_0]_1, [\mathcal{G}_2]_2), \tag{1}$$

which is transformed to

$$e([\boldsymbol{c}_y]_1, [\phi]_2\boldsymbol{e}_2) = e([\boldsymbol{c}_{y_0}]_1, [\boldsymbol{e}_2]_2) + e([\boldsymbol{u}_1]_1, [\boldsymbol{\pi}_1]_2) + e([\boldsymbol{u}_2]_1, [\boldsymbol{\pi}_2]_2) \tag{2}$$

where

$$[\boldsymbol{c}_y]_1 = \sum a_i 2^i [\boldsymbol{e}_2]_1 + r_3[\boldsymbol{u}_1]_1 + r_4[\boldsymbol{u}_2]_1, \quad [\boldsymbol{c}_{y_0}]_1 = [y_0]_1\boldsymbol{e}_2 + s_1[\boldsymbol{u}_1]_1 + s_2[\boldsymbol{u}_2]_1,$$
$$[\boldsymbol{\pi}_1]_2 = r_3[\phi]_2\boldsymbol{e}_2 - s_1[\boldsymbol{e}_2]_2, \quad [\boldsymbol{\pi}_2]_2 = r_4[\phi]_2\boldsymbol{e}_2 - s_2[\boldsymbol{e}_2]_2$$

for some $r_3, r_4, s_1, s_2 \leftarrow \mathbb{Z}_p$ chosen uniformly at random. Then, $\pi_{\mathsf{G\text{-}S}} := ([\pi_1]_1, [\pi_2]_1)$ where $[\pi_i]_2$ is the second component of $[\boldsymbol{\pi}_i]_2$ respectively.
The prover also computes a membership proof $\pi_\psi := [\mathbf{M}_{\boldsymbol{\Delta}}]_1(\boldsymbol{a}, r_1, r_4, r_5)^\top \in \mathbb{G}_1$ of

$$\begin{bmatrix} A - \alpha \\ \boldsymbol{c}_y \end{bmatrix}_1 \in \operatorname{Im}\left([\mathbf{M}]_1\right).$$

Finally, it sends the proof $\pi := (\pi_{\mathsf{SNARK}}, [\boldsymbol{c}_y]_1, [\boldsymbol{c}_{y_0}]_1, \pi_{\mathsf{G\text{-}S}}, \pi_\psi)$ to the verifier.

Verifier.
The verifier V with input (CRS, π) verify the proofs π_{SNARK}, $\pi_{\mathsf{G\text{-}S}}$, π_ψ, respectively:

$$\begin{aligned}
& e\left([A]_1, [B]_2\right) = ([\alpha]_1, [\beta]_2) + e\left([C]_1, [\delta]_2\right) \\
& e\left(\begin{bmatrix} A \\ \boldsymbol{c}_y \end{bmatrix}_1^\top, [\mathbf{A}_{\boldsymbol{\Delta}}]_2\right) = e\left([\pi_\psi]_1^\top, [\mathbf{A}]_2\right) \\
& e([\boldsymbol{c}_y]_1, [\phi]_2 \boldsymbol{e}_2) = e([\boldsymbol{c}_{y_0}]_1, [\boldsymbol{e}_2]_2) + e([\boldsymbol{u}_1]_1, [\boldsymbol{\pi}_1]_2) + e([\boldsymbol{u}_2]_1, [\boldsymbol{\pi}_2]_2)
\end{aligned}$$

Soundness If the verifier has accepted the membership proof, for soundness of ψ, there exists some $\boldsymbol{w} \in \mathbb{Z}_p^3$ such that

$$\begin{bmatrix} A - \alpha \\ \boldsymbol{c}_y \end{bmatrix}_1 = [\mathbf{M}]_1 \boldsymbol{w}.$$

A is a perfectly hiding commitment, so many $\hat{\boldsymbol{w}}$ may produce same

$$A - \alpha = \overline{[\mathbf{M}]}_1 \hat{\boldsymbol{w}} = \overline{[\mathbf{M}]}_1 \boldsymbol{w},$$

but $\boldsymbol{c}_y$ is a perfectly binding commitment because is a G-S commitment in the soundness setting and moreover $\boldsymbol{c}_y$ is extractable. Thus, $[y]_1 \in \mathbb{G}_1$ is the unique possible opening to $[\boldsymbol{c}_y]_1$, which fixes the first n_0 components of $\boldsymbol{a}$ in A (because y is represented uniquely as $y = \sum_{i=0}^{n_0} a_i 2^i$).

The SNARK proof is a proof of knowledge of some pre-image $\overline{y}$ of H such that $H(\overline{y}) = z$, so for SNARK soundness we have knowledge of this pre-image, which can be represented as $\overline{y} = \sum_{i=0}^{n_0} \overline{a}_i 2^i$.

For extractability of G-S commitments, $[y]_1, [y_0]_1$ can be extracted efficiently and also, for the G-S proof, we have a tuple $([y]_1, [\phi]_{1,2}, [y_0]_1)$ such that $e([y]_1, [\phi]_2) = e([y_0]_1, [\mathcal{G}_2]_2)$. So, for $\mathsf{SGBDH\text{-}KE}$ assumption the prover has knowledge of $x \in \mathbb{Z}_p$ such that $[y]_1 = x\mathcal{G}_1$.

Zero-Knowledge The simulator S with input CRS, $\tau = (\alpha, \beta, \delta, \boldsymbol{\Delta})$, is a compound simulator of the respective proofs:

– SNARK simulator ([3]) sample $A^S, B^S \leftarrow \mathbb{Z}_p$, compute $C^S = \dfrac{A^S B^S - \alpha\beta}{\delta}$ and $[A^S]_1, [B^S]_2, [C^S]_1$ have same distribution as honest SNARK proof.

– Membership proof in linear spaces simulator ([2]) sample $\mathbf{\Delta}\begin{bmatrix} A^S \\ \boldsymbol{c}_y^S \end{bmatrix}_1$, where $[\boldsymbol{c}_y^S]_1 = 0[\boldsymbol{e}_2]_1 + r_3[\boldsymbol{u}_1]_1 + r_4[\boldsymbol{u}_2]_1$ is the commitment to 0, which for perfectly hiding of G-S commitments in zero-knowledge setting has the same distribution of honest $[\boldsymbol{c}_y]_1$, and so π_ψ^S.
– Our simulator computes $[\boldsymbol{c}_{y_0}^S]_1 = 0[\phi]_1\boldsymbol{e}_2 + s_1[\boldsymbol{u}_1]_1 + s_2[\boldsymbol{u}_2]_1$ and above $[\boldsymbol{c}_y^S]_1$, with same distribution as honest ones.
– Groth-Sahai proof simulator [4] computes $[\pi_1^S]_2 = [\phi]_2 r_3 - s_1[\mathcal{G}_2]_2$, $[\pi_2^S]_2 = [\phi]_2 r_4 - s_2[\mathcal{G}_2]_2$.

4 Succinct proof for knowledge of $\boldsymbol{x}, \boldsymbol{y}$ s.t. $\boldsymbol{H}(\boldsymbol{x}||\boldsymbol{H}(\boldsymbol{y})) = \boldsymbol{z}$

4.1 Intuition

4.2 Proof

References

1. B. Abdolmaleki, K. Baghery, H. Lipmaa, and M. Zajac. A subversion-resistant SNARK. In T. Takagi and T. Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017, Part III*, volume 10626 of *Lecture Notes in Computer Science*, pages 3–33, Hong Kong, China, Dec. 3–7, 2017. Springer, Heidelberg, Germany. 1
2. A. González, A. Hevia, and C. Ràfols. QA-NIZK arguments in asymmetric groups: New tools and new constructions. In T. Iwata and J. H. Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 605–629, Auckland, New Zealand, Nov. 30 – Dec. 3, 2015. Springer, Heidelberg, Germany. 5
3. J. Groth. On the size of pairing-based non-interactive arguments. In M. Fischlin and J.-S. Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 305–326, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany. 2, 4
4. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 415–432, Istanbul, Turkey, Apr. 13–17, 2008. Springer, Heidelberg, Germany. 5