Zero Knowledge Succinct Noninteractive ARguments of Knowledge

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

October 15, 2019

zkSNARKs

- Arguments
  - ZK proofs where soundness guarantee is required only against PPT provers
- Noninteractive
  - Proof consists of a single message from prover to verifier
- Succinct
  - Proof size is $\mathcal{O}(1)$
  - Requires a trusted setup to generate a common reference string
  - CRS size is linear in size of assertion being proved

Bilinear Pairings

- Let G and G_T be two cyclic groups of prime order p
- In practice, G is an elliptic curve group and G_T is subgroup of $\mathbb{F}^*_{r^n}$ where r is a prime
- Let $G = \langle g \rangle$, i.e. $G = \{g^\alpha \mid \alpha \in \mathbb{Z}_p\}$
- A symmetric **pairing** is a efficient map $e : G \times G \mapsto G_T$ satisfying
  1. **Bilinearity**: $\forall \alpha, \beta \in \mathbb{Z}_p$, we have $e(g^\alpha, g^\beta) = e(g, g)^{\alpha\beta}$
  2. **Non-degeneracy**: $e(g, g)$ is not the identity in G_T
- Finding discrete logs is assumed to be difficult in both groups
- Pairings enable multiplication of secrets

Computational Diffie-Hellman Problem

- **The CDH experiment $\mathtt{CDH}_{\mathcal{A},\mathcal{G}}(n)$:**
  1. Run $\mathcal{G}(1^n)$ to obtain (G, q, g) where G is a cyclic group of order q (with $\|q\| = n$), and a generator $g \in G$.
  2. Choose a uniform $x_1, x_2 \in \mathbb{Z}_q$ and compute $h_1 = g^{x_1}, h_2 = g^{x_2}$.
  3. $\mathcal{A}$ is given G, q, g, h_1, h_2 and it outputs $h \in \mathbb{Z}_q$.
  4. Experiment output is 1 if $h = g^{x_1 \cdot x_2}$ and 0 otherwise.
- **Definition:** We say that **the CDH problem is hard relative to $\mathcal{G}$** if for every PPT adversary $\mathcal{A}$ there is a negligible function $\mathtt{negl}$ such that

$$\Pr\left[\mathtt{CDH}_{\mathcal{A},\mathcal{G}}(n) = 1\right] \leq \mathtt{negl}(n).$$

Decisional Diffie-Hellman Problem

- **The DDH experiment** $\mathtt{DDH}_{\mathcal{A},\mathcal{G}}(n)$:
  1. Run $\mathcal{G}(1^n)$ to obtain (G, q, g) where G is a cyclic group of order q (with $\|q\| = n$), and a generator $g \in G$.
  2. Choose a uniform $x, y, z \in \mathbb{Z}_q$ and compute $u = g^x, v = g^y$
  3. Choose a bit $b \xleftarrow{\$} \{0, 1\}$ and compute $w = g^{bz+(1-b)xy}$
  4. Give the triple u, v, w to the adversary $\mathcal{A}$
  5. $\mathcal{A}$ outputs a bit $b' = \mathcal{A}(G, q, g, u, v, w)$
- **Definition:** We say that **the DDH problem is hard relative to** $\mathcal{G}$ if for all PPT adversaries $\mathcal{A}$ there is a negligible function $\mathtt{negl}$ such that

$$\left|\Pr\left[\mathcal{A}\left(G, q, g, g^x, g^y, g^z\right) = 1\right] - \Pr\left[\mathcal{A}\left(G, q, g, g^x, g^y, g^{xy}\right) = 1\right]\right| \le \mathtt{negl}(n)$$

- If G has a pairing, then DDH problem is easy in G

Some Exercises on Pairings

- A symmetric **pairing** is a efficient map $e : G \times G \mapsto G_T \subset F^*_{r^n}$ satisfying
  1. **Bilinearity**: $\forall \alpha, \beta \in \mathbb{Z}_p$, we have $e(g^\alpha, g^\beta) = e(g, g)^{\alpha\beta}$
  2. **Non-degeneracy**: $e(g, g)$ is not the identity in G_T
- Reduce the following expressions
  - $e\left(g^a, g\right) e\left(g, g^b\right)$
  - $e\left(g, g^a\right) e\left(g^b, g\right)$
  - $e\left(g^a, g^{-b}\right) e(u, v) e\left(g, g\right)^c$
  - $\prod_{i=1}^m e\left(g, g^{a_i}\right)^{b_i}$
- Show that if $e(u, v) = 1$ then $u = 1$ or $v = 1$

Applications of Pairings

- Three-party Diffie Hellman key agreement
    - Three parties Alice, Bob, Carol have private-public key pairs $(a, g^a), (b, g^b), (c, g^c)$ where $G = \langle g \rangle$
    - Alice sends g^a to the other two
    - Bob sends g^b to the other two
    - Carol sends g^c to the other two
    - Each party can compute common key $K = e(g, g)^{abc} = e(g^b, g^c)^a = e(g^a, g^c)^b = e(g^a, g^b)^c$
- BLS Signature Scheme
    - Suppose $H : \{0,1\}^* \mapsto G$ is a hash function
    - Let (x, g^x) be a private-public key pair
    - BLS signature on message m is $\sigma = (H(m))^x$
    - Verifier checks that $e(g, \sigma) = e(g^x, H(m))$

Knowledge of Exponent Assumptions

- **Knowledge of Exponent Assumption (KEA)**
  - Let G be a cyclic group of prime order p with generator g and let $\alpha \in \mathbb{Z}_p$
  - Given g, g^α, suppose a PPT adversary can output $c, \hat{c}$ such that $\hat{c} = c^\alpha$
  - The only way he can do so is by choosing some $\beta \in \mathbb{Z}_p$ and setting $c = g^\beta$ and $\hat{c} = (g^\alpha)^\beta$
- **q-Power Knowledge of Exponent (q-PKE) Assumption**
  - Let G be a cyclic group of prime order p with a pairing $e : G \times G \mapsto G_T$
  - Let $G = \langle g \rangle$ and α, s be randomly chosen from $\mathbb{Z}_p^*$
  - Given $g, g^s, g^{s^2}, \ldots, g^{s^q}, g^\alpha, g^{\alpha s}, g^{\alpha s^2}, \ldots, g^{\alpha s^q}$, suppose a PPT adversary can output $c, \hat{c}$ such that $\hat{c} = c^\alpha$
  - The only way he can do so is by choosing some $a_0, a_1, \ldots, a_q \in \mathbb{Z}_p$ and setting $c = \Pi_{i=0}^q \left(g^{s^i}\right)^{a_i}$ and $\hat{c} = \Pi_{i=0}^q \left(g^{\alpha s^i}\right)^{a_i}$

Checking Polynomial Evaluation

- Prover knows a polynomial $p(x) \in \mathbb{F}_p[x]$ of degree d
- Verifier wants to check that prover computes $g^{p(s)}$ for some randomly chosen $s \in \mathbb{F}_p$
- Verifier does not care which $p(x)$ is used but cares about the evaluation point s
- Verifier sends $g^{s^i}, i = 0, 1, 2, \ldots, d$ to prover
- If $p(x) = \sum_{i=0}^{d} p_i x^i$, prover can compute $g^{p(s)}$ as

$$g^{p(s)} = \Pi_{i=0}^{d} \left(g^{s^i} \right)^{p_i}$$

- But prover could have computed $g^{p(t)}$ for some $t \neq s$
- Verifier also sends $g^{\alpha s^i}, i = 0, 1, 2, \ldots, d$ for some randomly chosen $\alpha \in \mathbb{F}_p^*$
- Prover can now compute $g^{\alpha p(s)}$
- Anyone can check that $e(g^{\alpha}, g^{p(s)}) = e(g^{\alpha p(s)}, g)$
- But why can't the prover cheat by returning $g^{p(t)}$ and $g^{\alpha p(t)}$?

Schwartz-Zippel Lemma

Lemma

Let $\mathbb{F}$ be any field. For any nonzero polynomial $f \in \mathbb{F}[x]$ of degree d and any finite subset S of $\mathbb{F}$,

$$\Pr[f(s) = 0] \leq \frac{d}{|S|}$$

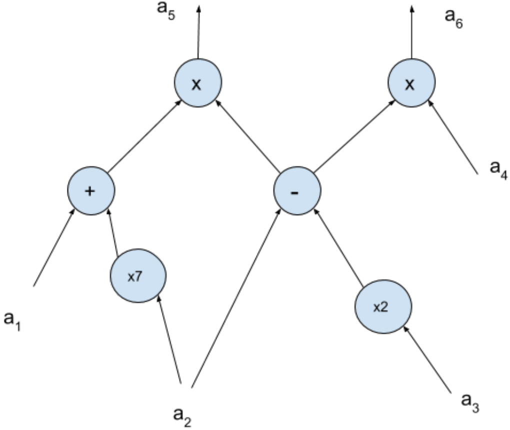
when s is chosen uniformly from S.

- Suppose $\mathbb{F}$ is a finite field of order $\approx 2^{256}$
- If s is chosen uniformly from $\mathbb{F}$, then it is unlikely to be a root of low-degree polynomials
- Equality of polynomials can be checked by evaluating them at the same random point
- **Application:** Suppose prover wants to prover that he knows a secret polynomial $p(x)$ which is divisible by another public polynomial $t(x)$
  - Verifier sends $g^{s^i}, g^{\alpha s^i}, i = 0, 1, 2, \ldots, d$ to prover
  - Prover computes $h(x) = \frac{p(x)}{t(x)} = \sum_{i=0}^{d} h_i x^i$ and calculates $g^{h(s)}$ using the coefficients h_i
  - Verifier gets $g^{p(s)}, g^{h(s)}, g^{\alpha p(s)}, g^{\alpha h(s)}$ and checks

$$e\left(g, g^{p(s)}\right) = e\left(g^{h(s)}, g^{t(s)}\right)$$

$$e\left(g^{\alpha}, g^{p(s)}\right) = e\left(g^{\alpha p(s)}, g\right), \quad e\left(g^{\alpha}, g^{h(s)}\right) = e\left(g^{\alpha h(s)}, g\right)$$

Arithmetic Circuits



Circuits consisting of additions and multiplications modulo *p*

Quadratic Arithmetic Programs

Definition

A QAP Q over a field $\mathbb{F}$ contains three sets of polynomials $\mathcal{V} = \{v_k(x)\}$, $\mathcal{W} = \{w_k(x)\}$, $\mathcal{Y} = \{y_k(x)\}$, for $k \in \{0, 1, \ldots, m\}$, and a target polynomial $t(x)$.

Suppose $f : \mathbb{F}^n \mapsto \mathbb{F}^{n'}$ having input variables with labels $1, 2, \ldots, n$ and output variables with labels $m - n' + 1, \ldots, m$. We say that Q computes f if:

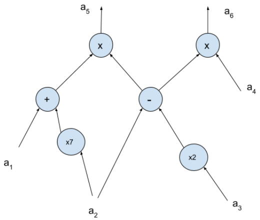
$(a_1, a_2, \ldots, a_n, a_{m=n'+1}, \ldots, a_n) \in \mathbb{F}^{n+n'}$ is a valid assignment of f's inputs and outputs, if and only if there exist $(a_{n+1}, \ldots, a_{m-n'})$ such that $t(x)$ divides $p(x)$ where

$$p(x) = \left(v_0(x) + \sum_{k=1}^{m} a_k v_k(x)\right) \cdot \left(w_0(x) + \sum_{k=1}^{m} a_k w_k(x)\right) - \left(y_0(x) + \sum_{k=1}^{m} a_k y_k(x)\right).$$

So there must exist polynomial $h(x)$ such that $h(x)t(x) = p(x)$.

- Arithmetic circuits can be mapped to QAPs efficiently

QAP for an Arithmetic Circuit



- $a_5 = (a_1 + 7a_2)(a_2 - 2a_3)$ and $a_6 = (a_2 - 2a_3)a_4$
- Choose distinct $r_5, r_6 \in \mathbb{F}$ and $t(x) = (x - r_5)(x - r_6)$
- Choose polynomials $\{v_k(x)\}, \{w_k(x)\}, \{y_k(x)\}, k = 0, 1, \ldots, m$ such that

$$\sum_{k=0}^{6} a_k v_k(r_5) = a_1 + 7a_2, \quad \sum_{k=0}^{6} a_k w_k(r_5) = a_2 - 2a_3, \quad \sum_{k=0}^{6} a_k y_k(r_5) = a_5,$$

$$\sum_{k=0}^{6} a_k v_k(r_6) = a_2 - 2a_3, \quad \sum_{k=0}^{6} a_k w_k(r_6) = a_4, \quad \sum_{k=0}^{6} a_k y_k(r_6) = a_6.$$

SNARK from QAP

- Let $R = \{(u, w)\} \subset \mathbb{F}^{n'} \times F^{n-n'}$ be a relation where $u \in \mathbb{F}^{n'}$ is the statement and $w \in \mathbb{F}^{n-n'}$ is
- Suppose R can verified with an arithmetic circuit, i.e. there is an arithmetic function f such that $f(u, w) = 1$ iff $(u, w) \in R$
- A QAP for f is derived
- Prover has to show he knows $(a_1, \ldots, a_n)$ such that $t(x)$ divides $v(x)w(x) - y(x)$
- **Common Reference String Generation**
  - For $\alpha, s \xleftarrow{\$} \mathbb{F}^*$ and upper bound d, $\{g^{s^i}, g^{\alpha s^i} \mid i = 0, 1, 2, \ldots, d\}$
  - Let $\mathcal{I}_{in}$ be input-related indices and $\mathcal{I}_{mid}$ be the non-input-related indices in $\{1, 2, \ldots, m\}$. Let $[m] = \{0, 1, 2, \ldots, m\}$
  - Generate $\{g^{v_k(s)}\}_{k \in [m]}, \{g^{w_k(s)}\}_{k \in [m]}, \{g^{y_k(s)}\}_{k \in [m]}, g^{t(s)}$
  - Generate $\{g^{\alpha v_k(s)}\}_{k \in [m]}, \{g^{\alpha w_k(s)}\}_{k \in [m]}, \{g^{\alpha y_k(s)}\}_{k \in [m]}$
  - Generate $\{g^{\beta_v v_k(s)}\}_{k \in \mathcal{I}_{mid}}, \{g^{\beta_w w_k(s)}\}_{k \in [m]}, \{g^{\beta_y y_k(s)}\}_{k \in [m]}$ where $\beta_v, \beta_w, \beta_y \xleftarrow{\$} \mathbb{F}^*$
  - Choose $\gamma \xleftarrow{\$} \mathbb{F}^*$ and generate $g^{\gamma}, g^{\beta_v \gamma}, g^{\beta_w \gamma}, g^{\beta_y \gamma}$

SNARK from QAP

- **Proof generation**
  - Prover will prove that $(u, w) \in R$ by showing that $f(u, w) = 1$
  - Prover computes QAP coefficients $(a_1, \ldots, a_m)$ such that

$$h(x)t(x) = \left(v_0(x) + \sum_{k=1}^{m} a_k v_k(x)\right) \cdot \left(w_0(x) + \sum_{k=1}^{m} a_k w_k(x)\right) - \left(y_0(x) + \sum_{k=1}^{m} a_k y_k(x)\right).$$

  - For $v_{mid}(x) = \sum_{k \in \mathcal{I}_{mid}} a_k v_k(x)$, $w(x) = \sum_{k \in [m]} a_k w_k(x)$, and $y(x) = \sum_{k \in [m]} a_k y_k(x)$ the prover outputs the proof π

$$g^{v_{mid}(s)}, g^{w(s)}, g^{y(s)}, g^{h(s)}, g^{\alpha v_{mid}(s)}, g^{\alpha w(s)}, g^{\alpha y(s)}, g^{\alpha h(s)}, g^{\beta_v v_{mid}(s)+\beta_w w(s)+\beta_y y(s)}$$

- **Proof verifier**
  - Let $V_{mid}, W, Y, H, V'_{mid}, W', Y', H', Z$ be the proof
  - Verifier computes $g^{v_{in}(s)}$ for $v_{in}(s) = \sum_{k \in \mathcal{I}_{in}} a_k v_k(s)$
  - Using pairing operations, the verifier confirms that

$$(v_0(s) + v_{in}(s) + V_{mid})(w_0(s) + W) - (y_0(s) + Y) - H \cdot t(s) = 0$$
$$V'_{mid} - \alpha V_{mid} = 0, W' - \alpha W = 0, Y' - \alpha Y = 0, H' - \alpha H = 0,$$
$$\gamma Z - (\beta_v \gamma) V_{mid} - (\beta_w \gamma) W - (\beta_y \gamma) Y = 0$$

References

- Pairing-Based Cryptographic Protocols : A Survey https://eprint.iacr.org/2004/064.pdf
- DDH and CDH Problems https://www.ee.iitb.ac.in/~sarva/courses/EE720/2019/notes/lecture-21.pdf
- Jens Groth's lecture in the 9th BIU Winter School on Cryptography
  - https://cyber.biu.ac.il/event/the-9th-biu-winter-school-on-cryptography/
  - NIZKs from Pairings https://cyber.biu.ac.il/wp-content/uploads/2019/02/BarIlan2019.pdf
  - NIZKs from Pairings https://www.youtube.com/watch?v=_mAKh7LFPOU
- Sections 7, 8 of *Quadratic Span Programs and Succinct NIZKs without PCPs*, GGPR13 https://eprint.iacr.org/2012/215