BP++ Scratch-pad

September 2022

1 Reciprocal Argument

Simple argument

Reciprocal Argument

Prover Input: $V, g, \mathbf{g}, \mathbf{h}, v, \gamma$ such that $V = g^v \mathbf{h}^\gamma$ such that $|\mathbf{g}| = max(n, b)$ where n is the maximum number of bits and b is the base.

Verifier Input: $V, g, \mathbf{g}, \mathbf{h}$

Round 1: Prover computes the digits($\mathbf{d}$) and multiplicities($\mathbf{m}$) of digits as $\forall i$ $0 \leq d_i \leq b$.

$$v = \Sigma_{i=0}^{n} (b^i d_i) \tag{1}$$

$$\forall j \; 0 \leq j \leq b : m_j = \Sigma_{i=0}^{n} (d_i = j) \tag{2}$$

Throughout the protocol, index i is associated with digits of the numbers d_i, index j is associated with multiplicities m_j. And sends commitments to M as

$$b_m \xleftarrow{\$} \mathbb{Z}_p \tag{3}$$

$$\mathbf{l_m} \xleftarrow{\$} \mathbb{Z}_p^6 \tag{4}$$

$$M = g^{b_m} \mathbf{g}^{\mathbf{m}} \mathbf{h}^{\mathbf{l_m}} \tag{5}$$

$$\mathbf{l_d} = (0, 0, -l_m(3), 0, -l_m(5), 0) \tag{6}$$

$$b_d \xleftarrow{\$} \mathbb{Z}_p \tag{7}$$

$$D = g^{b_d} \mathbf{g}^{\mathbf{d}} \mathbf{h}^{\mathbf{l_d}} \tag{8}$$

P sends the commitments D and M. Verifier then sends back challenge e

$$e \xleftarrow{\$} \mathbb{Z}_p \tag{9}$$

Round 2: Prover computes the reciprocal($\mathbf{r}$) sends the reciprocal commitment R where $r_i = \frac{1}{e+d_i}$

$$\forall \mathbf{i}\ \mathbf{l_{r_i}} = 0 \tag{10}$$

$$b_r \xleftarrow{\$} \mathbb{Z}_p \tag{11}$$

$$R = g^{b_r}\mathbf{g^r h^{l_r}} \tag{12}$$

Verifier sends back challenges x, y, q

$$x, q, y \xleftarrow{\$} \mathbb{Z}_p \tag{13}$$

Round 3: Prover samples the blinders($\mathbf{s}$) and sends the commitment S to the verifier as shown below. Let $\alpha_m = (\frac{1}{e+0}, \frac{1}{e+1}, \ldots, \frac{1}{e+b-1}), Q^{-1} = (q^{-1}, \ldots, q^{-n})$

$$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_p^6 \tag{14}$$

$$b_s = |\mathbf{s}|_q^2 \tag{15}$$

$$\delta(T) = Q^{-1} \odot (x\boldsymbol{\alpha_m} T^4 + -\mathbf{1}xT^2 + \mathbf{b}T^3) + e\mathbf{1}T^2 \tag{16}$$

$$\mathbf{c} = y(T, T^2, T^3, T^4, T^6, T^7) \tag{17}$$

$$\text{Compute } \mathbf{l_s} \text{such that} \tag{18}$$

$$\mathbf{w}(T) = \mathbf{s} + \mathbf{mT} + \mathbf{dT^2} + \mathbf{rT^3} + \delta(T) \tag{19}$$

$$\hat{v}(T) = 2vT^5 + b_s + b_m T + b_d T^2 + b_s T^3 \tag{20}$$

$$\langle \mathbf{c}, \mathbf{l_s} \rangle = \hat{v}(T) - |\mathbf{w}(T)|_q^2 - \langle \mathbf{c}, (\mathbf{l_m}T + \mathbf{l_d}T^2 + \mathbf{l_r}T^3 + \gamma T^5) \rangle \tag{21}$$

If the values are set correctly, we can uniquely determine values of l_s by comparing co-efficient of T on both sides. If the prover is honest, all powers but T^5 can be cancelled by attentively computing l_s. T^5 is zero only if prover is honest.

$$\text{Send } S = g^{b_s}\mathbf{g^s h^{l_s}} \tag{22}$$

$$\text{Verifier sends back challenge } t \tag{23}$$

Norm Argument: $|\mathbf{w}|_q^2 + \langle \mathbf{l}, \mathbf{c} \rangle = v$ for a given $C = g^v \mathbf{g^w} h^{\mathbf{l}}$. Run the norm argument with

$$\mathbf{w} = \mathbf{w}(t) \tag{24}$$

$$\mathbf{l} = \mathbf{l_s} + \mathbf{l_m t} + \mathbf{l_d t^2} + \mathbf{l_r t^3} + \gamma \mathbf{t^5} \tag{25}$$

$$v_g = 2t^5(\langle \mathbf{1}, \mathbf{Q} \rangle + e\langle \mathbf{1}, \mathbf{b} \rangle + -x\langle \mathbf{Q^{-1}}, \mathbf{b} \rangle) + x^2t^8\langle \boldsymbol{\alpha_m}, \boldsymbol{\alpha_m} \rangle \tag{26}$$

Verification: Compute C

$$C = SM^tD^{t^2}R^{t^3}V^{2t^5}\mathbf{g}^{\delta(t)}g^{v_g} \tag{27}$$

Run norm argument with C with the above computed q

$$\mathbf{c} = y(t, t^2, t^3, t^4, t^6, t^7) \tag{28}$$

2 Proof Outline:

In order to prove computational witness extended emulation, we construct an extractor χ as follows. The extractor χ runs the prover with $n\dot{m}$ different values of y, $m+2$ different values of z, and 7 different values of the challenge t. Additionally it invokes the extractor norm argument for the transcripts. This results in $7\dot{(}m+2)$ transcripts.

If for any other set of challenges (t, y, q) the extractor can compute a different representation of A or S, then this yields a non-trivial discrete logarithm relation between independent generators h, g, h which contradicts the discrete logarithm assumption.

3 Constraints on variables:

Power of t	co-efficient	constraint
t^{11}	$2R\gamma(4)$	$\gamma(4) = 0$
t^{10}	$2R\mathbf{l_r}(5)$	$\mathbf{l_r}(5) = 0$
t^9	$R(2\gamma(3) + \mathbf{l_d}(5) + \mathbf{l_r}(4))$	$\mathbf{l_r}(4) = -2\gamma(3) - \mathbf{l_d}(5)$
t^8	$R(2\gamma(2) + \mathbf{l_d}(4) + \mathbf{l_m}(5))$	$\mathbf{l_m}(5) = -2\gamma(2) - \mathbf{l_d}(4)$
t^5	$2R(\mathbf{l_r}(1) + \mathbf{l_d}(2) + \mathbf{l_m}(3))$	$\mathbf{l_r}(1) = -\mathbf{l_d}(2) - \mathbf{l_m}(3)$
t^0	$\Sigma_{i=0}^{n}(q^i(\mathbf{s}(i))^2) - b_s$	$b_s = \Sigma_{i=0}^{n}(q^i(\mathbf{s}(i))^2)$
$t^i\ i \geq 1 \wedge i \leq 7 \wedge i \neq 5$	21	21

Variables with constraints: $b_s, \mathsf{l_s}, \gamma(4), \mathbf{l_r}(4), \mathbf{l_m}(5), \mathbf{l_r}(1)$

4 Zero knowledge:

The proof transcript consists of $(M, D, R, S, \mathbf{l}, \mathbf{w})$. If we can show that $\mathbf{w}$ and $\mathbf{l}$ are uniformly distributed, we can use the simulator is rather straightforward. We compute $v = |w|_q^2 + \langle l, c\rangle$. We sample all other proof elements randomly and compute $S = \frac{g^v \mathbf{g}^{\mathbf{w}} \mathbf{h}^{\mathbf{l}}}{M^t D^{t^2} R^{t^3} V^{2t^5} P}$.

4.0.1 Lemma:

For any point $P = g^c \mathbf{g}^{\mathbf{a}} \mathbf{h}^{\mathbf{b}}$, as long as any of c or any of the components of $\mathbf{a}, \mathbf{b}$ are random. Then P is randomly distributed.

- $\mathbf{w}$ is randomly distributed as it contains the $\mathbf{s}$ which is sampled randomly in protocol.
- Informally, the constraint degree is the number of constraints that we have on blinding values. We have overall 10 constraints $|\mathbf{l_s}| = 6 + \mathbf{l_r}(1), \mathbf{l_r}(4), \mathbf{l_m}(5), b_s$ with 28(6 in $\mathbf{l}$ and 1 in b = 7; 4 l equations) free variables.

- we need to show that 4 points are M, D, R, S are uniformly distributed and $\mathbf{l_s}$ is also uniformly distributed.
- By 4.0.1, using values b_m, b_d, b_r we can easily argue that the points M, D, R are uniformly distributed. If $\mathbf{l_d}$ is sampled randomly, then $\mathbf{l}$ would also have a random distribution. Any one of the l_s values, say $l_s(2)$ depends on linear combination on $l_d(0)$(and other values) which is randomly distributed. Atleast one value of $\mathbf{l_s}$, namely, $l_s(2)$ is randomly distributed so according to 4.0.1, S is uniformly distributed.