Improved Bulletproofs

1 Introduction

More to come.

2 Compiler

We build an argument of knowledge for a valid witness to an R1CS program. We do so using the Bulletproofs inner product argument.

Let $\mathbb{G}$ be a group of prime order q. Recall that the core of the Bullerptoofs system is a succinct argument of knowledge for the following n-dimensional inner-product relation:

$$\begin{aligned} \mathcal{R}_{\mathrm{B}P} := \Big\{ (\boldsymbol{P}, \boldsymbol{Q}, R, S) \ ; \ (\boldsymbol{u}, \boldsymbol{v}, w) \Big\} & \text{ where} \\ & (1) \quad \boldsymbol{P}, \boldsymbol{Q} \in \mathbb{G}^n, \quad R, S \in \mathbb{G}, \quad \boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_q^n, \quad w \in \mathbb{Z}_q, \\ & (2) \quad S = \boldsymbol{u} \cdot \boldsymbol{P} + \boldsymbol{v} \cdot \boldsymbol{Q} + w \cdot R, \\ & (3) \quad \langle \boldsymbol{u}, \boldsymbol{v} \rangle = w \qquad /\!\!/ \text{ the inner product of } \boldsymbol{u} \text{ and } \boldsymbol{v} \text{ is } w. \end{aligned} \tag{1}$$

The resulting proof contains only $7 + 2\log_2 n$ group elements. The system ensures that either the prover has a witness for the statement, or one can extract a non-trivial linear relation among the generators $\boldsymbol{P}, \boldsymbol{Q}, R$. Hence, if discrete log holds in $\mathbb{G}$, and the generators $\boldsymbol{P}, \boldsymbol{Q}, R$ are part of a *common random string* (CRS), then the system is an argument of knowledge against a polynomial time prover.

The compiler. We will use the argument of knowledge for $\mathcal{R}_{\mathrm{B}P}$ to build an argument of knowledge for the following R1CS relation:

$$\begin{aligned} \mathcal{R}_{\mathrm{R1}CS} := \Big\{ (A, B, C, \boldsymbol{T}_1, \ldots, \boldsymbol{T}_r, S_1, \ldots, S_r, n, m, m', r) \ ; \ (\boldsymbol{a}, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_r) \Big\} & \text{ where} \\ & (0) \quad n, m, m', r \in \mathbb{N} \\ & (1) \quad A, B, C \in \mathbb{Z}_q^{n \times m}, \quad \boldsymbol{T}_i \in \mathbb{G}^{m'}, \quad S_i \in \mathbb{G}, \quad \boldsymbol{z} := (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_r, \boldsymbol{a}) \in \mathbb{Z}_q^{rm' + (m - rm')}, \\ & (2) \quad (A\boldsymbol{z}) \circ (B\boldsymbol{z}) = (C\boldsymbol{z}), \\ & (3) \quad \forall i \in [r], \ S_i = \boldsymbol{z}_i \cdot \boldsymbol{T}_i \qquad /\!\!/ \ S_i \text{ is a Pedersen hash of a prefix of the witness } \boldsymbol{z}_i. \end{aligned} \tag{2}$$

In other words, the prover needs to prove knowledge of a valid R1CS witness $\boldsymbol{z}$ such that the S_i are Pedersen hashes of a prefix of $\boldsymbol{z}$. The argument of knowledge for $\mathcal{R}_{\mathrm{R1}CS}$ is shown in Figure 1. The protocol description uses the following notation: for $\alpha \in \mathbb{Z}_q$ let

$$\boldsymbol{\alpha}^n := (\alpha, \alpha^2, \ldots, \alpha^n) \in \mathbb{Z}_q^n, \qquad \boldsymbol{\alpha}^{-n} := (\alpha^{-1}, \alpha^{-2}, \ldots, \alpha^{-n}) \in \mathbb{Z}_q^n.$$

Theorem 2.1 (The compiler theorem)**.** *The protocol in Figure 1 is an argument of knowledge for $\mathcal{R}_{R1CS}$, assuming DLOG is hard in $\mathbb{G}$, and $\boldsymbol{P}, \boldsymbol{Q}, R$ are independent generators in $\mathbb{G}$.*

Setup: $\boldsymbol{P}_1 = (\boldsymbol{T}_1, \ldots, \boldsymbol{T}_r) \in \mathbb{G}^{rm'}$, $\boldsymbol{P} = (\boldsymbol{P}_1, \boldsymbol{P}_2, \boldsymbol{P}_3) \in \mathbb{G}^{rm'+(m-rm')+n}$, $\boldsymbol{Q} = (\boldsymbol{Q}_1, \boldsymbol{Q}_2, \boldsymbol{Q}_3) \in \mathbb{G}^{rm'+(m-rm')+n}$, $R \in \mathbb{G}$, all known to both prover and verifier. Both also have an $\mathcal{R}_{\mathrm{R1}CS}$ statement $(A, B, C, \boldsymbol{T}_1, \ldots, \boldsymbol{T}_r, S_1, \ldots, S_r)$. The prover has a witness $\boldsymbol{z} := (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_r, \boldsymbol{a}) \in \mathbb{Z}_q^{rm'+(m-rm')}$. Recall that if the witness is valid then $\forall i \in [r], S_i = \boldsymbol{z}_1 \cdot \boldsymbol{T}_i$ and $(A\boldsymbol{z}) \circ (B\boldsymbol{z}) = C\boldsymbol{z}$.

- *step 1:* The prover sends to the verifier

$$S' \leftarrow \boldsymbol{a} \cdot \boldsymbol{P}_2 + (A\boldsymbol{z}) \cdot \boldsymbol{P}_3 + (B\boldsymbol{z}) \cdot \boldsymbol{Q}_3 \in \mathbb{G}$$

- *step 2:* The verifier samples $\alpha, \beta, \gamma, \epsilon \xleftarrow{\$} \mathbb{Z}_q$ and sends them to the prover.

- *step 3:* Both the prover and verifier locally compute

$$\begin{aligned}
&\mu \leftarrow \alpha\gamma \in \mathbb{Z}_q, \qquad\qquad w \leftarrow \langle \boldsymbol{\alpha}^n, \boldsymbol{\beta}^n \rangle \in \mathbb{Z}_q, \\
&\boldsymbol{c} \leftarrow \boldsymbol{\mu}^n A + \boldsymbol{\beta}^n B + \boldsymbol{\gamma}^n C \in \mathbb{Z}_q^m, \qquad \text{(encodes the R1CS program)} \\
&\boldsymbol{P}' = (\boldsymbol{P}'_1, \boldsymbol{P}'_2, \boldsymbol{P}'_3) \leftarrow \big(\epsilon \boldsymbol{T}_1, \epsilon^2 \boldsymbol{T}_2, \ldots, \epsilon^r \boldsymbol{T}_r,\ \boldsymbol{P}_2,\ (-\boldsymbol{\gamma}^{-n} \circ \boldsymbol{P}_3)\big) \in \mathbb{G}^{m+2n}, \\
&S'' \leftarrow \epsilon S_1 + \cdots + \epsilon^r S_r + S' + \boldsymbol{c} \cdot (\boldsymbol{Q}_1 \parallel \boldsymbol{Q}_2) - \boldsymbol{\alpha}^n \boldsymbol{Q}_3 - \boldsymbol{\beta}^n \boldsymbol{P}'_3 - wR \in \mathbb{G}.
\end{aligned}$$

- *step 4:* The prover computes

$$\begin{aligned}
\boldsymbol{u} &\leftarrow (\ \boldsymbol{z},\quad (-\boldsymbol{\gamma}^n \circ A\boldsymbol{z}) - \boldsymbol{\beta}^n\ ) \in \mathbb{Z}_q^{m+n}, \\
\boldsymbol{v} &\leftarrow (\ \boldsymbol{c},\quad B\boldsymbol{z} - \boldsymbol{\alpha}^n\ ) \in \mathbb{Z}_q^{m+n}.
\end{aligned}$$

  Observe that if $\boldsymbol{z}$ is a valid witness then $\boldsymbol{u}\boldsymbol{P}' + \boldsymbol{v}\boldsymbol{Q} + wR = S''$ and $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = w$.
  That is, $(\boldsymbol{u}, \boldsymbol{v}, w)$ is a valid witness for the $\mathcal{R}_{\mathrm{B}P}$ statement $(\boldsymbol{P}', \boldsymbol{Q}, R, S'')$.

- *step 5:* The prover and verifier use the succinct argument of knowledge for $\mathcal{R}_{\mathrm{B}P}$ to prove that

$$\mathcal{R}_{\mathrm{B}P}\Big((\boldsymbol{P}', \boldsymbol{Q}, R, S'')\ ;\ (\boldsymbol{u}, \boldsymbol{v}, w)\Big) = \textit{true}.$$

Figure 1: An argument of knowledge for $\mathcal{R}_{\mathrm{R1}CS}$

References