# A Security Review of Bulletproofs+ Aggregate Range Proof (Technical Report for Magic Monero Fund)

Nan Wang, Dongxi Liu
CSIRO, Australia

## Contents

# 1 Summary

## 1.1 Scope of the Review

This report presents a security review of the *aggregate range proof* of Bulletproofs+ based specifically on the ePrint version of the paper *Bulletproofs+: Shorter Proofs for Privacy-Enhanced Distributed Ledger*, available as IACR ePrint Report 2020/735 at `https://eprint.iacr.org/2020/735.pdf`. This review focuses exclusively on the aggregate range proof proving the relation

$$\left\{ \begin{array}{l} (\mathbf{g}, \mathbf{h} \in \mathbb{G}^{mn}, g, h \in \mathbb{G}, \mathbf{V} \in \mathbb{G}^m; \mathbf{v}, \boldsymbol{\gamma} \in \mathbb{Z}_p^m) : \\ V_j = g^{v_j} h^{\gamma_j} \wedge v_j \in [0, 2^n - 1], \quad j \in \{1, ..., m\} \end{array} \right\}$$

The reviewed components are:

1. the construction of the weighted inner-product argument in Section 3 and Figure 1.
2. the construction of the linear-sized aggregate range argument in Section 4.2 and Figure 3.
3. the security proof of the weighted inner-product argument, including completeness, witness-extended emulation, and special honest verifier zero-knowledge, in Appendix C.
4. the security proof of the linear-sized aggregate range argument, including completeness, witness-extended emulation, and special honest verifier zero-knowledge, in Appendix D.

Throughout this report, we adopt the same symbols and notation as the Bulletproofs+ paper, to which we refer the reader for their definitions and for the resolution of any ambiguities. Unlike a traditional review, this report provides a comprehensive analysis of the protocol and, where necessary, explicitly presents our corrections, revisions and comments to its specifications and security arguments.

## 1.2 Overall Security Assessment

We begin with our overall security assessment, with further details provided in the subsequent sections. The analyses in Appendices C and D contain the main ingredients for establishing the claimed properties, including perfect completeness, computational witness-extended emulation, and perfect special honest-verifier zero knowledge. However, some significant details are missing from the computational witness-extended emulation analysis and must be completed to establish the claimed soundness property fully. Accordingly, our overall assessment is as follows:

> *To the best of our knowledge, after completing the missing extraction details and addressing the necessary corrections and clarifications documented in this report, we identified no critical soundness or zero-knowledge vulnerability in the Bulletproofs+ aggregate range proof. The construction appears sound under the assumptions stated in the paper.*

## 1.3 Disclaimer

This report presents our best-effort security review of Bulletproofs+ aggregate range proof within the stated scope. To the best of our knowledge, we did not identify any security flaws in the protocol

during this review. However, this report should not be interpreted as a guarantee that the protocol is completely correct, secure, or free of errors, nor as a certification of the security of any particular implementation. Bulletproofs+ has already been deployed in Monero, and this review is intended to provide additional security analysis rather than a deployment endorsement.

### 1.4 Roadmap

This report is organized as follows. We begin with a brief overview of Bulletproofs+ aggregate range protocol in Section 2, followed by specific security analyses of perfect completeness, witness-extended emulation, and special honest-verifier zero knowledge (SHVZK) in Sections 3, 4, and 5, respectively.

## 2 Protocol Overview

At a high level, Bulletproofs+ follows a structure similar to Bulletproofs: it first constructs a linear-sized range protocol $\Pi_{\mathsf{RG}}$ and then recursively applies a sequence of weighted inner-product protocols $\Pi_{\mathsf{WIP}}$ for compression:

$$\Pi_{\mathsf{BP+}} := \Pi_{\mathsf{RG}} \diamond \Pi_{\mathsf{WIP}} \diamond \cdots \diamond \Pi_{\mathsf{WIP}}$$

- $\Pi_{\mathsf{RG}}$: The linear-sized aggregate range protocol reduces the original range relations to a weighted inner-product relation over vectors of dimension $mn$, as captured by Eqn. (34) on page 34 of the Bulletproofs+ paper.

$$\begin{aligned}
&(\mathbf{a}_L - \mathbf{1}^{mn} \cdot z) \odot_y (\mathbf{a}_R + \mathbf{d} \circ \overleftarrow{\mathbf{y}}^{mn} + \mathbf{1}^{mn} \cdot z) \\
&= \mathbf{a}_L \odot_y \mathbf{a}_R + \mathbf{a}_L \odot_y (\mathbf{d} \circ \overleftarrow{\mathbf{y}}^{mn} + \mathbf{1}^{mn} \cdot z) - (\mathbf{1}^{mn} \cdot z) \odot_y \mathbf{a}_R - (\mathbf{1}^{mn} \cdot z) \odot_y (\mathbf{d} \circ \overleftarrow{\mathbf{y}}^{mn} + \mathbf{1}^{mn} \cdot z) \\
&= \underbrace{\mathbf{a}_L \odot_y \mathbf{a}_R}_{=0} + y^{mn+1} \cdot \underbrace{\langle \mathbf{a}_L, \mathbf{d} \rangle}_{=\sum_{j=1}^{m} z^{2j} v_j} + \underbrace{(\mathbf{a}_L - \mathbf{a}_R) \odot_y (\mathbf{1}^{mn} \cdot z)}_{=\langle \mathbf{1}^{mn}, \overrightarrow{\mathbf{y}}^{mn} \rangle \cdot z} - \langle \mathbf{1}^{mn}, \mathbf{d} \rangle \cdot y^{mn+1} z - \langle \mathbf{1}^{mn}, \overrightarrow{\mathbf{y}}^{mn} \rangle \cdot z^2
\end{aligned}$$

  where $\mathbf{d} := \sum_{j=1}^{m} z^{2j} \mathbf{d}_j$, $\overrightarrow{\mathbf{y}}^{mn} = (y, y^2, ..., y^{mn})$ and $\overleftarrow{\mathbf{y}}^{mn} = (y^{mn}, y^{mn-1}, ..., y)$. Unlike Bulletproofs, the linear-sized range protocol does not satisfy zero-knowledge.

- $\Pi_{\mathsf{WIP}}$: The weighted inner-product protocol recursively compresses the above $mn$-dimensional relation until the dimension is reduced to one. The zero-knowledge mechanism is instead incorporated into the weighted inner-product protocol and delayed until the final recursion.

## 3 Review of Perfect Completeness

### 3.1 Assessment

> *To the best of our knowledge, no issue was identified in the perfect-completeness analysis of either the aggregate range protocol or the weighted inner-product protocol.*

### 3.2 Comments

#### 3.2.1 Linear-Sized Range Protocol

The perfect completeness of the linear-sized aggregate range protocol follows by showing that the reduction from the range relations produces a valid instance, as established in Eqn. (34) on page 34. Given the honest forms of $\hat{\mathbf{a}}_L$ and $\hat{\mathbf{a}}_R$, direct substitution shows that Eqn. (34) holds and that its left-hand side always equals the $g$-base exponent of $(\prod_{j=1}^{m} V_j^{z^{2j}})^{y^{mn+1}}$ on its right-hand side.

#### 3.2.2 Weighted Inner Product Protocol

The Bulletproofs+ paper proves perfect completeness of the weighted inner-product protocol by considering the two cases where the dimension $mn = 1$ and $mn > 1$. For the base case $mn = 1$, the proof directly substitutes the honestly generated responses into the verifier's checking equation and shows that the exponents corresponding to each base are equal. For the recursive case $mn > 1$, the proof shows that each compression step transforms a valid weighted inner-product instance into another valid weighted inner-product instance of half the dimension. Repeating this argument eventually reduces the protocol to the base case $mn = 1$, thereby establishing perfect completeness of the full recursive protocol.

## 4 Review of Computational Witness-Extended Emulation

### 4.1 Overview

For witness-extended emulation, a central step in public-coin protocols is to extract the algebraic forms of the prover's responses from the verification equation and then show that the extracted responses satisfy the relations required by the underlying statement. We observe that this step is more subtle in Bulletproofs+ range proof than in the original Bulletproofs construction.

- For the linear-sized range protocol, Bulletproofs distributes the relevant constraints across two separate verification equations, allowing the corresponding witness relations to be derived individually. Bulletproofs+, by contrast, combines these checks into a single group equation. Consequently, the extractor must carefully track the contribution of each commitment to the exponents of the independent generator vectors $\mathbf{g}$ and $\mathbf{h}$.
- For the weighted inner-product protocol, Bulletproofs+ adopts a zero-knowledge-delay mechanism, enforcing zero knowledge only in the final recursion of the compression phase rather than in the preceding range protocol. As a result, the extracted responses in the final recursion contain additional masking components whose algebraic forms must be characterized consistently with the protocol.

Thus, these two modifications require a more careful extraction argument to ensure that the extracted responses are consistent with their protocol-specified forms and that the intended witness relations can be correctly recovered.

### 4.2 Assessment

We identified three issues in the analyses of the linear-sized range protocol (RG) and the weighted inner-product protocol (WIP).

- The first concerns an inconsistency in the forms of the extracted responses in RG. This issue is significant because the extraction must be revised to account for the omitted challenge-dependent terms and complete the soundness argument. Since these terms may affect the extraction of the intended witnesses, additional analysis is required.
- The second concerns an inconsistency in the forms of the extracted responses in WIP. This issue is comparatively minor because the existing extraction remains sufficient to recover the principal witnesses. It can be addressed by clarifying the origin and roles of the additional auxiliary coefficients in the extraction.
- The third concerns the omission of the extraction of the randomness witnesses $\boldsymbol{\gamma}$ in RG. This issue is relatively minor, but the extraction argument should explicitly show how these witnesses are recovered and verify that they correctly open the commitments $V_j$.

*Overall, after completing the missing extraction details for RG and clarifying the roles of the auxiliary terms in WIP, we did not identify any concrete soundness attack that compromises the computational witness-extended emulation.*

### 4.3 Inconsistent Forms of Extracted Responses in RG

The following is the verification equation of the linear-sized aggregate range protocol, as given in Eqn. (35) on page 35 of the Bulletproofs+ paper.

$$\mathbf{g}^{\hat{\mathbf{a}}_L} \cdot \mathbf{h}^{\hat{\mathbf{a}}_R} \cdot g^{\hat{\mathbf{a}}_L \odot_y \hat{\mathbf{a}}_R} \cdot h^{\hat{\alpha}} = A \cdot \mathbf{g}^{-\mathbf{1}^{mn} \cdot z} \cdot \mathbf{h}^{\mathbf{d} \circ \overleftarrow{\mathbf{y}}^{mn} + \mathbf{1}^{mn} \cdot z} \cdot \left( \prod_{j=1}^{m} V_j^{z^{2j}} \right)^{y^{mn+1}} \cdot g^{\delta(y,z)} \tag{1}$$

where $\delta(y,z) \triangleq \langle \mathbf{1}^{mn}, \overrightarrow{\mathbf{y}}^{mn} \rangle z - \langle \mathbf{1}^{mn}, \mathbf{d} \rangle y^{mn+1} z - \langle \mathbf{1}^{mn}, \overrightarrow{\mathbf{y}}^{mn} \rangle z^2$.

#### 4.3.1 Problem

The extraction argument on page 36 of the Bulletproofs+ paper assumes that the extracted vectors $\hat{\mathbf{a}}_L$ and $\hat{\mathbf{a}}_R$ take the forms

$$\hat{\mathbf{a}}_L = \mathbf{a}_L - \mathbf{1}^{mn} \cdot z + \mathbf{v}_L \cdot y^{mn+1},$$
$$\hat{\mathbf{a}}_R = \mathbf{a}_R + \mathbf{d} \circ \overleftarrow{\mathbf{y}}^{mn} + \mathbf{1}^{mn} \cdot z + \mathbf{v}_R \cdot y^{mn+1}.$$

However, these expressions appear to suppress the challenge factors $z^{2j}$ arising from the vector openings of the commitments $V_j$. More precisely, in a witness-extended emulation, each commitment $V_j$ should be allowed to admit a general representation of the form

$$V_j = \mathbf{g}^{\mathbf{v}_{L,j}} \mathbf{h}^{\mathbf{v}_{R,j}} g^{v_j} h^{\gamma_j}, \qquad j \in \{1, ..., m\}.$$

Since the verification equation contains the aggregated term $\left(\prod_{j=1}^{m} V_j^{z^{2j}}\right)^{y^{mn+1}}$, the vector openings of the commitments contribute

$$y^{mn+1} \sum_{j=1}^{m} z^{2j} \mathbf{v}_{L,j}, \quad y^{mn+1} \sum_{j=1}^{m} z^{2j} \mathbf{v}_{R,j}$$

to the exponent of $\mathbf{g}$ and $\mathbf{h}$, respectively. Therefore, matching the corresponding generator exponents yields the more general extracted forms

$$\hat{\mathbf{a}}_L = \mathbf{a}_L - \mathbf{1}^{mn} \cdot z + y^{mn+1} \sum_{j=1}^{m} z^{2j} \mathbf{v}_{L,j} \in \mathbb{Z}_p^{mn},$$

$$\hat{\mathbf{a}}_R = \mathbf{a}_R + \mathbf{d} \circ \overleftarrow{\mathbf{y}}^{mn} + \mathbf{1}^{mn} \cdot z + y^{mn+1} \sum_{j=1}^{m} z^{2j} \mathbf{v}_{R,j} \in \mathbb{Z}_p^{mn}.$$

This distinction is important for witness-extended emulation. The individual openings $\mathbf{v}_{L,j}$ and $\mathbf{v}_{R,j}$ are extracted from the commitments $V_j$ and are therefore fixed independently of the subsequently sampled challenge $z$. In contrast, the weighted combinations

$$\sum_{j=1}^{m} z^{2j} \mathbf{v}_{L,j}, \qquad \sum_{j=1}^{m} z^{2j} \mathbf{v}_{R,j}$$

are explicitly challenge-dependent. Consequently, interpreting $\mathbf{v}_L$ and $\mathbf{v}_R$ in the original extraction as fixed vectors obscures this dependence and does not directly follow from the verification equation. This discrepancy does not by itself imply that the Bulletproofs+ protocol is unsound. Rather, it shows that the extraction argument, as stated, omits part of the algebraic structure induced by the aggregated commitments. A complete witness-extended emulation proof should retain the individual openings $\mathbf{v}_{L,j}$ and $\mathbf{v}_{R,j}$ throughout the extraction and explicitly account for their $z^{2j}$ weights. The resulting challenge-dependent terms must then be analyzed through polynomial interpolation to show that the auxiliary vector openings vanish. Only after establishing this can the simplified forms used in the subsequent range-witness extraction be recovered.

### 4.3.2 Revised Extraction of the Inner-Product Relation

The extraction of the inner-product relation must be re-established using the corrected forms of $\hat{\mathbf{a}}_L$ and $\hat{\mathbf{a}}_R$. We complete the missing part of the Bulletproofs+ analysis in Appendix D by expanding the weighted inner product and determining the constraints imposed on the auxiliary vector openings $\mathbf{v}_{L,j}$ and $\mathbf{v}_{R,j}$. Define

$$\mathbf{d}(z) = \sum_{k=1}^{m} z^{2k} \mathbf{d}_k, \qquad \mathbf{V}_L(z) = \sum_{j=1}^{m} z^{2j} \mathbf{v}_{L,j}, \qquad \mathbf{V}_R(z) = \sum_{j=1}^{m} z^{2j} \mathbf{v}_{R,j}$$

The corrected extracted vectors are

$$\hat{\mathbf{a}}_L = \mathbf{a}_L - \mathbf{1}^{mn} z + y^{mn+1} \mathbf{V}_L(z)$$

$$\hat{\mathbf{a}}_R = \mathbf{a}_R + \mathbf{d}(z) \circ \overleftarrow{\mathbf{y}}^{mn} + \mathbf{1}^{mn} z + y^{mn+1} \mathbf{V}_R(z)$$

Expanding their weighted inner product gives

$$\begin{aligned} \hat{\mathbf{a}}_L \odot_y \hat{\mathbf{a}}_R = {} & \underbrace{\mathbf{a}_L \odot_y \mathbf{a}_R}_{(1)} + \underbrace{y^{mn+1} \langle \mathbf{a}_L, \mathbf{d}(z) \rangle}_{(2)} \\ & + \underbrace{z\mathbf{a}_L \odot_y \mathbf{1}^{mn} - z\mathbf{1}^{mn} \odot_y \mathbf{a}_R}_{(3)} - \underbrace{z y^{mn+1} \langle \mathbf{1}^{mn}, \mathbf{d}(z) \rangle}_{(4)} - \underbrace{z^2 \mathbf{1}^{mn} \odot_y \mathbf{1}^{mn}}_{(5)} \end{aligned}$$

$$+\underbrace{y^{mn+1}\left(\mathbf{a}_L \odot_y \mathbf{V}_R(z) + \mathbf{V}_L(z) \odot_y \mathbf{a}_R\right)}_{(6)}$$
$$+\underbrace{zy^{mn+1}\left(\mathbf{V}_L(z) \odot_y \mathbf{1}^{mn} - \mathbf{1}^{mn} \odot_y \mathbf{V}_R(z)\right)}_{(7)}$$
$$+\underbrace{y^{2mn+2}\langle \mathbf{V}_L(z), \mathbf{d}(z)\rangle}_{(8)} + \underbrace{y^{2mn+2}\mathbf{V}_L(z) \odot_y \mathbf{V}_R(z)}_{(9)}$$

Terms (6)–(9) can then be expanded explicitly as bivariate polynomials in $y$ and $z$:

$$(6) = \sum_{j=1}^{m}\sum_{\ell=1}^{mn} z^{2j} y^{mn+1+\ell}\left(a_{L,\ell} v_{R,j,\ell} + v_{L,j,\ell} a_{R,\ell}\right)$$
$$(7) = \sum_{j=1}^{m}\sum_{\ell=1}^{mn} z^{2j+1} y^{mn+1+\ell}\left(v_{L,j,\ell} - v_{R,j,\ell}\right)$$
$$(8) = \sum_{j=1}^{m}\sum_{k=1}^{m} z^{2j+2k} y^{2mn+2}\left\langle \mathbf{v}_{L,j}, \mathbf{d}_k\right\rangle$$
$$(9) = \sum_{j=1}^{m}\sum_{k=1}^{m}\sum_{\ell=1}^{mn} z^{2j+2k} y^{2mn+2+\ell} v_{L,j,\ell} v_{R,k,\ell}$$

Their respective degree ranges are

| Term | $z$-degrees | $y$-degrees |
|---|---|---|
| (6) | $2, 4, \ldots, 2m$ | $mn+2, \ldots, 2mn+1$ |
| (7) | $3, 5, \ldots, 2m+1$ | $mn+2, \ldots, 2mn+1$ |
| (8) | $4, 6, \ldots, 4m$ | $2mn+2$ |
| (9) | $4, 6, \ldots, 4m$ | $2mn+3, \ldots, 3mn+2$ |

Although Terms (6) and (7) have the same range of $y$-degrees, they are separated by the parity of their $z$-degrees. Similarly, although Terms (8) and (9) have overlapping $z$-degrees, they have disjoint ranges of $y$-degrees. Moreover, the $y$-degrees of Terms (6) and (7) are strictly lower than those of Terms (8) and (9). Therefore, the four terms have disjoint bivariate monomial supports and cannot cancel one another.

The first five terms also occupy monomial positions distinct from those of Terms (6)–(9). In particular, Term (1) occupies $z$-degree zero and $y$-degrees $1, \ldots, mn$, while Term (3) occupies $z$-degree one and the same range of $y$-degrees. Term (2) occupies $y$-degree $mn+1$ and even $z$-degrees, while Term (4) occupies $y$-degree $mn+1$ and odd $z$-degrees. Term (5) occupies $z$-degree two and $y$-degrees $1, \ldots, mn$. Thus, interpolation over sufficiently many distinct values of $y$ and $z$ separates the intended range-proof constraints from the constraints induced by the auxiliary vector openings. The coefficients corresponding to Terms (1)–(5) yield

$$\mathbf{a}_R = \mathbf{a}_L - \mathbf{1}^{mn}, \qquad \mathbf{a}_L \circ \mathbf{a}_R = \mathbf{0}^{mn}, \qquad \langle \mathbf{a}_L, \mathbf{d}(z)\rangle = \sum_{j=1}^{m} z^{2j} v_j$$

Combining the first two relations gives

$$\mathbf{a}_L \circ (\mathbf{a}_L - \mathbf{1}^{mn}) = \mathbf{0}^{mn} \Longrightarrow \mathbf{a}_L \in \{0,1\}^{mn}$$

The binary and value-decomposition constraints can therefore be extracted independently of the auxiliary vector openings.

> *However, even if the intended binary and value-decomposition constraints are satisfied, nonzero auxiliary exponent vectors $\mathbf{v}_{L,j}$ and $\mathbf{v}_{R,j}$ would mean that $V_j$ does not necessarily admit the intended scalar Pedersen opening. It is therefore necessary to show that all such auxiliary vector openings vanish.*

Since Terms (6)–(9) have disjoint bivariate monomial supports, each term must vanish independently. In fact, Terms (7) and (9) suffice to establish

$$\mathbf{v}_{L,j} = \mathbf{v}_{R,j} = \mathbf{0}^{mn}, \qquad \forall j \in \{1, ..., m\}$$

- Term (7) gives

$$\sum_{j=1}^{m} \sum_{\ell=1}^{mn} z^{2j+1} y^{mn+1+\ell} \left(v_{L,j,\ell} - v_{R,j,\ell}\right) = 0$$

  Interpolation in $z$ and $y$ forces every coefficient to vanish:

$$v_{L,j,\ell} - v_{R,j,\ell} = 0, \qquad \forall j \in \{1, ..., m\}, \quad \forall \ell \in \{1, ..., mn\}$$

  Hence,

$$\mathbf{v}_{L,j} = \mathbf{v}_{R,j}, \qquad \forall j \in \{1, ..., m\}$$

- Term (9) gives

$$y^{2mn+2} \mathbf{V}_L(z) \odot_y \mathbf{V}_R(z) = 0$$

  Substituting $\mathbf{V}_R(z) = \mathbf{V}_L(z)$ yields

$$y^{2mn+2} \mathbf{V}_L(z) \odot_y \mathbf{V}_L(z) = 0$$

  Writing

$$\mathbf{V}_L(z) = \left(V_{L,1}(z), \ldots, V_{L,mn}(z)\right),$$

  this identity becomes

$$\sum_{\ell=1}^{mn} y^{2mn+2+\ell} V_{L,\ell}(z)^2 = 0$$

  Interpolation in $y$ therefore gives

$$V_{L,\ell}(z)^2 = 0, \qquad \forall \ell \in \{1, ..., mn\}$$

  Since $\mathbb{Z}_p[z]$ is an integral domain, it follows that

$$V_{L,\ell}(z) = 0, \qquad \forall \ell \in \{1, ..., mn\}.$$

  By the definition

$$V_{L,\ell}(z) = \sum_{j=1}^{m} z^{2j} v_{L,j,\ell},$$

interpolation in $z$ gives

$$v_{L,j,\ell} = 0, \qquad \forall j \in \{1, ..., m\}, \quad \forall \ell \in \{1, ..., mn\}.$$

Consequently,

$$\mathbf{v}_{L,j} = \mathbf{0}^{mn}, \qquad \forall j \in \{1, ..., m\}.$$

Together with the relation extracted from Term (7), this yields

$$\mathbf{v}_{L,j} = \mathbf{v}_{R,j} = \mathbf{0}^{mn}, \qquad \forall j \in \{1, ..., m\}$$

Once these auxiliary vector openings have been eliminated, Terms (6) and (8) vanish automatically. Consequently, each commitment $V_j$ has the intended scalar Pedersen form, with no auxiliary components relative to the generator vectors $\mathbf{g}$ and $\mathbf{h}$. Therefore, the omitted factors $z^{2j}$ do not appear to yield a concrete soundness attack. The intended range relations can still be recovered, provided that the extraction explicitly retains and analyzes the challenge-weighted vector openings. After eliminating these auxiliary openings, the extracted vectors reduce to their expected forms:

$$\hat{\mathbf{a}}_L = \mathbf{a}_L - \mathbf{1}^{mn} z$$

$$\hat{\mathbf{a}}_R = \mathbf{a}_R + \mathbf{d}(z) \circ \overleftarrow{\mathbf{y}}^{mn} + \mathbf{1}^{mn} z$$

The $\mathbf{g}$-component exponent $\mathbf{a}_L \odot_y \mathbf{a}_R$ can then be extracted according to the procedure described in the Bulletproofs+ paper, thereby recovering the intended range constraints.

### 4.3.3 Remarks

We observe that the soundness of Bulletproofs+ critically relies on the random weight vector $\mathbf{y}$ in the weighted inner-product relation associated with the $\mathbf{g}$-component. Since $\mathbf{y}$ is sampled after the relevant prover messages are fixed, its distinct powers assign the algebraic constraints to distinct polynomial coefficients that cannot be tailored by a probabilistic polynomial-time adversary. Polynomial interpolation then recovers the required coordinatewise relations and eliminates the additional algebraic degrees of freedom identified in the extraction, except with negligible probability. This mechanism allows the commitments $(V_j)_{j=1}^m$ to be incorporated into a single verification equation in an apparently sound manner, whereas the original Bulletproofs protocol enforces the corresponding constraints through two separate verification equations. This observation resolves our initial soundness concern, subject to the complete polynomial-extraction argument provided above, and demonstrates the essential role of the weighted inner-product structure in the soundness of Bulletproofs+.

## 4.4 Inconsistent Forms of Extracted Responses in WIP

The second inconsistency arises in the final recursion round of the weighted inner-product protocol, where zero knowledge is enforced through additional masking terms. The verifier checks the following equation:

$$P^{e^2} \cdot A^e \cdot B = \mathbf{g}^{r' \cdot e} \cdot \mathbf{h}^{s' \cdot e} \cdot g^{r' \odot_y s'} \cdot h^{\delta'}$$

where $P$ denotes the commitment to the current weighted inner-product instance, $A$ and $B$ are auxiliary commitments introduced in the final recursion to provide zero knowledge, and $e$ is the verifier's random challenge. The values $r'$, $s'$, and $\delta'$ are the prover's responses corresponding to $e$.

### 4.4.1 Problem

The protocol, however, is not fully consistent with the form assumed in the witness-extended emulation. In Figure 1 on page 13 of the Bulletproofs+ paper, the prover constructs the responses as

$$r' = r + \mathbf{a} \cdot e, \qquad s' = s + \mathbf{b} \cdot e$$

which contain only constant and positive-degree terms in the challenge $e$ and, in particular, do not involve any $e^{-1}$ term. By contrast, the extraction analysis later assumes the more general forms

$$r' = a_P e + a_A + a_B e^{-1}, \qquad s' = b_P e + b_A + b_B e^{-1}$$

The analysis does not appear to explain why the additional inverse-challenge terms $a_B e^{-1}$ and $b_B e^{-1}$ are introduced, or how these terms are consistent with the protocol-specified responses. In particular, the protocol in Figure 1 suggests the more specific forms

$$a_B = 0, \qquad b_B = 0$$

whereas the witness-extended emulation allows these coefficients to be arbitrary subject to the subsequently derived algebraic constraints.
This discrepancy does not necessarily affect the extraction of the principal witnesses $a_P$ and $b_P$. Nevertheless, the proof should explicitly justify why the more general response forms containing $e^{-1}$ are admissible in the simulation, or alternatively specialize the extraction to $a_B = b_B = 0$ so that it is consistent with the responses generated by the protocol.

### 4.4.2 Revised Extraction of the Inner-Product Relation

We now further complete the missing details in the extraction of the inner-product relation. Expanding the weighted inner product yields

$$\begin{aligned} r' \odot_y s' = {} & (a_P \odot_y b_P)e^2 \\ & + (a_P \odot_y b_A + b_P \odot_y a_A)e \\ & + (a_P \odot_y b_B + b_P \odot_y a_B + a_A \odot_y b_A) \\ & + (a_A \odot_y b_B + b_A \odot_y a_B)e^{-1} \\ & + (a_B \odot_y b_B)e^{-2}. \end{aligned} \tag{2}$$

Comparing this expression with

$$r' \odot_y s' = c_P e^2 + c_A e + c_B$$

and matching the coefficients of the corresponding powers of $e$ gives

$$a_P \odot_y b_P = c_P, \tag{3}$$

$$a_P \odot_y b_A + b_P \odot_y a_A = c_A, \tag{4}$$

$$a_P \odot_y b_B + b_P \odot_y a_B + a_A \odot_y b_A = c_B, \tag{5}$$

$$a_A \odot_y b_B + b_A \odot_y a_B = 0, \tag{6}$$

$$a_B \odot_y b_B = 0. \tag{7}$$

The last two equations constrain only the auxiliary coefficients and may admit multiple solutions. In particular, the following three representative cases satisfy these zero constraints.

- *Case 1:* $a_B = b_B = 0$. Both constraints are satisfied trivially, and the extracted responses reduce to

$$r' = a_P e + a_A, \qquad s' = b_P e + b_A$$

This coincides with the algebraic form of the responses specified by the honest protocol. The remaining constraints are

$$a_P \odot_y b_A + b_P \odot_y a_A = c_A, \qquad a_A \odot_y b_A = c_B$$

- *Case 2:* $a_A = a_B = 0$. In this case, the two zero constraints are again satisfied automatically, and

$$r' = a_P e, \qquad s' = b_P e + b_A + b_B e^{-1}.$$

The remaining constraints reduce to

$$a_P \odot_y b_A = c_A, \qquad a_P \odot_y b_B = c_B$$

Thus, the lower-degree coefficients are determined by $b_A$ and $b_B$, while the principal relation

$$a_P \odot_y b_P = c_P$$

remains unchanged.

- *Case 3:* $b_A = b_B = 0$. This case is symmetric to Case 2. The extracted responses become

$$r' = a_P e + a_A + a_B e^{-1}, \qquad s' = b_P e,$$

and the remaining constraints reduce to

$$b_P \odot_y a_A = c_A, \qquad b_P \odot_y a_B = c_B$$

Again, the lower-degree coefficients are determined by the auxiliary terms, whereas

$$a_P \odot_y b_P = c_P$$

is preserved.

These cases show that the auxiliary coefficients are generally not uniquely determined by the interpolation equations. The honest-prover response corresponds to the first case, while the latter two illustrate other admissible solutions of the extracted algebraic system. Crucially, in all three cases, the auxiliary components contribute only to terms of degree $e$ or lower. The principal witnesses $a_P$ and $b_P$ always appear together in the unique coefficient of $e^2$. Therefore, regardless of which admissible case occurs, the required inner-product relation $a_P \odot_y b_P = c_P$ is extracted unchanged.

### 4.5 Comments

The extraction for the other recursion rounds of the weighted inner-product protocol is seemingly well established, and the forms of the extracted vectors $\hat{\mathbf{a}}_i$ and $\hat{\mathbf{b}}_i$ are correctly derived on pages 32–34.

### 4.6 Extraction of the Randomness Witnesses

In this section, we complete the missing extraction of the randomness witnesses $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_m)$ associated with the commitments $V_1, \ldots, V_m$. Comparing the exponents of the blinding generator $h$ on both sides of the verification equation gives

$$\hat{\alpha} = \alpha + y^{mn+1} \sum_{j=1}^{m} \gamma_j z^{2j}$$

where $\alpha$ is the opening of the commitment $A$ with respect to $h$. Fix the preceding transcript, including the challenge $y \in \mathbb{Z}_p^*$, and rewind the prover using $m+1$ challenges

$$z_0, \ldots, z_m \in \mathbb{Z}_p^*$$

such that

$$z_i^2 \neq z_k^2 \qquad \text{for all } i \neq k.$$

Let $\hat{\alpha}_i$ denote the extracted response corresponding to the challenge $z_i$. The resulting equations are

$$\hat{\alpha}_i = \alpha + y^{mn+1} \sum_{j=1}^{m} \gamma_j z_i^{2j}, \qquad i \in \{0, \ldots, m\}.$$

Equivalently,

$$\begin{pmatrix} \hat{\alpha}_0 \\ \hat{\alpha}_1 \\ \vdots \\ \hat{\alpha}_m \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & y^{mn+1} z_0^2 & y^{mn+1} z_0^4 & \cdots & y^{mn+1} z_0^{2m} \\ 1 & y^{mn+1} z_1^2 & y^{mn+1} z_1^4 & \cdots & y^{mn+1} z_1^{2m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & y^{mn+1} z_m^2 & y^{mn+1} z_m^4 & \cdots & y^{mn+1} z_m^{2m} \end{pmatrix}}_{\mathcal{X}} \begin{pmatrix} \alpha \\ \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix}$$

The challenge matrix $\mathcal{X}$ is invertible because $y \neq 0$ and

$$z_i^2 \neq z_k^2 \qquad \text{for all } i \neq k.$$

Indeed, its determinant is

$$\det(\mathcal{X}) = y^{m(mn+1)} \prod_{0 \leq i < k \leq m} \left( z_k^2 - z_i^2 \right) \neq 0$$

Therefore, the extractor uniquely recovers

$$\begin{pmatrix} \alpha \\ \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix} = \mathcal{X}^{-1} \begin{pmatrix} \hat{\alpha}_0 \\ \hat{\alpha}_1 \\ \vdots \\ \hat{\alpha}_m \end{pmatrix}$$

After the auxiliary vector openings have been shown to vanish, the extracted values satisfy

$$V_j = g^{v_j} h^{\gamma_j}, \qquad \forall j \in \{1, ..., m\}.$$

Thus, the extractor recovers both the committed values $v_j$ and their corresponding randomness witnesses $\gamma_j$.

# 5 Review of Special Honest Verifier Zero-Knowledge

## 5.1 Assessment

> *To the best of our knowledge, no vulnerability was identified in the honest-verifier zero-knowledge analysis. All witness-dependent prover messages are appropriately randomized or masked, and the transcript can be perfectly simulated without knowledge of the witnesses.*

## 5.2 Comments

The protocol specified in Figure 1 of the Bulletproofs+ paper corresponds to Case 1, where

$$a_B = b_B = 0.$$

Accordingly, the prover's responses take the form

$$r' = a_P e + a_A, \qquad s' = b_P e + b_A$$

where $a_A$ and $b_A$ are fresh random masking values.
In Case 1, the full SHVZK property is achieved in the final recursion of the weighted inner-product protocol because both field-element responses are masked by fresh randomness. In addition, the group-element messages generated in the linear-sized range protocol and the weighted inner-product protocol have the Pedersen commitment form with fresh random blinding and are therefore perfectly hiding. Consequently, each witness-dependent prover message is either perfectly blinded as a group element or masked by fresh field-element randomness.
For any fixed public input and verifier randomness, the simulator can sample the masked responses according to the honest-prover distribution and construct the corresponding group-element messages without knowing the underlying witnesses. The resulting simulated transcript is therefore identically distributed to a transcript generated by the honest prover. Hence, when the prover follows the protocol-specified response form in Case 1, the protocol achieves perfect special honest-verifier zero knowledge.
The other two algebraic cases identified in the soundness extraction are characterized by

$$a_A = a_B = 0 \qquad \text{or} \qquad b_A = b_B = 0$$

These cases arise only as alternative solutions to the algebraic equations obtained from arbitrary accepting transcripts. They are not generated by the prescribed honest-prover algorithm and need not provide the same perfect zero-knowledge masking. Their existence in the soundness analysis does not contradict the SHVZK property because witness-extended emulation considers arbitrary accepting prover strategies, whereas zero knowledge concerns transcripts generated according to the prescribed honest-prover algorithm.