Veridise

Response to "A Further Review of the DL Gadget Of Interest" by Goodell, Salazar, Slaughter, Szramowski

Alp Bassa, Benjamin Sepanski

Veridise

In [Cyp] the authors provide a review and commentary on work by Eagen [Eag22] and Bassa [Bas24a, Bas24b, Bas24c]. We strongly agree with the authors that all claims have to be put on solid foundations and should be subject to scrutiny. They should be peer reviewed, critically analyzed, and challenged. Without doubt the best way of achieving this is through broad and open communication while demanding highest standards when it comes to details and clarity. This document aims to add to this discussion and address several perceived misunderstandings in [Cyp].

We appreciate the time taken by the authors to review various formalizations, proofs, and arguments and would be happy to engage in any kind of future exchange to ensure the correctness and security of the overall system. Where the claims in [Cyp] were unclear to us, we make our best guess as to their intended meaning. We will be happy to update this response if further updates and clarifications are added to [Cyp].

We keep the same numbering and naming of sections to make clear to which section the response relates to.

1 Introduction

The authors write

> *Even after Bassa's clarifications in [Bas24c], [Bas24a], and [Bas24b], there still seems to be some mistakes related to calculus and the application of the Schwartz-Zippel lemma. Specifically, the verification equations may have terms excluded which have no impact on correctness but do impact soundness. These mistakes seem to be restricted to generalizations over higher multiplicities, and they seem to be correctable. Nevertheless, such mistakes would not be caught by typical correctness tests, and fixing them will require a nontrivial amount of work.*

We are unsure which expressions the authors refer to as mistaken. We are also unsure what is meant by "generalizations over higher multiplicities". If this corresponds to the case where the random challenge line intersects the elliptic curve at points with multiplicities (i.e. is tangent to the curve), this case is explicitly excluded from the protocol by the abort conditions in protocol Π in Figure 1 in [Bas24b]. The effects on completeness (point (i) in Section 3.3 of [Bas24b]) are shown to be negligible in Section 3.3 in [Bas24b].

Even after corrections are made, the resulting scheme is (or rather, the schemes described in [Bas24c], [Eag24], and [Par24a] are) highly malleable and with a non-zero soundness error, introducing unnecessary attack surfaces and calling soundness results into question.

The claim about the schemes being highly malleable is unfounded. For the soundness error the explicit bound $13k/q$ (with q the cardinality of the finite field and k coming from to the degree of the divisor) is obtained (see [Bas24b, Corollary 6]). This bound has explicit constants, so is not an asymptotic result. The error may be bounded exactly by choosing k and q based on the desired security parameters. It is unclear what aspect of soundness is questionable from these explicit bounds.

For the proof to be malleable, a hash collision must be found. This lies outside the security model of all known constructions using hash functions. This is detailed later in the text at the corresponding point (Section 4.3 and 4.4).

2 High Level Description

2.0.1 Trivial Solution

2.0.2 Function Field $K(E)$ and div

2.0.3 Weil's Reciprocity

Theorem 2. *There exists a polynomial extension of $K[X, Y]$, say $K[\mathcal{X}]$, over which the points in* $\operatorname{div} g$ *are rational functions of the coefficients of g.]*

As a corollary, if $f(\operatorname{div} g) - g(\operatorname{div} f)$ can be handled as a rational function [VERIDISE: as a function of the coefficients of g], then logarithmic derivatives apply; otherwise, logarithmic derivatives must be extended to whatever set of functions contains $f(\operatorname{div} g) - g(\operatorname{div} f)$.

We first address the applicability of Schwartz-Zippel following the narrative in [Cyp]. Then, we explain why Theorem 2 is unnecessary for applying logarithmic derivatives.

Applicability of Schwartz-Zippel. If desired, the scheme can be interpreted as projecting (push-forward) onto a rational subfield (line) of the function field of the elliptic curve and applying univariate Schwarz–Zippel on the line. λ, μ, and hence the coefficients of g can be expressed in terms of the coordinates of the challenge points and hence there is no obstruction to using (a generalized) Schwartz-Zippel Lemma. As $f(\operatorname{div} g) - g(\operatorname{div} f)$ for any f and g with disjoint support, a corrected version of the narrative taken in [Cyp] would be to check $f(\operatorname{div} g) - g(\sum m_i(P_i) + (-Q) - m^*(O))$. However, this interpretation, and the reliance on Weil reciprocity, is not relied upon in any of [Eag22, Bas24a, Bas24b, Bas24c].

Applicability of logarithmic derivatives. Although the Schwartz–Zippel Lemma has been stated for univariate polynomials, it is customary for it to refer to a more general setup, e.g. multivariate polynomials or certain spaces of functions on algebraic curves. Used in this way, it refers to an argument based on randomly sampling from a large structured space for probabilistically testing identities in the corresponding ring of functions. This is also the approach taken in [Bas24b, Bas24c]. Rather than using the interpretation using Weil reciprocity, one can rewrite expressions involving the norm (which is what the proof of Weil reciprocity is based on). The norm is defined in terms of rational functions, making the applicability of logarithmic derivatives apparent.

2.0.4 Logarithmic Derivatives

This sections seems to contains some confusion regarding the definition of derivations. For a polynomial ring, the partial derivatives form a basis for the derivations as a module over the polynomial ring. However, rational functions defined over an elliptic curve do *not* form a polynomial ring, as there is a non-trivial relation (the curve equation) between the variables x, y. Hence partial derivatives are not derivations. For a curve E, a derivation $D : K(E) \to K(E)$ must satisfy $D(f) = 0$ for all $f \in K[X, Y]$ with $f|_E \equiv 0$ so that it is well-defined. For example, over a curve $y^2 = x^3 + Ax + B$, taking the partial derivative $\partial/\partial x$ on the left hand side produces 0, whereas the right hand side becomes $3x^2 + A$. As such, the partial derivatives do not form a basis for the space of derivations. One example $K(E)$-basis of derivations of the function field of the elliptic curve E would be $\{2y\frac{\partial}{\partial x} + (3x^2 + A)\frac{\partial}{\partial y}\}$.

The subsequent discussion regarding homogeneous polynomials also pertains to a different setup. After elaborating on derivations in a different context, the authors claim that it is not clear that the corresponding details were handled appropriately. Given the discrepancy between the setup this remark does not apply. While reasoning with the expressions for the logarithmic derivative, everything is put on formal foundations using the theory of derivations in function fields. For a self-contained reference for derivations of algebraic function fields, we refer to [Sti].

> *While justifying the use of logarithmic derivatives over rational functions in a finite field is a nontrivial but simple exercise, it is the method upon which all of Eagen's approach rests. A proof is not just customary, but necessary*

The use of logarithmic derivatives can require care, especially as they interact with the norm map, which is composed of evaluations at conjugate points. The derivation is defined on the space of functions but conjugation is defined more naturally at the level of points. Hence care needs to be taken to formalize this by passing to the Galois closure. This is done in detail in [Bas24a]. There it is also shown that for degrees smaller than the characteristic equality of the logarithmic derivative of functions implies equality of the functions themselves.

3 Rust Implementation

4 Elaborations

4.1 Slow is fast

There is certainly nothing to object about the authors description of the way research results should (and currently are) disseminated in an academic context: in a formal and rigorous way, with precise definition and background provided. While principal divisors, class groups of elliptic curves, their relation with the group law, and derivations of the function field of a curve are classical notions with standardized presentations in many textbooks, these are complicated theoretical notions requiring deep background knowledge.

The reviews provided by Veridise were prepared as part of time-boxed engagements, where the principal aim was to provide the necessary framework and proofs for the informally sketched arguments in [Eag22] for an audience that has been already working on this subject matter. The time allocated to each of the engagements included time for understanding the informal arguments, putting them into a working framework, producing proofs and the writing them up. Hence, the exposition only included references to literature with the precise definitions and

restricted background material. This is expected to provide sufficient references for the target audience.

Should an academic publication have been envisioned, the nature of the write-up and the accordingly the required allocated time would clearly have been very different. Additional work to create a unified document with enough background information for practitioners newer to these concepts would be a benefit for the understandability and long-term security of the scheme.

4.2 Disagreement in Sources

The "disconnect between Eagen's narrative and the subsequent papers" is self-explanatory and constitutes the raison d'être of the engagement. Eagen's exposition provides insight and motivation for new ideas and sketches proofs at a high level. The requirement to put them onto solid foundations and obtain rigorous proofs resulted in the subsequent papers. Hence the divergence in length of exposition and nature of the expositions. The first report [Bas24c] provides the framework for Eagen's arguments and provides the corresponding soundness proof. In the proof logarithmic derivatives have been used, which is formalized in terms of derivations of function fields in [Bas24a]. The expression for the logarithmic norm is derived as well. Finally in [Bas24b] a formalization of the of the protocol for the discrete logarithm relation and a soundness proof is provided.

4.3 Malleability

> *In this sense, Eagen's approach is an implication problem, not a malleability problem. Indeed, a proof π which convinces a reader that some tuple $(Q, \vec{P}, \vec{m}) \in \mathbb{G}^{N+1} \times \mathbb{Z}^m$ satisfies the relation $Q = \sum_i m_i P_i$, in truth, convinces a reader that a set of tuples $\left\{(Q_\ell, \vec{P}_\ell, \vec{m}_\ell)\right\}$ all satisfy $Q_\ell = \sum_i m_{\ell,i} P_{\ell,i}$ for every ℓ. This means that proving Eagen's approach to be sound under relation $Q = \sum_i m_i P_i$ is not the correct tactic. At best, such a proof demonstrates soundness only on a subset of proof implications!*

> *So, if f is a function field element attesting to the principality of a divisor corresponding to $D = \sum_i m_i P_i - m^* O$, and this principal divisor has a principal sub-divisor, say $\sum_i m'_i P_i - m'' O$, then the sub-divisor has some g attesting to this fact, and $\frac{f}{g}$ is an element of the function field. This implies that $\sum_i (m_i - m'_i) P_i - (m^* - m'') O$ is also a principal divisor. That is to say, principal divisors factor cleanly out of principal divisors. In this way, it seems that malleability for a proof π attesting to a principal divisor $D = \sum_i m_i P_i - m^* O$ is about all principal divisors containing D or contained within D as well as additional points which happen to vanish on the random challenge line L.*

We are unsure what the discussion on sub-divisors is intended to demonstrate. The discussion above derives a witness $\frac{f}{g}$ for principal divisor $D' \leq D$ given a witness f for principal divisor D. This seems intended to indicate that an adaptive attack may be possible, in which a proof π for divisor D is somehow reused for divisor D'.

As indicated in the text of [Cyp], this concern is prevented by the choice of a random line:

> *Unfortunately, each attempt comes with a new L, so this approach will require a collision in L... Either way, the verifier will compute the random challenge L using the new modified data, and so such a trick could only work if the resulting L collides.*

The challenge line L is provided once the points P_i and the function f have been fixed. These values are committed to the verifier in the interactive setup or provided as input to the hash function for the scheme rendered non-interactive using Fiat-Shamir. Hence changing the points without having to change the challenge is not possible in the protocol and is one of the security assumptions of the scheme. This boils down to being able to find hash collisions in the non-interactive setup.

All interactive proofs in the literature depend on the assumption that challenges are only available after the message of the prover has been sent and would be malleable in precisely the same way in case the prover is able to modify prior messages without changing the challenge.

4.3.1 Developer watermarking

> *Therefore, a principal divisor corresponding to a proof is not unique. A given function field element can work to prove the principality of related divisors obtained with subset-sums to O in the divisor, or which decompose 1 nontrivially through the line ℓ.*

The remarks from the previous section apply. f and the points P_i are committed to before the challenge line ℓ is drawn. Its use in another interactive proof with a different set of points would result in a different challenge line ℓ', and thus require a different proof π'. An adaptive attack as described above would once again require breaking the Fiat-Shamir scheme.

Moreover, in the framing of NP languages, the divisor constitutes the instance (the relation to be proven), whereas the function provides the witness. A verifier not checking the instance for coherence is in any case destined to erroneously accept proofs for wrong statements, regardless of the protocol used.

4.3.2 A practical attack for the cost of a hash collision

> *This specific attack does require the random challenge L to collide, which occurs with negligible probability, so the attacker will be looking for a long time.*

The cost of a hash collision is clearly a price too high to ask for a practical attack. The authors would probably agree that any cryptographer would be happy to break many schemes in their leisure time once granted any practical ability to produce hash collisions.

4.4 Soundness and Proof Implications

The authors write “soundness error is asymptotically negligible, it may still be the case that the practical soundness error in a given implementation may be unacceptably high. Indeed, all assessments of soundness error put forth so far have been only asymptotic assessments.”. This claim is not accurate. The soundness errors provided are given explicitly in terms of the degree of the divisor and the cardinality of the finite field, see [Bas24b, Corollary 6]. According to the desired security level, the cardinality of the finite field can be chosen large enough to ensure the required soundness error. This would rule out the possibility of a “bad proof”. Hence the subsequent argumentation regarding “malleating bad proofs” also is not well founded, as the argument about asymptotic soundness does not apply. Malleating proofs (in the way described in the preceding sections) can be ruled out.

Subsequently the authors reach the following conclusion:

> *If*
>
> *(i) bad proofs are practically likely even though they are asymptotically negligible, and*
>
> *(ii) any given bad proof can be malleated into a proof for an arbitrary, adversarially selected statement,*
>
> *then this scheme is not suitable for deployment. The former can be protected against with additional challenges, but the latter cannot. Bad proofs are inevitable, so the latter would be catastrophic. A spectrum is suggested by the latter point above by restricting which statements admit malleation. It is a hopeful sign that the hash collision attack described above seems to admit little malleation at all.*
> *Unfortunately, no firm understanding of these bad proofs or their implications is immediately forthcoming. Despite the work in all the references herein, we are not much closer to understanding these problems.*

As discussed above, the explicit error bounds rule out "bad proofs" except with a protocol-specified probability. As mentioned in Section 4.3.1, an adaptive attack taken by selecting an adversarial statement requires breaking a collision-resistant hash function. This conclusion, given the above responses, seem to stand without any foundation.

5 Some final words

As history has shown, with any proof there is always the possibility that there is a flaw in the argumentation, some edge cases were overlooked or some assumptions forgotten. The same clearly applies to work in [Bas24a, Bas24b, Bas24c]. Hence extensive critical analysis and review by peers and battle testing is a crucial component in the acceptance and subsequent utilization of these results. In that respect we highly value the time taken by the authors in reviewing and commenting on these results. We reiterate our commitment to be actively involved in any constructive endeavour to ensure the correctness of the proofs, the clarity and precision of its exposition and the security of the scheme based on it.

References

[Bas24a] Bassa, Alp; *On the Use of Logarithmic Derivatives in Eagen's Proof of Sums of Points*, Veridise Report, 2024.

[Bas24b] Bassa, Alp; *Soundness Proof for an Interactive Protocol for the Discrete Logarithm Relation*, Veridise Report, 2024.

[Bas24c] Bassa, Alp; *Soundness Proof for Eagen's Proof of Sums of Points*, Veridise Report, 2024.

[Eag22] Eagen, Liam; *Zero Knowledge Proofs of Elliptic Curve Inner Products from Principal Divisors and Weil Reciprocity*, Cryptology ePrint Archive, Paper 2022/596, 2022.

[Eag24] Sage implementation, https://gist.github.com/Liam-Eagen/666d0771f4968adccd6087465b8c5bd4.

[Cyp] Goodell, Brandon; Salazar, Rigo; Slaughter, Freeman; Szramowski, Luke; *A Further Review of the DL Gadget Of Interest*, Cypher Stack, May 24, 2025.

[Par24a] Parker, Luke; *Fcmp++* https://github.com/kayabaNerve/ fcmp-plus-plus-paper/blob/develop/fcmp%2B%2B.pdf.

[Sti] Stichtenoth, Henning; *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics 254, Springer Verlag, 2009.