Cryptanalysis of Pairing-Based Additive Masking with Prime-Field Secrets

Harliv Singh
Birla Institute of Technology and Science, Pilani, K. K. Birla Goa Campus,
Zuarinagar, Sancoale, Goa 403726, India
Email: sh.harliv@gmail.com
Repository: https://github.com/h-livv/pairing-mask-cryptanalysis

AI-use designation: Substantial AI contribution.

ChatGPT (OpenAI) was used to assist in scrutinizing the mathematical derivations and arguments for possible algebraic errors, logical gaps, and unsupported implications. It was also used to support the literature review by identifying and synthesizing potentially relevant prior work, as well as for manuscript organization, editing, and LaTeX troubleshooting. The author reviewed the AI-assisted material and takes full responsibility for the mathematical arguments, computational results, references, and conclusions presented in this work.

Abstract

We analyze the public values generated by a pairing-based multi-secret sharing construction in which each secret is added to a power of a common pairing value. The secrets lie in the prime subfield of the extension field containing the public values. We show that the first two public values determine the common mask whenever an explicit nonzero condition holds. We also show that the exceptional case is resolved for the parameter set considered in the numerical example. Consequently, the complete public transcript determines every secret, without requiring a participant share or an initially compromised secret. We further describe two related forms of leakage: recovery of all secrets after disclosure of one suitable secret, and a reduction in the possible values of a secret from a single public value. Our conclusions concern the field-valued, common-base masking construction analyzed here; they do not imply that pairing-based secret sharing in general is insecure.

Keywords: secret sharing; bilinear pairings; elliptic curves; finite fields; cryptanalysis.

1 Introduction

Pairing-based constructions have been used in threshold and multi-secret sharing schemes. This paper studies the field-valued masking step in the conjunctive hierarchical multi-secret sharing scheme of Chintamani, Paul, and Sa [3]. In that construction, the dealer publishes values obtained by adding each secret to a pairing output. By bilinearity, the pairing terms form consecutive powers of a common field element. Since the secrets lie in the prime subfield of the ambient extension field, this structure allows an adversary to recover the common mask from the first two public values.

1.1 Related work

Binu and Sreekumar [1] proposed a threshold multi-secret sharing scheme based on elliptic-curve self-pairings. Their public recovery codes contain indexed pairing terms involving a common point, which threshold participants reconstruct before recovering the secrets. Bahramian and Eslami [2] developed a verifiable threshold scheme in which both the pairing outputs and the secrets are elliptic-curve points. These constructions therefore use point-valued arithmetic. In contrast, Chintamani et al. [3] add prime-subfield secrets to pairing outputs in an extension field. Bilinearity gives their public values the form studied here, with masks that are consecutive powers of a common element. Our recovery result concerns this field-valued construction; it is not a claim about the earlier point-valued schemes or about pairing-based secret sharing in general.

1.2 Contributions and scope

The main result shows that the first two public values determine the common mask, subject to an explicit condition. When the subgroup order is relatively prime to $p-1$, the exceptional case is resolved as well. The remaining public values can then be used to recover every secret. The main attack uses only the public transcript and field arithmetic; it requires no participant share, dealer state, pairing evaluation, or prior secret compromise.

We also establish two supporting results. First, disclosure of one secret at an index relatively prime to the subgroup order reveals the common mask and hence all secrets. Second, a single public value can restrict the possible value of its corresponding secret. The latter result is illustrated for the numerical example considered below; uniqueness is not asserted in general.

2 Construction and notation

Let p be an odd prime and let F be a finite extension field of characteristic p. Its prime subfield is identified with $\mathbb{F}_p$. Thus, for every $K \in \mathbb{F}_p$,

$$K^p = K. \tag{1}$$

Also, since F has characteristic p, the binomial theorem gives

$$(x+y)^p = x^p + y^p, \qquad x, y \in F. \tag{2}$$

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be additive cyclic groups of prime order ℓ, and let

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mu_\ell \subseteq F^*$$

be a bilinear pairing, where μ_ℓ is the subgroup of F^* of order ℓ. For fixed $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, put

$$z = e(P, Q) \in \mu_\ell. \tag{3}$$

Bilinearity gives

$$e(P, iQ) = e(P, Q)^i = z^i. \tag{4}$$

We study public transcripts of the form

$$v_i = K_i + z^i, \qquad K_i \in \mathbb{F}_p, \quad z \in \mu_\ell, \qquad 1 \le i \le s, \tag{5}$$

where $s \ge 2$ and addition is in F. The construction in [3] has this form. The adversary is assumed to know the public transcript, the field representation, the characteristic p, and the subgroup order ℓ. No participant share, the point Q, or a secret is provided unless stated otherwise.

3 Recovery from two public values

The first two public values determine the common mask z. The full public transcript then determines every secret.

Write

$$v_1 = z + K_1, \qquad v_2 = z^2 + K_2. \tag{6}$$

First, raise both public values to the power p. Since $K_1, K_2 \in \mathbb{F}_p$, equation (1) gives $K_1^p = K_1$ and $K_2^p = K_2$. Using equation (2), we obtain

$$v_1^p = (z + K_1)^p = z^p + K_1, \; v_2^p = (z^2 + K_2)^p = z^{2p} + K_2. \tag{7}$$

Next, subtract the original public values. The secret terms cancel:

$$A := v_1^p - v_1 = z^p - z, \; B := v_2^p - v_2 = z^{2p} - z^2. \tag{8}$$

The first identity in equation (8) gives $z^p = A + z$. Substituting this into the expression for B yields

$$B = (z^p)^2 - z^2 \tag{9}$$
$$= (A + z)^2 - z^2 \tag{10}$$
$$= A^2 + 2Az. \tag{11}$$

Therefore, if $A \neq 0$,

$$\boxed{z = \frac{B - A^2}{2A}.} \tag{12}$$

Since p is odd, division by 2 is valid in F. Once z is known, each secret follows from its public value:

$$\boxed{K_i = v_i - z^i, \qquad 1 \leq i \leq s.} \tag{13}$$

Theorem 3.1 (Two-public-value recovery)**.** *Assume the transcript has the form in equation* (5)*, with p odd and ℓ prime. Define $A = v_1^p - v_1$ and $B = v_2^p - v_2$. If $A \neq 0$, then v_1 and v_2 determine z by equation* (12)*. If $A = 0$ and $\gcd(\ell, p-1) = 1$, then $z = 1$. Hence, when $\gcd(\ell, p-1) = 1$, the first two public values determine z in all cases, and the full public transcript determines every secret.*

Proof. The case $A \neq 0$ follows from equations (8)–(11). Now suppose $A = 0$. Then $z^p = z$, so z is a root of $X^p - X$. Every element of $\mathbb{F}_p$ is a root, and a degree-p polynomial has at most p roots. Therefore $z \in \mathbb{F}_p^*$. On the other hand, $z \in \mu_\ell$, so the multiplicative order of z divides ℓ and $p - 1$. If $\gcd(\ell, p-1) = 1$, the order of z is 1, and hence $z = 1$. Equation (13) then gives every secret. □

For the target construction's numerical parameters, $p = 47$ and $\ell = 37$, so $\gcd(37, 46) = 1$. Thus the exceptional case is resolved for those parameters. If this greatest common divisor is not 1, the argument above does not in general determine z when $A = 0$.

4 Further leakage results

4.1 Disclosure of one secret

Suppose an adversary learns K_t for some index t. The corresponding public value gives

$$v_t - K_t = z^t. \tag{14}$$

If $\gcd(t, \ell) = 1$, there is an integer d such that $td \equiv 1 \pmod{\ell}$. Since $z^\ell = 1$, equation (14) gives

$$(v_t - K_t)^d = z^{td} = z. \tag{15}$$

The adversary can then recover every secret using equation (13).

Proposition 4.1. *For a transcript of the form in equation* (5)*, disclosure of* K_t *reveals all secrets whenever* $\gcd(t, \ell) = 1$.

Proof. Equation (15) recovers z from v_t and K_t. Substituting this value into equation (13) recovers each K_i. □

In the target example, $\ell = 37$ and the secret indices are $1, 2, 3, 4$. Since each of these indices is relatively prime to 37, disclosure of any one of the four secrets is sufficient to recover the others.

4.2 Candidate reduction from one public value

A single public value $v_1 = K_1 + z$ restricts the possible values of K_1. A candidate $k \in \mathbb{F}_p$ is valid only if $v_1 - k \in \mu_\ell$, or equivalently

$$(v_1 - k)^\ell = 1. \tag{16}$$

Thus the candidate set is

$$\mathcal{C}(v_1) = \{k \in \mathbb{F}_p : (v_1 - k)^\ell = 1\}. \tag{17}$$

This set need not contain exactly one element in every instance.

For the numerical fixture used in the accompanying experiments, let $p = 47$, $F = \mathbb{F}_{47^3}$, and $\ell = 37$, with

$$F = \mathbb{F}_{47}[\alpha]/(\alpha^3 + 3\alpha + 42),$$

where $X^3 + 3X + 42$ is irreducible over $\mathbb{F}_{47}$. Take

$$v_1 = 37\alpha^2 + 28\alpha + 12. \tag{18}$$

A valid mask $w = v_1 - k$ must satisfy $w^{37} = 1$. Since $k \in \mathbb{F}_{47}$, its conjugates are $v_1 - k$, $v_1^{47} - k$, and $v_1^{47^2} - k$. Their product is

$$(v_1 - k)(v_1^{47} - k)(v_1^{47^2} - k) = w^{1+47+47^2} = w^{2257} = 1, \tag{19}$$

where $2257 = 37 \cdot 61$. Direct calculation gives

$$v_1^{47} = 22 + 27\alpha + 42\alpha^2,$$
$$v_1^{47^2} = 15 + 39\alpha + 15\alpha^2,$$

and hence

$$(v_1 - k)(v_1^{47} - k)(v_1^{47^2} - k) = 12 - k^3 + 2k^2 - 18k. \tag{20}$$

Equating this expression to 1 gives

$$(k - 8)(k - 12)(k - 29) = 0 \pmod{47}. \tag{21}$$

The subgroup test in equation (16) gives

k	$(v_1 - k)^{37}$
8	1
12	$42 + 5\alpha + 41\alpha^2$
29	$18 + 17\alpha + 9\alpha^2$

so only $k = 8$ is valid. Thus this public value uniquely determines $K_1 = 8$ in this fixture. This uniqueness is specific to the example.

The cubic field representation above is the one used in the accompanying experiments. The published numerical example in [3] uses a different irreducible cubic, so the coordinates in this subsection are not presented as a reproduction of that example's field representation.

5 Computational Examples

The computations use SageMath 10.9. The implementation, attack scripts, and example public transcripts are available in the accompanying `GitHub repository`.

The repository contains toy and BLS12-381 masking-layer demonstrations of two-public-value recovery and recovery after disclosure of K_1, as well as the corrected $p = 47$, $\ell = 37$ one-value candidate search.

The attacks use only public transcripts and field parameters, except that the disclosure attack additionally receives K_1. The BLS12-381 verifiers compare recovered keys with dealer values in two fresh runs, but model only the masking layer. Reproduction commands and validation limits are documented in `attack/README.md`.

6 Conclusion

For the masking rule $v_i = K_i + z^i$, with $K_i \in \mathbb{F}_p$ and z in a multiplicative subgroup of an extension field of characteristic p, the first two public values determine the common mask under the conditions proved above. For the target construction's parameters, the exceptional case is resolved as well. The remaining public values then reveal all secrets. This is the principal confidentiality failure identified here. We also showed that disclosure of one suitable secret reveals the full sequence, and that one public value can restrict the possible first secret.

The results apply to the field-valued, common-base masking pattern specified in this paper. They do not establish that pairing-based secret sharing generally is insecure, and they do not automatically apply to constructions with a different algebraic form. The attacks use the public field values directly; they do not require solving an elliptic-curve discrete logarithm problem or inverting the pairing.

7 Future work

Further work could examine other public exponent sequences and determine which sets of public values permit recovery of the common mask. The analysis could also be extended to secrets in larger subfields. Single-value leakage could be quantified through candidate counts or information-theoretic measures. Finally, related masking schemes and modifications intended to prevent these attacks merit further study.

References

[1] V. P. Binu and A. Sreekumar, "Threshold multi secret sharing using elliptic curve and pairing," *International Journal of Information Processing*, vol. 9, no. 4, pp. 100–112, 2015. An online preprint is available at arXiv:1603.09524 (2016).

[2] M. Bahramian and K. Eslami, "A new verifiable multi-secret sharing scheme based on elliptic curves and pairings," *Italian Journal of Pure and Applied Mathematics*, no. 41, pp. 456–468, 2019. Available at the journal website.

[3] M. Chintamani, P. Paul, and L. Sa, "Conjunctive hierarchical multi-secret sharing scheme using elliptic curves," *Indian Journal of Pure and Applied Mathematics*, vol. 55, pp. 1456–1464, 2024. doi:10.1007/s13226-023-00450-x.