Jacobi Signatures, Revisited

Yansong Feng

AMSS, CAS

Abstract. We remove the Boneh–Lipton conjecture from the proof of Corrigan-Gibbs and Wu (CRYPTO 2024) that Jacobi signatures modulo $N = p^2q$ are one-way. This relates the one-wayness of the pseudorandom generator proposed by Damgård in 1988 to a standard number-theoretic problem alone.

Keywords: Jacobi signatures, Jacobi symbols, One-way functions, Factoring, Pseudorandom generators

1 Introduction

For an odd integer N, Damgård proposed generating pseudorandom bits from consecutive Jacobi symbols [4]:

$$J_{N,\ell}(x) := \left[\left(\frac{x+1}{N}\right), \ldots, \left(\frac{x+\ell}{N}\right)\right].$$

Corrigan–Gibbs and Wu [2] studied the case $N = p^2q$. Under a conjecture of Boneh and Lipton [1], they showed that, given $J_{N,\ell}(x)$, finding any x' such that $J_{N,\ell}(x') = J_{N,\ell}(x)$ is as hard as factoring N. That conjecture says, roughly, that every residue modulo q has a unique Legendre signature of length $2\log^2 q$. They asked whether the conjecture could be removed. Recent work on quadratic and quartic characters instead considers random offsets and a secret modulus [3,5].

Recall the reduction in [2]. Given $N = p^2q$, they choose a random $x \in \mathbb{Z}_N^*$, give $(J_{N,\ell}, J_{N,\ell}(x))$ to a one-wayness adversary $\mathcal{A}$, receive x', and compute $\gcd(N, x - x')$. Ignoring the negligible event that Jacobi symbol could be zero, each coordinate satisfies

$$\left(\frac{x+i}{p^2q}\right) = \left(\frac{x+i}{p}\right)^2 \left(\frac{x+i}{q}\right) = \left(\frac{x+i}{q}\right). \tag{1}$$

Thus, whenever $\mathcal{A}$ succeeds, we have $J_{q,\ell}(x') = J_{q,\ell}(x)$. The Boneh-Lipton conjecture is used at this single point to conclude that $x' = x \pmod q$. At the same time, the signature reveals no information about $x \bmod p^2$, so $x' \neq x \pmod{p^2}$ except with negligible probability. Consequently, $\gcd(N, x - x')$ is q or pq and is a proper factor of N.

Our approach. We replace worst-case uniqueness by an expectation over a uniformly random residue. Let R be a uniformly random allowed residue modulo q, and let $S(R)$ be the set of allowed residues having the same Legendre signature as R. If m_σ is the number of residues having signature σ, then the relevant quantity is

$$\mathbb{E}_R[|S(R)|] = \frac{1}{q-1-\ell}\sum_\sigma m_\sigma^2,$$

not the worst-case value $\max_\sigma m_\sigma$. We bound this expectation unconditionally using complete character sums. A general probability lemma then shows that if $\mathcal{A}$ outputs an element of $S(R)$ with probability α, the probability that the induced algorithm outputs R itself is at least $\alpha^2/\mathbb{E}_R[|S(R)|]$. This is enough to replace the Boneh-Lipton conjecture used in [2].

Acknowledgment. GPT-5.6 Sol Ultra found this proof in conversation with the author while unsuccessfully attempting to prove the Boneh–Lipton conjecture [1]. The author verified every statement and proof, simplified and refined the argument, and wrote the final manuscript. The author is fully responsible for the correctness, writing and discussions of this paper.

2 Preliminaries

2.1 Notation

Throughout this work, $\lambda \in \mathbb{N}$ denotes the security parameter. Let Primes_λ denote the set of λ-bit odd primes. Unless stated otherwise, p and q are sampled uniformly from Primes_λ subject to $p \neq q$, and $N = p^2q$. An algorithm is *efficient* if it runs in probabilistic polynomial time in the length of its input. A function is negligible if it is $o(\lambda^{-c})$ for every constant $c \in \mathbb{N}$; we denote such a function by $\mathrm{negl}(\lambda)$.

2.2 Legendre and Jacobi signatures

Definition 1 (Jacobi and Legendre Signatures). *For a positive odd integer N and a signature length ℓ, define the Jacobi-signature function $J_{N,\ell} : \mathbb{Z}_N^* \to \{-1,1\}^\ell$ by*

$$J_{N,\ell}(x) := \left[\left(\frac{x+1}{N}\right), \left(\frac{x+2}{N}\right), \ldots, \left(\frac{x+\ell}{N}\right)\right].$$

When q is prime, we refer to $J_{q,\ell}$ as the Legendre signature.

Following the convention of Corrigan-Gibbs and Wu [2], we regard these signatures as elements of $\{-1,1\}^\ell$. Strictly speaking, one of the shifted values

$x + i$ can be a non-unit and produce the symbol 0. For a random unit x and $N = p^2q$, this happens with probability at most

$$\frac{\ell}{p-1} + \frac{\ell}{q-1} = \mathrm{negl}(\lambda). \tag{2}$$

We simply condition away this event and absorb its probability into the final negligible term.

We also recall the following standard consequence of the Weil bound for complete multiplicative-character sums [6].

Lemma 1 (Weil bound). *Let $f \in \mathbb{F}_q[X]$ be a square-free polynomial of degree $d \geq 1$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \left(\frac{f(x)}{q} \right) \right| \leq (d-1)\sqrt{q}.$$

2.3 Standard cryptographic definitions

We follow the definitions and notation of Corrigan-Gibbs and Wu [2].

Definition 2 (One-Way Function). *For a function ensemble $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$, where each $f \in \mathcal{F}_\lambda$ has type $f : \mathcal{X}_\lambda \to \mathcal{Y}_\lambda$, define the advantage of an adversary $\mathcal{A}$ at breaking the one-wayness of $\mathcal{F}$ as*

$$\mathsf{OWFAdv}[\mathcal{A}, \mathcal{F}](\lambda) := \Pr\left[f(x) = f(x') : \begin{array}{c} f \xleftarrow{\mathrm{R}} \mathcal{F}_\lambda, \quad x \xleftarrow{\mathrm{R}} \mathcal{X}_\lambda, \\ x' \leftarrow \mathcal{A}(f, f(x)) \end{array} \right]. \tag{3}$$

We say that $\mathcal{F}$ is one-way if $\mathsf{OWFAdv}[\mathcal{A}, \mathcal{F}](\lambda) = \mathrm{negl}(\lambda)$ for every efficient adversary $\mathcal{A}$.

For any fixed polynomially bounded signature-length function $\ell = \ell(\lambda)$, define the Jacobi-signature ensemble

$$\begin{aligned} \mathcal{J}_\lambda^{\mathsf{OWF}} &:= \left\{ J_{N,\ell} \;\middle|\; p, q \in \mathsf{Primes}_\lambda,\ p \neq q;\ N \leftarrow p^2 q \right\}, \\ \mathcal{J}^{\mathsf{OWF}} &:= \{\mathcal{J}_\lambda^{\mathsf{OWF}}\}_{\lambda \in \mathbb{N}}. \end{aligned} \tag{4}$$

where sampling a function means sampling p and q uniformly subject to $p \neq q$. In particular, the original choice in Corrigan-Gibbs and Wu [2] is $\ell(\lambda) = 2\lambda^2$. For a sampled member $f = J_{N,\ell}$, the domain $\mathcal{X}_\lambda$ in Equation (3) is understood to be the natural domain $\mathbb{Z}_N^*$ of that member.

Definition 3 (Factoring). *We define the advantage of an algorithm $\mathcal{B}$ at factoring integers of the form pq as*

$$\mathsf{FactAdv}[\mathcal{B}](\lambda) := \Pr\left[1 < \gcd(t, N) < N : \begin{array}{c} p \xleftarrow{\mathrm{R}} \mathsf{Primes}_\lambda, \quad q \xleftarrow{\mathrm{R}} \mathsf{Primes}_\lambda \setminus \{p\}, \\ N \leftarrow pq, \quad t \leftarrow \mathcal{B}(N) \end{array} \right].$$

We define $\mathsf{FactAdv}_{p^2q}[\mathcal{B}](\lambda)$ analogously, except that the experiment sets $N \leftarrow p^2q$. The p^2q-factoring assumption holds if $\mathsf{FactAdv}_{p^2q}[\mathcal{B}](\lambda) = \mathrm{negl}(\lambda)$ for every efficient algorithm $\mathcal{B}$.

Thus, $\mathsf{OWFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{OWF}}](\lambda)$ is the probability that the adversary $\mathcal{A}$, given a random function $J_{N,\ell}$ and the image of a uniform $x \in \mathbb{Z}_N^*$, outputs any x' satisfying $J_{N,\ell}(x') = J_{N,\ell}(x)$, up to the negligible conditioning loss above.

3 One-Wayness of Jacobi Signatures

3.1 Expected Number of Residues Sharing a Legendre Signature

Fix an odd prime q and an integer $1 \le \ell < q-1$. Let

$$\mathcal{R} := \mathbb{F}_q^* \setminus \{-1, \dots, -\ell\}$$

be the set of allowed residues. Then $|\mathcal{R}| = q - 1 - \ell$. For each $\sigma \in \{-1, 1\}^\ell$, let

$$m_\sigma := \#\{r \in \mathcal{R} : J_{q,\ell}(r) = \sigma\},$$

and define

$$D(q, \ell) := \frac{1}{q-1-\ell} \sum_{\sigma \in \{-1,1\}^\ell} m_\sigma^2.$$

If R is uniform over $\mathcal{R}$, define

$$S(R) := \{s \in \mathcal{R} : J_{q,\ell}(s) = J_{q,\ell}(R)\}.$$

Then

$$D(q, \ell) = \mathbb{E}_R[|S(R)|]\,.$$

Thus, $D(q, \ell)$ is the expected number of allowed residues with the same signature as R.

Lemma 2. *For every odd prime q and $1 \le \ell < q-1$,*

$$D(q, \ell) \le \frac{q^2 2^{-\ell} + q\left((\ell^2 - 3\ell + 4)/4 - 2^{-\ell}\right)}{q-1-\ell}. \tag{5}$$

In particular, if $\ell < q/2$, then $D(q, \ell) = O(q2^{-\ell} + \ell^2)$.

Proof. For any two allowed residues x, y, the indicator that their signatures are the same is

$$\mathbf{1}[J_{q,\ell}(x) = J_{q,\ell}(y)] = 2^{-\ell} \prod_{i=1}^{\ell} (1 + \left(\frac{x+i}{q}\right)\left(\frac{y+i}{q}\right)).$$

Since $\sum_\sigma m_\sigma^2$ counts ordered pairs of allowed residues that have the same signature, we may sum this identity over all such pairs. Each factor on the right is nonnegative, even if $x + i = 0$ or $y + i = 0$. Therefore, extending the sum to all $(x, y) \in \mathbb{F}_q^2$ can only make it larger. Expanding the product, the sums over x and y factor, giving

$$\sum_\sigma m_\sigma^2 \le 2^{-\ell} \sum_{S \subseteq \{1,\dots,\ell\}} A_S^2, \qquad A_S := \sum_{x \in \mathbb{F}_q} \left(\frac{\prod_{i \in S}(x+i)}{q}\right).$$

For $S = \varnothing$, $A_S = q$, and for $|S| = 1$, $A_S = 0$. If $|S| = s \geq 2$, the polynomial $\prod_{i \in S}(X + i)$ has s distinct roots and is not a square. Applying Lemma 1 gives

$$|A_S| \leq (s-1)\sqrt{q}.$$

Consequently,

$$\sum_{\sigma} m_\sigma^2 \leq q^2 2^{-\ell} + q 2^{-\ell} \sum_{s=2}^{\ell} \binom{\ell}{s} (s-1)^2 \leq q^2 2^{-\ell} + q \left(\frac{\ell^2 - 3\ell + 4}{4} - 2^{-\ell} \right). \quad (6)$$

Substitution into Equation (6), followed by division by $q - 1 - \ell$, proves Equation (5).

Remark 1. To verify the last equality in Equation (6), let $X \sim \mathrm{Bin}(\ell, 1/2)$. Then

$$\mathbb{E}\big[(X-1)^2\big] = \mathrm{Var}(X) + \big(\mathbb{E}[X] - 1\big)^2 = \frac{\ell^2 - 3\ell + 4}{4}.$$

The term with $s = 0$ is $2^{-\ell}$, while the term with $s = 1$ is zero. Therefore,

$$2^{-\ell} \sum_{s=2}^{\ell} \binom{\ell}{s} (s-1)^2 = \frac{\ell^2 - 3\ell + 4}{4} - 2^{-\ell}.$$

3.2 The Main Reduction

We fisrt introduce the following Lemma 3, which connects the one-wayness experiment to a number-theoretic calculation.

Lemma 3. *Let $h : X \to Y$ be a function on a finite nonempty set, let $m_y = |h^{-1}(y)|$, and choose R uniformly from X. Let Q be a randomized algorithm whose input is only $h(R)$. If*

$$\alpha = \Pr[Q(h(R)) \in h^{-1}(h(R))],$$

then

$$\Pr[Q(h(R)) = R] \geq \frac{\alpha^2}{|X|^{-1} \sum_{y \in Y} m_y^2}. \quad (7)$$

Proof. For each $y \in h(X)$, let $a_y = \Pr[Q(y) \in h^{-1}(y)]$. Conditioned on $h(R) = y$, the random point R is uniform over $h^{-1}(y)$ and is independent of the random coins used by Q. Therefore

$$\alpha = \frac{1}{|X|} \sum_y m_y a_y, \qquad \Pr[Q(h(R)) = R] = \frac{1}{|X|} \sum_y a_y.$$

Since $0 \leq a_y \leq 1$, the Cauchy–Schwarz inequality gives

$$\left(\sum_y m_y a_y \right)^2 \leq \left(\sum_y m_y^2 \right) \left(\sum_y a_y^2 \right) \leq \left(\sum_y m_y^2 \right) \left(\sum_y a_y \right).$$

Therefore, Equation (7) follows.

Now we can give the main reduction by applying Lemma 2.

Theorem 1 (Main reduction). *Let $\ell = \ell(\lambda)$ be polynomially bounded, and let $\mathcal{J}^{\mathsf{OWF}}$ denote the ensemble in Equation (4) induced by this length function. For every efficient adversary $\mathcal{A}$ there is an efficient algorithm $\mathcal{B}$ such that, for all sufficiently large λ,*

$$\mathsf{FactAdv}_{p^2q}[\mathcal{B}](\lambda) \geq \frac{\big(\mathsf{OWFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{OWF}}](\lambda)\big)^2}{2^{\lambda+1-\ell} + (\ell^2 - 3\ell + 4)/2} - \mathrm{negl}(\lambda). \tag{8}$$

Proof. On input N, algorithm $\mathcal{B}$ samples x uniformly modulo N and computes $d = \gcd(x, N)$. If $1 < d < N$, it outputs d; if $d = N$, it resamples. Otherwise, x is uniform in $\mathbb{Z}_N^*$. Algorithm $\mathcal{B}$ then runs

$$x' \leftarrow \mathcal{A}(J_{N,\ell}, J_{N,\ell}(x)).$$

If x' is a valid preimage, it computes $\gcd(N, x - x')$ and outputs it if it is a proper factor of N.

Fix $N = p^2q$. As explained in the preliminaries, we ignore the negligible zero-symbol event. By the Chinese remainder theorem, write

$$x \longleftrightarrow (u, r) \in \mathbb{Z}_{p^2}^* \times \mathbb{F}_q^*.$$

Here, r is uniform over $\mathcal{R}$, while u is independent and uniform over the $p(p-1-\ell)$ residues modulo p^2 for which none of $u+1, \ldots, u+\ell$ is divisible by p. By Equation (1),

$$J_{N,\ell}(x) = J_{q,\ell}(r).$$

Thus, the challenge given to $\mathcal{A}$ depends on r but not on u.

Let ε_N be the success probability of $\mathcal{A}$ for this fixed modulus. For the analysis, define $\mathcal{Q}$ as follows. On input a Legendre signature σ, it runs

$$x' \leftarrow \mathcal{A}(J_{N,\ell}, \sigma).$$

If x' is a valid preimage, it outputs $x' \bmod q$; otherwise, it outputs $\perp$. Whenever $\mathcal{A}$ succeeds, $\mathcal{Q}$ outputs an element of $S(r)$. Applying Lemma 3 to $J_{q,\ell} : \mathcal{R} \to \{-1, 1\}^\ell$ gives

$$\Pr[x' \equiv x \pmod q \text{ and } \mathcal{A} \text{ succeeds} \mid N] \geq \frac{\varepsilon_N^2}{D(q, \ell)}. \tag{9}$$

Since u is independent of the view and output of $\mathcal{A}$,

$$\Pr[x' \equiv x \pmod{p^2}] \leq \frac{1}{p(p-1-\ell)} = \mathrm{negl}(\lambda).$$

Therefore, except with negligible probability, the event in Equation (9) also satisfies $x' \not\equiv x \pmod{p^2}$. In this case, $\gcd(N, x - x')$ is either q or pq, and hence is a proper factor of N.

Since q is a λ-bit prime and $\ell = \mathrm{poly}(\lambda)$, for all sufficiently large λ we have $q - 1 - \ell \geq q/2$. Lemma 2 therefore gives

$$D(q, \ell) \leq 2^{\lambda+1-\ell} + \frac{\ell^2 - 3\ell + 4}{2}. \tag{10}$$

Averaging over N and applying Jensen's inequality, we obtain

$$\begin{aligned} \mathsf{FactAdv}_{p^2q}[\mathcal{B}](\lambda) &\geq \frac{\mathbb{E}_N[\varepsilon_N^2]}{2^{\lambda+1-\ell} + (\ell^2 - 3\ell + 4)/2} - \mathrm{negl}(\lambda) \\ &\geq \frac{\big(\mathbb{E}_N[\varepsilon_N]\big)^2}{2^{\lambda+1-\ell} + (\ell^2 - 3\ell + 4)/2} - \mathrm{negl}(\lambda). \end{aligned}$$

Finally,

$$\mathbb{E}_N[\varepsilon_N] \geq \mathsf{OWFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{OWF}}](\lambda) - \mathrm{negl}(\lambda).$$

Absorbing all negligible terms proves Equation (8).

Remark 2. Suppose that factoring $N = p^2q$, where p and q are independent random λ-bit primes, is hard. Then Theorem 1 implies that $\mathcal{J}^{\mathsf{OWF}}$ is one-way for every $\ell = \lambda^{O(1)}$ satisfying $\ell \geq \lambda - O(\log \lambda)$. Indeed, in this range, both $2^{\lambda-\ell}$ and ℓ^2 are bounded by $\lambda^{O(1)}$.

Remark 3. We follow the simpler convention used in [2]. A fully formal treatment could first define a signature function taking values in $\{-1, 0, 1\}^\ell$, and then restrict its domain to inputs whose signatures contain no zero entries. By Equation (2), a zero occurs with negligible probability. Hence, this convention changes the bounds by at most a negligible term and does not affect the main argument.

4 Future Work

Several questions remain open: whether similar reductions can establish collision resistance or pseudorandomness, and whether one-wayness extends to square-free pq or public prime moduli. Another direction is to replace consecutive offsets with public random offsets. Existing results for quadratic and quartic characters with random offsets use a secret prime modulus [3,5], the case of a public p^2q modulus remains open.

References

1. Boneh, D., Lipton, R.J.: Algorithms for black-box fields and their application to cryptography. In: Advances in Cryptology – CRYPTO '96. Lecture Notes in Computer Science, vol. 1109, pp. 283–297. Springer (1996)
2. Corrigan-Gibbs, H., Wu, D.J.: The One-Wayness of Jacobi Signatures. In: Advances in Cryptology – CRYPTO 2024. Lecture Notes in Computer Science, vol. 14924, pp. 3–13. Springer (2024)

3. Corrigan-Gibbs, H., Wu, D.J.: The Pseudorandomness of Legendre Symbols under the Quadratic-Residuosity Assumption. In: Theory of Cryptography – TCC 2025. Lecture Notes in Computer Science, vol. 16270, pp. 298–322. Springer (2025)
4. Damgård, I.B.: On the Randomness of Legendre and Jacobi Sequences. In: Advances in Cryptology – CRYPTO '88. Lecture Notes in Computer Science, vol. 403, pp. 163–172. Springer (1990)
5. Dey, M., Dey, S., Pal, S., Samajder, S., Barua, R.: Beyond quadratic: Unlocking pseudorandomness with quartic character. Cryptology ePrint Archive, Paper 2026/964 (2026), `https://eprint.iacr.org/2026/964`
6. Weil, A.: On some exponential sums. Proceedings of the National Academy of Sciences **34**(5), 204–207 (1948)