The One-Wayness of Jacobi Signatures

Henry Corrigan-Gibbs
MIT

David J. Wu
UT Austin

Abstract. We show that under a mild number-theoretic conjecture, recovering an integer from its Jacobi signature modulo $N = p^2q$, for primes p and q, is as hard as factoring N. This relates, for the first time, the one-wayness of a pseudorandom generator that Damgård proposed in 1988, to a standard number-theoretic problem. In addition, we show breaking the Jacobi pseudorandom function is no harder than factoring.

1 Introduction

In 1988, Damgård [8] proposed a pair of cryptographic pseudorandom generators, based on quadratic characters. For a fixed natural number N, he speculated that the function that maps $x \in \mathbb{Z}_N^*$ to the sequence of Jacobi symbols

$$\left[\left(\frac{x+1}{N}\right), \left(\frac{x+2}{N}\right), \ldots, \left(\frac{x+\ell}{N}\right) \right] \quad \in \{-1, 1\}^\ell,$$

for some $\ell \in \mathbb{N}$, is a pseudorandom generator. Following prior work [7], we refer to this sequence of Jacobi symbols as the *length-ℓ Jacobi signature of x modulo N*. Damgård also considered the case when the modulus is a prime p; in that case we replace Jacobi symbols with Legendre symbols and refer to the sequence as the *Legendre signature of x modulo p*.

He left as an open question whether is is possible to relate the task of breaking these pseudorandom generators to any other number-theoretic problem.

This work. We consider Damgård's pseudorandom generator based on Jacobi symbols modulo $N = p^2q$, for primes p and q. We show that this function is a one-way function if:

- factoring integers of the form p^2q is hard, and
- if every number modulo p has a unique Legendre signature of length $2\log^2(p)$.

Under a much stronger (and less plausible) number-theoretic assumption, we show that finding collisions in Damgård's Jacobi pseudorandom generator is as hard as factoring.

Both results are based on the simple observation that Jacobi symbol of x modulo $N = p^2q$ is equal to the Legendre symbol of x modulo q. Thus, if we give an attacker the Jacobi signature of a secret value x modulo N, we reveal no information to the attacker about the Legendre signature of x modulo p.

If the attacker succeeds at inverting the Jacobi-signature function modulo N, we then get a value $x' \in \mathbb{Z}_N^*$ such that x and x' have the same Legendre signature modulo q. Under a standard number-theoretic conjecture on the uniqueness

of Legendre signatures [7], this implies that $x = x' \bmod q$. At the same time, since the attacker has no information about $x \bmod p^2$, it is extremely likely that $x \neq x' \bmod p^2$. In this case, the the greatest common divisor of $x - x'$ and the modulus N will yield a non-trivial factor of N.

As an immediate consequence, if we additionally conjecture the hardness of distinguishing integers of the form p^2q, from integers of the form pq [1], for primes p and q, then our results also imply the one-wayness of the Jacobi pseudorandom generator modulo $N = pq$. (We thank an anonymous reviewer for this observation.)

Lastly, we consider the generalization of the Jacobi pseudorandom generator to a *pseudorandom function* [5]. Specifically, for a (public) composite modulus N, a secret key $k \in \mathbb{Z}_N$, and an input $x \in \mathbb{Z}_N$, the Jacobi pseudorandom function outputs the Jacobi symbol of $(k + x)$ modulo N. In Section 5, we show that an algorithm that can factor N can break this construction as a pseudorandom function. This immediately gives a subexponential-time attack on the Jacobi pseudorandom function and, via Shor's algorithm [20], a quantum polynomial-time attack as well.

Related work. Peralta and Okamoto [18] use Jacobi signatures modulo $N = p^2q$ to speed up the elliptic-curve factoring algorithm. In particular, they use Jacobi signatures modulo N to quickly search a list of integers $x_1, x_2, \ldots, x_k \in \mathbb{Z}_N^*$ for a pair whose difference has a non-trivial greatest common divisor with N. Several cryptosystems have also based their security on the hardness of factoring integers of the form p^2q [11,17].

Adleman and McCurley [1] discuss the problem of finding the smallest prime q whose Legendre symbols modulo the first ℓ primes matches a prescribed pattern in $\{-1, 1\}^\ell$. Solving this problem, they note, is as hard as factoring numbers of the form $N = p^2q$, provided that the signature length ℓ is long enough to uniquely identify the prime q.

Grassi et al. [13] propose using a variant of Damgård's construction as a pseudorandom function. For a fixed prime p, key $k \in \mathbb{Z}_p^*$, and input $x \in \mathbb{Z}_p^*$, the function's output is the Legendre symbol of $(k + x)$ modulo p. This function has a small arithmetic circuit over $\mathbb{F}_p$, which makes it useful in multiparty computation [13,9,4]. Several recent works have also studied the concrete hardness of the Legendre pseudorandom function [5,14,19].

2 Preliminaries

Throughout this work, we write $\lambda \in \mathbb{N}$ to denote a security parameter. For a positive integer $n \in \mathbb{N}$, we write $[n]$ to denote the set $[n] := \{1, \ldots, n\}$. We say that an algorithm is efficient if it runs in probabilistic polynomial time in the length of its input. We say that a function $f(\lambda)$ is negligible if $f = o(\lambda^{-c})$ for all constants $c \in \mathbb{N}$; we denote this by writing $f = \mathrm{negl}(\lambda)$. To denote the greatest common divisor of natural numbers x and y, we write $\gcd(x, y)$. For a natural number λ, we let Primes_λ denote the set of λ-bit primes.

2.1 Legendre and Jacobi Signatures

We now recall the concept of a Legendre signature and a Jacobi signature.

Definition 2.1 (Jacobi and Legendre Signatures). For an integer N and $x \in \mathbb{Z}_N^*$, let $\left(\frac{x}{N}\right) \in \{-1, 1\}$ denote the Jacobi symbol of x modulo N. Then, for a positive integer N and signature length ℓ, we define the Jacobi-signature function $J_{N,\ell} \colon \mathbb{Z}_N^* \to \{-1,1\}^\ell$ as the function

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

When p is a prime, we refer to the function $J_{p,\ell}$ as the "Legendre signature."

Fact 2.2 (Jacobi Signatures with $N = p^2 q$). *For odd primes p, q and $N = p^2 q$, for all $x \in \mathbb{Z}_N^*$ and $\ell \in \mathbb{Z}$, $J_{N,\ell}(x) = J_{q,\ell}(x)$.*

Proof. The statement follows because the Jacobi symbol is multiplicative and takes on values in $\{-1, 1\}$: $\left(\frac{x}{N}\right) = \left(\frac{x}{p}\right)^2 \cdot \left(\frac{x}{q}\right) = \left(\frac{x}{q}\right)$. □

2.2 Standard Cryptographic Definitions

We recall a few standard cryptographic definitions. For each of the following cryptographic notions or assumptions, we define the advantage of the adversary. Typically, we say that the associated scheme is secure or that the assumption holds if the advantage of every efficient (i.e., probabilistic polynomial time) adversary is bounded by a negligible function of the security parameter.

Definition 2.3 (One-Way Function). For a function ensemble $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$, where each function $f \in \mathcal{F}_\lambda$ has the type $f \colon \mathcal{X}_\lambda \to \mathcal{Y}_\lambda$, define the *advantage of an algorithm $\mathcal{A}$ at breaking the one-wayness of $\mathcal{F}$* as:

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

Definition 2.4 (Collision Resistance). For a function ensemble $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$, where each function $f \in \mathcal{F}_\lambda$ has the type $f \colon \mathcal{X}_\lambda \to \mathcal{Y}_\lambda$, define the *advantage of an algorithm $\mathcal{A}$ at breaking the collision resistance of $\mathcal{F}$* as:

$$\mathsf{CRHFAdv}[\mathcal{A}, \mathcal{F}](\lambda) := \Pr\left[f(x) = f(x') \text{ and } x \neq x' : \begin{array}{c} f \xleftarrow{R} \mathcal{F}_\lambda \\ (x, x') \leftarrow \mathcal{A}(f) \end{array} \right].$$

Definition 2.5 (Pseudorandom Function). For a function ensemble $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$, where each function $f \in \mathcal{F}_\lambda$ has the type $f \colon \mathcal{K}_f \times \mathcal{X}_f \to \mathcal{Y}_f$, for an algorithm $\mathcal{A}$, and a bit $b \in \{0, 1\}$, define

$$\rho_{\mathcal{A},\mathcal{F},b}(\lambda) := \Pr\left[\mathcal{A}^{f_b(\cdot)}(f) = 1 : \begin{array}{r} f \xleftarrow{R} \mathcal{F}_\lambda, k \xleftarrow{R} \mathcal{K}_f \\ f_0 := f(k, \cdot) \\ f_1 \xleftarrow{R} \mathsf{Funs}[\mathcal{X}_f, \mathcal{Y}_f] \end{array} \right],$$

where $\mathsf{Funs}[\mathcal{X}_f, \mathcal{Y}_f]$ denotes the set of all functions with domain $\mathcal{X}_f$ and co-domain $\mathcal{Y}_f$. Then, define the *advantage of an algorithm $\mathcal{A}$ at breaking the pseudorandomness of $\mathcal{F}$* as:

$$\mathsf{PRFAdv}[\mathcal{A}, \mathcal{F}](\lambda) := \left|\rho_{\mathcal{A},\mathcal{F},0}(\lambda) - \rho_{\mathcal{A},\mathcal{F},1}(\lambda)\right|.$$

Definition 2.6 (Factoring). We define the advantage of an algorithm $\mathcal{A}$ at factoring integers of the form pq, for primes p and q, as

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

We define $\mathsf{FactAdv}_{p^2q}[\mathcal{A}](\lambda)$ analogously, except that we run algorithm $\mathcal{A}$ on p^2q.

3 One-Wayness of Jacobi Signatures

Our first result relies on a conjecture of Boneh and Lipton [7], which states that, for a prime p, each value in $\mathbb{Z}_p^*$ has a unique Legendre signature of length $\lceil 2\log^2 p\rceil$:

Conjecture 3.1 (Boneh and Lipton [7]). *For all sufficiently large primes p, for all distinct $x, x' \in \mathbb{Z}_p^*$, and for $\ell = \lceil 2\log^2 p\rceil$, it holds that $J_{p,\ell}(x) \neq J_{p,\ell}(x')$.*

Our results also hold under a weaker conjecture, where the signature length is $\ell = \log^c(p)$, for any $c > 2$. At the end of this section, we further discuss Conjecture 3.1.

Under Conjecture 3.1, we show that inverting the Jacobi-signature function modulo an integer $N = p^2q$, for primes p and q, is as hard as hard as factoring N, provided that the Jacobi-signature length is at least $\lceil 2\log^2 N\rceil$. Specifically, we define $\mathcal{J}_\lambda^{\mathsf{OWF}}$ to be

$$\mathcal{J}_\lambda^{\mathsf{OWF}} := \{J_{N,2\lambda^2} \mid p, q \in \mathsf{Primes}_\lambda; N \leftarrow p^2 \cdot q\}.$$

We then have:

Proposition 3.2 (One-Wayness of Jacobi Signatures). *Under Conjecture 3.1, for every efficient algorithm $\mathcal{A}$, there is an efficient algorithm $\mathcal{B}$ such that for all $\lambda \in \mathbb{N}$*

$$\mathsf{OWFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{OWF}}](\lambda) \leq \mathsf{FactAdv}_{p^2q}[\mathcal{B}](\lambda) + \mathrm{negl}(\lambda).$$

Proof. Suppose there exists an efficient adversary $\mathcal{A}$ that breaks one-wayness of $\mathcal{J}^{\mathsf{OWF}}$ with advantage $\varepsilon = \mathsf{OWFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{OWF}}](\lambda)$. We construct an algorithm $\mathcal{B}$ for factoring integers of the form p^2q as follows:

- On input the modulus N, Algorithm $\mathcal{B}$ samples $x \xleftarrow{R} \mathbb{Z}_N$ and computes $t = \gcd(x, N)$. If $t \neq 1$, then Algorithm $\mathcal{B}$ outputs t.
- If $\gcd(x, N) = 1$, then $x \in \mathbb{Z}_N^*$, so Algorithm $\mathcal{B}$ runs $x' \leftarrow \mathcal{A}(J_{N,\ell}, J_{N,\ell}(x))$ where $\ell = 2\lambda^2$ is the signature length.

– Algorithm $\mathcal{B}$ computes $t = \gcd(N, x - x')$.

To complete the proof, we analyze the advantage of algorithm $\mathcal{B}$:

– By definition, the adversary receives $N = p^2 q$, where p and q are odd primes.
– Consider the initial value x that Algorithm $\mathcal{B}$ samples. If $\gcd(x, N) \neq 1$, then Algorithm $\mathcal{B}$ successfully factored N. If $\gcd(x, N) = 1$, then the distribution of x is uniform over $\mathbb{Z}_N^*$. By assumption, with probability at least ε, Algorithm $\mathcal{A}$ then outputs x' such that $J_{N,\ell}(x') = J_{N,\ell}(x)$.
– By Fact 2.2, $J_{N,\ell}(x') = J_{q,\ell}(x') = J_{q,\ell}(x) = J_{N,\ell}(x)$. By Conjecture 3.1, we then have that $x = x' \bmod q$.
– Next, consider the view of adversary $\mathcal{A}$. Again by Fact 2.2,

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

Since $J_{N,\ell}(x)$ is only a function of $x \bmod q$, we conclude via the Chinese Remainder Theorem that $J_{N,\ell}(x)$ information-theoretically hides the value of $x \bmod p^2$. This means the value of $x' \bmod p^2$ that Algorithm $\mathcal{B}$ chooses is independent of $x \bmod p^2$. Moreover, since the distribution of x is uniform over $\mathbb{Z}_N^*$, the value of $x \bmod p^2$ is uniform over $\mathbb{Z}_{p^2}^*$. Thus,

$$\Pr[x = x' \bmod p^2] = \frac{1}{|\mathbb{Z}_{p^2}^*|} = \frac{1}{p(p-1)} = \mathrm{negl}(\lambda).$$

Thus, with probability $1 - \mathrm{negl}(\lambda)$, it holds that $x \neq x' \bmod p^2$. If $x = x' \bmod q$ and $x \neq x' \bmod p^2$, then it follows that $\gcd(x - x', N) \in \{q, pq\}$ so algorithm $\mathcal{B}$ produces a non-trivial factor of N.

We conclude that algorithm $\mathcal{B}$ succeeds in factoring N with probability

$$\mathsf{FactAdv}_{p^2 q}[\mathcal{B}](\lambda) \geq \varepsilon - \mathrm{negl}(\lambda) = \mathsf{OWFAdv}[\mathcal{A}, \mathcal{J}_\lambda^{\mathsf{OWF}}](\lambda) - \mathrm{negl}(\lambda). \qquad \square$$

Remark 3.1 (Polynomial Number of Preimages). Conjecture 3.1 asserts that for $\ell = 2\lceil \log^2 p \rceil$, the length-$\ell$ Legendre signature of $x \in \mathbb{Z}_p^*$ *uniquely* determines p. We can relax this conjecture to require that for every length-ℓ signature $\sigma \in \{-1, 1\}^\ell$, there are *at most* $\mathrm{polylog}\, p$ number of values x where $J_{p,\ell}(x) = \sigma$. In this case, the reduction algorithm from Proposition 3.2 still applies, except its success probability is now smaller by a factor $1/\mathrm{polylog}\, p$. This is because the pre-image x' output by the one-wayness adversary $\mathcal{A}$ will only satisfy $x' = x \bmod q$ with probability $1/\mathrm{polylog}\, p$ rather than with probability 1. Several works focused on cryptanalyzing the Legendre-signature-based cryptosystems have relied on similar conjectures (c.f., [15, §2], [5, Assumption 1] and [10, Heuristic 1]).

Discussion of Conjecture 3.1. If Conjecture 3.1 were true unconditionally, it would imply a surprising number-theoretic result. Specifically, Conjecture 3.1 implies that the least quadratic non-residue modulo p is at most $\lceil 2 \log^2 p \rceil + 1$:

Proposition 3.3. *If all length-ℓ Legendre signatures modulo a prime p are distinct, then the least quadratic non-residue modulo p is at most $\ell + 1$.*

Proof. If the least quadratic non-residue is n_p, then the length-ℓ Legendre signatures of the first $\max\{0, n_p - \ell\}$ positive integers are identical—i.e., they consist of strings of ℓ ones. If all length-ℓ signatures are to be distinct, it must then be that $n_p - \ell \leq 1$. □

There is no known proof that the least quadratic non-residue modulo an arbitrary prime is even bounded by polylog(p), except under the Generalized Riemann Hypothesis [2,3,16]. The tightest bound currently known is $n_p \leq \log^2 p$ under the Generalized Riemann Hypothesis [16]. If Conjecture 3.1 were true unconditionally, it would imply an $O(\log^2 p)$ bound on the least quadratic non-residue, which in turn would give an $O(\log^2 p)$-time *deterministic* algorithm for producing a quadratic non-residue. Whether such an algorithm exists (unconditionally) is a longstanding open question [1].

The smallest signature length ℓ for which we know Conjecture 3.1 to be unconditionally true is $\ell \geq p^{\varepsilon}$ for some $\varepsilon > 0$ [6]. This would only imply the hardness of inverting the Jacobi pseudorandom generator with exponentially long output, which is not interesting in the standard cryptographic setting.

4 Collision Resistance of Jacobi Signatures

In this section, we show that if:

- factoring numbers of the form $N = p^2 q$, for primes p and q, is hard, and
- there exists a constant $k \in (2, 3)$ such that for most primes p, all Legendre signatures of length $\lceil k \log p \rceil$ are unique

then the Jacobi-signature function modulo N is collision resistant when the signature length is $\lceil \frac{k}{3} \log N \rceil$.

More precisely, our argument for collision resistance relies on the following number-theoretic assumption:

Assumption 4.1 (Uniqueness of Jacobi Signatures). *There exists a constant $k \in (2, 3)$ such that for a random λ-bit prime p, for all distinct $x, x' \in \mathbb{Z}_p^*$, and for $\ell = \lceil k \log p \rceil$, it holds that $J_{p,\ell}(x) \neq J_{p,\ell}(x')$, except with probability negligible in λ, only over the choice of prime p. More formally, we assume that for $\ell = \lceil k \log p \rceil$, there exists a negligible function* $\mathrm{negl}(\cdot)$ *such that for all $\lambda \in \mathbb{N}$,*

$$\Pr[\exists x \neq x' : J_{p,\ell}(x) = J_{p,\ell}(x') \mid p \leftarrow \mathsf{Primes}_\lambda] = \mathrm{negl}(\lambda).$$

This assumption differs from Conjecture 3.1 in two ways. In particular,

1. this assumption considers Legendre signatures of length $O(\log p)$ whereas Conjecture 3.1 considers Legendre signatures of length $\Omega(\log^2 p)$, and
2. this assumption is a statement about *a large fraction* of primes p, whereas Conjecture 3.1 is a statement about *all* large enough primes p.

We need the first modification since for the Jacobi-signature function $J_{N,\ell}$ to be compressing, the signature length ℓ must satisfy $\ell < \log N$. When $N = p^2q$, this requires $k < 3$. In addition, we require $k > 2$ to evade the birthday bound. Specifically, for a prime p, if we *heuristically* model the Jacobi signatures $J_{p,\ell}(x)$ for each $x \in \mathbb{Z}_p^*$ as uniform random strings drawn from $\{-1,1\}^\ell$, then by the birthday bound, with constant probability, there will exist two distinct $x, x' \in \mathbb{Z}_p^*$ with a common Jacobi signature. However, if we consider signatures of length $\ell = (2+\varepsilon)\lceil \log p \rceil$ for any constant $\varepsilon > 0$ then, again heuristically, the probability that there exist $x \neq x'$ with the same Jacobi signature is at most $p^2/p^{2+\varepsilon} = 1/p^\varepsilon = \mathrm{negl}(\lambda)$.

The second modification is also necessary, since the conclusion of the assumption does not hold for all primes p. That is, there are infinitely many primes p for which there exist pairs $x, x' \in \mathbb{Z}_p^*$ whose Legendre signatures of length $\lceil 100 \log p \rceil$ are identical. This follows from the fact that there are infinitely many primes p for which the least quadratic non-residue is $\Omega(\log p \log\log\log p)$ [12]. For such primes p, the Legendre signatures of the elements "1" and "2" will be identical, whenever that the signature length is $O(\log p)$.

It is not at all obvious to us that Assumption 4.1 is true. That said, prior work has used similar assumptions in the cryptanalysis of the Legendre-signature-based cryptosystems [5,15,10] (see also Remark 4.1).

Collision resistant hash function from Jacobi signatures. We now give the main result of this section. Let $k \in (2,3)$ be the constant from Assumption 4.1. On security parameter λ, let

$$\mathcal{J}_\lambda^{\mathsf{CRHF}} := \{ J_{N,k\lambda} \mid p, q \xleftarrow{\mathrm{R}} \mathsf{Primes}_\lambda;\ N \leftarrow p^2 \cdot q \}$$

be the family of Jacobi-signature functions defined on number of the form $N = p^2q$. Notice that on modulus N, the signature length is $k\lambda = \lceil \frac{k}{3} \log N \rceil$. For this signature length, the Jacobi-signature function is compressing.

Proposition 4.2 (Collision Resistance of Jacobi Signatures). *Under Assumption 4.1, for every efficient algorithm $\mathcal{A}$, there is an algorithm $\mathcal{B}$ such that*

$$\mathsf{CRHFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{CRHF}}](\lambda) \leq \mathsf{FactAdv}_{p^2q}[\mathcal{B}](\lambda) + \mathrm{negl}(\lambda).$$

Proof. Suppose there exists an efficient adversary $\mathcal{A}$ that breaks collision resistance of $\mathcal{J}^{\mathsf{CRHF}}$ with advantage $\varepsilon = \mathsf{CRHFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{CRHF}}](\lambda)$. We use Algorithm $\mathcal{A}$ to construct Algorithm $\mathcal{B}$ of the claim. Algorithm $\mathcal{B}$, on input $N = p^2q$, runs the collision finder $(x, x') \leftarrow \mathcal{A}(J_{N,\ell})$ where $\ell = k\lambda$, and outputs $\gcd(N, x - x')$. We analyze Algorithm $\mathcal{B}$'s advantage:

- Whenever Algorithm $\mathcal{A}$ outputs a valid collision in $J_{N,\ell}$, we have $J_{N,\ell}(x) = J_{N,\ell}(x')$ and $x \neq x' \bmod N$.
- Since N is of the form p^2q, by Fact 2.2, a collision in the Jacobi signature modulo N implies a collision in the Legendre signature modulo q: $J_{q,\ell}(x) = J_{q,\ell}(x')$.

– By Assumption 4.1, if $J_{q,\ell}(x) = J_{q,\ell}(x')$, then

$$x = x' \bmod q \quad \Longrightarrow \quad (x - x') = 0 \bmod q,$$

except with probability negligible in λ.
– However, since $x \neq x' \bmod N$, it must be that

$$x \neq x' \bmod p^2 \quad \Longrightarrow \quad (x - x') \neq 0 \bmod p^2.$$

Therefore $(x - x')$ is a multiple of q and not a multiple of p^2. This means $\gcd(x - x', N) \in \{q, pq\}$, and Algorithm $\mathcal{B}$ obtains a factor of N with advantage

$$\mathsf{FactAdv}_{p^2q}[\mathcal{B}](\lambda) \geq \varepsilon - \mathrm{negl}(\lambda) = \mathsf{CRHFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{CRHF}}] - \mathrm{negl}(\lambda). \qquad \square$$

Remark 4.1 (Assumption 4.1 with $k \geq 3$). Assumption 4.1 above requires the constant k to be strictly smaller than 3. If we consider the hardness of factoring $N = p^2q$ when the primes p and q have *different* bit-lengths, then our results follow from a weaker version of Assumption 4.1 that takes $k \geq 3$. To illustrate this, suppose it is hard to factor $N = p^2q$ where $p \xleftarrow{R} \mathsf{Primes}_{\lambda+1}$ and $q \xleftarrow{R} \mathsf{Primes}_{\lambda}$ (i.e., p is a $(\lambda+1)$-bit prime and q is a λ-bit prime). Then, for $k = 3$, the Jacobi-signature function $J_{N,k\lambda}$ maps a $(3\lambda + 2)$-bit input to a $k\lambda = 3\lambda$-bit output. This is a compressing function, and moreover, by an analogous proof as that for Proposition 4.2, the Jacobi-signature functions $J_{N,k\lambda}$ is collision-resistant assuming Assumption 4.1 holds for $k = 3$.

Assumption 4.1 with $k = 3$ coincides with the conjecture made by Frixons and Schrottenloher [10, Heuristic 1] for the cryptanalysis of the Legendre pseudorandom function.

5 Factoring Breaks the Jacobi Pseudorandom Function

In this section, we attack the Jacobi pseudorandom function [5], a natural generalization of the Legendre pseudorandom function [13] proposed by Grassi et al. On a public modulus N, secret key $k \in \mathbb{Z}_N$, and input $x \in \mathbb{Z}_N$, the Jacobi pseudorandom function outputs the Jacobi symbol of $(k + x)$ modulo N.

We show that breaking the pseudorandomness of the Jacobi pseudorandom function is no harder than factoring the modulus N. This gives the first subexponential-time distinguisher on the Jacobi pseudorandom function, and gives a quantum-polynomial-time distinguisher as well [20].

Definition 5.1 (Jacobi Pseudorandom Function). The *Jacobi pseudorandom function* is the function ensemble $\mathcal{J}^{\mathsf{PRF}} := \{\mathcal{J}^{\mathsf{PRF}}_\lambda\}_{\lambda \in \mathbb{N}}$, where for each $\lambda \in \mathbb{N}$, we define

$$\mathcal{J}^{\mathsf{PRF}}_\lambda := \left\{ J_N(k, x) := \left(\frac{k + x}{N}\right) \;\middle|\; \begin{array}{c} p, q \xleftarrow{R} \mathsf{Primes}_\lambda \\ N \leftarrow pq \end{array} \right\},$$

where the key space and input space of J_N are $\mathcal{K}_{J_N} = \mathcal{X}_{J_N} = \mathbb{Z}_N$, and the output space is $\{-1, 1\}$.

Proposition 5.2 (Using Factoring to Break the Jacobi PRF). *For every efficient algorithm $\mathcal{A}$, there exists an efficient algorithm $\mathcal{B}$ such that for all $\lambda \in \mathbb{N}$,*

$$\mathsf{PRFAdv}[\mathcal{B}, \mathcal{J}^{\mathsf{PRF}}](\lambda) \geq \frac{1}{2} \cdot \mathsf{FactAdv}[\mathcal{A}](\lambda).$$

Proof. Given a factoring algorithm $\mathcal{A}$, we construct the algorithm $\mathcal{B}$ as follows:

Algorithm $\mathcal{B}^{f(\cdot)}(J_N)$:
- Invoke $\mathcal{A}(N)$ to obtain a factorization of N. If factorization fails, then $\mathcal{B}$ aborts with output $\perp$.
- Using the prime factors $N = pq$, compute the four distinct square roots of $1 \in \mathbb{Z}_N^*$. (Since the square roots of 1 modulo both p and q are $\{-1, 1\}$, we can deterministically compute the four square roots of 1 modulo $N = pq$ using the Chinese Remainder Theorem.) Call these roots $(r, -r, s, -s)$.
- Query the oracle f four times, once on each value in $\{r, -r, s, -s\}$.
- Output "1" if $f(r) \cdot f(-r) = f(s) \cdot f(-s) \in \mathbb{Z}_N^*$. Output "0" otherwise.

With probability $\mathsf{FactAdv}[\mathcal{A}](\lambda)$, algorithm $\mathcal{A}$ outputs a factorization of N. We now compute the advantage when this happens:

- When f is pseudorandom—i.e., $f(x) := J_N(k, x)$ for some modulus N and key $k \in \mathbb{Z}_N^*$, we have by the multiplicativity of the Jacobi symbol,

$$f(s) \cdot f(-s) = \left(\frac{k+s}{N}\right)\left(\frac{k-s}{N}\right) = \left(\frac{k^2 - s^2}{N}\right) = \left(\frac{k^2 - 1}{N}\right),$$

  since $r^2 = s^2 = 1 \bmod N$. By the same argument, we have $f(r) \cdot f(-r) = (\frac{k^2-1}{N})$. In this experiment, the adversary always outputs 1.
- When f is a uniformly random function, then $f(s)$, $f(-s)$, $f(r)$, and $f(-r)$ are each independently and uniformly distributed over $\{-1, 1\}$. Thus, the probability that $f(s)f(-s) = f(r)f(-r)$ is exactly $1/2$.

Thus, whenever algorithm $\mathcal{B}$ successfully factors N, algorithm $\mathcal{B}$ achieves distinguishing advantage $1/2$. We conclude that

$$\mathsf{PRFAdv}[\mathcal{B}, \mathcal{J}^{\mathsf{PRF}}](\lambda) \geq \frac{1}{2} \cdot \mathsf{FactAdv}[\mathcal{A}](\lambda). \qquad \square$$

6 Open Problems

We have given a new connection between the hardness of inverting Jacobi signatures and factoring. One potential next step is whether it is possible to remove our results' reliance on number-theoretic conjectures, or to show hardness under the sole assumption that factoring integers of the form $N = pq$, for primes p and q, is intractable. Finally, it remains to show that is it hard to invert Legendre signatures, under a more well-studied number-theoretic conjecture.

Acknowledgements. We thank Dan Boneh for his comments on a draft of this work, particularly on the formulation of Assumption 4.1. We are grateful to Mark Zhandry for pointing out a bug in an earlier version of this work. We thank the Crypto 2024 reviewers for their extensive feedback. This work was funded in part by NSF and gifts from Capital One, Facebook, Google, Microsoft, Mozilla, NASDAQ, Seagate, and MIT's FinTech@CSAIL Initiative.

References

1. Leonard M. Adleman and Kevin S. McCurley. Open problems in number theoretic complexity, II. In *Algorithmic Number Theory*, 1994.
2. Nesmith Cornett Ankeny. The least quadratic non residue. *Annals of mathematics*, 1952.
3. Eric Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191), 1990.
4. Marshall Ball, Justin Holmgren, Yuval Ishai, Tianren Liu, and Tal Malkin. On the complexity of decomposable randomized encodings, or: How friendly can a garbling-friendly PRF be? In *ITCS*, 2020.
5. Ward Beullens, Tim Beyne, Aleksei Udovenko, and Giuseppe Vitto. Cryptanalysis of the Legendre PRF and generalizations. *IACR Transactions on Symmetric Cryptology*, 2020.
6. Jonathan W Bober and Leo Goldmakher. Pólya–Vinogradov and the least quadratic nonresidue. *Mathematische Annalen*, 366, 2016.
7. Dan Boneh and Richard J. Lipton. Algorithms for black-box fields and their application to cryptography (extended abstract). In *CRYPTO*, 1996.
8. Ivan Damgård. On the randomness of Legendre and Jacobi sequences. In *CRYPTO*, 1988.
9. Dankard Feist. Legendre pseudo-random function, 2019. `https://legendreprf.org/`.
10. Paul Frixons and André Schrottenloher. Quantum security of the Legendre PRF. *IACR Cryptol. ePrint Arch.*, 2021.
11. Atsushi Fujioka, Tatsuaki Okamoto, and Shoji Miyaguchi. ESIGN: An efficient digital signature implementation for smart cards. In *EUROCRYPT*, 1991.
12. Sidney West Graham and CJ Ringrose. Lower bounds for least quadratic nonresidues. In *Analytic Number Theory*, 1990.
13. Lorenzo Grassi, Christian Rechberger, Dragos Rotaru, Peter Scholl, and Nigel P. Smart. MPC-friendly symmetric key primitives. In *ACM CCS*, 2016.
14. Novak Kalujerović, Thorsten Kleinjung, and Dušan Kostić. Cryptanalysis of the generalised Legendre pseudorandom function. In *Algorithmic Number Theory Symposium*, 2020.
15. Dmitry Khovratovich. Key recovery attacks on the legendre prfs within the birthday bound. *IACR Cryptol. ePrint Arch.*, 2019.
16. Youness Lamzouri, Xiannan Li, and Kannan Soundararajan. Conditional bounds for the least quadratic non-residue and related problems. *Math. Comput.*, 84(295), 2015.
17. Tatsuaki Okamoto and Shigenori Uchiyama. A new public-key cryptosystem as secure as factoring. In *EUROCRYPT*, 1998.
18. René Peralta and Eiji Okamoto. Faster factoring of integers of a special form. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 79(4), 1996.

19. István András Seres, Máté Horváth, and Péter Burcsi. The Legendre pseudorandom function as a multivariate quadratic cryptosystem: security and applications. *Applicable Algebra in Engineering, Communication and Computing*, 2023.
20. Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5), 1997.