The One-Wayness of Jacobi Signatures

Henry Corrigan-Gibbs
MIT

David J. Wu
UT Austin

Abstract. In this short note, 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.

1 Introduction

In 1988, Damgård [5] 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 [4], 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. In this short note, 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 $\log^2(p)$.

Under a much stronger (and less plausible) number-theoretic assumption, we can 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 [4], 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.

Related work. Peralta and Okamoto [12] 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 moduli of the form p^2q [7,11].

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. Adleman and McCurley's problem becomes easy if we ask only for some prime q (and not the smallest) that matches the given Legendre pattern.

Grassi et al. [9] 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 [2,6,9]. Several recent works have also studied the concrete hardness of the Legendre pseudorandom function [3,10].

2 Preliminaries

Throughout this work, we write $\lambda \in \mathbb{N}$ to denote a security parameter. 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 $N = p^2q$). *For odd primes p, q and $N = p^2q$, 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 $\{-1, 1\}$:

$$\left(\frac{x}{N}\right) = \left(\frac{x}{p}\right)^2 \left(\frac{x}{q}\right) = \left(\frac{x}{q}\right). \qquad \square$$

2.2 Standard Cryptographic Definitions

We recall a few standard cryptographic definitons.

Definition 2.3 (One-Way Function). For a family of functions $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$, 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:

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

Definition 2.4 (Collision Resistance). For a family of functions $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$, 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:

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

Definition 2.5 (Factoring $N = p^2q$). We define the advantage of an algorithm $\mathcal{A}$ at factoring integers of the form p^2q, for primes p and q, as

$$\mathsf{FactAdv}[\mathcal{A}](\lambda) := \Pr\left[1 < \gcd(t, N) < N : \begin{array}{c} p, q \xleftarrow{\text{R}} \mathsf{Primes}_\lambda. \\ t \leftarrow \mathcal{A}(p^2q) \end{array}\right]$$

3 One-Wayness of Jacobi Signatures

Our first result relies on a conjecture of Boneh and Lipton [4], which states that, for a fixed 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 [4]). *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 $c > 2$.

Under Conjecture 3.1, we can 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

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

We then have:

Proposition 3.2 (One-Wayness of Jacobi Signatures). *Under Conjecture 3.1, for every efficient algorithm $\mathcal{A}$ that breaks the one-wayness of $\mathcal{J}^{\mathsf{OWF}} = \{\mathcal{J}_\lambda^{\mathsf{OWF}}\}_{\lambda\in\mathbb{N}}$ with advantage $\mathsf{OWFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{OWF}}](\lambda)$, there is an efficient algorithm $\mathcal{B}$ for factoring integers of the form p^2q, for primes p and q, with advantage $\mathsf{FactAdv}[\mathcal{B}](\lambda)$ where*

$$\mathsf{OWFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{OWF}}](\lambda) \le \mathsf{FactAdv}[\mathcal{B}](\lambda) + \mathrm{negl}(\lambda).$$

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 $x \xleftarrow{\mathrm{R}} \mathbb{Z}_N$ 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 challenger samples $N = p^2q$, 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, this means $x = x' \bmod q$.
- 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

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

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. *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. More formally, we assume that for $\ell = \lceil k \log p \rceil$, there exists a negligible function* 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 $N = p^2 q$, this requires $k < 3$. For our argument to go through, we must argue about relatively *short* Legendre signatures. We consider values $k > 2$ 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 $\varepsilon > 0$ and again heuristically modeling the Jacobi signatures as uniform random strings, then 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 $\Omega(\log p \log \log \log p)$ [8]. For such primes p, the Legendre signatures of the elements “1” and “2” will be identical, provided that the signature length is $O(\log p)$.

It is not at all obvious to us that Assumption 4.1 is true. That said, assumptions used in the cryptanalysis of the Legendre-signature-based cryptosystems [3] imply Assumption 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.

Claim 4.2 (Collision Resistance of Jacobi Signatures). *Under Assumption 4.1, for every efficient algorithm $\mathcal{A}$ that breaks the collision-resistance of the family of Jacobi-signature functions $\mathcal{J}^{\mathsf{CRHF}} = \{\mathcal{J}_\lambda^{\mathsf{CRHF}}\}_{\lambda \in \mathbb{N}}$ with advantage $\mathsf{CRHFAdv}[\mathcal{A}, \mathcal{J}^{\mathsf{CRHF}}](\lambda)$, there is an algorithm $\mathcal{B}$ for factoring integers of the form p^2q, for primes p and q, that achieves advantage $\mathsf{FactAdv}[\mathcal{B}](\lambda)$ where*

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

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

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

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

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

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

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

5 Open Problems

This note shows a new connection between the hardness of inverting Jacobi sequences and factoring. One potential next step would be to show that *distinguishing* a Jacobi sequence from random is as hard as a more traditional number-theoretic problem (e.g., quadratic residuosity). Another question is whether it is possible to remove our results' reliance on number-theoretic conjectures, or to show hardness under the assumption that factoring integers of the form $p \cdot q$, for primes p and q, is intractable.

Acknowledgements

We thank Dan Boneh for his comments on a draft of this work, particularly on the formulation of Assumption 4.1. 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. In *Discrete Algorithms and Complexity*. 1987.

[2] 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.

[3] Ward Beullens, Tim Beyne, Aleksei Udovenko, and Giuseppe Vitto. Cryptanalysis of the Legendre PRF and generalizations. *IACR Transactions on Symmetric Cryptology*, 2020.

[4] Dan Boneh and Richard J. Lipton. Algorithms for black-box fields and their application to cryptography (extended abstract). In *CRYPTO*, 1996.

[5] Ivan Damgård. On the randomness of Legendre and Jacobi sequences. In *CRYPTO*, 1988.

[6] Dankard Feist. Legendre pseudo-random function, 2019. `https://legendreprf.org/`.

[7] Atsushi Fujioka, Tatsuaki Okamoto, and Shoji Miyaguchi. Esign: An efficient digital signature implementation for smart cards. In *EUROCRYPT*, 1991.

[8] Sidney West Graham and CJ Ringrose. Lower bounds for least quadratic non-residues. In *Analytic Number Theory*, 1990.

[9] Lorenzo Grassi, Christian Rechberger, Dragos Rotaru, Peter Scholl, and Nigel P. Smart. MPC-friendly symmetric key primitives. In *ACM CCS*, 2016.

[10] Novak Kalujerović, Thorsten Kleinjung, and Dušan Kostić. Cryptanalysis of the generalised legendre pseudorandom function. In *Algorithmic Number Theory Symposium*, 2020.

[11] Tatsuaki Okamoto and Shigenori Uchiyama. A new public-key cryptosystem as secure as factoring. In *EUROCRYPT*, 1998.

[12] 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.