The Legendre Pseudorandom Function as a Multivariate Quadratic Cryptosystem: Security and Applications*

István András Seres[1], Máté Horváth[2], and Péter Burcsi[1]

[1]Eötvös Loránd University, Faculty of Informatics, 3in Research Group
[2]Budapest University of Technology and Economics, CrySyS Lab

September 1, 2021

Abstract

Sequences of consecutive Legendre and Jacobi symbols as pseudorandom bit generators were proposed for cryptographic use in 1988. Major interest has been shown towards pseudorandom functions (PRF) recently, based on the Legendre and power residue symbols, due to their efficiency in the multi-party setting. The security of these PRFs is not known to be reducible to standard cryptographic assumptions.

In this work, we show that key-recovery attacks against the Legendre PRF are equivalent to solving a specific family of multivariate quadratic (MQ) equation system over a finite prime field. This new perspective sheds some light on the complexity of key-recovery attacks against the Legendre PRF. We conduct algebraic cryptanalysis on the resulting MQ instance. We show that the currently known techniques and attacks fall short in solving these sparse quadratic equation systems. Furthermore, we build novel cryptographic applications from the Legendre PRF, e.g., verifiable random function and (verifiable) oblivious (programmable) PRFs.

1 Introduction

Zero-knowledge proofs (ZKP) and secure multi-party computation (MPC) protocols are eating the crypto-world. These advanced cryptographic tools are applied and deployed in countless applications, for instance, in privacy-preserving cryptocurrencies, threshold cryptography and secure instant-messaging. The widespread adoption of ZKPs and MPC protocols necessitates novel symmetric-key primitives [GRR+16]. Traditional symmetric-key primitives, like AES or SHA-3, cause significant overhead in ZKPs or MPC due to their immense multiplicative complexity.

Therefore, recently, revived interest has been shown towards algebraic symmetric key primitives with low multiplicative depth [GRR+16]. Lately, several novel algebraic MACs [DKPW12, CMZ14], hash functions [AGR+16, GKR+20] or algebraic pseudorandom functions [Dam88] have been proposed for cryptographic use. New algebraic constructions with low multiplicative complexity are especially attractive due to their distinguished efficiency properties in ZKPs or MPC protocols. However, this new algebraic design paradigm possibly opens up new venues for attacks [AABS+20]. The cryptanalysis of these new symmetric-key primitives is an active research field with notable published works. For instance, Albrecht et al. conducted an algebraic cryptanalysis of MARVELlous [AD18] and MiMC hash functions [ACG+19], while Li and Preneel refined interpolation attacks on low algebraic degree cryptosystems [LP19]. One of the most promising cryptosystems for use in ZKPs and MPC protocols is a pseudorandom function (PRF) that is based on quadratic and power residue symbols. Recall that if p is a prime, the Legendre symbol $\left(\frac{a}{p}\right)$ is 1 if a is a square modulo p and -1 otherwise (the symbol of zero modulo p is 0 by convention). In this work, we focus on the cryptographic security of a PRF family, called the Legendre PRF, and its extensions that are derived from the evaluation of the Legendre symbol.

There exists vast mathematics literature asserting that Legendre and power residue symbols are particularly well suited to be applied in pseudorandom functions since they exhibit high pseudorandomness. One of the first results is due to Pólya and Vinogradov [Vin16]. They assert that character sums behave like independent fair coin tosses, i.e. $\sum_{a=M+1}^{M+N}\left(\frac{a}{p}\right) \leq \sqrt{p}\log p$. In the case of Legendre symbols, Peralta extended

*For any comment on our manuscript, please reach us at istvanseres@caesar.elte.hu, mhorvath@crysys.hu, bupe@inf.elte.hu.

this result by showing that any n-grams of Legendre symbols are asymptotically equally distributed [Per92]. Mauduit and Sárközy introduced several metrics to measure the pseudorandomness of binary sequences and argued that "Legendre symbol sequences are the most natural candidate for pseudorandomness" [MS97]. Ding et al. confirmed the high linear complexity of Legendre symbol sequences [DHS98]. Tóth and Gyarmati et al. introduced new pseudorandomness measures (avalanche effect and cross-correlation) and asserted high values of those in Legendre symbol sequences [Tót07, GMS14].

Related work. In spite of the above results, surprisingly, the security guarantees of the Legendre PRF from a cryptographic standpoint are poorly understood. The quantum case is settled whenever a quantum oracle is available for the attacker as polynomial quantum algorithms are known to recover the key of a Legendre PRF [vDHI06, RS04]. However, if the oracle can only be queried classically, then no efficient quantum algorithm is known. In concurrent and independent work, Frixons and Schrottenloher [FS21] investigated the quantum security of the Legendre PRF without quantum random-access to an oracle. While they presented two new attacks in this setting, both of them remain impractical for key-recovery, strengthening the security intuition. On the other hand, in the classical setting, only exponential key-recovery algorithms are known due to Khovratovich [Kho19], Beullens et al. [BBUV20] and Kaluderovic et al. [KKK20]. One might ask, whether there could be sub-exponential key-recovery attacks on the Legendre PRF. Damgård in 1988 proposed as an open problem to assess the security and complexity of predicting Legendre or Jacobi symbols. He was contemplating on reducing well-known number-theoretic assumptions to the problem of predicting Legendre or Jacobi symbol sequences [Dam88]. This approach in the last decades has been eluding researchers. Thus, in this paper, we show connections of the Legendre and Jacobi sequences to a different branch of cryptography, namely, multivariate quadratic cryptography. This study is useful in establishing the security of various cryptographic applications derived from the Legendre PRF, e.g. the digital signature scheme by Beullens et al. [BdSG20].

Our contributions. In this work, we make the following contributions.

Legendre PRF as an MQ instance. We show that key-recovery attacks against the Legendre PRF are equivalent to solving a specific family of sparse multivariate quadratic equation system over a finite field. Moreover, the weak unpredictability of the PRF is reducible to the decidability of the aforementioned equation system. These connections naturally extend to higher-degree Legendre PRFs and power residue symbol PRFs.

Algebraic cryptanalysis. We conduct the first algebraic cryptanalysis on the MQ instance induced by the Legendre PRF. We find that the Legendre PRF is immune to interpolation, direct (Gröbner basis) and rank attacks. We also present algebraic geometric arguments to support the complexity of finding solutions in these sparse MQ instances over a finite field. However, all these standard cryptanalytic tools from multivariate cryptography do not improve the state of the art key recovery attacks against the Legendre PRF [Kho19, BBUV20, KKK20]. On the other hand, we find that the induced MQ instances behave like random MQ instances in terms of degree of regularity, i.e., the corresponding ideals are semi-regular. This observation might be interpreted as an evidence of the difficulty of breaking the Legendre PRF.

Novel cryptographic applications of the Legendre PRF. Besides assessing the security of the Legendre PRF, we utilise its special properties to apply it in various cryptographic tasks. Expressing the Legendre PRF as an MQ instance facilitates novel cryptographic applications, i.e. verifiable random functions. Furthermore, we exploit its multiplicativity to construct efficient (verifiable) oblivious (programmable) pseudorandom functions. Thanks to their efficiency, these novel extensions can be applied in several cryptographic protocols, such as state-of-the-art private set intersection (PSI) protocols.

Organisation. The rest of this paper is organised as follows. In Section 2, we provide the necessary background on Legendre symbols and related hard cryptographic problems. In Section 3, we show that key-recovery attacks against the Legendre PRF are equivalent to solving a specific MQ instance. In Section 4, we analyze the security of the MQ instance induced by the Legendre PRF. In Section 5, we describe several extensions to the Legendre PRF. Finally, we conclude our paper in Section 6 by pointing out promising future directions.

2 Preliminaries

Notations. Whenever we sample x from set S uniformly at random we write $x \in_R S$. Let p be an odd prime and secret key $K \in_R \mathbb{F}_p$. The modular square root function $\mod p$ is denoted as $\mathsf{sqrt}_p(\cdot)$. Vectors of group elements are denoted in bold. In the following, n, m denote the number of variables and equations, respectively. Throughout this work, we will work in the multivariate polynomial ring $\mathbb{F}_p[x_1, \ldots, x_n]$ over a finite field $\mathbb{F}_p$. $\mathsf{LT}(I)$ denotes the ideal generated by the leading terms of the ideal I. For the ease of exposition we use $[x]$ to denote a secret share of the value $x \in \mathbb{F}_p$.

Background on the Legendre PRF. Damgård proposed using the sequence of consecutive Legendre symbols with respect to a large prime p for "pseudorandom bit generation" [Dam88].

Definition 2.1 (Sequential Legendre PRF) *Let p be a prime, depending on the security parameter λ, then let $\{a\}_K$ denote the following sequence:*

$$\{a\}_K := \left(\frac{K}{p}\right), \left(\frac{K+1}{p}\right), \ldots, \left(\frac{K+a-1}{p}\right).$$

Damgård conjectured that the sequence is pseudorandom, when starting at a secret K. Sometimes, it is easier to work with bits, rather than the original Legendre symbols themselves, therefore the Legendre PRF is defined with Boolean output (for a key- and input-space $\mathbb{F}_p$).

Definition 2.2 (Legendre pseudorandom function) *The function $L_K(x)$ is defined by mapping the corresponding Legendre symbol to the set {0,1}, i.e.*

$$L_K(x) = \left\lfloor \frac{1}{2}\left(1 - \left(\frac{K+x}{p}\right)\right)\right\rfloor.$$

Assumptions. Grassi et al. formulated the following problem that underpins the security of the Legendre PRF [GRR+16].

Definition 2.3 (Shifted Legendre Symbol (SLS) Problem) *Let K be uniformly sampled from $\mathbb{F}_p$, and define $\mathcal{O}_{Leg}$ to be an oracle that takes $x \in \mathbb{F}_p$ and outputs $\left(\frac{K+x}{p}\right)$. Then the Shifted Legendre Symbol (SLS) problem is to find K given oracle access to $\mathcal{O}_{Leg}$ with non-negligible probability.*

It is conjectured that no classical adversary running in sub-exponential time could recover the hidden shift K. One might also consider generalisations of the problem, such as changing the linear polynomial to a secret degree-d polynomial in the Legendre symbol evaluations or changing the quadratic symbol to an rth power residue symbol. For more details, see Appendix A.

Definition 2.4 (Multivariate Quadratic (MQ) problem) *Given m random quadratic polynomials in n variables over a finite field, i.e., $\mathbf{f} = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) \in \mathbb{F}[x_1, \ldots, x_n]^m$, find a common zero $\mathbf{x} \in \mathbb{F}^n$ of the polynomials $f_1, \ldots, f_m$.*

It is well-known that the MQ problem is **NP**-hard for any choice of finite field $\mathbb{F}$ [GJ79]. In cryptographic applications, $\mathbb{F}$ is often $\mathbb{F}_2$ or an extension of it. However, throughout this work, we consider MQ problems over $\mathbb{F}_p$, for some large prime p. The MQ problem is one of the major candidates on which post-quantum secure cryptosystems can be based. Currently, there are no known sub-exponential algorithms to solve the MQ problem.

3 The Legendre PRF as an MQ instance

Hereby, we describe how to express the sequential Legendre PRF, cf. Definition 2.1, as a multivariate quadratic equation system. We remark that in a similar fashion, all the variants (higher-degree) and extensions (power-residue and Jacobi PRF) of the sequential Legendre PRF could be expressed as a suitable MQ instance. Most of our results and observations can be easily ported to those MQ instances as well. Therefore, in this work, we solely focus on the sequential Legendre PRF.

3.1 The Ideal

Let us fix an arbitrary quadratic non-residue $r \in \mathbb{Z}_p^*$. Furthermore, it is assumed that we are given $\{a\}_K$, oft $a \approx \log(p)$. Let $b_i := \left(\frac{K+i}{p}\right)$ and x_i be the corresponding unknown. We think of the unknown x_i as the square root of $K+i$ if $b_i = 1$, otherwise x_i denotes the square root of $r(K+i)$, which is a quadratic residue.

Therefore, for each pair of neighboring Legendre symbols (b_i, b_{i+1}), we define a unique quadratic equation. If $b_i = b_{i+1} = 1$, then we know that $x_{i+1}^2 = K + i + 1$ and $x_i^2 = K + i$, hence

$$x_{i+1}^2 - x_i^2 = 1. \tag{1}$$

If $b_i = b_{i+1} = -1$, then we have that $x_{i+1}^2 = r(K + i + 1)$ and $x_i^2 = r(K + i)$, hence

$$x_{i+1}^2 - x_i^2 = r. \tag{2}$$

Finally if $b_i = 1 = -b_{i+1}$ or $b_i = -1 = -b_{i+1}$ then we obtain the following two quadratic equations:

$$x_{i+1}^2 - r x_i^2 = r, \qquad x_{i+1}^2 - r^{-1} x_i^2 = 1. \tag{3}$$

Altogether, this allows us to efficiently transform any Legendre symbol sequence into an equivalent multivariate quadratic equation system. If we have n Legendre symbols, then we obtain $m = n - 1$ independent equations in n variables, hence the MQ instance is underdefined. Note, that the equation system is rather sparse.

Example 1 *We consider the following example to illustrate the quadratic equation system induced by the Legendre PRF. Let p =* `0xffffffffffffffffffdd` *and K =* `0x27aaa97c746c22e12d10`*. The smallest quadratic non-residue modulo p is 2. We display the MQ instance induced by the evaluation of the sequential Legendre PRF, $\{5\}_K = (1, 1, -1, -1, 1)$. Each consecutive Legendre symbol pairs define an equation. The ideal corresponding to $\{5\}_K$ has the following form:*

$$\langle x_1^2 - x_0^2 - 1, x_2^2 - 2x_1^2 - 2, x_3^2 - x_2^2 - 2, x_4^2 - 2^{-1} x_3^2 - 1 \rangle$$

Let $I := \langle f_1, f_2, \ldots, f_m \rangle$ be the ideal generated by the quadratic polynomials defined by Equations 1, 2 and 3. We are interested in solving simultaneously this equation system, i.e. finding points in the variety $V(I)$. If the sequence of Legendre symbols is long enough, namely $\mathcal{O}(\log p)$, then there are $\mathcal{O}(1)$ solutions in $\mathbb{F}_p$ (only considering solutions where $x_i \in [0, \frac{p-1}{2}]$ for all i) and one of them corresponds to the secret key K of the Legendre PRF. Note that $V(I)$ might contain additional solutions when considered above the algebraic closure $\overline{\mathbb{F}}_p$.

3.2 The Gröbner basis

To better understand the variety $V(I)$, first we describe the Gröbner basis of I. Interestingly, we can easily compute the Gröbner basis of I regardless of the size of p or the length of the Legendre sequence $\{a\}_K$.

Theorem 3.1 *Given a Legendre symbol sequence $\{n\}_K = (b_0, \ldots, b_{n-1})$ and its corresponding ideal $I = \langle f_1, f_2, \ldots, f_m \rangle$, where $m = n - 1$ as defined by the Equations 1, 2 and 3, its Gröbner basis with respect to the (graded) lexicographic ordering, consists of the polynomials g_i, for $i \in [0, n-2]$ such that,*

$$g_i = \begin{cases} x_i^2 - x_{n-1}^2 + (n-i), \textit{if } b_{n-1} = 1 \land b_i = 1 \\ x_i^2 - r x_{n-1}^2 + r(n-i), \textit{if } b_{n-1} = 1 \land b_i = -1 \\ x_i^2 - r^{-1} x_{n-1}^2 + (n-i), \textit{if } b_{n-1} = -1 \land b_i = 1 \\ x_i^2 - x_{n-1}^2 + r(n-i), \textit{if } b_{n-1} = -1 \land b_i = -1 \end{cases} \tag{4}$$

Specifically, $I = \langle g_0, \ldots, g_{n-2} \rangle$ and $G := (g_i)_{i=0}^{n-2}$ is a reduced Gröbner basis.

Proof: With an easy case-distinction one can show that G generates I. For instance, if $b_i = b_j = b_{n-1} = 1$, then $g_i - g_j = f_i$. The other cases are similar. Thus $I \subset \langle G \rangle$.

By the Buchberger-criterion, we only need to verify that for all i, j, it holds that the S-polynomial $S(g_i, g_j)$ divided by the Gröbner basis has no remainder, i.e. $\overline{S(g_i, g_j)}^G = 0$. We let $i < j$ and hereby solely consider the case when $b_i = b_j = b_{n-1} = 1$. The rest of the cases result in a similar calculation. By the definition of the S-polynomials, we have $S(g_i, g_j) = x_j^2 g_i - x_i^2 g_j$. First, we divide $S(g_i, g_j)$ by g_i. We observe that the remainder of the polynomial division is $g_j(x_{n-1}^2 - (n-i))$, which is divisible by g_j. Therefore, indeed $\overline{S(g_i, g_j)}^G = 0$. Hence, the polynomials in G indeed form a Gröbner basis.

G is reduced, since all of its basis polynomials have a leading coefficient one. Moreover, $\langle \mathsf{LT}(g_i) \rangle = \langle \mathsf{LT}(I) \rangle$ and no trailing term of any $g_i \in G$ lies in $\langle \mathsf{LT}(I) \rangle$. ■

Example 2 *The Gröbner basis of the polynomials corresponding to the Legendre symbol sequence* $\{5\}_K$*, from Example 1, consists of the following quadratic bi-variate polynomials:*

$$\langle x_0^2 - x_4^2 + 4, x_1^2 - x_4^2 + 3, x_2^2 - 2x_4^2 + 4, x_3^2 - 2x_4^2 + 2\rangle.$$

We remark that one can view the resulting equation system as a simultaneous Pell-equation system over $\mathbb{F}_p$. Each polynomial in the Gröbner basis is quadratic bi-variate and has $p-1$ solutions in $\mathbb{F}_p$. Put differently, seemingly no elimination ideal turns out to be helpful in finding a common zero.

First, we observe that the polynomials in I lack any special internal structure, i.e. the only relations holding are the trivial ones. More formally, the $m = n-1$ multivariate quadratic polynomials of I in n variables define a *regular ideal*, i.e., $V(I)$ is a 1-dimensional variety, namely, it contains an infinite number of solutions in $\overline{\mathbb{F}}_p$.

Lemma 3.2 *I is a regular ideal.*

Proof: Let $I = \langle f_1, \ldots, f_m\rangle$ be the ideal induced by the Legendre PRF, and we assume that f_i forms a reduced Gröbner basis. For a homogeneous sequence of polynomials $(f_1, \ldots, f_m)$ being regular, we need to show that if for all $i \in [1, m]$ and g such that $gf_i \in \langle f_1, \ldots, f_{i-1}\rangle$, then $g \in \langle f_1, \ldots, f_{i-1}\rangle$. An affine sequence of polynomials $(f_1, \ldots, f_m)$ is regular by definition, if the homogeneous sequence $(f_1^h, \ldots, f_m^h)$ is regular, where f_i^h is the homogeneous part of f_i of highest degree with respect to the (graded) lexicographic monomial ordering. In our case $(f_1^h, f_2^h, \ldots, f_m^h) = (x_1^2, x_2^2, \ldots, x_m^2)$.

Since $f_i^h = x_i^2$, in our case for every i, therefore the ideal $I_{i-1} := \langle f_1^h, \ldots, f_{i-1}^h\rangle$ is a monomial ideal. If $gf_i^h \in I_{i-1}$, then gf_i^h is divisible by a generator of I_{i-1}, since I_{i-1} is a monomial ideal [CLO13]. Since $(f_i, f_j) = 1$, for every $j \in [1, i-1]$, thus it is necessary that g is divisible by some $f_j^h = x_j^2 \in I_{i-1}$, for $j \leq i-1$. Namely $g = x_j^2 g' \in I_{i-1}$, for some polynomial g'. This completes the proof. ∎

3.3 The Field Equations

As we have seen previously the corresponding variety $V(I)$ of the ideal I has dimension 1. However, in the cryptanalysis of the Legendre PRF, we wish to obtain a 0-dimensional variety that contains the secret key K of the PRF. As we will show, this can be achieved by adding the field equations to the ideal I.

A Legendre sequence $\{n\}_K$ can be described with polynomials in $\mathbb{F}_p[x_0, x_1, \ldots, x_n]$. Let us define I_{FE} as follows:

$$I_{\mathsf{FE}} = I \cup \{x_i^p - x_i | i \in [0, n]\}. \tag{5}$$

Example 3 *We illustrate the ideal I_{FE} complemented with the field equations with parameters $p = 191$ and $\{9\}_{45} = (1, 1, -1, 1, 1, 1, 1, 1, -1)$. The smallest quadratic non-residue is $r = 7 \bmod 191$.*

$$\begin{aligned} I_{\mathsf{FE}} = \langle -x_0^2 + x_1^2 - 1, -7x_1^2 + x_2^2 - 7, -x_2^2 + 7x_3^2 - 7, -x_3^2 + x_4^2 - 1, -x_4^2 + x_5^2 - 1, \\ -x_5^2 + x_6^2 - 1, -x_6^2 + x_7^2 - 1, -7x_7^2 + x_8^2 - 7, \\ x_0^{191} - x_0, x_1^{191} - x_1, x_2^{191} - x_2, x_3^{191} - x_3, x_4^{191} - x_4, x_5^{191} - x_5, x_6^{191} - x_6, x_7^{191} - x_7, x_8^{191} - x_8\rangle \end{aligned}$$

The corresponding Gröbner basis has the following form,

$$\langle x_0^2 - 45, x_1^2 - 46, x_2^2 + 53, x_3^2 - 48, x_4^2 - 49, x_5^2 - 50, x_6^2 - 51, x_7^2 - 52, x_8^2 + 11\rangle.$$

Note, how helpful the Gröbner bases are in obtaining the secret key K. In addition, one can also read off all the evaluated points from the Gröbner bases. If the variable x_i corresponds to a residue, then x_i^2 is one of the evaluated points in the PRF. Alternatively, if x_i corresponds to a non-residue, then $r^{-1}x_i^2 \bmod p$ is the evaluated point in the PRF.

Using the intuition of the Example 3, we can show in general the structure of the Gröbner basis of I_{FE}.

Theorem 3.3 *Let $\{n\}_K = (b_0, \ldots, b_{n-1})$ be a Legendre symbol sequence for which there exists a unique key K. We consider its corresponding ideal complemented with the field equations $I_{\mathsf{FE}} = \langle f_1, f_2, \ldots, f_m\rangle$, where $m = 2(n-1)+1$ as defined by Equation 5. Then the Gröbner basis of I_{FE} with respect to the (graded) lexicographic ordering, consists of the polynomials g_i, for $i \in [0, n-1]$ such that,*

$$g_i = \begin{cases} x_i^2 - (K+i), \text{if } b_i = 1 \\ x_i^2 - r(K+i), \text{if } b_i = -1 \end{cases} \tag{6}$$

Moreover, $G := (g_i)_{i=0}^{n-1}$ is a reduced Gröbner basis.

Proof: G generates the ideal I_{FE}, since each f_i can be expressed by using the generators g_i. The generating polynomials of I can be expressed as $r^{L_0(K+i+1)}g_{i+1} - r^{L_0(K+i)}g_i = f_i$. The field polynomials can be also expressed using the generators of G. Specifically, let us denote the modular square roots of $r^{L_0(K+i)}(K+i)$ as b and c. Then, $x_i^p - x_i = g_i \Pi_{a \neq b,c}(x-a)$. Hence, $I_{\mathsf{FE}} \subset \langle G \rangle$. By the uniqueness of K, we also have that that $\langle G \rangle \subset I_{\mathsf{FE}}$, since the corresponding varieties are equal above the algebraic closure.

Next, we verify that the Buchberger-criterion holds for the polynomials in G. In this case, $S(g_i, g_j) = x_j^2 g_i - x_i^2 g_j$. Depending on the residuosity of b_i, b_j we have four cases, but for the sake of simplicity we only consider here the case of $b_i = b_j = 1$. The other cases follow similarly. The S-polynomial is divisible by G, since $S(g_i, g_j) = x_j^2(x_i^2 - (K+i)) - x_i^2(x_j^2 - (K+j)) = -(K+i)x_j^2 + (K+j)x_i^2 = (K+j)g_i - (K+i)g_j$, that is clearly divisible by the polynomials of G.

G is clearly a reduced Gröbner basis as each leading coefficient is one and no monomial of g_i lies in $\langle \mathsf{LT}(G \setminus g_i) \rangle$.
■

In Section 4.2, we evaluate empirically the time complexity of computing the Gröbner basis of MQ instances (the I_{FE} ideal) induced by Legendre PRF sequences. The ideal I_{FE} cannot be regular as it contains more polynomials than variables. However, the Gröbner basis of I_{FE} allows us to observe easily that in I_{FE} there are no internal dependencies between the ideal's generating polynomials. More precisely, the following holds.

Lemma 3.4 *I_{FE} is a semi-regular ideal, whenever the conditions of Theorem 3.3 are satisfied.*

We are very much interested in showing that I_{FE} is a semi-regular ideal since the asymptotic behavior of *the degree of regularity* of semi-regular ideals is well understood [BFSY05]. The degree of regularity d_{reg} of an ideal is a measure the assess the theoretical complexity of computing the Gröbner basis of an ideal. For a precise definition, the reader is referred to [CLO13]. **Proof:** The proof's blueprint is the same as that of Lemma 3.2.

We consider the generating set for I_{FE} provided by the Gröbner basis, i.e., $I_{\mathsf{FE}} = (f_1, \ldots, f_m)$. By definition, a homogeneous sequence of polynomials $(f_1, \ldots, f_m)$ is semi-regular if for all $i = 1, \ldots, m$ and g such that $gf_i \in \langle f_1, \ldots, f_{i-1} \rangle \wedge deg(gf_i) < d_{reg}$ then g is also in $\langle f_1, \ldots, f_{i-1} \rangle$. An affine sequence of polynomials $(f_1, \ldots, f_m)$ is semi-regular if the sequence $(f_1^h, \ldots, f_m^h)$ is semi-regular, where f_i^h is the homogeneous part of f_i of highest degree. In our case $(f_1^h, \ldots, f_m^h)) = (x_1^2, \ldots, x_m^2)$. Previously in the proof of Lemma 3.2, we saw why $(x_1^2, \ldots, x_m^2)$ forms a regular ideal. ■

Finally, we show the usefulness of I_{FE} in connection with the Legendre PRF.

Lemma 3.5 *A successful Legendre key-recovery attack is equivalent in polynomial time to solving the MQ system defined by the ideal I_{FE}. On the other hand, the weak unpredictability of the Legendre PRF is equivalent to the decidability of the induced MQ instance over the finite prime field.*

Proof: Let us define the variety V and ideal I defined by the Legendre PRF evaluation $\{n\}_K$. More precisely, we fix a quadratic non-residue $r \in \mathbb{Z}_p$. In polynomial-time, we can construct the variety $V^* = \{(x_0, x_1, \ldots, x_n) | x_i = \pm \mathsf{sqrt}_p(r^{L_K(i)}(K+i)), i \in [0, n-1]\}$. The corresponding ideal is denoted as I^*. Our goal is to show that $V^* = V(I_{\mathsf{FE}})$.

First, $V^* \subset V(I_{\mathsf{FE}})$, because this is how the polynomials in I_{FE} are constructed, such that all the points in V^* vanish on the polynomials of I_{FE}. The other inclusion is again trivial by the construction of the polynomials of I_{FE}. I_{FE} is a radical ideal, since every ideal that contains its field equations is a radical ideal [Ull12, Lemma 2.2.3.]. Therefore, I_{FE} is the smallest ideal that vanishes on V^*.

As for the unpredictability of the Legendre PRF, if the equation system corresponding to a purported Legendre PRF evaluation is not solvable, then one can be sure that the psuedo-random sequence is not obtained by evaluating the Legendre PRF. ■

We highlight again the extreme sparsity of the induced MQ instance. This is in contrast with most MQ public-key cryptosystems, where the MQ instance is generated uniformly at random by the signer or encryptor. Typically, a random MQ instance has many non-zero coefficients resulting in large public keys. Contrarily, in the case of the Legendre PRF, the MQ instances exhibit a very specific structure (cf. Example 1, 3) stemming from the multiplicative group of the field $\mathbb{F}_p$. Interestingly, if a single coefficient in the Legendre MQ instance became 0, then the whole equation system suddenly would be trivially solvable by "back-substitution". The Legendre MQ instance seems to be the smallest possible, yet still secure MQ instance.

In Section 4, we turn our attention to assessing the security of the MQ instance induced by the Legendre PRF outputs. In particular, we want to assess the complexity of solving the particular equation systems. According to [HLY12], in order to prove the security of a multivariate PRF, it suffices to show that the family of MQ instances $\mathbf{f}$ induced by the PRF is hard to solve. This is because then the distributions

$D_1 = (\mathbf{f}, \mathbf{f}(x_0, x_1, \ldots, x_{n-1}))$ and $D_2 = (\mathbf{f}, U_m)$ are computationally indistinguishable, where U_m is a uniform distribution over $\mathbb{F}_p^m$ [HLY12].

3.4 Adding More Polynomials to the Ideal

As we have seen in Section 3.3, the Legendre key-recovery attack is equivalent to solving an overtedermined MQ instance. However, when $p \equiv 3 \mod 4$ or $p \equiv 5 \mod 8$, we might decrease the complexity of solving the resulting MQ instance by adding new equations. Observe that in these cases, we can express the modular square root function $\mathsf{sqrt}_p : \mathbb{F}_p^* \to \mathbb{F}_p^*$ as a polynomial function:

$$\mathsf{sqrt}_p(x) : y = \begin{cases} \pm x^{\frac{p+1}{4}} \mod p, \text{ if } p \equiv 3 \mod 4 \\ \pm x(2x)^{\frac{p-5}{8}}(4x^{\frac{p-1}{4}} - 1) \mod p, \text{ if } p \equiv 5 \mod 8. \end{cases} \tag{7}$$

If $p \equiv 1 \mod 8$, it is not possible to express easily the $\mathsf{sqrt}_p(\cdot)$ function as a polynomial function, since in that case the root-finding Tonelli-Shank algorithm is a probabilistic algorithm. Nevertheless, we can obtain $\mathcal{O}(\log^2 p)$ new polynomials in the other cases, one for each quadratic term $x_i x_j$:

$$x_i x_j = \mathsf{sqrt}_p(x_i^2 x_j^2). \tag{8}$$

Similarly, we can add new polynomials to the system involving the linear terms of the unknowns for every $i \neq j$,

$$x_i = \mathsf{sqrt}_p(r^{L_0(x_i) - L_0(x_j)}(x_j^2 - r^{L_0(x_j)}(j - i))). \tag{9}$$

Observe, that all polynomials in Equations 8 and 9 have almost full degree, i.e. they have degree $\approx p$. Therefore, the addition of each of those polynomials incur the inclusion of $\approx \log p$ new quadratic equations in $\approx \log p$ new variables in order to break down the almost full degree polynomials to quadratic polynomials. All in all, we end up with an equation system in n variables and $m = n + k$ equations, where $m, n \in \mathcal{O}(\log^3 p)$ and $k \approx \log^2 p$. We leave it as an interesting future work to analyze the independence of the newly introduced polynomials of Equation 8 and 9 from the polynomials of the ideal I_{FE}. We suspect that adding these high-degree polynomials to the ideal will not significantly speed up the Gröbner basis computation. Hence, these new polynomials might not have cryptanalytic relevance.

4 Security of the Legendre PRF as MQ instances

In this section, we evaluate the complexity of a key recovery attack on the Legendre PRF as an MQ instance. We find that direct attacks, solvers and other traditional algebraic attacks (interpolation attacks, MinRank etc.) do not improve on the state-of-the-art classical attack due to Kaluderovic et al [KKK20].

4.1 Interpolation Attacks

Interpolation attacks aim to interpolate a cryptosystem's polynomial without knowing its secret key [JK97]. In a single party setting, the Legendre PRF is typically evaluated more than once for a particular key K, i.e. $\{a\}_K$ is used as a pseudo-random bit-string, where $a > 0$. In these cases, the resulting bit-string is mapped to integers, for instance, in the following way,

$$F_K(a) = \sum_{i=0}^{a-1} 2^{a-1-i}(K + i)^{\frac{p-1}{2}} \mod p \tag{10}$$

Note that $deg(F_K(a)) = \frac{p-1}{2}$, i.e. the degree of the polynomial representing the Legendre PRF has almost full degree over $\mathbb{F}_p$, that is exponential in the security parameter. The polynomial is dense (all possible monomials appear) and no coefficient is dependent on the key K. These properties make interpolation attacks infeasible as they would require at least $\frac{p-1}{2} + 1$ pairs of keys and pseudo-random field elements to interpolate $F_K(a)$.

4.2 Direct Algebraic Attacks

Direct algebraic attacks, such as Gröbner basis [Buc65], F_5 [Fau02], XL [CKPS00] aim to directly solve the cryptosystem's underlying MQ instance. The computational complexity of these attacks is equivalent to that of computing the Gröbner basis [SKI04], which in turn depends on the *degree of regularity* of the MQ instance at hand. Therefore, it is of great interest to compute the degree of regularity of an MQ cryptosystem. However, in many cases, this is not possible without actually calculating the Gröbner basis itself. For m

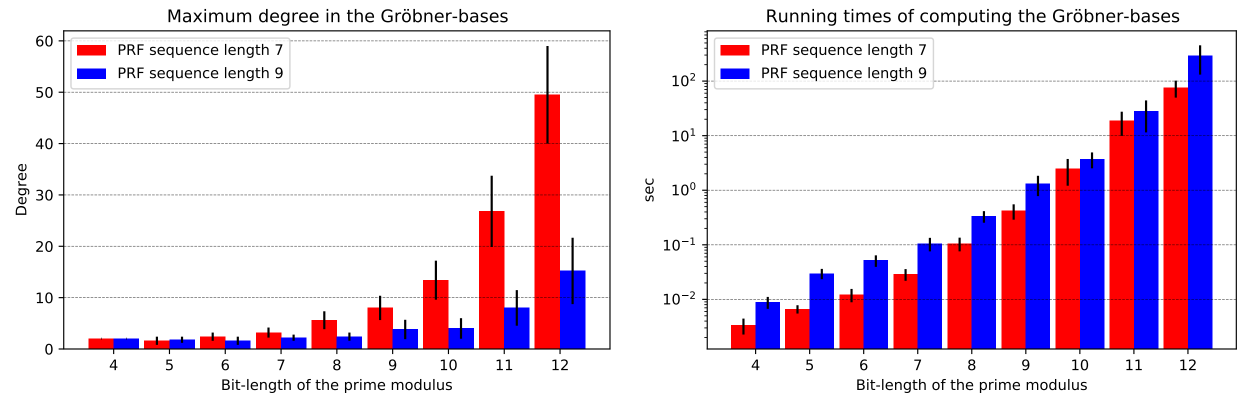

Figure 1: The maximum degree in the Gröbner basis (left) and the exponential time complexity of computing the Gröbner bases (right) for the ideals I_{FE} defined by the Legendre PRF.

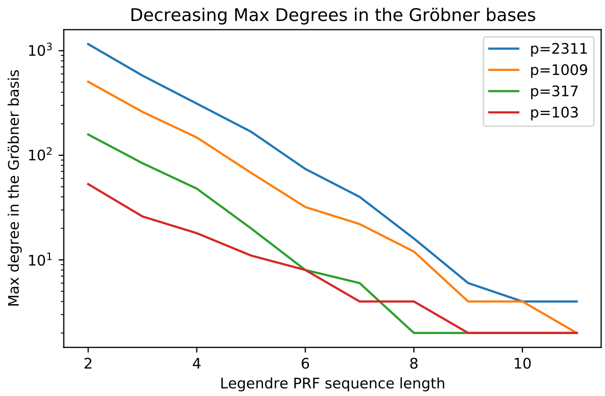

Figure 2: The maximum degrees in the Gröbner basis of the ideal I_{FE} as a function of the Legendre PRF sequence length.

equations of degree at most d in n variables, the arithmetic complexity of Gröbner basis computation are $2^{2^{\mathcal{O}(n)}}$ in general and $\mathcal{O}\left(m \cdot \binom{n+d_{reg}-1}{n}^{\omega}\right)$ in case of 0-dimensional regular systems, where $2 \leq \omega \leq 3$ is the linear algebra constant of matrix multiplication.

We empirically evaluated the performance of computing the Gröbner basis for the ideal I_{FE} induced by the Legendre PRF evaluations, see Figure 1. We sampled random small primes with a given bit-length and evaluated the Legendre PRF for a sequence of length seven and nine. We computed and recorded the time it takes to compute the Gröbner basis of the corresponding ideal I_{FE}. We repeated the experiment 10 times. We observe that computing the Gröbner basis takes exponential time in the bit-length of the prime modulus. We also expect that launching key-recovery attacks against the Legendre PRF using Gröbner basis methods is hopeless for cryptographic parameter sets, i.e., for primes larger than $\approx 2^{128}$.

As expected, the longer the analyzed sequence is, the smaller the maximum degrees are in the Gröbner bases, see Figure 2. Eventually, when the length of the PRF sequence reaches $\log(p)$, the maximum degree in the Gröbner basis becomes 2, since there is a unique sequence that solves the MQ system induced by I_{FE}. However, for shorter sequences we observe high maximum degrees in the Gröbner basis, see Figure 1.

4.3 MinRank Attacks

The MinRank attack is a powerful and ubiquitous tool in the cryptanalysis of multivariate cryptography. MinRank attacks broke numerous multivariate cryptosystems, such as the cryptanalysis of HFE due to Kipnis and Shamir [KS99] or the cryptanalysis of SRP encryption system [PPST17]. In the following, we show that the Legendre PRF has high Q-rank, therefore it is immune to MinRank attacks. For the complete calculation the reader is referred to Appendix C.1.

m	1	2	3	4	5	6	7	8	9	10
genus	0	1	1	5	17	49	129	321	769	1793

Figure 3: The genus of the algebraic curves containing the solutions corresponding to a Legendre symbol sequence of length $m+1$.

4.4 Group Structure of the Legendre PRF MQ Instances' Solutions

In Section 3.1, it was shown, that the PRF seed lies in the intersection of multiple Pell-conics. It is well known, that the solutions of a single Pell-equation over a finite field form a cyclic Abelian-group over $\mathbb{F}_p$, cf. [Déc07]. These groups were previously suggested for use in cryptography by Lemmermeyer as it is believed that the discrete logarithm problem is hard in these groups [Lem03]. A single Pell conic has 0 genus. The intersection of two Pell-conics yields a nonsingular elliptic curve with genus 1. Therefore, if one wants to find every secret key K that results in a 3-long specific binary sequence produced by the Legendre PRF, e.g. $(1,-1,1)$, then every satisfying secret key K is a rational point on a sequence-specific elliptic curve. For a concrete example on how to obtain the corresponding curve equation, see Appendix D.1.

However, if one considers longer sequences, then the resulting curve has a genus greater than 1, cf. Figure 3. This implies, that the solutions of those algebraic curves *do not have an Abelian group structure equipped with them.* In the following we compute the genus of the high-degree surfaces induced by the Legendre PRF in the general case.

We want to calculate the genus of the algebraic curve containing the solutions of a Legendre PRF key-recovery attack. More formally, we want to compute $1-P(0)$, where $P(\cdot)$ is the Hilbert-polynomial of the curve defined by the intersection of several Pell conics. Let $(f_1, f_2, \ldots, f_m)$ be the given Pell conics in variables $x_0, x_1, \ldots, x_n$ and I the corresponding ideal generated by them. Note that n denotes the length of the given Legendre sequence. For $N \gg 0$, we have that $P(N)$ is the dimension over $\mathbb{F}_p$ of the degree-N homogenous part of $\mathbb{F}_p[x_0, \ldots, x_n]/I$ [Har13]. This is a linear polynomial. Since for all $i, j, i \neq j$ we have $(f_i, f_j) = 1$, we obtain the following inclusion-exclusion type equation,

$$P_n(N) = g_n(N) - \binom{n-1}{1} g_n(N-2) + \binom{n-1}{2} g_n(N-4) - \binom{n-1}{3} g_n(N-6) + \ldots, \tag{11}$$

where $g_n(N)$ denotes the number of N-degree monomials in $\mathbb{F}_p[x_0, \ldots, x_n]$. Therefore $g_n(N) = \binom{N+n}{n}$. For the sake of concreteness and as a simple example let us consider the case of four intersecting Pell-conics, i.e. Legendre-sequences of length five. We have the following expression for the Hilbert-polynomial, when $n=4$:

$$P_4(N) = \binom{N+4}{4} - 3\binom{N+2}{4} + 3\binom{N}{4} - \binom{N-2}{4}. \tag{12}$$

By substituting $N=0$, we obtain that $P_4(0) = -4$, namely the arithmetic genus is $1 - P_4(0) = 5$.

We can obtain the following closed formula for the Hilbert-polynomial:

Lemma 4.1 $P_n(N) = 2^{(n-1)} \cdot N - (n-3) \cdot 2^{(n-2)}$.

Proof: We first determine the linear coefficient by considering the difference polynomial $Q_n(N) = P_n(N+1) - P_n(N)$, which is a constant by the linearity of P_n.

Using the inclusion-exclusion argument again, we see that $Q_n(N)$ is also a Hilbert-polynomial. To obtain an ideal with $Q_n(N)$ as its Hilbert polynomial, take an $(n-1)$-variable ring and $n-1$ polynomials, each of which is quadratic in a distinct single variable. The ideal generated by these polynomials is zero-dimensional, and therefore has a constant Hilbert polynomial whose value is the size of the corresponding variety, i.e. 2^{n-1}.

For the constant term, first note that for any real value of x, $\binom{x}{n} = (-1)^n \binom{-x+n-1}{n}$. Therefore, by substituting $N = (n-3)/2$ into (11), the terms $g_n(N-2k)\binom{n-1}{k}$ and $g_n(N-2(n-k))\binom{n-1}{n-k}$ cancel, and the middle term (for odd n) is 0, hence $P_n(n-3/2) = 0$, which gives the constant term. ■

5 Extensions of the Legendre PRF

In this section, we construct various extensions of the Legendre PRF and compare them with other state-of-the-art constructions. We build verifiable random functions in Section 5.1 and oblivious pseudorandom functions with several extensions in Section 5.2.

5.1 Verifiable Random Functions from the Legendre PRF

Verifiable random functions (VRFs) are natural extensions of PRFs due to Micali, Rabin and Vadhan [MRV99]. In a VRF, the PRF evaluator can produce a publicly verifiable short proof about the correct evaluation of the PRF $F_K(x)$ given the PRF input x, the output $F_K(x) = y$ and a public key pk, without revealing anything about the secret key K. In many applications, in addition to the efficient production of pseudorandom strings, one also needs to prove the correctness of those pseudorandom objects, e.g. proof-of-stake consensus algorithms [GHM+17].

We start off by observing that one of the main advantages of the Legendre PRF arithmetization as an MQ instance, is that it allows to model the PRF as a low-degree polynomial equation system, namely as a multivariate quadratic equation system. This low-degree arithmetization easily facilitates the construction of efficient Legendre VRFs. By contrast, if one models the Legendre PRF as a high-degree $\frac{p-1}{2}$ univariate polynomial by Euler's criterion, then it hinders applying efficient proof systems for the correct evaluation statement. More formally, the Legendre PRF evaluator wants to prove that the following binary relation $\mathcal{R} : \{0,1\}^* \times \{0,1\}^*$ holds:

$$\mathcal{R}_{PRF} = \left\{ \left(\{n\}_K, K \right) : \{n\}_K = \left(\left(\frac{K}{p}\right), \left(\frac{K+1}{p}\right), \dots, \left(\frac{K+n-1}{p}\right) \right) \right\}, \tag{13}$$

which is equivalent to the relation:

$$\mathcal{R}^*_{PRF} = \left\{ \left(\{n\}_K, \mathbf{x} \right) : (f_1(\mathbf{x}) = 0, f_2(\mathbf{x}) = 0, \dots, f_m(\mathbf{x}) = 0) \right\}, \tag{14}$$

where the multivariate quadratic polynomials $(f_i)_{i=1}^m$ are defined in Section 3.1. Note that, for the relation $\mathcal{R}_{PRF}$, it suffices for the PRF evaluator to prove that she knows the roots of $m = n-1$ quadratic equations.The arithmetic circuit $\mathcal{C}_n$ expressing the relation $\mathcal{R}^*_{PRF} = \{\{n\}_K, \mathbf{x}\}$ can be characterized with the following metrics. The arithmetic circuit $\mathcal{C}_n$ has a constant circuit depth 3 (two layers of multiplication gates and one layer of subtraction (addition) gates), circuit width of $2n$, multiplication complexity of $\approx 1.5n$ (on average, since every $(1,-1)$ or $(-1,1)$ pair induces an extra multiplication gate in comparison with the $(1,1)$ and $(-1,-1)$ Legendre symbol pairs) and witness complexity of $n\lambda$ bits, i.e. n group elements. For an illustrative example, see Figure 4. Observe the low multiplicative complexity of the statement a Legendre PRF evaluator needs to prove in zero-knowledge to obtain a VRF from the Legendre PRF.

To prove in zero-knowledge the computational integrity of the arithmetic circuit evaluation, one might choose from several off-the-shelf zero-knowledge proof systems. Still, as of time of writing, the state-of-the-art zkSNARK proof system is due to Groth [Gro16]. It provides proofs of size 3 group elements and verifier complexity of 3 pairings and n group operations and last but not least significant developer tooling. However, this proof system does not provide post-quantum security and furthermore, it would require a trusted setup, which is undesirable or even unattainable in many applications.

The most important proof system family of zero-knowledge succinct transparent arguments of knowledge was pioneered by the work of Ben-Sasson et al. [BSBHR18]. STARK proof systems, on top of being succinct and zero-knowledge, provide post-quantum security and does not rely on trusted setups. The performance evaluation of [BSBHR18] shows, that the proof of a Legendre PRF statement with 2^{21} multiplication gates, i.e. verifying $\approx 2^{19}$ Legendre symbols, can be generated in less than a second, while can be verified in 100ms.

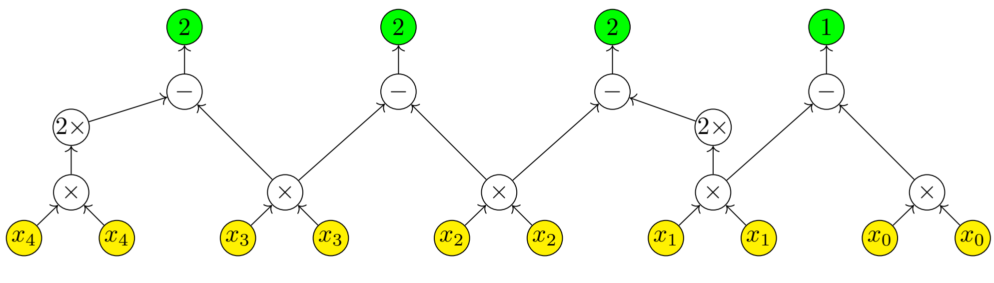

Figure 4: Arithmetic circuit representation of the ZKP statement that proves the relation $\mathcal{R}_{PRF} = \{\{5\}_K = (1,1,-1,-1,1), K\}$ from Example 1 where 2 is the least quadratic non-residue. Applying our arithmetization the PRF evaluator proves that it knows the zeros of the following polynomials $(2x_4^2 - x_3^2 = 2, x_3^2 - x_2^2 = 2, x_2^2 - x_1^2 = 2, x_1^2 - x_0^2 = 1)$. Secret input nodes are colored with yellow, while public output nodes are colored with green. Nodes with $2x$ denote a multiplication gate, where one of the inputs is the constant quadratic non-residue 2. Note, that for any Legendre PRF statement $\mathcal{R}^*_{PRF}$ the arithmetic circuit has a constant multiplicative depth of two.

The proof size is ≈ 100KB. In Table 5.1, we compare the proposed VRF to the state of the art. Note that the Legendre VRF is the most efficient post-quantum VRF in terms of proof size, prover and verifier complexity.

	$\lvert\pi\rvert$	Time complexity		Assumption
		Prove	Verify	
[GNP+15]	$1\mathbb{G}$	$1\mathsf{H}+1\mathbb{G}$	$1\mathsf{H}+1\mathbb{G}$	Factoring
[PWH+17]	$1\mathbb{G}+2\mathbb{F}_p$	$3\mathsf{H}+2\mathbb{G}$	$3\mathsf{H}+4\mathbb{G}$	EC-DDH
[BGLS03]	$1\mathbb{G}$	$2\mathsf{H}+1\mathbb{G}$	$1P$	co-DH
[DY05]	$1\mathbb{G}$	$1\mathbb{G}+1\mathbb{F}_p$	$2\mathbb{G}+2P$	q-DBDHI
[LBM20]	$1\mathbb{G}$	$1\mathbb{G}$	$1P$	q-DDHE
[EKS+20]†	$\mathcal{O}(k+l)$	$\mathcal{O}(kl)$	$\mathcal{O}(kl)$	Module-SIS
§5.1+SNARK	$3\mathbb{G}$	$9n\mathbb{G}$	$n\mathbb{G}+3P$	SLS, KEA
§5.1+STARK	$\mathcal{O}(\log(n))\mathbb{G}$	$\mathcal{O}(n\log(n))\mathbb{G}$	$\mathcal{O}(\log(n))\mathbb{G}$	SLS

Table 5.1: Overview of various VRF constructions. Hashing, group operations, exponentiation and pairings are denoted as $\mathsf{H}, \mathbb{G}, \mathbb{F}_p, P$ respectively. Note that [EKS+20] only provides a few-time VRF. Module-SIS and module-LWE ranks are denoted as k and l, respectively. In case of the Legendre VRF, n is the length of the Legendre symbol sequence being proved. Assumptions written in red are not post-quantum secure, while assumptions in green are post-quantum secure.

5.2 Oblivious PRFs from the Legendre PRF

An oblivious PRF (OPRF) [NR97, FIPR05] is a two-party secure computation protocol (2PC) to evaluate a PRF $F(\cdot,\cdot)$ in an oblivious fashion. Specifically, it allows a sender and a receiver with inputs K and x, respectively, to compute $F(K, x)$ such that the sender does not learn anything new from the protocol messages, while the receiver can output $F(K, x)$ without obtaining information about the used key K. In this section, we show how to build an OPRF relying on the hardness of the SLS problem and also extend this result to two variants of OPRFs, namely to programmable and to verifiable OPRFs (denoted as OPPRF and VOPRF respectively).

These protocols are extensively used in various tasks. A non-exhaustive list of OPRF applications include secure keyword search [FIPR05], private set intersection (PSI) [HL08, JL09, KKRT16, KLS+17], secure deduplicated storage [KBR13], password-protected secret sharing [JKKX16], password-authenticated key exchange [JKX18]. OPPRFs were successfully used to build two-party PSI [PSTY19, KK20], multi-party PSI [KMP+17] and circuit-PSI that enables secure function evaluation on the intersection of sets [CGS22]. Finally, VOPRF is the cornerstone of Privacy Pass, a privacy-preserving lightweight authentication mechanism [DGS+18] and password-protected secret sharing [JKK14]. The importance of (V)OPRF is also indicated by the ongoing effort to standardize them [DFHSW21].

5.2.1 The Legendre OPRF

Motivated by the wide range of applications, our goal is to present a novel pathway to the realization of OPRFs that we formally define in Figure 5a.

Functionality $\mathcal{F}_{\mathrm{OPPRF}}$

Participants: sender $\mathcal{S}$, receiver $\mathcal{R}$.
Parameters: a PRF $F : \mathcal{K}\times\mathcal{X} \to \{0,1\}$ for key-space $\mathcal{K}$ input-space $\mathcal{X}$, the number of programmed points n.
Input: - $\mathcal{S}$: $K \in \mathcal{K}$, $x'_1, \ldots, x'_n \in \mathcal{X}$ and $y'_1, \ldots, y'_n \in \{0,1\}$,
- $\mathcal{R}$: $x \in \mathcal{X}$.
Output: - $\mathcal{S}$ obtains nothing,
- $\mathcal{R}$ obtains $F(K, x)$ that is y'_i if $x = x'_i$ $\forall i \in \{1, \ldots, n\}$.

(a) The ideal OPRF functionality. Together with the extensions in blue, we get the OPPRF ideal functionality.

Functionality $\mathcal{F}_{\mathrm{Prep}}$

RandSquare: Sample $s \in_R \mathbb{F}_p$ and output shares $[s^2]$.
RandSquare′: Sample $0 \neq s \in_R \mathbb{F}_p$ and output shares $[s^2]$.
TripleGen: Sample $a, b \in_R \mathbb{F}_p$ and output shares $[a], [b], [ab]$.

(b) Ideal preprocessing functionality.

Figure 5: Ideal functionalities.

The main observation – that was already used in [GRR+16] for the secure computation of the Legendre PRF in the multi-party setting – is that the key of the PRF can be masked without changing the PRF value by utilizing the multiplicative property of the Legendre symbol. Namely, if we choose a random square and multiply it with some number, the Legendre symbol of the resulting value will be equal to the symbol of the original number. This fact gives rise to the arithmetic sharing-based[1] OPRF protocol $\Pi^{OPRF}_{\text{Legendre}}$, depicted in Figure 6a. The protocol can be divided into online and offline parts. In an offline preprocessing phase the parties can compute the shares of the previously mentioned random square and a so-called Beaver multiplication triple $[a], [b], [ab]$ (for some random a, b) both of which operations are entirely independent of the inputs of the participants. For simplicity, we abstract away the underlying details of preprocessing and use the necessary operations in a black-box manner through the ideal functionality of Figure 5b. The realization of $\mathcal{F}_{\text{Prep}}$ is possible using a 2PC framework in the semi-honest model, such as ABY by [DSZ15].

After exchanging secret shares of their inputs, both participants execute the same computation on their shares in the online phase. While the addition of secret shares is for free, i.e. corresponds to ordinary local addition, share multiplication, which we denote with $\boxdot$, consumes one multiplication triple and requires one round of interaction and 2 group elements of communication. Concretely, $[x] \boxdot [y] = [xy]$ can be computed by revealing $(x + a)$ and $(y + b)$ (that does not disclose information about x and y, because a, b are random), then $(x + a) \cdot (y + b) - (x + a) \cdot [b] - (y + b) \cdot [a] + [ab] = [xy]$ can be evaluated. The resulting online part then consists of three rounds of interaction and 5 group elements of communication.

Protocol $\Pi^{OPRF}_{\text{Legendre}}$

Participants: sender $\mathcal{S}$, receiver $\mathcal{R}$.
Preprocessing:
1. execute $\mathcal{F}_{\text{Prep}}.\mathsf{RandSquare}$,
2. execute $\mathcal{F}_{\text{Prep}}.\mathsf{TripleGen}$.

Input:
- $\mathcal{S}$: $K \in \mathbb{F}_p$,
- $\mathcal{R}$: $x \in \mathbb{F}_p$.

Evaluation:
1. $\mathcal{S}, \mathcal{R}$ share $[K], [x]$ with each other,
2. both compute $[c] = [s^2] \boxdot ([K] + [x])$,
3. $\mathcal{S}$ sends $[c]$ to $\mathcal{R}$,
4. $\mathcal{R}$ outputs $L_p(c) = L_p(K + x)$.

(a) Legendre OPRF based on [GRR+16]

Algorithm $\mathsf{OPPRF.KeyGen}(1^\lambda, (x_1, y_1), \ldots, (x_n, y_n)) \to (K, p)$
1. Compute $y_i(-1)^{\frac{(p-1)(x_i-1)}{4}} = \left(\frac{p}{x_i}\right)$,
2. identify $m_i \in \mathbb{Z}_{x_i}$, s.t. $\left(\frac{m_i}{x_i}\right) = y_i(-1)^{\frac{(p-1)(x_i-1)}{4}}$,
3. $\forall i$ let $M_i = \left\{m | m \in \mathbb{Z}_{x_i} \wedge b_i(-1)^{\frac{(p-1)(x_i-1)}{4}} = \left(\frac{m}{x_i}\right)\right\}$,
4. $\forall m_{ij} \in M_i$ and $i \in [1, n]$ solve the following system of congruences for p using the Chinese-Remainder Theorem: $p \equiv m_{ij} \mod x_i$.

Output: (K, p)

(b) Programming the Legendre OPRF of Figure 5a by appropriate parameter selection. For ease of exposition, we assume that for all the programmed points x_i are primes.

Figure 6: Legendre OPRF and the algorithm to extend it to be an OP**P**RF.

Theorem 5.1 *The protocol $\Pi^{OPRF}_{\text{Legendre}}$ securely computes the functionality $\mathcal{F}_{OPRF}$ in the $\mathcal{F}_{\text{Prep}}$-hybrid model, if the SLS problem is hard.*

For brevity, we omit the proof since it follows the blueprint of the proof of [GRR+16, Theorem 2.]. We note that $\Pi^{OPRF}_{\text{Legendre}}$ is only statistically correct as with probability $1/p = \Pr(s^2 = 0)$ the output is necessarily zero. For perfect correctness, we need to use $\mathsf{RandSquare}'$ in the preprocessing phase to rule out $s^2 = 0$ the cost of which appears in the round complexity, resulting in *expected* constant (one) round.

Our efficiency comparisons in Table 5.2 show that in terms of both message size and computational complexity, the Legendre OPRF is a promising candidate for a post-quantum OPRF since the underlying SLS problem is not known to be vulnerable to quantum attacks.

OPRF	Comm. Complexity			Comp. Complexity		Model	Assumption
	Rounds	Msg. Size	Concr. eff.	Client	Server		
RSA-OPRF	2	2 $\mathbb{G}$	0.77KB	1H + 2 $\mathbb{G}$	1 $\mathbb{G}$	ROM	1-more-RSA-inv
[JKK14]	2	2 $\mathbb{G}$	64 byte	1H + 2 $\mathbb{G}$	1 $\mathbb{G}$	ROM/Standard	EC-DDH
[KKRT16]†	5	2λ bits	256 bits	1H + 2XOR	2H + 2XOR	ROM	OT*
[ADDS19]	2	$\mathcal{O}(\lambda^c)$ $\mathbb{F}_p$	≈ 1MB	$\mathcal{O}(\lambda^c)$ $\mathbb{F}_p$	$\mathcal{O}(\lambda^c)$ $\mathbb{F}_p$	QROM	RLWE
[BKW20]	2	$\mathcal{O}(\lambda)$ $\mathbb{G}$	≈ 2MB	$\mathcal{O}(\lambda)$ $\mathbb{G}$	$\mathcal{O}(\lambda)$ $\mathbb{G}$	ROM	SIDH
Figure 6a	3	5λ $\mathbb{G}$	13.44KB	17λ $\mathbb{G}$	17λ $\mathbb{G}$	ROM	SLS, OT*

Table 5.2: Comparing the online costs of various Oblivious PRF protocols. In the columns of communication and computation complexity $\mathbb{G}$ denotes a group element or group operation, while H denotes a hashing operation. Concrete efficiency of obtaining λ pseudorandom bits with the corresponding OPRFs were computed with $\lambda = 128$ bit-security. (Q)ROM stands for the (quantum) random oracle model. Note, that the PRF of [KKRT16] is only a relaxed PRF. SIDH stands for the Supersingular Isogeny Diffie-Hellman assumption, while RLWE is the abbreviation for the ring-learning with errors assumption. Oblivious transfer (OT) can be instantiated both with classic and post-quantum security. Non post-quantum secure assumptions are written in red, while assumptions written in green are secure even against quantum attackers.

[1] We denote secret shares in square brackets, i.e. $[x]_1 = r \in_R \mathbb{F}_p$ and $[x]_2 = x - r$ so $[x]_1 + [x]_2 = x$. For simplicity, we omit the lower indices denoting the owner of the given secret share, when this does not cause confusion.

5.2.2 OPPRF: Programming the Legendre OPRF

The notion of oblivious *programmable* PRF (OP**P**RF) was introduced in [KMP+17]. A PRF is said to be OP**P**RF if it is in addition to being an OPRF, also allows the sender to program the output of the OPRF at certain evaluation points (see Figure 5a). Kolesnikov et al. [KMP+17] formulated three *generic* OP**P**RF constructions, that can turn any OPRF into an OP**P**RF. In the sequel, we follow the terminology of these generic constructions and introduce two algorithms that aims to turn an OPRF into an OP**P**RF:

- $\mathsf{OPPRF.KeyGen}(1^\lambda, \mathcal{P}) \rightarrow (K, \mathsf{hint})$: Given a security parameter and set of points $\mathcal{P} = \{(x_1, y_1), \ldots, (x_n, y_n)\}$ with distinct x_i-values, generates a PRF key K and (public) auxiliary information hint.
- $\mathsf{OPPRF.Eval}\big(F(K, x), \mathsf{hint}\big) \rightarrow y$: Using the hint turns the OPRF output into the OP**P**RF output y.

We require from an OP**P**RF the following high-level security notions to hold (for the formal security definitions, the reader is referred to [KMP+17]):

Correctness:
$$(x, y) \in \mathcal{P} \wedge \big((K, \mathsf{hint}) \leftarrow \mathsf{OPPRF.KeyGen}(\mathcal{P})\big) \implies \mathsf{OPPRF.Eval}\big(F(K, x), \mathsf{hint}\big) = y.$$

(n, t)-security: No efficient adversary should be able to distinguish the n programmed points from non-programmed points given oracle access to the PRF using t queries. Note that this definition implies that unprogrammed PRF outputs (i.e., those not set by the input to $\mathsf{OPPRF.KeyGen}$) are pseudorandom.

Programming the Legendre OPRF. We show how one can program efficiently the output of the Legendre PRF by carefully choosing the prime modulus, which defines our $\mathsf{OPPRF.KeyGen}$ algorithm. This strategy already highlights the strength of the resulting OP**P**RF: it does not require an explicit hint beyond the prime modulus that is a public parameter anyway. Moreover, the $\mathsf{OPPRF.Eval}$ algorithm can simply return the output of the Legendre OPRF.

The naïve way to program the Legendre PRF would be to generate primes randomly and hope that the PRF outputs match the desired values y_i at the programmed points x_i for a given key K. This certainly works for small number of programmed points, however, this naïve PRF programming method incurs an exponential time-complexity in the number of programmed points.

To circumvent the exponential time-complexity of the programming, we take a different approach, cf. Figure 6b. The goal of the algorithm is to find a prime p, such that

$$i \in [0, n) : y_i = \left(\frac{x_i}{p}\right) = \left(\frac{p}{x_i}\right)(-1)^{\frac{(p-1)(x_i-1)}{4}}.$$

Without loss of generality, we search p in the form $p \equiv 1 \mod 4$. Moreover, we assume that the programmed points x_i are prime numbers. This assumption is natural and eases our exposition. This is because programming the PRF output at a composite x_i is reducible to programming the PRF output at the prime factors of x_i due to the multiplicativity of the Legendre symbol. For each x_i the value $\left(\frac{p}{x_i}\right)$ establishes possible residue classes for p mod x_i. The appropriate modulus p can be obtained via the Chinese remainder theorem. Therefore, the "programmability" of the Legendre PRF is rather space-inefficient, since $p \approx \prod_{i=1}^{n} x_i$. Hence, the number of programmed points is somewhat limited with our algorithm. We note that the main ideas of this programming method were already proposed in a different context (secure comparison protocols) by Yu [Yu11]. In a similar fashion, one could generalize the approach of Figure 6b to power residue symbols, i.e. programming power residue symbol PRFs. Such generalization was shown recently by Cascudo et al. [CS20] who proposed as an open question to find concrete applications for their protocol. We note that their methods can be applied to program power residue symbol OPRFs.

Hint size and batch OPPRFs. As our novel programming methods – specifically designed for the Legendre OPRF – minimize the necessary auxiliary information for the OP**P**RF evaluation, it outperforms all existing solutions in this metric. For a detailed comparison, we refer to Table 5.3. Finally, we note that [PSTY19] uses a so-called "Batch OP**P**RF" that – informally – invokes independent OP**P**RF instances with a total number of programmed points σ (the number of programmed points per instance may vary but has to remain hidden) and only uses a single hint with size linear in σ. Since the hint size of the Legendre OP**P**RF is independent of the number of programmed points, it naturally fulfils the requirement of Batch OP**P**RFs.

OPPRF	Programming complexity	Hint size	Online communication complexity	Constraint on no. of programmed points	No. of evaluations
Lagrange interpol.	$O(n^2)$	$O(n)$	$(n+kn)$ $\mathbb{G}$	space-efficiency	any
Garbled Bloom Filter	$O(n\lambda_{\mathsf{BF}})$	$n\lambda_{\mathsf{BF}}$	$(60n+kn)$ $\mathbb{G}$	space-efficiency	any
Table-based	$O(n)$	$O(n)$	$(n+kn)$ $\mathbb{G}$	space-efficiency	1
Legendre (Fig. 6b)	$O(n \log n)$	1	$\mathcal{O}(n)$ $\mathbb{G}$	depends on λ	any
Legendre bruteforce	$O(2^n)$	1	1 $\mathbb{G}$	time-efficiency	any

Table 5.3: Comparison of the generic OP**P**RF constructions of [KMP+17] (which can be based on an OPRF, e.g. that of [KKRT16]) and the Legendre OPRF that was shown to be programmable in Section 5.2.2. The number of programmed input positions is denoted as n, λ_{BF} is the soundness parameter of the Bloom filter, while k denotes the number of base-OTs, typically $k \approx 4\lambda$.

5.2.3 The Legendre Verifiable OPRF

In Section 5.2, we built an OPRF relying on semi-honest 2PC that clearly cannot prevent the participants from deviating the protocol. What is even more problematic in practice is that sometimes the server is supposed to behave consistently in multiple OPRF evaluations, namely, it is assumed to use the same key. To check this on the receiver side – without obtaining information about the key – active security alone is not enough, but in an initialization phase the sender has to commit to the key(s) it wishes to use. Such commitments can then be published (as a "public key") to enable the receiver the verification of whether distinct OPRF evaluations happened under the same or different keys. OPRF protocols that guarantee such verifiability are called verifiable OPRFs (VOPRFs). In Figure 7a, we recall the ideal functionality as defined in [ADDS21], for the precise security definition we also refer to this work. We note that different formalizations of VOPRF exist, e.g. [JKK14] considered in the concurrent setting when defining the universal composable VOPRF.

Turning our attention towards the realization, it seems obvious that special purpose protocols beat general ones in all efficiency metrics. Indeed, known realizations [JKK14, BKW20, ADDS21, DFHSW21] try to avoid generic tools such as 2PC that leads to highly efficient solutions in case of constructions using pre-quantum assumptions but not when aiming protocols that offer post-quantum security. Besides their theoretical post-quantum solutions, Albrecht et al. [ADDS21] mention an alternative pathway towards post-quantum VOPRFs that has comparable efficiency with their lattice-based solutions. This solution consists of a hash (say SHA3) commitment to a key K, and an actively secure MPC evaluation of the AES circuit on inputs K and x (from $\mathcal{S}$ and $\mathcal{R}$ respectively) together with comparison of the hash of the used key with the committed key, after which $\mathcal{R}$ receives output iff the check goes through. At this point, one may recall the Legendre OPRF of Figure 6a that requires a single multiplication in the online phase for one bit output (or 128 multiplications for 128 bits). This is in contrast to the 960 multiplication of the AES circuit evaluation [GRR+16]. This observation motivates our Legendre VOPRF protocol, that is described in details in Figure 7b.

Functionality $\mathcal{F}_{\text{VOPRF}}$

Participants: sender $\mathcal{S}$, receiver $\mathcal{R}$.
Parameters: a PRF $F : \mathcal{K} \times \mathcal{X} \to \{0,1\}$ for key-space $\mathcal{K}$ input-space $\mathcal{X}$
Init-$\mathcal{S}$: On input init from $\mathcal{S}$ the functionality waits for an input K from $\mathcal{S}$. If $\mathcal{S}$ returns abort then the functionality aborts. Otherwise, it stores the value K if it is a valid key (i.e. conforming to a predefined distribution.) and aborts if not.
Init-$\mathcal{R}$: On input of init from $\mathcal{R}$, the functionality will return abort if **Init-$\mathcal{S}$** has not successfully completed.
Query: On input of $(\mathsf{query}; x)$ from $\mathcal{R}$, if $x \neq \perp$ then the functionality waits for an input from $\mathcal{S}$. If $\mathcal{S}$ returns deliver then the functionality sends $y = F(K, x)$ to $\mathcal{R}$. If $\mathcal{S}$ returns abort then the functionality aborts.

(a) Ideal functionality for VOPRF adapted from [ADDS21].

Protocol $\Pi^{\text{VOPRF}}_{\text{Legendre}}$

Participants: sender $\mathcal{S}$, receiver $\mathcal{R}$.
Initialization of $\mathcal{S}$:
- samples and stores $K, r \in \mathbb{F}_p$,
- computes and publishes commitment $h = H(K||r)$.

Input:
- $\mathcal{S}$: $K, r \in \mathbb{F}_p$,
- $\mathcal{R}$: $x \in \mathbb{F}_p, h$.

Evaluation: $\mathcal{S}$ and $\mathcal{R}$ run a secure 2-party computation with the above inputs to
1. sample a random non-zero square $s^2 \in \mathbb{F}_p$,
2. compute $c = s^2 \cdot (K + x)$,
3. $b \leftarrow (h \neq H(K||r))$,
4. output to $\mathcal{R}$: $c' = (b \cdot \perp) + (1 - b) \cdot c$.

Finally $\mathcal{R}$ computes $L_p(c') = L_p(K + x) \Leftrightarrow K$ is consistent to h.

(b) Legendre VOPRF based on actively secure 2PC and collision-rasistant hashing (H).

Figure 7: Legendre VOPRF.

Theorem 5.2 (Informal) *When instantiated with actively secure 2PC, protocol $\Pi^{\text{VOPRF}}_{\text{Legendre}}$ securely realizes $\mathcal{F}_{\text{VOPRF}}$ under the SLS assumption and the assumptions which the 2PC protocol relies on as long as H is a collusion-resistant hash function.*

The generality of the utilized 2PC protocol leads to various instantiation opportunities causing that the above result can have several different flavours. We mention some of these. [KO04] showed that actively secure 2PC in the standard model requires 5 rounds of interaction. With some relaxations, namely by allowing the simulator to run in superpolynomial time while the adversary is still restricted to polynomial time (a.k.a. SPS security), actively secure non-interactive secure computation (NIZK) is possible in the plain model under the subexponential security of the LWE assumption [BGI+17, BD18] leading to a VOPRF realization under the same assumptions. Leaving the plain model, it is also possible to instantiate our VOPRF utilizing NIZK built on oblivious transfer (OT) in the OT-hybrid model [IKO+11], in the common reference string model [MR17] or in the global random oracle model [CJS14].

6 Future Directions

We perceive three main areas for future work. There is still quite some work to be done on the *provable security* part of the Legendre PRF. It would be fascinating to find new connections to other post-quantum secure cryptographic assumptions, e.g. LWE. For instance, note that in Equation 17, the probability distribution of the coefficients of the quadratic terms in the induced MQ instance follows a discrete Gaussian distribution. Could one reframe the MQ instance as an LWE instance for a suitable change in the variables? Moreover, it would be fruitful to establish concrete and asymptotic lower bounds on the degree of regularity of the Legendre PRF's MQ instances. That would pave the path for settling the provable security of this PRF.

It is quintessential to improve on existing key-recovery attacks or find new, more performant cryptanalytic approaches. It would allow us to better estimate the *bit-security* of the Legendre PRF and other variants.

We foresee many more *novel cryptographic applications* of the Legendre PRF due to its homomorphic properties and MPC-friendliness. For instance, it seems accessible to prove the existence of related-key secure PRFs or key-homomorphic PRFs from quadratic and power residue symbol PRFs.

Acknowledgements

We are grateful for the insightful conversations to Gergő Zábrádi.

References

[AABS+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. Design of symmetric-key primitives for advanced cryptographic protocols. *IACR Transactions on Symmetric Cryptology*, pages 1–45, 2020.

[ACG+19] Martin R Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. Algebraic cryptanalysis of stark-friendly designs: application to marvellous and mimc. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 371–397. Springer, 2019.

[AD18] Tomer Ashur and Siemen Dhooghe. Marvellous: a stark-friendly family of cryptographic primitives. *IACR Cryptol. ePrint Arch.*, 2018:1098, 2018.

[ADDS19] Martin R Albrecht, Alex Davidson, Amit Deo, and Nigel P Smart. Round-optimal verifiable oblivious pseudorandom functions from ideal lattices. *IACR Cryptol. ePrint Arch.*, 2019:1271, 2019.

[ADDS21] Martin R Albrecht, Alex Davidson, Amit Deo, and Nigel P Smart. Round-optimal verifiable oblivious pseudorandom functions from ideal lattices. In *IACR International Conference on Public-Key Cryptography*, pages 261–289. Springer, 2021.

[AGR+16] Martin Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. Mimc: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 191–219. Springer, 2016.

[BBUV20] Ward Beullens, Tim Beyne, Aleksei Udovenko, and Giuseppe Vitto. Cryptanalysis of the legendre prf and generalizations. *IACR Transactions on Symmetric Cryptology*, pages 313–330, 2020.

[BD18] Zvika Brakerski and Nico Döttling. Two-message statistically sender-private OT from LWE. In Amos Beimel and Stefan Dziembowski, editors, *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*, volume 11240 of *Lecture Notes in Computer Science*, pages 370–390. Springer, 2018.

[BdSG20] Ward Beullens and Cyprien Delpech de Saint Guilhem. Legroast: Efficient post-quantum signatures from the legendre prf. In *International Conference on Post-Quantum Cryptography*, pages 130–150. Springer, 2020.

[BFSY05] Magali Bardet, Jean-Charles Faugere, Bruno Salvy, and Bo-Yin Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In *Proc. of MEGA*, volume 5, 2005.

[BGI+17] Saikrishna Badrinarayanan, Sanjam Garg, Yuval Ishai, Amit Sahai, and Akshay Wadia. Two-message witness indistinguishability and secure computation in the plain model from new assumptions. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part III*, volume 10626 of *Lecture Notes in Computer Science*, pages 275–303. Springer, 2017.

[BGLS03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 416–432. Springer, 2003.

[BKW20] Dan Boneh, Dmitry Kogan, and Katharine Woo. Oblivious pseudorandom functions from isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 520–550. Springer, 2020.

[BSBHR18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. *IACR Cryptol. ePrint Arch.*, 2018:46, 2018.

[Buc65] Bruno Buchberger. Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal. *PhD thesis, Universitat Insbruck*, 1965.

[CGS22] Nishanth Chandran, Divya Gupta, and Akash Shah. Circuit-psi with linear complexity via relaxed batch opprf. In *22nd Privacy Enhancing Technologies Symposium (PETS 2022)*, June 2022.

[CJS14] Ran Canetti, Abhishek Jain, and Alessandra Scafuro. Practical UC security with a global random oracle. In Gail-Joon Ahn, Moti Yung, and Ninghui Li, editors, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*, pages 597–608. ACM, 2014.

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer, 2000.

[CLO13] David Cox, John Little, and Donal OShea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.

[CMZ14] Melissa Chase, Sarah Meiklejohn, and Greg Zaverucha. Algebraic macs and keyed-verification anonymous credentials. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 1205–1216, 2014.

[CS20] Ignacio Cascudo and Reto Schnyder. A note on secure multiparty computation via higher residue symbol techniques. *IACR Cryptol. ePrint Arch.*, 2020:183, 2020.

[Dam88] Ivan Bjerre Damgård. On the randomness of legendre and jacobi sequences. In *Conference on the Theory and Application of Cryptography*, pages 163–172. Springer, 1988.

[Déc07] Isabelle Déchene. *Generalized Jacobians in cryptography*. ProQuest, 2007.

[DFHSW21] Alex Davidson, Armando Faz-Hernández, Nick Sullivan, and Christopher Wood. Oblivious pseudorandom functions (OPRFs) using prime-order groups, 2021. https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/.

[DGS+18] Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda. Privacy pass: Bypassing internet challenges anonymously. *Proc. Priv. Enhancing Technol.*, 2018(3):164–180, 2018.

[DHS98] Cunsheng Ding, T Hesseseth, and Weijuan Shan. On the linear complexity of legendre sequences. *IEEE Transactions on Information Theory*, 44(3):1276–1278, 1998.

[DKPW12] Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs. Message authentication, revisited. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 355–374. Springer, 2012.

[DSZ15] Daniel Demmler, Thomas Schneider, and Michael Zohner. ABY - A framework for efficient mixed-protocol secure two-party computation. In *NDSS*. The Internet Society, 2015.

[DY05] Yevgeniy Dodis and Aleksandr Yampolskiy. A verifiable random function with short proofs and keys. In *International Workshop on Public Key Cryptography*, pages 416–431. Springer, 2005.

[EKS+20] Muhammed F Esgin, Veronika Kuchta, Amin Sakzad, Ron Steinfeld, Zhenfei Zhang, Shifeng Sun, and Shumo Chu. Practical post-quantum few-time verifiable random function with applications to algorand. *IACR Cryptol. ePrint Arch*, 2020:1222, 2020.

[Fau02] Jean Charles Faugere. A new efficient algorithm for computing gröbner bases without reduction to zero (f 5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, 2002.

[FIPR05] Michael J. Freedman, Yuval Ishai, Benny Pinkas, and Omer Reingold. Keyword search and oblivious pseudorandom functions. In *TCC*, volume 3378 of *Lecture Notes in Computer Science*, pages 303–324. Springer, 2005.

[FS21] Paul Frixons and André Schrottenloher. Quantum security of the legendre prf. Cryptology ePrint Archive, Report 2021/149, 2021. https://eprint.iacr.org/2021/149.

[GHM+17] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles*, pages 51–68, 2017.

[GJ79] Michael R Garey and David S Johnson. *Computers and intractability*, volume 174. freeman San Francisco, 1979.

[GKR+20] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A new hash function for zero-knowledge proof systems. In *Proceedings of the 30th USENIX Security Symposium*. USENIX Association, 2020.

[GMS14] Katalin Gyarmati, Christian Mauduit, and András Sárközy. The cross-correlation measure for families of binary sequences., 2014.

[GNP+15] Sharon Goldberg, Moni Naor, Dimitrios Papadopoulos, Leonid Reyzin, Sachin Vasant, and Asaf Ziv. Nsec5: Provably preventing dnssec zone enumeration. In *NDSS*, 2015.

[Gro16] Jens Groth. On the size of pairing-based non-interactive arguments. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 305–326. Springer, 2016.

[GRR+16] Lorenzo Grassi, Christian Rechberger, Dragos Rotaru, Peter Scholl, and Nigel P Smart. Mpc-friendly symmetric key primitives. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 430–443. ACM, 2016.

[Har13] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[HL08] Carmit Hazay and Yehuda Lindell. Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries. In Ran Canetti, editor, *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008*, volume 4948 of *Lecture Notes in Computer Science*, pages 155–175. Springer, 2008.

[HLY12] Yun-Ju Huang, Feng-Hao Liu, and Bo-Yin Yang. Public-key cryptography from new multivariate quadratic assumptions. In *International Workshop on Public Key Cryptography*, pages 190–205. Springer, 2012.

[IKO+11] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai. Efficient non-interactive secure computation. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 406–425. Springer, 2011.

[JK97] Thomas Jakobsen and Lars R Knudsen. The interpolation attack on block ciphers. In *International Workshop on Fast Software Encryption*, pages 28–40. Springer, 1997.

[JKK14] Stanislaw Jarecki, Aggelos Kiayias, and Hugo Krawczyk. Round-optimal password-protected secret sharing and T-PAKE in the password-only model. In *ASIACRYPT (2)*, volume 8874 of *Lecture Notes in Computer Science*, pages 233–253. Springer, 2014.

[JKKX16] Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk, and Jiayu Xu. Highly-efficient and composable password-protected secret sharing (or: How to protect your bitcoin wallet online). In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 276–291. IEEE, 2016.

[JKX18] Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu. Opaque: an asymmetric pake protocol secure against pre-computation attacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 456–486. Springer, 2018.

[JL09] Stanislaw Jarecki and Xiaomin Liu. Efficient oblivious pseudorandom function with applications to adaptive OT and secure computation of set intersection. In Omer Reingold, editor, *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings*, volume 5444 of *Lecture Notes in Computer Science*, pages 577–594. Springer, 2009.

[KBR13] Sriram Keelveedhi, Mihir Bellare, and Thomas Ristenpart. Dupless: Server-aided encryption for deduplicated storage. In *22nd {USENIX} Security Symposium ({USENIX} Security 13)*, pages 179–194, 2013.

[Kho19] Dmitry Khovratovich. Key recovery attacks on the legendre prfs within the birthday bound. Cryptology ePrint Archive, Report 2019/862, 2019. https://eprint.iacr.org/2019/862.

[KK20] Ferhat Karakoç and Alptekin Küpçü. Linear complexity private set intersection for secure two-party protocols. In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, *Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings*, volume 12579 of *Lecture Notes in Computer Science*, pages 409–429. Springer, 2020.

[KKK20] Novak Kaluderovic, Thorsten Kleinjung, and Dusan Kostic. Improved key recovery on the legendre prf. *IACR Cryptol. ePrint Arch.*, 2020:98, 2020.

[KKRT16] Vladimir Kolesnikov, Ranjit Kumaresan, Mike Rosulek, and Ni Trieu. Efficient batched oblivious PRF with applications to private set intersection. In *CCS*, pages 818–829. ACM, 2016.

[KLS+17] Ágnes Kiss, Jian Liu, Thomas Schneider, N. Asokan, and Benny Pinkas. Private set intersection for unequal set sizes with mobile applications. *Proc. Priv. Enhancing Technol.*, 2017(4):177–197, 2017.

[KMP+17] Vladimir Kolesnikov, Naor Matania, Benny Pinkas, Mike Rosulek, and Ni Trieu. Practical multi-party private set intersection from symmetric-key techniques. In *CCS*, pages 1257–1272. ACM, 2017.

[KO04] Jonathan Katz and Rafail Ostrovsky. Round-optimal secure two-party computation. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 335–354. Springer, 2004.

[KS99] Aviad Kipnis and Adi Shamir. Cryptanalysis of the hfe public key cryptosystem by relinearization. In *Annual International Cryptology Conference*, pages 19–30. Springer, 1999.

[LBM20] Bei Liang, Gustavo Banegas, and Aikaterini Mitrokotsa. Statically aggregate verifiable random functions and application to e-lottery. *Cryptography*, 4(4):37, 2020.

[Lem03] Franz Lemmermeyer. Conics-a poor man's elliptic curves. *arXiv preprint math/0311306*, 2003.

[LP19] Chaoyun Li and Bart Preneel. Improved interpolation attacks on cryptographic primitives of low algebraic degree. In *International Conference on Selected Areas in Cryptography*, pages 171–193. Springer, 2019.

[MR17] Payman Mohassel and Mike Rosulek. Non-interactive secure 2pc in the offline/online and batch settings. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 425–455, 2017.

[MRV99] Silvio Micali, Michael Rabin, and Salil Vadhan. Verifiable random functions. In *40th annual symposium on foundations of computer science (cat. No. 99CB37039)*, pages 120–130. IEEE, 1999.

[MS97] Christian Mauduit and András Sárközy. On finite pseudorandom binary sequences i: Measure of pseudorandomness, the legendre symbol. *Acta Arithmetica*, 82(4):365–377, 1997.

[NR97] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. In *FOCS*, pages 458–467. IEEE Computer Society, 1997.

[Osp16] Daniel Esteban Escudero Ospina. *Groebner bases and applications to the security of multivariate public key cryptosystems.* PhD thesis, Ph. D. dissertation, Escuela de Matemáticas, Univ. Nacional de Colombia ..., 2016.

[Per92] Rene Peralta. On the distribution of quadratic residues and nonresidues modulo a prime number. *Mathematics of Computation*, 58(197):433–440, 1992.

[PPST17] Ray Perlner, Albrecht Petzoldt, and Daniel Smith-Tone. Total break of the srp encryption scheme. In *International Conference on Selected Areas in Cryptography*, pages 355–373. Springer, 2017.

[PSTY19] Benny Pinkas, Thomas Schneider, Oleksandr Tkachenko, and Avishay Yanai. Efficient circuit-based PSI with linear communication. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 122–153. Springer, 2019.

[PWH+17] Dimitrios Papadopoulos, Duane Wessels, Shumon Huque, Moni Naor, Jan Včelák, Leonid Reyzin, and Sharon Goldberg. Making nsec5 practical for dnssec. *Cryptology ePrintArchive, Report 2017/099*, 2017.

[RS04] Alexander Russell and Igor E Shparlinski. Classical and quantum function reconstruction via character evaluation. *Journal of Complexity*, 20(2-3):404–422, 2004.

[SKI04] M Sugita, M Kawazoe, and H Imai. Relation between xl algorithm and gröbner bases algorithms, iacr eprint server, 2004.

[Tót07] Viktória Tóth. Collision and avalanche effect in families of pseudorandom binary sequences. *Periodica Mathematica Hungarica*, 55(2):185–196, 2007.

[Ull12] Ehsan Ullah. New techniques for polynomial system solving. 2012.

[vDHI06] Wim van Dam, Sean Hallgren, and Lawrence Ip. Quantum algorithms for some hidden shift problems. *SIAM J. Comput.*, 36(3):763–778, 2006.

[Vin16] Ivan Matveevich Vinogradov. *Elements of number theory.* Courier Dover Publications, 2016.

[Yu11] Ching-Hua Yu. Sign modules in secure arithmetic circuits. *IACR Cryptol. ePrint Arch.*, 2011:539, 2011.

A Background

For completeness, we define possible generalisations of the Legendre PRF.

Definition A.1 (Higher-degree Legendre PRF) *In case of the Higher-degree Legendre PRF with a secret polynomial $f \in_R \mathbb{F}_p[x]$, let $\{a\}_f$ denote the following sequence:*

$$\{a\}_f := \left(\frac{f(0)}{p}\right), \left(\frac{f(1)}{p}\right), \ldots, \left(\frac{f(a-1)}{p}\right).$$

Definition A.2 (rth power residue function) *Let $p \equiv 1 \mod r$ and $g \in \mathbb{F}_p^\times$ a generator. The rth power residue function $l^{(r)} : \mathbb{F}_p \to \mathbb{Z}_r$ is defined as*

$$l^{(r)}(a) := \begin{cases} k, & \textit{if} \quad a \not\equiv 0 \mod p \wedge a/g^k \textit{is an } r\textit{th power} \mod p \\ 0, & \textit{if} \quad a \equiv 0 \mod p. \end{cases}$$

Similarly to Definitions 2.1 and A.1, we might introduce the power residue PRF and its higher-degree variants, relying on the power residue function. Once again, we note that our results and observations can be generalized to the higher-degree and other variants of the Legendre PRF.

B The MQ Instance Induced by the Legendre PRF

B.1 An Alternative View

We view the resulting equation system globally and assess the probability distribution of each coefficient to appear in the MQ instance. Adjacent pairs of Legendre symbols are asymptotically equi-distributed [Per92]. Therefore we can easily describe the discrete probability distribution of the coefficients in the induced equation system. Let $X_q^{(i,j)}, X_l^{(i)}, X_c$ be the random discrete variables corresponding to the ith unknown's quadratic, linear and constant terms. For the equation system's coefficients, we have the following discrete probability distributions given Equations 1, 2 and 3. For the constant terms, we have that

$$\Pr[X_c = 1] = \Pr[X_c = r] = \frac{1}{2}. \tag{15}$$

Every linear term is zero, namely,

$$\Pr[X_l^{(i)} = 0] = 1, \forall i \in [1, n]. \tag{16}$$

Finally, the quadratic terms' coefficients have the following probability distribution. The $\Pr[X_q^{(i,j)} = 0] = 1$, if $i \neq j$,. Otherwise, we have that

$$\begin{gathered} \Pr[X_q^{(i,i)} = 1] = \frac{1}{n}, \quad \Pr[X_q^{(i,i)} = -1] = \frac{1}{2n}, \\ \Pr[X_q^{(i,i)} = -r] = \Pr[X_q^{(i,i)} = -r^{-1}] = \frac{1}{4n}, \quad \Pr[X_q^{(i,i)} = 0] = 1 - \frac{2}{n}. \end{gathered} \tag{17}$$

We remark that the discrete probability distribution of the quadratic terms is reminiscent of a discrete normal Gaussian distribution with average 0, whenever n goes to infinity. If the linear terms, cf. Equation 16, would follow a uniformly random distribution after a suitable change in the variables, the resulting MQ instance could be seen asymptotically as a learning with errors (LWE) instance. We leave this as an interesting future direction to investigate further connections to other post-quantum secure assumptions.

C Algebraic Cryptanalysis of the Legendre PRF

C.1 Computing the Q-rank of the Legendre PRF

The Q-rank of a MQ cryptosystem plays a crucial role in cryptanalysis. Every multivariate quadratic equation system $\mathbf{f}$ can be lifted to a quadratic form $\mathcal{Q}$ in an extension field. Let $\mathbb{E}$ denote an extension field over $\mathbb{F}_p$. Informally, Q-rank is the rank of the quadratic form $\mathcal{Q}$ as a matrix over the field $\mathbb{E}$. Low Q-rank is detrimental, since it facilitates successful cryptanalysis (key-recovery, decryption etc.) [KS99, PPST17].

Definition C.1 (Q-rank) *The Q-rank of a multivariate quadratic map* $\mathbf{f} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *over the finite field* $\mathbb{F}_q$ *is the rank of the quadratic form* $\mathcal{Q}$ *on the extension field* $\mathbb{E}[X_0, \ldots, X_{n-1}]$ *defined by* $Q(X_0, \ldots, X_{n-1}) = \phi \circ \mathbf{f} \circ \phi^{-1}(X, X^q, \ldots, X^{q^{n-1}})$*, under the identification* ϕ*:* $X_0 = X, X_1 = X^q, \ldots, X_{n-1} = X^{q^{n-1}}$*.*

We compute now the Q-rank (cf. Definition C.1) of the Legendre PRF equation system [Osp16]. We rewrite each generator polynomial f_i in the ideal $I = \langle f_1, \ldots, f_m \rangle$ induced by the Legendre PRF, as folllows:

$$f_i(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j + \sum_{i=1}^{n} b_i x_i + c = \mathbf{x}^T A_i \mathbf{x} + B_i \mathbf{x} + c, \tag{18}$$

where $\mathbf{x} = [x_1, \ldots, x_n]^T, A_i \in \mathcal{M}_{n\times n}(\mathbb{F})$ is the matrix $[a_{ij}]_{ij}$ and $B_i \in \mathcal{M}_{1\times n}(\mathbb{F})$ is the matrix $[b_i]_{1i}$. We note, that in the case of the Legendre PRF, $B_i = \mathbf{0}$. Each polynomial f_i can be represented in the extension field, in the following form:

$$\mathcal{F}_i(X) = \sum_{i,j=1}^{n} \alpha_{ij} X^{q^{i-1}+q^{j-1}} + \sum_{i=1}^{n} \beta_i X^{q^{i-1}} + \gamma = \mathbf{X}^T M_i \mathbf{X} + N_i \mathbf{X} + \gamma, \tag{19}$$

where $\mathbf{X} = [X^{q^0}, \ldots, X^{q^{n-1}}]^T, M_i \in \mathcal{M}_{n\times n}(\mathbb{E})$ is the matrix $[\alpha_{ij}]_{ij}$ and $B \in \mathcal{M}_{1\times n}(\mathbb{F})$ is the matrix $[\beta_i]_{1i}$. It is well-known that a quadratic polynomial equation system F defined by the generating polynomials f_i of I, can be lifted to the extension field by

$$\mathsf{Lft}(F)(X) = \phi^{-1} \circ \mathcal{F} \circ \phi(X) = \mathbf{X}^T M \mathbf{X} + N\mathbf{X} + \gamma, \tag{20}$$

where $\mathbf{x} = \phi(X)$. Our goal is to establish the rank of the matrix $M \in \mathcal{M}_{n\times n}(\mathbb{E})$. We start off by defining $\mathbf{X} = \Delta \cdot \phi(X)$, where Δ is the following invertible matrix,

$$\Delta = \begin{bmatrix} y^0 & y^1 & \cdots & y^{n-2} & y^{n-1} \\ (y^0)^{q^1} & (y^1)^{q^1} & \cdots & (y^{n-2})^{q^1} & (y^{n-1})^{q^1} \\ (y^0)^{q^2} & (y^1)^{q^2} & \cdots & (y^{n-2})^{q^2} & (y^{n-1})^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (y^0)^{q^{n-1}} & (y^1)^{q^{n-1}} & \cdots & (y^{n-2})^{q^{n-1}} & (y^{n-1})^{q^{n-1}} \end{bmatrix} \tag{21}$$

Equipped with all this, we can now define $M \in \mathcal{M}_{n\times n}(\mathbb{F}), N \in \mathcal{M}_{1\times n}(\mathbb{F})$ and $\gamma \in \mathbb{E}$ from the lifting Equation 20. We define $\gamma = c_1 + c_2 y + \cdots + c_n y^{n-1}$ and the matrices as,

$$M = (\Delta^T)^{-1} \left(\sum_{i=1}^{n} y^{i-1} A_i \right) \Delta^{-1} \qquad \textit{and} \qquad N = \left(\sum_{i=1}^{n} y^{i-1} B_i \right) \Delta^{-1}. \tag{22}$$

Note that in case of the Legendre PRF MQ instance, $N = 0$, since $B_i = \mathbf{0}$ for all i. The second term in matrix M, $\sum y^{i-1} A_i$ is a double diagonal non-singular matrix. Hence, matrix M has full rank, since it is the product of non-singular matrices.

D Group Structure of the Solutions of a Legendre PRF key-recovery attack

In Section 4.4, we showed that if there exists a probabilistic polynomial-time algorithm that breaks the SLS problem, then it could be used to find solutions of high order algebraic curves over $\mathbb{F}_p$. This is essentially an equivalent restatement of viewing the Legendre PRF as an MQ instance.

Moreover, the resulting algebraic curves have a genus greater than 1, implying that the solutions lying on the curve lack an Abelian group structure. However, in the case of shorter sequences, e.g. Legendre sequences of length three, all the points that result in a specific Legendre symbol sequence of length three lie on a sequence-specific non-singular elliptic curve. In the sequel, we show how to obtain the Legendre-sequence specific elliptic curve equation by elementary methods.

D.1 The Case of Consecutive Legendre symbol triplets

Let us suppose that one wants to generate key candidates $K^{'}$, whose subsequent Legendre symbols match the first three symbols of a sequence, i.e. $\left(\left(\frac{K^{'}}{p}\right), \left(\frac{K^{'}+1}{p}\right), \left(\frac{K^{'}+2}{p}\right) \right) = (b_0, b_1, b_2)$. Hereby, we show that such key candidates can be obtained as solutions of an elliptic curve over $\mathbb{F}_p$. One might generalise this approach to potentially speed up key-recovery attacks against the Legendre PRF and reduce its security to finding rational points on higher order algebraic curves over $\mathbb{F}_p$.

For the sake of concreteness, let us assume that $(b_0, b_1, b_2) = (1, 1, 1)$. Similar techniques apply for other bit-sequence patterns. Put it differently, the shifted Legendre sequence starts with 3 quadratic residues. Let us denote the corresponding square roots as $a, b, c \mod p$. Therefore we wish to solve the following equations:

$$c^2 - b^2 = b^2 - a^2 = 1$$

We introduce the following notation: $s := b - a$, $\frac{1}{s} := b + a$ and $\frac{c-b}{b-a} = \lambda$. We have that $2b = s + \frac{1}{s}$ and $2b = \frac{1}{s\lambda} - s\lambda$. This implies the following:

$$s + \frac{1}{s} = \frac{1}{s\lambda} - s\lambda$$

$$s^2\lambda + \lambda = 1 - s^2\lambda^2$$

$$s^2 = \frac{1-\lambda}{\lambda^2 + \lambda}$$

$$s^2(1+\lambda)^2\lambda^2 = (1-\lambda)(1+\lambda)\lambda \tag{23}$$

By denoting the left hand side of Equation 23. as t^2, we finally obtain the following nonsingular elliptic curve of genus 1:

$$t^2 = \lambda^3 - \lambda.$$

4-symbol case (sketch): Now, let us assume we have an additional $b_3 = 1$. Let d be the square-root of $K + 3$. Furhtermore, let $r := c - b$ and $\mu := \frac{d-c}{c-b}$. Given Equation 23, we also have that

$$r^2(1+\mu)^2\mu^2 = (1-\mu)(1+\mu)\mu \tag{24}$$

Since, $r = s\lambda$ we can squeeze Equation 23 and Equation 24 into a single two-variable quartic equation:

$$\lambda^2\mu^2 + \lambda^2\mu - \lambda\mu^2 - \lambda\mu + \lambda - \mu - \lambda\mu + 1 = 0$$