Chapter 7

Efficient Quantum Algorithms for Shifted Quadratic Character Problems

In this chapter we give efficient quantum algorithms for the Shifted Legendre Symbol Problem (SLSP) and its variants. There is some evidence that this is an intractable problem classically, and a closely related problem has been proposed as a cryptographic primitive [18]. In Section 7.1 we give an overview of the problems and related work. In Section 7.2 we give an efficient quantum algorithm for the SLSP and say how two variants follow as corollaries. In Section 7.3 we give an efficient quantum algorithm for the generalization of the SLSP to general fields, called the Shifted Quadratic Character Problem.

7.1 Definitions and Related Work

For a prime p, the *Legendre Symbol* $\left(\frac{x}{p}\right)$ is defined to be 1 if x is a quadratic residue, -1 if x is a quadratic nonresidue modulo p, and 0 if $p|x$. The Legendre Symbol can be extended in several ways. Here we will do so by defining it for rings $\mathbb{Z}_N$ and finite fields $\mathbb{F}_q$. For an integer $N = p_1 \cdots p_k$ the *Jacobi Symbol* $\left(\frac{x}{N}\right)$ is defined by $\left(\frac{x}{N}\right) = \left(\frac{x}{p_1}\right) \cdots \left(\frac{x}{p_k}\right)$, where the $\left(\frac{x}{p_i}\right)$ are Legendre Symbols and the product is over all the prime factors p_i of N (including repetitions). For a finite field $\mathbb{F}_q$ and $x \in \mathbb{F}_q$, the *quadratic character* $\chi(x)$ is 1 if x is a quadratic residue, -1 if x is a quadratic nonresidue, and 0 if $x = 0$.

We can now define the problems solved in this chapter. The first problem is the basic example on which the others build.

Definition 7.1 (Shifted Legendre Symbol Problem) *Given an odd prime p and a function $f_s : \mathbb{F}_p \to \{-1, 0, 1\}$ such that $f_s(x) = \left(\frac{x+s}{p}\right)$ for some $s \in \mathbb{F}_p$, find s.*

The first variant extends the definition to rings.

Definition 7.2 (Shifted Jacobi Symbol Problem) *Given a squarefree odd integer N and a function $f_s : \mathbb{Z}_N \to \{-1, 0, 1\}$ such that $f_s(x) = \left(\frac{x+s}{N}\right)$ for some $s \in \mathbb{Z}_N$, find s.*

If the integer N is not square-free, the Shifted Jacobi Problem does not have a unique answer. For example, if $N = p^2$ for a prime p, then $\left(\frac{i}{N}\right) = \left(\frac{i}{p}\right)^2 = 1$ for all i. Instead we could define the task to find one of the values s' such that $f_s(x) = \left(\frac{x+s'}{N}\right)$. This problem is again efficiently solvable on a quantum computer.

The goal of the second variant is to also keep N unknown in the Shifted Jacobi Symbol Problem. Notice that the SLSP with p unknown is a special case of this problem.

Definition 7.3 (Shifted Jacobi Symbol Problem, unknown N) *Given an integer M and a function $f_s : \mathbb{Z}_M \to \{-1, 0, 1\}$ such that $f_s(x) = \left(\frac{x+s}{N}\right)$ for some integer N, with $N^2 < M$, find s and N.*

The last variant is a generalization to general finite fields.

Definition 7.4 (Shifted Quadratic Character Problem) *Given $q = p^r$, a power of an odd prime p, and a function $f_s : \mathbb{F}_q \to \{-1, 0, 1\}$ such that $f_s(x) = \chi(x+s)$ for some $s \in \mathbb{F}_q$, find s. Here χ is the quadratic character of $\mathbb{F}_q$.*

Finding an efficient quantum algorithm for the Shifted Legendre Symbol Problem was originally posed as an open question by van Dam [48]. Damgard [18] has suggested using shifted Legendre and Jacobi sequences as pseudo-random bits. The seed to the pseudo-random number generator consists of s and p, and the output is the sequence $\left(\frac{s}{p}\right), \left(\frac{s+1}{p}\right), \ldots, \left(\frac{s+k}{p}\right)$, where k is bounded by some polynomial in $\log p$. He shows that if Legendre sequences are unpredictable in a very weak sense, then Jacobi sequences (defined similarly) are unpredictable in a very strong sense. The SLSP with unknown p is at least as hard as the shifted Legendre sequence problem in the sense that solving the SLSP results in s, and then the next bits can be computed. However, it is potentially much easier to solve, because adaptive attacks are possible.

Many papers have studied the properties of Legendre sequences, as referenced in [18, 42]. Peralta [42] examines the distributions of the Legendre sequences. A corollary related to the problem of proving an oracle lower bound for the SLSP is: for a fixed plus/minus sequence of length t, the number of occurrences of that sequence in $\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right)$ is in the range of $\frac{p}{2^t} \pm t(3 + \sqrt{p})$. So from an information theoretic viewpoint, the best

bounds currently known do not rule out an algorithm that queries $\log p$ consecutive values to reconstruct the offset.

7.2 An Algorithm for Prime Size Fields

In this section we give algorithms solving the Shifted Legendre Symbol Problem and variants when working over a finite field of prime size. The main ideas are contained in the algorithm for the Shifted Legendre Symbol Problem, and we can apply the same algorithm to solve the Shifted Jacobi Symbol Problem, and for the case when N is unknown.

The idea for the algorithm follows from a few known facts. Assume we start the algorithm in the standard way, i.e. by putting the function value in the phase to get $|f_s\rangle = \sum_{i \in \mathbb{Z}_p} \left(\frac{i+s}{p}\right) |i\rangle$. Assume the functions f_i are orthogonal (they are close to orthogonal). Define the matrix C where the i^{th} row is $|f_i\rangle$. Our quantum state $|f_s\rangle$ is one of the rows, so $C|f_s\rangle = |s\rangle$. The issue now is how to efficiently implement C. C is a circulant matrix, i.e. $c_{i,j} = c_{i+1,j+1}$. The Fourier transform diagonalizes a circulant matrix: $C = F_p(F_p^{-1} C F_p) F_p^{-1} = F_p D F_p^{-1}$, where D is diagonal, so we can implement C if we can implement D. It turns out that the vector on the diagonal of D is the vector $F_p|f_0\rangle$, but $|f_0\rangle$ is an eigenvector of the Fourier transform, so up to a global phase which we can ignore, we are done. To summarize: to implement C, we compute the Fourier transform, compute f_0 into the phases (this is just the Legendre Symbol), and then compute the Fourier transform again (it is not important whether we use F_p or F_p^{-1}). We will now present this algorithm step-by-step.

Algorithm 7.1 (Shifted Legendre Symbol Problem)

Input: *An odd prime p and a function f_s with $f_s(x) = \left(\frac{x+s}{p}\right)$.*

Output: *s.*

1. *Compute the Fourier transform over $\mathbb{Z}_p$ of $|0\rangle$ and compute f_s into the phases, approximating:*

$$\frac{1}{\sqrt{p-1}} \sum_{a \in \mathbb{F}_p} \left(\frac{a+s}{p}\right) |a\rangle$$

2. *Compute the Fourier transform over $\mathbb{Z}_p$, yielding:*

$$\frac{1}{\sqrt{p-1}} \sum_{b \in \mathbb{F}_p} \omega_p^{-bs} \left(\frac{b}{p}\right) |b\rangle$$

3. *Compute f_0 into the phases, approximating:*

$$\frac{1}{\sqrt{p}} \sum_{b \in \mathbb{F}_p} \omega_p^{-bs} |b\rangle$$

4. *Compute the Fourier transform over $\mathbb{Z}_p$; this gives the answer $|s\rangle$.*

Theorem 7.1 *Algorithm 7.1 solves the Shifted Legendre Symbol Problem in two queries and polynomial time with probability exponentially close to one.*

Proof: The first step is a standard setup used in quantum algorithms. The only difference is that f_s evaluates to zero in one position. In this case, just treat it as a one. After this the state is exponentially close to the state shown. Recall that the Legendre Symbol $\left(\frac{a}{p}\right)$ is zero when $p|a$, so one amplitude is zero.

The result of applying the Fourier transform is (where we replace a with $a - s$)

$$\frac{1}{\sqrt{p-1}} \sum_{a \in \mathbb{F}_p} \left(\frac{a+s}{p}\right) |a\rangle \longrightarrow \frac{1}{\sqrt{p-1}} \sum_{b \in \mathbb{F}_p} \frac{1}{\sqrt{p}} \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \omega_p^{b(a-s)} |b\rangle.$$

The sum b is over $\mathbb{F}_p^*$ since the Legendre Symbol is 1 for half the nonzero elements and -1 for the other half, so we can invert b. Factoring out the ω_p^{-bs} term, using the change of variable $c = ab$, and using the facts that $\left(\frac{cb^{-1}}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{b^{-1}}{p}\right)$ and $\left(\frac{b^{-1}}{p}\right) = \left(\frac{b}{p}\right)$ we have

$$\frac{1}{\sqrt{p-1}} \sum_{b \in \mathbb{F}_p} \left(\frac{b}{p}\right) \omega_p^{-bs} \left(\frac{1}{\sqrt{p}} \sum_{c \in \mathbb{F}_p} \left(\frac{c}{p}\right) \omega_p^{c} \right) |b\rangle$$

So we are left to evaluate $\sum_{c \in \mathbb{F}_p} \left(\frac{c}{p}\right) \omega_p^c$, which is the Gauss sum [13, 47], and is $\sqrt{p}$ if $p \equiv 1 \bmod 4$, and is $\sqrt{-1}\sqrt{p}$ if $p \equiv 3 \bmod 4$. Hence, up to a global constant which we can ignore, the state follows. ■

Corollary 7.1 *Algorithm 7.1 can be used to solve the Shifted Jacobi Symbol Problem.*

Proof: We start with the uniform superposition of $\mathbb{Z}_N$ and calculate the function value f_s for each element:

$$\frac{1}{\sqrt{N}} \sum_{a \in \mathbb{Z}_N} |a, 0\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{a \in \mathbb{Z}_N} |a, \left(\tfrac{a+s}{N}\right)\rangle.$$

Next, we measure if the rightmost value is nonzero. If this is the case, which happens with probability $\phi(N)/N$ (where ϕ is Euler's phi-function obeying $\phi(N) = |\mathbb{Z}_N^*|$), the state has collapsed to the superposition:

$$\frac{1}{\sqrt{\phi(N)}} \sum_{a \in \mathbb{Z}_N^*} |a, \left(\tfrac{a+s}{N}\right)\rangle.$$

Otherwise, we simply try the same procedure again. (The success probability $\phi(N)/N$ has a lower bound of $\Omega(1/\log(\log N))$, see [3], hence we can expect to be successful after $O(\log(\log N))$ trials.)

We continue with the reduced state by changing the phase of $|a\rangle$ to $\left(\frac{a+s}{N}\right)$ and

computing the function value again, giving

$$\frac{1}{\sqrt{\phi(N)}} \sum_{a \in \mathbb{Z}_N} \left(\frac{a+s}{N}\right) |a\rangle.$$

Let $N = p_1 \cdot p_2 \cdots p_k$ be the prime decomposition of N such that $\mathbb{Z}_N = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$. Since $\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right)$, we can just consider each p_j component separately (with $s_1 \equiv s \bmod p_1$, $s_2 \equiv s \bmod p_2$, and so on). Hence, by performing the 'inverse Chinese remainder' map $|a\rangle \longrightarrow |a \bmod p_1, \ldots, a \bmod p_k\rangle$, we obtain the state

$$\sum_{a_1 \in \mathbb{Z}_{p_1}} \cdots \sum_{a_k \in \mathbb{Z}_{p_k}} \left(\frac{a_1+s_1}{p_1}\right) \cdots \left(\frac{a_k+s_k}{p_k}\right) |a_1, \ldots, a_k\rangle = \bigotimes_{j=1}^{k} \sum_{a_j \in \mathbb{Z}_{p_j}} \left(\frac{a_j+s_j}{p_j}\right) |a_j\rangle.$$

But now we use Algorithm 7.1 on each factor to get $|s_1, \ldots, s_k\rangle$, after which the Chinese remainder theorem gives us the answer s. ■

We now give an algorithm for the case when N is unknown. In addition to using known techniques, the algorithm depends on the fact that sampling the Fourier transform of the shifted Legendre Symbol results in the uniform distribution.

Algorithm 7.2 (Shifted Jacobi Symbol Problem, unknown N)

Input: *An integer M and a function $f_s : \{0, \ldots, M-1\} \to \{-1, 0, 1\}$ such that $f_s(x) = \left(\frac{x+s}{N}\right)$ for some integer N, with $N^2 < M$*

Output: *N and s.*

1. *Create the following state as in Corollary 7.1:*

$$c \cdot \sum_{x=0}^{M-1} \left(\frac{x+s}{N}\right) |x\rangle$$

2. *Compute the Fourier transform over $\mathbb{Z}_M$.*

3. Measure, with outcome i, and use continued fractions on i and M, returning j/N.

4. Run Algorithm 7.1 using f_s and N.

Theorem 7.2 *Algorithm 7.2 solves the Shifted Jacobi Symbol Problem with unknown N with high probability.*

Proof: Let $|\psi_s\rangle = \frac{1}{\sqrt{\phi(N)}} \sum_{x=0}^{N-1} \left(\frac{x+s}{N}\right) |x\rangle$ be the state after the setup in Corollary 7.1, and let $|\tilde{\psi}_s\rangle = c \sum_{x=0}^{M-1} \left(\frac{x+s}{N}\right)$ be the repeated version in Algorithm 7.2, where c is the normalizing constant. We can relate the distributions induced by Fourier sampling $|\phi_s\rangle$ and $|\tilde{\phi}_s\rangle$ using Corollary 5.5. If $M = N$, then Lemma 7.1 implies that i is uniformly distributed over $\mathbb{Z}_N^*$, and we would be done since the denominator returned by continued fractions is N in this case. However, this will still be the case even if $M \neq N$. If M is a multiple of N and if the Fourier transform of $|\psi_s\rangle$ is $\sum_{x=0}^{N-1} \alpha_x |x\rangle$, then the Fourier transform of $|\tilde{\psi}_s\rangle$ is $\sum_{x=0}^{N-1} \alpha_x |M/N \cdot x\rangle$, and N can be computed from samples. If M is any integer which is large enough compared to N, the distributions are ϵ-close by Corollary 5.5. ■

Lemma 7.1 *Let N be an odd squarefree integer. If we apply the quantum Fourier transform over $\mathbb{Z}_N$ to the superposition of the states $\left(\frac{x+s}{N}\right) |x\rangle$ for all $x \in \mathbb{Z}_N$, we have*

$$\frac{1}{\sqrt{\phi(N)}} \sum_{x \in \mathbb{Z}_N} \left(\frac{x+s}{N}\right) |x\rangle \quad \xrightarrow{F_{N_1}} \quad \frac{\sum_{z \in \mathbb{Z}_N} \left(\frac{z}{N}\right) \omega_N^z}{\sqrt{N \cdot \phi(N)}} \sum_{y \in \mathbb{Z}_N} \omega_N^{-sy} \left(\frac{y}{N}\right) |y\rangle.$$

Proof: First, we note that we can rewrite the output as

$$\frac{1}{\sqrt{N \cdot \phi(N)}} \sum_{y \in \mathbb{Z}_N} \sum_{x \in \mathbb{Z}_N} \left(\frac{x+s}{N}\right) \omega_N^{xy} |y\rangle \quad = \quad \frac{1}{\sqrt{N \cdot \phi(N)}} \sum_{y \in \mathbb{Z}_N} \omega_N^{-sy} \left[\sum_{x \in \mathbb{Z}_N^*} \left(\frac{x}{N}\right) \omega_N^{xy} \right] |y\rangle,$$

by substituting x with $x + s$ in the summation and using the fact that $\left(\frac{x}{N}\right) = 0$ for all $x \notin \mathbb{Z}_N^*$.

The amplitudes between the square brackets depend on y in the following way. If y is coprime to N, then

$$\sum_{x \in \mathbb{Z}_N^*} \left(\frac{x}{N}\right) \omega_N^{xy} \quad = \quad \left(\frac{y^{-1}}{N}\right) \sum_{z \in \mathbb{Z}_N^*} \left(\frac{z}{N}\right) \omega_N^{z},$$

where we used the substitution $x = zy^{-1}$ and the multiplicativity of the Jacobi symbol.

Suppose N and y have a common, nontrivial, factor f. Let $N = mf$ and $y = rf$. By the Chinese remainder theorem, there is a bijection between the elements $x \in \mathbb{Z}_N$ and the coordinates $(x \bmod m, x \bmod f) \in \mathbb{Z}_m \times \mathbb{Z}_f$, which also establishes a one-to-one mapping between $\mathbb{Z}_N^*$ and $\mathbb{Z}_m^* \times \mathbb{Z}_f^*$. This allows us to rewrite the expression as follows.

$$\begin{aligned} \sum_{x \in \mathbb{Z}_N^*} \left(\frac{x}{N}\right) \omega_N^{xy} \quad &= \quad \sum_{x \in \mathbb{Z}_{mf}^*} \left(\frac{x}{mf}\right) \omega_{mf}^{xrf} \\ &= \quad \sum_{x_1 \in \mathbb{Z}_m^*} \left(\frac{x_1}{m}\right) \omega_m^{x_1 r} \sum_{x_2 \in \mathbb{Z}_f^*} \left(\frac{x_2}{f}\right). \end{aligned}$$

Because f is odd and squarefree $\sum_{x \in \mathbb{Z}_f^*} \left(\frac{x}{f}\right) = 0$, and hence the above term equals zero. This concludes the proof of the lemma. ■

7.3 An Algorithm for General Finite Fields

Here will solve the general case of the Shifted Legendre Symbol Problem for a finite field $\mathbb{F}_q$. From now on $q = p^r$, with p an odd prime, and the degree r an integer. Field elements are polynomials and are computed modulo some irreducible polynomial of degree r. We will write a to mean $\sum_{i=0}^{r-1} a_i x^i$. The actual representation is just $|a\rangle = |a_{r-1}, \ldots, a_0\rangle$.

Lemma 7.2 (Trace-Fourier Transform over $\mathbb{F}_q$) *The unitary mapping*

$$|a\rangle \longrightarrow \frac{1}{\sqrt{q}} \sum_{b \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(ab)} |b\rangle$$

is computable in polynomial time.

Proof: First apply the map

$$|a\rangle \longrightarrow \bigotimes_{j=0}^{r-1} |\mathrm{Tr}(ax^j)\rangle,$$

and then compute the Fourier transform over $\mathbb{Z}_p^r$. This gives us the final state

$$\bigotimes_{j=0}^{r-1} \frac{1}{\sqrt{p}} \sum_{b_j \in \mathbb{F}_p} \omega_p^{\mathrm{Tr}(ax^j)b_j} |b_j\rangle = \frac{1}{\sqrt{q}} \sum_{b \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(ab)} |b\rangle.$$

Now we will show how to compute the map above. First we will show that the map

$$|a\rangle \longrightarrow |\mathrm{Tr}(a), \mathrm{Tr}(ax), \ldots, \mathrm{Tr}(ax^{r-1})\rangle$$

is reversible. Let $T(a) = [\mathrm{Tr}(a), \mathrm{Tr}(ax), \ldots, \mathrm{Tr}(ax^{r-1})]$. T is a linear functional since Tr is, so if $T(a) = T(b)$ then $T(a-b)$ is the zero vector. We will show that $T(a)$ is not the zero vector except for $a = 0$. Suppose $T(a)$ is the zero vector. Since Tr is not the zero map, choose $b \in \mathbb{F}_q$ such that $\mathrm{Tr}(b) \neq 0$. Choose $c_0, \ldots, c_{r-1}$ such that $\sum_i c_i a x^i = b$. Then $\mathrm{Tr}(b) = \mathrm{Tr}(\sum_i c_i a x^i) = \sum_i c_i \mathrm{Tr}(ax^i) = 0$, since $\mathrm{Tr}(ax^i) = 0$ for all i. But this is a contraction by the choice of b. So T is 1-1.

We will now show that the map is computable in polynomial time. It is enough if a can be computed from $\mathrm{Tr}(a), \mathrm{Tr}(ax), \ldots, \mathrm{Tr}(ax^{r-1})$. But the equations $\mathrm{Tr}(a) = \sum_{j=0}^{r-1} a_j \mathrm{Tr}(x^j)$, $\mathrm{Tr}(ax) = \sum_{j=0}^{r-1} a_j \mathrm{Tr}(x^{j+1})$, $\ldots$, $\mathrm{Tr}(ax^{r-1}) = \sum_{j=0}^{r-1} a_j \mathrm{Tr}(x^{j+r-1})$ are r linear equations in r unknowns, and the values $\mathrm{Tr}(a), \mathrm{Tr}(ax), \ldots, \mathrm{Tr}(ax^{r-1})$ and $\mathrm{Tr}(x^j)$ for all j are known, so the coefficients a_j of a can be solved for using linear algebra. ■

Notice that the only properties of Tr used are that it is a linear functional, and that it could be computed efficiently. We can now give the algorithm for the general finite field case.

Algorithm 7.3

Input: *A power of a prime $q = p^r$ and a function f_s such that $f_s(x) = \chi(x+s)$.*

Output: *s.*

1. *Compute the Fourier transform over $\mathbb{Z}_p^r$ of $|0\rangle$ and compute the function value f_s into the phases, approximating:*

$$\frac{1}{\sqrt{q-1}} \sum_{a \in \mathbb{F}_q} \chi(a+s)|a\rangle.$$

2. *Compute the Trace-Fourier transform of Lemma 7.2 over $\mathbb{F}_q$, yielding:*

$$\frac{1}{\sqrt{q-1}} \sum_{b \in \mathbb{F}_q} \chi(b)\omega_p^{\mathrm{Tr}(-sb)}|b\rangle.$$

3. *Uncompute the phases $\chi(b)$ for $b \neq 0$, approximating:*

$$\frac{1}{\sqrt{q}} \sum_{b \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(-sb)}|b\rangle.$$

4. *Compute the inverse Trace-Fourier transform over $\mathbb{F}_q$. This gives us the requested shift parameter as $|-s\rangle$.*

Theorem 7.3 *Algorithm 7.3 solves the Shifted Quadratic Character Problem over any finite field with two queries and in polynomial time with probability exponentially close to one.*

Proof: The proof is the same as the proof of Theorem 7.1. At step 2, we perform the Trace-Fourier transform to the state, yielding

$$\frac{1}{\sqrt{q-1}} \sum_{a \in \mathbb{F}_q} \chi(a+s)|a\rangle \longrightarrow \frac{1}{\sqrt{q-1}} \sum_{b \in \mathbb{F}_q} \frac{1}{\sqrt{q}} \sum_{a \in \mathbb{F}_q} \chi(a)\omega_p^{\mathrm{Tr}(b(a-s))}|b\rangle.$$

The sum b is over $\mathbb{F}_q^*$ since the quadratic character is 1 for half the nonzero elements and -1 for the other half, so we can invert b. Factoring out the $\omega_p^{\mathrm{Tr}(-bs)}$ term, using the change of variable $c = ab$, and using the facts that $\chi(cb^{-1}) = \chi(c)\chi(b^{-1})$ and $\chi(b^{-1}) = \chi(b)$ we have

$$\frac{1}{\sqrt{q-1}} \sum_{b \in \mathbb{F}_q} \chi(b) \omega_p^{\mathrm{Tr}(-bs)} \left(\frac{1}{\sqrt{q}} \sum_{c \in \mathbb{F}_q} \chi(c) \omega_p^{\mathrm{Tr}(c)} \right) |b\rangle$$

So we are left to evaluate $\sum_{c \in \mathbb{F}_q} \chi(c) \omega_p^{\mathrm{Tr}(c)}$, which is the Gauss sum [13, 47], and is $\sqrt{p}$ if $p \equiv 1 \bmod 4$ and is $\sqrt{-1}\sqrt{p}$ if $p \equiv 3 \bmod 4$. Hence, up to a global constant which we can ignore, the state follows. ■