Calculating Square Roots in $\mathbb{F}_{p^2}$

I present an exposition of the calculation of square roots in $\mathbb{F}_{p^2}$, where p is a prime with $p \equiv -1 \pmod 4$, and $\mathbb{F}_{p^2}$ is defined as $\frac{\mathbb{F}_p[i]}{i^2+1}$, so that elements of $\mathbb{F}_{p^2}$ are of the form $x + iy$, with $i^2 = -1$ and $x, y \in \mathbb{F}_p$.

Definition 1. For $a \in \mathbb{F}_p$, define the function $L : \mathbb{F}_p \to \mathbb{F}_p$ as follows:

$$L(a) = \begin{cases} 1 & a \text{ is a non-zero square in } \mathbb{F}_p, \\ -1 & a \text{ is not a square in } \mathbb{F}_p, \\ 0 & a \equiv 0 \pmod p. \end{cases}$$

That is, $L(a) = (\frac{a}{p})$, the Legendre symbol on p.

Recall the following elementary fact (which we can treat as an alternative definition of L):

Fact. *For all $a \in \mathbb{F}_p$, $L(a) \equiv a^{\frac{p-1}{2}} \pmod p$.*

Remark. Note that $L(-1) \equiv -1 \pmod p$ by definition of p, and thus $\mathbb{F}_{p^2}$ really is a quadratic extension of $\mathbb{F}_p$, as -1 has no square root in $\mathbb{F}_p$.

We also define the following function.

Definition 2. For $a \in \mathbb{F}_p$, define the function $K : \mathbb{F}_p \to \mathbb{F}_p$ by $L(a) \equiv a^{\frac{p+1}{4}} \pmod p$

Lemma 3. *K has the following properties:*

- $K(a) \equiv 0 \pmod p$ *if and only if* $a \equiv 0 \pmod p$.
- $K(a)^2 \equiv aL(a) \pmod p$.
- $K(a^2) \equiv aL(a) \pmod p$.

Proof. The first property is trivial. For the second and third properties, simply note that $aL(a) \equiv aa^{\frac{p-1}{2}} \equiv a^{\frac{p+1}{2}} \equiv (a^2)^{\frac{p+1}{4}} \equiv (a^{\frac{p+1}{4}})^2 \pmod p$. □

Remark. K, of course, is a square root function for quadratic residues on $\mathbb{F}_p$, but we can define it over all of $\mathbb{F}_p$.

We now prove constructively a necessary and sufficient condition for $s \in \mathbb{F}_{p^2}$ having a square root, and from that derive an algorithm for the calculation of square roots in $\mathbb{F}_{p^2}$.

Theorem 4. *Let s be a member of $\mathbb{F}_{p^2}$, with $s = x + iy$, with $x, y \in \mathbb{F}_p$. Then there exists an $r \in \mathbb{F}_{p^2}$ such that $r^2 = s$ if and only if $L(x^2 + y^2) \neq -1$.*

Proof. Suppose there exists such an r, and say $r = \alpha + i\beta$, with $\alpha, \beta \in \mathbb{F}_p$. Then $r^2 = (\alpha^2 - \beta^2) + i(2\alpha\beta)$, and so we must have $x = \alpha^2 - \beta^2$ and $y = 2\alpha\beta$.

Define $\bar{r} = \alpha - i\beta$. Then

$$\bar{r}^2 = (\alpha^2 - \beta^2) - i(2\alpha\beta) = x - iy.$$

Note that $r\bar{r} = \alpha^2 + \beta^2$. It follows that

$$(\alpha^2 + \beta^2)^2 = (r\bar{r})^2 = r^2\bar{r}^2 = (x + iy)(x - iy) = x^2 + y^2.$$

This shows that $x^2 + y^2$ is a square, and thus $L(x^2 + y^2) \neq -1$.

Conversely, suppose $L(x^2 + y^2) \neq -1$.

Suppose firstly that $L(x^2 + y^2) = 0$. This happens just when $x^2 + y^2 \equiv 0 \pmod{p}$, and so $y^2 \equiv x^2 \pmod{p}$. Suppose, in that case, that $x \not\equiv 0 \pmod{p}$. Then it follows that $\frac{y}{x}^2 \equiv -1 \pmod{p}$. However, $L(-1) = -1$, so this is a contradiction, and thus $x \equiv 0 \pmod{p}$. It follows that $y^2 \equiv 0 \pmod{p}$, and thus $y \equiv 0 \pmod{p}$. As such, $s = 0 + i0$. Set $r = 0 + i0$ also: then $r^2 = s$, trivially.

So now suppose $L(x^2 + y^2) = 1$. This means that at least one of x and y is non-zero modulo p, as otherwise we would have $L(x^2 + y^2) = 0$.

Thus far, so elementary - but now we reach the fiddly part. Let $w = x + K(x^2 + y^2)$. Can it be true that $w \equiv 0 \pmod{p}$? The Reference Implementation assumes not, but this is not so.

$w \equiv 0 \pmod{p} \implies -x \equiv \pmod{p} \implies x^2 \equiv K(x^2 + y^2)^2 \equiv (x^2 + y^2)L(x^2 + y^2) \equiv x^2 + y^2 \pmod{p}$. It follows that $y \equiv 0 \pmod{p}$, and thus $-x \equiv K(x^2) \pmod{p}$ - and so $L(x) = -1$, as $K(x^2) \equiv xL(x) \pmod{p}$ - thus, x is a quadratic non-residue in $\mathbb{F}_p$. This is exactly the case where s is a quadratic non-residue in $\mathbb{F}_p$ (and hence we would expect its square root to be purely "imaginary").

Now consider $w' = x - K(x^2 + y^2)$. When is $w' \equiv 0 \pmod{p}$? An identical argument shows that it is when $y \equiv 0 \pmod{p}$ and x is a quadratic residue in $\mathbb{F}_p$ (non-zero by our assumption) - which corresponds to s being a quadratic residue in $\mathbb{F}_p$ (and hence having a purely "real" root).

It follows, then, that we can never have $w \equiv w' \equiv 0 \pmod{p}$. That motivates the following definition: let

$$u \equiv \frac{x + tK(x^2 + y^2)}{2},$$

where $t \in 1, -1$ is chosen such that $u \not\equiv 0 \pmod{p}$. Specifically, if $w \not\equiv 0 \pmod{p}$, $u = \frac{w}{2}$, and otherwise $u = \frac{w'}{2}$.

Let $\alpha = K(u)$. $\alpha^2 \equiv uL(u) \pmod{p}$, and so it follows that $\alpha \not\equiv 0 \pmod{p}$ either. Let $\beta = \frac{y\alpha}{2u}$. Then $\beta \equiv \frac{y\alpha^2}{2u\alpha} \equiv \frac{yuL(u)}{2u\alpha} \equiv y\frac{L(u)}{2\alpha} \pmod{p}$, and so it follows that $2\alpha\beta \equiv yL(u) \pmod{p}$.

Note that $L(u)^2 = 1$. It follows that we have $2\alpha^2 L(u) \equiv 2u \pmod{p}$, and hence the following equivalence holds:

$$(2\alpha^2 L(u) - x)^2 \equiv (2u - x)^2 \equiv t^2 K(x^2 + y^2)^2 \equiv (x^2 + y^2)L(x^2 + y^2) \pmod{p}.$$

Thus, by the assumption, we have $(2\alpha^2 L(u) - x)^2 \equiv x^2 + y^2 \pmod{p}$.

Expanding and cancelling the x^2 from both sides, we get $4\alpha^4 - 4\alpha^2 L(u)x \equiv y^2 \pmod{p}$.

Thus, rearranging, we get that $xL(u) \equiv \alpha^2 - \frac{y^2}{4\alpha^2} \equiv \alpha - \frac{y}{2\alpha}^2 \equiv \alpha^2 - \frac{yL(u)}{2\alpha}^2 \equiv \alpha^2 - \beta^2$.

Now, $(\alpha + i\beta)^2 = \alpha^2 - \beta^2 + i2\alpha\beta = L(u)(x + iy) = L(u)s$, where equality here is over $\mathbb{F}_{p^2}$ and thus modulo p. Similarly, $(\beta - i\alpha)^2 = \beta^2 - \alpha^2 - i2\alpha\beta = -L(u)s$.

Thus, if $\alpha^2 \equiv u \pmod{p}$, $L(u) = 1$, and thus if we set $r = \alpha + i\beta$, $r^2 = s$. If $\alpha^2 \not\equiv u \pmod{p}$, then in fact $\alpha^2 \equiv -u \pmod{p}$, $L(u) = -1$, and so it will follow that if we set $r = \beta - i\alpha$, $r^2 = s$. This proves the result. □

Remark. We may slightly simplify the last part. If we set $\beta' = \frac{y}{2\alpha}$, then:

- In the $L(u) = 1$ case, $\beta' = \beta$ and thus $r = \alpha + i\beta'$.
- In the $L(u) = -1$ case, $\beta' = -\beta$, and thus $r = -\beta' - i\alpha$. But then $r' = \beta' + i\alpha$ is also a square root of s.

As such, if we set $\alpha = K(u)$, $\beta = \frac{y}{2\alpha}$, then:

- If $\alpha^2 \equiv u \pmod{p}$, $\alpha + i\beta$ is a square root of s.
- Otherwise, $\beta + i\alpha$ is a square root of s.

There is, as we have seen here, some slightly ambiguity about what "the" square root of s should be, and what the SIKE specification [] *does* do is define this.

Definition 5. Suppose $s \in \mathbb{F}_{p^2}$ and there exists some $r = \alpha + i\beta \in \mathbb{F}_{p^2}$ with $r^2 = s$, with α and β considered as integers in $[0, p-1]$.

Then define

$$\sqrt{s} = \begin{cases} r & \alpha \neq 0, \alpha \equiv 0 \mod 2, \\ r & \alpha = 0, \beta \equiv 0 \mod 2, \\ -r & \text{otherwise.} \end{cases}$$

All of this suggests the following algorithm. In the following, all members of $\mathbb{F}_p$ are considered as elements of $[0, p-1]$, with equality modulo p.

Algorithm 1: An algorithm for calculating square roots in $\mathbb{F}_{p^2} = \frac{\mathbb{F}_p[i]}{i^2+1}$, where p is a prime and $p \equiv -1 \pmod 4$.

Input: An element $s = x + iy$ of $\mathbb{F}_{p^2}$, with $x, y \in \mathbb{F}_p$, such that there exists some $r \in \mathbb{F}_{p^2}$, $r^2 = s$. We may check if s is a valid input by checking that $(x^2 + y^2)^{\frac{p-1}{2}} \not\equiv -1 \pmod p$.

Output: $\sqrt{s}$, as defined above.

if $x = 0$ **and** $y = 0$ **then**
- $\alpha \leftarrow 0$
- $\beta \leftarrow 0$

else
- $t_0 \leftarrow (x^2 + y^2)^{\frac{p+1}{4}}$
- $u \leftarrow \frac{x+t_0}{2}$
- **if** $u = 0$ **then**
  - $u \leftarrow u - t_0$
- $\alpha \leftarrow u^{\frac{p+1}{4}}$
- $\beta \leftarrow \frac{y}{2\alpha}$
- **if** $\alpha^2 \neq u$ **then**
  - $t_1 \leftarrow \alpha$
  - $\alpha \leftarrow \beta$
  - $\beta \leftarrow t_1$
- **if** $\alpha \equiv 1 \pmod 2$ **or** $(\alpha = 0$ **and** $\beta \equiv 1 \pmod 2)$ **then**
  - $\alpha \leftarrow -\alpha$
  - $\beta \leftarrow -\beta$

return $\alpha + i\beta$

Lemma 6. *Algorithm 1 calculates* $\sqrt{s}$ *as claimed.*

Proof. Follows from the theorem, the remark which follows it, and the definition of $\sqrt{s}$. □