Proof. By Theorem 4.3, the result holds for $q \geq 194$. For $q < 194$ and $q \equiv 1 \pmod 6$, we first look at $q = 7$ and $q = 13$. When $q = 7$, one has $x^6 = 1$ for all $x \in \mathbb{F}_7^\times$. But $g^2 + g + 1 \neq 0$ for any primitive root g of $\mathbb{F}_7$. So it is not solvable in this case. For $q = 13$, $x^6 = \pm 1$ for all $x \in \mathbb{F}_{13}^\times$. It is easy to check that $g^2X^6 + gY^6 + 1 = 0$ is not solvable for all primitive roots $g = 2, 6, 7, 11$ of $\mathbb{F}_{13}$. For the rest of cases that $13 < q < 194$, the following table gives a solution for some primitive root g:

q	19	25	31	37	43	49	61	67	73	79	97	103
g	2	α	3	2	3	β	2	2	5	3	5	5
X	1	α^3	19	2	1	β^3	24	4	1	6	5	5
Y	2	α	27	1	28	β^3	4	43	59	6	29	32

q	109	121	127	139	151	157	163	169	181	193
g	6	γ	3	2	6	5	2	κ	2	5
X	16	γ^7	84	2	1	22	8	1	86	1
Y	26	γ^4	3	103	132	82	1	κ^2	148	127

where $\alpha = 3 + \sqrt{2}$ in $\mathbb{F}_{25} = \mathbb{F}_5(\sqrt{2})$, $\beta = 4 + \sqrt{-1}$ in $\mathbb{F}_{49} = \mathbb{F}_7(\sqrt{-1})$, $\gamma = 2 + \sqrt{2}$ in $\mathbb{F}_{121} = \mathbb{F}_{11}(\sqrt{2})$ and $\kappa = 7 + 2\sqrt{2}$ in $\mathbb{F}_{169} = \mathbb{F}_{13}(\sqrt{2})$. $\square$

5. Application: Conflict-Avoiding Codes of Weight 3

In this section, we apply our main result to the construction of CAC. We consider the special case where $q = p$ and $\ell = \ell_0$ the index of H in $\mathbb{F}_p^\times$. Let's start with a proof of Corollary B.

Proof. Let p be a prime such that the multiplicative order $o_p(2)$ of 2 is not a multiple of 4. Suppose that p satisfies the condition

$$p \geq (2^{\omega(\ell_0)}(\ell_0 - 3 - \delta) + 2)^2 - 2$$

where $\delta = 1$ if $4 \mid \ell_0$ and $\delta = 0$ otherwise. It follows from Theorem A that there exists a generator g of $\mathbb{F}_p^\times$ such that Equation (2) is solvable over $\mathbb{F}_p$. By Corollary 2.3 for $1 \leq \ell_0 \leq 4$ and Lemma 2.1 for $\ell_0 \geq 5$, we see that there exists a solution $(x, y) \in \mathbb{F}_p^2$ to Equation (2) satisfying $xy \neq 0$. Thus, Conjecture C and hence Conjecture B holds for prime numbers p satisfying the inequality given above. As it is explained in Section 1, Conjecture A is also true for these prime numbers. Combining the algorithm given in [FLS14], we conclude that an optimal CAC of length p and weight 3 has the size

$$M(p, \ell_0) = \frac{p - 1 - 2\ell_0}{4} + \left\lfloor \frac{\ell_0}{3} \right\rfloor$$

as desired. $\square$

Our strategy for studying the size of optimal CAC of prime lengths is through investigating Conjecture B (equivalently, Conjecture C). In the paper [MZS14] the authors