Conjecture C. Let p be an odd prime. If $\ell_0 \geq 3$, then there is a generator g of $\mathbb{F}_p^\times$ such that the diagonal equation

$$g^2X^{\ell_0} + gY^{\ell_0} + 1 = 0 \tag{2}$$

is solvable over $\mathbb{F}_p$.

The formulation in Conjecture C has the advantage that the number of $\mathbb{F}_p$-rational solutions to Equation (2) can be computed in terms of certain character sums which have been well studied in number theory. By establishing valid cases in Conjecture C, we also obtain the cases where Conjecture B as well as Conjecture A are true. Therefore, by studying the solvability of Equation (2) over $\mathbb{F}_p$, we are able to provide new results to the construction of optimal CACs.

Motivated by Conjecture C, instead of working on the diagonal equations as (2) over the prime field $\mathbb{F}_p$ and the specific exponent ℓ_0, we will look at general situations by taking the base field to be a finite extension of $\mathbb{F}_p$ and the exponent in the equation is allowed to be more general than ℓ_0. Let q be a prime power and ℓ be a proper divisor of $q-1$. We consider the solvability of the following diagonal equation

$$g^2X^{\ell} + gY^{\ell} + 1 = 0 \tag{3}$$

over a finite field $\mathbb{F}_q$ of q elements, where g is a generator of the multiplicative group $\mathbb{F}_q^\times$ of $\mathbb{F}_q$. In view of Conjecture C, we're interested in whether or not there exists a generator g such that Equation (3) has a $\mathbb{F}_q$-rational solution. However, the answer can be false for divisors of $q-1$ other than ℓ_0. For example, in the case where $(q,\ell) = (13,6), (23,11)$ there does not exist any generator of $\mathbb{F}_q^\times$ such that (3) has a $\mathbb{F}_q$-rational solution. On the other hand, as a consequence of our main result below, Equation (3) does have a $\mathbb{F}_q$-rational solution for some generator g of $\mathbb{F}_q^\times$ provided that $q \geq 19$ if $\ell = 6$ and $q \geq 322$ if $\ell = 11$. Our first main result is to give a lower bound for q such that Equation (3) has a $\mathbb{F}_q$-rational solution for some generator g of $\mathbb{F}_q^\times$.

Theorem A (= Theorem 4.3)**.** *Let q be a prime power and let ℓ be a proper divisor of $q-1$. If*

$$q \geq (2^{\omega(\ell)}(\ell - 3 - \delta) + 2)^2 - 2$$

where $\omega(\ell)$ is the number of distinct prime divisors of ℓ and

$$\delta = \begin{cases} 1 & \textit{if } 4 \mid \ell, \\ 0 & \textit{otherwise,} \end{cases}$$

then there is a generator g of $\mathbb{F}_q^\times$ such that Equation (3) is solvable over $\mathbb{F}_q$.

Remark 1.2. It follows from the Hasse-Weil bound (see Theorem 1) that the number of $\mathbb{F}_q$-rational solutions to Equation (3) is bounded below by $q + 1 - 2\mathfrak{g}_\ell\sqrt{q}$ where $\mathfrak{g}_\ell = (\ell - 1)(\ell - 2)/2$ is the genus of the curve defined by (3) over $\mathbb{F}_q$. As a result, Equation (3) has a $\mathbb{F}_q$-rational solution for any $g \in \mathbb{F}_q^\times$ provided that $q > (\ell-1)^2(\ell-2)^2$. It is reasonable to expect that this lower bound can be improved under the weaker condition given in