**Notes on Number Theory and Discrete Mathematics**
**Print ISSN 1310–5132, Online ISSN 2367–8275**
**Vol. 25, 2019, No. 1, 75–83**
**DOI: 10.7546/nntdm.2019.25.1.75-83**

# Complete solving the quadratic equation mod $2^n$

**S. M. Dehnavi[1], M. R. Mirzaee Shamsabad[2] and A. Mahmoodi Rishakani[3]**

[1] Department of Mathematical and Computer Sciences
University of Kharazmi, Tehran, Iran
e-mail: dehnavism@ipm.ir

[2] Department of Mathematics
Shahid Beheshti University, Tehran, Iran
e-mail: m_mirzaee@sbu.ac.ir

[3] Department of Sciences
Shahid Rajaee Teacher Training University, Tehran, Iran
e-mail: am.rishakani@sru.ir

**Received:** 24 December 2017 **Accepted:** 24 December 2018

**Abstract:** Quadratic functions have applications in cryptography. In this paper, we investigate the modular quadratic equation

$$ax^2 + bx + c = 0 \quad (mod\ 2^n),$$

and provide a complete analysis of it. More precisely, we determine when this equation has a solution and in the case that it has a solution, we give not only the number of solutions, but also the set of solutions, in $O(n)$ time. One of the interesting results of our research is that, if this equation has a solution, then the number of solutions is a power of two. Most notably, as an application, we characterize the number of fixed-points of quadratic permutation polynomials over $\mathbb{Z}_{2^n}$, which are used in symmetric cryptography.

**Keywords:** Quadratic equation mod $2^n$, Number of solutions, Set of solutions, Number of fixed-points, Cryptography.
**2010 Mathematics Subject Classification:** 11Z05, 14G50.

# 1 Introduction

The square mapping is one of the tools which is used in cryptography. For instance, the Rabin cryptosystem [6] employs a modular quadratic mapping. As another example, in the design of the stream cipher Rabbit [1], the square map is used. A quadratic polynomial modulo $2^{32}$ is used in the AES finalist block cipher RC6 [5].

The quadratic equation has been solved over various algebraic structures. For example, the quadratic equation over $\mathbb{F}_{2^n}$ is solved in Theorem 3.2.15 of [3]. Note that an algorithm for finding the solutions of quadratic equation over $\mathbb{F}_{2^n}$ is also given in [8]. This research is not the first one concerning the quadratic equation mod $2^n$. For instance, [7] gives the solutions of equation (1) in spacial cases.

In this paper, we examine the quadratic equation mod $2^n$. We verify when this equation has a solution and, in the case that it has a solution, we give the number of solutions as well as the set of its solutions in $O(n)$ time. As an application for symmetric cryptography, we characterize the number of fixed-points of quadratic permutation polynomials over $\mathbb{Z}_{2^n}$.

In section 2, we give the preliminary notations and definitions. Section 3 is devoted to the main theorems of the paper which solve the modular quadratic equation mod $2^n$, completely, and presents its number of solutions along with its set of solutions. In section 4, we conclude the paper.

# 2 Notations and definitions

We denote the well-known ring of integers mod $2^n$ by $\mathbb{Z}_{2^n}$. For every nonzero element $a \in \mathbb{Z}_{2^n}$, we define $p_2(a)$ as the greatest power of 2 that divides $a$. The odd part of $a$ or $\dfrac{a}{2^{p_2(a)}}$ is denoted by $o_2(a)$, in the current paper. Note that, we define $p_2(0) := n$.

The number of elements (cardinal) of a finite set $R$ is denoted by $|R|$. For a function $f : R \to S$, the preimage of an element $b \in S$ is defined as $\{a \in R | b = f(a)\}$ and is denoted by $f^{-1}(b)$. If $f(x) = x$ for some $x \in R$, then $x$ is called a fixed-point of $f$. The $i$-th bit of a natural number $x$ in its binary representation is denoted by $[x]_i$. For an integer $j$, we define $e_j$ as follows

$$e_j = \begin{cases} 0, & j \text{ odd}, \\ 1, & j \text{ even}. \end{cases}$$

A mapping

$$f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n},$$
$$f(x) = ax^2 + bx + c \ \ (mod \ \ 2^n),$$

is called a quadratic polynomial over $\mathbb{Z}_{2^n}$. When $f$ is a permutation, it is called a quadratic permutation polynomial over $\mathbb{Z}_{2^n}$.

Let $(G, *)$ be a group and $\varphi : G \to G$ be a group endomorphism. We denote the kernel of $\varphi$ by $ker(\varphi)$ and the image of $\varphi$ by $Im(\varphi)$.

## 3 Solving the quadratic equation mod $2^n$

In this section, we study the modular quadratic equation

$$ax^2 + bx + c = 0 \quad (mod\ 2^n), \tag{1}$$

and wish to solve it. More precisely, we want to determine:

a) whether (1) has a solution;

b) if it has a solution, then what is the number of its solutions;

c) the set of its solutions.

In the sequel, we note that $x = 0$ is equivalent to $p_2(x) = n$.

**Lemma 3.1.** *Let $a$, $b$, and $c$ be even and $t = min\{p_2(a),\ p_2(b),\ p_2(c)\}$. Set $A = \frac{a}{2^t}$, $B = \frac{b}{2^t}$, and $C = \frac{c}{2^t}$. Consider the equations (1) and*

$$Ax^2 + Bx + C = 0 \quad (mod\ 2^{n-t}). \tag{2}$$

*Let $N_1$ and $N_2$ be the number of solutions of (1) and (2), respectively. Also, let $\{x_1, \ldots, x_{N_2}\}$ be the set of solutions of (2). Then, the set of solutions of (1) is as follows*

$$\{x_i + r2^{n-t} :\ 0 \le r < 2^t,\ 1 \le i \le N_2\}.$$

*Further, $N_1 = 2^t N_2$.*

*Proof.* Firstly, fix $1 \le i \le N_2$ and $0 \le r < 2^t$. We show that $x_i + r2^{n-t}$ is a solution of (1):

$$\begin{aligned}
&a(x_i + r2^{n-t})^2 + b(x_i + r2^{n-t}) + c \\
&= 2^t A(x_i^2 + r^2 2^{2n-2t} + x_i r 2^{n-t+1}) + 2^t B(x_i + r2^{n-t}) + 2^t C \\
&= 2^t A x_i^2 + Ar^2 2^{2n-t} + Ax_i r 2^{n+1} + Bx_i 2^t + Br2^n + 2^t C \\
&= 2^t(Ax_i^2 + Bx_i + C) = 0 \quad (mod\ 2^n).
\end{aligned}$$

Conversely, let $x \in \mathbb{Z}_{2^n}$ be a solution of (1). Then

$$2^t(Ax^2 + Bx + C) = 0\ (mod\ 2^n).$$

So,

$$Ax^2 + Bx + C = 0\ (mod\ 2^{n-t}).$$

One can check that $\chi = x\ (mod\ 2^{n-t})$ is a solution of (2). Thus, all of solutions $y$ of (1) are such that $y = x_i + r2^{n-t}$, for some $1 \le i \le N_2$ and $0 \le r < 2^t$. $\square$

**Example.** Consider the equations

$$4x^2 + 4x + 24 = 0 \quad (mod\ 2^5) \tag{3}$$

and

$$x^2 + x + 6 = 0 \quad (mod\ 2^3). \tag{4}$$

The set of solutions of (3) and (4) are $A = \{1, 6, 9, 14, 17, 22, 25, 30\}$ and $B = \{1, 6\}$, respectively. One can check that Lemma 3.1 holds for this example and $|A| = 2^2|B|$.

The proof of the following lemma is straightforward.

**Lemma 3.2.** *The equation (1) has no solutions when $p_2(a) = p_2(b) = p_2(c) = 0$ or when $p_2(a) > 0$, $p_2(b) > 0$, and $p_2(c) = 0$.*

**Lemma 3.3.** *If $p_2(a) > 0$ and $p_2(b) = 0$, then the equation (1) has a unique solution.*

*Proof.* Consider the two following cases:
Case I) Let $p_2(a) > 0$, $p_2(b) = p_2(c) = 0$, $a = 2A$, $b = 2B + 1$, and $c = 2C + 1$. In this case, any solution $x$ of (1) is odd; so, we have $x = 2X + 1$. Thus, we have

$$2A(2X+1)^2 + (2B+1)(2X+1) + 2C + 1 = 0 \quad (mod\ 2^n),$$

which simplifies to

$$4AX^2 + (4A + 2B + 1)X + A + B + C + 1 = 0 \quad (mod\ 2^{n-1}).$$

So, if we set $\alpha = 4A$, $\beta = 4A + 2B + 1$, and $\gamma = A + B + C + 1$, then $[x]_0 = 1$ and we must solve the equation

$$\alpha X^2 + \beta X + \gamma = 0 \quad (mod\ 2^{n-1}),$$

such that $p_2(\alpha) > 0$ and $p_2(\beta) = 0$. Now, we have either $p_2(\gamma) = 0$, which is this same case or $p_2(\gamma) > 0$, which is Case II, below.
Case II) Let $p_2(a) > 0$, $p_2(c) > 0$, $p_2(b) = 0$, $a = 2A$, $b = 2B + 1$, and $c = 2C$. In this case, $x = 2X$. So we have

$$2A(2X)^2 + (2B+1)(2X) + 2C = 0 \quad (mod\ 2^n),$$

or

$$4AX^2 + (2B+1)X + C = 0 \quad (mod\ 2^{n-1}).$$

Put $\alpha = 4A$, $\beta = 2B + 1$, and $\gamma = C$. Then $[x]_0 = 0$ and we should solve the equation

$$\alpha X^2 + \beta X + \gamma = 0 \quad (mod\ 2^{n-1}),$$

with $p_2(\alpha) > 0$ and $p_2(\beta) = 0$. Now, if $p_2(\gamma) = 0$, then we transit to Case I and if $p_2(\gamma) > 0$, then we transit to this same case. Therefore, (1) has a unique solution. $\square$

The trend of the proof of Lemma 3.3 justifies the correctness of Algorithm 1, which computes the solution of (1) with the conditions of Lemma 3.3 in $O(n)$ time.

**Algorithm 1: Solve**$(a, b, c, n)$
Input: $a,\ b,\ c \in \mathbb{Z}_{2^n}$ with $p_2(a) > 0$ and $p_2(b) = 0$.
Output: The solution of (1) in binary form.
for $i = 0$ to $n - 1$ do
begin
if $p_2(c) > 0$ then
$[x]_i = 0$
Solve$(2a, b, \frac{c}{2}, n-1)$
else
$[x]_i = 1$
Solve$(2a, 2a + b, \frac{a}{2} + \lfloor \frac{b}{2} \rfloor + \lfloor \frac{c}{2} \rfloor + 1, n-1)$.

**Lemma 3.4.** *In the case that $p_2(a) = p_2(b) = 0$ and $p_2(c) > 0$, the equation (1) has two solutions.*

*Proof.* Consider the equation $2ay^2 + by + \frac{c}{2} = 0 \quad (mod\ 2^{n-1})$. Lemma 3.3 shows that this equation has a unique solution $\delta \in \mathbb{Z}_{2^{n-1}}$. One can check that $\pi = 2\delta$ is a solution of (1), in this case. On the other hand, Lemma 3.3 shows that the equation

$$2az^2 + (2a + b)z + \frac{a + b + c}{2} = 0 \quad (mod\ 2^{n-1})$$

has a unique solution $\rho \in \mathbb{Z}_{2^{n-1}}$. It is straightforward to see that $\varepsilon = 2\rho + 1$ is a solution of (1) in $\mathbb{Z}_{2^n}$. Now, we show that (1) has no other solutions. Suppose that $x$ is a solution of (1). We have the two following cases:
Case I) $x = 2X$; we have

$$4aX^2 + 2bX + c = 0 \quad (mod\ 2^n).$$

So,

$$2aX^2 + bX + \frac{c}{2} = 0 \quad (mod\ 2^{n-1}),$$

which is not a new solution.
Case II) $x = 2X + 1$; in this case we have

$$4aX^2 + (4a + 2b)X + a + b + c = 0 \quad (mod\ 2^n).$$

So,

$$2aX^2 + (2a + b)X + \frac{a + b + c}{2} = 0 \quad (mod\ 2^{n-1}),$$

which is not a new solution. □

The proof of next lemma is straightforward.

**Lemma 3.5.** *If $a$ is an odd element in $\mathbb{Z}_{2^n}$, then $a^2 = 1 \ (mod\ 8)$.*

The next theorem provides the set of solutions of the equation $x^2 = a \pmod{2^n}$.

**Theorem 3.6.** *Suppose that $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is defined as $f(x) = x^2 \ (mod\ 2^n)$. Then,*
***a)*** *For the three cases $p_2(a) = n$, $p_2(a) = n - 1$ with $e_n = 0$, and $a = 2^{n-2}$ with $e_n = 1$, we have*

$$|f^{-1}(a)| = 2^{\frac{n-1+e_n}{2}}.$$

***b)*** *For the two cases $p_2(a) = 1 \ (mod\ 2)$, and $p_2(a) = 0 \ (mod\ 2)$ with $0 \le p_2(a) \le n - 3$ and $o_2(a) \ne 1 \ (mod\ 8)$, we have*

$$|f^{-1}(a)| = 0.$$

***c)*** *For the case of $p_2(a) = 0 \ (mod\ 2)$ with $0 \le p_2(a) \le n - 3$ and $o_2(a) = 1 \ (mod\ 8)$, we have*

$$|f^{-1}(a)| = 2^{\frac{p_2(a)+4}{2}}.$$

*Proof.* **Case a)** On one hand, every $a \in \mathbb{Z}_{2^n}$ with $p_2(a) \geq \lceil \frac{n}{2} \rceil$ satisfies $x^2 = 0 \ (mod\ 2^n)$. So, $|f^{-1}(a)|$ is at least $2^{n-\lceil \frac{n}{2} \rceil} = 2^{\frac{n-1+e_n}{2}}$. On the other hand, for each $a \in \mathbb{Z}_{2^n}$ with $p_2(a) < \lceil \frac{n}{2} \rceil$, $a^2 \neq 0 \ (mod\ 2^n)$. Thus, $|f^{-1}(a)| = 2^{\frac{n-1+e_n}{2}}$.

Now, suppose that $n$ is odd and $p_2(a) = n-1$; i.e., $a = 2^{n-1}$. Let $x = 2^r q$ with odd $q$. We have

$$2^{2r} q^2 = 2^{n-1} \ (mod\ 2^n).$$

So, $r = \frac{n-1}{2}$, $1 \leq q \leq 2^{\frac{n+1}{2}} - 1$ and $q^2 = 1 \ (mod\ 2)$. Thus, only the odd $q$'s satisfy the equation $x^2 = 2^{n-1} \ (mod\ 2^n)$. Therefore, $|f^{-1}(a)| = 2^{\frac{n-1+e_n}{2}}$.

Now, let $n$ be even and $p_2(a) = n-2$. So, $a = s2^{n-2}$, where $s \in \{1, 3\}$. If $s = 1$, put $x = 2^r q$ with odd $q$. Then

$$2^{2r} q^2 = 2^{n-2} \ (mod\ 2^n).$$

Hence $r = \frac{n-2}{2}$, $1 \leq q \leq 2^{\frac{n+2}{2}} - 1$ and $q^2 = 1 \ (mod\ 4)$. Thus, only half of odd $q$'s satisfy the equation $x^2 = 2^{n-1} \ (mod\ 2^n)$. Therefore, $|f^{-1}(a)| = 2^{\frac{n-1+e_n}{2}}$.

**Case b)** In the proof of the Case **a)**, put $s = 3$. Consider the equation $x^2 = 2^{n-2} \times 3 \ (mod\ 2^n)$ and suppose that $x = 2^r q$ with odd $q$. Then,

$$2^{2r} q^2 = 2^{n-2} \times 3 \ (mod\ 2^n).$$

So, $r = \frac{n-2}{2}$ and $q^2 = 3 \ (mod\ 4)$. Thus, by Lemma 3.5, we have $|f^{-1}(a)| = 0$.

Now, suppose that $p_2(a) = 1 \ (mod\ 2)$. Since the square of any odd element is odd, so only even elements $x \in \mathbb{Z}_{2^n}$ can satisfy $x^2 = a \ (mod\ 2^n)$. Let $x = 2^r q$, $r \neq 0$, and suppose that $q$ is odd. Then $p_2(x^2) = 2r$ which contradicts $p_2(a) = 1 \ (mod\ 2)$. Therefore, $|f^{-1}(a)| = 0$.

Now, let $p_2(a) = 0 \ (mod\ 2)$ and $o_2(a) \neq 1 \ (mod\ 8)$. So, $a = 2^{2j} t$, where $p_2(a) = 2j$ and $t = o_2(a)$. If $x = 2^r q$ with odd $q$, then

$$2^{2r} q^2 = 2^{2j} t \ (mod\ 2^n).$$

Consequently, $r = j$ and $q^2 = t \ (mod\ 2^{n-2j})$. Thus, regarding Lemma 3.5, $|f^{-1}(a)| = 0$.

**Case c)** We use Theorem 13.3 in [2] to prove this case. Suppose that $p_2(a) = 0$ and $a = 1 \ (mod\ 8)$. The algebraic structure $(G, *)$, where $G$ is the subset of odd elements in $\mathbb{Z}_{2^n}$ and $*$ is the operator of multiplication modulo $2^n$ is a group structure. The function $\phi : G \to G$ with $\phi(g) = g * g$ is a group endomorphism on $G$. To compute $|ker(\phi)|$, we must count the number of solutions for the equation $x * x = 1_G$. In other words, we must count the number of solutions for the equation $x^2 = 1 \ (mod\ 2^n)$. We have

$$(x-1)(x+1) = 0 \ (mod\ 2^n).$$

Since $x$ is odd, so for some $q \in \mathbb{Z}_{2^n}$, $x = 2q + 1 \ (mod\ 2^n)$. So,

$$4q(q+1) = 0 \ (mod\ 2^n).$$

Consequently, $q = 0$, $q = 2^{n-2}$, $q = 2^{n-1}$, $q + 1 = 2^{n-2}$, $q + 1 = 2^{n-1}$. Substituting the values of $q$, we have the solutions $x_1 = 1$, $x_2 = 2^n - 1$, $x_3 = 2^{n-1} + 1$, and $x_4 = 2^{n-1} - 1$. Thus $|ker(\phi)| = 4$ and since $|Im(\phi)| = \frac{|G|}{|ker(\phi)|}$, we have

$$|Im(\phi)| = \frac{2^{n-1}}{4} = 2^{n-3}.$$

| Conditions | Verified in | Number of solutions |
|---|---|---|
| $p_2(a) > 0,\, p_2(b) > 0,\, p_2(c) > 0$<br>$t = min\{p_2(a),\, p_2(b),\, p_2(c)\}$ | Lemma 3.1 | $2^t$ times the number of solutions of a corresponding other case |
| $p_2(a) = 0,\, p_2(b) = 0,\, p_2(c) = 0$ | Lemma 3.2 | 0 |
| $p_2(a) > 0,\, p_2(b) > 0,\, p_2(c) = 0$ | Lemma 3.2 | 0 |
| $p_2(a) > 0,\, p_2(b) = 0,\, p_2(c) = 0$ | Lemma 3.3 | 1 |
| $p_2(a) > 0,\, p_2(b) = 0,\, p_2(c) > 0$ | Lemma 3.3 | 1 |
| $p_2(a) = 0,\, p_2(b) = 0,\, p_2(c) > 0$ | Lemma 3.4 | 2 |
| $p_2(a) = 0,\, p_2(b) > 0,\, p_2(c) = 0$<br>$b = 2B,\, s = a^{-2}B^2 - a^{-1}c,\, r = p_2(s)$ | Corollary 3.6.1 | 0 in some cases and $2^{\frac{r}{2}+2}$ o.w. |
| $p_2(a) = 0,\, p_2(b) > 0,\, p_2(c) > 0$<br>$b = 2B,\, s = a^{-2}B^2 - a^{-1}c,\, r = p_2(s)$ | Corollary 3.6.1 | 0 in some cases and $2^{\frac{r}{2}+2}$ o.w. |

Table 1. The summary of cases of solving equation (1)

On the other hand, according to Lemma 3.5 and since the number of elements in $\mathbb{Z}_{2^n}$ in the form of $8q + 1$ is equal to $2^{n-3}$ and $|Im(\phi)| = 2^{n-3}$, so every element in the form of $8q + 1$ in $\mathbb{Z}_{2^n}$ is a square. Thus, the equation $x^2 = a \ (mod\ 2^n)$ has at least one solution. Obviously this solution, say $x$, is odd: $x = 2y + 1$. So we have $(2y + 1)^2 = 8q + 1$ or $y^2 + y - 2q = 0$, for some $q$. By Lemma 3.4, this equation has two solutions $q_1$ and $q_2$. One can check that $q_3 = 2^n - q_1$ and $q_4 = 2^n - q_2$ are the two other solutions. Consequently,

$$|f^{-1}(a)| = |ker(\phi)| = 4 = 2^{\frac{p_2(a)+4}{2}}.$$

Now, suppose that $p_2(a) = 0 \ (mod\ 2)$, $2 \leq p_2(a) \leq n - 3$ and $o_2(a) = 1 \ (mod\ 8)$. In this case, we have $a = 2^{2j}t$ with $p_2(a) = 2j$ and $t = o_2(a)$. Let $x = 2^r q$ with odd $q$. Then,

$$2^{2r}q^2 = 2^{2j}t \ (mod\ 2^n).$$

So, $r = j$ and $q^2 = t \ (mod\ 2^{n-2j})$. Regarding Lemma 3.5 and the proof of **Case b)**, this equation has four solutions $q_1,\, q_2,\, q_3,\, q_4$ with $0 \leq q_i \leq 2^{n-2j} - 1$. For each of these solutions, we present $2^j$ solutions

$$x_{s,t} = 2^j \left(s2^{n-2j+1} + q_t\right), \quad 0 \leq s < 2^j, \quad 1 \leq t \leq 4.$$

We have,

$$\begin{aligned} x_{s,t}^2 &= 2^{2j}\left(s^2 2^{2n-4j+2} + q_t^2 + 2s2^{n-2j+1}\right) \\ &= s^2 2^{2n-2j+2} + 2^{2j}q_t^2 + s2^{n+2} \\ &= 2^{2j}q_t^2 \ (mod\ 2^n). \end{aligned}$$

Regarding $2j \leq n - 3$, we have $2n - 2j \geq n + 3$. Therefore,

$$|f^{-1}(a)| = 2^{\frac{p_2(a)+4}{2}}.$$

□

Note that Theorem 3.6 gives the set of solutions that are needed in the next corollary.

**Corollary 3.6.1.** *Let* $p_2(a) = 0$, $p_2(b) > 0$, *and* $b = 2B$. *Put* $s = a^{-2}B^2 - a^{-1}c$, $r = p_2(s)$, *and* $q = o_2(s)$. *If* $p_2(r) = 0$ *or* $q \neq 1 \pmod 8$, *then (1) has no solutions. Otherwise, (1) has* $2^{\frac{r}{2}+2}$ *solutions.*

*Proof.* We have

$$ax^2 + 2Bx + c = 0 \quad (mod\ 2^n)$$

or

$$x^2 + 2a^{-1}Bx + a^{-1}c = 0 \quad (mod\ 2^n).$$

So, we get

$$(x + a^{-1}B)^2 = s \quad (mod\ 2^n).$$

Now, by Theorem 3.6, if $p_2(r) = 0$ or $q \neq 1$ $(mod\ 8)$, then (1) has no solutions and, otherwise, it has $2^{\frac{r}{2}+2}$ solutions. □

In Corollary 3.6.1, one should note that if $p_2(c) = 2(p_2(b) - 1)$ or $p_2(c) > 2(p_2(b) - 1)$ with $p_2(p_2(c)) = 0$, then equation (1) has no solutions. In Corollary 3.6.1, if $p_2(c) < 2(p_2(b) - 1)$ or $p_2(c) > 2(p_2(b) - 1)$ with $p_2(p_2(c)) > 0$, then we should compute $s$ $(mod\ 8)$. The interesting point is that, since $a^{-2} = 1$ $(mod\ 8)$, it suffices to compute $S = B^2 - a^{-1}c$.

It is a well-known fact that (see [4] for example) a polynomial $ax^2 + bx + c$ over $\mathbb{Z}_{2^n}$ is a permutation polynomial, iff $p_2(a) > 0$ and $p_2(b) = 0$. Lemma 3.3 provides another proof of this fact. The number of fixed-points, is one of the properties which is studied in symmetric cryptography. The less is the number of fixed-points, the stronger is the component, from this aspect. In the next corollary, we characterize the number of fixed-points for quadratic permutation polynomials over $\mathbb{Z}_{2^n}$.

**Corollary 3.6.2.** *Suppose that* $f(x) = ax^2 + bx + c$ *on* $\mathbb{Z}_{2^n}$ *is a permutation polynomial; i.e.,* $p_2(a) > 0$ *and* $p_2(b) = 0$. *Obviously, the number of fixed-points of* $f$ *is equal to the number of solutions for* $ax^2 + (b-1)x + c = 0$, $(mod\ 2^n)$. *So, regarding Table 1,* $f$ *has no fixed-points (the best case, from the viewpoint of cryptography) if* $p_2(c) = 0$. *Otherwise, it has* $2^t$ *fixed-points, for some* $t \geq 1$, *if it has any.*

# 4 Conclusion

Quadratic functions have applications in cryptography. In this paper, we study the quadratic equation mod $2^n$. We determine whether this equation has a solution or not and in the case that it has a solution, we give the number of solutions along with the set of its solutions in $O(n)$ time.

One of our results is the fact that, when the quadratic equation modulo a power of two has a solution, then the number of its solutions is a power of two. The other interesting application is characterizing the number of fixed-points of a quadratic permutation polynomial over $\mathbb{Z}_{2^n}$.

# References

[1] Boesgaard, M., Vesterager, M., & Zenner, E. (2008). *The Rabbit Stream Cipher*. New Stream Cipher Designs - The eSTREAM Finalists, 69–83.

[2] Fraleigh, J. B. (1999). *A First Course in Abstract Algebra*. Sixth edition, Addison-Wesley Publishing Company Inc.

[3] Goresky, M., & Klapper, A. (2005). *Algebraic Shift Register Sequences*. Cambridge University Press.

[4] Rivest, R. L. (2001). Permutatin Polynomials modulo $2^w$. *Finite Fields and Their Apllication*, 7, 287–292.

[5] Rivest, R. L., Robshaw, M. J. B., Sidney, R., & Yin, Y. L. (1998). *The RC6 Block Cipher*. M.I.T., RSA Laboratories.

[6] Stinson, D. R. (2003). *Cryptography – Theory and Practice*. 3rd edn. Chapman and Hall/CRC, Boca Raton.

[7] Vincent, C. (2017). *Notes on solving* $x^2 = a \pmod{n}$, Available online: `https://www.uvm.edu/~cvincen1/files/teaching/spring2017-math255/quadraticequation.pdf`.

[8] Pommerening, K. (2000). *Quadratic Equation in Finite Fields of Characteristic 2*. English version (February 2012), Available online: `http://www.klauspommerening.de/MathMisc/QuGlChar2.pdf`.