



# Representing the inverse map as a composition of quadratics in a finite field of characteristic 2

Florian Luca<sup>1,2</sup> · Santanu Sarkar<sup>3</sup> · Pantelimon Stănică<sup>4</sup>

Received: 28 September 2023 / Accepted: 1 February 2024

This is a U.S. Government work and not under copyright protection in the US; foreign copyright protection may apply 2024

## Abstract

In 1953, Carlitz showed that all permutation polynomials over  $\mathbb{F}_q$ , where  $q > 2$  is a power of a prime, are generated by the special permutation polynomials  $x^{q-2}$  (the inversion) and  $ax + b$  (affine functions, where  $0 \neq a, b \in \mathbb{F}_q$ ). Recently, Nikova, Nikov and Rijmen (2019) proposed an algorithm (NNR) to find a decomposition of the inverse function in quadratics, and computationally covered all dimensions  $n \leq 16$ . Petrides (2023) theoretically found a class of integers for which it is easy to decompose the inverse into quadratics, and improved the NNR algorithm, thereby extending the computation up to  $n \leq 32$ . In this paper, we extend Petrides' result, as well as we propose a new number theoretical approach, which allows us to easily cover all (surely, odd) exponents up to 250, at least.

**Keywords** Permutations · Decompositions · Quadratics · Algorithm · Primes · Sieves

**Mathematics Subject Classification (2010)** 11A41 · 11N13 · 11N36 · 20B99 · 94A60 · 94D10

---

This is an expanded and vastly improved version of the Extended Abstract, which was presented at the 8th International Workshop on Boolean Functions and their Applications (BFA) in Voss in September 2023.

---

✉ Pantelimon Stănică  
pstanica@nps.edu

Florian Luca  
Florian.Luca@wits.ac.za

Santanu Sarkar  
santanu@iitm.ac.in

<sup>1</sup> School of Mathematics, University of the Witwatersrand, Private Bag X3, Wits 2050, Johannesburg, South Africa

<sup>2</sup> Centro de Ciencias Matemáticas, UNAM, Morelia, Mexico

<sup>3</sup> Department of Mathematics, Indian Institute of Technology Madras, Sardar Patel Road, Chennai, TN 600036, India

<sup>4</sup> Applied Mathematics Department, Naval Postgraduate School, Monterey 93943, USA

# 1 Introduction

Threshold implementations (TI) are a kind of side-channel attack countermeasures, based on secret sharing schemes and techniques from multiparty computation. The idea is to split a variable  $x$  into  $s$  additive shares  $x_i$  with  $x = \sum_{i=1}^s x_i$ . Let  $\mathbf{x} = (x_1, x_2, \dots, x_s)$ . To implement a function  $F(x, y, z, \dots) = a$  from  $\mathbb{F}_2^m$  to  $\mathbb{F}_2^n$ , the TI method requires *sharing*, that is, a set of  $s$  functions  $F_i$ , which together can compute the output of  $F$ . Sharing needs to satisfy some properties, namely, correctness, non-completeness and uniformity [10]:

- **Correctness:**  $a = F(x, y, z, \dots) = \sum_{i=1}^s F_i(\mathbf{x}, \mathbf{y}, \mathbf{z}, \dots)$ , for all  $\mathbf{x}, \mathbf{y}, \mathbf{z}, \dots$ , with  $x = \sum_{i=1}^s x_i, y = \sum_{i=1}^s y_i, z = \sum_{i=1}^s z_i$ .
- **Non-completeness:** Every function is independent of at least one share of the input variables  $x, y, z$  ( $F_i$  should be independent of  $x_i, y_i, z_i$ ).
- **Uniformity (balancedness):** For all  $(a_1, a_2, \dots, a_s)$  with  $\sum_{i=1}^s a_i = a$ , the number of tuples  $(\mathbf{x}, \mathbf{y}, \mathbf{z}, \dots) \in \mathbb{F}_2^{ms}$  for which  $F_j(\mathbf{x}, \mathbf{y}, \mathbf{z}, \dots) = a_j, 1 \leq j \leq s$ , is equal to  $2^{(s-1)(m-n)}$  times the number of  $(x, y, z, \dots) \in \mathbb{F}_2^m$ , for which  $a = F(x, y, z, \dots)$ . So, if  $F$  is a permutation on  $\mathbb{F}_2^m$ , then the  $F_i$ 's form together a permutation on  $\mathbb{F}_2^{ms}$  (sharing preserves the output distribution).

We should mention earlier work on the Gold function, where TI was achieved for all  $3 \times 3, 4 \times 4$  S-boxes [1], and the realization of the inversion in  $\mathbb{F}_{16}$  with 5 shares [10]. One notes that since each  $F_i$  is completely independent of the unmasked values, also the subcircuits implementing them are, even in the presence of glitches. Because of the linearity of the expectation operator, the same holds true for the average power consumption of the whole circuit, or any linear combination of the power consumptions of the subcircuits. This has, as a consequence, the implication that one has perfect resistance against all first-order side-channel attacks [10] (this approach was extended and applied to Noekeon, Keccak, Present, and AES).

Now, in order to share a nonlinear function (S-box) with algebraic degree  $d$ , at least  $d + 1$  shares are needed. For example, (quadratic) Gold (APN or not) functions can be realized with 3 shares. Since the algebraic degree of a vectorial Boolean function is one of the main parameters driving the cost of its hardware implementation, a natural question is whether we decompose every permutation using affine/quadratics/cubics (especially of those whose shares are investigated).

Prior to this, in [2], Carlitz showed that all permutation polynomials over  $\mathbb{F}_q$ , where  $q > 2$  is a power of a prime, are generated by the special permutation polynomials  $x^{q-2}$  (the inversion) and  $ax + b$  (affine functions, where  $0 \neq a, b \in \mathbb{F}_q$ ). The smallest number of inversions in such a decomposition is called the *Carlitz rank*.

Here, we ask whether the inverse in  $\mathbb{F}_{2^n}$  (the finite field of dimension  $n$  over the two-elements prime field  $\mathbb{F}_2$ ) can be written as a composition of quadratics, or quadratics and cubics. That is, we ask if there are integers  $r \geq 1$  and  $a_1 \geq 0, \dots, a_r \geq 0$  such that

$$-1 \equiv \prod_{i=1}^r (2^{a_i} + 1) \pmod{2^n - 1}.$$

Nikova, Nikov and Rijmen [9] proposed an algorithm to find such a decomposition. Leveraging Carlitz's work [2], they utilized the algorithm to demonstrate that for all  $n \leq 16$ , any permutation can be decomposed into quadratic permutations, when  $n$  is not a multiple of 4, and into cubic permutations, when  $n$  is a multiple of 4. In addition to a theoretical result, which we will discuss below, Petrides [11] improved the complexity of the algorithm and

presented a computational table of shortest decompositions for  $n \leq 32$ , allowing also cubic permutations in addition to quadratics. Here, we find a new number theoretical approach that allows us to cover all (surely, odd) exponents up to 250, at least.

## 2 Heuristics and some conjectures

Let  $v_2$  be the 2-valuation, that is, the largest power of 2 dividing the argument. We start with a proposition, extending one of Petrides' results [11], which states that if  $n$  is an odd integer and  $\frac{n-1}{2^{v_2(n-1)}} \equiv 2^k \pmod{2^n - 1}$ , for some  $k$ , then

$$\begin{aligned} 2^n - 2 &= 2 \left( 2^{\left(\frac{n-1}{2^{v_2(n-1)}}\right)2^{v_2(n-1)}} - 1 \right) \\ &= 2 \left( 2^{\frac{n-1}{2^{v_2(n-1)}}} - 1 \right) \prod_{j=1}^{v_2(n-1)} \left( 2^{\frac{n-1}{2^j}} + 1 \right) \\ &\equiv 2 \left( 2^{2^k} - 1 \right) \prod_{j=1}^{v_2(n-1)} \left( 2^{\frac{n-1}{2^j}} + 1 \right) \\ &= 2 \prod_{j=0}^{k-1} \left( 2^{2^j} + 1 \right) \prod_{j=1}^{v_2(n-1)} \left( 2^{\frac{n-1}{2^j}} + 1 \right). \end{aligned}$$

This implies, via Carlitz [2], that for all odd integers (coined *good integers*, with the counterparts named *bad integers* in [7]) satisfying the congruence  $\frac{n-1}{2^{v_2(n-1)}} \equiv 2^k \pmod{2^n - 1}$ , one can decompose any permutation polynomial in  $\mathbb{F}_{2^n}$  into affine and quadratic power permutations.

The smallest odd positive integer that is not *good* is  $n = 7$ . We note however that in that case

$$2^7 - 2 = 2(2^6 - 1) = 2(2^2 - 1)(2^4 + 2^2 + 1) = 2(2 + 1)(2^4 + 2^2 + 1),$$

and so, any permutation in  $\mathbb{F}_{2^7}$  can be decomposed into affine, quadratic and cubic permutations. We are ready to generalize this observation.

**Theorem 1** *Let  $n$  be an odd integer satisfying*

$$\frac{n-1}{2^{v_2(n-1)}} \equiv 2^k 3^s \pmod{2^n - 1},$$

*for some non-negative integers  $k, s$ . Then, the inverse power permutation in  $\mathbb{F}_{2^n}$  has a decomposition into affine, quadratic and cubic power permutations of length  $k + s + v_2(n - 1)$ .*

**Proof** As we have already alluded to above, using the difference of cubes factorization,  $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$ , we have

$$\begin{aligned} 2^n - 2 &= 2 \left( 2^{\frac{n-1}{2^{v_2(n-1)}}} - 1 \right) \prod_{j=1}^{v_2(n-1)} \left( 2^{\frac{n-1}{2^j}} + 1 \right) \\ &\equiv 2 \left( 2^{2^k 3^s} - 1 \right) \prod_{j=1}^{v_2(n-1)} \left( 2^{\frac{n-1}{2^j}} + 1 \right) \end{aligned}$$

$$\begin{aligned}
 &= 2 \left( 2^{2^k 3^{s-1}} - 1 \right) \left( 2^{2^{k+1} 3^{s-1}} + 2^{2^k 3^{s-1}} + 1 \right) \prod_{j=1}^{v_2(n-1)} \left( 2^{\frac{n-1}{2^j}} + 1 \right) \\
 &\dots\dots\dots \\
 &= 2 \left( 2^{2^k} - 1 \right) \prod_{j=0}^{s-1} \left( 2^{2^{k+1} 3^j} + 2^{2^k 3^j} + 1 \right) \prod_{j=1}^{v_2(n-1)} \left( 2^{\frac{n-1}{2^j}} + 1 \right) \\
 &\equiv 2 \prod_{j=0}^{k-1} \left( 2^{2^j} + 1 \right) \prod_{j=0}^{s-1} \left( 2^{2^{k+1} 3^j} + 2^{2^k 3^j} + 1 \right) \prod_{j=1}^{v_2(n-1)} \left( 2^{\frac{n-1}{2^j}} + 1 \right).
 \end{aligned}$$

The claim is shown.

**Example 1** *It is natural to investigate the counting function  $\mathcal{B}(x)$  of superbad integers (that is, integers  $n$  such that  $\frac{n-1}{2^{v_2(n-1)}} \not\equiv 2^k 3^s \pmod{2^n - 1}$ ), with  $\mathcal{B}(x) = \{n \leq x : n \text{ is superbad}\}$ , or its complement*

$$\mathcal{A}(x) = \{n \leq x : \frac{n-1}{2^{v_2(n-1)}} \equiv 2^k 3^s \pmod{2^n - 1}\}.$$

As an example,  $|\mathcal{B}(50)| = 16$ , more precisely,

$$\mathcal{B}(50) = \{1, 2, 3, 4, 5, 7, 9, 10, 13, 17, 19, 25, 28, 33, 37, 49\}.$$

*Petrides [11] noted that 25 integers up to 50 are bad, so our extension surely prunes the integers better. In a recent paper [5], two of us showed that*

$$\mathcal{A}(x) \ll \frac{x}{(\log \log x)^{1+o(1)}}, \text{ as } x \rightarrow \infty.$$

In the first part of our paper, we restrict our attention to  $n = p$ , a prime, and propose some conjectures that will help us in designing our algorithm. Surely, there is no reason why we should not expect the algorithm to work for odd integers, also.

Let  $p \geq 3$  be prime,  $N := N_p = 2^p - 1$ . It is known that if  $q \mid N_p$ , then  $q \equiv 1 \pmod{p}$ . We ask if we can say anything about the number of distinct prime factors  $\omega(N_p)$  of  $N_p$ . We propose the following conjecture.

**Conjecture 1** *There exists  $p_0$  such that for  $p > p_0$ ,  $\omega(N_p) < 1.36 \log p$ .*

Similar heuristics regarding lower bounds for  $\Omega(2^n - 1)$  and  $\omega(2^n - 1)$  can be found in [4] and [6].

Our Conjecture 1 is based on statistical arguments originating from sieve methods. The Turán-Kubilius inequality asserts that

$$\sum_{n \leq x} (\omega(n) - \log \log x)^2 = O(x \log \log x).$$

So, if  $\delta > 0$  is fixed, the set of  $n \leq x$  such that  $\omega(n) \geq (1 + \delta) \log \log x$  is of counting function  $O_\delta(x / \log \log x)$ . One can do better using sieves. Indeed, Exercise 04 in [3] shows that for fixed  $\delta > 0$  we, in fact, have that

$$\#\{n \leq x : \omega(n) \geq (1 + \delta) \log \log x\} \ll_\delta \frac{x}{(\log x)^{Q(\delta)}},$$

where  $Q(\delta) := (1 + \delta) \log((1 + \delta)/e) + 1$ . We would like to apply such heuristics to  $N_p = 2^p - 1$ . But note that if  $q \mid N_p$ , then  $2^p \equiv 1 \pmod{q}$ . In particular,  $\left(\frac{2}{q}\right) = 1$ , so  $q \equiv \pm 1 \pmod{8}$ . But then the same proof as Exercise 04 in [3] shows that

$$\begin{aligned} & \# \{n \leq x : q \mid n \Rightarrow q \equiv \pm 1 \pmod{8} \text{ and } \omega(n) \geq (1 + \delta) \log \log x\} \\ & \leq \frac{x}{(\log x)^{Q_1(\delta)+o(1)}} \end{aligned}$$

as  $x \rightarrow \infty$ , where  $Q_1(\delta) := (1 + \delta) \log((1 + \delta)/(0.5e)) + 1$ . Taking  $\delta = 0.36$ , we get  $Q_1(\delta) = 1.00086 \dots$ . Thus, the probability that a number having only prime factors congruent to  $\pm 1 \pmod{8}$  has more than  $1.36 \log \log n$  distinct prime factors is

$$O\left(\frac{1}{(\log n)^{1.00008}}\right).$$

Applying this to  $N_p$ , we get

$$O\left(\frac{1}{(\log(2^p - 1))^{1.0008}}\right) \ll \frac{1}{p^{1.0008}},$$

and since the series

$$\sum_{p \geq 3} \frac{1}{p^{1.0008}}$$

is convergent, we are led to believe that maybe there are at most finitely many prime numbers  $p$  such that  $\omega(N_p) \geq 1.36 \log p$ . It has been noted that perhaps infinitely often  $\omega(N_p) \geq 2$ . For example, this is the case if  $p \equiv 3 \pmod{4}$  is such that  $q = 2p + 1$  is prime. Indeed, then 2 is a quadratic residue modulo  $q$  so  $2^{(q-1)/2} \equiv 1 \pmod{q}$ , showing that  $q \mid N_p$ . Since  $N_p$  is never a perfect power, in particular it cannot be a power of  $q$ , we get the desired conclusion that  $\omega(N_p) \geq 2$ .

**Conjecture 2** *There exists  $p_0$  such that if  $p > p_0$ , then  $N_p$  is squarefree.*

We offer some heuristic evidence for Conjecture 2. Knowing that the prime  $q$  divides  $N_p$ , the conditional probability that  $N_p$  is divisible by  $q^2$  is  $1/q$ . Thus, the probability that  $N_p$  is not squarefree is bounded above by

$$\sum_{q:q \mid N_p \text{ for some prime } p} \frac{1}{q},$$

and it was shown by Murata and Pomerance in [8] that the above sum is finite under GRH.

So, assuming Conjectures 1 and 2, let  $N_p := q_1 \cdots q_k$  for some distinct primes  $q_1, \dots, q_k$  with  $k \leq 1.36 \log p$ . We take numbers of the form  $2^a + 1$  with an odd  $a \in [5, p - 2]$ . We want to compute

$$\left(\frac{2^a + 1}{2^p - 1}\right).$$

This was done by Rotkiewicz in [12]. Namely, write the Euclidean algorithm with even quotients and signed remainders:

$$\begin{aligned} p &= (2k_1)a + \varepsilon_1 r_1, & \varepsilon_1 \in \{\pm 1\}, & 1 \leq r_1 \leq a - 1 \\ a &= (2k_2)r_1 + \varepsilon_2 r_2, & \varepsilon_2 \in \{\pm 1\}, & 1 \leq r_2 \leq r_1 - 1, \\ &\dots = \dots \\ r_{\ell-2} &= (2k_\ell)r_{\ell-1} + \varepsilon_\ell r_\ell, & \varepsilon_\ell \in \{\pm 1\}, & r_\ell = 1, \end{aligned}$$

where  $\ell := \ell(a, p)$  is minimal with  $r_\ell = 1$ . Note that  $r_i$  are all odd for  $i = 1, \dots, \ell$ . In particular,  $r_j \geq 3$  for  $j = 1, \dots, \ell - 1$ . Then

$$\left(\frac{2^a + 1}{2^p - 1}\right) = \left(\frac{2^p - 1}{2^a + 1}\right) = \left(\frac{(2^a)^{2k_1} \cdot 2^{\varepsilon_1 r_1} - 1}{2^a + 1}\right) = \left(\frac{2^{\varepsilon_1 r_1} - 1}{2^a + 1}\right) = \left(\frac{2^{r_1} - 1}{2^a + 1}\right).$$

The right-most equality is clear if  $\varepsilon_1 = 1$ , and if  $\varepsilon_1 = -1$ , then

$$\begin{aligned} \left(\frac{2^{-r_1} - 1}{2^a + 1}\right) &= \left(\frac{2}{2^a + 1}\right)^{r_1} \left(\frac{2^{-r_1} - 1}{2^a + 1}\right) = \left(\frac{2^{r_1}(2^{-r_1} - 1)}{2^a + 1}\right) \\ &= \left(\frac{1 - 2^{r_1}}{2^a + 1}\right) = \left(\frac{-1}{2^a + 1}\right) \left(\frac{2^{r_1} - 1}{2^a + 1}\right) = \left(\frac{2^{r_1} - 1}{2^a + 1}\right). \end{aligned}$$

The above calculation shows how to transit from the first step to the second step, or more generally from a step with  $2^{r_j} - 1$  in the bottom to a step with  $2^{r_{j+1}} - 1$  in the top. For the next step, we write

$$\left(\frac{2^{r_1} - 1}{2^a + 1}\right) = \left(\frac{2^a + 1}{2^{r_1} - 1}\right) = \left(\frac{(2^{r_1})^{2k_2} \cdot 2^{\varepsilon_2 r_2} + 1}{2^{r_1} - 1}\right) = \left(\frac{2^{\varepsilon_2 r_2} + 1}{2^{r_1} - 1}\right) = \left(\frac{2^{r_2} + 1}{2^{r_1} - 1}\right).$$

The last inequality above is clear if  $\varepsilon_2 = 1$ . If  $\varepsilon_2 = -1$ , then since  $r_1 \geq 3$ , we have

$$\left(\frac{2^{-r_2} + 1}{2^{r_1} - 1}\right) = \left(\frac{2}{2^{r_1} - 1}\right)^{r_2} \left(\frac{2^{-r_2} + 1}{2^{r_1} - 1}\right) = \left(\frac{2^{r_2}(2^{-r_2} + 1)}{2^{r_1} - 1}\right) = \left(\frac{2^{r_2} + 1}{2^{r_1} - 1}\right).$$

At step  $\ell$  we end up with

$$\left(\frac{2^{r_\ell} + (-1)^\ell}{2^{r_{\ell-1}} + (-1)^{\ell-1}}\right).$$

If  $\ell(a, p)$  is odd, we get

$$\left(\frac{2^1 - 1}{2^{r_{\ell-1}} + 1}\right) = 1,$$

and if  $\ell(a, p)$  is even we get

$$\left(\frac{2^1 + 1}{2^{r_{\ell-1}} - 1}\right) = -\left(\frac{2^{r_{\ell-1}} - 1}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

We thus get that

$$\left(\frac{2^a + 1}{2^p - 1}\right) = (-1)^{\ell+1}.$$

We select the subset  $\mathcal{A}(p)$  of odd  $a$  in the interval  $[5, p - 2]$  such that  $\ell \equiv 0 \pmod{2}$ . We assume that there are a positive proportion of such, namely that there is a constant  $c_1 > 0$  such that for large  $p$ , there are  $> c_1 p$  odd numbers  $a \in [5, p - 2]$  such that  $\ell(a, p) \equiv 0 \pmod{2}$ . So, we have

$$\prod_{i=1}^k \left(\frac{2^a + 1}{q_i}\right) = -1 \quad \text{for } a \in \mathcal{A}(p).$$

We next conjecture that for such  $a$ , the values are

$$\left(\left(\frac{2^a + 1}{q_i}\right), 1 \leq i \leq k\right) \tag{1}$$

are uniformly distributed among the  $2^k$  vectors  $(\pm 1, \pm 1, \dots, \pm 1)$ . Indeed, if not, then some-

how for some  $a$  the value of  $2^a + 1$  of the Legendre symbol  $\left(\frac{2^a + 1}{p_i}\right)$  should be determined in terms of the values of the same symbol for  $b \leq a - 1$ . This can happen for example if:

- (i)  $2^a + 1$  is a square. This never happens for  $a \geq 4$ .
- (ii)  $2^a + 1$  is multiplicatively dependent over  $\{2^b + 1 : 0 \leq b \leq a - 1\}$ . This does not happen for  $a \geq 4$  because of the Carmichael’s Primitive Divisor Theorem:  $2^a + 1$  has a prime factor  $p_a$  which is primitive in the sense that  $p_a$  does not divide  $2^b + 1$  for any  $b \leq a - 1$ .

Well, so we fix  $i \in \{1, \dots, k\}$  and search for  $a_i$  such that

$$\left(\frac{2^{a_i} + 1}{q_i}\right) = (-1)^{\delta_{ij}}, \tag{2}$$

where  $\delta_{ij}$  is the Kronecker symbol. That is,  $2^{a_i} + 1$  is a quadratic residue modulo  $p_j$  for all  $j \neq i$  but it is not a quadratic residue modulo  $q_i$ . Do we expect to find it? Well, let us see. Fix  $i$  in  $\{1, \dots, k\}$ . The probability that  $2^{a_i} + 1$  verifies the Legendre conditions given by (2) is  $1/2^k$  so it is  $(1 - 1/2^k)$  that they are not satisfied. Note that since  $\left(\frac{2^{a_i} + 1}{N_p}\right) = -1$  we

know that an odd number of the  $p = p_j$ ’s satisfy that  $\left(\frac{2^{a_i} + 1}{p_j}\right) = 1$ . So, if we assume that this is so for all possible  $a_i$ ’s, and assuming that these events are independent, we get that the probability that this be so is

$$\ll \left(1 - \frac{1}{2^k}\right)^{c_1 p} < \left(1 - \frac{1}{p^{1.36 \log 2}}\right)^{c_1 p} < \left(1 - \frac{1}{p^{0.95}}\right)^{c_1 p} \ll \frac{1}{e^{c_1 p^{0.05}}}.$$

In the above, we used that  $k < 1.36 \log p$  and  $1.36 \cdot \log 2 < 0.95$ . Of course, this is for  $i$  fixed and now we sum up over  $i$  from 1 to  $k$  introducing another logarithmic factor in the above count. Since the series

$$\sum_p \frac{\log p}{e^{c_1 p^{0.05}}}$$

converges, so we expect that the above event does not occur when  $p > p_0$ . So, we have the following conjecture.

**Conjecture 3** *Assume Conjectures 1 and 2. Write  $2^p - 1 = q_1 \dots q_k$  for  $p > p_0$  with prime factors  $q_1 < \dots < q_k$  and  $k < 1.36 \log p$ . Then for each  $i = 1, \dots, k$ , there exists an odd  $a_i \in [5, p - 2]$  such that equalities (2) hold.*

### 3 Unconditional argument and our decomposition algorithm

The rest of the proof is unconditional. We will show that there exist integers  $x_i$  such that

$$(-1) = \prod_{i=1}^k (2^{a_i} + 1)^{x_i} \pmod{2^p - 1}. \tag{3}$$

We will be more precise later, but the idea of our approach is the following. For a prime  $p$  below some bound (depending upon the speed of the computer), factor (via the database from the Cunningham project or the computer),  $2^p - 1 = q_1 \dots q_k$ , ( $q_i$  primes), and for

each  $i$  we search for  $a_i$  in  $[5, p - 2]$  odd such that for each such,  $2^{a_i} + 1$  is a QR (quadratic residue) modulo  $q_j$  for all  $j \neq i$  in  $\{1, \dots, k\}$  and a QNR (quadratic non-residue) modulo  $q_i$ . We then generate some primitive roots modulo  $q_i$  and compute the invertible matrix  $\mathcal{B}$  and find values for the  $x_i$ 's. There is no reason why we should not expect this to happen to odd integers  $n$  (again under some manageable bound) and do the same for  $2^n - 1$  (choose  $a$  odd with  $\gcd(a, n) = 1$ ). We now detail this below.

Write  $q_i - 1 =: 2^{\alpha_i} R_i$  for  $i = 1, \dots, k$ , where  $R_i$  is odd. Let

$$R := \text{lcm}[R_i : 1 \leq i \leq k]$$

and write  $x_i = y_i R$  for  $i = 1, \dots, k$ . Let  $\rho_i$  be a primitive root modulo  $q_i$ . Write

$$2^{a_i} + 1 = \rho_j^{b_{ij}} \pmod{q_j}. \tag{4}$$

Conditions (2) show that  $b_{ij} \equiv \delta_{ij} \pmod{2}$ . Equation (3) holds if and only if it holds one prime  $q_j$  at a time. Thus, we want

$$\rho_j^{(q_j-1)/2} \equiv \rho_j^{R \sum_{i=1}^k y_i b_{ij}} \pmod{q_j},$$

which holds provided that

$$\frac{(q_j - 1)}{2} \equiv R \sum_{i=1}^k y_i b_{ij} \pmod{q_j - 1}.$$

This in turn is equivalent to

$$2^{\alpha_j-1} \equiv (R/R_j) \sum_{i=1}^k y_i b_{ij} \pmod{2^{\alpha_j}}.$$

Since  $R/R_j$  is odd, it follows that it is invertible modulo  $2^{\alpha_j}$ . Writing  $(R/R_j)^*$  for the inverse of  $(R/R_j)$  modulo  $2^{\alpha_j}$ , we get that

$$2^{\alpha_j-1} (R/R_j)^* \equiv \sum_{i=1}^k y_i b_{ij} \pmod{2^{\alpha_j}}.$$

Since  $(R/R_j)^*$  is odd the left-hand side is just  $2^{\alpha_j-1} \pmod{2^{\alpha_j}}$ . Thus,

$$2^{\alpha_j-1} \equiv \sum_{i=1}^k y_i b_{ij} \pmod{2^{\alpha_j}}.$$

This is a linear system of modular equations for  $i = 1, \dots, k$ . To see that it is nondegenerate note that the coefficient matrix  $\mathcal{B} = (b_{ij})_{1 \leq i, j \leq k}$  modulo 2 is in fact the identity matrix. Hence, its determinant is an odd integer, so invertible modulo powers of 2, which shows that there exist an integer solution  $y_1, \dots, y_k$ . To solve it, we can generate for each  $i, j$  the number  $b_{i,j} \pmod{2^{\alpha_j}}$  appearing in (4) as an integer in the interval  $[0, 2^{\alpha_j} - 1]$ . Having done that, we solve the linear system

$$\sum_{i=1}^k y_i b_{ij} = 2^{\alpha_j-1} \text{ for } j = 1, 2, \dots, k.$$

This is non-degenerate since the determinant of the coefficient matrix is odd. Thus,  $(y_1, \dots, y_k)$  are some rational numbers. Now we treat them as residue classes modulo  $2^\alpha$ ,



where  $\alpha := \max\{\alpha_i : 1 \leq i \leq k\}$  (by inverting the odd determinant modulo  $2^\alpha$ ). These ones are the  $y_i$ 's that we are looking for.

We implemented this and checked it for all primes  $p \leq 250$ . We present our approach in Algorithm 1.

**Algorithm 1**

```

1 for Prime  $p \leq 250$  do
2   Factor  $2^p - 1 = q_1 \cdots q_k$ , where  $q_i$  is prime for  $1 \leq i \leq k$ ;
3   for  $j = 1$  to  $k$  do
4     Find odd  $a_j \in [5, p - 2]$  such that the Legendre symbol  $\left(\frac{2^{a_j} + 1}{q_j}\right) = (-1)^{\delta_{ij}}$  where  $\delta_{ij}$  is the
     Kronecker symbol.
5   end
6   Take a primitive root  $\rho_i$  modulo  $q_i$  for  $1 \leq i \leq k$ ;
7   Find  $b_{ij}$  such that  $2^{a_i} + 1 = \rho_j^{b_{ij}} \pmod{q_j}$  for  $1 \leq i, j \leq k$ ;
8   Find largest  $\alpha_i$  such that  $2^{\alpha_i}$  is a divisor of  $q_i - 1$  for  $1 \leq i \leq k$ ;
9   Calculate  $\alpha = \max\{\alpha_i : 1 \leq i \leq k\}$ ;
10  Solve the system of linear equations  $\sum_{i=1}^k y_i b_{ij} = 2^{\alpha j - 1}$  for  $j = 1, 2, \dots, k$  in  $\mathbb{Z}_{2^\alpha}$ 
11 end

```

The factorization of  $2^p - 1$  is known for all primes  $p < 1000$ . Surely, we can use the same algorithm modulo  $2^n - 1$  for  $n \leq 250$  and odd. Note that if

$$2^n - 1 = \prod_{j=1}^k q_j^{\alpha_j},$$

then we only want to find a relation of the form

$$(-1) \equiv \prod_{i=1}^k (2^{a_i} + 1)^{x_i} \pmod{q_1 \cdots q_k}. \tag{5}$$

Indeed, if we have found the above relation, then

$$q_1 \cdots q_k \mid (2^{a_1} + 1)^{x_1} \cdots (2^{a_k} + 1)^{x_k} + 1.$$

Writing  $Q := (2^n - 1)/(q_1 \cdots q_k)$ , we then get easily that

$$(2^n - 1) \mid (2^{a_1} + 1)^{x_1} Q (2^{a_2} + 1)^{x_2} Q \cdots (2^{a_k} + 1)^{x_k} Q + 1.$$

Thus,

$$(-1) \equiv \prod_{i=1}^k (2^{a_i} + 1)^{x_i} Q \pmod{2^n - 1}.$$

Thus, we factor  $2^n - 1$ , take  $q_1, \dots, q_k$  to be all its distinct prime factors and attempt to find some numbers  $a_1, \dots, a_k$  in  $[5, n - 2]$  such that the congruences (2) are satisfied. If we are successful, then the argument based on the matrix with an odd determinant will work to find a solution of (5), which in turn can be easily lifted to a solution modulo  $2^n - 1$ . The factorizations of  $2^n - 2$  with weight 2 factors for odd  $33 \leq n \leq 249$  are given in Table 1, in the appendix.

**Remark 1** We have checked that Algorithm 1 works for most primes up to 250. But there are a few primes like 47 for which there is no  $a_j \in [5, p - 2]$  such that  $\left(\frac{2^{a_j} + 1}{q_i}\right) = (-1)^{\delta_{ij}}$ . In these cases, we use the following trick. We first find  $a_i$  and calculate  $\left(\frac{2^{a_j} + 1}{q_i}\right) = (-1)^{d_{i,j}}$ . Ideally,  $d_{i,j}$  should be Kronecker symbols, but if they are not, we can just record what they are. Because  $d_{i,j}$  are no longer Kronecker symbols, we cannot be certain that the system is solvable because it may have an even determinant and we cannot invert the matrix modulo powers of 2. However, we checked primes (and odd integers) up to 250. We observed that in the case of failure, we can use this trick and always get suitable  $a_i$ 's such that the corresponding matrix has odd determinant, and is therefore invertible.

#### 4 Further comments

One can go further than our choice of bound, namely 250, by using our method. We have yet to encounter an exponent for which we cannot apply Algorithm 1. If there is such an exponent  $n$  for which we cannot find  $a_j, d_{i,j}$  as above, then we can involve cubics in the factorization of  $-1 \pmod{2^n - 1}$ . More precisely, we do something similar as above using  $2^{a_i} + 2^{b_i} + 1$  and check if we can find such powers  $a_i, b_i$  such that the number above is a quadratic nonresidue modulo  $q_i$  and quadratic residue modulo  $q_j$  for all  $j \neq i$ . The rest of Algorithm 1 runs unchanged.

While, via Carlitz' result, we know that any permutation can be decomposed as a composition of inverses and affine functions, it would also be interesting to check whether one can modify our method in this paper to other exponents, other than the inverse and surely, the Gold  $2^k + 1$  exponents, to directly find their decomposition in quadratics, or quadratics and cubics, and we leave that for future work and the interested reader.

#### Appendix

**Table 1** Factorization of  $2^n - 2 \pmod{2^n - 1}$  for odd  $33 \leq n \leq 249$

$n = 33$	$(2^5 + 1) \cdot 599478 \cdot (2^{13} + 1) \cdot 299739 \cdot (2^{29} + 1) \cdot 1798434$
$n = 35$	$((2 + 1)(2^{17} + 1))^{967995} \cdot (2^{29} + 1) \cdot 276570$
$n = 37$	$(2^5 + 1) \cdot 77039772 \cdot (2^{13} + 1) \cdot 19259943$
$n = 39$	$((2^{11} + 1)(2^{21} + 1))^{1592955}$
$n = 41$	$(2^9 + 1) \cdot 20111512782 \cdot (2^{13} + 1) \cdot 3351918797$
$n = 43$	$((2^5 + 1)(2^{17} + 1)(2^{23} + 1))^{593211015}$
$n = 45$	$(2 + 1) \cdot 407925 \cdot (2^{13} + 1) \cdot 349650 \cdot ((2^{25} + 1)(2^{33} + 1)(2^{41} + 1))^{116550}$
$n = 47$	$(2^{11} + 1) \cdot 1927501725 \cdot (2^{37} + 1) \cdot 435242325 \cdot (2^{41} + 1) \cdot 1616614350$
$n = 49$	$(2^9 + 1) \cdot 34630287489 \cdot (2^{11} + 1) \cdot 3393768173922$
$n = 51$	$(1 + 2^{29}) \cdot 1500009615$
$n = 53$	$(1 + 2^5) \cdot 6512186850 \cdot (1 + 2^{15}) \cdot 3506562150 \cdot (1 + 2^{21}) \cdot 250468725$
$n = 55$	$(1 + 2) \cdot 6588945 \cdot (1 + 2^{11}) \cdot 5856840 \cdot (1 + 2^{17}) \cdot 732105$
$n = 57$	$(1 + 2^5) \cdot 1464210 \cdot (1 + 2^{33}) \cdot 10249470 \cdot (1 + 2^{47}) \cdot 732105$
$n = 59$	$(1 + 2^5) \cdot 396029391534 \cdot (1 + 2^{17}) \cdot 1188088174602 \cdot (1 + 2^{21}) \cdot 594044087301 \cdot (1 + 2^{47}) \cdot 198014695767$
$n = 61$	$(1 + 2^7) \cdot 3663925098759300 \cdot (1 + 2^{13}) \cdot 305327091563275$
$n = 63$	$(1 + 2^9) \cdot 1152921504606846975$
$n = 65$	$(1 + 2) \cdot 42958503 \cdot (1 + 2^5) \cdot 3735522 \cdot (1 + 2^{39}) \cdot 56032830 \cdot (1 + 2^{43}) \cdot 44826264 \cdot (1 + 2^{47}) \cdot 29884176$
$n = 67$	$(1 + 2^{17}) \cdot 72647571779055 \cdot (1 + 2^{23}) \cdot 72647571779055 \cdot (1 + 2^{29}) \cdot 72647571779055$
$n = 69$	$(1 + 2^5) \cdot 15295807610659665$
$n = 71$	$(1 + 2^{11}) \cdot 36566619637113225 \cdot (1 + 2^{17}) \cdot 243774642474215 \cdot (1 + 2^{53}) \cdot 19502197139793720 \cdot (1 + 2^{67}) \cdot 21939971782267935$
$n = 73$	$(1 + 2^{11}) \cdot 3659326099961865 \cdot (1 + 2^{13}) \cdot 14637304399847460$
$n = 75$	$(1 + 2^{31}) \cdot 1726845200475585 \cdot (1 + 2^{45}) \cdot 107064402429486270$

Table 1 continued

$n = 75$	$(1 + 2)^{36654975} \cdot (1 + 2^{39})^{17832150} \cdot (1 + 2^{41})^{9906750} \cdot$ $(1 + 2^{43})^{7925400} \cdot (1 + 2^{53})^{57459150} \cdot (1 + 2^{55})^{15850800} \cdot (1 + 2^{63})^{43589700}$
$n = 77$	$(1 + 2^{25})^{290641821624556479} \cdot (1 + 2^{31})^{290641821624556479} \cdot$ $(1 + 2^{41})^{290641821624556479} \cdot (1 + 2^{67})^{581283643249112958}$
$n = 79$	$(1 + 2^9)^{12102186118644337359} \cdot (1 + 2^{15})^{12102186118644337359} \cdot (1 + 2^{41})^{12102186118644337359}$
$n = 81$	$(1 + 2)^{106331083505919} \cdot (1 + 2^{25})^{155626336778778} \cdot (1 + 2^{37})^{105108887143782} \cdot$ $(1 + 2^{39})^{155626336778778} \cdot (1 + 2^{43})^{4073987873790}$
$n = 83$	$(1 + 2^{11})^{7239076764159456135965}$
$n = 85$	$(1 + 2^9)^{4760486403166879215} \cdot (1 + 2^{13})^{4760486403166879215} \cdot (1 + 2^{23})^{4760486403166879215}$
$n = 87$	$(1 + 2^{39})^{3371346107168004} \cdot (1 + 2^{41})^{280945508930667} \cdot (1 + 2^{53})^{2809455089306670} \cdot$ $(1 + 2^{61})^{4214182633960005} \cdot (1 + 2^{71})^{16856730535584002} \cdot (1 + 2^{83})^{280945508930667}$
$n = 89$	$(1 + 2^{13})^{309485009821345068724781055}$
$n = 91$	$(1 + 2^{59})^{280368506850705} \cdot (1 + 2^{67})^{1682211041104230} \cdot$ $(1 + 2^{71})^{280368506850705} \cdot (1 + 2^{73})^{280368506850705} \cdot (1 + 2^{81})^{3364422082208460}$
$n = 93$	$(1 + 2^{17})^{2305843010287435773}$
$n = 95$	$(1 + 2^{43})^{735437817756963125} \cdot (1 + 2^{51})^{7354378117756963125}$
$n = 97$	$(1 + 2^5)^{612535370185410489825162846} \cdot (1 + 2^9)^{102089228364235081637527141}$
$n = 99$	$(1 + 2)^{160190876329840719} \cdot (1 + 2^{23})^{160190876329840719} \cdot (1 + 2^{35})^{58251227756305716} \cdot$ $(1 + 2^{57})^{29125613878152858} \cdot (1 + 2^{59})^{101939648573535003} \cdot (1 + 2^{75})^{58251227756305716}$
$n = 101$	$(1 + 2^7)^{261479084205457681314981849} \cdot (1 + 2^9)^{1045916336821830725259927396}$
$n = 103$	$(1 + 2^5)^{8204858250687037849538541156} \cdot (1 + 2^9)^{2051214562671759462384635289}$
$n = 105$	$(1 + 2^7)^{736412106675} \cdot (1 + 2^{29})^{6627708960075} \cdot (1 + 2^{37})^{1472824213350} \cdot$ $(1 + 2^{55})^{6627708960075} \cdot (1 + 2^{69})^{15464654240175} \cdot (1 + 2^{79})^{736412106675} \cdot$ $(1 + 2^{83})^{4418472640050} \cdot (1 + 2^{85})^{441847264005} \cdot (1 + 2^{87})^{13255417920150}$

Table 1 continued

$n = 107$	$(1 + 2^5)27043212804868893898596335048021$
$n = 109$	$(1 + 2^7)744308608310570490215126499806 \cdot (1 + 2^{15})372154304155285245107563249903$
$n = 111$	$(1 + 2^{17})2078233794395472907116 \cdot (1 + 2^{31})742226355141240323970 \cdot (1 + 2^{39})890671626169488388764$
$n = 113$	$(1 + 2^{71})180254971962872650107 \cdot (1 + 2^{87})519558448598868226779$ $(1 + 2^{15})82901226266607482846190 \cdot (1 + 2^{25})13816871044434580474365$ $(1 + 2^{29})37854441217628987601 \cdot (1 + 2^{75})13816871044434580474365$ $(1 + 2^{97})82901226266607482846190$
$n = 115$	$(1 + 2^{17})23588654041464621525 \cdot (1 + 2^{23})165120578290252350675$ $(1 + 2^{39})23588654041464621525 \cdot (1 + 2^{45})23588654041464621525$
$n = 117$	$(1 + 2^{75})188709232331716972200$ $(1 + 2^5)350280341971560 \cdot (1 + 2^{11})481635470210895 \cdot (1 + 2^{31})1225981196900460$ $(1 + 2^{55})1269766239646905 \cdot (1 + 2^{71})1225981196900460 \cdot (1 + 2^{87})744345726689565$ $(1 + 2^{93})1903697510715 \cdot (1 + 2^{111})1094626068661125 \cdot (1 + 2^{115})1182196154154015$ $(1 + 2^{21})121807344007626864485535 \cdot (1 + 2^{25})28109387078683122573585$ $(1 + 2^{51})6635419517925198843570 \cdot (1 + 2^{81})5968559856373716359791215$ $(1 + 2^{97})852651408053388051398745 \cdot (1 + 2^{109})6635419517925198843570$
$n = 121$	$(1 + 2^9)99244104353509123769903900571 \cdot (1 + 2^{19})893196939181582113929135105139$ $(1 + 2^{25})893196939181582113929135105139 \cdot (1 + 2^{43})1786393878363164227858270210278$ $(1 + 2^5)38263506571610465341512132024 \cdot (1 + 2^9)19131753285805232670756066012$ $(1 + 2^{27})4782938321451308167689016503 \cdot (1 + 2^{53})28697629928707849006134099018$ $(1 + 2^{113})7726284980805959347805334351$
$n = 123$	$(1 + 2^{23})2898591397871459238374625 \cdot (1 + 2^{29})644131421749213164083250$ $(1 + 2^{95})1610328554373032910208125 \cdot (1 + 2^{109})4186854241369885566541125$ $(1 + 2^{121})1932394265247639492249750$
$n = 125$	

Table 1 continued

$n = 127$	$(1 + 2^5)28356863910078205288614550619314017621$
$n = 129$	$(1 + 2^9)8471295533565243108183419405055 \cdot (1 + 2^{79})9529016348217371325290685495$
$n = 131$	$(1 + 2^9)1293849303881895298339827404683529321 \cdot (1 + 2^{15})2587698607763790596679654809367058642$
$n = 133$	$(1 + 2^5)27256203475454233141905720953493 \cdot (1 + 2^{17})81768610426362699425717162860479$
	$(1 + 2^{45})81768610426362699425717162860479$
$n = 135$	$(1 + 2^9)1390256215369200900 \cdot (1 + 2^{25})9826330930229511961200 \cdot (1 + 2^{47})38551429107264868200$
	$(1 + 2^{55})2813183451799578021150 \cdot (1 + 2^{89})7686726614776311776100$
	$(1 + 2^{101})1406591725899789010575 \cdot (1 + 2^{109})4576375896941567062575$
	$(1 + 2^{117})1042692161526900675 \cdot (1 + 2^{121})2119793164384189072275$
$n = 137$	$(1 + 2^5)39741006355730039527321333167397040041 \cdot (1 + 2^7)79482012711460079054642666334794080082$
$n = 139$	$(1 + 2^9)17408530362059304982034022473992637175 \cdot (1 + 2^{17})457116770994992690994328817697837300$
$n = 141$	$(1 + 2)1216799735702178355508978464575 \cdot (1 + 2^{51})110618157791107123228088951325$
	$(1 + 2^{65})63210375880632641844622257900 \cdot (1 + 2^{121})56889338292569377660160032110$
$n = 145$	$(1 + 2^{41})534639083977880631530660485081925505 \cdot (1 + 2^{49})76377011996840090218665783583132215$
	$(1 + 2^{135})305508047987360360874663134332528860 \cdot (1 + 2^{137})4144489023084345980857833217689345$
	$(1 + 2^{139})534639083977880631530660485081925505$
$n = 147$	$(1 + 2^{15})17249119260282613026137951811234 \cdot (1 + 2^{59})51747357780847839078413855433702$
	$(1 + 2^{67})43122798150706532565344879528085 \cdot (1 + 2^{71})96786724738252439757774062940813$
	$(1 + 2^{73})8624559630141306513068975905617$
$n = 149$	$(1 + 2^9)29933886172524326364132038117944134026225$
$n = 151$	$(1 + 2^{35})47657859344287051433215338407025 \cdot (1 + 2^{53})47657859344287051433215338407025$
	$(1 + 2^{55})95315718688574102866430676814050 \cdot (1 + 2^{81})95315718688574102866430676814050$
	$(1 + 2^{119})47657859344287051433215338407025$
$n = 153$	$(1 + 2^{67})74105228687928761744692516074690 \cdot (1 + 2^{85})566868663181345103125787385$

Table 1 continued

$n = 155$	$(1 + 2^{101})_{185263071719821904361731290186725} \cdot (1 + 2^{115})_{24701742895976253914897505358230}$ , $(1 + 2^{125})_{66694705819135885570223264467221} \cdot (1 + 2^{147})_{22231568606378628523407754822407}$ $(1 + 2^{17})_{62671642336461616797239779725} \cdot (1 + 2^{43})_{35812367049406638169851302700}$ , $(1 + 2^{51})_{17906183524703319084925651350} \cdot (1 + 2^{59})_{2984363920783886514154275225}$ , $(1 + 2^{73})_{26859275287054978627388477025} \cdot (1 + 2^{101})_{17906183524703319084925651350}$ , $(1 + 2^{123})_{865014224607504542831738415625}$ $(1 + 2^{15})_{1707444675887681902216221662393643900} \cdot (1 + 2^{17})_{341488935177536380443244332478728780}$ , $(1 + 2^{29})_{3841750520747284279986498740385698775} \cdot (1 + 2^{45})_{30734004165978274239891989923085590200}$ $(1 + 2^{57})_{9362516203257056384802075} \cdot (1 + 2^{65})_{44348760962796582875378250}$ , $(1 + 2^{69})_{4434876096279658287537825} \cdot (1 + 2^{89})_{38435592834423705158661150}$ , $(1 + 2^{101})_{79907677410444293469150} \cdot (1 + 2^{123})_{5913168128372877167171100}$ , $(1 + 2^{127})_{2002242486366485713350} \cdot (1 + 2^{137})_{48783637059076241162916075}$ $(1 + 2^{29})_{93343471924356402246389002034385} \cdot (1 + 2^{43})_{62228981282904268164259334689590}$ , $(1 + 2^{47})_{82971975043872357552345779586120} \cdot (1 + 2^{87})_{217801434490164938574907671413565}$ , $(1 + 2^{157})_{248915925131617072657037338758360}$ $(1 + 2^{13})_{168486137937535997136381884224759350} \cdot (1 + 2^{87})_{5616204597917866571212729474158645}$ , $(1 + 2^{89})_{1925555862143268538701507248282964} \cdot (1 + 2^{119})_{78626864370850131996978212638221030}$ $(1 + 2^{61})_{39948352158132627380823842541450} \cdot (1 + 2^{105})_{9321282170230946388858896593005}$ , $(1 + 2^{109})_{13316117386044209126941280847150} \cdot (1 + 2^{113})_{15535470283718243981431494321675}$ , $(1 + 2^{119})_{19974176079066313690411921270725} \cdot (1 + 2^{123})_{79896704316265254761647685082900}$ , $(1 + 2^{127})_{3698921496123391424150355790875} \cdot (1 + 2^{135})_{5326446954417683650776512338860}$ , $(1 + 2^{147})_{4438705795348069708980426949050} \cdot (1 + 2^{157})_{13316117386044209126941280847150}$ $(1 + 2^{25})_{3500601233908136352424481302564849390771914057740}$ , $(1 + 2^{33})_{17503006169540681762122406512824469538595702887}$
$n = 157$	
$n = 159$	
$n = 161$	
$n = 163$	
$n = 165$	
$n = 167$	

Table 1 continued

$n = 169$	$(1 + 2^{15})_{7089726406583596958466287242575266870940}$ , $(1 + 2^{25})_{7286663251210919096201461888202357617355}$ , $(1 + 2^{55})_{29146653004843676384805847552809430469420}$ $(1 + 2^{49})_{49149123355767553400835304429946193135}$ , $(1 + 2^{55})_{9829824671153510680167060885989238627}$ , $(1 + 2^{77})_{9829824671153510680167060885989238627}$ , $(1 + 2^{99})_{9829824671153510680167060885989238627}$ , $(1 + 2^{109})_{9829824671153510680167060885989238627}$ , $(1 + 2^{159})_{9829824671153510680167060885989238627}$ , $(1 + 2^{163})_{9829824671153510680167060885989238627}$ $(1 + 2^{21})_{752712011377013221558430642567508556008861}$ , $(1 + 2^{61})_{752712011377013221558430642567508556008861}$ , $(1 + 2^{69})_{752712011377013221558430642567508556008861}$ , $(1 + 2^{77})_{31613904477834555305450869878353593552372162}$ $(1 + 2^{19})_{281198684623467689204913686779425}$ , $(1 + 2^{43})_{540766701198976325394064782268125}$ , $(1 + 2^{61})_{12329480787336660218984677035713250}$ , $(1 + 2^{97})_{129784008287754318094575547744350}$ , $(1 + 2^{105})_{6651799969190141587990774087125}$ , $(1 + 2^{123})_{11139794044698912303117734514723375}$ , $(1 + 2^{141})_{4975053651030582193625395996866750}$ , $(1 + 2^{163})_{1838606784076519506339820259711625}$ , $(1 + 2^{165})_{111492889070054279163020169625}$ $(1 + 2^{19})_{102104448867391604403906908898445293975}$ , $(1 + 2^{57})_{4288386852430447384964090173734702346950}$ , $(1 + 2^{93})_{81683559093913283523125527118756235180}$ , $(1 + 2^{103})_{1286516055729134215489227052120410704085}$ , $(1 + 2^{133})_{183788007961304887920324360172015291550}$ , $(1 + 2^{163})_{568867643689753224536052778148480923575}$ $(1 + 2^{21})_{1713334865061395551905989490523888483510297545}$ , $(1 + 2^{29})_{17731656063809998410201669013040877638868476180}$ $(1 + 2^{11})_{168252628616094460214312446168738419261880}$ , $(1 + 2^{21})_{21031578285770118075267890557710923024077350}$ , $(1 + 2^{31})_{2103157828577011807526789055771092302407735}$ , $(1 + 2^{17})_{5301342361191869603932356617428842175355175}$ .
$n = 171$	
$n = 173$	
$n = 175$	
$n = 177$	
$n = 179$	
$n = 181$	
$n = 183$	



Table 1 continued

$n = 185$	$(1 + 2^5)$ , $171011043909415148513946987658994908882425$ , $(1 + 2^{17})$ , $1279634363046313352673327459379375697499525$ $(1 + 2^1)$ , $24289606148175875174394125504156277451293856980$ , $(1 + 2^5)$ , $56675747679077042073586292843031314053018999620$ , $(1 + 2^6)$ , $6072401537043968793598531376039069362823464245$ , $(1 + 2^7)$ , $28337873839538521036793146421515657026509499810$ , $(1 + 2^{12})$ , $3333867510533943651387428990766547885471705860$ $(1 + 2^9)$ , $52332852605905914814562661586433935229041537035$ , $(1 + 2^{19})$ , $52332852605905914814562661586433935229041537035$ , $(1 + 2^4)$ , $203629776676711340710745472505584548799755$ , $(1 + 2^8)$ , $104665705211811829629125323172867870458083074070$ $(1 + 2^7)$ , $954808575327093401067436576289941581$ , $(1 + 2^{11})$ , $76741427691674298191288254054776183774$ , $(1 + 2^1)$ , $862835224381042468504831900414614$ , $(1 + 2^{33})$ , $8687708795283882814108104232616171748$ , $(1 + 2^{39})$ , $6515781596462912110581078174462128811$ , $(1 + 2^7)$ , $6081396156698719698756729628313202236$ , $(1 + 2^8)$ , $5309155374895706164171748088209938460$ , $(1 + 2^{125})$ , $62503238277181268023722194340210791187$ , $(1 + 2^{157})$ , $121386597889660918208232678583498177479$ $(1 + 2^{55})$ , $1025444869877616060103489665965652402208725$ , $(1 + 2^{77})$ , $1860992541629747664632259023419146952156575$ , $(1 + 2^{179})$ , $1063424309502712951218433727668083972660900$ , $(1 + 2^{183})$ , $2126848619005425902436867455336167945321800$ , $(1 + 2^{189})$ , $138245160235352683658396384596850916445917$ $(1 + 2^5)$ , $690644713229389686815238348164730529976649425988651$ , $(1 + 2^9)$ , $76738301469932187423915372018303392219627713998739$ , $(1 + 2^{13})$ , $98663530461341383830748335452104361425235632284093$
$n = 187$	
$n = 189$	
$n = 191$	
$n = 193$	

Table 1 continued

$n = 195$	$(1 + 2^{31})_{397218618589975176651322156679935564968150}$ , $(1 + 2^{129})_{42129247426209488432715986314538620526925}$ , $(1 + 2^{163})_{66203103098329196108553692779989260828025}$
$n = 197$	$(1 + 2^5)_{47788807121282329843547481918370106279929779662675299482}$ , $(1 + 2^{13})_{7964801186880388307257913653061684379988296610445883247}$
$n = 199$	$(1 + 2^7)_{9012349943070385113930109307619809450853768536749084363}$ , $(1 + 2^{27})_{234321098519830012962182841998115045722197981955476193438}$
$n = 201$	$(1 + 2^{67})_{201 \cdot (1 + 2^{107})_{91503141262546293397851719230754031960084170}}$ , $(1 + 2^{119})_{14182986896113175476667016480770187495381304635}$ , $(1 + 2^{145})_{3507620415167774580250982570513057122513655985}$ , $(1 + 2^{177})_{83184673877496630361683381118886730178189470}$
$n = 203$	$(1 + 2^{57})_{718674251279934430341052428990271148449812}$ , $(1 + 2^{81})_{51205540403695328161799985565556819327049105}$ , $(1 + 2^{111})_{6288399698699426265484208753664872548935855}$ , $(1 + 2^{127})_{18865199096098278796452626260994617646807565}$ , $(1 + 2^{153})_{2695028442299754113778946608713516806686795}$ , $(1 + 2^{175})_{64680682615194098730694718609124403360483080}$ , $(1 + 2^{193})_{8085085326899262341336839826140550420060385}$ , $(1 + 2^{43})_{9467961424350347777980448419013907428323430550}$ , $(1 + 2^{67})_{29756450190815378730795695031186566203302210300}$ , $(1 + 2^{131})_{676282958882167698427174887072421959165959325}$ , $(1 + 2^{145})_{7213684894743122116556532128772500897770232800}$ , $(1 + 2^{157})_{7728948101510487982024855852256250961896667800}$ , $(1 + 2^{187})_{16907073972054192460679372176810548979148983125}$
$n = 205$	

Table 1 continued

$n = 207$	$(1 + 2^5)$ , 33192619261066535128289058132930982761836775, $(1 + 2^{121})$ , 46469666965493149179604681386103375866571485, $(1 + 2^{127})$ , 1021311361878970311639666332716710716190267, $(1 + 2^{179})$ , 19915571556639921076973434879758589657102065, $(1 + 2^{187})$ , 39831143113279842153946869759517179314204130, $(1 + 2^{199})$ , 3983114311327984215394686975951717931420413 $(1 + 2^{59})$ , 27025033704215459392793016292662090505143401152585, $(1 + 2^{61})$ , 3603337827228274585705735505688278340191201536780, $(1 + 2^{87})$ , 180166891361436372928528677528441393670095600768390, $(1 + 2^{97})$ , 25738127337348053275504096789777341952870800109770 $(1 + 2^9)$ , 11549298719735652752241081615533051512738585560465529713690, $(1 + 2^{13})$ , 64162770665198070845783786752947306263254753359196095205, $(1 + 2^{55})$ , 2309859743947130550448216323106103025477171120931059427380 $(1 + 2^{11})$ , 549773658931870098609894638477660690688115321335, $(1 + 2^{41})$ , 140967604854325666310253708678914376684310649265, $(1 + 2^{85})$ , 183257886310623366203329821282588689696038440445, $(1 + 2^{119})$ , 2356172823993728994042811987918997438866335137715, $(1 + 2^{161})$ , 1099547317863740197219978927695552138137623064267, $(1 + 2^{203})$ , 157078188262485996028541325279331625910890091810 $(1 + 2^{41})$ , 66443114885376278757699109185773253174500402025, $(1 + 2^{97})$ , 31006786946508930086926250953360851481433520945, $(1 + 2^{119})$ , 186040721679053580521557505720165108888601125670, 
$n = 209$	
$n = 211$	
$n = 213$	
$n = 215$	

Table 1 continued

$n = 217$	$(1 + 2^{151})_{186040721679053580521557505720165108888601125670}$ .	
	$(1 + 2^{203})_{2790610825185803707823336258580247663332901688505}$	
	$(1 + 2^{13})_{1126940817087752014462533930787563178937611179075}$ .	
	$(1 + 2^{57})_{125215646343083557162503770087507019881956797675}$ .	
	$(1 + 2^{89})_{50086258537233422865001508035002807952782719070}$ .	
	$(1 + 2^{185})_{751293878058501342975022620525042119291740786050}$ .	
	$(1 + 2^{215})_{9537309672323317621714046370301517484866488275}$	
	$(1 + 2^{19})_{2066997275827785054568851212103878502402165134820}$ .	
	$(1 + 2^{63})_{15659070271422614049764024334120291684846887385}$ .	
	$(1 + 2^{107})_{826798910331140218275404848415514009608660539280}$ .	
$n = 219$	$(1 + 2^{113})_{861248864928243772737021338376616042667568806175}$ .	
	$(1 + 2^{115})_{2239247048813433809116255479779201710935678896055}$ .	
	$(1 + 2^{139})_{9802832608939360014892925802660670404346311615}$ .	
	$(1 + 2^{189})_{574165909952162515158014225584410695111712537450}$	
	$(1 + 2^9)_{3989486683832532366484265709728099870565523986917322701595}$ .	
	$(1 + 2^{19})_{3989486683832532366484265709728099870565523986917322701595}$ .	
	$(1 + 2^{29})_{3989486683832532366484265709728099870565523986917322701595}$	
	$(1 + 2^{17})_{1014848095919801109402176209373936431577327592183}$ .	
	$(1 + 2^{91})_{1503478660621927569484705495368794713447892729160}$ .	
	$(1 + 2^{103})_{1691413493199668515670293682289894052628879320305}$ .	
$n = 223$	$(1 + 2^{113})_{563804497733222838556764560763298017542959773435}$ .	
	$(1 + 2^{145})_{2631087656088373246598234616895390748533812276030}$	
	$(1 + 2^{29})_{64638048753257449056214060125 \cdot (1 + 2^{31})_{788456198653595814230254674000}}$ .	
	$(1 + 2^{49})_{5797472048923498634045990250 \cdot (1 + 2^{51})_{84063344709390730193666858625}}$ .	
	$n = 225$	

Table 1 continued

$n = 227$	$(1 + 2^{85})_{4479864765077248944490083375} \cdot (1 + 2^{97})_{1809865365091208573573993683500}$ , $(1 + 2^{99})_{365703246128755015876741500} \cdot (1 + 2^{105})_{5302697068866947730212751750}$ , $(1 + 2^{115})_{68066717742077353015043250} \cdot (1 + 2^{131})_{5270429135384998758223627500}$ , $(1 + 2^{203})_{152315402012626464112662834750} \cdot (1 + 2^{207})_{828774981539291054730665424375}$ , $(1 + 2^{217})_{438130774024554946771130154075} \cdot (1 + 2^{219})_{9407716006662227834291750875}$ $(1 + 2^5)_{59383142438657794704063431302361624145812280978139757521155099815}$ , $(1 + 2^7)_{118766284877315589408126862604723248291624561956279515042310199630}$ $(1 + 2^9)_{14738569738721986750960956555361987370219507869771466051}$ , $(1 + 2^{21})_{1768628368646638410115314786424343848442634094437257592612}$ , $(1 + 2^{121})_{589542789548879470038438262141447949480878031479085864204}$ $(1 + 2^{41})_{459189704451443127647362594916155732882807466830218}$ , $(1 + 2^{55})_{1567200356489566988557551518485173149770673948226}$ , $(1 + 2^{69})_{2755138226708658765884175569496934397296844800981308}$ $(1 + 2^{91})_{1147974261128607819118406487290389332207018667075545}$ , $(1 + 2^{131})_{535721321860016982252526360735515021696608711301921}$ , $(1 + 2^{157})_{918379408902886255294725189832311465765614933660436}$ $(1 + 2^{159})_{1147974261128607819118406487290389332207018667075545}$ , $(1 + 2^{209})_{235080053473435048283632727727759724656010922339}$ $(1 + 2^{15})_{170383215223200602421013846948443997824061934891243478185488130}$ , $(1 + 2^{23})_{2839720253866767070168974491407332970676989148540579697581355}$ $(1 + 2^{49})_{2839720253866767070168974491407332970676989148540579697581355}$ , $(1 + 2^{113})_{2839720253866767070168974491407332970676989148540579697581355}$ $(1 + 2^{73})_{23191222403616672243206263595493280420250247335633250}$ , $(1 + 2^{105})_{26891949382917205047973220552220931551141244250893875}$
$n = 229$	
$n = 231$	
$n = 233$	
$n = 235$	

Table 1 continued

	(1 + 2 <sup>119</sup> ), 8141599354461172170487305304800832487960193213573375.
	(1 + 2 <sup>141</sup> ), 363659699007176721748930895080669461243705878250
	(1 + 2 <sup>167</sup> ), 14062762521342024658114436435565074297385788277990375.
	(1 + 2 <sup>171</sup> ), 23684652667523409950508524523056967237702380257668000
	(1 + 2 <sup>197</sup> ), 2556865912971277210566261170102740781342870595998250
$n = 237$	(1 + 2 <sup>9</sup> ), 312620627852416761979153117722703908013332701360090433.
	(1 + 2 <sup>169</sup> ), 3647240658278195556423453040098212260155548182534388385
	(1 + 2 <sup>173</sup> ), 104206875950805587326384372574234636004444237866968110.
	(1 + 2 <sup>175</sup> ), 173678126584675978877307287623724393340740389644494685
	(1 + 2 <sup>199</sup> ), 4290871362680230066638053298835083795312417433239339810.
	(1 + 2 <sup>225</sup> ), 416827503803222349305537490296938544017776935146787244
	(1 + 2 <sup>33</sup> ), 67961006054873209125902851678848675655072326382628355
$n = 239$	(1 + 2 <sup>59</sup> ), 137903930258717580167839711391793163262983138814261779866.
	(1 + 2 <sup>73</sup> ), 251729396504008281258755028731051012305445412121217150293.
	(1 + 2 <sup>87</sup> ), 2068558953880763702517595670876897448944747082213922669799.
	(1 + 2 <sup>197</sup> ), 298791848893888090363652708015551853736463467430900523043.
	(1 + 2 <sup>199</sup> ), 91935953505811720111893140927862108841988759209507853244.
	(1 + 2 <sup>237</sup> ), 6566853821843694293706652923418722060142054229250560946
$n = 241$	(1 + 2 <sup>7</sup> ), 916414411031455987244373856003197176202834172185057465573737668369009.
	(1 + 2 <sup>9</sup> ), 5498486466188735923466243136019183057217005033110344793442426010214054
$n = 243$	(1 + 2 <sup>3</sup> ), 785013025560884300793728032156196770104389659275.
	(1 + 2 <sup>31</sup> ), 22335098635205076340574688781013129860710668130.
	(1 + 2 <sup>35</sup> ), 847419918806310249392392603750204044715198879050.
	(1 + 2 <sup>61</sup> ), 13203984781400648071927977793636444176554243945.

Table 1 continued

$n = 245$	(1 + 2151) 41135370735706828274307725135899531886322869175. (1 + 2155) 725890705644164981068677385382926720473096714225. (1 + 2163) 160944093106624814807082316216124023996297461525. (1 + 2177) 387579652787382207086443128846992547582920417550. (1 + 2181) 91968053203785608461189894980642299426455692300 (1 + 269) 404534281273826986829987345146663806009193260698421162909645. (1 + 2117) 652474647215849978758044105075264203240634291449066391789750. (1 + 2125) 1096157407322627964313514096526443861444265609634431538206780. (1 + 2141) 1057008928489676965588031450221928009249827552147487554699395. (1 + 2151) 404534281273826986829987345146663806009193260698421162909645. (1 + 2165) 1578988646262356948594466734282139371842334985306740668131195. (1 + 2167) 404534281273826986829987345146663806009193260698421162909645 (1 + 2) 13405735738844138070454028628033486890775035828909707815645. (1 + 29) 130787665744820859223941742712520475015390278857472885673800. (1 + 235) 16348458218102607402992717839065059376923784857184110709225. (1 + 271) 85011982734133558495562132763138308760003681257357375687970. (1 + 2147) 81742291090513037014963589195325296884618924285920555546125. (1 + 2195) 150405815606543988107553300411939854626769882068609381852487 (1 + 297) 2925277021907294342301024913121771097283901482612310325863937852070. (1 + 2119) 204769391533510603961071743918939768098731037828617228104756496449. (1 + 2137) 585055404381458868460204982625542194567802965224620651727875704140. (1 + 2173) 633810021413247107498555397844337377448453212326672372705198679485. (1 + 2199) 536300787349670629421854567406747011687152718122568930750552728795
$n = 247$	
$n = 249$	

**Acknowledgements** The authors would like to thank the editor for efficiently handling our paper and the reviewers for their careful reading, beneficial comments and constructive suggestions. The first and the third-named authors worked on this paper during visits to the Max Planck Institute for Software Systems in Saarbrücken, Germany in Spring of 2022 and 2023. They thank Professor J. Ouaknine for the invitation and the Institute for hospitality and support. During the final stages of the preparation of this paper, the first-named author was a fellow at the Stellenbosch Institute for Advanced Study. He thanks this Institution for hospitality and support.

## References

1. Bilgin, B., Nikova, S., Nikov, V., Rijmen, V., Stütz, G.: Threshold Implementations of All  $3 \times 3$  and  $4 \times 4$  S-Boxes. In: Prouff, E., Schaumont, P. (eds.) *Cryptographic Hardware and Embedded Systems - CHES 2012*, LNCS 7428. Springer, Berlin, Heidelberg (2012)
2. Carlitz, L.: Permutations in a finite field<sup>\*</sup>. *Proc. Amer. Math. Soc.* **4**, 538 (1953)
3. Hall, R.T., Tenenbaum, G.: *Divisors*, Cambridge Tracts in Mathematics, 90. Cambridge University Press, Cambridge (1988)
4. Kontorovich, A., Lagarias, J.: On toric orbits in the affine sieve. *Exp. Math.* **30**, 575–587 (2021)
5. Luca, F., Stănică, P.: Asymptotics on a class of  $\mathcal{S}$ -unit integers. *Periodica Math. Hungarica*, <https://doi.org/10.1007/s10998-023-00551-4>
6. Luca, F., Stănică, P.: Prime divisors of Lucas sequences and a conjecture of Skalba. *Int. J. Number Theory* **1**(4), 583–591 (2005)
7. Moree, P.: On the divisors of  $a^k + b^k$ . *Acta Arith.* LXXX.3, 197–212 (1997)
8. Murata, L., Pomerance, C.: On the largest prime factor of a Mersenne number. In: *Number Theory*, 209–218, CRM Proc. Lecture Notes 36, Amer. Math. Soc., Providence, RI, (2004)
9. Nikova, S., Nikov, V., Rijmen, V.: Decomposition of permutations in a finite field. *Cryptogr. Commun.* **11**, 379–384 (2019)
10. Nikova, S., Rechberger, C., Rijmen, V.: Threshold Implementations Against Side-Channel Attacks and Glitches. In: Ning, P., Qing, S., Li, N. (eds.) *Information and Communications Security - ICICS, LNCS 4307*. Springer, Berlin, Heidelberg (2006)
11. Petrides, G.: On decompositions of permutation polynomials into quadratic and cubic power permutations. *Cryptogr. Commun.* **15**, 199–207 (2023)
12. Rotkiewicz, A.: Applications of Jacobi’s symbol to Lehmer’s numbers. *Acta Arith.* **42**, 163–187 (1983)

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.