Cryptography and Communications
https://doi.org/10.1007/s12095-024-00702-5

RESEARCH

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

Florian Luca[1,2] · Santanu Sarkar[3] · Pantelimon Stănică[4]

Received: 28 September 2023 / Accepted: 1 February 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

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

2 Centro de Ciencias Matemáticas, UNAM, Morelia, Mexico

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

4 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 $\mathbf{x} = (x_1, x_2, \ldots, x_s)$. To implement a function $F(x, y, z, \ldots,) = a$ 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**: $a = F(x, y, z, \ldots) = \sum_{i=1}^{s} F_i(\mathbf{x}, \mathbf{y}, \mathbf{z}, \ldots)$, for all $\mathbf{x}, \mathbf{y}, \mathbf{z}, \ldots$, 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 $(a_1, a_2, \ldots, a_s)$ with $\sum_{i=1}^{s} a_i = a$, the number of tuples $(\mathbf{x}, \mathbf{y}, \mathbf{z}, \ldots) \in \mathbb{F}_2^{ms}$ for which $F_j(\mathbf{x}, \mathbf{y}, \mathbf{z}, \ldots) = a_j$, $1 \leq j \leq s$, is equal to $2^{(s-1)(m-n)}$ times the number of $(x, y, z, \ldots) \in \mathbb{F}_2^m$, for which $a = F(x, y, z, \ldots)$. So, if F is a permutation on $\mathbb{F}_2^m$, then the F_i's form together a permutation on 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 $a_1 \geq 0, \ldots, a_r \geq 0$ 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 ν_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 $\frac{n-1}{2^{\nu_2(n-1)}} \equiv 2^k \pmod{2^n-1}$, for some k, then

$$\begin{aligned} 2^n - 2 &= 2\left(2^{\left(\frac{n-1}{2^{\nu_2(n-1)}}\right)2^{\nu_2(n-1)}} - 1\right) \\ &= 2\left(2^{\frac{n-1}{2^{\nu_2(n-1)}}} - 1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}} + 1\right) \\ &\equiv 2\left(2^{2^k} - 1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}} + 1\right) \\ &= 2\prod_{j=0}^{k-1}\left(2^{2^j} + 1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}} + 1\right). \end{aligned}$$

This implies, via Carlitz [2], that for all odd integers (coined *good integers*, with the counterparts named *bad integers* in [7]) satisfying the congruence $\frac{n-1}{2^{\nu_2(n-1)}} \equiv 2^k \pmod{2^n-1}$, 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*

$$\frac{n-1}{2^{\nu_2(n-1)}} \equiv 2^k 3^s \pmod{2^n-1},$$

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 $k + s + \nu_2(n-1)$.

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

$$\begin{aligned} 2^n - 2 &= 2\left(2^{\frac{n-1}{2^{\nu_2(n-1)}}} - 1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}} + 1\right) \\ &\equiv 2\left(2^{2^k 3^s} - 1\right)\prod_{j=1}^{\nu_2(n-1)}\left(2^{\frac{n-1}{2^j}} + 1\right) \end{aligned}$$

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

$$\cdots\cdots\cdots\cdots$$

$$= 2\left(2^{2^k} - 1\right)\prod_{j=0}^{s-1}\left(2^{2^{k+1}3^j} + 2^{2^k 3^j} + 1\right)\prod_{j=1}^{v_2(n-1)}\left(2^{\frac{n-1}{2^j}} + 1\right)$$

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

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 $\mathcal{B}(x) = \{n \le x : n \text{ is superbad}\}$, or its complement*

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

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

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

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*

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

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 $p \ge 3$ 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

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

So, if $\delta > 0$ is fixed, the set of $n \le x$ such that $\omega(n) \ge (1 + \delta)\log\log x$ 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

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

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

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

as $x \to \infty$, where $Q_1(\delta) := (1+\delta)\log((1+\delta)/(0.5e))+1$. Taking $\delta = 0.36$, we get $Q_1(\delta) = 1.00086\ldots$. 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

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

is convergent, we are led to believe that maybe there are at most finitely many prime numbers p such that $\omega(N_p) \ge 1.36\log p$. It has been noted that perhaps infinitely often $\omega(N_p) \ge 2$. 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 $\omega(N_p) \ge 2$.

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 $q_1, \ldots, q_k$ with $k \le 1.36\log p$. 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:

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

where $\ell := \ell(a, p)$ is minimal with $r_\ell = 1$. Note that r_i are all odd for $i = 1, \ldots, \ell$. In particular, $r_j \geq 3$ for $j = 1, \ldots, \ell - 1$. 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 $2^{r_j} - 1$ 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 ℓ 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

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

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 $\underbrace{(\pm 1, \pm 1, \cdots, \pm 1)}_{k \text{ times}}$. Indeed, if not, then somehow 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 $i \in \{1, \ldots, k\}$ and search for a_i such that

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

where δ_{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 $\{1, \ldots, k\}$. 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 $2^p - 1 = q_1 \ldots q_k$ for $p > p_0$ with prime factors $q_1 < \cdots < q_k$ and $k < 1.36 \log p$. Then for each $i = 1, \ldots, k$, 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), $2^p - 1 = q_1 \cdots q_k$, (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 $\{1, \ldots, k\}$ 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 $i = 1, \ldots, k$, where R_i is odd. Let

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

and write $x_i = y_i R$ for $i = 1, \ldots, k$. Let ρ_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^{α_j}. Writing $(R/R_j)^*$ for the inverse of (R/R_j) modulo 2^{α_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 $i = 1, \ldots, k$. 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 $y_1, \ldots, y_k$. 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

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

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

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

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

Algorithm 1

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

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

Indeed, if we have found the above relation, then

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

Writing $Q := (2^n - 1)/(q_1 \ldots q_k)$, 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 $q_1, \ldots, q_k$ to be all its distinct prime factors and attempt to find some numbers $a_1, \ldots, a_k$ 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 $33 \le n \le 249$ 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* $(\frac{2^{a_j}+1}{q_i}) = (-1)^{d_{i,j}}$*. 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 $33 \le n \le 249$

$n = 33$	$(2^5 + 1)^{599478} \cdot (2^{13} + 1)^{299739} \cdot (2^{29} + 1)^{1798434}$
$n = 35$	$\left((2 + 1)(2^{17} + 1)\right)^{967995} \cdot (2^{29} + 1)^{276570}$
$n = 37$	$(2^5 + 1)^{77039772} \cdot (2^{13} + 1)^{19259943}$
$n = 39$	$\left((2^{11} + 1)(2^{21} + 1)\right)^{1592955}$
$n = 41$	$(2^9 + 1)^{20111512782} \cdot (2^{13} + 1)^{3351918797}$
$n = 43$	$\left((2^5 + 1)(2^{17} + 1)(2^{23} + 1)\right)^{593211015}$
$n = 45$	$(2 + 1)^{407925} \cdot (2^{13} + 1)^{349650} \cdot \left((2^{25} + 1)(2^{33} + 1)(2^{41} + 1)\right)^{116550}$
$n = 47$	$(2^{11} + 1)^{1927501725} \cdot (2^{37} + 1)^{435242325} \cdot (2^{41} + 1)^{1616614350}$
$n = 49$	$(2^9 + 1)^{34630287489} \cdot (2^{11} + 1)^{3393768173922}$
$n = 51$	$(1 + 2^{29})^{150009615}$
$n = 53$	$(1 + 2^5)^{6512186850} \cdot (1 + 2^{15})^{3506562150} \cdot (1 + 2^{21})^{250468725}$
$n = 55$	$(1 + 2)^{6588945} \cdot (1 + 2^{11})^{5856840} \cdot (1 + 2^{17})^{732105} \cdot$ $(1 + 2^{25})^{1464210} \cdot (1 + 2^{33})^{10249470} \cdot (1 + 2^{47})^{732105}$
$n = 57$	$(1 + 2^5)^{396029391534} \cdot (1 + 2^{17})^{1188088174602} \cdot (1 + 2^{21})^{594044087301} \cdot (1 + 2^{47})^{198014695767}$
$n = 59$	$(1 + 2^7)^{3663925098759300} \cdot (1 + 2^{13})^{305327091563275}$
$n = 61$	$(1 + 2^9)^{1152921504606846975}$
$n = 63$	$(1 + 2)^{42958503} \cdot (1 + 2^5)^{3735522} \cdot (1 + 2^{39})^{56032830} \cdot (1 + 2^{43})^{44826264} \cdot (1 + 2^{47})^{29884176}$
$n = 65$	$(1 + 2^{17})^{72647571779055} \cdot (1 + 2^{23})^{72647571779055} \cdot (1 + 2^{29})^{72647571779055}$
$n = 67$	$(1 + 2^5)^{15295807610659665}$
$n = 69$	$(1 + 2^{11})^{36566619637113225} \cdot (1 + 2^{17})^{2437774642474215} \cdot (1 + 2^{53})^{19502197139793720} \cdot (1 + 2^{67})^{21939971782267935}$
$n = 71$	$(1 + 2^{11})^{3659326099961865} \cdot (1 + 2^{13})^{14637304399847460}$
$n = 73$	$(1 + 2^{31})^{1726845200475585} \cdot (1 + 2^{45})^{107064402429486270}$

Table 1 continued

$n = 75$	$(1+2)^{36654975} \cdot (1+2^{39})^{17832150} \cdot (1+2^{41})^{9906750} \cdot$
	$(1+2^{43})^{7925400} \cdot (1+2^{53})^{57459150} \cdot (1+2^{55})^{15850800} \cdot (1+2^{63})^{43589700}$
$n = 77$	$(1+2^{25})^{290641821624556479} \cdot (1+2^{31})^{290641821624556479} \cdot$
	$(1+2^{41})^{290641821624556479} \cdot (1+2^{67})^{581283643249112958}$
$n = 79$	$(1+2^{9})^{12102186118644337359} \cdot (1+2^{15})^{12102186118644337359} \cdot (1+2^{41})^{12102186118644337359}$
$n = 81$	$(1+2)^{106331083505919} \cdot (1+2^{25})^{155626336778778} \cdot (1+2^{37})^{105108887143782} \cdot$
	$(1+2^{39})^{155626336778778} \cdot (1+2^{43})^{4073987873790}$
$n = 83$	$(1+2^{11})^{7239076764159456135965}$
$n = 85$	$(1+2^{9})^{4760486403166879215} \cdot (1+2^{13})^{4760486403166879215} \cdot (1+2^{23})^{4760486403166879215}$
$n = 87$	$(1+2^{39})^{3371346107168004} \cdot (1+2^{41})^{280945508930667} \cdot (1+2^{53})^{2809455089306670} \cdot$
	$(1+2^{61})^{4214182633960005} \cdot (1+2^{71})^{1685673053584002} \cdot (1+2^{83})^{280945508930667}$
$n = 89$	$(1+2^{13})^{309485009821345068724781055}$
$n = 91$	$(1+2^{59})^{280368506850705} \cdot (1+2^{67})^{1682211041104230} \cdot$
	$(1+2^{71})^{280368506850705} \cdot (1+2^{73})^{280368506850705} \cdot (1+2^{81})^{3364422082208460}$
$n = 93$	$(1+2^{17})^{2305843010287435773}$
$n = 95$	$(1+2^{43})^{7354378117756963125} \cdot (1+2^{51})^{7354378117756963125}$
$n = 97$	$(1+2^{5})^{61253537018541048982516284 6} \cdot (1+2^{9})^{10208922836423508163752714 1}$
$n = 99$	$(1+2)^{160190876329840719} \cdot (1+2^{23})^{160190876329840719} \cdot (1+2^{35})^{58251227756305716} \cdot$
	$(1+2^{57})^{29125613878152858} \cdot (1+2^{59})^{101939648573535003} \cdot (1+2^{75})^{58251227756305716}$
$n = 101$	$(1+2^{7})^{26147908420545768131498184 9} \cdot (1+2^{9})^{10459163368218307252599273 96}$
$n = 103$	$(1+2^{5})^{82048582506870378495385411 56} \cdot (1+2^{9})^{20512145626717594623846352 89}$
$n = 105$	$(1+2^{7})^{736412106675} \cdot (1+2^{29})^{6627708960075} \cdot (1+2^{37})^{1472824213350} \cdot$
	$(1+2^{55})^{6627708960075} \cdot (1+2^{69})^{15464654240175} \cdot (1+2^{79})^{736412106675} \cdot$
	$(1+2^{83})^{4418472640050} \cdot (1+2^{85})^{441847264005} \cdot (1+2^{87})^{13255417920150}$

Table 1 continued

$n = 107$	$(1+2^5)^{27043212804868893898596335048021}$
$n = 109$	$(1+2^7)^{744308608310570490215126499806} \cdot (1+2^{15})^{372154304155285245107563249903}$
$n = 111$	$(1+2^{17})^{2078233794395472907116} \cdot (1+2^{31})^{742226355141240323970} \cdot (1+2^{39})^{890671626169488388764}$
	$(1+2^{71})^{180254971962872650107} \cdot (1+2^{87})^{519558448598868226779}$
$n = 113$	$(1+2^{15})^{82901226266607482846190} \cdot (1+2^{25})^{13816871044434580474365}.$
	$(1+2^{29})^{37854441217628987601} \cdot (1+2^{75})^{13816871044434580474365}.$
	$(1+2^{97})^{82901226266607482846190}$
$n = 115$	$(1+2^{17})^{23588654041464621525} \cdot (1+2^{23})^{165120578290252350675}.$
	$(1+2^{39})^{23588654041464621525} \cdot (1+2^{45})^{23588654041464621525}.$
	$(1+2^{75})^{188709232331716972200}$
$n = 117$	$(1+2^5)^{350280341971560} \cdot (1+2^{11})^{481635470210895} \cdot (1+2^{31})^{1225981196900460}.$
	$(1+2^{55})^{1269766239646905} \cdot (1+2^{71})^{1225981196900460} \cdot (1+2^{87})^{744345726689565}.$
	$(1+2^{93})^{1903697510715} \cdot (1+2^{111})^{1094626068661125} \cdot (1+2^{115})^{1182196154154015}$
$n = 119$	$(1+2^{21})^{1218073440076268644855 35} \cdot (1+2^{25})^{281093870786831225735 85}.$
	$(1+2^{51})^{66354195179251988435 70} \cdot (1+2^{81})^{59685598563737163597912 15}.$
	$(1+2^{97})^{85265140805338805139 8745} \cdot (1+2^{109})^{66354195179251988435 70}$
$n = 121$	$(1+2^9)^{99244104353509123769903900571} \cdot (1+2^{19})^{89319693918158211392913 5105139}.$
	$(1+2^{25})^{89319693918158211392913 5105139} \cdot (1+2^{43})^{17863938783631642278582 70210278}$
$n = 123$	$(1+2^5)^{38263506571610465341512132024} \cdot (1+2^9)^{19131753285805232670756066012}.$
	$(1+2^{27})^{47829383214513081676890165 03} \cdot (1+2^{53})^{28697629928707849006134099018}.$
	$(1+2^{113})^{77262849808059595347805334351}$
$n = 125$	$(1+2^{23})^{28985913978714592383746 25} \cdot (1+2^{29})^{64413142174921316408325 0}.$
	$(1+2^{95})^{16103285543730329102081 25} (1+2^{109})^{41868542413698855665411 25}.$
	$(1+2^{121})^{19323942652476394922497 50}$

Table 1 continued

$n = 127$	$(1+2^5)^{2835686391007820528861455061931401762 1}$
$n = 129$	$(1+2^9)^{847129553356524310818341940505 5} \cdot (1+2^{79})^{952901634821737132529068549 5}$
$n = 131$	$(1+2^9)^{1293849303881895298339827404683529321} \cdot (1+2^{15})^{2587698607763790596679654809367058642}$
$n = 133$	$(1+2^5)^{2725620347545423314190572095349 3} \cdot (1+2^{17})^{8176861042636269942571716286047 9}$
	$(1+2^{45})^{8176861042636269942571716286047 9}$
$n = 135$	$(1+2^9)^{1390256215369200900} \cdot (1+2^{25})^{9826330930229511961200} \cdot (1+2^{47})^{38551429107264868200}$
	$(1+2^{55})^{2813183451799578021150} \cdot (1+2^{89})^{7686726614776311776100}$
	$(1+2^{101})^{1406591725899789010575} \cdot (1+2^{109})^{4576375896941567062575}$
	$(1+2^{117})^{1042692161526900675} \cdot (1+2^{121})^{21197931643841890722 75}$
$n = 137$	$(1+2^5)^{3974100635573003952732133316739704004 1} \cdot (1+2^7)^{7948201271146007905464266633479408008 2}$
$n = 139$	$(1+2^9)^{1740853036205930498203402247399263717 5} \cdot (1+2^{17})^{4571167709949926909943288176978373 00}$
$n = 141$	$(1+2)^{1216799735702178355508978464575} \cdot (1+2^{51})^{1106181577911071232280889513 25}.$
	$(1+2^{65})^{6321037588063264184462225790 0} \cdot (1+2^{121})^{5688933829256937766016003211 0}$
$n = 145$	$(1+2^{41})^{5346390839778806315306604850819255 05} \cdot (1+2^{49})^{7637701199684009021866578358313221 5}.$
	$(1+2^{135})^{3055080479873603608746631343325288 60} \cdot (1+2^{137})^{4144489023084345980857833217689345}.$
	$(1+2^{139})^{5346390839778806315306604850819255 05}$
$n = 147$	$(1+2^{15})^{1724911926028261302613795181123 4} \cdot (1+2^{59})^{5174735778084783907841385543370 2}.$
	$(1+2^{67})^{4312279815070653256534487952808 5} \cdot (1+2^{71})^{9678672473825243975777406294081 3}.$
	$(1+2^{73})^{8624559630141306513068975905617}$
$n = 149$	$(1+2^9)^{2993388617252432636413203811794413402 6225}$
$n = 151$	$(1+2^{35})^{4765785934428705143321533840702 5} \cdot (1+2^{53})^{4765785934428705143321533840702 5}.$
	$(1+2^{55})^{9531571868857410286643067681405 0} \cdot (1+2^{81})^{9531571868857410286643067681405 0}.$
	$(1+2^{119})^{4765785934428705143321533840702 5}$
$n = 153$	$(1+2^{67})^{7410522868792876174469251607469 0} \cdot (1+2^{85})^{5668686631813451031257873 85}.$

Table 1 continued

	$(1+2^{101})^{185263071719821904361731290186725} \cdot (1+2^{115})^{247017428959762539148975053582 30}$.
	$(1+2^{125})^{666947058191358855702232644672 21} \cdot (1+2^{147})^{222315686063786285234077548224 07}$
$n=155$	$(1+2^{17})^{626716423364616167972397797 25} \cdot (1+2^{43})^{358123670494066381698513027 00}$.
	$(1+2^{51})^{179061835247033190849256513 50} \cdot (1+2^{59})^{298436392078388651415427522 5}$.
	$(1+2^{73})^{268592752870549786273884770 25} \cdot (1+2^{101})^{179061835247033190849256513 50}$.
	$(1+2^{123})^{865014224607504542831738415625}$
$n=157$	$(1+2^{15})^{170744467588768190221622166239364 3900} \cdot (1+2^{17})^{341488935177536380443244332478728780}$.
	$(1+2^{29})^{384175052074728427998649874038569 8775} \cdot (1+2^{45})^{307340041659782742398919899230855902 00}$
$n=159$	$(1+2^{57})^{936251620325705638480207 5} \cdot (1+2^{65})^{443487609627965828753782 50}$.
	$(1+2^{69})^{443487609627965828753782 5} \cdot (1+2^{89})^{384355928344237051586611 50}$.
	$(1+2^{101})^{79907677410444293469150} \cdot (1+2^{123})^{591316812837287716717100}$.
	$(1+2^{127})^{2002242486366485713350} \cdot (1+2^{137})^{48783637059076241162916075}$
$n=161$	$(1+2^{29})^{933434719243564022463890020343 85} \cdot (1+2^{43})^{622289812829042681642593346895 90}$.
	$(1+2^{47})^{829719750438723575523457795861 20} \cdot (1+2^{87})^{217801434490164938574907671413565}$.
	$(1+2^{157})^{248915925131617072657037338758360}$
$n=163$	$(1+2^{13})^{168486137937535997136381884224759 350} \cdot (1+2^{87})^{561620459791786657121272947415 8645}$.
	$(1+2^{89})^{192555586214326853870150724828296 4} \cdot (1+2^{119})^{786268643708501319969782126382210 30}$
$n=165$	$(1+2^{61})^{399483521581326273808238425414 50} \cdot (1+2^{105})^{932128217023094638885889659300 5}$.
	$(1+2^{109})^{133161173860442091269412808471 50} \cdot (1+2^{113})^{155354702837182439814314932 1675}$.
	$(1+2^{119})^{199741760790663136904119212707 25} \cdot (1+2^{123})^{798967043162652547616476850829 00}$.
	$(1+2^{127})^{369892149612339142415035579087 5} \cdot (1+2^{135})^{532644695441768365077651233886 0}$.
	$(1+2^{147})^{443870579534806970898042694905 0} \cdot (1+2^{157})^{133161173860442091269412808471 50}$
$n=167$	$(1+2^{5})^{350060123390813635242448130256489390771914057740}$.
	$(1+2^{33})^{175030061695406817621224065128244695385957028 87}$

Table 1 continued

$n = 169$	$(1+2^{15})^{7089726406583596958466287242575266870940} \cdot$
	$(1+2^{25})^{7286663251210919096201461888202357617355} \cdot$
	$(1+2^{55})^{291466530048436763848058475528094306469420}$
$n = 171$	$(1+2^{49})^{491491233557675534008353044299461931 35} \cdot (1+2^{55})^{98298246711535106801670608859892386 27} \cdot$
	$(1+2^{77})^{98298246711535106801670608859892386 27} \cdot (1+2^{99})^{98298246711535106801670608859892386 27} \cdot$
	$(1+2^{109})^{98298246711535106801670608859892386 27} \cdot (1+2^{159})^{98298246711535106801670608859892386 27} \cdot$
	$(1+2^{163})^{98298246711535106801670608859892386 27}$
$n = 173$	$(1+2^{21})^{75271201137701322155843064256750855600886 1} \cdot (1+2^{61})^{752712011377013221558430642567508556008861} \cdot$
	$(1+2^{69})^{752712011377013221558430642567508556008861} \cdot (1+2^{77})^{31613904477834555305454086987835359352372162}$
$n = 175$	$(1+2^{19})^{2811986846234676892049136867794 25} \cdot (1+2^{43})^{5407667011989763253940647822681 25} \cdot$
	$(1+2^{61})^{1232948078733666021898467703571 3250} \cdot (1+2^{97})^{1297840082877543180945755477443 50} \cdot$
	$(1+2^{105})^{6651799969190141587990774087125} \cdot (1+2^{123})^{1113979404469891230311773451472 3375} \cdot$
	$(1+2^{141})^{4975053651030582193625395996866750} \cdot (1+2^{163})^{1838606784076519506339820259711625} \cdot$
	$(1+2^{165})^{1114982889070054279163020169625}$
$n = 177$	$(1+2^{19})^{1021044488673916044039069088984452939 75} \cdot (1+2^{57})^{4288386852430447384964090173734702346950} \cdot$
	$(1+2^{93})^{8168355909391328352312552711875623518 0} \cdot (1+2^{103})^{1286516055729134215489227052120410704085} \cdot$
	$(1+2^{133})^{1837880079613048879270324360172015291550} \cdot (1+2^{163})^{5688676436897532245360527781484809235 75}$
$n = 179$	$(1+2^{21})^{1713334865061395551905989490523888483510297545} \cdot$
	$(1+2^{29})^{1773165606380999841020166901304087763886847618 0}$
$n = 181$	$(1+2^{11})^{1682526262861609446021431244616873841926188 0} \cdot$
	$(1+2^{21})^{2103157828577011807526789055771092302407735 0} \cdot$
	$(1+2^{31})^{2103157828577011807526789055771092302407735} \cdot$
$n = 183$	$(1+2^{17})^{5301342361191869603932356617428842175355175} \cdot$

Table 1 continued

	$(1+2^{75})^{17101104390941514851394698765899490888242 5}$.
	$(1+2^{177})^{127963436304631335267332745937937569749952 5}$
$n=185$	$(1+2^{21})^{24289606148175875174394125504156277451293856980}$.
	$(1+2^{25})^{56675747679077042073586292843031314053018999620}$.
	$(1+2^{61})^{60724015370439687935985313760390693628234642 45}$.
	$(1+2^{73})^{28337873839538521036793146421515657026509499810}$.
	$(1+2^{121})^{33338675105339436513874289907665478854717058 60}$
$n=187$	$(1+2^{9})^{52332852605905914814562661586433935229041537035}$.
	$(1+2^{19})^{52332852605905914814562661586433935229041537035}$.
	$(1+2^{41})^{20362977667667671134071074547250558454879975 5}$.
	$(1+2^{89})^{10466570521181182962912532317286787045808307407 0}$
$n=189$	$(1+2^{7})^{95480857532709340106743657628994158 1}\cdot(1+2^{11})^{76741427691674298191288254054776183774}$.
	$(1+2^{21})^{86283522438104246850483190041461 4}\cdot(1+2^{33})^{86877087952838828141081042326161717 48}$.
	$(1+2^{39})^{65157815964629121105810781744621288 11}\cdot(1+2^{73})^{60813961566987179698756729628313202236}$.
	$(1+2^{89})^{53091553748957061641771748088209938460}\cdot(1+2^{125})^{62503238277181268023722194340210791187}$.
	$(1+2^{157})^{12138659788966091820823267858349817747 9}$
$n=191$	$(1+2^{55})^{10254448698776160601034896659656524022087 25}$.
	$(1+2^{77})^{18609925416297476646322590234191469521565 75}$.
	$(1+2^{179})^{10634243095027129512184337276680839726609 00}$.
	$(1+2^{183})^{21268486190054259024368674553361679453218 00}$.
	$(1+2^{189})^{13824516023535268365839638459685091644591 7}$
$n=193$	$(1+2^{5})^{69064471322938968681523834816473052997664942598865 1}$.
	$(1+2^{9})^{76738301469932187423915372018303392219627713998739}$.
	$(1+2^{13})^{98663530461341383830748335452104361425235632284093}$

Table 1 continued

$n = 195$	$(1+2^{31})^{39721861858997517665132215667993556496815 0}$.
	$(1+2^{129})^{42129247426209488432715986314538620526925}$.
	$(1+2^{163})^{66203103098329196108553692779989260828025}$
$n = 197$	$(1+2^{5})^{47788807121282329843547481918370106279929779662675299482}$.
	$(1+2^{13})^{79648011868803883072579136530616843799882966104458832 47}$
$n = 199$	$(1+2^{7})^{90123499430703851139301093076198094508537685367490843 63}$.
	$(1+2^{27})^{23432109851983001296218284199811504572219798195547619343 8}$
$n = 201$	$(1+2^{67})^{201} \cdot (1+2^{107})^{91503141265246293397851719230775403196008417 0}$.
	$(1+2^{119})^{14182986896113175476667016480770187495381304635}$.
	$(1+2^{145})^{35076204151677745802509825705130571225136559 85}$.
	$(1+2^{177})^{83184673877496630361683381111888673017818947 0}$
$n = 203$	$(1+2^{57})^{71867425127993443034105242899027114844981 2}$.
	$(1+2^{81})^{51205540403695328161799985565556819327049105}$.
	$(1+2^{111})^{62883996986994262654842087536648725489358 55}$.
	$(1+2^{127})^{18865199096098278796452626260994617646807565}$.
	$(1+2^{153})^{26950284422997541137789466087135168066867 95}$.
	$(1+2^{175})^{64680682615194098730694718609124403360483080}$.
	$(1+2^{193})^{80850853268992623413368398261405504200603 85}$
$n = 205$	$(1+2^{43})^{94679614243503477779804484190139074283234305 50}$.
	$(1+2^{67})^{29756450190815378730795695031186566203302210300}$.
	$(1+2^{131})^{67628295888216769842717488707242195916595932 5}$.
	$(1+2^{145})^{72136848947431221165565321287725008977702328 00}$.
	$(1+2^{157})^{77289481015104879820248558522562509618966780 0}$.
	$(1+2^{187})^{16907073972054192460679372176810548979148983125}$

Table 1 continued

$n = 207$	$(1+2^{5})^{3319261926106653512828905813293098276183677 5}$.
	$(1+2^{121})^{4646966696549314917960468138610337586657148 5}$.
	$(1+2^{127})^{1021311361878970311639663327167107161902 67}$.
	$(1+2^{179})^{1991557155663992107697343487975858965710206 5}$.
	$(1+2^{187})^{3983114311327984215394686975951717931420413 0}$.
	$(1+2^{199})^{3983114311327984215394686975951717931420413}$
$n = 209$	$(1+2^{59})^{2702503370421545593927930162926620905051434011525 85}$.
	$(1+2^{61})^{3603337827228727458570573550568827873401912015367 80}$.
	$(1+2^{87})^{1801668913614363729285286775284413936700956007683 90}$.
	$(1+2^{97})^{2573812733734805327550409678977734195287080010977 0}$
$n = 211$	$(1+2^{9})^{1154929871973565275224108161553051512738585560465529713690}$.
	$(1+2^{13})^{6416277066519807084578378675294730626325475335919609520 5}$.
	$(1+2^{55})^{2309859743947130550448216323106103025477171120931059427380}$
$n = 213$	$(1+2^{11})^{5497736589318700986099894638477660690688115321335}$.
	$(1+2^{41})^{1409676048543256663102537086789143766843106492 65}$.
	$(1+2^{85})^{1832578863106233662033298212825886896896038440445}$.
	$(1+2^{119})^{2356172823993728994042811987918997438866335137715}$.
	$(1+2^{161})^{1099547317863740197219978927695532138137623064267}$.
	$(1+2^{203})^{1570781882662485996028541325279331625910890091810}$
$n = 215$	$(1+2^{41})^{6644311488537627875769910918577325317450040202 5}$.
	$(1+2^{97})^{3100678694650893008692625095336085148143352094 5}$.
	$(1+2^{119})^{1860407216790535805215575057201651088886011256 70}$.

Table 1 continued

	$(1+2^{151})^{1860407216790535805215575057201651088886011256 70}$.
	$(1+2^{203})^{279061082518580370782336258580247663332901688505}$
$n=217$	$(1+2^{13})^{1126940817087752014462533930787563178937611179075}$.
	$(1+2^{57})^{125215646343083557162503770087507019881956797675}$.
	$(1+2^{89})^{500862585372334228650015080350028079527827190 70}$.
	$(1+2^{185})^{751293878058501342975022620525042119291740786050}$.
	$(1+2^{215})^{953730967232331762171404637030151748486648827 5}$
$n=219$	$(1+2^{19})^{206699727582778505456885121210387850240216513482 0}$.
	$(1+2^{63})^{156590702714226140497640243341202916848648873 85}$.
	$(1+2^{107})^{826798910331114021827540484841551400960866053928 0}$.
	$(1+2^{113})^{861248864928243772737021338376616042667568806175}$.
	$(1+2^{115})^{223924704881343380911625547977920171093567889605 5}$.
	$(1+2^{139})^{980283260893936001489292580266067040434631161 5}$.
	$(1+2^{189})^{574165909952162515158014225584410695111712537450}$
$n=221$	$(1+2^{9})^{39894866838325323664842657097280998705655239869173227015 95}$.
	$(1+2^{19})^{39894866838325323664842657097280998705655239869173227015 95}$.
	$(1+2^{29})^{3989486683832532366484265709728099870565523986917322701595}$
$n=223$	$(1+2^{17})^{1014848095919801109402176209373936431577327592183}$.
	$(1+2^{91})^{1503478660621927569484705495368794713447892729160}$.
	$(1+2^{103})^{1691413493199668515670293682289894052628879320305}$.
	$(1+2^{113})^{5638044977332228385567645607632980175429597734 35}$.
	$(1+2^{145})^{2631087656088373246598234616895390748533812276030}$
$n=225$	$(1+2^{29})^{64638048753257449056214060125} \cdot (1+2^{31})^{7884561986535958142302546740 00}$.
	$(1+2^{49})^{5797472048923498634045990250} \cdot (1+2^{51})^{8406334470939073019366685862 5}$.

Table 1 continued

	$(1+2^{85})^{44798647650772489444900833 75} \cdot (1+2^{97})^{18098653650912085735739936835 00}$.
	$(1+2^{99})^{36570324612875501587674150 0} \cdot (1+2^{105})^{53026970688669473302127517 50}$.
	$(1+2^{115})^{68066717742077353015043250} \cdot (1+2^{131})^{52704291353849987582236275 00}$.
	$(1+2^{203})^{15231540201262646411266283475 0} \cdot (1+2^{207})^{82877498153929105473066542437 5}$.
	$(1+2^{217})^{43813077402455494677113015407 5} \cdot (1+2^{219})^{94077160066622227834291750875}$
$n=227$	$(1+2^{5})^{59383142438657794704063431302361624145812280978139757521155099815}$.
	$(1+2^{7})^{11876628487731558940812686260472324829162456195627951504231019963 0}$
$n=229$	$(1+2^{9})^{14738569738721986750960956553536198737021950786977146605 1}$.
	$(1+2^{21})^{17686283686466384101153147864243438484426340944372575926 12}$.
	$(1+2^{121})^{58954278954887947003843826214144794948087803147908586420 4}$
$n=231$	$(1+2^{41})^{45918970445144312764736259491615573288280746683021 8}$.
	$(1+2^{55})^{15672003564895669885575515184851731497706739482 26}$.
	$(1+2^{69})^{27551382267086587658841755694969343972968448009813 08}$
	$(1+2^{91})^{11479742611286078191184064872903893322070186670755 45}$.
	$(1+2^{131})^{53572132186001698225525636073551502169660871130192 1}$.
	$(1+2^{157})^{91837940890288625529472518983231146576561493366043 6}$
	$(1+2^{159})^{11479742611286078191184064872903893322070186670755 45}$.
	$(1+2^{209})^{23508005347343504828363272777277597246560109223 39}$
$n=233$	$(1+2^{15})^{17038321523200602421013846948443997824061934891243478185488130}$.
	$(1+2^{23})^{28397202538667670701689744914073329706769891485405796975813 55}$
	$(1+2^{49})^{28397202538667670701689744914073329706769891485405796975813 55}$.
	$(1+2^{113})^{28397202538667670701689744914073329706769891485405796975813 55}$
$n=235$	$(1+2^{73})^{23191222403616672243206263595493280420250247335633250}$.
	$(1+2^{105})^{26891949382917205047973220552220931551141244250893875}$

Table 1 continued

	$(1+2^{119})^{8141599354461172170487305304800832487960193213573375}$.
	$(1+2^{141})^{3636596990071767217489308950806694612437058782 50}$
	$(1+2^{167})^{1406276252134202465811443643556507429738578827799 0375}$.
	$(1+2^{171})^{2368465266752340995050852452305696723770238025766 8000}$
	$(1+2^{197})^{2556865912971277210566261170102740781342870595998250}$
$n=237$	$(1+2^{9})^{3126206278524167619791531177227039080133327013600904 33}$.
	$(1+2^{169})^{3647240658278195556423453040098212260155548182534388385}$
	$(1+2^{173})^{1042068759508055873263843725742346360044442337866968110}$.
	$(1+2^{175})^{1736781265846759788773072876237243933407403896444946 85}$
	$(1+2^{199})^{4290871362680230066380532988350837953124174332393398 10}$.
	$(1+2^{225})^{4168275038032223493055374902969385440177769351467872 44}$
	$(1+2^{233})^{6796100605487320912590285167884867565507232638262835 5}$
$n=239$	$(1+2^{59})^{1379039302587175801678397113917931632629831388142617798 66}$.
	$(1+2^{73})^{2517293965040082812587550287310510123054454121212715029 3}$.
	$(1+2^{87})^{2068558953880763702517595670876897448944747082213926697 99}$.
	$(1+2^{197})^{2987918488938880903636527080155518537364634674309005230 43}$.
	$(1+2^{199})^{9193595350581172011189314092786210884198875920950785324 4}$.
	$(1+2^{237})^{6566853821843694293706652923418722060142054229250560946}$
$n=241$	$(1+2^{7})^{9164144110314559872443738560031971762028341721850574655737376683690 09}$.
	$(1+2^{9})^{5498486466188735923466243136019183057217005033110344793442426010214054}$
$n=243$	$(1+2^{23})^{7850130255608843007937280321561967701043896592 75}$.
	$(1+2^{31})^{2233509863520507634057468878101312986071066813 0}$.
	$(1+2^{35})^{8474199188063102493923926037502040447151988790 50}$.
	$(1+2^{61})^{1320398478140064807192797777936364441765542439 45}$.

Table 1 continued

	$(1+2^{151})^{4113537073570682827430772513589953188632286917 5}$.
	$(1+2^{155})^{7258907056441649810686773853829267204730967142 25}$.
	$(1+2^{163})^{1609440931066248148070823162161240239962974615 25}$.
	$(1+2^{177})^{3875796527873822070864431288469925475829204175 50}$.
	$(1+2^{181})^{9196805320378560846118989498064229942645569230 0}$
$n=245$	$(1+2^{69})^{4045342812738269868299873451466638060091932606984211629096 45}$.
	$(1+2^{117})^{6524746472158499787580441050752642032406342914490663917897 50}$.
	$(1+2^{125})^{1096157407322627964313514096526443861444265609634431538206780}$.
	$(1+2^{141})^{1057008928489676965588031450221928009249827552147487554699395}$.
	$(1+2^{151})^{4045342812738269868299873451466638060091932606984211629096 45}$.
	$(1+2^{165})^{1578988646262356948594466734282139371842334985306740668131195}$.
	$(1+2^{167})^{4045342812738269868299873451466638060091932606984211629096 45}$
$n=247$	$(1+2)^{1340573573884413807045402862803334868907750358289097078156 45}$.
	$(1+2^{9})^{1307876657448208592239417427125204750153902788574728856738 00}$.
	$(1+2^{35})^{1634845821810260740299271783906505937692378485718411070922 5}$.
	$(1+2^{71})^{8501198273413355849556213276313830876000368125735737568797 0}$.
	$(1+2^{147})^{8174229109051303701496358919532529688461892428592055354612 5}$.
	$(1+2^{195})^{1504058156065439881075330041193985462676988206860938185248 7}$
	$(1+2^{97})^{2925277021907294342301024913127710972839014826123103258639378520 70}$.
	$(1+2^{119})^{2047693915335106039610717439189397680987310378286172281047564964 49}$.
$n=249$	$(1+2^{137})^{5850554043814588684602049826255421945678029652246206517278757041 40}$.
	$(1+2^{173})^{6338100214132471074985553978443373774484532123266723727057 1986794 85}$.
	$(1+2^{199})^{5363007873496706294218545674067470116871527181225689307505527287 95}$

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 3×3 and 4×4 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'. 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 Skałba. 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)