Threshold implementations of cryptographic functions between finite Abelian groups

Enrico Piccione

University of Bergen, Bergen, Norway enrico.piccione@uib.no

Abstract. Side-channel attacks pose a significant threat to the security of cryptographic hardware implementations and Threshold Implementation (TI) is a well-established countermeasure to mitigate those attacks. In 2023, Piccione et al. proposed a general construction of (first-order) TIs that is universal for S-boxes that are bijective vectorial Boolean function (functions from a binary vector space $\mathbb{F}_2^n$ into itself). This paper presents a novel approach to TI by addressing a broader class of cryptographic functions and providing a new construction for quadratic balanced functions in the framework of second-order attacks. We investigate the case of functions (also not necessarily bijective) that are defined between two finite Abelian groups by using the notion of functional degree introduced by Aichinger and Moosbauer in 2021. We show that if a function F has functional degree (at most) d and the cardinality of the domain is divisible by the cardinality of the codomain, then F admits a TI with $s \geq d+2$ shares, and for the case $d=2$ and F is balanced we have that F admits a second order TI with $s \geq 7$ shares. As a real-world application, we present a general construction for the TI of any multiplication map with 4 shares. Furthermore, we introduce first-order secure conversion procedures between an additive sharing over $\mathbb{F}_p^n$ (called Boolean sharing if $p=2$) and an additive sharing over $\mathbb{Z}_{p^n}$ (called Arithmetic sharing if $p=2$).

Keywords: Threshold Implementation, Arithmetic masking, Abelian groups, Functional Degree, Boolean Functions

1 Introduction

Differential Power Analysis (DPA) attacks [KJJ99] target the hardware implementations of a cryptographic algorithm by measuring the power consumption of the physical device. Since then, many countermeasures were developed in order to mitigate those attacks. One of the most common is called *Boolean masking* [GP99, CJRR99] which is a technique based on *Boolean sharing* that secure the implementation against a formally defined adversary model. However, if the effect of glitches is not taken into account, this can lead to an attack on a masked implementation [MPO05]. Nikova, Rechberger, and Rijmen [NRR06] published in 2006 a countermeasure called *Threshold Implementation* (TI) which builds upon Boolean masking and takes glitches into account.

In mathematical terms, a threshold implementation is a vectorial Boolean function $\mathcal{F}$ that satisfies three fundamental properties with respect to a given vectorial Boolean function F. Those properties are correctness, non-completeness, and uniformity. Throughout the years, the problem of constructing $\mathcal{F}$ for a given F was considered a challenging problem [BNN$^+$12, BGN$^+$15, BBS17]. In [PAB$^+$23], this has been solved for the case where F is bijective but with $d+2$ shares (both in input and output) where d is the algebraic degree of F. The theoretical optimal number is $d+1$, but there is some evidence reported in [BNN$^+$12, PAB$^+$23] to the fact that for many functions F the number of optimal shares is actually $d+2$ with one example for which it is mathematically proven. In this paper, we do not discuss the case $d+1$ further and, instead, we consider a more general mathematical setting where we can generalize the construction in [PAB$^+$23]. With this, we provide a better understanding of the threshold implementation theory. We consider the problem of constructing a threshold implementation for a function $F\colon \mathbb{X} \to \mathbb{Y}$ between two finite Abelian groups $\mathbb{X}$ and $\mathbb{Y}$ where we use the definition provided by Dhooghe et al. [DNR19] with *additive sharing* both in the input and the output. For any $x \in \mathbb{X}$ (resp. $y \in \mathbb{Y}$), a vector of shares $(x_1, \ldots, x_s) \in \mathbb{X}^s$ (resp. $(y_1, \ldots, y_t) \in \mathbb{Y}^t$) is such that $x_1 + \cdots + x_s = x$ (resp. $y_1 + \cdots + y_s = y$). The additive sharing over $\mathbb{Z}_{2^n}$ is called *arithmetic sharing* (or *arithmetic masking*) [Gou01] and it has been the building block of the implementations of two of the NIST standards for post quantum cryptography, Kyber and Dilithium [Bou22]. Moreover, there has been a recent interest in *prime-field sharing* (also called *prime-field masking*) over Mersenne primes $2^n - 1$ [CMM$^+$23] which is the additive sharing over $\mathbb{F}_{2^n-1}$. Moreover, among Arithmetic-Oriented (AO) symmetric ciphers and post-quantum schemes, there are numerous examples of schemes that require, or are already being implemented with, additive masking.

A fundamental notion in the threshold implementation theory is the one of algebraic degree. For functions between Abelian groups, we are going to use the notion of *functional degree*. Aichinger and Moosbauer in [AM21] introduce such notion with the purpose of extending Chevalley-waring type results to the general case of a function $F\colon \mathbb{X} \to \mathbb{Y}$ between two Abelian groups $\mathbb{X}$ and $\mathbb{Y}$. The functional degree of F is defined by the smallest positive natural number such that Fréchet's equation is satisfied, which is equivalent to ask that every $d+1$-th order derivative vanishes. A derivative of F through a direction $a \in \mathbb{X}$ is defined by $\Delta_a F(x) = F(x+a) - F(x)$ for any $x \in \mathbb{X}$. The idea of using Fréchet's equation to introduce a notion of degree was already studied by many authors in the past (see for instance [Lac04]). However, we refer to the paper [AM21] because this is the first work that gives solid mathematical foundations without the use of any representation of F. We also build upon the following works [Sch14, CS22] which have studied the Integer-Valued (IV) polynomial representation of functions with finite functional degree. We believe that this representation could be useful for cryptographic application in the case where a polynomial representation is not possible. For instance, in the context of Fully Homomorphic Encryption (FHE), in the TFHE scheme [CGGI20] the programmable bootstrapping can evaluate any function from $\mathbb{Z}_{2^n}$ to itself defined only by a lookup table. It is then considered while designing or cryptanalyzing symmetric schemes over $\mathbb{Z}_{2^n}$ [CHMS22, GMAH$^+$23].

In Section 2, we introduce the preliminaries necessary for this paper including the notion of functional degree and the IV polynomial representation. In Section 3, we present a general theory for the notion of threshold implementation of functions between Abelian groups and we show that many classical results still hold. In Section 4, we present the main result of this paper. We provide a general construction of threshold implementations with $s \geq d+2$ shares in input and $d+2$ shares in output for all $F\colon \mathbb{X} \to \mathbb{Y}$ with functional degree at most $d < \infty$ and such that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$. In particular, the result holds for any vectorial Boolean function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ with $m \leq n$ and F having algebraic degree at most d. Then we present a threshold implementation with 4 shares of the multiplication map over a finite ring. In Section 5, we present a general construction of second order threshold implementations with $s \geq 7$ shares in input and 7 shares in output for all quadratic balanced functions. In Section 6, we present first-order secure conversion algorithms between additive sharings in $\mathbb{F}_p^n$ and $\mathbb{Z}_{p^n}$ that are built upon the general construction defined in Section 4.

2 Preliminaries

For any $n \in \mathbb{N}$ with $n \geq 2$, the set $\mathbb{Z}_n$ denotes the ring of integers modulo n and we represent elements of $\mathbb{Z}_n$ as integers between 0 and $n-1$ or as classes $a + n\mathbb{Z} = \{a + bn : b \in \mathbb{Z}\}$ for some $a \in \mathbb{Z}$. The set $\mathbb{F}_q$ denotes the finite field with q elements, where q is a power of a prime p. We recall that $\mathbb{F}_p = \mathbb{Z}_p$ and that $\mathbb{F}_q \neq \mathbb{Z}_q$ if $q \neq p$.

Let $r, s \in \mathbb{N}$. We set $[r, s] = \{i \in \mathbb{N} : r \leq i \leq s,\ i \geq 1\}$, $[s] = [1, s]$ (notice that $[0] = \emptyset$), $\mathcal{P}_s$ denotes the power set of $[s]$, and $\mathcal{P}_s^* = \mathcal{P}_s \setminus \{[s]\}$ (notice that $\mathcal{P}_0 = \{\emptyset\}$). Moreover, for all $j \in \{0, \ldots, s\}$, we write $\mathcal{P}_{s,j} = \{I \in \mathcal{P}_s \mid |I| = j\}$ (notice that $\mathcal{P}_{s,0} = \mathcal{P}_0$).

In this paper, we consider every Abelian group $\mathbb{X}$ with additive notation. Let $x_1, \ldots, x_s \in \mathbb{X}$, then we use the convention that $\sum_{i \in \emptyset} x_i = 0$.

2.1 Functions between Abelian groups

Let $F : \mathbb{X} \to \mathbb{Y}$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups.

We say that F is a linear function if $F(x + x') = F(x) + F(x')$ for all $x, x' \in \mathbb{X}$. We say that F is an affine function if $F' = F - F(0)$ is a linear function. Note that we use the terms *linear* and *affine* here, even though $\mathbb{X}$ and $\mathbb{Y}$ are general Abelian groups, not necessarily vector or affine spaces. The *derivative* of F in the direction $a \in \mathbb{X}$ is denoted by $\Delta_a F(x) = F(x + a) - F(x)$ for all $x \in \mathbb{X}$ and the *k-th order derivative* of F in $\underline{a} = (a_1, \ldots, a_k) \in \mathbb{X}^k$ is denoted by $\Delta_{\underline{a}}^{(k)} F = \Delta_{a_1}\Delta_{a_2} \cdots \Delta_{a_k} F$. If $\mathbb{X}$ is $\mathbb{Z}_n$ or $\mathbb{Z}$, we denote $\Delta = \Delta_1$ and $\Delta^{(k)} = \Delta_{(1,\ldots,1)}^{(k)}$.

Let $\mathbb{X}_1, \ldots, \mathbb{X}_n, \mathbb{Y}_1, \ldots, \mathbb{Y}_m$ be Abelian groups. Let $F : \prod_{i \in [n]} \mathbb{X}_i \to \prod_{j \in [m]} \mathbb{Y}_j$. For any $x \in \prod_{i \in [n]} \mathbb{X}_i$, we can write $F(x) = (F_1(x), \ldots, F_m(x))$ where $F_j : \prod_{i \in [n]} \mathbb{X}_i \to \mathbb{Y}_j$ for all $j \in [m]$. Let $i \in [n]$, the *partial derivative* of F in $a \in \mathbb{X}_i$ through the direction of the i-th coordinate is denoted by $\partial_a^i F(x) = F(x_1, \ldots, x_i + a, \ldots, x_n) - F(x)$ for all $x = (x_1, \ldots, x_n) \in \prod_{i \in [n]} \mathbb{X}_i$ and the *k-th order partial derivative* of F in $\underline{a} = (a_1, \ldots, a_k) \in (\mathbb{X}_i)^k$ is denoted by $\partial_{\underline{a}}^{i,(k)} F = \partial_{a_1}^i \partial_{a_2}^i \cdots \partial_{a_k}^i F$. We say that the function F depends on its i-th coordinate input if there exists $a \in \mathbb{X}$ such that $\partial_a^i F \neq 0$. Similarly as before, if $\mathbb{X}_i$ is $\mathbb{Z}_{m_i}$ or $\mathbb{Z}$, we denote $\partial^i = \partial_1^i$ and $\partial^{i,(k)} = \partial_{(1,\ldots,1)}^{i,(k)}$. Moreover, for all $\underline{k} = (k_1, \ldots, k_n) \in \mathbb{N}^n$, we denote $\partial^{(\underline{k})} = \partial^{1,k_1} \cdots \partial^{1,k_n}$. In some cases, we will use the calligraphic letter $\mathcal{F}$ to denote a function from $\mathbb{X}^s$ to $\mathbb{Y}^t$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups.

Suppose that $\mathbb{X}$ and $\mathbb{Y}$ are finite Abelian groups. We say that F is balanced if $|F^{-1}(y)| = |\mathbb{X}|/|\mathbb{Y}|$ for all $y \in \mathbb{Y}$. Observe that if F is balanced and $|\mathbb{X}| = |\mathbb{Y}|$, then F is bijective.

2.2 The functional degree

We will use an equivalent definition of the functional degree based on Fréchet's equation, $\Delta_{\underline{a}}^{(d+1)} F = 0$, as given in [AM21], rather than the original definition from abstract algebra.

Let $F : \mathbb{X} \to \mathbb{Y}$ where $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups. Then the functional degree of F is equal to

$$\mathrm{d}^\circ(F) = \inf\{d \in \mathbb{N} \mid \Delta_{\underline{a}}^{(d+1)} F = 0, \text{ for all } \underline{a} \in \mathbb{X}^{d+1}\}.$$

We have that $\mathrm{d}^\circ(F) = 0$ if and only if F is constant and $\mathrm{d}^\circ(F) \leq 1$ if and only if F is affine [AM21, Lemma 3.1]. If we can write $\mathbb{Y} = \prod_{j \in [m]} \mathbb{Y}_j$ where $\mathbb{Y}_1, \ldots \mathbb{Y}_m$ are Abelian groups, then we can write $F = (F_1, \ldots, F_m)$ where $F_j : \mathbb{X} \to \mathbb{Y}_j$ for all $j \in [m]$. By [AM21, Lemma 3.4], we have that $\mathrm{d}^\circ(F) = \sup_{j \in [m]} \mathrm{d}^\circ(F_j)$.

A useful notion is the one of *partial degree*. Assuming we can write $\mathbb{X} = \prod_{i \in [n]} \mathbb{Y}_i$ where $\mathbb{X}_1, \ldots \mathbb{X}_n$ are Abelian groups. Then the partial degree of F in $i \in [n]$ is denoted as

$$\mathrm{d}_i^\circ(F) = \inf(\{d \in \mathbb{N} \mid \partial_a^{i,(d+1)} F = 0 \text{ for all } a \in \mathbb{X}_i\}).$$

By [AM21, Theorem 5.2], for all $i \in [n]$ we have that $\mathrm{d}^\circ_i(F) \le \mathrm{d}^\circ(F) \le \sum_{i' \in [n]} \mathrm{d}^\circ_{i'}(F)$.

Let p be a prime. Any function $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ has a unique representation of the following form

$$F(x_1, \dots, x_n) = \sum_{\underline{u} \in \{0,\dots,p-1\}^n} c_{\underline{u}} x_1^{u_1} \cdots x_n^{u_n}, \quad c_{\underline{u}} \in \mathbb{F}_p^m$$

that is called the *algebraic normal form (ANF)*. The *algebraic degree* of F is denoted by $\mathrm{d}^{\mathrm{a}}(F) = \sup\left\{\sum_{i \in [n]} u_i \colon c_{\underline{u}} \neq 0\right\}$. By using [AM21, Theorem 10.3], it follows that $\mathrm{d}^\circ(F) = \mathrm{d}^{\mathrm{a}}(F)$. For $p = 2$, a function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is called a Boolean function and a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called a vectorial Boolean function.

2.3 Integer-Valued (IV) polynomials

We use the following definition for the binomial coefficient. That is, for all $n, k \in \mathbb{Z}$ we have that

$$\binom{n}{k} = \begin{cases} \frac{n(n-1)\cdots(n-k+1)}{k!} & \text{if } k > 0, \\ 1 & \text{if } k = 0, \\ 0 & \text{if } k < 0. \end{cases}$$

Let $p \in \mathbb{N}$ be a prime, $a_1, \dots, a_n, b_1, \dots, b_n \in \{0, \dots, p-1\}$, and $a = \sum_{i \in [n]} a_i p^{i-1}$, $b = \sum_{i \in [n]} b_i p^{i-1}$. We have that the Lucas' Theorem holds:

$$\binom{a}{b} = \prod_{i \in [n]} \binom{a_i}{b_i} \pmod{p}.$$

For us, an *Integer-Valued (IV) polynomial* is any polynomial in $\mathbb{Q}[x_1, \dots, x_n]$ such that when it is evaluated over $\mathbb{Z}^n$ takes values over $\mathbb{Z}$. We will use [CC97] as a reference. A univariate Integer-Valued (IV) monomial of degree $d \in \mathbb{N}$ is the polynomial $\binom{x}{d}$ in $\mathbb{Q}[x]$. A multivariate Integer-Valued (IV) monomial of multidegree $(d_1, \dots, d_n) \in \mathbb{N}^n$ is the polynomial $\binom{x_1,\dots,x_n}{d_1,\dots,d_n} = \prod_{j=1}^n \binom{x_j}{d_j}$ in $\mathbb{Q}[x_1, \dots, x_n]$. An Integer-Valued (IV) polynomial P is a polynomial in $\mathbb{Q}[x_1, \dots, x_n]$ that can be written as

$$P(x_1, \dots, x_n) = \sum_{\underline{d} \in \mathbb{N}^n} P_{\underline{d}} \binom{x_1, \dots, x_n}{d_1, \dots, d_n} \tag{1}$$

where $P_{\underline{d}} \in \mathbb{Z}$ and $P_{\underline{d}} \neq 0$ only for finitely many $\underline{d} \in \mathbb{N}^n$. Moreover, $P_{\underline{d}}$ in (1) is equal to $\partial^{(\underline{d})} P(0)$ and

$$\partial^{(\underline{d})} P(x) = \sum_{\underline{a} \in \mathbb{N}^n \colon a_i \le d_i} (-1)^{\sum_{i \in [n]} (d_i - a_i)} \binom{d_1, \dots, d_n}{a_1, \dots, a_n} P(x + a).$$

We present the connection between IV polynomials and the functional degree as in [CS23]. We have that $\mathrm{d}^\circ\binom{x_1,\dots,x_n}{d_1,\dots,d_n} = \sum_{i \in [n]} d_i$ and $\mathrm{d}^\circ_i\binom{x_1,\dots,x_n}{d_1,\dots,d_n} = d_i$ for all $i \in [n]$. Let $\mathbb{Y}$ be a finite Abelian group and let $P\colon \mathbb{Z}^n \to \mathbb{Y}$ with $\mathrm{d}^\circ(P) < \infty$. We say that P admits an IV polynomial representation if we can write P as in (1) where for all $\underline{d} \in \mathbb{N}^n$ the coefficients $P_{\underline{d}}$ are equal to $\partial^{(\underline{d})} P(0)$. In that case, we have that $\mathrm{d}^\circ(P) = \sup\left\{\sum_{i \in [n]} d_i \colon \partial^{(\underline{d})} P(0) \neq 0\right\}$ and that $\mathrm{d}^\circ_i(P) = \sup\{d \in \mathbb{N} \mid \partial^{i,(d)} P(0) \neq 0\}$ for all $i \in [n]$. Let $\mathbb{X} = \prod_{i \in [n]} \mathbb{Z}_{q_i}$ for some $q_i \in \mathbb{N}$ where $\mathbb{Z}_0 = \mathbb{Z}$ and $\mathbb{Z}_1 = \{0\}$. We say that $P\colon \mathbb{Z}^n \to \mathbb{Y}$ is the pullback of a function $F\colon \mathbb{X} \to \mathbb{Y}$ if $P = F \circ \varepsilon$ where $\varepsilon(x_1, \dots, x_n) = (x_1 + q_1\mathbb{Z}, \dots, x_n + q_n\mathbb{Z})$. By using [CS22, Lemma 3.8], we have that $\mathrm{d}^\circ(F) = \mathrm{d}^\circ(P)$. For the case of functions of the form $f\colon \prod_{i \in [n]} \mathbb{Z}_{p^{\alpha_i}} \to \mathbb{Z}_{p^\beta}$, we know the best possible upper bound for the functional degree.

Proposition 1 ([CS22, Theorem 4.9])**.** *Let p be prime and $\alpha_1, \dots, \alpha_n, \beta$ be positive integers. Let $\delta_p(\underline{\alpha}, \beta) = \sum_{i\in[n]} p^{\alpha_i} - n + (\beta-1)(p-1)p^{\alpha_{\max}-1}$ where $\alpha_{\max} = \max_{i\in[n]} \alpha_i$. Then the best upper bound of the functional degree of any $f\colon \prod_{i\in[n]} \mathbb{Z}_{p^{\alpha_i}} \to \mathbb{Z}_{p^\beta}$ is given by $\mathrm{d}^\circ(f) \leq \delta_p(\underline{\alpha}, \beta)$. Moreover, $\mathrm{d}^\circ(f) = \delta_p(\underline{\alpha}, \beta)$ if f is such that $f(0) = 1$ and $f(x) = 0$ for all $x \neq 0$.*

3 Threshold Implementations over Abelian groups

The notion of *Threshold Implementation (TI)* was generalized by Dhooghe et al. [DNR19], who proved that the threshold implementation technique using *Boolean sharing* (also known as *Boolean masking*) is secure in the first-order robust probing model [DNR19, Theorem 3.2]. We are interested in the case where the secret sharing scheme of both input and output is the *additive sharing* (also called *additive masking*). Let $\mathbb{X}$ be an Abelian group. An *additive s-sharing* of $x \in \mathbb{X}$ is a vector $\underline{x} = (x_1, \dots, x_s) \in \mathbb{X}^s$ such that $\sum_{i\in[s]} x_i = x$. The set of such vectors is denoted by $\mathrm{Sh}_s(x)$. Note that $\mathrm{Sh}_s(x) = \underline{x} + \mathrm{Sh}_s(0)$ for all $\underline{x} \in \mathrm{Sh}_s(x)$ and that $\mathrm{Sh}_s(0)$ is an Abelian group of cardinality $|\mathbb{X}|^{s-1}$. Indeed, for all $\underline{x}, \underline{x}' \in \mathrm{Sh}_s(x)$, we have that $\underline{x} - \underline{x}' \in \mathrm{Sh}_s(0)$. In this section (if not specified otherwise), $\mathbb{X}$ and $\mathbb{Y}$ are Abelian groups, $F\colon \mathbb{X} \to \mathbb{Y}$ and $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{X}^t$.

The *correctness property* follows from [DNR19, Definition 6.3]. We say that $\mathcal{F}$ is *correct* with respect to F if for all $x \in \mathbb{X}$ and for all $\underline{x} \in \mathrm{Sh}_s(x)$ we have that $\mathcal{F}(\underline{x}) \in \mathrm{Sh}_t(F(x))$. An equivalent definition is that $F\left(\sum_{i\in[s]} x_i\right) = \sum_{j\in[t]} \mathcal{F}_j(\underline{x})$ for all $\underline{x} = (x_1, \dots, x_s) \in \mathbb{X}^s$.

The *non-completeness property* is almost identical to the one given in [DNR19, Definition 6.4]. We say that $\mathcal{F}$ is non-complete if for all $j \in [t]$, there exists $i \in [s]$ such that $\partial_a^i \mathcal{F}_j = 0$ for all $a \in \mathbb{X}$. Indeed, this is equivalent to say that any of the output share depends on at most on $s-1$ input shares.

The *uniformity property* follows from [DNR19, Definition 6.5]. For the definition to be meaningful, we assume that both $\mathbb{X}$ and $\mathbb{Y}$ are finite, and that $\mathcal{F}$ is correct with respect to F. We say that $\mathcal{F}$ is *uniform* if for all $x \in \mathbb{X}$ and any $\underline{y} \in \mathrm{Sh}_t(F(x))$, we have that

$$|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = \frac{|\mathbb{X}|^{s-1}}{|\mathbb{Y}|^{t-1}}.$$

Indeed, there a positive integer c such that $|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = c$ for all $x \in \mathbb{X}$ and for all $\underline{y} \in \mathrm{Sh}_t(F(x))$. This implies that, for all $x \in \mathbb{X}$, the restriction of $\mathcal{F}$ from $\mathrm{Sh}_s(x)$ to $\mathrm{Sh}_t(F(x))$ is balanced, and therefore $|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = |\mathrm{Sh}_s(x)|/|\mathrm{Sh}_t(F(x))| = |\mathbb{X}|^{s-1}/|\mathbb{Y}|^{t-1}$.

We are ready to give the definition of threshold implementation. We say that $\mathcal{F}$ is a *threshold implementation* of F if $\mathcal{F}$ is correct with respect to F, non-complete, and uniform. In this case, we say that F admits a threshold implementation with s shares in input and t shares in output.

We also discuss higher order threshold implementations. We refer to the definition given in [DNR19, Definition 3.7] for the *k-th order non-completeness property.* We say that $\mathcal{F}$ is *k-th order non-complete* if for all $J \in \mathcal{P}_{t,k}$, there exists $i \in [s]$ such that $\partial_a^i \mathcal{F}_j = 0$ for all $a \in \mathbb{X}$ and all $j \in J$. Then a *k-th order threshold implementation* is a threshold implementation that is also k-th order non-complete.

In this paper, we will also construct threshold implementations $\mathcal{F}$ of F with a particular shape. We say that $\mathcal{F}$ is an *F-implementation* if there exists integers $z_{I,j}$ where $I \in \mathcal{P}_s$ and $j \in [t]$ such that

$$\mathcal{F}_j(x_1, \dots, x_s) = \sum_{I\in\mathcal{P}_s} z_{I,j} F\left(\sum_{i\in I} x_i\right)$$

for all $x_1, \dots, x_s \in \mathbb{X}$. Such threshold implementations can be very interesting for applications when the cost of implementing the evaluation of F is low. For instance, when F is the conversion map from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^n}$ or vice versa.

3.1 On the uniformity property

We discuss the uniformity property of $\mathcal{F}$ for the cases of F balanced and F bijective.

Proposition 2. *Let $\mathcal{F}$ be correct with respect to F. Then we have the following:*

1. *If $\mathcal{F}$ is uniform, then F is balanced if and only if $\mathcal{F}$ is balanced.*
2. *If F is bijective, then $\mathcal{F}$ is uniform if and only if $\mathcal{F}$ is balanced.*

Proof. Let us prove item 1. Let $y \in \mathbb{Y}$ and $\underline{y} \in \mathrm{Sh}_t(y)$. Since $\mathcal{F}$ is uniform, we have that $|\mathcal{F}^{-1}(\underline{y})| = \sum_{x \in F^{-1}(y)} |\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = |F^{-1}(y)| \left(|\mathbb{X}|^{s-1}/|\mathbb{Y}|^{t-1}\right)$. This is enough to prove item 1.

Let us prove item 2. Since F is bijective, then $|\mathbb{X}| = |\mathbb{Y}| = q$. Since any bijective function is balanced, we can use item 1 to conclude that if $\mathcal{F}$ is uniform, then $\mathcal{F}$ is balanced. Suppose that $\mathcal{F}$ is balanced and we claim that $\mathcal{F}$ is uniform. Let $\underline{y} = (y_1, \dots, y_t) \in \mathbb{Y}^t$, $y = \sum_{j \in [t]} y_j$, and $x = F^{-1}(y)$. Observe that $\left|\mathcal{F}^{-1}(\underline{y})\right| = \sum_{z \in F^{-1}(y)} |\mathrm{Sh}_s(z) \cap \mathcal{F}^{-1}(\underline{y})| = \left|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})\right|$. Since $\mathcal{F}$ is balanced, then $|\mathcal{F}^{-1}(\underline{y})| = \frac{|\mathbb{X}|^{s-1}}{|\mathbb{Y}|^{t-1}} = q^{s-t}$ and $|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})| = q^{s-t}$. This concludes the proof of item 2. □

We note that Proposition 2 addresses all the cases. See Appendix A for the details. We can have that F and $\mathcal{F}$ are unbalanced and $\mathcal{F}$ is uniform. Moreover, we can have F and $\mathcal{F}$ are balanced and $\mathcal{F}$ is not uniform.

3.2 Functional expansions and non-completeness

We say that F admits a *functional expansion of the s-th order* if there exists a family of integers $\{k_I\}_{I \in \mathcal{P}_s^*}$ such that

$$F\left(\sum_{i \in [s]} x_i\right) = \sum_{I \in \mathcal{P}_s^*} k_I \cdot F\left(\sum_{i \in I} x_i\right)$$

for all $x_1, \dots, x_s \in \mathbb{X}$. In [CPRR15, Corollary 1], it was shown that every function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ admits a functional expansion of the s-th order where $s \geq \mathrm{d}^{\mathrm{a}}(F) + 1$. Moreover, we have that if $\mathcal{F} \colon (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^m)^t$ is non-complete and correct with respect to F, then both s and t must be greater than or equal to $\mathrm{d}^{\mathrm{a}}(F) + 1$ [NRR06, Theorem 1]. Indeed, one can use a functional expansion of the s-th order and construct $\mathcal{F}$. This observation was made first in [PAB+23] and used to construct a family of threshold implementations. Clearly, there is a connection between functional expansions and the algebraic degree of F. We want to achieve similar results by using the notion of functional degree introduced by Aichinger and Moosbauer in [AM21].

In [AM21, Lemma 4.1], it is proven that for a function F to have finite functional degree is equivalent to three other properties. The first two can be described as the existence of particular functional expansions of F while the last one is the existence of a function $\mathcal{F}$ which is correct with respect to F and non-complete. We present the following lemma in our notation and prove that it is equivalent to [AM21, Lemma 4.1].

Lemma 1. *Let d be a non-negative integer. Then the following are equivalent:*

1. $\mathrm{d}^{\circ}(F) \leq d$.

2. *For every positive integer $s \geq d+1$, the function F admits the following functional expansion of the s-th order:*
$$F\left(\sum_{i\in[s]} x_i\right) = \sum_{j=0}^{s-1}(-1)^{s-1-j} \sum_{I\in\mathcal{P}_{s,j}} F\left(\sum_{i\in I} x_i\right).$$

3. *For every positive integer $s \geq d+1$, the function F admits a functional expansion of the s-th order for some family of integers $\mathcal{K}_s = \{k_I\}_{I\in\mathcal{P}_s^*}$ where $k_I = 0$ if $|I| \geq d+1$.*

4. *For every positive integer $s \geq d+1$, there exists a function $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^{d+1}$ that is correct with respect to F and non-complete.*

Proof. 1, 2, 3 are equivalent respectively to the first three items in [AM21, Lemma 4.1]. Let us call $4a$ the fourth item in [AM21, Lemma 4.1] which states that there exist functions $\mathcal{F}_1, \dots, \mathcal{F}_{d+1}\colon \mathbb{X}^{d+1} \to \mathbb{Y}$ such that for all $\underline{x} = (x_1, \dots, x_{d+1}) \in \mathbb{X}^{d+1}$ we have $F\left(\sum_{i\in[d+1]} x_i\right) = \sum_{j\in[d+1]} \mathcal{F}_j(\underline{x})$ and for each $j \in [d+1]$, the function $\mathcal{F}_j$ does not depend on its j-th coordinate. We show that 4 is equivalent to $4a$. It is clear that $4a$ implies 4 since for any $s \geq d+1$, we can set $\mathcal{F} = (\mathcal{F}_1, \dots, \mathcal{F}_{d+1}, 0, \dots, 0)$. We conclude by proving that 4 implies $4a$. Let $\mathcal{F}\colon \mathbb{X}^{d+1} \to \mathbb{Y}^{d+1}$ be correct with respect to F and non-complete. Let $\mathcal{F}_1, \dots, \mathcal{F}_{d+1}\colon \mathbb{X}^{d+1} \to \mathbb{Y}$ be such that $\mathcal{F} = (\mathcal{F}_1, \dots, \mathcal{F}_{d+1})$. We define $J_1 = \{i \in [d+1] \mid \partial_a^1 \mathcal{F}_i = 0 \text{ for all } a \in \mathbb{X}\}$ and $J_j = \{i \in [d+1] \setminus J_{j-1} \mid \partial_a^j \mathcal{F}_i = 0 \text{ for all } a \in \mathbb{X}\}$ for $j \in [2, d+1]$. Set $\mathcal{F}'_j = \sum_{i\in J_j} \mathcal{F}_i$ where we recall that $\sum_{i\in\emptyset} \mathcal{F}_i = 0$. Then $\mathcal{F}'_1, \dots, \mathcal{F}'_{d+1}$ satisfies $4a$. □

A natural problem that rises from Lemma 1 is to give an explicit form of the functional expansion described in item 3. To the best of our knowledge, we are not aware if this result is known for the general case. In the binary case, this problem was solved in [CPRR15, Corollary 1].

Proposition 3. *Let d be a non-negative integer. Let $\mathbb{X}$ and $\mathbb{Y}$ be Abelian groups and $F\colon \mathbb{X} \to \mathbb{Y}$. Then $\mathrm{d}^\circ(F) \leq d$ if and only if for any positive integer $s \geq d+1$, F admits the following functional expansion of the s-th order:*
$$F\left(\sum_{i\in[s]} x_i\right) = \sum_{j=0}^{d} \mu_{s,d}(j) \sum_{I\in\mathcal{P}_{s,j}} F\left(\sum_{i\in I} x_i\right)$$
where $\mu_{s,d}(j) = \binom{s-j-1}{d-j}(-1)^{d-j}$.

Proof. Let us prove it by induction on d starting from $s-1$ and descending to $\mathrm{d}^\circ(F)$. The case $d = s-1$ follows by Lemma 1 because $\mu_{s,s-1}(j) = (-1)^{s-1-j}$. Assume $\mathrm{d}^\circ(F) < d \leq s-1$. Let $I \in \mathcal{P}_{s,d}$, then we have that
$$F\left(\sum_{i\in I} x_i\right) = \sum_{j=0}^{d-1}(-1)^{d-1-j} \sum_{J\subseteq I,\, |J|=j} F\left(\sum_{i\in J} x_i\right).$$
Now take any $J \in \mathcal{P}_{s,j}$ with $j < d$. There exists exactly $\binom{s-j}{d-j}$ sets I in $\mathcal{P}_{s,d}$ such that $J \subseteq I$. Therefore, we have that
$$F\left(\sum_{i\in[s]} x_i\right) = \sum_{j=0}^{d-1}\left(\mu_{s,d}(j) + \mu_{s,d}(d)\binom{s-j}{d-j}(-1)^{d-1-j}\right) \sum_{I\in\mathcal{P}_{s,j}} F\left(\sum_{i\in I} x_i\right).$$
Since $\mu_{s,d}(d) = 1$, we have that $\mu_{s,d}(j) + \mu_{s,d}(d)\binom{s-j}{d-j}(-1)^{d-1-j} = \binom{s-j-1}{d-j}(-1)^{d-j} + \binom{s-j}{d-j}(-1)^{d-1-j} = \left(-\binom{s-j-1}{d-j} + \binom{s-j}{d-j}\right)(-1)^{d-1-j} = \binom{s-j-1}{d-1-j}(-1)^{d-1-j} = \mu_{s,d-1}(j)$. This concludes the proof. □

3.3 On the minimal number of input and output shares

With the following proposition, we generalize [NRR06, Theorem 1] for our setting.

Proposition 4. *Let d be a non-negative integer. Let $\mathcal{F}$ be correct with respect to F. If $\mathrm{d}^\circ(F) = d$ and $\mathcal{F}$ is non-complete, then s and t are greater than or equal to $d+1$.*

Proof. Suppose that $t \leq d$. Let $\underline{x} = (x_1, \dots, x_s) \in \mathbb{X}^s$. Since $\mathcal{F}$ is non-complete, then for any $j \in [t]$ there exists $i_j \in [s]$ such that $\partial^{i_j}_a \mathcal{F}_j(\underline{x}) = 0$ for all $a \in \mathbb{X}$. Let $\mathcal{H}(\underline{x}) = F\left(\sum_{i\in[s]} x_i\right)$, $x = \sum_{i\in[s]} x_i$, and $\underline{a} = (a_1, \dots, a_t) \in \mathbb{X}^t$. Then we have that $0 = \sum_{j\in[t]} \partial^{i_j}_{a_j}\mathcal{F}_j(\underline{x}) = \partial^{i_1}_{a_1}\cdots\partial^{i_t}_{a_t}\sum_{j\in[t]}\mathcal{F}_j(\underline{x}) = \partial^{i_1}_{a_1}\cdots\partial^{i_t}_{a_t}\mathcal{H}(\underline{x}) = \Delta^{(t)}_{\underline{a}}F(x)$ because $\partial^k_a\mathcal{H}(\underline{x}) = F\left(\sum_{i\in[s]} x_i + a\right) - F\left(\sum_{i\in[s]} x_i\right) = \Delta_a F(x)$ for any $k \in [s]$ and any $a \in \mathbb{X}$. Therefore, we have that $\Delta^{(t)}_{\underline{a}}F(x) = 0$ but this is not possible because $\mathrm{d}^\circ(F) = d > t-1$. So we have that $t \geq d+1$. Suppose that $s \leq d$ and $t \geq d+1$. By item 4 of Lemma 1, this implies that $\mathrm{d}^\circ(F) = d < s$ and this is not possible since $s \leq d$. □

We discuss now higher order non-completeness. Instead of deriving all the results from the beginning, we are going to prove that the existence of a correct and k-th order non-complete function is equivalent to the existence of a particular set covering [Pet19, Definition 2.1] and then we are going to use the theory developed in [Pet19] to derive some results.

Proposition 5. *Let k be a positive integers and d be a non-negative integer such that $d = \mathrm{d}^\circ(F)$. Then there exists a k-th order non-complete function $\mathcal{F}$ correct with respect to F if and only if there exists $\mathrm{S}^{\mathrm{nc}}_{s,d,k} \subseteq \mathcal{P}_s$ such that*

1. *$t \geq |\mathrm{S}^{\mathrm{nc}}_{s,d,k}|$.*

2. *For every $I \in \mathcal{P}_{s,d}$ there exists $J \in \mathrm{S}^{\mathrm{nc}}_{s,d,k}$ such that $I \subseteq J$.*

3. *Every $J \in \mathrm{S}^{\mathrm{nc}}_{s,d,k}$ is such that $|J| \geq d$.*

4. *For every $J_1, \dots, J_k \in \mathrm{S}^{\mathrm{nc}}_{s,d,k}$ we have that $\cup_{i=1}^k J_i \neq \mathcal{P}_s$.*

In particular, we can choose $\mathcal{F}$ to be such that for each $j \in [t]$ there exists $I_j \in \mathrm{S}^{\mathrm{nc}}_{s,d,k}$ such that $\partial^i_a\mathcal{F}_j = 0$ for all $a \in \mathbb{X}$ and all $i \in [s] \setminus I_j$.

Proof. If $\mathrm{S}^{\mathrm{nc}}_{s,d,k} \subseteq \mathcal{P}_s$ exists, then by using item 2 and 3, we must have that $s \geq d+1$. Then we can construct $\mathcal{F}$ by using a functional expansion of the s-th order for some family of integers $\mathcal{K}_s = \{k_I\}_{I\in\mathcal{P}^*_s}$ where $k_I = 0$ if $|I| \geq d+1$. We known that it exists because of Lemma 1 item 3.

If $\mathcal{F}$ exists, then we must have that $s \geq d+1$ because of Proposition 4. Then we can construct $\mathrm{S}^{\mathrm{nc}}_{s,d,k}$ by including for each $j \in [t]$ the set $I_j \in \mathcal{P}_s$ such that $\partial^i_a\mathcal{F}_j = 0$ for all $a \in \mathbb{X}$ and all $i \in [s] \setminus I_j$. □

Corollary 1. *Let k be a positive integer and d be a non-negative integer such that $d = \mathrm{d}^\circ(F)$. If there exists a k-th order non-complete function $\mathcal{F}$ correct with respect to F, then s and t are greater than or equal to $kd+1$. Moreover, if $s = kd+1$ then $t \geq \binom{kd+1}{k}$.*

Proof. It follows from [Pet19, Proposition 2.5], [Pet19, Proposition 2.6] and [Pet19, Corollary 2.8]. □

3.4 Compositions of threshold implementations

We want to discuss the property of the composition of two threshold implementations. Let $\mathbb{W}$ be an Abelian group, let u be a positive integer, let $G\colon \mathbb{Y} \to \mathbb{W}$, let $H = G \circ F$, let $\mathcal{G}\colon \mathbb{Y}^t \to \mathbb{W}^u$ and let $\mathcal{H} = \mathcal{G} \circ \mathcal{F}$. We have that if $\mathcal{F}$ is correct with respect to F and $\mathcal{G}$ is correct with respect to G, then $\mathcal{H}$ is correct with respect to H. Indeed, if $\underline{x} \in \mathrm{Sh}_s(x)$ then $\mathcal{F}(\underline{x}) \in \mathrm{Sh}_t(F(x))$ and $\mathcal{H}(\underline{x}) = \mathcal{G}(\mathcal{F}(\underline{x})) \in \mathrm{Sh}_u(G(F(x))) = \mathrm{Sh}_u(H(x))$. Moreover, if $\mathcal{F}$ is uniform and $\mathcal{G}$ is uniform, then $\mathcal{H}$ uniform. The proof is basically identical to the one given in [DNR19, Lemma 3.2], but we do it for completeness. Indeed, for all $\underline{x} \in \mathrm{Sh}_s(x)$ and $\underline{w} \in \mathrm{Sh}_u(H(x))$ then

$$\begin{aligned}\left|\mathrm{Sh}_s(x) \cap \mathcal{H}^{-1}(\underline{w})\right| &= \left|\{\underline{x} \in \mathrm{Sh}_s(x)\colon \mathcal{H}(\underline{x}) = \underline{w}\}\right| = \left|\left\{\underline{x} \in \mathrm{Sh}_s(x)\colon \mathcal{F}(\underline{x}) \in \mathcal{G}^{-1}(\underline{w})\right\}\right| \\ &= \sum_{\underline{y} \in \mathrm{Sh}_t(F(x)) \cap \mathcal{G}^{-1}(\underline{w})} \left|\mathrm{Sh}_s(x) \cap \mathcal{F}^{-1}(\underline{y})\right| = \frac{|\mathbb{X}|^{s-1}}{|\mathbb{Y}|^{t-1}} \frac{|\mathbb{Y}|^{t-1}}{|\mathbb{W}|^{u-1}} = \frac{|\mathbb{X}|^{s-1}}{|\mathbb{W}|^{u-1}}.\end{aligned}$$

Regarding non-completeness, the problem can be addressed in the concrete implementation by waiting to the end of the current clock cycle and run the second implementation in the next clock cycle. Since the number of shares is related to the functional degree of F, in most cases, it is a good idea to decompose it in low degree functions $F_1, \ldots, F_\ell$ such that $F = F_1 \circ \cdots \circ F_\ell$ because the respective threshold implementations will need fewer shares. We can say, by oversimplifying a lot, that such implementation need k clock cycles of the CPU. In itself, the decomposition problem is very hard even by restricting to permutations of $\mathbb{F}_2^n$ [NNR19, Pet23, LSaa24, APB$^+$23]. For k-th order non-completeness, what we have discussed previously is usually not enough to make the whole implementation k-th order secure. For this reason, we will not discuss real-world examples with higher order security than one.

4 On a general construction of threshold implementations with $d + 2$ shares

In this section, we are going to generalize the construction defined in [PAB$^+$23]. We will consider those functions $F\colon \mathbb{X} \to \mathbb{Y}$ between two finite Abelian groups such that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$ and $\mathrm{d}^\circ(F) < \infty$. The hypothesis $\mathrm{d}^\circ(F) < \infty$ is strictly necessary because of Lemma 1. We impose that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$ because we will need the existence of at least one balanced function from $\mathbb{X}$ to $\mathbb{Y}$. Therefore, we need that $s \geq t$ because if $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ is uniform then $|\mathbb{X}|^{s-1}/|\mathbb{Y}|^{t-1} = |\mathbb{X}|^{s-t}(|\mathbb{X}|/|\mathbb{Y}|)^{t-1}$ must be a positive integer.

Remark 1. If $\mathrm{d}^\circ(F) = 1$, then we can easily construct a threshold implementation of F for any $t \geq 2$ by setting $\mathcal{F}_j(\underline{x}) = F(x_j)$ for all $j \in [t-1]$ and $\mathcal{F}_t(\underline{x}) = \sum_{i \in [t,s]} F(x_i) - (s-1)F(0)$.

First, we describe a way to construct functions $\mathcal{F}$ that are correct and uniform. This includes the result obtained in [PAB$^+$23] but requires a completely different proof. Indeed, in the proof of [PAB$^+$23, Proposition 3] it is enough to prove that the function $\mathcal{F}$ is a permutation (because F is a permutation, $s = t$ and by Proposition 2), but instead we are going to prove the uniformity property by using only the definition. Then we present a functional expansion into terms that can be distributed in the coordinate functions of $\mathcal{F}$ in order to make it non-complete.

In the following, we have the main theorem of this section that we are going to prove.

Theorem 1. *Let $\mathbb{X}$ and $\mathbb{Y}$ be finite Abelian groups such that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$. Let s, d be positive integers such that $s \geq d+2$. Then any function $F\colon \mathbb{X} \to \mathbb{Y}$ with functional degree at most d admits a threshold implementation $\mathcal{F}$ with s shares in input and $d+2$ shares in output. Moreover, if F is balanced, then we can choose $\mathcal{F}$ to be an F-implementation.*

As a direct consequence of Theorem 1, we have the following corollary.

Corollary 2. *Let m, n, p, s, d be positive integers such that $m \leq n$, $s \geq d+2$, and p is a prime. Then any function $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ with algebraic degree at most d admits a threshold implementation $\mathcal{F}$ with s shares in input and $d+2$ shares in output. Moreover, if F is balanced, then we can choose $\mathcal{F}$ to be an F-implementation.*

We provide a general form for the construction of a correct and uniform function.

Proposition 6. *Let $\mathbb{X}$ and $\mathbb{Y}$ be finite Abelian groups such that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$. Let $F\colon \mathbb{X} \to \mathbb{Y}$ be any function. Let s and t be positive integers such that $2 \leq t \leq s$. For any $j \in \{1, \dots, t-1\}$, let $P_j\colon \mathbb{X} \to \mathbb{Y}$ be balanced and let $\mathcal{C}_j\colon \mathbb{X}^j \to \mathbb{Y}$. Let $\underline{b} = (b_1, \dots, b_{t-1}) \in \{0,1\}^{t-1}$ and let $\mathcal{F}\colon \mathbb{X}^s \to \mathbb{Y}^t$ be a function defined as follows for any $\underline{x} = (x_1, \dots, x_s) \in \mathbb{X}^s$:*

$$\mathcal{F}_t(\underline{x}) = F\left(\sum_{i\in[s]} x_i\right) - \sum_{j\in[t-1]} \mathcal{F}_j(\underline{x})$$

and for any $j \in [t-1]$ we have

$$\mathcal{F}_j(\underline{x}) = (1-b_j)\cdot P_j\left(x_j\right) + b_j \cdot P_j\left(\sum_{i\in[j+1,s]} x_i\right) + \mathcal{C}_j(\underline{x}^{(j)}),$$

where $\underline{x}^{(j)} = ((x_i)_{i\in[j-1]}, \sum_{i\in[j,s]} x_i)$ with the abuse of notation that $\underline{x}^{(1)} = \sum_{i\in[s]} x_i$.

Then the following holds:

1. *$\mathcal{F}$ is correct with respect to F.*
2. *$\mathcal{F}$ is uniform.*

Proof. Let us prove 1. Function $\mathcal{F}$ is correct with respect to F because

$$\sum_{j\in[t]} \mathcal{F}_j(\underline{x}) = \sum_{j\in[t-1]} \mathcal{F}_j(\underline{x}) + \mathcal{F}_t(\underline{x}) = F\left(\sum_{i\in[s]} x_i\right).$$

Let us prove 2. Let $x \in \mathbb{X}$ and let $\underline{y} \in \mathrm{Sh}_t(F(x))$. Consider the system

$$\begin{cases} y_1 = \mathcal{F}_1(\underline{x}) \\ y_2 = \mathcal{F}_2(\underline{x}) \\ \dots \\ y_t = \mathcal{F}_t(\underline{x}) \\ x = \sum_{i\in[s]} x_i \end{cases} \tag{2}$$

in the variable $\underline{x} \in \mathbb{X}^s$. Observe that the number of solutions of system (2) is equal to $|\mathrm{Sh}_s(x) \cap (\mathcal{F})^{-1}(\underline{y})|$. So if we prove that system (2) has exactly $|\mathbb{X}|^{s-1}/|\mathbb{Y}|^{t-1}$ solutions, then we have that $\mathcal{F}$ is uniform. To do that, we are going to turn system (2) into a triangular system. Observe that by summing the first t equations of system (2), we have that $\sum_{j\in[t]} y_j = \sum_{j\in[t]} \mathcal{F}_j(\underline{x}) = F\left(\sum_{i\in[s]} x_i\right) = F(x)$. So we can replace the t-th equation of system (2) with the equation $\sum_{j\in[t]} y_j = F(x)$. For any $j \in [t-1]$, we claim that we can replace the j-th equation of system (2) with a condition of the form $x_j \in \Gamma_j(x_i)_{i\in[j-1]}$

where $\Gamma_j(x_i)_{i\in[j-1]} \subseteq \mathbb{X}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$ for all $(x_i)_{i\in[j-1]} \in \mathbb{X}^{j-1}$. So we have that system (2) is equivalent to the following system

$$\begin{cases} x_j \in \Gamma_j(x_i)_{i\in[j-1]}, \quad j \in [t-1] \\ \sum_{j\in[t]} y_j = F(x) \\ x = \sum_{i\in[s]} x_i \end{cases} . \tag{3}$$

System (3) can be solved in the following way. Let $\underline{x} \in \mathbb{X}^s$ be any solution of system (3). By solving the first $t-1$ equations in order, we have that the number of choices of the first $t-1$ coordinates of $\underline{x}$ are exactly $(|\mathbb{X}|/|\mathbb{Y}|)^{t-1}$. Observe that the t-th equation is not written in terms of $\underline{x}$. By using the $t+1$-th equation, we have that there are $|\mathbb{X}|^{s-t}$ choices for the remaining $s-t$ coordinates of $\underline{x}$. So the number of solutions of system (3) is $(|\mathbb{X}|)^{s-1}/(|\mathbb{Y}|)^{t-1}$ and so is the number of solution of system (2).

Let us prove that for any $j \in [t-1]$ we can replace the j-th equation of system (2) with a condition of the form $x_j \in \Gamma_j(x_i)_{i\in[j-1]}$ where $\Gamma_j(x_i)_{i\in[j-1]} \subseteq \mathbb{X}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$. By using the $t+1$-th equation of system (2), we have that $\sum_{i\in[j,s]} x_i = x - \sum_{i\in[j-1]} x_i$. Therefore, the term $\mathcal{C}_j(\underline{x}^{(j)})$ depends only on $(x_i)_{i\in[j-1]}$. Suppose that $b_j = 0$. Then $y_j = P_j(x_j) + \mathcal{C}_j(\underline{x}^{(j)})$ and so we have that

$$\Gamma_j(x_i)_{i\in[j-1]} = P_j^{-1}\left(y_j - \mathcal{C}_j(\underline{x}^{(j)})\right)$$

and that $\Gamma_j(x_i)_{i\in[j-1]}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$ because P_j is balanced. Suppose that $b_j = 1$. Then $y_j = P_j(\sum_{i\in[j+1,s]} x_i) + \mathcal{C}_j(\underline{x}^{(j)})$ and $x_j \in \Gamma_j(x_i)_{i\in[j-1]} = (x - \sum_{i\in[j-1]} x_i) - P_1^{-1}(y_1 - \mathcal{C}_1(x))$ because

$$\begin{aligned} y_j &= P_j\left(\sum_{i\in[j+1,s]} x_i\right) + \mathcal{C}_j(\underline{x}^{(j)}), \\ \sum_{i\in[j+1,s]} x_i &\in P_j^{-1}\left(y_j - \mathcal{C}_j(\underline{x}^{(j)})\right), \\ x_j &\in \left(\sum_{i\in[j-1]} x_i - x\right) - P_j^{-1}\left(y_j - \mathcal{C}_j(\underline{x}^{(j)})\right) = \Gamma_j(x_i)_{i\in[j-1]}, \end{aligned}$$

by using the $t+1$-th equation of system (2). We claim that $\Gamma_j(x_i)_{i\in[j-1]}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$. Since P_j is balanced, the set $P_j^{-1}\left(y_j - \mathcal{C}_j(\underline{x}^{(j)})\right)$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$ and therefore $\left(\sum_{i\in[j-1]} x_i - x\right) - P_j^{-1}\left(y_j - \mathcal{C}_j(\underline{x}^{(j)})\right)$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$ as well. This proves that $\Gamma_j(x_i)_{i\in[j-1]}$ has cardinality $|\mathbb{X}|/|\mathbb{Y}|$. □

We have established some sufficient conditions to construct a correct and uniform function. One can recognize that we can prove the uniformity property of the construction in [PAB+23] by using directly Proposition 6. With the following lemma, we will address the non-completeness property. This follows the same rationale of the proof of the construction in [PAB+23].

Lemma 2 ([PAB+23, Lemma 2])**.** *Let t be a positive integer. For any $j \in [2, t+1]$, let $\mathcal{J}_j = \{I \cup [j,t] \colon I \in \mathcal{P}_{j-2}\}$. Then $\mathcal{P}^*_{t+1} = \mathcal{P}_t \cup \{I \cup \{t+1\} \colon I \in \mathcal{P}^*_t\}$ and the sets $\mathcal{J}_2, \dots, \mathcal{J}_{t+1}$ form a partition of $\mathcal{P}^*_t$.*

Lemma 3. *Let $\mathbb{X}$ and $\mathbb{Y}$ be finite Abelian groups and let $F \colon \mathbb{X} \to \mathbb{Y}$ be a function. If $\mathrm{d}^\circ(F) \le d$ for some positive integer d, then for any positive integer $s \ge d+2$ we have that*

F admits the following functional expansion of the s-th order:

$$F\left(\sum_{i\in[s]} x_i\right) = \sum_{j\in[2,d+1]}\sum_{I\in\mathcal{P}_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right) + \sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} x_i\right).$$

Proof. Let $z_i = x_i$ for $i = 1,\dots,d$ and $z_{d+1} = \sum_{i\in[d+1,s]} x_i$. Then the result follows by using Lemma 1 and Lemma 2:

$$F\left(\sum_{i\in[s]} x_i\right) = F\left(\sum_{i\in[d+1]} z_i\right) = \sum_{I'\in\mathcal{P}^*_{d+1}} (-1)^{d-|I'|} F\left(\sum_{i\in I'} z_i\right)$$

$$= \sum_{j\in[2,d+1]}\sum_{I\in\mathcal{P}_{j-2}} (-1)^{d-|I|-(d-j)} F\left(\sum_{i\in I} z_i + \sum_{i\in[j,d+1]} z_i\right) + \sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} z_i\right)$$

$$= \sum_{j\in[2,d+1]}\sum_{I\in\mathcal{P}_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right) + \sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} x_i\right).$$

□

Lemma 4. *Suppose to be in the hypothesis of Proposition 6. Let d be a positive integer. If $\mathrm{d}^\circ(F) \le d$ and $t = d+2$, then there exists at least one choice of $\mathcal{C}_1,\dots,\mathcal{C}_{d+1}$ such that the following holds:*

- *$\mathcal{C}_1$ is constant,*
- *for any $j \in [2, d+1]$ and any $a \in \mathbb{X}$ we have that $\partial_a^{j-1}\mathcal{C}_j = 0$.*
- *there exists $k \in [d+1, s]$ such that $\partial_a^k \mathcal{F}_{d+2} = 0$ for all $a \in \mathbb{X}$.*

In this case, $\mathcal{F}$ is a threshold implementation of F.

Proof. We set $\mathcal{C}_1 = 0$ and

$$\mathcal{C}_j(\underline{x}^{(j)}) = \sum_{I\in\mathcal{P}_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right) - b_{j-1}\cdot P_{j-1}\left(\sum_{i\in[j,s]} x_i\right)$$

for any $j \in [2, d+1]$ and any $\underline{x} \in \mathbb{X}^s$. So $\mathcal{C}_1,\dots,\mathcal{C}_{d+1}$ satisfy the first two items. Let us prove the last item. By using Lemma 3, we have that $\mathcal{F}_{d+2}(\underline{x})$ is equal to

$$F\left(\sum_{i\in[s]} x_i\right) - \sum_{j\in[d+1]}\left(\mathcal{C}_j(\underline{x}^{(j)}) + (1-b_j)\cdot P_j(x_j) + b_j\cdot P_j\left(\sum_{i\in[j+1,s]} x_i\right)\right)$$

$$= F\left(\sum_{i\in[s]} x_i\right) - \sum_{j\in[2,d+1]}\sum_{I\in\mathcal{P}_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right)$$

$$- \sum_{j\in[d+1]} (1-b_j)\cdot P_j(x_j) - b_{d+1}\cdot P_{d+1}\left(\sum_{i\in[d+2,s]} x_i\right)$$

$$= \sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} x_i\right) - \sum_{j\in[d+1]} (1-b_j)\cdot P_j(x_j) - b_{d+1}\cdot P_{d+1}\left(\sum_{i\in[d+2,s]} x_i\right).$$

So we have that $\partial_a^{d+2}\mathcal{F}_{d+2}(\underline{x}) = 0$ if $b_{d+1} = 0$ and $\partial_a^{d+1}\mathcal{F}_{d+2}(\underline{x}) = 0$ if $b_{d+1} = 1$.

Let us show that $\mathcal{F}$ is a threshold implementation of F. Since all the hypothesis of Proposition 6 are satisfied, then $\mathcal{F}$ is correct and uniform. To conclude, we claim that $\mathcal{F}$ is non-complete. Let $a \in \mathbb{X}$ and $\underline{x} \in \mathbb{X}^s$. Since $\mathcal{C}_1$ is constant, we have that $\partial_a^2\mathcal{F}_1 = 0$ if $b_1 = 0$ and $\partial_a^1\mathcal{F}_1 = 0$ if $b_1 = 1$. For any $j \in [2, d+1]$, we have that $\partial_a^{j-1}\mathcal{F}_j = \partial_a^{j-1}\mathcal{C}_j = 0$. Then there exists $k \in [d+1, s]$ such that $\partial_a^k\mathcal{F}_{d+2} = 0$. □

In Appendix B, we write explicitly the example described in the proof of Lemma 4.

Proof of Theorem 1. Take $\mathcal{F}$ as in Appendix B and if F is balanced set $P_j = F$. □

Remark 2. Let $\mathcal{F}$ be as in Appendix B. We can use Proposition 3 to simplify some expressions in the definition of $\mathcal{F}$. Let j be a positive integer greater or equal than 2. Then $\sum_{I\in\mathcal{P}_{j-2}}(-1)^{j-|I|}F\left(\sum_{i\in I}x_i + \sum_{i\in[j,s]}x_i\right)$ is equal to 0 if $j > \mathrm{d}^\circ(F) + 2$ and to $\sum_{I\in\mathcal{P}_{j-2}}(-1)^{j-|I|}F\left(\sum_{i\in I}x_i\right)$ if $j = \mathrm{d}^\circ(F) + 2$.

Remark 3. Let us consider the case where F is balanced. We want to give an explicit form of the construction given in Appendix B that minimizes the number of sums of the input shares. We present an elegant solution. For each $j \in [2, d+1]$, we have that the term $(-1)^jF\left(\sum_{i\in[j,s]}x_i\right)$ appears in the expression of $\mathcal{F}_j(\underline{x})$. However, if $P_{j-1} = (-1)^{j-2}F$ and $b_{j-1} = 1$ then such term is cancelled in the expression of $\mathcal{F}_j(\underline{x})$ and computed instead in $\mathcal{F}_{j-1}(\underline{x})$. Indeed, we have that

$$\begin{aligned}\mathcal{F}_j(\underline{x}) =&(1-b_j)\cdot P_j(x_j) + b_j\cdot P_j\left(\sum_{i\in[j+1,s]}x_i\right) + \sum_{I\in\mathcal{P}_{j-2}}(-1)^{j-|I|}F\left(\sum_{i\in I}x_i + \sum_{i\in[j,s]}x_i\right)\\ &-(-1)^jF\left(\sum_{i\in[j,s]}x_i\right)\\ =&(1-b_j)\cdot P_j(x_j) + b_j\cdot P_j\left(\sum_{i\in[j+1,s]}x_i\right) + \sum_{I\in\mathcal{P}^*_{j-2}}(-1)^{j-|I|}F\left(\sum_{i\in I}x_i + \sum_{i\in[j,s]}x_i\right).\end{aligned}$$

One can find the explicit expression in Appendix B.1.

Remark 4. We estimate the number of operations needed to evaluate $\mathcal{F}$ as in Appendix B.1. Let $\mathcal{F}'$ be as in Appendix B.1 with $s = d+2$, then $\mathcal{F}(\underline{x}) = \mathcal{F}'\left(x_1, \ldots, x_{d+1}, \sum_{i\in[d+2,s]}x_i\right)$. So we can assume $d = s-2$. Without loss of generality, assume $d = \mathcal{O}(\mathrm{d}^\circ)$. The number of evaluations of F is $\mathcal{O}(2^{\mathrm{d}^\circ})$. The number of additions (considering also subtractions) in $\mathbb{Y}$ is equal to $\mathcal{O}(2^{\mathrm{d}^\circ})$. The number of additions in $\mathbb{X}$ is equal to $\mathcal{O}(\mathrm{d}^\circ\cdot 2^{\mathrm{d}^\circ})$.

4.1 On a Threshold implementation of the multiplication map with 4 shares

There are numerous uses of the multiplication maps in cryptography, such as the square and multiply algorithm used for the side-channel secure implementation of AES in [Bar86] and the Pseudo-Random Function Ciminion [DGGK21]. We are going to give an implementation with 4 shares. To the best of our knowledge, it does not exist in literature an implementation with fewer shares that does not use some extra assumption.

Let R be a finite ring. Let $F\colon R^2 \to R$ be the multiplication map, i.e. $F(a,b) = ab$. Then it is easy to show that F has functional degree 2. Let $L\colon R^2 \to R$ defined by $L(a,b) = a+b$. Observe that L is linear and balanced. Let $\underline{x} = (x_1, x_2, x_3, x_4) \in (R^2)^4$

where $x_i = (a_i, b_i) \in R^2$ for $i \in [4]$. Then we can construct $\mathcal{F} \colon (R^2)^4 \to R^4$ as in Appendix B with $b_1 = b_2 = b_3 = 0$ and $P_1 = P_2 = P_3 = L$. Therefore, $\mathcal{F}(\underline{x})$ is equal to

$$\begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 + \sum_{i,j\in[2,4]} a_i b_j \\ a_3 + b_3 + a_1b_1 + a_1b_3 + a_1b_4 + a_3b_1 + a_4b_1 \\ a_1b_2 + a_2b_1 - a_1 - a_2 - a_3 - b_1 - b_2 - b_3 \end{pmatrix}.$$

5 On a construction for second order Threshold Implementation of quadratic balanced functions

In this section, we present a construction for second order Threshold Implementation of quadratic balanced functions. We want to demonstrate that it is possible to do general construction of higher order threshold implementations with a similar idea to the one used in Section 4. We recall that using a higher order threshold implementation of a cryptographic function is usually not enough, as one need to implement the entire cryptographic scheme by taking into account the same level of security. For this reason, we do not present real-world applications of the main result of this section.

As in Section 4, we want $|\mathbb{X}|$ to be divisible by $|\mathbb{Y}|$ and $s \geq t$. By Proposition 5, the minimum value for s is equal to 5 but then $t \geq \binom{5}{2} = 10$. If we take $s = 6$, then by [Pet19, Theorem 2.15] we have that $t \geq 6$. Similarly to the construction in Section 4, the minimal number of shares is not suited for a general construction, but we are going to prove that if we take $s \geq 7$ and $t = 7$ then a general construction is possible. In this section, we are going to prove the following theorem.

Theorem 2. *Let $\mathbb{X}$ and $\mathbb{Y}$ be finite Abelian groups such that $|\mathbb{X}|$ is divisible by $|\mathbb{Y}|$. Let $F \colon \mathbb{X} \to \mathbb{Y}$ be a quadratic balanced function. Let s be a positive integer such that $s \geq 7$. Then the function $\mathcal{F} \colon \mathbb{X}^s \to \mathbb{Y}^7$ defined by $\mathcal{F}(\underline{x})$ equal to*

$$\begin{pmatrix} F(x_1) \\ F\left(x_1 + x_5 + x_6 + \sum_{i\in[7,s]} x_i\right) \\ F\left(x_2 + x_3 + x_6 + \sum_{i\in[7,s]} x_i\right) \\ F(x_2 + x_4 + x_5) \\ F(x_1 + x_3) + F(x_1 + x_2) - 4F(x_1) - 2F(x_2) \\ F\left(\sum_{i\in[7,s]} x_i\right) + F(x_1 + x_4) + F\left(x_4 + x_6 + \sum_{i\in[7,s]} x_i\right) - 3F(x_4) - 2F\left(x_6 + \sum_{i\in[7,s]} x_i\right) \\ F(x_3 + x_4) + F(x_3 + x_5) + 7F(0) - 3F(x_3) - 2F(x_5) - F\left(\sum_{i\in[7,s]} x_i\right) \end{pmatrix}$$

is a second order Threshold Implementation of F that is also an F-implementation.

Lemma 5. *The set $S = \{\{1,5,6\},\{2,3,6\},\{2,4,5\},\{1,2,3\},\{1,4,6\},\{3,4,5\}\}$ satisfies the properties described in Proposition 5 with $(s,t,d,k) = (6,6,2,2)$.*

Lemma 6. *Let $F \colon \mathbb{X} \to \mathbb{Y}$ be quadratic. Let $S_3 = \{\{1,5,6\},\{2,3,6\},\{2,4,5\}\}$, let $S_2 = \{\{3,4\},\{3,5\},\{1,3\},\{1,2\},\{1,4\},\{4,6\}\}$ and let $z_1, \ldots, z_6 \in \mathbb{X}$. Then $F\left(\sum_{i=1}^{6} z_i\right)$ is equal to*

$$\sum_{I\in S_3} F\left(\sum_{i\in I} z_i\right) + \sum_{I\in S_2} F\left(\sum_{i\in I} z_i\right) + 7F(0) - 3\sum_{i\in\{1,3,4\}} F(z_i) - 2\sum_{i\in\{2,5,6\}} F(z_i). \quad (4)$$

Proof. By using Proposition 3 with $(s,d)=(6,2)$ we have that

$$F\left(\sum_{i=1}^{6} z_i\right) = \sum_{I\in\mathcal{P}_{6,2}} F\left(\sum_{i\in I} z_i\right) - 4\sum_{i\in[6]} F(z_i) + 10F(0) \tag{5}$$

because $\mu_{6,2}(2)=\binom{3}{0}(-1)^0=1$, $\mu_{6,2}(1)=\binom{4}{1}(-1)^1=-4$ and $\mu_{6,2}(0)=\binom{5}{2}(-1)^2=10$. If we take the expression in (4) and we apply Proposition 3 with $(s,d)=(3,2)$ on $F\left(\sum_{i\in I} z_i\right)$ with $I\in S_3$, then we obtain

$$F\left(\sum_{i\in I} z_i\right) = \sum_{J\subseteq I,\,|J|=2} F\left(\sum_{i\in J} z_i\right) - \sum_{i\in I} F(z_i) + F(0)$$

because $\mu_{3,2}(j)=\binom{2-j}{2-j}(-1)^{2-j}=(-1)^j$. Since $\{J\subseteq I \mid I\in S_3,\ |J|=2\}\cup S_2=\mathcal{P}_{6,2}$, we have that (4) turns into

$$\begin{aligned}&\sum_{I\in\mathcal{P}_{6,2}} F\left(\sum_{i\in I} z_i\right) + 10F(0) - 3\sum_{i\in\{1,3,4\}} F(z_i) - 2\sum_{i\in\{2,5,6\}} F(z_i) + \\ &- \sum_{i\in\{1,5,6\}} F(z_i) - \sum_{i\in\{2,3,6\}} F(z_i) - \sum_{i\in\{2,4,5\}} F(z_i)\end{aligned}$$

that is equal to the right side of (5). This concludes the proof. □

Proof of Theorem 2. The function $\mathcal{F}$ is second order non-complete by Lemma 5. Indeed, since $S=\{\{1,5,6\},\{2,3,6\},\{2,4,5\},\{1,2,3\},\{1,4,6\},\{3,4,5\}\}$ defines a second order non-complete function, then the same holds for the set $\mathrm{S}^{\mathrm{nc}}_{s,2,2}=\{J\cup[7,s]\colon J\in S\}$. We prove that $\mathcal{F}$ is correct by using Lemma 6. Indeed, the sum $\sum_{j\in[7]}\mathcal{F}_j(\underline{x})$ is equal to (4) by setting $z_i=x_i$ for $i\in[5]$ and $z_6=x_6+\sum_{i\in[7,s]}x_i$. To conclude, let us prove the uniformity of $\mathcal{F}$. Let $x\in\mathbb{X}$ and $\underline{y}\in\mathrm{Sh}_7(F(x))$. Consider the system

$$\begin{cases}\mathcal{F}_1(\underline{x})=y_1\\ \vdots\\ \mathcal{F}_7(\underline{x})=y_7\\ \sum_{i\in[s]}x_i=x\end{cases}. \tag{6}$$

in the variable $\underline{x}\in\mathbb{X}^s$. Observe that the number of solutions of system (6) is equal to $|\mathrm{Sh}_7(x)\cap(\mathcal{F})^{-1}(\underline{y})|$. So if we prove that system (2) has exactly $|\mathbb{X}|^{s-1}/|\mathbb{Y}|^{7-1}=|\mathbb{X}|^{s-7}(|\mathbb{X}|/|\mathbb{Y}|)^6$ solutions, then we have that $\mathcal{F}$ is uniform.

Similarly to the proof of Proposition 6, we can turn the seventh equation of system (6) into $\sum_{j\in[7]}y_j=F(x)$. Let us rewrite the eight equation of system (6) into $\sum_{i\in[7]}x_i=x-\sum_{i\in[8,s]}x_i$. Let us fix $\bar{x}_8,\dots,\bar{x}_s\in\mathbb{X}$. We claim that there are exactly $(|\mathbb{X}|/|\mathbb{Y}|)^6$ choices of $(\bar{x}_1,\dots,\bar{x}_7)\in\mathbb{X}^7$ such that $(\bar{x}_1,\dots,\bar{x}_s)$ is a solution of system (6). This will be enough to conclude the proof.

Let $\underline{X}=(X_1,\dots,X_7)\in\mathbb{X}^7$ be such that $X_1=x_1$, $X_2=x_1+x_5+x_6+x_7$, $X_3=x_2+x_3+x_6+x_7$, $X_4=x_2+x_4+x_5$, $X_5=x_1+x_3$, $X_6=x_7$, $X_7=x_6$. It follows that the linear transformation that maps $(x_1,\dots,x_7)$ into $(X_1,\dots,X_7)$ is bijective and that $x_1=X_1$, $x_2=X_1+X_3-X_5-X_6-X_7$, $x_3=-X_1+X_5$, $x_4=-X_2-X_3+X_4+X_5+2X_6+2X_7$, $x_5=-X_1+X_2-X_6-X_7$, $x_6=X_7$, $x_7=X_6$. Observe that the eighth equation of system (6) turns into $X_4+X_5+X_6+X_7=x$. We claim that for $j\in[6]$ we have that $y_j=F(X_j)+\mathcal{G}_j(X_1,\dots,X_{j-1},x)$ where $\mathcal{G}_j\colon\mathbb{X}^j\to\mathbb{Y}$ is some function. Similarly to the proof of Proposition 6, such claim is enough to prove that system (6) where $x_8,\dots,x_s$ are fixed, has $(|\mathbb{X}|/|\mathbb{Y}|)^6$ solutions. The claim is true for $j \in [4]$ since we have that $y_j = F(X_j)$. Since

$$x_2 = X_1 + X_3 - X_5 - X_6 - X_7 = X_1 + X_3 + X_4 - x,$$

the fifth equation of (6) turns into $F(X_5)+\mathcal{G}_5(X_1, X_2, X_3, X_4, x)$. Since $x_6+x_7 = X_6+X_7 = x - X_4 - X_5$ and

$$x_4 = -X_2 - X_3 + X_4 + X_5 + 2X_6 + 2X_7 = -X_2 - X_3 - X_4 - X_5 + 2x,$$

the sixth equation of (6) turns into $F(X_6) + \mathcal{G}_6(X_1, X_2, X_3, X_4, X_5, x)$. □

6 On the conversion between additive sharings in $\mathbb{F}_p^n$ and $\mathbb{Z}_{p^n}$

Let p be a prime and n be a positive integer. In this section, we construct procedures to convert from an additive sharing over $\mathbb{F}_p^n$ to an additive sharing over $\mathbb{Z}_{p^n}$ and vice versa by studying the functional degree of the conversion maps between $\mathbb{F}_p^n$ and $\mathbb{Z}_{p^n}$. These procedures need $s \geq (n-1)(p-1)+3$ shares, cost $\mathcal{O}(n^2 2^n)$ elementary operations (with the assumption $p << n$ and $s = \mathcal{O}(n)$), do not need extra randomness, need 1 clock cycle for the conversion $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^n}$ and $\lceil n - \log_p((n-1)(p-1)+1) \rceil$ clock cycles for the conversion $\mathbb{Z}_{p^n}$ to $\mathbb{F}_p^n$. We must say that there exists several techniques [CGV14, CGTV15, SPOG19, SH24] for this type of conversion and each uses at minimum 2 shares, but they all need extra randomness while our procedure does not need any. It could be argued that to compare those techniques with ours, one need to generate extra shares and use randomness for that. However, in some cases, that generation process can be done in preprocessing. Indeed, let $(X_1, X_2) \in \mathrm{Sh}_2(x)$ for some $x \in \mathbb{X}$ ($\mathbb{X}$ being either $\mathbb{F}_p^n$ or $\mathbb{Z}_{p^n}$) one can take $\underline{x} = (x_1, \ldots, x_s) \in \mathrm{Sh}_s(0)$ and then $(x_1 + X_1, x_2 + X_2, x_3, \ldots, x_s)$ is in $\mathrm{Sh}_s(x)$. Another aspect is the number of clock cycles. In this case, we need to look at the state of the art regarding real-world implementation [SPOG19, BC22, NDKV24, SH24]. We conclude that our algorithm is very competitive, as there are many implementations that require way more clock cycles than ours. The only tradeoff of our algorithm is the operation count that is exponential in n, while most known procedures are at most polynomial in n. So, in its current state, the scope is limited to low values of n.

Remark 5. Let p be odd. We show that using the representation in $\mathbb{A}_p = \{0, \ldots, p-1\}$ or in $\mathbb{B}_p = \{-(p-1)/2, \ldots, (p-1)/2\}$ does not change the functional degree of the conversion maps. Let $x_{(1)}, \ldots, x_{(n)} \in \mathbb{B}_p$ and let $\bar{x}_{(j)} = x_{(j)} + \frac{p-1}{2} \in \mathbb{A}_p$ for all $j \in [n]$. Then $\sum_{i\in[n]} \bar{x}_{(i)} p^{i-1} = \sum_{i\in[n]} x_{(i)} p^{i-1} + \frac{p^n-1}{2}$. So if F is the conversion map from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^n}$ that uses the representation in $\mathbb{A}_p$, then $G(x_{(1)}, \ldots, x_{(n)}) = F\left(x_{(1)} + \frac{p-1}{2}, \ldots, x_{(n)} + \frac{p-1}{2}\right) - \frac{p^n-1}{2}$ is the conversion map from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^n}$ that uses the representation in $\mathbb{B}_p$. Therefore, we have that $\mathrm{d}^\circ(F) = \mathrm{d}^\circ(G)$ and $\mathrm{d}^\circ(F^{-1}) = \mathrm{d}^\circ(G^{-1})$.

We show that by using Lucas' Theorem, we can compute the functional degree of the conversion map from $\mathbb{Z}_{p^n}$ to $\mathbb{F}_p^n$.

Proposition 7. *Let p be a prime number and let $x \in \mathbb{Z}$. Let $x_{(1)}, \ldots, x_{(n)} \in \{0, \ldots, p-1\}$ be such that $x = \sum_{i\in[n]} x_{(i)} p^{i-1} \pmod{p^n}$. Then, for any $j \in [n]$, we have that*

$$\binom{x}{p^{j-1}} = x_{(j)} \pmod{p}.$$

Proof. If $x < 0$, then $x = \sum_{i\in[n]} x_{(i)} p^{i-1} - mp^n$ where $m > 0$. If $j = 1$, then $\binom{x}{1} = x = x_{(1)} \pmod{p}$. Assume $j > 1$. Observe that

$$\binom{x}{p^{j-1}} = (-1)^{p^{j-1}} \binom{-x + p^{j-1} - 1}{p^{j-1}} = -\binom{-x + p^{j-1} - 1}{p^{j-1}} \pmod{p}$$

because $(-1)^{p^{j-1}} = -1 \pmod p$ since $j > 1$. Then $-x+p^{j-1}-1 = \left(mp^n - \sum_{i\in[j,n]} x_{(i)}p^{i-1}\right)+ \left(p^{j-1} - \sum_{i\in[j-1]} x_{(i)}p^{i-1} - 1\right)$. Since $0 \leq \left(p^{j-1} - \sum_{i\in[j-1]} x_{(i)}p^{i-1} - 1\right) < p^{j-1}$ and $\left(mp^n - \sum_{i\in[j,n]} x_{(i)}p^{i-1}\right) \geq p^{j-1}$, then by Lucas' Theorem we have that

$$\begin{aligned}\binom{x}{p^{j-1}} &= -\binom{-x+p^{j-1}-1}{p^{j-1}} = -\binom{mp^n - \sum_{i\in[j,n]} x_{(i)}p^{i-1}}{p^{j-1}} \pmod p\\ &= -\left(mp^{n-j+1} - \sum_{i\in[j,n]} x_{(i)}p^{i-j}\right) = x_{(j)} \pmod p.\end{aligned}$$

□

A direct consequence of Proposition 7 is that the functional degree of the conversion map from $\mathbb{Z}_{p^n}$ to $\mathbb{F}_p^n$ is equal to p^{n-1}. Indeed, its IV polynomial representation is given by $\sum_{i\in[n]} \binom{x}{p^{i-1}} e_i$ where $\{e_1, \dots, e_n\}$ is the canonical basis of $\mathbb{F}_p^n$. We will show that we can do better by decomposing this conversion map into functions of small degree.

We use the following notation. Let p be a prime number and let $F \colon \mathbb{Z}^m \to \mathbb{Z}$. We denote by $F^{(n)}$ the function from $\mathbb{Z}^m$ to $\mathbb{Z}_{p^n}$ defined by $F^{(n)}(x) = F(x) + p^n\mathbb{Z}$ and we set $F_{\underline{d}} = \partial^{(\underline{d})}F(0)$ for any $\underline{d} \in \mathbb{N}^m$. We prove the following lemma that will be useful for the rest of the section.

Lemma 7. *Let p be a prime number and let $F \colon \mathbb{Z}^m \to \mathbb{Z}$. Then for any positive integers n, k such that $k \leq n$, we have that $\mathrm{d}^\circ(p^k F^{(n)}) = \mathrm{d}^\circ(F^{(n-k)})$.*

Proof. Let $\underline{d} \in \mathbb{N}^m$ then we have that that $p^k\partial^{(\underline{d})}F^{(n)} = 0$ if and only if $p^k\partial^{(\underline{d})}F = 0 \pmod{p^n}$ if and only if $\partial^{(\underline{d})}F = 0 \pmod{p^{n-k}}$ if and only if $\partial^{(\underline{d})}F^{(n-k)} = 0$. This is enough to conclude the proof. □

Let $\chi \colon \mathbb{Z} \to \mathbb{Z}$ be the function defined by $\chi(x) = 1$ if $x = 0 \pmod p$ and $\chi(x) = 0$ otherwise. Let $\alpha \colon \mathbb{Z} \to \mathbb{Z}$ be such that $\alpha(x) = x \pmod p$ and that the image of α is equal to $\{0, \dots, p-1\}$.

Lemma 8. *Let p be a prime number and n a positive integer. Then we have that $\mathrm{d}^\circ(\chi^{(n)}) = n(p-1)$.*

Proof. Since $\chi^{(n)}$ is the pullback of the function that maps $x + p\mathbb{Z}$ to $1 + p^n\mathbb{Z}$ if $x = 0 \pmod p$ and to $0 + p^n\mathbb{Z}$ otherwise, then $\mathrm{d}^\circ(\chi^{(n)}) = n(p-1)$ by Proposition 1. □

Lemma 9. *Let p be a prime number and n be a positive integer. Then we have that $\mathrm{d}^\circ(\alpha^{(n)}) = (n-1)(p-1)+1$ and we have the following:*

1. *$\alpha_0 = 0$, $\alpha_1 = 1$ and $\alpha_d = -p\Delta^{(d-1)}\chi(1)$ for all $d \geq 2$.*
2. *In particular, if $p = 2$ we have that $\alpha_d = (-1)^{d-1}2^{d-1}$ for all $d \geq 1$.*

Proof. Observe that $\mathrm{d}^\circ(\alpha^{(1)}) = 1$. Suppose that $n > 1$. Observe that $\Delta\alpha(x) = 1-p$ if $x = p-1 \pmod p$ and $\Delta\alpha(x) = 1$ otherwise. So we have that $\Delta\alpha(x) = 1 - p\chi(x+1)$. So for any $d \in \mathbb{N}$ with $d \geq 2$ we have that $\Delta^{(d)}\alpha(x) = -p\Delta^{(d-1)}\chi(x+1)$. By Lemma 7, we have $\mathrm{d}^\circ(p\chi^{(n)}) = \mathrm{d}^\circ(\chi^{(n-1)})$. So we have that $\mathrm{d}^\circ(\alpha^{(n)}) = \mathrm{d}^\circ(\chi^{(n-1)}) + 1$ and $\mathrm{d}^\circ(\alpha^{(n)}) = (n-1)(p-1)+1$ by Lemma 8.

Suppose that $p = 2$, then $\alpha(x) = \frac{1-(-1)^x}{2}$ for any $x \in \mathbb{Z}$. We claim that $\Delta^{(d)}\alpha(x) = 2^{d-1}(-1)^{x+d-1}$. For $d = 1$, we have that $\Delta\alpha(x) = \frac{1-(-1)^{x+1}}{2} - \frac{1-(-1)^x}{2} = (-1)^x$. Suppose the claim is true for $d \geq 1$ and let us prove it for $d+1$. We have that

$$\Delta^{(d+1)}\alpha(x) = \Delta\Delta^{(d)}\alpha(x) = 2^{d-1}\left((-1)^{x+d} - (-1)^{x+d-1}\right) = 2^d(-1)^{x+d}.$$

This concludes the proof because $\alpha_d = \Delta^{(d)}\alpha(0) = 2^{d-1}(-1)^{d-1}$. □

6.1 Conversion from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^n}$

Let $\sigma\colon \mathbb{Z}^n \to \mathbb{Z}$ be defined by $\sigma(x_{(1)},\dots,x_{(n)}) = \sum_{i\in[n]} \alpha(x_{(i)})p^{i-1}$. Then $\sigma^{(n)}$ is the pullback of the conversion map from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^n}$. We claim that $\mathrm{d}^\circ(\sigma^{(n)}) = (n-1)(p-1)+1$. We observe that if $i,j \in [n]$ are such that $i \neq j$, then we have that $\partial^i\partial^j\sigma = 0$. So for any $i \in [n]$, we have that $\partial^{i,(d_i)}\sigma^{(n)}(0,\dots,0) = p^{i-1}\Delta^{(d_i)}\alpha^{(n)}(0)$ and therefore $\mathrm{d}_i^\circ(\sigma^{(n)}) = \mathrm{d}^\circ(p^{i-1}\alpha^{(n)})$. By Lemma 7, we have $\mathrm{d}^\circ(p^{i-1}\alpha^{(n)}) = \mathrm{d}^\circ(\alpha^{(n-i+1)})$ and so we have that $\mathrm{d}_i^\circ(\sigma^{(n)}) = \mathrm{d}^\circ(\alpha^{(n-i+1)})$. By Lemma 9, we have that $\mathrm{d}_i^\circ(\sigma^{(n)}) = (n-i)(p-1)+1$ for any $i \in [n]$ and therefore $\mathrm{d}^\circ(\sigma^{(n)}) = (n-1)(p-1)+1$.

Let $s \geq (n-1)(p-1)+3$ and let $x_1,\dots,x_s \in \{0,\dots,p-1\}^n$. Let $\oplus^n$ be the addition over $\mathbb{F}_p^n$ and let $\boxplus^n$ be the addition over $\mathbb{Z}_{p^n}$. We want to use the threshold implementation defined in Appendix B.1 to get $y_1,\dots,y_s \in \{0,\dots,p-1\}^n$ such that $\bigoplus^n_{i\in[s]} x_i = \boxplus^n_{j\in[s]} y_j$. See Appendix C for the explicit construction. By using the estimates in Remark 4 and the fact that each addition either in $\mathbb{F}_p^n$ or in $\mathbb{Z}_{p^n}$ costs $\mathcal{O}(n)$ elementary operations, we have that the total cost is $\mathcal{O}(n^2 2^n)$ if $p << n$ and $s = \mathcal{O}(n)$.

6.2 Conversion from $\mathbb{Z}_{p^n}$ to $\mathbb{F}_p^n$

We now have the tools to define a conversion from $\mathbb{Z}_{p^n}$ to $\mathbb{F}_p^n$ by decomposing it into functions of smaller degree. We consider the conversion map from $\mathbb{Z}_{p^n}$ to $\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}$, then the one from $\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}$ to $\mathbb{Z}_p^2 \times \mathbb{Z}_{p^{n-2}}$ and so on until we get the conversion to $\mathbb{Z}_p^n = \mathbb{F}_p^n$. We must say that this technique is similar to the one described in the paper by Geelen et al.[GIKV23] even though their scope is very different from us. Indeed, digit extraction is an important step in the bootstrapping for Homomorphic Encryption [HS15, CH18, GV23]. In [GIKV23], they approach this problem by using *polyfunctions* which are polynomials in $\mathbb{Z}_{p^n}[x]$ represented using the factorial basis $\{x(x-1)\cdots(x-d+1)\}_{d\in\mathbb{N}}$. This representation is closely related to the IV polynomial representation since $\binom{x}{d} = \frac{x(x-1)\cdots(x-d+1)}{d!}$. We must remark that using the IV polynomial representation instead of the polyfunction representation has the advantage of determining the exact functional degree of a function by its representation. Indeed, [GIKV23, Corollary 3] is a direct consequence of the theory developed by Clark et al. in [CS22].

Let $\eta\colon \mathbb{Z} \to \mathbb{Z}$ be defined by $\eta(x) = \frac{x-\alpha(x)}{p}$. We claim that $\mathrm{d}^\circ(\eta^{(n)}) = \mathrm{d}^\circ(\alpha^{(n+1)}) = n(p-1)+1$. By Lemma 9, we have that $\Delta\eta(0) = \frac{1-\Delta\alpha(0)}{p} = 0$ and that $\Delta^{(d)}\eta(0) = -\Delta^{(d)}\alpha(0)/p$ for all $d \geq 2$. Therefore, we have that $\mathrm{d}^\circ(p\eta^{(n+1)}) = \mathrm{d}^\circ(\alpha^{(n+1)})$ and we can conclude by Lemma 7. Moreover, we have that the function from $\mathbb{Z}_{p^n}$ to $\mathbb{Z}_{p^{n-1}}$ that maps $x + p^n\mathbb{Z}$ to $\eta^{(n-1)}(x)$ is balanced. Indeed, for any $y \in \mathbb{Z}$ we can choose $x = py + z$ where z is any element in $\{0,\dots,p-1\}$.

We can use η to define a procedure that takes an integer $x \in \mathbb{Z}$ and extract $x_{(1)},\dots,x_{(n)} \in \{0,\dots,p-1\}$ such that $x = \sum_{i\in[n]} x_{(i)}p^{i-1} \pmod{p^n}$. Let η^j be the application j times of the function η. Let us consider the map from $\mathbb{Z}_{p^n}$ to $\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}$ with $n \geq 2$ defined by

$$x + p^n\mathbb{Z} \mapsto (x + p\mathbb{Z}, \eta(x) + p^{n-1}\mathbb{Z}) = (x + p\mathbb{Z}, \eta^{(n-1)}(x)).$$

Then we have that

$$\begin{aligned} x + p^n\mathbb{Z} &\mapsto \left(x_{(1)} + p\mathbb{Z}, \eta^{(n-1)}(x)\right) \\ &\mapsto \left(x_{(1)} + p\mathbb{Z}, x_{(2)} + p\mathbb{Z}, \eta^{(n-2)}(\eta(x))\right) \mapsto \cdots \\ \cdots &\mapsto \left(x_{(1)} + p\mathbb{Z}, \dots, x_{(n-1)} + p\mathbb{Z}, \eta^{(1)}\left(\eta^{n-1}(x)\right)\right) \\ &= \left(x_{(1)} + p\mathbb{Z}, \dots, x_{(n-1)} + p\mathbb{Z}, x_{(n)} + p\mathbb{Z}\right). \end{aligned}$$

There are $n-1$ steps in this procedure, and each step k involves a function of degree $\mathrm{d}^\circ(\eta^{(n-k)}) = (n-k)(p-1)+1$ for $k = 1, \dots, n-1$. However, we can make it shorter depending on the value of p. Observe that if after the first $k-1$ steps we have that $(n-1)(p-1)+1 \geq p^{n-k}$ (that is when $k = \lceil n - \log_p\left((n-1)(p-1)+1\right)\rceil$), then we can conclude the conversion by mapping $\eta^{k-1}(x) + p^{n-k+1}\mathbb{Z}$ to

$$\left(\binom{\eta^{k-1}(x)}{1} + p\mathbb{Z}, \dots, \binom{\eta^{k-1}(x)}{p^{n-k}} + p\mathbb{Z}\right) = \left(x_{(k)} + p\mathbb{Z}, \dots, x_{(n)} + p\mathbb{Z}\right).$$

Let $s \geq (n-1)(p-1)+3$ and let $x_1, \dots, x_s \in \{0, \dots, p-1\}^n$. Let $\oplus^n$ be the addition over $\mathbb{F}_p^n$ and let $\boxplus^n$ be the addition over $\mathbb{Z}_{p^n}$. We want to use the threshold implementation defined in Appendix B.1 to get $y_1, \dots, y_s \in \{0, \dots, p-1\}^n$ such that $\mathop{\boxplus^n}_{i\in[s]} x_i = \mathop{\bigoplus^n}_{j\in[s]} y_j$. We use a combination of the threshold implementation in Appendix E and in Appendix D. By using the estimates in Remark 4 and the fact that each addition either in $\mathbb{F}_p^n$ or in $\mathbb{Z}_{p^n}$ costs $\mathcal{O}(n)$ elementary operations, we have that the total cost is $\mathcal{O}(n^2 2^n)$ if $p << n$ and $s = \mathcal{O}(n)$.

7 Conclusion

In this work, we extended the threshold implementation technique to cryptographic functions defined over finite Abelian groups, demonstrating that many classical properties remain valid in this broader setting. This generalization significantly expands the applicability of threshold implementations beyond vectorial Boolean functions, enabling their use in diverse cryptographic scenarios, particularly those involving arithmetic and prime-field sharing. We proved that functions with functional degree d admit a threshold implementation with $s \geq d+2$ shares, thereby generalizing and improving the results presented in [PAB+23]. Furthermore, we extended these findings to second-order threshold implementations by proposing a general construction for quadratic balanced functions. Additionally, we provided novel constructions with practical relevance, including a threshold implementation for any multiplication map with four shares and first-order secure conversion algorithms between additive sharings over $\mathbb{F}_p^n$ and $\mathbb{Z}_{p^n}$.

There are many open problems that are left unsolved such as addressing the case of threshold implementation with $d+1$ shares, doing more general constructions for higher order implementation and improving the operation count of the conversion algorithms. For the latter, one could reduce the operation count to $\mathcal{O}(n)$ by finding decompositions into low degree functions (ideally quadratic or cubic) of the conversion maps.

Acknowledgements We thank Samuele Andreoli, Lilya Budaghyan, Claude Carlet, Siemen Dhooghe, Svetla Nikova and Quinten Norga for useful discussions. The research of this paper is supported by the Norwegian Research Council.

References

[AM21] Erhard Aichinger and Jakob Moosbauer. Chevalley-warning type results on abelian groups. *Journal of Algebra*, 569:30–66, 2021.

[APB+23] Samuele Andreoli, Enrico Piccione, Lilya Budaghyan, Pantelimon Stănică, and Svetla Nikova. On decompositions of permutations in quadratic functions. *Cryptology ePrint Archive*, 2023.

[Bar86] Paul Barrett. Implementing the rivest shamir and adleman public key encryption algorithm on a standard digital signal processor. In *Conference* *on the Theory and Application of Cryptographic Techniques*, pages 311–323. Springer, 1986.

[BBS17] Dusan Bozilov, Begül Bilgin, and Haci Ali Sahin. A note on 5-bit quadratic permutations' classification. *IACR Trans. Symmetric Cryptol.*, 2017(1):398–404, 2017.

[BC22] Olivier Bronchain and Gaëtan Cassiers. Bitslicing arithmetic/boolean masking conversions for fun and profit with application to lattice-based kems. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2022(4):553–588, 2022.

[BGN$^+$15] Begül Bilgin, Benedikt Gierlichs, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. Trade-offs for threshold implementations illustrated on AES. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 34(7):1188–1200, 2015.

[BNN$^+$12] Begül Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen, and Georg Stütz. Threshold implementations of all 3 ×3 and 4 ×4 s-boxes. In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *Lecture Notes in Computer Science*, pages 76–91. Springer, 2012.

[Bou22] Chad Boutin. Nist announces first four quantum-resistant cryptographic algorithms. *National Institute of Standards and Technology*, 2022.

[CC97] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*, volume 48. American Mathematical Soc., 1997.

[CGGI20] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Tfhe: fast fully homomorphic encryption over the torus. *Journal of Cryptology*, 33(1):34–91, 2020.

[CGTV15] Jean-Sébastien Coron, Johann Großschädl, Mehdi Tibouchi, and Praveen Kumar Vadnala. Conversion from arithmetic to boolean masking with logarithmic complexity. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 130–149. Springer, 2015.

[CGV14] Jean-Sébastien Coron, Johann Großschädl, and Praveen Kumar Vadnala. Secure conversion between boolean and arithmetic masking of any order. In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, volume 8731 of *Lecture Notes in Computer Science*, pages 188–205. Springer, 2014.

[CH18] Hao Chen and Kyoohyung Han. Homomorphic lower digits removal and improved FHE bootstrapping. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 315–337. Springer, 2018.

[CHMS22] Orel Cosseron, Clément Hoffmann, Pierrick Méaux, and François-Xavier Standaert. Towards case-optimized hybrid homomorphic encryption: Featuring the elisabeth stream cipher. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 32–67. Springer, 2022.

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer, 1999.

[CMM$^+$23] Gaëtan Cassiers, Loïc Masure, Charles Momin, Thorben Moos, and François-Xavier Standaert. Prime-field masking in hardware and its soundness against low-noise sca attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 482–518, 2023.

[CPRR15] Claude Carlet, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche. Algebraic decomposition for probing security. In *CRYPTO (1)*, volume 9215 of *Lecture Notes in Computer Science*, pages 742–763. Springer, 2015.

[CS22] Pete L Clark and Uwe Schauz. Functional degrees and arithmetic applications i: The set of functional degrees. *Journal of Algebra*, 608:691–718, 2022.

[CS23] Pete L Clark and Uwe Schauz. Functional degrees and arithmetic applications ii: The group-theoretic prime ax-katz theorem. *arXiv preprint arXiv:2305.01304*, 2023.

[DGGK21] Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters. Ciminion: symmetric encryption based on toffoli-gates over large finite fields. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 3–34. Springer, 2021.

[DNR19] Siemen Dhooghe, Svetla Nikova, and Vincent Rijmen. Threshold implementations in the robust probing model. In Begül Bilgin, Svetla Petkova-Nikova, and Vincent Rijmen, editors, *Proceedings of ACM Workshop on Theory of Implementation Security, TIS@CCS 2019, London, UK, November 11, 2019*, pages 30–37. ACM, 2019.

[GIKV23] Robin Geelen, Ilia Iliashenko, Jiayi Kang, and Frederik Vercauteren. On polynomial functions modulo pe and faster bootstrapping for homomorphic encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 257–286. Springer, 2023.

[GMAH$^+$23] Lorenzo Grassi, Irati Manterola Ayala, Martha Norberg Hovd, Morten Øygarden, Håvard Raddum, and Qingju Wang. Cryptanalysis of symmetric primitives over rings and a key recovery attack on rubato. In *Annual International Cryptology Conference*, pages 305–339. Springer, 2023.

[Gou01] Louis Goubin. A sound method for switching between boolean and arithmetic masking. In *Cryptographic Hardware and Embedded Systems—CHES 2001: Third International Workshop Paris, France, May 14–16, 2001 Proceedings 3*, pages 3–15. Springer, 2001.

[GP99] Louis Goubin and Jacques Patarin. DES and differential power analysis (the "duplication" method). In Çetin Kaya Koç and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*, volume 1717 of *Lecture Notes in Computer Science*, pages 158–172. Springer, 1999.

[GV23] Robin Geelen and Frederik Vercauteren. Bootstrapping for bgv and bfv revisited. *Journal of Cryptology*, 36(2):12, 2023.

[HS15] Shai Halevi and Victor Shoup. Bootstrapping for helib. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 641–670. Springer, 2015.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology - CRYPTO '99 Proceedings*, pages 388–397, 1999.

[Lac04] Miklós Laczkovich. Polynomial mappings on abelian groups. *aequationes mathematicae*, 68:177–199, 2004.

[LSaa24] Florian Luca, Santanu Sarkar, and Pantelimon Stănică. Representing the inverse map as a composition of quadratics in a finite field of characteristic 2. *Cryptogr. Commun.*, 2024.

[MPO05] Stefan Mangard, Norbert Pramstaller, and Elisabeth Oswald. Successfully attacking masked AES hardware implementations. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*, volume 3659 of *Lecture Notes in Computer Science*, pages 157–171. Springer, 2005.

[NDKV24] Quinten Norga, Jan-Pieter D'Anvers, Suparna Kundu, and Ingrid Verbauwhede. Mask conversions for d+ 1 shares in hardware, with application to lattice-based pqc. *Cryptology ePrint Archive*, 2024.

[NNR19] Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. Decomposition of permutations in a finite field. *Cryptogr. Commun.*, 11(3):379–384, 2019.

[NRR06] Svetla Nikova, Christian Rechberger, and Vincent Rijmen. Threshold implementations against side-channel attacks and glitches. In Peng Ning, Sihan Qing, and Ninghui Li, editors, *Information and Communications Security, 8th International Conference, ICICS 2006, Raleigh, NC, USA, December 4-7, 2006, Proceedings*, volume 4307 of *Lecture Notes in Computer Science*, pages 529–545. Springer, 2006.

[PAB$^+$23] Enrico Piccione, Samuele Andreoli, Lilya Budaghyan, Claude Carlet, Siemen Dhooghe, Svetla Nikova, George Petrides, and Vincent Rijmen. An optimal universal construction for the threshold implementation of bijective s-boxes. *IEEE Trans. Inf. Theory*, 69(10):6700–6710, 2023.

[Pet19] George Petrides. On non-completeness in threshold implementations. In Begül Bilgin, Svetla Petkova-Nikova, and Vincent Rijmen, editors, *Proceedings of ACM Workshop on Theory of Implementation Security, TIS@CCS 2019, London, UK, November 11, 2019*, pages 24–28. ACM, 2019.

[Pet23] George Petrides. On decompositions of permutation polynomials into quadratic and cubic power permutations. *Cryptogr. Commun.*, 15(1):199–207, 2023.

[Sch14] Uwe Schauz. Classification of polynomial mappings between commutative groups. *Journal of Number Theory*, 139:1–28, 2014.

[SH24] Aein Rezaei Shahmirzadi and Michael Hutter. Efficient boolean-to-arithmetic mask conversion in hardware. *Cryptology ePrint Archive*, 2024.

[SPOG19] Tobias Schneider, Clara Paglialonga, Tobias Oder, and Tim Güneysu. Efficiently masking binomial sampling at arbitrary orders for lattice-based crypto. In Dongdai Lin and Kazue Sako, editors, *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part II*, volume 11443 of *Lecture Notes in Computer Science*, pages 534–564. Springer, 2019.

A Complementary content for Subsection 3.1

We show an example for the case F unbalanced and $\mathcal{F}$ both uniform and unbalanced. Let $F\colon \mathbb{Z}_4 \to \mathbb{Z}_2$ defined by $F(0) = 0$, $F(1) = 0$, $F(2) = 0$, and $F(3) = 1$. Let $\mathcal{F}\colon \mathbb{Z}_4^2 \to \mathbb{Z}_2^2$ be defined as follows:

$$\begin{aligned}
&\mathcal{F}(\underline{x}) = (0,0),\ \underline{x} \in \{(0,0),(0,1),(0,2),(1,3),(1,0),(1,1)\},\\
&\mathcal{F}(\underline{x}) = (1,1),\ \underline{x} \in \{(2,2),(2,3),(2,0),(3,1),(3,2),(3,3)\},\\
&\mathcal{F}(\underline{x}) = (1,0),\ \underline{x} \in \{(0,3),(1,2)\},\\
&\mathcal{F}(\underline{x}) = (0,1),\ \underline{x} \in \{(2,1),(3,0)\}.
\end{aligned}$$

By construction, we have that $\mathcal{F}$ is unbalanced and it is correct with respect to F. One can verify that $|\mathrm{Sh}_2(x) \cap \mathcal{F}^{-1}(\underline{y})| = 2 = \frac{|\mathbb{Z}_4|^{2-1}}{|\mathbb{Z}_2|^{2-1}}$ for all $x \in \mathbb{Z}_4$ and all $\underline{y} \in \mathrm{Sh}_2(F(x))$. So we have that $\mathcal{F}$ is uniform.

We show an example for the case F balanced and $\mathcal{F}$ both balanced and not uniform. Let $F\colon \mathbb{Z}_4 \to \mathbb{Z}_2$ defined by $F(0) = 0$, $F(1) = 0$, $F(2) = 1$, and $F(3) = 1$. Let $\mathcal{F}\colon \mathbb{Z}_4^2 \to \mathbb{Z}_2^2$ be defined as follows:

$$\begin{aligned}
&\mathcal{F}(\underline{x}) = (0,0),\ \underline{x} \in \{(0,0),(1,0),(2,3),(3,2)\},\\
&\mathcal{F}(\underline{x}) = (1,1),\ \underline{x} \in \{(0,1),(1,3),(2,2),(3,1)\},\\
&\mathcal{F}(\underline{x}) = (1,0),\ \underline{x} \in \{(0,2),(1,2),(2,1),(3,0)\},\\
&\mathcal{F}(\underline{x}) = (0,1),\ \underline{x} \in \{(0,3),(1,1),(2,0),(3,3)\}.
\end{aligned}$$

By construction, we have that $\mathcal{F}$ is correct with respect to F and $\mathcal{F}$ is balanced. However, $\mathcal{F}$ is not uniform because $|\mathrm{Sh}_2(0) \cap \mathcal{F}^{-1}(0,0)| = 1 \neq \frac{|\mathbb{Z}_4|^{2-1}}{|\mathbb{Z}_2|^{2-1}} = 2$.

B An example from the general construction of threshold implementations with $d+2$ shares

$$
\begin{aligned}
\mathcal{F}_1(\underline{x}) =& (1-b_1)\cdot P_1\left(x_1\right) + b_1 \cdot P_1\left(\sum_{i\in[2,s]} x_i\right),\\
\mathcal{F}_j(\underline{x}) =& (1-b_j)\cdot P_j\left(x_j\right) + b_j \cdot P_j\left(\sum_{i\in[j+1,s]} x_i\right) + \sum_{I\in\mathcal{P}_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right)\\
& - b_{j-1}\cdot P_{j-1}\left(\sum_{i\in[j,s]} x_i\right) \quad j\in[2,d+1],\\
\mathcal{F}_{d+2}(\underline{x}) =& \sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} x_i\right) - \sum_{j\in[d+1]} (1-b_j)\cdot P_j\left(x_j\right) - b_{d+1}\cdot P_{d+1}\left(\sum_{i\in[d+2,s]} x_i\right).
\end{aligned}
$$

B.1 An example with F balanced

Assume $\mathrm{d}^\circ = \mathrm{d}^\circ(F) \geq 2$. We set P_k equal to $(-1)^{k-1}F$ if $k\in[\mathrm{d}^\circ]$ and equal to F if $k\in[\mathrm{d}^\circ, d+1]$. We set b_k equal to 1 if $k\in[\mathrm{d}^\circ]$ and equal to 0 if $k\in[\mathrm{d}^\circ, d+1]$.

B.1.1 $d = \mathrm{d}^\circ(F)$

$$
\begin{aligned}
\mathcal{F}_1(\underline{x}) =& F\left(\sum_{i\in[2,s]} x_i\right),\\
\mathcal{F}_j(\underline{x}) =& (-1)^{j-1} F\left(\sum_{i\in[j+1,s]} x_i\right) + \sum_{I\in\mathcal{P}^*_{j-2}} (-1)^{j-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right) \quad j\in[2,d],\\
\mathcal{F}_{d+1}(\underline{x}) =& F\left(x_{d+1}\right) + \sum_{I\in\mathcal{P}^*_{d-1}} (-1)^{d+1-|I|} F\left(\sum_{i\in I} x_i + \sum_{i\in[d+1,s]} x_i\right),\\
\mathcal{F}_{d+2}(\underline{x}) =& \sum_{I\in\mathcal{P}_d} (-1)^{d-|I|} F\left(\sum_{i\in I} x_i\right) - F\left(x_{d+1}\right).
\end{aligned}
$$

B.1.2 $d > \mathrm{d}^\circ(F)$

$$
\begin{aligned}
\mathcal{F}_1(\underline{x}) =& F\left(\sum_{i\in[2,s]} x_i\right), \\
\mathcal{F}_j(\underline{x}) =& (-1)^{j-1}F\left(\sum_{i\in[j+1,s]} x_i\right) + \sum_{I\in\mathcal{P}^*_{j-2}} (-1)^{j-|I|}F\left(\sum_{i\in I} x_i + \sum_{i\in[j,s]} x_i\right) \quad j\in[2,\mathrm{d}^\circ], \\
\mathcal{F}_{\mathrm{d}^\circ+1}(\underline{x}) =& F(x_{\mathrm{d}^\circ+1}) + \sum_{I\in\mathcal{P}^*_{\mathrm{d}^\circ-1}} (-1)^{\mathrm{d}^\circ+1-|I|}F\left(\sum_{i\in I} x_i + \sum_{i\in[\mathrm{d}^\circ+1,s]} x_i\right) \\
\mathcal{F}_{\mathrm{d}^\circ+2}(\underline{x}) =& F\left(x_{\mathrm{d}^\circ+2}\right) + \sum_{I\in\mathcal{P}_{\mathrm{d}^\circ}} (-1)^{\mathrm{d}^\circ-|I|}F\left(\sum_{i\in I} x_i\right), \\
\mathcal{F}_j(\underline{x}) =& F\left(x_j\right) \quad j\in[\mathrm{d}^\circ+3, d+1], \\
\mathcal{F}_{d+2}(\underline{x}) =& -\sum_{i\in[\mathrm{d}^\circ+1,d+1]} F\left(x_i\right).
\end{aligned}
$$

C Conversion from additive sharing in $\mathbb{F}_p^n$ to additive sharing in $\mathbb{Z}_{p^n}$

Let $\oplus^n$ be the addition over $\mathbb{F}_p^n$ and let $\boxplus^n$ be the addition over $\mathbb{Z}_{p^n}$. We use the construction from Appendix B.1. Let $\mathrm{d}^\circ = (n-1)(p-1)+1$.

C.1 $s = \mathrm{d}^\circ + 2$

$$
\begin{aligned}
y_1 =& \bigoplus_{i\in[2,\mathrm{d}^\circ+2]}^n x_i, \\
y_j =& (-1)^{j-1}\left(\bigoplus_{i\in[j+1,\mathrm{d}^\circ+2]}^n x_i\right) \boxplus^n \mathop{\boxplus}\limits_{I\in\mathcal{P}^*_{j-2}}^n (-1)^{j-|I|}\left(\bigoplus_{i\in I\cup[j,\mathrm{d}^\circ+2]}^n x_i\right) \quad j\in[2,\mathrm{d}^\circ], \\
y_{\mathrm{d}^\circ+1} =& \left(x_{\mathrm{d}^\circ+1}\right) \boxplus^n \mathop{\boxplus}\limits_{I\in\mathcal{P}^*_{\mathrm{d}^\circ-1}}^n (-1)^{\mathrm{d}^\circ+1-|I|}\left(\bigoplus_{i\in I\cup[\mathrm{d}^\circ+1,\mathrm{d}^\circ+2]}^n x_i\right), \\
y_{\mathrm{d}^\circ+2} =& \mathop{\boxplus}\limits_{I\in\mathcal{P}^*_{\mathrm{d}^\circ}}^n (-1)^{\mathrm{d}^\circ-|I|}\left(\bigoplus_{i\in I}^n x_i\right) \boxplus^n (-1)\left(x_{\mathrm{d}^\circ+1}\right).
\end{aligned}
$$

C.2 $s > \mathrm{d}^\circ + 2$

$$\begin{aligned}
y_1 &= \bigoplus_{i\in[2,s]}^{n} x_i,\\
y_j &= (-1)^{j-1}\left(\bigoplus_{i\in[j+1,s]}^{n} x_i\right) \boxplus^n \mathop{\boxplus}_{I\in\mathcal{P}^*_{j-2}}^{n} (-1)^{j-|I|}\left(\bigoplus_{i\in I\cup[j,s]}^{n} x_i\right) \quad j\in[2,\mathrm{d}^\circ],\\
y_{\mathrm{d}^\circ+1} &= (x_{\mathrm{d}^\circ+1}) \boxplus^n \mathop{\boxplus}_{I\in\mathcal{P}^*_{\mathrm{d}^\circ-1}}^{n} (-1)^{\mathrm{d}^\circ+1-|I|}\left(\bigoplus_{i\in I\cup[\mathrm{d}^\circ+1,s]}^{n} x_i\right),\\
y_{\mathrm{d}^\circ+2} &= (x_{\mathrm{d}^\circ+2}) \boxplus^n \mathop{\boxplus}_{I\in\mathcal{P}^*_{\mathrm{d}^\circ}}^{n} (-1)^{\mathrm{d}^\circ-|I|}\left(\bigoplus_{i\in I}^{n} x_i\right),\\
y_j &= x_j \quad j\in[\mathrm{d}^\circ+3, s-1],\\
y_s &= -\left(\mathop{\boxplus}_{i\in[\mathrm{d}^\circ+1,s-1]}^{n} x_i\right)
\end{aligned}$$

D Conversion from additive sharing in $\mathbb{Z}_{p^n}$ to additive sharing in $\mathbb{F}_p^n$

Let $\oplus^n$ be the addition over $\mathbb{F}_p^n$ and let $\boxplus^n$ be the addition over $\mathbb{Z}_{p^n}$. We use the construction from Appendix B.1. Let $\mathrm{d}^\circ = p^{n-1}$.

D.1 $s = \mathrm{d}^\circ + 2$

$$\begin{aligned}
y_1 &= \mathop{\boxplus}_{i\in[2,\mathrm{d}^\circ+2]}^{n} x_i,\\
y_j &= (-1)^{j-1}\left(\mathop{\boxplus}_{i\in[j+1,\mathrm{d}^\circ+2]}^{n} x_i\right) \oplus^n \bigoplus_{I\in\mathcal{P}^*_{j-2}}^{n} (-1)^{j-|I|}\left(\mathop{\boxplus}_{i\in I\cup[j,\mathrm{d}^\circ+2]}^{n} x_i\right) \quad j\in[2,\mathrm{d}^\circ],\\
y_{\mathrm{d}^\circ+1} &= (x_{\mathrm{d}^\circ+1}) \oplus^n \bigoplus_{I\in\mathcal{P}^*_{\mathrm{d}^\circ-1}}^{n} (-1)^{\mathrm{d}^\circ+1-|I|}\left(\mathop{\boxplus}_{i\in I\cup[\mathrm{d}^\circ+1,\mathrm{d}^\circ+2]}^{n} x_i\right),\\
y_{\mathrm{d}^\circ+2} &= \bigoplus_{I\in\mathcal{P}^*_{\mathrm{d}^\circ}}^{n} (-1)^{\mathrm{d}^\circ-|I|}\left(\mathop{\boxplus}_{i\in I}^{n} x_i\right) \oplus^n (-1)\,(x_{\mathrm{d}^\circ+1}).
\end{aligned}$$

D.2 $s > \mathrm{d}^\circ + 2$

$$\begin{aligned}
y_1 &= \mathop{\boxplus}_{i\in[2,s]}^{n} x_i,\\
y_j &= (-1)^{j-1}\left(\mathop{\boxplus}_{i\in[j+1,s]}^{n} x_i\right) \oplus^n \bigoplus_{I\in\mathcal{P}^*_{j-2}}^{n} (-1)^{j-|I|}\left(\mathop{\boxplus}_{i\in I\cup[j,s]}^{n} x_i\right) \quad j\in[2,\mathrm{d}^\circ],\\
y_{\mathrm{d}^\circ+1} &= (x_{\mathrm{d}^\circ+1}) \oplus^n \bigoplus_{I\in\mathcal{P}^*_{\mathrm{d}^\circ-1}}^{n} (-1)^{\mathrm{d}^\circ+1-|I|}\left(\mathop{\boxplus}_{i\in I\cup[\mathrm{d}^\circ+1,s]}^{n} x_i\right),\\
y_{\mathrm{d}^\circ+2} &= (x_{\mathrm{d}^\circ+2}) \oplus^n \bigoplus_{I\in\mathcal{P}^*_{\mathrm{d}^\circ}}^{n} (-1)^{\mathrm{d}^\circ-|I|}\left(\mathop{\boxplus}_{i\in I}^{n} x_i\right),\\
y_j &= x_j \quad j\in[\mathrm{d}^\circ+3, s-1],\\
y_s &= -\left(\bigoplus_{i\in[\mathrm{d}^\circ+1,s-1]}^{n} x_i\right)
\end{aligned}$$

E Conversion from additive sharing in $\mathbb{Z}_{p^n}$ to additive sharing in $\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}$

Let $\boxplus^k$ be the addition over $\mathbb{Z}_{p^k}$. We use the construction from Appendix B.1. Let $\mathrm{d}^\circ = (n-1)(p-1)+1$.

E.1 $s = \mathrm{d}^\circ + 2$

$$\begin{aligned}
y_{1,(1)} =& \bigoplus_{i\in[2,\mathrm{d}^\circ+2]} x_{i,(1)},\\
(y_1)_{(2,n)} =& \left(\mathop{\boxplus}\limits_{i\in[2,\mathrm{d}^\circ+2]}^{n} x_i\right)_{(2,n)},\\
y_{j,(1)} =& (-1)^{j-1} \bigoplus_{i\in[j,\mathrm{d}^\circ+2]} x_{i,(1)} \oplus (-1)^{j-1} \bigoplus_{i\in[j+1,\mathrm{d}^\circ+2]} x_{i,(1)} \quad j\in[2,\mathrm{d}^\circ],\\
(y_j)_{(2,n)} =& (-1)^{j-1} \left(\mathop{\boxplus}\limits_{i\in[j+1,\mathrm{d}^\circ+2]}^{n} x_i\right)_{(2,n)} \boxplus^{n-1} \mathop{\boxplus}\limits_{I\in\mathcal{P}^*_{j-2}}^{n-1} (-1)^{j-|I|} \left(\mathop{\boxplus}\limits_{i\in I\cup[j,\mathrm{d}^\circ+2]}^{n} x_i\right)_{(2,n)} \qquad j\in[2,\mathrm{d}^\circ],\\
y_{\mathrm{d}^\circ+1,(1)} =& x_{\mathrm{d}^\circ+1,(1)} \oplus (-1)^{\mathrm{d}^\circ+1} \left(x_{\mathrm{d}^\circ+1,(1)} \oplus x_{\mathrm{d}^\circ+2,(1)}\right),\\
(y_{\mathrm{d}^\circ+1})_{(2,n)} =& (x_{\mathrm{d}^\circ+1})_{(2,n)} \boxplus^{n-1} \mathop{\boxplus}\limits_{I\in\mathcal{P}^*_{\mathrm{d}^\circ-1}}^{n-1} (-1)^{\mathrm{d}^\circ+1-|I|} \left(\mathop{\boxplus}\limits_{i\in I\cup[\mathrm{d}^\circ+1,\mathrm{d}^\circ+2]}^{n} x_i\right)_{(2,n)},\\
y_{\mathrm{d}^\circ+1,(1)} =& -x_{\mathrm{d}^\circ+1,(1)},\\
(y_{\mathrm{d}^\circ+2})_{(2,n)} =& \mathop{\boxplus}\limits_{I\in\mathcal{P}^*_{\mathrm{d}^\circ}}^{n-1} (-1)^{\mathrm{d}^\circ-|I|} \left(\mathop{\boxplus}\limits_{i\in I}^{n} x_i\right)_{(2,n)} \boxplus^{n-1} (-1)\,(x_{\mathrm{d}^\circ+1})_{(2,n)}.
\end{aligned}$$

E.2 $s > \mathrm{d}^\circ + 2$

$$\begin{aligned}
y_{1,(1)} =& \bigoplus_{i\in[2,s]} x_{i,(1)},\\
(y_1)_{(2,n)} =& \left(\mathop{\boxplus}\limits_{i\in[2,s]}^{n} x_i\right)_{(2,n)},\\
y_{j,(1)} =& (-1)^{j-1} \bigoplus_{i\in[j+1,s]} x_{i,(1)} \oplus (-1)^{j-1} \bigoplus_{i\in[j,s]} x_{i,(1)} \quad j\in[2,\mathrm{d}^\circ],\\
(y_j)_{(2,n)} =& (-1)^{j-1} \left(\mathop{\boxplus}\limits_{i\in[j+1,s]}^{n} x_i\right)_{(2,n)} \boxplus^{n-1} \mathop{\boxplus}\limits_{I\in\mathcal{P}^*_{j-2}}^{n-1} (-1)^{j-|I|} \left(\mathop{\boxplus}\limits_{i\in I\cup[j,s]}^{n} x_i\right)_{(2,n)} \qquad j\in[2,\mathrm{d}^\circ],\\
y_{\mathrm{d}^\circ+1,(1)} =& x_{\mathrm{d}^\circ+1,(1)} \oplus (-1)^{\mathrm{d}^\circ+1} \left(\bigoplus_{i\in[\mathrm{d}^\circ+1,s]} x_{i,(1)}\right),\\
(y_{\mathrm{d}^\circ+1})_{(2,n)} =& (x_{\mathrm{d}^\circ+1})_{(2,n)} \boxplus^{n-1} \mathop{\boxplus}\limits_{I\in\mathcal{P}^*_{\mathrm{d}^\circ-1}}^{n-1} (-1)^{\mathrm{d}^\circ+1-|I|} \left(\mathop{\boxplus}\limits_{i\in I\cup[\mathrm{d}^\circ+1,s]}^{n} x_i\right)_{(2,n)},\\
y_{\mathrm{d}^\circ+2,(1)} =& x_{\mathrm{d}^\circ+2,(1)},\\
(y_{\mathrm{d}^\circ+2})_{(2,n)} =& (x_{\mathrm{d}^\circ+2})_{(2,n)} \boxplus^{n-1} \mathop{\boxplus}\limits_{I\in\mathcal{P}^*_{\mathrm{d}^\circ}}^{n-1} (-1)^{\mathrm{d}^\circ-|I|} \left(\mathop{\boxplus}\limits_{i\in I}^{n} x_i\right)_{(2,n)},\\
y_j =& x_j \quad j\in[\mathrm{d}^\circ+3, s-1],\\
y_{s,(1)} =& -\left(\bigoplus_{i\in[\mathrm{d}^\circ+1,s-1]} x_{i,(1)}\right)\\
(y_s)_{(2,n)} =& -\left(\mathop{\boxplus}\limits_{i\in[\mathrm{d}^\circ+1,s-1]}^{n-1} (x_i)_{(2,n)}\right).
\end{aligned}$$