SIAM J. OPTIM.
Vol. 27, No. 4, pp. 2182–2201

GENERALIZED LEXICOGRAPHIC MULTIOBJECTIVE COMBINATORIAL OPTIMIZATION. APPLICATION TO CRYPTOGRAPHY*

PEDRO J. ZUFIRIA† AND JOSÉ A. ÁLVAREZ-CUBERO†

Abstract. This paper formalizes a family of prioritized multicriteria optimization problems and assesses the corresponding up-to-date known suboptimal solutions. The resulting framework is then employed to characterize and search for Boolean functions which are valuable for a robust symmetric (mainly block) cipher design. The proposed optimality definitions generalize the lexicographic method by establishing an ordered sequence of multiobjective combinatorial optimization problems, which, in turn, gathers the relative relevance of the criteria, so that the optimal solutions can be obtained from a sequential application of the Pareto efficiency. The relationship among the different formulable problems is characterized in terms of both their respective solutions sets and computing costs. Since, in practice, only a limited set of functions can be evaluated (i.e., are known), the best known Pareto efficient functions are also defined. Finally, this framework is employed to obtain new functions having known (Pareto) maximal robustness against linear, differential, randomness-based, interpolation, algebraic and correlation attacks.

Key words. Pareto efficiency, combinatorial optimization, block cipher, S-box, balancedness, nonlinearity, algebraic degree, algebraic immunity, absolute indicator, sums-of-squares indicator, correlation immunity order, propagation criterion degree

AMS subject classifications. 90C27, 90C29, 68P25, 4904

DOI. 10.1137/16M1107826

1. Introduction.

In recent decades, multicriteria optimization (also known as multiobjective optimization or, in a more general setting, vector optimization) has become an expansive and mature field of research [9, 21, 28, 32]. When operating in such a vast arena, different subfields can be considered depending on the mathematical structures in both the search and criteria sets and the analytical properties of the criteria (or cost) functions. In this framework, multiobjective combinatorial optimization (MOCO) addresses those problems wherein the search set is discrete, usually finite but huge, such that an exhaustive search is not computationally viable.

The solution of a multiobjective problem is executed through the following two stages: the proper determination of the optimal solutions set and the multicriteria *decision-making* among the existing solutions, where preferences among the criteria play an important role. Accordingly, the most established classification of multiobjective techniques relies on the different manners of articulation of such preferences between those two stages: a priori (make decisions before searching), a posteriori (search before making decisions), and progressive (integrating search and decision [21]). In this context, the definition of user preferences among criteria and its application to the efficient design of evolutionary algorithms has been extensively addressed [8, 7, 23, 22, 25, 26, 30, 46, 53].

*Received by the editors December 13, 2016; accepted for publication (in revised form) May 3, 2017; published electronically October 10, 2017.

http://www.siam.org/journals/siopt/27-4/M110782.html

Funding: This work was funded by Ministerio de Ciencia e Innovación and Ministerio de Economía y Competitividad, Spain, under projects MTM2010-15102 and MTM2015-67396-P.

†Departmento Matemática Aplicada a las TIC, and Information Processing and Telecommunications Center, Universidad Politécnica de Madrid. ETSI Telecomunicación, 28040 Madrid, Spain (pedro.zufiria@upm.es, jaacubero@gmail.com).

Due to the limitations in terms of the analytical treatment of the criteria functions in MOCO problems, the expected structure of the Pareto front set cannot be easily characterized. Taking that into consideration, the determination of the optimal solutions is a bigger challenge than the posterior decision-making; hence, an a priori articulation of preferences seems to be the most suitable approach. Among the several existing techniques, the lexicographic method can be considered as a basic reference due to its conceptual and computational simplicity, although generalizations of such method and more sophisticated methods are frequently employed in practice [6]. Here, one such generalization of the lexicographic method is formalized to help define and compare sets of solutions and computational costs.

MOCO techniques are being applied to the existing design of Boolean functions with good ciphering properties, as the fundamental components of the S-boxes employed in robust cipher design [44, 45]. These properties are characterized via several relevant criteria from the cryptographic perspective [43], usually posing a trade-off between them [19, 36, 11, 54, 51, 16], so that the resultant design of robust Boolean functions looks for a compromise among these criteria [17, 20, 33, 41, 24, 18, 1, 10, 34, 48, 47, 50, 35, 14, 38, 4, 49, 52]. The systematic selection of such criteria (not to mention the determination of their relative relevance) is an open issue in the existing literature on the subject matter. For instance, [38, 49] address only nonlinearity, [34] focuses on balancedness and autocorrelation (although nonlinearity, algebraic degree and algebraic immunity are also considered), [35] considers nonlinearity, balancedness, and autocorrelation (interestingly, they also look at resiliency and propagation as secondary criteria), while [19, 36, 18] address balancedness, nonlinearity, autocorrelation, and algebraic degree. Recently, in the context of stream ciphers, [52, 14, 54, 51, 16] take into account balancedness, nonlinearity, algebraic degree, algebraic immunity, and immunity to fast algebraic attacks; [14, 54] focus on optimizing balancedness and algebraic immunity, [51] optimizes algebraic immunity and algebraic degree, whereas [16] additionally keeps track of correlation immunity order. In brief, very different optimization problems keep getting addressed, depending on the cipher specific application and the expected types of attacks.

The first part of this paper formalizes a family of prioritized MOCO problems [28] that depend on the selected criteria and their assigned relative relevance. The set of potentially formulable problems is partially ordered, its elements being comparatively characterized with regard to their corresponding solution sets and computational costs. The solution functions of each MOCO problem are defined as optimal (or efficient) in the Pareto sense. Since the determination of the whole Pareto efficient (PE) set is computationally unfeasible for many of the typically employed values of n (e.g., $n \geq 8$), a practical objective is to find those solutions that are PE within the set of known (analyzed) up-to-date functions. These are called *best known Pareto efficient (BKPE)* functions.

Based on the previous characterization, the second part of the paper addresses the determination of optimal Boolean functions for robust block cipher design. The selected relevant criteria are balancedness, nonlinearity, algebraic degree, algebraic immunity, absolute indicator, and sum-of-squares indicator, as well as two secondary ones, which are correlation immunity order and propagation criterion degree. The search for BKPE functions employs the vector Boolean function (VBF) library developed in [3, 5] to characterize VBFs from a cryptographic perspective. Several optimization computational techniques have been developed and integrated with VBF to address MOCO problems for the design of Boolean functions with 8, 9, and 11 input variables, leading to new BKPE Boolean functions.

The paper is organized as follows. In section 2, the MOCO formulation is presented, the significance of removing or including new criteria is analyzed, and the implications of defining preferences among the criteria are also characterized. BKPE functions for any given MOCO problem are defined in section 3. The Pareto optimality of Boolean functions *with respect to* (*wrt*) the criteria relevant for cipher design is presented in section 4, where the fundamental concepts are also illustrated with a simple example. The proposed search schemes for solving Pareto optimality problems and the obtained BKPE functions are presented in section 5. Finally, conclusions are summarized in section 6.

2. Problem formulation. Since the construction of Boolean functions for cipher design must satisfy several performance criteria, it can be formalized via a multiobjective optimization problem [28]. We begin by formulating the classical basic problem that does not consider preferences among the criteria.

2.1. Multiobjective optimization. Let $f \in \mathcal{F}_n$ be the set of n-input variable Boolean functions, let $\mathcal{C} = \{C_1, \ldots, C_K\}$ be a set of criteria (whose order is not relevant a priori for solving the problem), and let $\mathbf{C}(f) = (C_1(f), \ldots, C_K(f))$ be the vector of the criteria that have been ordered for the ease of notation, applied on f, so that each

$$C_k : \ \mathcal{F}_n \to \mathbb{R}, \ k = 1, \ldots, K, \tag{1}$$

represents a measure of the goodness of f wrt criterion k (we keep a general formulation, although, usually, $C_k(f) \in \mathbb{Z} \subset \mathbb{R}$).

The fact that all the criteria of $\mathbf{C}(f)$ need to be taken into account for determining the goodness of a given function makes the problem a *multiobjective* one as well. Moreover, since the set of n-variable Boolean functions $\mathcal{F}_n$ is a finite set, the search within $\mathcal{F}_n$ is framed as a *combinatorial optimization problem.* Hence, we can formulate the problem as obtaining

$$\mathcal{E}_n = \arg\max_{f \in \mathcal{F}_n} \ \mathbf{C}(f), \tag{2}$$

where the multiobjective maximality will be grounded on the concepts of *(weak) dominance* and *(strict) Pareto efficiency* [28].[1]

DEFINITION 2.1. *Let $f, g \in \mathcal{F}_n$; if $\mathbf{C}(g) \geqq \mathbf{C}(f)$ (i.e., $C_k(g) \geq C_k(f)$, $k = 1, \ldots, K$), then we say that $\mathbf{C}(g)$ weakly dominates $\mathbf{C}(f)$, and g* weakly dominates *f.*

Note that although dominance is defined in the criterion space, the domination relationship can also be transferred to be able to relate the corresponding elements in the decision space [28]; from now on, this definition form will be employed in this paper.

DEFINITION 2.2. *If $\mathbf{C}(g) \geq \mathbf{C}(f)$ (i.e., $\mathbf{C}(g) \geqq \mathbf{C}(f)$ and $\mathbf{C}(g) \neq \mathbf{C}(f)$), then we say that g* dominates *f.*

Note that if g dominates f, then g is preferred over f.

DEFINITION 2.3. *$f \in \mathcal{F}_n$ is* PE *if $\nexists \ g \in \mathcal{F}_n$, such that g dominates f.*

[1] The concepts of *strong dominance*, *weak Pareto efficiency* [28], and *proper efficiency* [31] (the last one always being satisfied in combinatorial optimization) do not have relevant applicability in this paper.

DEFINITION 2.4. *$f \in \mathcal{F}_n$ is* strict Pareto efficient (SPE) *if $\nexists\, g \in \mathcal{F}_n$ ($g \neq f$) such that g weakly dominates f.*

If f is PE, then we will call vector $\mathbf{C}(f)$ a *nondominated profile*. The set of all PE functions f is called the efficient set, $\mathcal{E}_n \subseteq \mathcal{F}_n$; since $\mathcal{F}_n$ is finite and the dominance relationship defines a partial ordering under which only dominated functions are discarded, then it is always $\mathcal{E}_n \neq \emptyset$. The set of profiles of all nondominated functions is called the nondominated profiles set, $N_n = \mathbf{C}(\mathcal{E}_n) \subset \mathbb{R}^K$. Note that different elements $f_1 \neq f_2 \in \mathcal{E}_n$ may satisfy $\mathbf{C}(f_1) = \mathbf{C}(f_2) = \mathbf{C}^d$ for some $d \in \{1, \ldots, D\}$. Accordingly, since $N_n = \{\mathbf{C^1}, \ldots, \mathbf{C^D}\}$ is a finite set, we can partition $\mathcal{E}_n = \mathcal{E}_n^1 \sqcup \cdots \sqcup \mathcal{E}_n^d \sqcup \cdots \sqcup \mathcal{E}_n^D$, where each

$$\mathcal{E}_n^d = \{f \in \mathcal{E}_n : \mathbf{C}(f) = \mathbf{C^d}\},\ d = 1, \ldots, D, \tag{3}$$

is called a *same profile efficient set*. When $|\mathcal{E}_n^d| = 1$ (i.e., the set has only one element), it contains a single SPE function. On the other hand, when $|\mathcal{E}_n^d| > 1$, it contains some $f_1 \neq f_2$ such that $\{f_1, f_2\} \subset \mathcal{E}_n^d$, meaning that they are PE but not SPE. This allows one to define $\mathcal{E}_n = \mathcal{E}_n^o \sqcup \mathcal{E}_n^t$, so that $\mathcal{E}_n^o = \cup_d \mathcal{E}_n^d$, for those $\mathcal{E}_n^d$ satisfying $|\mathcal{E}_n^d| = 1$, and $\mathcal{E}_n^t = \cup_d \mathcal{E}_n^d$, for those $\mathcal{E}_n^d$ satisfying $|\mathcal{E}_n^d| > 1$. We call $\mathcal{E}_n^o$ the *optimal set* (composed of SPE functions) and $\mathcal{E}_n^t$ the *ties set* (composed of PE but not SPE functions).

Ideally, our final aim would be to determine set N_n and its subsets $\mathcal{E}_n^d$, $d = 1, \ldots D$, that correspond to the optimal and ties sets.

2.2. Significance of removing or adding new criteria. As to be illustrated in section 4, many practical design problems may not have a unique clear-cut statement of the criteria set $\mathcal{C}$ to be considered when defining problem (2); obviously, the selection of $\mathcal{C}$ determines the corresponding solution set $\mathcal{E}_n$. We begin by illustrating the manner in which the PE property depends on the exclusion of criteria or the inclusion of new ones (by considering subsets or supersets of $\mathcal{C}$).

LEMMA 2.5. *Let $\mathcal{C}$, $\mathcal{C}'$, and $\mathcal{C}''$ be three criteria sets, such that $\mathcal{C}' \subsetneq \mathcal{C} \subsetneq \mathcal{C}''$.*

1. *If f_1 is SPE wrt $\mathcal{C}$, then it is SPE wrt $\mathcal{C}''$, but it may or may not be PE wrt $\mathcal{C}'$.*
2. *If f_2 is PE (but not SPE) wrt $\mathcal{C}$, then f_2 may or may not be PE wrt $\mathcal{C}'$ and $\mathcal{C}''$. Let us call its corresponding same profile efficient set $\mathcal{E}_n^d = \{f \in \mathcal{E}_n : \mathbf{C}(f) = \mathbf{C}(f_2) = \mathbf{C^d}\} \subset \mathcal{E}_n^t$; then*
   (a) *$\exists f_2' \in \mathcal{E}_n^d$, which is also PE wrt $\mathcal{C}'' \setminus \mathcal{C}$ when restricted to $\mathcal{E}_n^d$, and this f_2' will be PE wrt $\mathcal{C}''$ in the whole $\mathcal{F}_n$;*
   (b) *if such f_2' is also SPE wrt $\mathcal{C}'' \setminus \mathcal{C}$ when restricted to $\mathcal{E}_n^d$, it will be SPE wrt $\mathcal{C}''$ in the whole $\mathcal{F}_n$.*
3. *If f_3 is not PE wrt $\mathcal{C}$, then f_3 may or may not be PE wrt $\mathcal{C}'$ and $\mathcal{C}''$.*

Proof. Respectively, the following apply:

1. If f_1 is not SPE in $\mathcal{F}_n$ wrt $\mathcal{C}''$, then $\exists f_2 \neq f_1 \in \mathcal{F}_n$, which weakly dominates f_1 wrt $\mathcal{C}'' \supset \mathcal{C}$, implying that f_2 weakly dominates f_1 wrt $\mathcal{C}$, which leads to a contradiction.
   On the other hand, there may exist $f_2 \neq f_1 \in \mathcal{F}_n$, which weakly dominates f_1 wrt $\mathcal{C}' \subset \mathcal{C}$; however, f_2 does not weakly dominate f_1 wrt $\mathcal{C}$.
2. Let us consider $\mathcal{E}_n^d$, the same profile efficient set of f_2 where all functions are PE wrt $\mathcal{C}$.
   (a) Since problems of type (2) always produce nonempty solution, $\exists f_2' \in \mathcal{E}_n^d$ that is PE wrt $\mathcal{C}'' \setminus \mathcal{C}$ in $\mathcal{E}_n^d$. If f_2' is not PE in $\mathcal{F}_n$ wrt $\mathcal{C}''$, then $\exists f_2'' \in \mathcal{F}_n$, which strictly dominates f_2' wrt $\mathcal{C}''$. Since f_2' is not strictly dominated

wrt $\mathcal{C}$, f_2'' must only weakly dominate f_2' in $\mathcal{C}$ (i.e., it must belong to the $\mathcal{E}_n^d$ set of f_2) and must strictly dominate f_2' wrt $\mathcal{C}'' \setminus \mathcal{C}$, leading to a contradiction.

(b) Let us now consider that f_2' is SPE wrt $\mathcal{C}'' \setminus \mathcal{C}$ in $\mathcal{E}_n^d$. If f_2' is not SPE in $\mathcal{F}_n$ wrt $\mathcal{C}''$, then $\exists f_2'' \in \mathcal{F}_n$, which dominates f_2' wrt $\mathcal{C}''$. Then f_2'' dominates f_2' wrt $\mathcal{C}'' \setminus \mathcal{C}$, leading to a contradiction.

Finally, since the initial f_2 may or may not be equal to f_2', we conclude that f_2 may or may not be PE wrt $\mathcal{C}''$.

3. Functions initially discarded as not being PE wrt $\mathcal{C}$ (such as f_3) may be SPE wrt $\mathcal{C}'' \setminus \mathcal{C}$, becoming SPE (and hence, PE) wrt $\mathcal{C}''$. Finally, f_3 might have been (nonstrict) PE wrt $\mathcal{C}'$ (i.e., tied with another function), such that the additional criteria considered in $\mathcal{C}$ would have broken the tie against it. ∎

Note that Lemma 2.5.3 can be concluded from Lemma 2.5.2, but it has been included as an additional statement for the sake of completeness. Lemma 2.5.2 states a refinement of an obvious weaker result: if f is both PE wrt $\mathcal{C}_1$ and (S)PE wrt $\mathcal{C}_2$ *in the whole* $\mathcal{F}_n$, then it will be (S)PE wrt $\mathcal{C}_1 \cup \mathcal{C}_2$ in $\mathcal{F}_n$.

The properties demonstrated in Lemma 2.5 will be the basis for analyzing the variety of problems that are posed in section 2.3, encountered when considering different types of preferences among the criteria.

2.3. Preferences or priorities among criteria. Problem (2) does not consider any preference (i.e., relative relevance or priority) among the criteria C_k. In the case that some criteria are more important than others, such additional information can be incorporated into the problem, leading to a new formulation, sometimes a computationally simpler one. In fact, the study of preferences among criteria can be seen from two different perspectives. In some cases, it reflects a refinement in the formulation of the problem that needs to be solved; in other cases, it may help to simplify the formulation while guaranteeing the derivation of *some* solutions of the original problem.

Here, we propose to characterize preferences among criteria by splitting the criteria set into a sequence of disjoint subsets

$$\mathcal{C} = \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_j \sqcup \cdots \sqcup \mathcal{C}_L, \quad L \leq K, \tag{4}$$

ordered by preference. Then, a new optimization problem can be defined, where only $\mathcal{C}_1 = \{C_{11}, \ldots, C_{1l_1}\}$ is initially considered (with corresponding criteria vector $\mathbf{C}_1(f)$); once this initial subproblem is solved, then $\mathcal{C}_2 = \{C_{21}, \ldots, C_{2l_2}\}$ is considered (with corresponding criteria vector $\mathbf{C}_2(f)$), but only for choosing among the elements of the ties set obtained in the previous stage and so forth. This formulation generalizes the well-known lexicographic ordering [28], and it has been recently employed to computationally address some search problems in continuous spaces [6]. Overall, this optimization problem can be formulated, in a recurrent manner, as obtaining

$$\mathcal{E}_n = E_{n,1}^o \sqcup E_{n,2}^o \sqcup \cdots \sqcup E_{n,L-1}^o \sqcup E_{n,L}^o \sqcup E_{n,L}^t, \tag{5}$$

where

$$E_{n,0}^t = \mathcal{F}_n, \tag{6}$$

$$E_{n,j} = E_{n,j}^o \sqcup E_{n,j}^t = \underset{f \in E_{n,j-1}^t}{\arg\max}\ \mathbf{C}_j(f),\ j = 1, \ldots, L, \tag{7}$$

and where each $E_{n,j}^o, j \geq 1$, represents the optimal set of SPE elements obtained at stage j, and each $E_{n,j}^t, j \geq 1$, represents the ties set of (nonstrict) PE elements

obtained at this stage. Finally, $\mathcal{E}_n$ would be the corresponding solution set. Note that the elements of $E^o_{n,j}$ obtained in step j, according to Lemma 2.5.1, will always remain SPE when considering larger criteria sets, so that they can be preserved without considering them in the following steps. On the other hand, elements of $E^t_{n,j}$ belong to the ties set, and hence (based on Lemma 2.5.2) we perform a search within them to obtain functions with are PE wrt $\mathcal{C}_{j+1}$ (hence, PE wrt $\mathcal{C}_1 \sqcup \ldots \sqcup \mathcal{C}_{j+1}$ in $\mathcal{F}_n$) and so on. Note that if $E^t_{n,j} = \emptyset$ (i.e., all obtained functions are SPE and there are no more ties), the iterative procedure can be stopped since $E^o_{n,j'} = E^t_{n,j'} = \emptyset \; \forall j' > j$.

In this context, we redefine the *profile* $P(f)$ of a Boolean function to also reflect the criteria priorities as

$$P(f) = (n|C_{11}(f), \ldots, C_{1l_1}(f)| \ldots |C_{L1}(f), \ldots, C_{Ll_L}(f)), \tag{8}$$

where the vertical bar "|" separates the different sets of criteria $\mathcal{C}_1, \ldots, \mathcal{C}_L$, classified by priority. Once the optimal Pareto set is obtained wrt $\mathcal{C}_j$, the corresponding nonstrict PE set is "piped" to become the whole search space where a new multi-objective optimization process is applied, based on the set of criteria $\mathcal{C}_{j+1}$, and so forth. Note that the value of n can be interpreted as a most preeminent criterion implicitly satisfied (since we restrict the search within $\mathcal{F}_n$); one might formally name this criterion $C_0(f)$, although it will not be explicitly stated in our exposition, and, whenever obvious, this information will be removed from the profile (e.g., in the tables shown in section 5). Note that the profile provides information on both the type of problem addressed (in this case, problem (5)) and the values associated with such function f.

Given an *ordered* set $\mathcal{C} = (C_1, \ldots, C_K)$ of K criteria, there are 2^{K-1} different ways to split it into disjoint subsets in the form of (4), preserving the order, so that each splitting defines a corresponding different optimization problem (5). Each splitting of $\mathcal{C}$ can be represented either by the collection of subsets (4) or, equivalently, as following the profile notation (8), by a set of (at most $K-1$) vertical bars between the ordered elements of $\mathcal{C}$. If the presence of a bar between two criteria is coded as "1," when there is the absence as "0," all possible splittings can be labeled with the number corresponding to this form of binary representation (no bars would correspond to 0 and all the bars to $2^{K-1} - 1$).

Let $S_{\mathcal{C}} = \{s_0, \ldots, s_{2^{K-1}-1}\}$ be the set of all 2^{K-1} possible ways to split $\mathcal{C}$ (remember that this set includes the special case $s_0 \in S_{\mathcal{C}}$ of no splitting of $\mathcal{C}$). Whenever suitable, we will use notation s_i to denote both the splitting (4) and the corresponding problem (5), whose associated solution set will be denoted $\mathcal{E}(s_i)$ as well. One can define the relationship "$\succ$" ("finer than") between some of the elements of $S_{\mathcal{C}}$.

DEFINITION 2.6. *Let $s_{i_1}, s_{i_2} \in S_{\mathcal{C}}$ be two splittings of $\mathcal{C}$. $s_{i_2} \succ s_{i_1}$ (s_{i_2} is finer than s_{i_1}) if it can be obtained from s_{i_1} by splitting some subset(s) characterizing s_{i_1} (i.e., by adding some vertical bar(s) to its profile).*

The relationship $\succ$ defines a partial order in $S_{\mathcal{C}}$. Note that if s_{i_1} is defined by (4), and, for instance, if $\mathcal{C}_1$ is split into $\mathcal{C}_1 = \mathcal{C}_{1_1} \sqcup \mathcal{C}_{1_2}$ to define $s_{i_2} \succ s_{i_1}$, then from Lemma 2.5.1, it is clear that there may exist elements of $\mathcal{E}_n(s_{i_1})$ that do not belong to $\mathcal{E}_n(s_{i_2})$, since a function may be PE wrt $\mathcal{C}_1$ while being fully dominated wrt $\mathcal{C}_{1_1} \subsetneq \mathcal{C}_1$.

The following lemma illustrates the relationship between the solutions of ordered problems.

LEMMA 2.7. *If $s_{i_2} \succ s_{i_1}$ then $\mathcal{E}_n(s_{i_2}) \subseteq \mathcal{E}_n(s_{i_1})$.*

Proof. Given any pair $s_{i_1} \prec s_{i_2}$, we can find a sequence $\{s_{i_1}, s_{i'_1}, \ldots, s_{i'_m}, s_{i_2}\}$ so that $s_{i_1} \prec s_{i'_1} \prec \cdots \prec s_{i'_m} \prec s_{i_2}$, wherein each next element is obtained by applying a

single splitting to the previous one. Then, it suffices to prove that Lemma 2.7 applies to consecutive elements, differing by only one splitting since, by recursively applying the reasoning, we can conclude that the lemma applies to any pair $s_{i_1} \prec s_{i_2}$.

Hence, without loss of generality, let s_{1_1} correspond to partition $\mathcal{C} = \mathcal{C}_1 \sqcup \ldots \sqcup \mathcal{C}_j \sqcup \ldots \sqcup \mathcal{C}_L$ and s_{i_2} correspond to $\mathcal{C} = \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{j-1} \sqcup \mathcal{C}_{j_1} \sqcup \mathcal{C}_{j_2} \sqcup \mathcal{C}_{j+1} \sqcup \ldots \sqcup \mathcal{C}_L$. Let $\mathcal{E}_n(s_{1_1}) = E^o_{n,1}(s_{i_1}) \sqcup \cdots \sqcup E^o_{n,j}(s_{i_1}) \sqcup \cdots \sqcup E^o_{n,L-1}(s_{i_1}) \sqcup E^o_{n,L}(s_{i_1}) \sqcup E^t_{n,L}(s_{i_1})$, and $\mathcal{E}_n(s_{i_2}) = E^o_{n,1}(s_{i_2}) \sqcup \cdots \sqcup E^o_{n,j_1}(s_{i_2}) \sqcup E^o_{n,j_2}(s_{i_2}) \sqcup \cdots \sqcup E^o_{n,L-1}(s_{i_2}) \sqcup E^o_{n,L}(s_{i_2}) \sqcup E^t_{n,L}(s_{i_2})$. Since both splittings are the same until stage $j-1$, so is the search for s_{i_1} and s_{i_2}, meaning that $E^o_{n,j'}(s_{i_2}) = E^o_{n,j'}(s_{i_1}) \, \forall j' \leq j-1$; then it suffices to prove that $E^o_{n,j_1}(s_{i_2}) \cup E^o_{n,j_2}(s_{i_2}) \subset \mathcal{E}^o_{n,j}(s_{i_1})$ and $E^t_{n,j_2}(s_{i_2}) \subset \mathcal{E}^t_{n,j}(s_{i_1})$. Since $E^o_{n,j_1}(s_{i_2})$ contains SPE functions wrt $\mathcal{C}_{j_1}$, they are also SPE wrt $\mathcal{C}_j$ (Lemma 2.5.1) and, hence, belong to $E^o_{n,j}(s_{i_1})$.

Let us now consider $E^t_{n,j_1}(s_{i_2})$, whose elements are PE wrt $\mathcal{C}_{j_1}$. The algorithm performs the next search step in $E^t_{n,j_1}(s_{i_2})$ by considering $\mathcal{C}_{j_2}$. Following Lemma 2.5.2(b), the resulting set satisfies $E^o_{n,j_2}(s_{i_2}) \subseteq E^o_{n,j}(s_{i_1})$, and following Lemma 2.5.2(a), we get $E^t_{n,j_2}(s_{i_2}) \subseteq E^t_{n,j}(s_{i_1})$. Then, since the following criteria $\mathcal{C}_{j+1} \sqcup \cdots \sqcup \mathcal{C}_L$ are the same for s_{i_1} and s_{i_2}, we recursively obtain $E^o_{n,j'}(s_{i_2}) \subseteq E^o_{n,j'}(s_{i_1}), j' = j+1, \ldots, L$, and $E^t_{n,L}(s_{i_2}) \subseteq E^t_{n,L}(s_{i_1})$. ∎

On the other hand, if we call $T(s)$ the computational (time) cost of determining the solution set $\mathcal{E}_n(s)$ of a problem s, then we have the following.

LEMMA 2.8. *If $s_{i_2} \succ s_{i_1}$, then $T(s_{i_2}) \leq T(s_{i_1})$.*

Proof. Following the same reasoning applied in the previous proof of Lemma 2.7, if suffices to prove that Lemma 2.8 applies to elements differing in only one splitting since, by recursively applying the reasoning, we would conclude that the lemma applies to any pair $s_{i_1} \prec s_{i_2}$. Hence, without loss of generality, we consider that s_{1_1} corresponds to partition $\mathcal{C} = \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_j \sqcup \cdots \sqcup \mathcal{C}_L$, and s_{i_2} corresponds to $\mathcal{C} = \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{j-1} \sqcup \mathcal{C}_{j_1} \sqcup \mathcal{C}_{j_2} \sqcup \mathcal{C}_{j+1} \sqcup \cdots \sqcup \mathcal{C}_L$.

Let us call $T(C_{ij})$ the computational (time) cost of evaluating criterion C_{ij}. The cost of determining the solution set $\mathcal{E}_n(s_{i_1})$ involves, at each stage j', the computation of the corresponding criteria for each function (with cost $|\mathcal{E}^t_{n,j'-1}(s)| \cdot \sum_{l=1}^{l_{j'}} T(C_{j'l})$) and the ordering (at least partial) of the corresponding search set of functions $\mathcal{E}(s)$ (with cost $l_{j'} \cdot |\mathcal{E}^t_{n,j'-1}(s)| \cdot \mathcal{O}(\log(|\mathcal{E}^t_{n,j'-1}(s)|))$). Hence,

$$
\begin{aligned}
(9) \qquad T(s_{i_1}) &= \sum_{j'=1}^{L} |E^t_{n,j'-1}(s_{i_1})| \cdot \left[\sum_{l=1}^{l_{j'}} T(C_{j',l}) + l_{j'} \cdot \mathcal{O}(\log(|E^t_{n,j'-1}(s_{i_1})|)) \right] \\
&= \sum_{\substack{j'=1 \\ j' \neq j}}^{L} |E^t_{n,j'-1}(s_{i_1})| \cdot \left[\sum_{l=1}^{l_{j'}} T(C_{j',l}) + l_{j'} \cdot \mathcal{O}(\log(|E^t_{n,j'-1}(s_{i_1})|) \right] \\
&\quad + |E^t_{n,j-1}(s_{i_1})| \cdot \left[\sum_{l=1}^{l_j} T(C_{j,l}) + l_j \cdot \mathcal{O}(\log(|E^t_{n,j-1}(s_{i_1})|)) \right] \\
&= \sum_{\substack{j'=1 \\ j' \neq j}}^{L} |E^t_{n,j'-1}(s_{i_1})| \cdot \left[\sum_{l=1}^{l_{j'}} T(C_{j',l}) + l_{j'} \cdot \mathcal{O}(\log(|E^t_{n,j'-1}|)) \right]
\end{aligned}
$$

$$
\begin{aligned}
&+ |E^t_{n,j-1}(s_{i_1})| \cdot \left[\sum_{l=1}^{l_{j_1}} T(C_{j_1,l}) + l_{j_1} \cdot \mathcal{O}(\log(|E^t_{n,j-1}(s_{i_1})|)) \right. \\
&\left. + \sum_{l=1}^{l_{j_2}} T(C_{j_2,l}) + l_{j_2} \cdot \mathcal{O}(\log(|E^t_{n,j-1}(s_{i_1})|)) \right] \\
&= \sum_{\substack{j=1 \\ j' \neq j}}^{L} |E^t_{n,j'-1}(s_{i_1})| \cdot \left[\sum_{l=1}^{l_{j'}} T(C_{j',l}) + l_{j'} \cdot \mathcal{O}(\log(|E^t_{n,j'-1}(s_{i_1})|)) \right] \\
&\quad + |E^t_{n,j-1}(s_{i_1})| \cdot \left[\sum_{l=1}^{l_{j_1}} T(C_{j_1,l}) + l_{j_1} \cdot \mathcal{O}(\log(|E^t_{n,j-1}(s_{i_1})|)) \right] \\
&\quad + |E^t_{n,j-1}(s_{i_1})| \cdot \left[\sum_{l=1}^{l_{j_2}} T(C_{j_2,l}) + l_{j_2} \cdot \mathcal{O}(\log(|E^t_{n,j-1}(s_{i_1})|)) \right] \\
&\geq \sum_{\substack{j=1 \\ j' \neq j}}^{L} |E^t_{n,j'-1}(s_{i_2})| \cdot \left[\sum_{l=1}^{l_{j'}} T(C_{j',l}) + l_{j'} \cdot \mathcal{O}(\log(|E^t_{n,j'-1}(s_{i_2})|)) \right] \\
&\quad + |E^t_{n,j-1}(s_{i_2})| \cdot \left[\sum_{l=1}^{l_{j_1}} T(C_{j_1,l}) + l_{j_1} \cdot \mathcal{O}(\log(|E^t_{n,j-1}(s_{i_2})|)) \right] \\
&\quad + |E^t_{n,j_1}(s_{i_2})| \cdot \left[\sum_{l=1}^{l_{j_2}} T(C_{j_2,l}) + l_{j_2} \cdot \mathcal{O}\left(\log(|E^t_{n,j_1}(s_{i_2})|)\right) \right] \\
&= T(s_{i_2}).
\end{aligned}
$$

Note that we have denoted $E^t_{n,j_2}(s_{i_2}) = E^t_{n,j}(s_{i_2})$ to simplify the notation. The inequality is based on the following facts: $l_j = l_{j_1} + l_{j_2}$; $|E^t_{n,j'-1}(s_{i_1})| = |E^t_{n,j'-1}(s_{i_2})|$ $\forall j' \in \{1, \ldots, j\}$; $|E^t_{n,j-1}(s_{i_1})| \geq |E^t_{n,j_1}(s_{i_2})|$; and $|E^t_{n,j'-1}(s_{i_1})| \geq |E^t_{n,j'-1}(s_{i_2})| \forall j' \in \{j+1, \ldots L\}$; all of these are directly derived from the inclusion relationships obtained in the (previous) proof of Lemma 2.7. ∎

Hence, if we are interested in solving problem s_{i_1}, the following trade-off is posed: to address a finer (and, hence, computationally simpler) problem s_{i_2} at the cost of obtaining only a subset of the initially desired set of solutions. Alternatively, if problem s_{i_1} has been initially solved, the solution of s_{i_2} is easily computable by just solving its corresponding problem (5), with the search restricted to $E^t_{n,0}(s_{i_2}) = \mathcal{E}_n(s_{i_1})$ instead of the whole $\mathcal{F}_n$.

In the following section, we illustrate some special cases of interest.

2.3.1. From problem (2) to the sequence of single priorities (lexicographic order). The splitting refinement contains two extremes. On the one hand, problem s_0 corresponding to no splitting (i.e., no vertical bar in the profile), which is precisely what problem (2) entails, and on the other hand, problem $s_{2^{K-1}-1}$, where each $C_k, k = 1, \ldots, K$, follows a strict order of preference, the profile taking the form $(n|C_1|\ldots|C_K)$. Note that $s_{2^{K-1}-1}$ corresponds to the above-mentioned optimality problem based on the lexicographic order.

Then, since any splitting $s_i \in S_{\mathcal{C}}$ satisfies $s_{2^{K-1}-1} \succeq s_i \succeq s_0$ (i.e., s_i is finer than or equal to the null splitting of $\mathcal{C}$ and coarser than or equal to its full splitting), we have the following.

COROLLARY 2.9. *Let $\mathcal{E}_n(s_0)$ be the solution set of problem* (2)*, let $\mathcal{E}_n(s_{2^{K-1}-1})$ be the solution set of the lexicographic optimality problem, and let $\mathcal{E}_n(s_i)$ be the solution set of any problem of the form* (5)*. Then, $\mathcal{E}_n(s_{2^{K-1}-1}) \subseteq \mathcal{E}_n(s_i) \subseteq \mathcal{E}_n(s_0)$ and $T(s_{2^{K-1}-1}) \leq T(s_i) \leq T(s_0)$.*

2.3.2. Prioritizing only one criterion. In the case that some subset $\mathcal{C}_j$ of (4) gathers only one criterion, the corresponding $E_{n,j}$ will be either $E_{n,j} = E^o_{n,j}$ (when $|E_{n,j}| = 1$, hence finishing the search procedure) or $E_{n,j} = E^t_{n,j}$. A simple and relevant case gets defined when $\mathcal{C}_1 = \{C_1\}$, meaning that C_1 is the single most relevant criterion, so that we are only interested in functions reaching the value $c_1^{\max} = \max_{f \in \mathcal{F}_n} C_1(f)$. This will be the case when only either the bent functions or the balanced functions are considered. The corresponding problem (5) boils down to a search restricted within the subset $E_{n,1} = \{f \in \mathcal{F}_n : C_1(f) = c_1^{\max}\}$; if $|E_{n,1}| > 1$, the remaining criteria (with the established priority) are considered for optimization in the following stages, so that the corresponding profile for the searched functions would be $(n|c_1^{\max}|C_2(f), \ldots, C_K(f))$.

This framework relates to the so-called ϵ-constraint methods [28], where restrictions of the type $C_k(x) \leq \epsilon_k$ are imposed to guide the search. If $\epsilon_k = C_k^{\max}$ was selected, then $C_k(x) \leq \epsilon_k$ would be equivalent to imposing $C_k(x) = C_k^{\max}$. Note that although ϵ-restriction methods could serve to approximate the (fully) restricted search performed in the second and the following steps of the problem (5) formulation, their efficiency depends highly on the a priori appropriate selection of the ϵ values.

The following case corresponds to a formulation alternative to (5), which, in turn, leads to scalar optimization problems.

2.3.3. Scalarizations. The weighted sum method. Scalarization methods [29] provide an alternative way to simplify the search, although they are more relevant in a continuous search setting than in a combinatorial one. Among them, the *weighted sum method* (WSM) [28, 55] can be interpreted as having defined a (soft) relative relevance among the criteria. It assigns different "weights" to each criterion, so that solutions of (2) can be searched by addressing an associated simpler scalar optimization problem:

$$\max_{f \in \mathcal{F}_n} \sum_{i=1}^{K} w_i \cdot C_i(f), \quad w \geq 0. \tag{10}$$

Obviously, the ordering induced in $\mathcal{F}_n$ by this scalarization (and, hence, the corresponding solutions of (10)) depend on the assigned weights w_i, $i = 1, \ldots, K$, and the shape of the PE set of (2) [28, 55]. Unique solutions (optima) of (10) are also SPE solutions of problem (2), whereas for $w > 0$, any solution (unique or not) of (10) is also a PE solution of (2). Note that the WSM can be applied at each stage of problem (5) [6]. For instance, the set of solutions of (10) with $w_i > 0$ for $i = 1, \ldots l_1$ (set of weights associated with criteria set $\mathcal{C}_1$) and $w_i = 0$ for $i = l_1 + 1, \ldots, K$ (rest of the criteria) would be a subset of $E_{n,1}$ in (5), and it would be composed by the union of *same profile efficient sets*.

Furthermore, the WSM could also be used to define problems that establish *soft* priorities among the criteria, whose solutions would approximate solutions of the

whole problem (5) at a stroke. For instance, a set of weights satisfying $w_i > \mathcal{O}(1)$ for $i = 1, \dots l_1$ (weights associated with criteria set $\mathcal{C}_1$), $w_i > \mathcal{O}(\epsilon)$ for $i = l_1 + 1, \dots l_1 + l_2$ (weights associated with criteria set $\mathcal{C}_2$), $w_i > \mathcal{O}(\epsilon^2)$ for $i = l_1 + l_2 + 1, \dots l_1 + l_2 + L_3$ (weights associated with criteria set $\mathcal{C}_3$), and so on, for $\epsilon \ll 1$, defines a WSM problem whose solutions are expected to be close to the solutions of (5).

Simulations have shown both the sensitivity of the WSM method wrt the selected weights values and its limited efficiency when it comes to finding solutions when addressing combinatorial problems (such as Boolean function design) due to the confined applicability of topological properties and the computational requirements in this scenario.

The efficiency and theoretical results corresponding to the above-mentioned methods suffer from serious limitations when dealing with highly computationally demanding practical scenarios where only a partial search can be performed, as is the case with the Boolean function design problem. The next section formalizes how to interpret any search result obtained in this context.

3. Best known Pareto efficient Boolean functions. Let us consider problem (5) without loss of generality. For practical values of n, the size of $\mathcal{F}_n$ is too large, so that the determination of PE functions (elements of $\mathcal{E}_n$) becomes computationally unfeasible. In practice, the profile $P(f)$ will be known only for a subset of *known functions* (i.e., functions whose criteria values are known), which we denote as follows.

DEFINITION 3.1. $\mathcal{K}_n = \{f \in \mathcal{F}_n : P(f) \textit{ is known}\}$.

We can now define the *BKPE* set.

DEFINITION 3.2. $\mathcal{B}_n = \{f \in \mathcal{K}_n : \nexists g \in \mathcal{K}_n \textit{ such that } g \textit{ dominates } f\}$.

The elements of $\mathcal{B}_n$ are the *BKPE functions*. In general, if $f \in \mathcal{B}_n$, we cannot guarantee $f \in \mathcal{E}_n$, until $\mathcal{K}_n = \mathcal{F}_n$ (unless it can be supported by some theoretical results). Accordingly, elements of $f \in \mathcal{B}_n$ may or may not be PE. Conversely, we can guarantee that $f \in \mathcal{K}_n \cap \mathcal{E}_n$ implies $f \in \mathcal{B}_n$, meaning that all known functions that happen to be PE (even if at this stage we do not have a guarantee of them being PE) will be BKPE. In Figure 1, we illustrate the evolution of $\mathcal{B}_n$ as $\mathcal{K}_n$ increases: time index t symbolically indicates successive research steps, so that $\mathcal{K}_n^t \subsetneq \mathcal{K}_n^{t+1}$, meaning that the number of known functions increases with time.

Note that $\mathcal{B}_n^t$ can be considered as an approximation of $\mathcal{E}_n$, in the sense that, as $\mathcal{K}_n^t$ increases toward $\mathcal{F}_n$, $\mathcal{B}_n^t$ tends to $\mathcal{E}_n$ (dashed lines approach the boundary of $\mathcal{E}_n$ and eventually $\lim_{t\to\infty} \mathcal{B}_n^t = \mathcal{E}_n \subset \lim_{t\to\infty} \mathcal{K}_n^t = \mathcal{F}_n$).

From now on, this paper addresses the practical problem of improving the sets $\mathcal{B}_n^t$ (i.e., increasing t) to approximate $\mathcal{E}_n$, the solution set of the corresponding problem (5).

4. Application in S-box design. Block ciphers can suffer mainly linear, differential, randomness-based, interpolation, algebraic, and correlation attacks; hence, Boolean functions for S-box design in block ciphers are required to be as balanced as possible,[2] to achieve high nonlinearity, high algebraic degree, high algebraic immunity, and low autocorrelation (both absolute[3] and sum-of-squares indicators).

[2]Although only strictly balanced functions are used for ciphers design in practice, this condition has been initially relaxed in order to illustrate the generality of the problem formulation. Balancedness is imposed in the next section.

[3]The linearity distance property is not explicitly considered in this paper, since it can be directly derived from the absolute indicator, which is more frequently employed in the literature and characterizes the same Boolean function property.

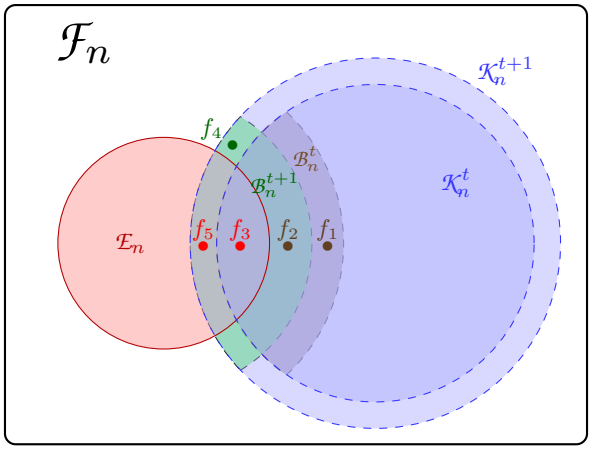

FIG. 1. *Relationship between $\mathcal{E}_n$, $\mathcal{K}_n$, and $\mathcal{B}_n$ at different stages of knowledge. $f_1, f_2, f_3 \in \mathcal{B}_n^t$ (i.e., they are BKPE), when $\mathcal{K}_n^t$ is the set of known functions. Note that, since $f_3 \in \mathcal{E}_n$ (i.e., it is PE, although we may not be aware of that), additional knowledge will not discard it ($f_3 \in \mathcal{B}_n^{t+k}\ \forall k > 0$). On the other hand, when the set of known functions increases to $\mathcal{K}_n^{t+1}$, $f_1 \notin \mathcal{B}_n^{t+1}$ (i.e., it is not BKPE anymore) and $f_2, f_3, f_4, f_5 \in \mathcal{B}_n^{t+1}$, meaning that two new solutions show up: f_4, which eventually will be discarded (together with f_2) as the set of known functions keeps increasing, and f_5, which is PE (together with f_3).*

Furthermore, two common additional criteria in cryptoanalysis, but not so relevant for block cipher design, are the correlation immunity order (t-CI) and the propagation criterion degree ($PC(m)$). These criteria will be considered with less priority, only for tie-breaking purposes, and their notation will be simplified to CI and PC, respectively.

Therefore, we initially define $\mathcal{C} = \mathcal{C}_1 \sqcup \mathcal{C}_2$, where $\mathcal{C}_1 = \{C_1, \dots, C_6\} = \{\text{-}I, NL, deg, AI, \text{-}AC_{\max}, \text{-}\sigma\}$ and $\mathcal{C}_2 = \{C_7, C_8\} = \{CI, PC\}$. Accordingly, the profile $P(f)$ is

$$P(f) = (n|\text{-}I, NL, deg, AI, \text{-}AC_{\max}, \text{-}\sigma|CI, PC), \tag{11}$$

where I stands for the imbalance, NL the nonlinearity, deg the algebraic degree, AI the algebraic immunity, $AC_{\max}$ the absolute indicator, σ the sum-of-squares indicator, CI the correlation immunity order, and PC the propagation criterion degree. When the value of n is obvious from the context, it will be removed from the profile. Note that criteria NL, deg, AI, CI, and PC are to be maximized, whereas I, $AC_{\max}$, and σ are to be minimized (hence, their minus sign in the profile).

As explained above, the selected order for enumerating the profile criteria within each $\mathcal{C}_i, i = 1, 2$, does not indicate any formal priority; nevertheless, in (11) such enumeration has been ordered according to the most common relative importance given to the criteria in the existing literature. Any relative importance of this kind could be formalized by accordingly splitting the corresponding $\mathcal{C}_i, i = 1, 2$, into smaller subsets, so that a new (finer) problem would be posed. (Remember that, according to Lemma 2.7, the solution set of the new problem would be a subset of the solution set of the original problem.)

4.1. Further priority requirements. Frequently, [27, 42, 39, 15, 40, 37, 14] the balancedness criterion is considered preeminent and is required to reach the optimal value ($I = 0$) corresponding to balanced functions, so that we enter the framework

analyzed in section 2.3.2. Hence, the problem is redefined via $\mathcal{C} = \mathcal{C}_1 \sqcup \mathcal{C}_2 \sqcup \mathcal{C}_3$, so that the new *profile* $P(f)$ becomes

$$P(f) = (n|0|NL, deg, AI, \text{-}AC_{\max}, \text{-}\sigma|CI, PC). \tag{12}$$

On the other hand, some authors have considered NL to be preeminent [12, 13, 35, 38, 49] (postponing balancedness). In the following example, we will illustrate results for both the approaches.

4.2. Basic example for $n = 4$. For $n = 4$, it is computationally viable to carry out an exhaustive analysis of $\mathcal{F}_4$ (composed by 2^{2^4} functions). If problems defined by profile $(4|\text{-}I|\dots)$ are considered, the first stage solution set $E_{4,1}$ (which we will call $E_{4,1}(\text{-}I)$) contains 12870 balanced functions ($I = 0$ is attained); obviously none of them is SPE (i.e., $E^o_{4,1}(\text{-}I) = \emptyset$ and $E_{4,1}(\text{-}I) = E^t_{4,1}(\text{-}I)$). On the other hand if we define problems prioritizing nonlinearity (i.e., $\mathcal{C}_1 = \{NL\}$ being the profiles of the form $(4|NL|\dots)$, the corresponding first stage solution set $E_{4,1}$ (redenoted now as $E_{4,1}(NL)$) contains 896 bent functions (i.e., those which attain the maximum nonlinearity, $NL = 6$, that can be attained); again none of them is SPE (i.e., $E^o_{4,1}(NL) = \emptyset$ and $E_{4,1}(NL) = E^t_{4,1}(NL)$). Note that $E_{4,1}(\text{-}I) \cap E_{4,1}(NL) = \emptyset$ since, as is well known, there is no function that is both balanced and bent.

Let us now consider a respective second stage in each of the two types of problems considered above. The problem represented by profile $(4|\text{-}I|NL)$, has a solution set $E_{4,2}$ (which we may call $E_{4,2}(\text{-}I|NL)$), composed of 10920 balanced functions (1950 dominated ones have been neglected in the second stage when breaking the ties with criterion NL) whose profile is $(4|0|4)$. Equivalently, the problem represented by profile $(4|NL|\text{-}I)$ has a solution set (now called $E_{4,2}(NL|\text{-}I)$) composed of the same 896 bent functions (no tie is broken in the second stage with criterion $\text{-}I$), whose profile is $(4|6|-2)$.

Alternatively, if we define a problem that equally prioritizes both balancedness and nonlinearity (i.e., $\mathcal{C}_1 = \{\text{-}I, NL\}$, with profile $(4|\text{-}I, NL)$), the solution set $E_{4,1}(\text{-}I, NL)$ has 20776 functions. From Lemma 2.7, we know that 10920 of them are balanced with profile $(4|0, 4)$, and 896 are bent with profile $(4|-2, 6)$, since all elements of $E_{4,2}(NL|\text{-}I)$ and $E_{4,2}(\text{-}I|NL)$ are in $E_{4,1}(\text{-}I, NL)$ (i.e., they are also PE in this new problem), whereas there are 8960 PE functions that are neither balanced nor bent, with profile $(4|-1, 5)$. Further selection could be performed by considering successive new criteria on these sets of PE functions.

Finally, if we solve the optimization problem corresponding to profile (11) via the procedure indicated in (5), the solution set $E_{4,1}$ (result of first stage, solving wrt the $\mathcal{C}_1 = \{\text{-}I, NL, deg, AI, \text{-}AC_{\max}, \text{-}\sigma\}$) is composed of 19936 functions, where there is no SPE function (i.e., $E^o_{4,1} = \emptyset$ and $E_{4,1} = E^t_{4,1}$), and whose corresponding nondominated set is $N_4 = \{(4|-2, 6, 2, 2, 0, -256|*, *), (4|-1, 5, 4, 2, -4, -496|*, *), (4|0, 4, 3, 2, -8, -640|*, *)\}$ whose elements are associated with 896, 8960, and 10080 functions, respectively (note that $E_{4,1}(\text{-}I, NL, deg, AI, \text{-}AC_{\max}, \text{-}\sigma) \subset E_{4,1}(\text{-}I, NL)$ from which 840 balanced functions have been now discarded). The symbol $*$ indicates that, at this stage, we do not care about criteria in $\mathcal{C}_2$.

When considering the two additional criteria in $\mathcal{C}_2$ (correlation immunity and propagation criterion), ties are broken only in the set of balanced functions. The resulting nondominated set is $N'_4 = \{(4|-2, 6, 2, 2, 0, -256|0, 4), (4|-1, 5, 4, 2, -4, -496|0, 0), (4|0, 4, 3, 2, -8, -640|0, 1)\}$, whose elements are associated with 896, 8960, and 1056 functions, respectively. Note that the second stage optimization has led to a much reduced (sub)set of optimal balanced functions.

TABLE 1
BKPE results for $I = 0$, wrt (NL, deg, AC_{max}) *upon* [36].

	$n = 8$	$n = 9$	$n = 10$	$n = 11$
Kavut and Yücel [36]	$(116, 7, -24)$ $(114, 7, -16)$	$(238, 8, -40)$ $(234, 8, -32)$ $(236, 8, -32)$	$(486, 9, -56)$	$(984, 10, -80)$
Clark et al. [17], [19], [20]	$(116, 7, -24)$ $(112, 5, -16)$	$(238, 8, -40)$	$(486, 9, -72)$ $(484, 9, -56)$	$(984, 9, -96)$ $(982, 10, -88)$

5. Search schemes and results.

5.1. History of some BKPE functions for $n = 8, 9, 11$. Although the formal definition of BKPE is new to the best of our knowledge, such functions have been (implicitly) searched upon by many authors. Kavut and Yücel in [36] addressed the determination of balanced Boolean functions that have good properties wrt the following criteria: high nonlinearity, low autocorrelation, and high algebraic degree. They presented some balanced 8-and 9-variable functions that were the best-known ones in the computer search literature (i.e., they were BKPE according to our definition). Table 1, from [36], compares the best achieved computer search results up to that time.

Note that the results of Kavut and Yücel in [36] proved that some of the profiles provided by Clark et al. [17], [19], [20] were not PE (precisely, the second one for $n = 8$, and all for $n = 10$ and $n = 11$). Later on, Burnett et al. [11] provided the profiles $(8|116, 7, -16)$ and $(10|488, 9, -40)$, showing that the functions presented in [36] were not PE wrt to these three criteria. Kavut and Yücel [36] provide the representation of only one of the 8-input balanced functions (see Appendix A), whose profile (including now all the criteria in $\mathcal{C}_1$ and $\mathcal{C}_2$ of profile (12)) is $P(f) = (8|0|114, 7, 4, -16, -88960)$. Similarly, Burnett et al. [11] provide the representation of only one of the 8-input balanced functions (see Appendix A), whose profile wrt profile (12) is $P(f) = (8|0|116, 7, 3, -16, -89728)$. Hence, both functions (in [11] and [36]) are still BKPE wrt the profile in (12) (note that criteria of $\mathcal{C}_3$ need not be considered since there are no ties in the comparative analysis).

5.1.1. 9-input balanced functions. The case for 9-variable balanced Boolean functions with good profiles was further studied, now taking into account the first stage of the optimization problem defined in profile (12), meaning balanced functions with high nonlinearity, high algebraic degree, high algebraic immunity, low absolute indicator, and low sum-of-squares indicator comprising the preeminent criteria. In [34], results are provided, shown here in Table 2.

TABLE 2
BKPE functions $n = 9$, $I = 0$, *upon* [34].

Authors	profile
Kavut, Maitra, and Yücel [34]	$(240, 7, 4, -24, -354176)$
Saber, Uddin, and Youssef [48]	$(240, 5, 4, -160, -524288)$
Read [47]	$(240, 5, 3, -32, -524288)$
Burnett [10]	$(240, 5, 4, -128, -524288)$
Stanică and Sung [50]	$(240, 2, 2, -512, -524288)$
Misty 1 and KASUMI 9×9 S-box [1]	$(240, 2, 2, -512, -524288)$

TABLE 3
Comparison of profiles with $n = 11$, $I = 0$.

Reference	Profile
[33]	$(992, 5, *, *, *)$
[41]	$(992, 6, *, -240, *)$
[34]	$(988, 10, 5, -56, -5980928), (992, 8, *, -64, *)$
[47]	$(992, 4, 3, -64, -8388608), (992, 5, 3, -96, -8388608)$ $(984, 9, 4, 232, 8514560), (970, 10, 3, -192, -9404288)$
[24]	$(992, 5, 5, *, *)$

Note again that the Kavut, Maitra, and Yücel results in [34] proved that all the profiles provided by other authors or the ones corresponding to the known systems were not PE. (It is worth mentioning that in [11] functions with $(240, 7, *, *, *)$ are obtained, whose resilience degree is 1 as a relevant criterion, but no values for the remaining criteria are provided.)

5.1.2. 11-input balanced functions. Table 3 illustrates further results for 11-variable balanced Boolean functions with good profiles. Note that different authors have considered different criteria sets, limiting the comparison between results. Again, the results of Kavut, Maitra, and Yücel in [34] proved that the profiles provided by Johansson and Passalic [33] and Maximov, Hell, and Maitra [41] were not PE (wrt to the corresponding set of criteria considered in each case). They also proved that the two profiles in the second row provided by Read [47] were not PE either.

5.2. Our search schemes and results for $n = 9, 11$. When problem (2) with no preferences among the criteria (i.e., problem s_0) was considered, a search scheme based on a genetic algorithm and the WSM[4] provided limited results. Although functions with degrees $deg = 8$, 9, and 11 for $n = 8$, 9, and 11, respectively, were found, none of them were balanced and their nonlinearity was below $NL = 112$, 232, and 962, respectively. Hence, despite the fact that these solutions are BKPE (wrt problem (2)) when compared with published results, their applicability in cryptography is very limited due to the practical prioritized relevance among the criteria.

Therefore, we focused on problems of type (5), keeping in mind the practical preferences among criteria. As a general procedure, when addressing a given problem s_{i_1} of type (5), we first solved a problem s_{i_2}, which was computationally more treatable, its solution set $\mathcal{E}(s_{i_2})$ satisfying $\mathcal{E}(s_{i_2}) \subseteq \mathcal{E}(s_{i_1})$, as stated in Lemma 2.7. Thereafter, elements of $\mathcal{E}(s_{i_2})$ were employed as initial starting points for applying different iterative search procedures to problem s_{i_1} in order to find new elements of $\mathcal{E}(s_{i_1})$. Search procedures of this type have already been employed by other authors in a heuristic manner [11].

5.2.1. Hill climbing and derivatives of criteria. If the truth table of f is modified in a single output bit, the corresponding values of several criteria do not change significantly. This fact can be characterized by computing the derivative of the criteria wrt bit changes in the truth table of f. Precisely, a single bit change in the truth table of f leads to a change of one nonlinearity unit and two balancedness units. This fact implies that if a step hill climbing search algorithm is employed, one can

[4]Computations were performed over several months on a cluster of computers using the VBF library [5].

compute a bound on both the nonlinearity and the balancedness differences between the initial and the final elements, depending on the number of performed iterations.

5.2.2. Prioritizing nonlinearity for $n = 9$ functions. The search for 9-input Boolean functions of highest nonlinearity (i.e., the corresponding profile being $P(f) = (9|NL)$) was performed (with the VBF library) by applying a one-step hill climbing search. Millions of Boolean functions were found with maximum known nonlinearity 242 (the same as obtained in [38]), which can be grouped into five different affine equivalence classes [3]. There are some function properties that are invariant under affine equivalence. In fact, the five obtained affine equivalence classes can be identified by invariant properties such as the frequency distribution of the absolute values of the Walsh spectrum and the autocorrelation spectrum. The truth tables of these Boolean functions together with their corresponding frequency distribution of the absolute values of the Walsh spectrum and the autocorrelation spectrum are available at [2].

Using the VBF library, the value of other cryptographic criteria (algebraic degree, algebraic immunity, absolute indicator, and sum-of-squares indicator) was easily computed for each one of these millions of Boolean functions. Since such criteria values are invariant under affine transformations, they take the same value within each class; such values are also provided in [2]. If we consider the profile characteristics of the five classes, four of them are not found to be PE, since they are dominated by a fifth one (our best choice). To the best of our knowledge, this whole set may be PE (i.e., it is BKPE), the profile of its functions being the same as the one provided by Kavut and Yücel [38]. If balancedness is considered as a tie-breaking criterion, Kavut's function weight is 250 (6 steps away from balancedness), whereas function f_1 with weight 254 and function f_2 with weight 258 (2 steps away from balancedness) were found in our set with profile $P(f_1) = P(f_2) = (9|-2|242, 7, 4, -32, -324608)$ (see Appendix A for their hexadecimal representation). Hence, the function provided by Kavut's would not be BKPE anymore.

In the following sections, 5.2.3 and 5.2.4, balancedness is prioritized, and the profile $P(f) = (n|0|NL, deg, AI, \text{-}AC_{\max}, \text{-}\sigma)$ is considered for comparative purposes along with existing results.

5.2.3. Prioritizing balancedness for $n = 9$ functions. Looking back to balancedness, an ad hoc one-step iteration was applied to the functions we already had with nonlinearity 242, whose unbalancedness was $I = 2$. Changing only two bits in order to obtain balanced Boolean functions guarantees that the resulting nonlinearity is either greater than or equal to than 240. A detailed description of the ranges of the values obtained for the different criteria can be seen in [2]. Here, we show several examples of balanced Boolean functions with BKPE profiles:

- $P(f_3) = (9|0|240, 8, 4, -24, -339200)$ with hexadecimal representation shown in Appendix A. Note that by obtaining this profile, we have proved that the profile provided by Kavut, Maitra, and Yücel [34] is not PE.
- $P(f_4) = (9|0|240, 8, 5, -40, -347648)$ with hexadecimal representation shown in Appendix A.

5.2.4. Prioritizing balancedness for $n = 11$ functions. The same algorithm was executed to obtain balanced Boolean functions for $n = 11$, and a detailed description of the ranges of values obtained for the different criteria can be seen in [2]. Two examples of balanced Boolean functions with BKPE profiles are $P(f_5) =$

TABLE 4
Comparison of the best results for $(NL, deg, AI, AC_{max}, \sigma)$.

Results	$(NL, deg, AI, AC_{max}, \sigma)$ for	
	$n = 9,\ I = 0$	$n = 11,\ I = 0$
Kavut, Maitra, and Yücel [36], [34]	$(238, 8, *, -40, *)$ $(240, 7, 4, -24, -354176)$	$(984, 10, *, -80, *)$ $(988, 10, 5, -56, -5980928)$ $(992, 8, *, -64, *)$
This paper	$(240, 8, 4, -48, -323456)$ $(240, 8, 4, -32, -323840)$ $(240, 8, 4, -24, -339200)$ $(240, 8, 5, -40, -347648)$	$(992, 10, 5, -120, -5309312)$ $(992, 10, 5, -128, -5255168)$ $(992, 10, 5, -168, -5253632)$ $(992, 10, 5, -224, -5244800)$

$(11|0|992, 10, 5, -120, -5309312)$ and $P(f_6) = (11|0|992, 10, 5, -168, -5253632)$, with hexadecimal representations shown in Appendix A.

In Table 4, we compare the profiles of these functions with the best profiles for balanced Boolean functions obtained for $n = 9$ and $n = 11$.

5.3. Discussion. The new BKPE Boolean functions obtained satisfy the following:

- For $n = 9$, they are the *only* BKPE existing functions, since they dominate all the functions provided by other authors. (Remember that the functions provided in Kavut, Maitra, and Yücel [36], [34] discarded all alternative proposals, and now, we have discarded Kavut's functions by proving that they were not PE either).
- For $n = 11$, they provide better values for criteria $(NL, deg, AI, \text{-}\sigma)$ and worse values for $\text{-}AC_{max}$. In general, (NL, deg) are considered to be more relevant than $-AC_{max}$. Hence, the obtained BKPE functions would dominate the solutions found in [36], [34] for any problem of type (5) with associated profile $\mathcal{P} = (11| - I|(NL, deg)|\ldots)$.

6. Concluding remarks. The proposed formalization of the selected criteria and their relative relevance via a family of MOCO problems has been proven to be useful for rigorously defining, characterizing, and addressing the design of optimal Boolean functions for robust block cipher design. This new framework may especially help for a more systematic comparison of the different functions provided in the existing literature.

The successful determination of new BKPE functions suggests that alternative search algorithms will also be easily and profitably applicable within this framework.

Appendix A. Hexadecimal representations.

- f from [36] such that $P(f) = (8|0|114, 7, 4, -16, -88960)$:

  $149016cdd1931f10860b4b8becef5557b8177a8565229b775e08f97b7692c32d.$

- f from [11] such that $P(f) = (8|0|116, 7, 3, -16, -89728)$:

  $7eb4719b4da742a8bbe124ce18fa17fd7e6b716c4d58c2572b3e3431180d1702.$

- f_1 such that$P(f_1) = (9| - 2|242, 7, 4, -32, -324608)$ with weight 254:

  $b80170795f932563fad9532b2e44b87b70a73d66beac2304802094fcb858f154a41$
  $810df91877a17c930be0da9f5efebce85993c2be0b42c63b25ec1dea3abaa.$

- f_2 such that $P(f_2) = (9|-2|242, 7, 4, -32, -324608)$ with weight 258:

  $b7f18076af9c2a930ad65cdb21b4487480a83296b15cd30b8fd064f34857fea454$
  $171f2f9e778a18c6c04e0259fae01bc1756933dbefbbdc93bd5131d1535ba5.$

- f_3 such that $P(f_3) = (9|0|240, 8, 4, -24, -339200)$:

  $115bd52305367fc6a07c098e8b1e1d21d5fd983ce40979a1da85ce591d02540efe$
  $bd4a7a34dddf4d6c6a1b57f350b54e9420c3998eba1176c6e8fb9b8406f10f.$

- f_4 such that $P(f_4) = (9|0|240, 8, 5, -40, -347648)$:

  $1de90d23b5024350f57f9f6020396aa70b8775b1ccb4c9b01dec1d00b6435a0e631$
  $4f2d55afcfd3955df9b7383dc69f1c786b9a0cc91daae7529a9323d274047.$

- f_5 such that $P(f_5) = (11|0|992, 10, 5, -120, -5309312)$:

  $037788777877838887788787888778787788888787787778777887787778788877$
  $888787787777878787888788878787377777777888778887787788887877877877777$
  $878877878788778888788788888778787877777888778778887787787777877877888$
  $877887777878788877887888787887788787778787887778887778878887788888$
  $787887777887777888778788888787877788788878877788787877777878878787777$
  $777787787877788877878788878877777777887787878778778887888887878777$
  $878888888878888877778887778888878878777787877788787788787777778887$
  $788877788888888777877877778788788888887777887.$

- f_6 such that $P(f_6) = (11|0|992, 10, 5, -168, -5253632)$:

  $fcb4b4bb4bbb4b44bb4b44bb444b44cb4bb444bbbbbbb44444bb444b444444b4b44bbb4$
  $444bb444b4bbb4b4b4bb4b4b44b4b444bbbb44b4b4b4bb44b44b4b44bbb44444bb4444b$
  $4b4444b4bbb444444bb444b4b4bbb4b44b444bbbbb4b44bbbbb4444bb4bbb44b4bbbbb44$
  $b444bb444b444b444b4b4b44bb444bbb44bbb44bbb4bbb4b44b44bbb44bb4bbbbb4444bb$
  $4bb4444bb4b4b4b4bb4444b4444bbb44b4cb44bbbb4b4b4b444b44bb4444bb44bbbbbb4b$
  $bb444bb4444b44444b44b444bb4b4bb44b444bbbbbbb4bb4bbb4b4b4b4bb4bbb4bb44b4b$
  $b4b4444bb44b444444b4bb4b4bb44bbbbbbbbbb444b4b4bb4b44bbb4bb4bb4b4bbbbb44bb$
  $b44b4bbb4.$

Acknowledgment. The authors thank the anonymous referees for their constructive comments and suggestions.

REFERENCES

[1] *Specification of the 3GPP Confidentiality and Integrity Algorithms—Document 2: Kasumi Specification (Release 6) no. 3gpp ts* 35.202 v6.1.0 (2005-09), Tech. report, 3rd Generation Partnership Project, 2005.

[2] J. A. Álvarez-Cubero, *Analysis of Cryptographic Algorithms*, http://vbflibrary.tk (2014).

[3] J. A. Álvarez-Cubero, *Vector Boolean Functions: Applications in Symmetric Cryptography*, Ph.D. thesis, Universidad Politécnica de Madrid, Spain, 2015.

[4] J. A. Álvarez-Cubero and P. J. Zufiria, *Cryptographic criteria on vector boolean functions*, in Cryptography and Security in Computing, J. Sen. ed., InTech, 2012, pp. 51–70; http://www.intechopen.com/books/cryptography-and-security-in-computing/cryptographic-criteria-on-vector-boolean-functions.

[5] J. A. Álvarez-Cubero and P. J. Zufiria, *Algorithm* 959: *VBF: A library of C++ classes for vector Boolean functions in cryptography*, ACM Trans. Math. Softw., 42 (2016), pp. 16:1–16:22, http://dx.doi.org/10.1145/2794077.

[6] E. Bonacker, A. Gibali, K.-H. Küfer, et al., *Speedup of lexicographic optimization by superiorization and its applications to cancer radiotherapy treatment*, Inverse Problems, 1 (2016), http://dx.doi.org/10.1088/1361-6420/33/4/044012.

[7] J. Branke, *Consideration of partial user preferences in evolutionary multiobjective optimization*, in Multiobjective Optimization, Lecture Notes in comput. Sci. 5252, Springer, New York, 2008, pp. 157–178, http://dx.doi.org/10.1007/978-3-540-88908-3_6.

[8] J. Branke and K. Deb, *Integrating user preferences into evolutionary multi-objective optimization*, in Knowledge Incorporation in Evolutionary Computation, Stud. Fuzziness soft. Comput. 167, Springer, New York, 2005, pp. 461–477, http://dx.doi.org/10.1007/978-3-540-44511-1_21.

[9] J. Branke, K. Deb, K. Miettinen, and R. Slowiński, *Multiobjective Optimization: Interactive and Evolutionary Approaches*, Lecture Notes in Comput. Sci. 5252, Springer, New York, 2008, http://dx.doi.org/10.1007/978-3-540-88908-3.

[10] L. Burnett, *Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography*, Ph.D. thesis, Queensland University of Technology, Australia, 2005.

[11] L. Burnett, W. Millan, E. Dawson, and A. Clark, *Simpler methods for generating better boolean functions with good cryptographic properties*, Australas. J. Combin., 29 (2004), pp. 231–247.

[12] C. Carlet, *On the secondary constructions of resilient and bent functions*, in Coding, Cryptography and Combinatorics, Progr. Comput. Sci. Appl. Logic 23, Birkhäuser Boston, Boston, MA, 2004, pp. 3–28, http://dx.doi.org/10.1007/978-3-0348-7865-4_1.

[13] C. Carlet, H. Dobbertin, and G. Leander, *Normal extensions of bent functions*, IEEE Trans. Inform. Theory, 50 (2004), pp. 2880–2885, http://dx.doi.org/10.1109/TIT.2004.836681.

[14] C. Carlet and K. Feng, *An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity*, in ASIACRYPT 2008, J. Pieprzyk, ed., Lecture Notes in Comput. Sci. 5350, Springer, Berlin, 2008, pp. 425–440, http://dx.doi.org/10.1007/978-3-540-89255-7_26.

[15] C. Carlet and P. Gaborit, *On the construction of balanced boolean functions with a good algebraic immunity*, in Proceedings of the International Symposium on Information Theory, 2005, pp. 1101–1105, http://dx.doi.org/10.1109/ISIT.2005.1523510.

[16] J. H. Chung, P. Stănică, C. H. Tan, and Q. Wang, *Construction of boolean functions with good cryptographic properties*, Int. J. Comput. Math., 92 (2015), pp. 700–711, http://dx.doi.org/10.1080/00207160.2014.920085.

[17] J. Clark and J. Jacob, *Two-stage optimisation in the design of boolean functions*, in Information Security and Privacy, ACISP 2000, Lecture Notes in Comput. Sci. 1841, Springer, New York, 2000, pp. 242–254, http://dx.doi.org/10.1007/10718964_20.

[18] J. Clark, J. Jacob, S. Maitra, and P. Stănică, *Almost boolean functions: The design of boolean functions by spectral inversion*, Comput. Intell., 20 (2004), pp. 450–462, https://doi.org/10.1111/j.0824-7935.2004.00245.x.

[19] J. Clark, J. Jacob, S. Stepney, S. Maitra, and W. Millan, *Evolving boolean functions satisfying multiple criteria*, in Progress in Cryptology—INDOCRYPT 2002, Lecture Notes in Comput. Sci. 2551, A. Menezes and P. Sarkar, eds., Springer, Berlin, 2002, pp. 246–259, http://dx.doi.org/10.1007/3-540-36231-2_20.

[20] J. Clark, *Metaheuristic Search as a Cryptological Tool*, Ph.D. thesis, University of York, 2001, https://books.google.es/books?id=_TtWnQEACAAJ.

[21] C. A. C. Coello, G. B. Lamont, D. A. Van Veldhuizen, et al., *Evolutionary Algorithms for Solving Multi-Objective Problems*, Genet. Evol. Comput. Ser. 5, Springer, New York, 2007, http://dx.doi.org/10.1007/978-0-387-36797-2.

[22] C. C. Coello, *Handling preferences in evolutionary multiobjective optimization: A survey*, in Proceedings of the 2000 Congress on Evolutionary Computation, Vol. 1, IEEE, 2000, pp. 30–37, http://dx.doi.org/10.1109/CEC.2000.870272.

[23] D. Cvetković and C. A. C. Coello, *Human preferences and their applications in evolutionary multiobjective optimization*, in Knowledge Incorporation in Evolutionary Computation, Stud. Fuzziness Soft. Comput. 167, Springer, New York, 2005, pp. 479–502, http://dx.doi.org/10.1007/978-3-540-44511-1_22.

[24] D. K. Dalai, K. C. Gupta, and S. Maitra, *Results on algebraic immunity for cryptographically significant boolean functions*, in Progress Cryptology—INDOCRYPT, Lectore Notes in Comput. Sci. 3348, Springer, New York, 2004, pp. 92–106, http://dx.doi.org/10.1007/978-3-540-30556-9_9.

[25] I. Das, *A preference ordering among various pareto optimal alternatives*, Struct. Optim., 18 (1999), pp. 30–35, https://doi.org/10.1007/BF01210689.

[26] F. di Pierro, S.-T. Khu, and D. A. Savic, *An investigation on preference order ranking scheme for multiobjective evolutionary optimization*, IEEE Trans. Evolutionary Comput., 11 (2007), pp. 17–45, https://doi.org/10.1109/TEVC.2006.876362.

[27] H. Dobbertin, *Construction of bent functions and balanced boolean functions with high nonlinearity*, in Fast Software Encryption, Lecture Notes in Comput. Sci. 1008, Springer, New York, 1994, pp. 61–74, https://doi.org/10.1007/3-540-60590-8_5.

[28] M. Ehrgott, *Multicriteria Optimization*, Springer, New York, 2006, http://dx.doi.org/10.1007/3-540-27659-9.

[29] G. Eichfelder, *Scalarizations for adaptively solving multi-objective optimization problems*, Comput. Optim. Appl., 44 (2009), p. 249, https://doi.org/10.1007/s10589-007-9155-4.

[30] J. W. Fowler, E. S. Gel, M. M. Köksalan, P. Korhonen, J. L. Marquis, and J. Wallenius, *Interactive evolutionary multi-objective optimization for quasi-concave preference functions*, European J. Oper. Res., 206 (2010), pp. 417–425, https://doi.org/10.1016/j.ejor.2010.02.027.

[31] A. M. Geoffrion, *Proper efficiency and the theory of vector maximization*, J. Math. Anal. Appl., 22 (1968), pp. 618–630, https://doi.org/10.1016/0022-247X(68)90201-1.

[32] J. Jahn, *Vector Optimization*, Springer, New York, 2009, https://doi.org/10.1007/978-3-642-17005-8.

[33] T. Johansson and E. Pasalic, *A construction of resilient functions with high nonlinearity*, IEEE Trans. Inform. Theory, 49 (2003), pp. 494–501, https://doi.org/10.1109/TIT.2002.807297.

[34] S. Kavut, S. Maitra, and M. Yücel, *Autocorrelation spectra of balanced boolean functions on an odd number of input variables*, in Proceedings of BFCA'06 Conference, 2006, Rouen, France, J.-F. Michon, P. Valarcher, and J.-B. Yunès, eds., 2006, pp. 73–86.

[35] S. Kavut, S. Maitra, and M. D. Yücel, *Search for boolean functions with excellent profiles in the rotation symmetric class*, IEEE Trans. Inform. Theory, 53 (2007), pp. 1743–1751, http://dblp.uni-trier.de/db/journals/tit/tit53.html#KavutMY07.

[36] S. Kavut and M. D. Yücel, *Improved cost function in the design of boolean functions satisfying multiple criteria*, in Progress in Cryptology—INDOCRYPT 2003, Lecture Notes in Comput. Sci. 2904, T. Johansson and S. Maitra, eds., Springer, Berlin, 2003, pp. 121–134, https://doi.org/10.1007/978-3-540-24582-7_9.

[37] S. Kavut and M. D. Yücel, *Balanced Boolean Functions with Nonlinearity* $> 2^{n-1} - 2^{(n-1)/2}$, IACR Cryptology ePrint Archive, http://eprint.iacr.org/2007/321, 2007.

[38] S. Kavut and M. D. Yücel, 9*-variable boolean functions with nonlinearity* 242 *in the generalized rotation symmetric class*, Inf. Comput., 208 (2010), pp. 341–350, https://doi.org/10.1016/j.ic.2009.12.002.

[39] S. Maitra, *Highly nonlinear balanced boolean functions with good local and global avalanche characteristics*, Inform. Process. Lett., 83 (2002), pp. 281–286, https://doi.org/10.1016/S0020-0190(02)00207-7.

[40] S. Maitra, *Balanced Boolean Function on* 13*-Variables Having Nonlinearity Strictly Greater Than the Bent Concatenation Bound*, IACR Cryptology ePrint Archive, http://dblp.uni-trier.de/db/journals/iacr/iacr2007.html#Maitra07, 2007.

[41] A. Maximov, M. Hell, and S. Maitra, *Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables*, IACR Cryptology ePrint Archive, http://eprint.iacr.org/2004/144, 2004.

[42] W. Millan, A. Clark, and E. Dawson, *Heuristic design of cryptographically strong balanced boolean functions*, in EUROCRYPT, 1998, pp. 489–499, https://doi.org/10.1007/BFb0054148.

[43] S. Murphy, *Description of Methodology for Security Evaluation*, Tech. report NES/DOC/RHU/WP3/D10/3, European Commission, 2002.

[44] *Data Encryption Standard*, National Bureau of Standards U.S. Department of Commerce, Washington, DC, 1977.

[45] *Advanced Encryption Standard*, National Institute for Standards and Technology U.S. Department of Commerce, Washington, DC, 2001.

[46] L. Rachmawati and D. Srinivasan, *Preference incorporation in multi-objective evolutionary algorithms: A survey*, in IEEE International Conference on Evolutionary Computation, 2006, pp. 962–968, https://doi.org/10.1109/CEC.2006.1688414.

[47] M. Read, *Explicable Boolean Functions*, Ph.D. thesis, University of York, UK, 2007.
[48] Z. Saber, M. Uddin, and A. Youssef, *On the existence of $(9, 3, 5, 240)$ resilient functions*, IEEE Trans. Inform. Theory, 52 (2006), pp. 2269–2270, https://doi.org/10.1109/TIT.2006.872862.
[49] P. Stănică, T. Martinsen, S. Gangopadhyay, and B. K. Sing, *Bent and generalized bent boolean functions*, Designs Codes Cryptography, 69 (2013), pp. 77–94, https://doi.org/10.1007/s10623-012-9622-5.
[50] P. Stănică and S. H. Sung, *Improving the nonlinearity of certain balanced boolean functions with good local and global avalanche characteristics*, Inform. Process. Lett., 79 (2001), pp. 167–172, https://doi.org/http://dx.doi.org/10.1016/S0020-0190(00)00221-0.
[51] D. Tang, C. Carlet, and X. Tang, *Highly nonlinear boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks*, IEEE Trans. Inform. Theory, 59 (2013), pp. 653–664, https://doi.org/10.1109/TIT.2012.2217476.
[52] Q. Wang, C. Carlet, P. Stănică, and C. H. Tan, *Cryptographic properties of the hidden weighted bit function*, Discrete Appl. Math., 174 (2014), pp. 1–10, https://doi.org/10.1016/j.dam.2014.01.010.
[53] Y. Wang and Y. Yang, *Particle swarm optimization with preference order ranking for multi-objective optimization*, Inform. Sci., 179 (2009), pp. 1944–1959, https://doi.org/10.1016/j.ins.2009.01.005.
[54] X. Zeng, C. Carlet, J. Shan, and L. Hu, *More balanced boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks*, IEEE Trans. Inform. Theory, 57 (2011), pp. 6310–6320, https://doi.org/10.1109/TIT.2011.2109935.
[55] E. Zitzler, *Evolutionary Algorithms for Multiobjective Optimization: Methods and Applications*, 1999.