Perfect nonlinear S-boxes on the real-line

Laurent Poinsot

Université du Sud Toulon-Var
Institut des Sciences de l'Ingénieur de Toulon et du Var
Laboratoire Systèmes Navals Complexes
BP 56
83 162 La Valette du Var
France

poinsot@univ-tln.fr

Abstract

The objective of this contribution is to introduce an analogue to the classical secret-key block ciphers, such as DES, IDEA or AES, in the nondenumerable setting, namely where cleartexts, plaintexts and keys are real numbers. The nonlinear part of traditional secret-key block ciphers, the S-boxes, is designed to provide *confusion i.e.* to resist to several kind of cryptanalysis such as algebraic, differential or linear attacks. By analogy we construct S-boxes in the uncountable setting which provide the best resistance to a classical or modified version of the differential attack. Since our S-boxes are real-valued functions defined on the real-line, we also need to prevent possible new attacks based on real analysis (such as continuity and derivability), which are ignored since impossible in the finite case: we must hide the topological structure. So we introduce a new kind of *Discontinuous*-boxes for this purpose.

Keywords: S-boxes, differential attack, perfect nonlinear functions, group actions, topological groups and transfinite cardinal numbers.

1 Introduction and purpose of this contribution

In a classical block cipher, plaintexts, ciphertexts and keys are treated as bit-strings of finite sizes. The finiteness of lengths is obviously due to implementation and practical requirements. Nevertheless from a mathematical and theoretical point of view, there are less reasons to restrict ourselves to this finite case. In other words one can imagine ideal cryptosystems that deal with some infinite size quantities such as for instance real numbers rather than binary vectors. This unrestricted approach can lead to new and relevant idealized results by using some real analysis tools rather than our usual discrete mathematics toolbox. Obviously such formal realizations need to be interpreted when they are projected onto the finite framework, for instance as asymptotical results. This step is far from obvious and must be carried out with caution since one may lose a large (and even infinite) number of degrees of freedom when restricting to the finite universe. This approach is not usual in the theory of secret-key cryptosystems but is well-known and efficient for public-key cryptologists. Indeed a popular methodology for designing cryptographic protocols consists of the following two steps. One first designs an ideal system in which all parties (including the adversary) have oracle access to a truly random function, and proves the security of this ideal system. Next, one replaces the random oracle by a « good cryptographic hashing function » (such as MD5 or SHA), providing all parties (including the adversary) with the succinct description of this function. Thus, one obtains an implementation

of the ideal system in a « real-world » where random oracles do not exist. This methodology, explicitly formulated by Bellare and Rogaway in [3], which is called the *random oracle model*, has been used in many works and allows to consider ideal hash functions that map infinite bit-strings to bit-strings of fixed finite length. Apart from pathological protocols (see [7]) which are secure in the random oracle model but which any implementation of the random oracle results in insecure schemes, this method seems to be enough efficient to obtain relevant proofs of security. Moreover some secret-keys cryptosystems over real numbers, called *chaos-based cryptosystems* have already been studied ([11, 12, 22, 14]). Their security is relied on ergodic and chaotic properties rather than algebraic ones. Ergodicity means from a cryptographic point of view that the output has the same distribution for any input and the term « chaos » refers to a sensitivity to the initial conditions: a small deviation in the input can cause a large change at the output. In this paper we do not study such notions since our ambition is to extend the classical notion of resistance against the differential attack, namely the property of perfect nonlinearity, to the case of real (or complex) numbers.

In this contribution we consider an ideal mathematical world in which every parties are able to compute and store real (or complex) numbers. We provide several secret-key cryptosystems that we prove secure against differential attacks. More precisely we exhibit real-valued S-boxes defined on the real-line that are maximally resistant to a **generalized differential cryptanalysis**. The classical differential attack, as introduced by Biham and Shamir [4], takes advantage on an additive difference in output of a S-box for a fixed additive difference in input (the addition is usually given by a XOR operation on bit-strings or an addition in a cyclic or abelian finite group). But there are many other ways to define a « difference » for plaintexts, keys and ciphertexts: for instance in a field, we can consider both additive and multiplicative differences. More generally we can define differential attacks based on the notion of group actions (see [16, 17, 18]). Thus we need to construct S-boxes that are resistant against such new attacks; these maps are called *G-perfect nonlinear functions* (similar to classical perfect nonlinear functions with one XOR replaced by a general group action). In short we provide in this paper several real-valued S-boxes defined on the real-line which are maximally resistant against a multiplicative or additive version of the differential attack.

Outline

Our objective is the construction of S-boxes defined and valued on real numbers that are maximally resistant to a group action based differential attack. The achievement of this purpose is obtained in three steps: first we introduce the generalized version of the differential attack (roughly speaking the XOR operation is replaced by some general group actions) and its corresponding notion of resistance (called *G-perfect nonlinearity*) in the finite framework (see subsection 2.1). In a second step, in subsection 2.2, we extend the concept of G-perfect nonlinear functions for real-valued maps defined on the real-line. Finally in section 3 several G-perfect nonlinear S-boxes defined and valued on the real-line are presented and organized into ideal secret-key encryption schemes. We also introduce some nowhere continuous components for these cryptosystems, called **D-boxes**, in order to prevent topological attacks.

2 Group action version of perfect nonlinearity

2.1 The finite framework

In an r-round iterative block cipher such as the Data Encryption Standard (DES) [9] or its successor as an American standard, the Advanced Encryption Standard (AES) [10], the ciphertext

x_r is obtained from a plaintext x_0 by iterating r times the round function T

$$y = T(x_{i-1}, k_i)\ 1 \leq i \leq r$$

where k_i is the ith round key obtained from a secret quantity (the secret key) by a scheduling algorithm. Following Shannon's design recommendations [20] of diffusion and confusion, the round function is traditionnally divided into two parts. Its *linear* component should provide a good level of diffusion *i.e.* it may distribute the statistics of single or several input symbols of a plaintext into long sequences of output symbols of the corresponding ciphertext. Usually, in an iterative round scheme, linear functions are used for this purpose. Confusing the algebraic relations between plaintexts, ciphertexts or keys means to destroy or hide the mathematical structures. The *nonlinear* part of T is designed to provide this *confusion*. In most cases this is satisfied by using substitutions over the set of ciphertexts: nonlinear components are then called *S(ubstitution)-boxes*. In practice (when we consider blocks as bit-strings), an S-box f is used after the linear part and a XOR combination between an internal message (or a part of it) and the round-key (or a part of it)

$$y = f(k_i \oplus x_{i-1})$$

where the symbol «$\oplus$» denotes the XOR operation. The S-boxes are in fact designed to be resistant against last-round key attacks that try to recover the last-round key. In particular the distribution of the output (additive) differences $f(\alpha \oplus x) \oplus f(x)$ must be as close as possible to the uniform distribution for any nonzero input difference α. If it is not the case, Biham and Shamir's differential attack [4] may take advantage on the resulting bias. One uses XOR differences in a differential attack because this is exactly the way keys and plaintexts are combined and one wants to control the key influence on the differences propagation into the round sequence.

However the key can operate on the message in many other fashions. This is not a new remark since for instance Lai and Massey's IDEA [13] makes use of an addition and multiplication of a ring of modular integers. Moreover in the Russian analogue of DES, GOST [21], keys and plaintexts are combined via an addition of a cyclic group. Our own idea, which has been introduced in [16, 17, 18], consits in replacing the internal law of a group by a particular external law: a group action.

Definition 1. Let G be a group and X be any nonempty set. The group G *acts on* X if there is a group homomorphism ϕ from G to $S(X)$ the symmetric group of X (*i.e.* the set of bijective maps of X equipped with the composition); ϕ is called a *group action*. The action is called *faithful* if ϕ is one-to-one.

In order to simplify the notations, we forget any explicit reference to ϕ by using the convenient notation

$$\alpha.x := \phi(\alpha)(x)$$

with $x \in X$ and $\alpha \in G$. Thus the symbol «.» can be interpreted as an external law of composition.

Definition 2. A *topological group* is a group G which is a Hausdorff topological space such that the multiplication $(g, g') \mapsto gg'$ is a continuous function from $G \times G$ to G and the inverse function $g \mapsto g^{-1}$ is continuous from G to itself. A *homomorphism* between two topological groups G and H is just a continuous group homomorphism from G to H. An *isomorphism* of topological groups is a group isomorphism which is also a homeomorphism for the underlying topological spaces.

For instance, $(\mathbb{R}, +, 0)$ and $(\mathbb{C}, +, 0)$ with their natural topology are topological groups. $(\mathbb{R}^*, \times, 1)$ and $(\mathbb{C}^*, \times, 1)$ with their usual topology (as open of respectively $\mathbb{R}$ and $\mathbb{C}$) are topological groups.

Definition 3. If G is a topological group and X a nonempty topological space, we define a *topological group action* of G on X as a continuous group homomorphism $\phi : G \to Homeo(X)$, where $Homeo(X)$ is the homeomorphism group[1] of X.

As instances of (topological) group actions one can cite the following. $(\mathbb{R}^*, \times, 1)$ acts faithfully on $\mathbb{R}$ by $\alpha.x = \alpha \times x$ and $(\mathbb{R}, +, 0)$ acts regularly[2] (and thus faithfully) on itself by $\alpha.x = \alpha + x$. Moreover if G is a nontrivial subgroup of $(\mathbb{R}^*, \times, 1)$ (for instance $(\{\pm 1\}, \times, 1)$, $]0; +\infty[$ or also $(\mathbb{K}^*, \times, 1)$ when $\mathbb{K}$ is a subfield of $\mathbb{R}$ such as $\mathbb{Q}$) G acts faithfully on the nonzero real numbers by multiplication. In the same way, if G is a nontrivial additive subgroup of $\mathbb{R}$ (so G must be either closed in the usual topology of $\mathbb{R}$, and then must have the form $\alpha\mathbb{Z}$ for a nonzero real number α, or a dense part of $\mathbb{R}$ such as $\mathbb{Q}$) acts faithfully on the real line by addition.

Now let suppose that we keep the same simple block ciphers previously described in which we replace the XOR by a faithful group action of a finite group G on a finite set X. Let H be any finite group, written additively. In this setting, an S-box is a map f from X to H that is used in the encryption scheme in the following way

$$y = f(\alpha.x)$$

where $y \in H$, $\alpha \in G$ and $x \in X$. This kind of modified ciphers may be vulnerable to a differential attack that does no more take advantage on a XOR difference but on a group action difference (that is the most natural notion of difference occurring in this context). The algorithm of such an attack is easily derivated from the classical one.

1. Suppose that the enemy finds a pair (α, β) so that the probability

   $$Pr(R(\alpha.x) - R(x) = \beta)$$

   is far from the uniform distribution, where R is the *reduced cipher* defined as $R = T_{k_1} \circ \ldots \circ T_{k_{r-1}}$ (with the fixed-key round function $T_k : x \mapsto T(x, k)$ one-to-one and onto).
2. The enemy chooses a cleartext x_0 and he encrypts both x_0 and $\alpha.x_0$. Two pairs of plaintexts/ciphertexts are obtained: (x_0, x_r) and $(\alpha.x_0, x'_r)$.
3. He finds all the rth round keys K so that

   $$T_K^{-1}(x'_r) - T_K^{-1}(x_r) = \beta \ .$$

4. He iterates steps (3) and (4) until he is able to distinguish the good value K for the last key k_r.

In order to construct a differential resistant round function f, we need to use differential resistant S-boxes called *G-perfect nonlinear functions* [16, 17, 18].

Definition 4. Let X and Y be two finite nonempty sets. A function $f : X \to Y$ is called *balanced* if for each $y \in Y$, $|\{x \in X | f(x) = y\}| = \frac{|X|}{|Y|}$.

Such a balanced function is obviously onto.

[1] The topology of $Homeo(X)$ is the topology of simple convergence.

[2] An action $\phi : G \to S(X)$ is called *regular* if for each $(x, y) \in X^2$ there is one and only one $\alpha \in G$ so that $\alpha.x = y$. Such an ation is always faithful.

Definition 5. Let G be a finite group that acts faithfully on a finite nonempty set X and H be any finite group (written additively). A function $f : X \to H$ is called *G-perfect nonlinear* if for each nonidentity element α in G, the *derivative of f in α*

$$\begin{array}{rccc} d_\alpha f : & X & \to & H \\ & x & \mapsto & f(\alpha.x) - f(x) \end{array}$$

is balanced.

When $X = G$, G-perfect nonlinear functions are exactly the classical perfect nonlinear functions as introduced by Nyberg in [15].

Our objective in this contribution is to construct a cryptosystem on real numbers that is optimally resistant against a differential attack. So we need to adapt the previous definitions to the infinite countable or uncountable setting.

2.2 The infinite framework

In order to deal with infinite cardinalities, we introduce the following notations. The *(transfinite) cardinal number* of $X \subseteq \mathbb{R}$ (or $\mathbb{C}$) is defined as

$$|X| := \begin{cases} \text{the number of elements of } X \text{ when } X \text{ is a finite set;} \\ \aleph_0 \text{ if } X \text{ is infinite countable;} \\ 2^{\aleph_0} \text{ if } X \text{ has the power of the continuum.} \end{cases}$$

A set X is *infinite countable* if there is a bijection from X to $\mathbb{N}$ and X has the *power of the continuum* if X and $\mathbb{R}$ are equipotent. For instance $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$ (read « aleph zero ») and $|[0;1]| = |\mathbb{R}| = |\mathbb{C}| = 2^{\aleph_0}$. If there is a one-to-one map from X to Y we define $|X| \leq |Y|$ and if there is a one-to-one map from X to Y but no bijective functions, we define $|X| < |Y|$. Then $\mathbb{N} \cup \{\aleph_0, 2^{\aleph_0}\}$ is totally ordered. In particular if $n \in \mathbb{N}$, we have $n < \aleph_0 < 2^{\aleph_0}$. The classical arithmetical operations on finite cardinal numbers can be extended to deal with transfinite cardinal numbers (see [2]). Let $\mathfrak{c}_1$ and $\mathfrak{c}_2$ be two cardinal numbers then we have

$$\mathfrak{c}_1 + \mathfrak{c}_2 := \begin{cases} \max\{\mathfrak{c}_1, \mathfrak{c}_2\} & \text{if either } \mathfrak{c}_1 \text{ or } \mathfrak{c}_2 \text{ is infinite;} \\ \mathfrak{c}_1 + \mathfrak{c}_2 & \text{if both } \mathfrak{c}_1 \text{ and } \mathfrak{c}_2 \text{ are finite.} \end{cases}$$

In particular $+$ is associative, commutative and has 0 as neutral element. Similarly we can define a multiplication of transfinite cardinals[3] that extends the usual integer multiplication:

$$\mathfrak{c}_1\mathfrak{c}_2 := \max\{\mathfrak{c}_1, \mathfrak{c}_2\}$$

if either $\mathfrak{c}_1$ or $\mathfrak{c}_2$ are infinite and both are non zero. In particular $2^{\aleph_0} = 2^{\aleph_0}2^{\aleph_0} = 2^{\aleph_0}\aleph_0 = 2^{\aleph_0}n$ and $\aleph_0 = \aleph_0\aleph_0 = \aleph_0 n$ for each $n \in \mathbb{N}^*$. Moreover one can show that $\mathfrak{c}0 = 0\mathfrak{c} = 0$, 1 is the neutral element, the multiplication is associative, commutative, distributive over $+$ and there is no zero divisors. Moreover the following inequality holds

$$\sum_{i \in I} \mathfrak{c}_i \leq \max\{\mathfrak{c}_i\}_{i \in I} |I|$$

for $\mathfrak{c}_i \in \mathbb{N} \cup \{\aleph_0, 2^{\aleph_0}\}$ and $0 \leq |I| \leq 2^{\aleph_0}$.

Using these numbers one can extend the notion of balanced functions for infinite cardinalities. If X and Y are two finite sets so that $|Y|$ divides $|X|$, a function $f : X \to Y$ is balanced if for each $y \in Y$, the inverse image $f^{-1}(\{y\}) := \{x \in X | f(x) = y\}$ has the same cardinal number $\frac{|X|}{|Y|}$ or in other terms $\{f^{-1}(\{y\})\}_{y \in Y}$ is a partition of X in subsets of same size $\frac{|X|}{|Y|}$.

[3] In order to define such a multiplication, we need to suppose that the *axiom of choice* holds in our underlying theory of sets ([2]).

Definition 6. Let X and Y be two sets so that $0 < |X| \leq 2^{\aleph_0}$, $0 < |Y| \leq 2^{\aleph_0}$ and $|X| \geq |Y|$. Let $f : X \to Y$ be a mapping. The function f is *balanced* if $|f^{-1}(\{y\})|$ is a constant in $\mathbb{N} \cup \{\aleph_0, 2^{\aleph_0}\}$ when y describes Y.

The assumption $|X| \geq |Y|$ in the previous definition is necessary since a balanced function is onto. We can also observe that when $|X|$ and $|Y|$ are both finite then this is equivalent to the classical notion of balancedness. Now let suppose that we have a balanced map $f : X \to Y$. Let's try to compute the constant $\mathfrak{c} := |f^{-1}(\{y\})|$. The set $\{f^{-1}(\{y\})\}_{y \in Y}$ is a partition of X and then $X = \bigcup_{y \in Y} f^{-1}(\{y\})$. Since f is balanced, we obtain $|X| = |Y|\mathfrak{c}$.

For each of the following cases, we compute the constant $\mathfrak{c}$ by using the particular multiplication of transfinite cardinal numbers:

1. $|X| = \aleph_0$ and $0 < |Y| < \aleph_0$. Then $\mathfrak{c} = \aleph_0$;
2. $|X| = \aleph_0$ and $|Y| = \aleph_0$. Then $\mathfrak{c} \in \mathbb{N}^* \cup \{\aleph_0\}$;
3. $|X| = 2^{\aleph_0}$ and $0 < |Y| < 2^{\aleph_0}$. Then $\mathfrak{c} = 2^{\aleph_0}$;
4. $|X| = 2^{\aleph_0}$ and $|Y| = 2^{\aleph_0}$. Then $\mathfrak{c} \in \mathbb{N}^* \cup \{\aleph_0, 2^{\aleph_0}\}$.

Below are given some instances and counter-examples of balanced functions in each case.

Examples 1.

1. The indicator function f of the even integers is a balanced function from $\mathbb{Z}$ to $\mathbb{Z}_2 = \{0, 1\}$ with $\mathfrak{c} = \aleph_0$. Let E be a nonempty finite subset of $\mathbb{Z}$, then the function $g : \mathbb{Z} \to \mathbb{Z}_2$ defined as the indicator function of E is surjective but not balanced since $|g^{-1}(\{1\})| = |E| \in \mathbb{N}^*$ and $|g^{-1}(\{0\})| = |\mathbb{Z} \setminus E| = \aleph_0$;
2. The identity function f of $\mathbb{Z}$ is a balanced function with $\mathfrak{c} = 1$. Let define the mapping

$$\begin{array}{rccl} f: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \begin{cases} 0 & \text{if } n \in \{0, 1\}; \\ f(2k-1)+1 & \text{if } n \in \{2k, 2k+1\} \text{ with } k \in \mathbb{N}^*. \end{cases} \end{array}$$

   Then f is balanced with $\mathfrak{c} = 2$. Let $g : \mathbb{Z} \to \mathbb{N}$ such that for each $n \in \mathbb{Z}$, $g(\pm n) = n$. Then g is surjective but not balanced since for each nonzero $n \in \mathbb{N}$, $|g^{-1}(\{n\})| = |\{\pm n\}| = 2$ and $|g^{-1}(\{0\})| = |\{0\}| = 1$;
3. Let $f : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q}$ defined as $f(a, b) = \frac{a}{b}$. Then f is balanced with $\mathfrak{c} = \aleph_0$. Let $g : \mathbb{Z} \times \mathbb{Z}^* \cup \{(0, 0)\} \to \mathbb{Q} \cup \{\uparrow\}$ (with $\uparrow \notin \mathbb{Q}$) such that for each $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, $g(a, b) = f(a, b)$ as previously defined and $g(0, 0) = \uparrow$. Then g is surjective but not balanced since for each $q \in \mathbb{Q}$, $|g^{-1}(\{q\})| = |f^{-1}(\{q\})| = \aleph_0$ but $|g^{-1}(\{\uparrow\})| = |\{(0, 0)\}| = 1$;
4. Let f be the indicator function of $[0; +\infty[$ then $f : \mathbb{R} \to \mathbb{Z}_2$ is balanced with $\mathfrak{c} = 2^{\aleph_0}$. The map $g : \mathbb{R} \to \mathbb{Z}_2$ defined as the indicator function of a finite or countable subset E ($E \neq \emptyset$) of $\mathbb{R}$ is surjective but not balanced since $|g^{-1}(\{1\})| = |E| \in \mathbb{N}^* \cup \{\aleph_0\}$ and $|g^{-1}(\{0\})| = |\mathbb{R} \setminus E| = 2^{\aleph_0}$;
5. Let $f : [0; +\infty[\to \mathbb{N}$ defined by $f([n, n+1[) = n$ for each $n \in \mathbb{N}$. Then f is balanced with $\mathfrak{c} = 2^{\aleph_0}$. The function $g : \{-1\} \cup [0; +\infty[\to \{-1\} \cup \mathbb{N}$ defined as f when restricted to $[0; +\infty[$ and $g(-1) = -1$ is surjective but not balanced since for each $n \in \mathbb{N}$, $|g^{-1}(\{n\})| = |[n; n+1[| = 2^{\aleph_0}$ but $|g^{-1}(\{-1\})| = |\{-1\}| = 1$;
6. Let define $f : \mathbb{R}^* \to]0; +\infty[$ so that $f(x) = x^2$. Then f is balanced with $\mathfrak{c} = 2$. Now if we consider $g : \mathbb{R} \to [0; +\infty[$ such that $g(x) = x^2$. Then g is surjective but not balanced since $|g^{-1}(\{0\})| = 1$ and for each $x \in]0; +\infty[$, $|g^{-1}(\{x\})| = 2$;

7. The function
$$\begin{array}{rccc} f: & \mathbb{R} & \to & \{z \in \mathbb{C} \mid |z| = 1\} \\ & t & \mapsto & e^{it} \end{array}$$
is balanced with $\mathfrak{c} = \aleph_0$ since $f^{-1}(\{z\}) = arg(z) + 2\pi\mathbb{Z}$;

8. The projection
$$\begin{array}{rccc} f: & \mathbb{C} & \to & \mathbb{R} \\ & a+ib & \mapsto & a \end{array}$$
is balanced with $\mathfrak{c} = 2^{\aleph_0}$ since for each $a \in \mathbb{R}$, $f^{-1}(\{a\}) = a + i\mathbb{R}$.

The notion of infinite balancedness allows us to extend the concept of (G)-perfect nonlinearity in the transfinite setting.

Definition 7. Let G be a group acting faithfully on a nonempty set X ($|X| \leq 2^{\aleph_0}$) and let H be a group in an additive notation with ($|H| \leq |X|$). A map $f : X \to H$ is called *G-perfect nonlinear* if for each nonidentity $\alpha \in G$, the *derivative of f in direction α*
$$\begin{array}{rccc} d_\alpha f: & X & \to & H \\ & x & \mapsto & f(\alpha.x) - f(x) \end{array}$$
is balanced.
If G is a topological group, X a (nonempty) topological space such that there is a faithful topological group action of G on X and H is a topological group, we say that $f : X \to H$ is *(topological) G-perfect nonlinear* if f is continuous and for each nonidentity $\alpha \in G$, $d_\alpha f$ is continuous and balanced.

When in a cryptosystem, keys and plaintexts are combined via a topological group action as it is the case in the encryption schemes presented in section 3, we must confuse the group and topological structures. We make the assumption that the two requirements are independent and must be provided by different components. As in the finite case, we use (G-)perfect nonlinear functions to hide the group structure; but they have no role in confusing the topological structure. This is the reason why we define the notion of *topological* G-perfect nonlinear functions. In the next section, we introduce the notion of *D-boxes*[4] whose role in an encryption scheme is precisely to provide the topological confusion.

3 Proposed cryptosystems and their security

In this section are presented several versions of an iterative block cipher in an ideal world where the plaintexts, keys and ciphertexts are taken in some noncountable subsets of the real line. In its version first the block cipher is maximally resistant against a multiplicative differential attack but vulnerable against its additive version. The second block cipher is an improvement that ensures both resistance against multiplicative and additive differential cryptanalysis. Moreover since we deal with real-valued functions defined on real numbers, we need to consider some attacks based on real analysis. So we introduce a new kind of cryptographic components, the *D-boxes*, to prevent such attacks by hiding the topological structures. Finally we present an extension in the complex plane.

[4]The letter « D » refers to the word « discontinuous ».

3.1 First encryption scheme using a multiplicative perfect nonlinear S-box

Theorem 1. *The exponential function*

$$\begin{array}{rccc} Exp: & \mathbb{R} & \leftrightarrow &]0;+\infty[\\ & x & \mapsto & e^x \end{array}$$

is a $(\mathbb{R}^*,\times,1)$*-perfect nonlinearity homeomorphism from* $\mathbb{R}$ *onto* $(]0;+\infty[,\times,1)$.

Proof. We only need to check the property of perfect nonlinearity. Let α be a nonidentity element of $(\mathbb{R}^*,\times,1)$ *i.e.* $\alpha \in \mathbb{R}^* \setminus \{1\}$. The derivative of *Exp* in direction α is defined as

$$\begin{array}{rccc} d_\alpha Exp: & \mathbb{R} & \rightarrow &]0;+\infty[\\ & x & \mapsto & \frac{Exp(\alpha x)}{Exp(x)} \end{array}.$$

Then we need to prove that $d_\alpha Exp$ is balanced. So let $\beta \in]0;+\infty[$. Let us compute the number of solutions $x \in \mathbb{R}$ such that $d_\alpha Exp(x) = \beta$.

$$\begin{array}{rccl} & d_\alpha Exp(x) & = & \beta \\ \Leftrightarrow & \frac{e^{\alpha x}}{e^x} & = & \beta \\ \Leftrightarrow & e^{\alpha x - x} & = & \beta \\ \Leftrightarrow & e^{(\alpha-1)x} & = & \beta \\ \Leftrightarrow & (\alpha-1)x & = & ln(\beta) \text{ (since } \beta > 0) \\ \Leftrightarrow & x & = & \frac{ln(\beta)}{\alpha-1} \text{ (because } \alpha \neq 1) \end{array}$$

and then $d_\alpha Exp$ is onto. But actually since $d_\alpha Exp = Exp \circ \tau_{\alpha-1}$, where for $\gamma \in \mathbb{R}^*$

$$\begin{array}{rccc} \tau_\gamma: & \mathbb{R} & \rightarrow & \mathbb{R} \\ & x & \mapsto & \gamma x \end{array}$$

which is a homeomorphism since $\gamma \neq 0$, by composition of homeomorphisms ($\alpha \neq 1$ then $\tau_{\alpha-1}$ is one-to-one and onto), $d_\alpha Exp$ is also a homeomorphism and thus is balanced. □

Corollary 1. *Let* $a \in]0;+\infty[\setminus\{1\}$. *We define the exponential function with base* a *by*

$$\begin{array}{rccc} Exp_a: & \mathbb{R} & \rightarrow &]0;+\infty[\\ & x & \mapsto & a^x := e^{x ln(a)} \end{array}.$$

Note that $Exp_e = Exp$. *Then* Exp_a *is a* $(\mathbb{R}^*,\times,1)$*-perfect nonlinear homeomorphism from* $\mathbb{R}$ *to* $(]0;+\infty[,\times,1)$.

Proof. Exp_a is a homeomorphism because $Exp_a = Exp \circ \tau_{ln(a)}$ and $ln(a) \neq 0$ since $a \neq 1$. Moreover for each $\alpha \in \mathbb{R}^* \setminus \{1\}$ we have $d_\alpha Exp_a = Exp \circ \tau_\alpha \circ \tau_{ln(a)}$ and then $d_\alpha Exp_a$ is an homeomorphism and thus is balanced. □

Cryptosystem $\mathcal{K}_1(\mathbb{R})$:
For each $a \in]0;+\infty[\setminus\{1\}$, we can define the following block cipher. The set of plaintexts is $\mathbb{R}$, the set of keys is $\mathbb{R}^*$ and the set of ciphertexts is $]0;+\infty[$. For each key k, one encrypts a message x by $T(x,k) = T_k(x) := Exp_a(kx) = a^{kx}$. The decryption algorithm is given by $T_k^{-1}(c) := \tau_{\frac{1}{kln(a)}} \circ ln(c)$ for each ciphertext $c \in]0;+\infty[$. Obviously this is the description of one round and $\mathcal{K}_1(\mathbb{R})$ can be seen as a *Substitution-Permutation Network* (SPN).

According to corollary 1 this cryptosystem is secure against a multiplicative differential attack. Nevertheless it is vulnerable against a classical additive differential cryptanalysis since the map Exp_a is a morphism: $Exp_a(\alpha + x) = Exp_a(\alpha)Exp_a(x)$. So an enemy should be able to use this linearity in order to recover the key. To avoid such an additive attack, we need to complete $\mathcal{K}_1(\mathbb{R})$ with an additive perfect nonlinear S-box.

3.2 Second encryption scheme using an additive perfect nonlinear S-box

Theorem 2. *The map*

$$\begin{array}{rccc} X^2: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & x^2 \end{array}$$

is continuous and perfect nonlinear from $(\mathbb{R}, +, 0)$ *to itself.*

Proof. Let $\alpha \in \mathbb{R}^*$. We have $d_\alpha X^2(x) = X^2(\alpha + x) - X^2(x) = (\alpha + x)^2 - x^2 = 2\alpha x + \alpha^2$. Then $d_\alpha X^2$ is a homeomorphism of $\mathbb{R}$ and therefore is balanced. □

Cryptosystem $\mathcal{K}_2(\mathbb{R})$:
So now in order to avoid both multiplicative and additive differential attacks, we complete the SPN $\mathcal{K}_1(\mathbb{R})$ in the following way. The set of plaintexts is $\mathbb{R}$, the set of keys is $]0; +\infty[^2$ and the set of ciphertexts is $]0; +\infty[$. Let x be a message to encrypt and let $(k_1, k_2) \in]0; +\infty[^2$ be the round key. At first, the quantity $Exp_a(k_1 x) = a^{k_1 x}$ is computed. This step ensures the resistance against the multiplicative differential attack. Then we insert the second part k_2 of the secret key by addition: $k_2 + a^{k_1 x}$. Finally the ciphertext is given by

$$X^2(k_2 + a^{k_1 x}) = (k_2 + a^{k_1 x})^2 = k_2^2 + 2k_2 a^{k_1 x} + a^{2k_1 x} \ .$$

This last step guarantees the solidity against the additive version of the differential cryptanalysis. Given a ciphertext $c \in]0; +\infty[$ and a secret key $(k_1, k_2) \in]0; +\infty[^2$ we obtain the plaintext x by computing

$$x := \frac{1}{k_1 ln(a)} ln(\sqrt{c} - k_2) \ .$$

3.3 Real analysis based attacks and discontinuous D-boxes

The two maps used in the block cipher $\mathcal{K}_2(\mathbb{R})$ both are continuous and even (indefinitely) derivable by respect to the usual topology of the real-line. These properties lead to possible cryptanalysis of the system.
Continuity attack: By continuity two close ciphertexts are obtained from two close plaintexts. Therefore the diffusion aspect is not guaranteed in such a cryptosystem.
Derivability attack: Let x_0 be a plaintext and h be an infinitely small number. Since Exp_a is derivable, $Exp_a(k(x_0 + h)) - Exp_a(kx_0) = a^{k(x_0+h)} - a^{kx_0}$ is close to hka^{kx_0} and then an enemy may be able to distinguish the key k. In a similar way, if h is sufficient small, $(x_0 + h + k)^2 - (x_0 + k)^2$ is close to $h(2x_0 + 2k)$ and such a linear relation may be use to find the key k.

In order to avoid such topological attacks we need to use another kind of components which must hide the topological structures: so we need discontinuous ***D*-boxes**. They must ensure the diffusion requirement by destroying the underlying topological structures.

Theorem 3. *Let define the following function.*

$$\begin{array}{rccc} D: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & 1_{\mathbb{Q}}(x)+x \end{array}$$

where $1_{\mathbb{Q}}$ *is the indicator function of the field of rational numbers. Then* D *is a permutation nowhere continuous. Moreover* $D \circ ln :]0;+\infty[\to \mathbb{R}$ *is also a permutation nowhere continuous.*

Proof. D is nowhere continuous on $\mathbb{R}$: let $x_0 \in \mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$ for each $\nu > 0$, there is $x \in \mathbb{R} \setminus \mathbb{Q}$ so that $|x_0 - x| < \nu$ but $|D(x_0) - D(x)| = |1 + x_0 - x| > 1$. Let $x_0 \in \mathbb{R} \setminus \mathbb{Q}$. By density for each $\nu > 0$, there is $x \in \mathbb{Q}$ such that $|x_0 - x| < \nu$ and $|D(x_0) - D(x)| > 1$. Thus D is nowhere continuous.
Now let prove that D is a bijection. Let $x \in \mathbb{Q}$. Then $x-1$ is also an element of $\mathbb{Q}$. So we have $D(x-1) = 1_{\mathbb{Q}}(x-1) + x - 1 = 1 + x - 1 = x$. Let $x \in \mathbb{R} \setminus \mathbb{Q}$. We have $D(x) = x$. So D is onto. Finally let suppose that $D(x) = D(y)$. Then if $x \in \mathbb{R} \setminus \mathbb{Q}$, $x = D(x) = D(y)$. If $y \in \mathbb{R} \setminus \mathbb{Q}$ then $D(y) = y$ and $x = y$. If $y \in \mathbb{Q}$, $D(y) = y + 1 \in \mathbb{Q}$ and in particular $x = y + 1 \in \mathbb{Q}$ which is a contradiction. If $x \in \mathbb{Q}$, then $x + 1 = D(x) = D(y)$. If $y \in \mathbb{Q}$, $D(y) = y + 1$, then $x = y$. If $y \in \mathbb{R} \setminus \mathbb{Q}$ then $x + 1 = D(y) = y \in \mathbb{R} \setminus \mathbb{Q}$ which is a contradiction. Therefore D is one-to-one. Note that for each $x \in \mathbb{R}$, we have $D^{-1} = x - 1_{\mathbb{Q}}(x)$. By composition of permutations, $D \circ ln$ is bijective. Since ln is a homeomorphism, $D \circ ln$ is continuous at every point where D is continuous. □

Cryptosystem $\mathcal{K}_3(\mathbb{R})$:
We can use the permutation $D \circ ln$ as a D-box in order to avoid the attacks based on continuity or derivability of the S-boxes. We just use the output of $\mathcal{K}_2(\mathbb{R})$ as an imput of D. So a plaintext $x \in \mathbb{R}$ is encrypted via the following round function, for the secret key $(k_1, k_2) \in]0;+\infty[^2$:

$$T(x,(k_1,k_2)) := D \circ ln \circ X^2(k_2 + Exp_a(k_1 x)) = 1_{\mathbb{Q}}(ln(k_2^2 + 2k_2 a^{k_1 x} + a^{2k_1 x})) + ln(k_2^2 + 2k_2 a^{k_1 x} + a^{2k_1 x}) \, .$$

If $c \in \mathbb{R}$ is a ciphertext corresponding to the key (k_1, k_2), the plaintext x is recovered by

$$x := \frac{1}{k_1 ln(a)} ln(\sqrt{e^{c - 1_{\mathbb{Q}}(c)}} - k_2) \, .$$

3.4 Complex-plane extension

In this subsection we propose to extend our results to the complex-plane. Unfortunatly, due to inversion problems, the cryptosystem $\mathcal{K}_3(\mathbb{R})$ does not fit naturally into the complex setting. Therefore we will use some complex extensions of the previous S-boxes but in a Feistel structure in order to neglect the inversibility of the internal components.

Theorem 4. *The map*

$$\begin{array}{rccc} Exp: & \mathbb{C} & \to & \mathbb{C} \\ & z = x + iy & \mapsto & e^z := e^x e^{iy} = e^x(cos(y) + isin(y)) \end{array}$$

is holomorphic $(\mathbb{C}^*, \times, 1)$*-perfect nonlinear from* $\mathbb{C}$ *to* $(\mathbb{C}^*, \times, 1)$.

Proof. Let $\beta \in \mathbb{C}^*$. Then $e^z = \beta \Leftrightarrow$ there is $k \in \mathbb{Z}$ such that $z = ln(|\beta|) + i(arg(\beta) + 2k\pi)$. Let $\alpha \in \mathbb{C}^* \setminus \{1\}$. We have $d_\alpha e^z = e^{\alpha z} e^{-z} = e^{(\alpha-1)z}$ and therefore $d_\alpha Exp$ is holomorphic on the complex-plane and thus is continuous. Moreover $e^{(\alpha-1)z} = \beta$ if and only if there is $k \in \mathbb{Z}$ such that $z = \frac{1}{(\alpha-1)} \left(ln(|\beta|) + i(arg(\beta) + 2k\pi)\right)$ (since $\alpha \neq 1$). Finally we deduce that for each $\alpha \in \mathbb{C}^* \setminus \{1\}$ and each $\beta \in \mathbb{C}$, $(d_\alpha Exp)^{-1}(\{\beta\}) = \{\frac{1}{(\alpha-1)} \left(ln(|\beta|) + i(arg(\beta) + 2k\pi)\right)\}_{k \in \mathbb{Z}}$ and therefore $|(d_\alpha Exp)^{-1}(\{\beta\})| = \aleph_0$ and Exp is $(\mathbb{C}^*, \times, 1)$-perfect nonlinear from $\mathbb{C}$ to $(\mathbb{C}^*, \times, 1)$. □

Theorem 5. *The map*

$$\begin{array}{rccc} Z^2: & \mathbb{C} & \to & \mathbb{C} \\ & z & \mapsto & z^2 \end{array}$$

is holomorphic perfect nonlinear from $(\mathbb{C}, +, 0)$ *to itself.*

Proof. Let $\alpha \in \mathbb{C}^*$. We have

$$\begin{array}{rcl} Z^2(\alpha + z) - Z^2(z) & = & (\alpha + z)^2 - z^2 \\ & = & \alpha^2 + 2\alpha z + z^2 - z^2 \\ & = & \alpha^2 + 2\alpha z \ . \end{array}$$

Since $\alpha \neq 0$, $d_\alpha Z^2$ is a bijection (and even a homeomorphism since it is holomorphic as a polynomial function) and therefore is balanced. □

Note that both *Exp* and Z^2 are holomorphic at every point of the complex plane (since they are entire functions) and thus, as analytic functions, they are infinitely often complex-differentiable at every point of $\mathbb{C}$. As in the real case, we need to use a nonholomorphic components, the D-boxes, in order to avoid an attack based on continuity or derivability and to ensure a good level of diffusion.

Theorem 6. *Let define the function*

$$\begin{array}{rccc} D: & \mathbb{C} & \to & \mathbb{C} \\ & z = x + iy & \mapsto & x + iy + 1_{\mathbb{Q}}(x) + i1_{\mathbb{Q}}(y) \end{array}$$

Then D *is a permutation nowhere continuous.*

Proof. Let $z_0 \in \mathbb{C}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, for each $\nu > 0$ one can always find $z \in \mathbb{C}$, $|z - z_0| < \nu$ but $|D(z) - D(z_0)| > 1$ and therefore D is noncontinuous.
Let $z = x + iy$. Then we have

$$x + iy = \begin{cases} D(x + iy) & \text{if } (x, y) \in (\mathbb{R} \setminus \mathbb{Q})^2; \\ D(x - 1 + iy) & \text{if } (x, y) \in \mathbb{Q} \times (\mathbb{R} \setminus \mathbb{Q}); \\ D(x + iy - i) & \text{if } (x, y) \in (\mathbb{R} \setminus \mathbb{Q}) \times \mathbb{Q}; \\ D(x - 1 + iy - i) & \text{if } (x, y) \in \mathbb{Q}^2. \end{cases}$$

Therefore D is onto.
Let suppose that $D(z) = D(z')$. In order to prove that D is one-to-one, we should make a proof by cases. But since the proof is almost the same in all cases, we only detail a single case: let suppose that $z \in (\mathbb{R} \setminus \mathbb{Q}) + i(\mathbb{R} \setminus \mathbb{Q})$ then $z = D(z) = D(z')$. If $z' \in (\mathbb{R} \setminus \mathbb{Q}) + i(\mathbb{R} \setminus \mathbb{Q})$ then $z = D(z') = z'$. If $z' = x' + iy' \in \mathbb{Q} + i(\mathbb{R} \setminus \mathbb{Q})$ then $z = D(z') = x + 1 + iy$. This implies that the real part of z is equal to $x + 1$ which is a contradiction. If $z' = x' + iy' \in (\mathbb{R} \setminus \mathbb{Q}) + i\mathbb{Q}$ then $z = D(z') = x + iy + i$. So in particular the imaginary part of z is equal to $y + 1 \in \mathbb{Q}$ which is a contradiction. If $z' = x' + iy' \in \mathbb{Q} + i\mathbb{Q}$ then $z = D(z') = x' + iy'$ and we also find a contradiction. □

Cryptosystem $\mathcal{K}_4(\mathbb{C})$:

The complex exponential function *Exp* is a permutation from $\mathbb{R} + i[0; 2\pi[$ onto $\mathbb{C}^*$. Unfortunatly $\mathbb{R} + i[0; 2\pi[$ is not invariant under the multiplication of $\mathbb{C}^*$. Moreover Z^2 is not a permutation of the entire complex-plane even if in some cases it is possible to define an holomorphic function of square root as it is briefly recalled now (see for instance [5] for more details). A *determination* of the logarithm on an open set $U \subset \mathbb{C}^*$ is an holomorphic function $L : U \to \mathbb{C}$ such that $\forall z \in U$, $e^{L(z)} = z$. Note that there is no determination of the logarithm on the open set $\mathbb{C}^*$ but there

is a determination on $\mathbb{C}^*\backslash]-\infty;0[$ and more generally there is a determination on every simply connected open that does not contain 0. On every open U of $\mathbb{C}^*$ where there is a determination L of the logarithm, we can define a determination of the power of exponent $a \in \mathbb{C}$ by

$$\forall z \in U,\ z^a := Exp(aL(z)) \ .$$

In particular if n is an integer greater or equal to 2 the function

$$\begin{array}{rccc} \sqrt[n]{}: & U & \to & \mathbb{C} \\ & z & \mapsto & \sqrt[n]{z} := Exp(\frac{1}{n}L(z)) \end{array}$$

is holomorphic on U and satisfies $\forall z \in U,\ (\sqrt[n]{z})^n = z$. Such a function is called a *determination* on U of the nth square root.
The sequence of S-boxes compositions used in $\mathcal{K}_3(\mathbb{R})$ can not be easily and naturally adapted to the complex-plane. In this case, it seems to be more accurate to use a Feistel network. For instance we can sequentially use two Feistel's permutations F_1 and F_2, defined by

$$F_1((x,y),k_1) := (y, e^{k_1 y} + x)$$

and

$$F_2((x,y),k_2) := (D(y), D((k_2+y)^2 + x))$$

for $(x,y) \in \mathbb{C}^2$ and $(k_1,k_2) \in \mathbb{C}^* \times \mathbb{C}$. So in a single round we compute the ciphertext c as follows (the secret-key is (k_1,k_2)).

$$c := (D(e^{k_1 y} + x), D((k_2 + e^{k_1 y} + x)^2 + y)) \ .$$

The decryption of $c = (c_1, c_2)$ is obtained by the following formula.

$$(x,y) = (D^{-1}(c_1) - Exp(k_1(D^{-1}(c_2) - X^2(k_2 + D^{-1}(c_1)))), D^{-1}(c_2) - X^2(k_2 + D^{-1}(c_1))) \ .$$

3.5 How to implement such cryptosystems on the real-line or the complex-plane ?

The construction of ideal cryptosystems on the real-line or the complex-plane raises the crucial question of their practical implementation in the « real world ». In this contribution we do not give a detailed and rigorous method to solve this problem but a possible direction to follow: the super-Turing computations.
Super-Turing models of computations: Hypercomputation or super-Turing computation refers to various models for the computation of non-Turing-computable functions or recursive functions. Within these models the so-called *Church-Turing thesis* ([6, 23]) ceases to be valid. Such a powerful model was already intoduced by Alan Turing himself in his 1939 paper [24]. This paper invistigated some mathematical ideal systems in which an oracle was available, which could compute a single arbitrary non-recursive function over natural integers. Since then other methods have been proposed by different authors. One can cite (see [25]) the *accelerated Turing machine* independently proposed by Russel [19], Blake [1] and Weyl [26] which is defined as a process that performs its first step in one unit of time and each subsequent step in half the time of the step before such that a process could complete an infinity of steps in only two units of time, a *neural network with real numbers as weights* should be able to compute over real numbers and finally a Turing machine in a special kind of relativistic spacetime, called *Malament-Hogarth spacetime* [8], can perform an infinite number of operations while remaining in the past light cone of a particular event. This kind of models of computation should be very relevant to compute over the real-line or the complex-plane and thus should be used to implement our « continuous » cryptosystems. However at this stage, none of these models seem physically plausible. Thus these « hypercomputers » are likely to remain as mathematical ideal models.

References

[1] R. M. Blake. The paradox of temporal process. *Journal of Philosophy*, 23:645-654, 1926.

[2] N. Bourbaki. Elements of Mathematics - Theory of sets. Springer, 2004.

[3] M. Bellare and P. Rogaway. Random oracles are practical : a paradigm for designing efficient protocols. In *Proceedings of the ACM Conference on Computer and Communication Security*, pp. 63-73, 1993.

[4] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3-72, 1991.

[5] H. Cartan. Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes. Hermann, 1961.

[6] A. Church. An unsolvable problem of elementary number theory. *American Journal of Mathematics*, 58:345-363, 1936.

[7] R. Canetti, O. Goldreich and S. Halevi. The random oracle methodology, revisited. *Journal of the ACM*, 51(4):557-594, 2004.

[8] G. Etesi, I. Nemeti. Non-Turing computations via Malament-Hogarth space-times. *Int. J. Theor. Phys.*, 41:341-370, 2002.

[9] FIPS 46-3, Data encryption standard, Federal Information Processing Standards Publication 46-3 (1999), U.S. Department of Commerce/N.I.S.T.

[10] FIPS 197, Advanced encryption standard, Federal Information Processing Standards Publication 197 (2001), U.S. Department of Commerce/N.I.S.T.

[11] S. Harari and P. Liardet. Rational interval maps and cryptography. In *Proceedings of Eurocode 1992*, vol. 339 of *CISM courses and lectures*, pp. 185-199, 1993.

[12] M. Hasler. Synchronization of chaotic systems and transmission of information, *Int. J. Bifurc. Chaos*, 8:647-659, 1998.

[13] X. Lai and J. L. Massey. A proposal for a new block encryption standard. In *Advances in Cryptology - Eurocrypt '90*, vol. 473 of *Lecture Notes in Computer Science*, pp. 389-404, 1991.

[14] S. Li. Analyse and new designs of digital chaotic ciphers. PhD thesis, School of Electronics and Information Engineering, Xi'an Jiaotong University, 2003.

[15] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology - Eurocrypt'92*, vol. 547 of *Lecture Notes in Computer Science*, pp. 378-386, 1992.

[16] L. Poinsot and S. Harari. Generalized Boolean bent functions. In *Progress in Cryptology - Indocrypt 2004*, vol. 3348 of *Lecture Notes in Computer Science*, pp. 107-119, 2004.

[17] L. Poinsot and S. Harari. Group actions based perfect nonlinearity. *GESTS International Transactions on Computer Science and Engineering*, 12(1):1-14, 2005.

[18] L. Poinsot. *Non linéarité parfaite généralisée au sens des actions de groupe, contribution aux fondements de la solidité cryptographique*. PhD thesis, University of South Toulon-Var, 2005.

[19] B.A.W. Russell. The limits of empiricism. In *Proceedings of the Aristotelian Society*, vol. 36, 131-150, 1936.

[20] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656-715, 1949.

[21] V. V. Shorin, V. V. Jelezniakov and E. M. Gabidulin. Linear and differential cryptanalysis of Russian GOST. D. Augot, C. Carlet (Eds.), Workshop on Coding and Cryptography 2001, pp. 467-476, 2001.

[22] C. P. Silva C. P. and A. M. Young. Introduction to chaos-based communications and signal processing. In *Proc. IEEE Aerospace Conference*, pp. 279-299, 2000.

[23] A. M. Turing. On computable numbers with an application to the Entscheidungsproblem. In *Proceedings of the London Mathematical Society*, serie 2, vol. 42, pp. 230-265, 1936.

[24] A. M. Turing. Systems of logic based on ordinals. In *Proceddings of the London Mathematical Society*, serie 2, vol. 45, pp. 161-228, 1939.

[25] T. Ord. The many forms of hypercomputations. *Applied Mathematics and Computation*, 178:143-153, 2006.

[26] H. Weyl. Philosophie der Mathematik and Naturwissenschaft. R. Oldenburg, Munich, 1927.