Abstract. We introduce two frameworks in order to deal with fractal and multi-fractal analysis for subset sum problems where some embedding into the 1-dimensional Euclidean space plays an important role. As one of these frameworks, non-classical generalized dimensions for a family of subset sum functions are defined. These generalized dimensions not only include the box-counting dimension, the information dimension and the correlation dimension, but also include the density of the subset sum problem. As the other framework, we construct a self-similar set for a particular subset sum function in a family of subset sum functions by using a graph theoretical technique. We show the relations between the three parameters: the number of connected component in a graph, the Hausdorff dimension and an approximate value of the non-classical box-counting dimension.

Keywords: Fractal Analysis, Multi-fractal Analysis, Subset Sum Problems, Linear Diophantine Equations, Combinatorics and Graph Theory, Cryptography.

AMS Subject Classification: 05A16, 05A20, 05C62, 11D04, 11D45, 28A80, 60C05, 94A60.

1 Introduction

As knapsack problems, the subset sum problem, the subset product problem and the compact knapsack problem have been used in cryptography (e.g. [3]). These knapsack
problems are known to be NP-hard (22, 12, 40). Cryptosystems that allow a transformation between easy and hard knapsack problems are sometimes called knapsack cryptosystems. The several Merkle-Hellman cryptosystems in [30] are the first knapsack cryptosystems. The “basic” Merkle-Hellman cryptosystem was completely broken by Shamir [38].

For the compact knapsack problem ([40]), it requires small coefficients and moderate multiplicities in a solution. The subset product problem has an aspect as a multiplicative analogue of the subset sum problem, which is related to the discrete logarithm problem. See also Table I.

| Subset Sum or Subset Product | a binary sequence ↔ a set |
|-----------------------------|--------------------------|
| Compact Knapsack            | a multi-ary sequence ↔ a multiset |

Table 1: A solution for a linear diophantine equation over positive integers.

With one of motivations in the Shamir’s attack, Lagarias [25] showed that the simultaneous Diophantine approximation problems are NP-hard by using a reduction from the weak partition problem which is a special case of the bounded homogeneous equation problem (see also 39, 8).

However, a lot of knapsack cryptosystems are broken (e.g. see 32, 3, 42). As one of such cryptosystems, the Chor-Rivest (CR) cryptosystem [4] is known. Although the CR cryptosystem was completely broken by Vaudenay [42], it took about a decade to break. As a consequence, the CR cryptosystem was rather stronger, compared with any other knapsack cryptosystems until 1990s. As an improvement of the CR cryptosystem, the Okamoto-Tanaka-Uchiyama (OTU) cryptosystem [33] is known. In the CR cryptosystem, one must solve an easy discrete logarithm problem over a finite field in order to obtain public information with respect to the (modular) subset sum problem. On the other hand, in order to avoid the attack by Vaudenay, the OTU cryptosystem requires a quantum computer to find discrete logarithms over a residue field (finite field) in an algebraic field. The security of the OTU cryptosystem mainly depends on the shortest vector problem or the closest vector problem in a lattice ([31]). The shortest vector problem is NP-hard under the randomized reduction from the “restricted” subset sum problem [1] and the closest vector problem is NP-hard under the (deterministic) reduction from the (weak) partition problem [8]. It is unknown whether an algorithm to break the OTU cryptosystem exists or not.

In post quantum cryptography, it is important to find multi-collisions ([18]). One of the purposes in this paper is to give some foundations in order to investigate multi-collisions for subset sum functions via fractal and multi-fractal analysis.

Finding a solution to the subset sum problem can be replaced by finding an inverse image of a function which is sometimes called the subset sum function. Impagliazzo and Naor [20] showed that a subset sum function modulo a power of 2 can be used as several cryptographic primitives such as a universal one-way function or a pseudorandom generator.
under one-wayness of the subset sum function with a modulus. In [21], the subset sum function as a hash function is used without a modulus.

The OTU cryptosystem does not have some provable security. However, as the cryptosystems based on the hardness of subset sum problems after 2010, the Lyubashevsky-Palacio-Segev cryptosystem [27] achieves the indistinguishability against chosen plaintext attacks (IND-CPA) and the Faust-Masny-Vebturi cryptosystem [10] achieves the indistinguishability against chosen ciphertext attacks (IND-CCA). In these cryptosystems, the subset sum function as a pseudo-random generator is used.

For a cryptosystem based on the subset sum problem, the low density attack has been investigated since the result of Lagarias and Odlyzko [26]. For the low density attack, it is easy to break when the density of the subset sum problem is low. In [30, 39], it was used another density, called “the density of solutions”, before the result of Lagarias and Odlyzko. This density is related to a certain “dimension” in this paper. Compared with the density of the subset sum problem, each of fractal dimensions we use in this paper is a generalization of the density of the subset sum problem.

Mandelbrot posed the concept of “fractal” in 1970s and contributed to “fractal geometry”. Fractal analysis is the well-known research area which has many applications such as natural sciences, engineering and economics. The study of fractal analysis is to investigate fractal dimensions. A fractal set is a set that has some self-similar structure. Fractal analysis has become the standards in many research areas. Fractal analysis is a basic tool using fractal dimensions to deal with a power law of some phenomena. The readers refer to [28, 9] for more details of fractal analysis or fractal geometry.

The research of multifractal analysis has begun from 1980s. In the independent works of Grassberger [13] and Hentschel and Procaccia [17], the generalized dimensions for discrete dynamical systems, which we refer to as the classical generalized dimensions, were introduced. The classical generalized dimensions include the box-counting dimension, the information dimension and the correlation dimension (for details, see [15]). Non-classical generalized dimensions have been used in complex networks since 2000s [11]. Here, Rényi entropy [35] gives rise to the (classical or non-classical) generalized dimension.

The organization of this paper is as follows. In Section 2, we describe basic definitions and subset sum problems, which are used in the latter sections. In Section 3, we give non-classical generalized dimensions for subset sum problems and describe several properties. In Section 4, we give an approach from the Hausdorff dimension to a particular subset sum problem in a family of subset sum functions.

2 Preliminaries

2.1 Basic Definitions

Throughout this paper, we denote by \( s \in \mathbb{Z}_{>0} \) a security parameter.
Definition 2.1 (Collision and Multi-Collision). Let $\mathcal{M}$ and $\mathcal{N}$ denote finite sets, let $G: \mathcal{M} \to \mathcal{N}$ denote a function and let $G^{-1}(c)$ denote the inverse image of $c \in \mathcal{N}$. If there exists $c \in \mathcal{N}$ such that $\#G^{-1}(c) \geq 2$, then for some $l \geq 2$, we call an $l$-element subset of $G^{-1}(c)$ an $l$-collision or a multi-collision. We also call a 2-collision a collision.

Definition 2.2 (Collision Finding Problem). Let $\mathcal{M}$ and $\mathcal{N}$ denote finite sets and let $G: \mathcal{M} \to \mathcal{N}$ denote a function. Then, find $x_1, x_2 \in \mathcal{M}$ such that $G(x_1) = G(x_2), \quad x_1 \neq x_2$.

2.2 Subset Sum Problems

In this section, we describe subset sum problems which we need in Sections 3 and 4. For $s \in \mathbb{Z}_{>0}$, let $A_s \in \mathbb{Z}_{>0}$ denote a modulus. In this paper, we consider the subset sum problem and the corresponding subset sum function for a given set of positive integers.

We refer the subset sum problem to the following modular subset sum problem.

Definition 2.3 (Subset Sum Problem). Given a set \{a_1, \ldots, a_s\} $\subseteq \mathbb{Z}_{>0}$ and $c \in \mathbb{Z}$, find a solution $(x_1, \ldots, x_s) \in \{0, 1\}^s$ to the equation

$$x_1a_1 + \cdots + x_s a_s \equiv c \pmod{A_s}.$$  

(2.1)

In the above definition, we call $\#\{i: x_i \neq 0\}$ the size or Hamming weight of the solution $(x_1, \ldots, x_s) \in \{0, 1\}^s$.

The subset sum function is defined as follows.

Definition 2.4 (Subset Sum Function). Let $G_s: \{0, 1\}^s \to \mathbb{Z}/A_s\mathbb{Z}$ be a function, which is given by

$$G_s(x_1, \ldots, x_s) := x_1a_1 + \cdots + x_s a_s \pmod{A_s}.$$  

We call the function $G_s$ the subset sum function.

Put $U = \{1, \ldots, s\}$. For $(x_1, \ldots, x_s) \in \{0, 1\}^s$, let $S \subseteq U$ be a subset such that $j \in S$ if and only if $x_j \neq 0$, i.e. $S = \{j: x_j \neq 0\}$. The left hand side of (2.1) can be replaced by $\sum_{j \in S} a_j$. From this, we also use the subset $S$ as a solution to the subset sum problem and the power set $2^U$ as the domain of the subset sum function $G_s$ in this paper.

Definition 2.5 (Family of Subset Sum Functions). Let $\{A_s\}_s$ denote a sequence of positive integers such that $A_s \to \infty$ as $s \to \infty$ where each index $s$ is of infinitely many positive integers. Then we call a family $\{G_s\}_s = \{G_s: \{0, 1\}^s \to \mathbb{Z}/A_s\mathbb{Z}\}_s$ a family of subset sum functions.
The hardness of a subset sum problem depends on the density

$$\rho_s = \frac{s}{\log_2 A_s}. \quad (2.2)$$

For the density $\rho_s$, there is the pioneering work due to Lagarias and Odlyzko [26]. It is clear that the density $\rho_s$ is an approximate measure of the information rate.

In the usual subset sum problem (i.e. without modulus $A_s$), $\log_2 A_s$ in the denominator of (2.2) is replaced by $\log_2 \max_i a_i$. As the connection to the usual subset sum problem, we can consider

$$\sum_{j \in S} a_j = c + k A_s$$

for some $k = 0, 1, \ldots, s - 1$. After the result of Lagarias and Odlyzko, there are a lot of subsequent works with respect to the low density attacks (e.g. [5, 31, 24]). In these contexts, the results due to Mazo and Odlyzko [29] are frequently used to investigate the failure probability of the reduction from the subset sum problem to some lattice problems. If $\rho_s \leq 0.8677$ and $|\sum_{j=1}^s x_j - s/2| = \Omega(s)$ for any sufficiently large $s$, then subset sum problems with density $\rho_s$ can be solved asymptotically almost surely as $s \to \infty$ by a single call of a lattice oracle, which solves the shortest vector problem or the closest vector problem in a lattice ([26, 5, 31, 24]). In general, the subset sum problem with density close to 1 is known to be very hard [37, 20].

We summarize several results for the subset sum function as the cryptographic primitives.

**Proposition 2.6 ([20, 27]).** Here we put $A_s = p^s$ for integers $s \geq 1$ and $p \geq 2$. Assume that a subset sum function $G_s$ is one-way. Then

- $G_s$ is a universal one-way hash function when $2^s > A_s$ ($\rho_s > 1$),
- $G_s$ is a cryptographic pseudorandom generator when $2^s < A_s$ ($\rho_s < 1$).

### 2.3 Related Problems

We use the following (modular) weak partition problem in order to investigate multicollisions of the subset sum function.

**Definition 2.7 (Weak Partition Problem).** Given a set $\{a_1, \ldots, a_s\} \subset \mathbb{Z}_{\geq 0}$, find a non-zero solution $(y_1, \ldots, y_s) \in \{-1, 0, 1\}^s \setminus \{(0, \ldots, 0)\}$ such that

$$y_1 a_1 + \cdots + y_s a_s \equiv 0 \pmod{A_s}. \quad (2.3)$$

For a solution $y = (y_1, \ldots, y_s) \in \{-1, 0, 1\}^s$ to the weak partition problem, we call $\#\{j : y_j \neq 0\}$ the size of solution $y$. For $y = (y_1, \ldots, y_s) \in \{-1, 0, 1\}^s \setminus \{(0, \ldots, 0)\}$, we consider two sets $S_1 = \{j : y_j = 1\}$ and $S_2 = \{j : y_j = -1\}$. Notice that the above weak
partition problem needs a modulus although the usual (weak) partition problem does not necessarily need a modulus in some literatures (e.g. [12, SP12], [8]). Hence, if \( S_1 \neq \emptyset \) and \( S_2 = \emptyset \), then \( \{S_1, \emptyset\} \) has the possibility to be a solution to the weak partition problem. Alternatively, we can also consider such sets \( S_1 \) and \( S_2 \) for \(-y\). So, we can see that a collection \( \{S_1, S_2\} \) is the essential solution to the weak partition problem. This implies that if \( y \) is a solution to the weak partition problem, then \(-y\) is equivalent to \( y \). Thus, \( \{y, -y\} \) is essential for a solution to the weak partition problem. Hence, we refer one of the elements in \( \{y, -y\} \) to a solution to the weak partition problem, if it is needed. In the rest of this paper, we denote by \( y \) any non-zero solution to the weak partition problem and we also use a collection \( \{S_1, S_2\} \) as a solution to the weak partition problem. One may assume that \( y \) is chosen so that the first non-zero components in \( y \) is positive.

3 Generalized Dimensions for A Family of Subset Sum Functions

In this section, we make some combinatorial sense from (multi-)fractal analysis to subset sum problems. A unit interval of the 1-dimensional Euclidean space plays an important role. Let \( X \) denote an unit interval of \( \mathbb{R} \) (which can be sometimes regarded as a fundamental region of the torus \( \mathbb{R}/\mathbb{Z} \)). For \( s \in \mathbb{Z}_{>0} \), let \( C_s(X) := \{X_s(c) : c \in \mathcal{A}_s\} \) denote a minimal cover of \( X \) by the intervals with equal diameters \( 1/\mathcal{A}_s \), where \( \mathcal{A}_s \) is some complete residue system for \( \mathbb{Z}/\mathcal{A}_s\mathbb{Z} \). Hence, there is the one-to-one correspondence between \( \mathbb{Z}/\mathcal{A}_s\mathbb{Z} \) and \( C_s(X) \). Since the cover \( C_s(X) \) is minimal, it sometimes holds that

\[
\bigcup_{c \in \mathcal{A}_s} C_s(X) = \bigcup_{c \in \mathcal{A}_s} X_s(c) = X. \quad (3.1)
\]

If all intervals in the minimal cover \( C_s(X) \) are pairwise disjoint, then the minimal cover \( C_s(X) \) is a minimal partition of \( X \). For example, if \( X \) and any \( X_s(c) \in C_s(X) \) are all half-closed, then (3.1) holds and \( C_s(X) \) is a minimal partition of \( X \). For this, the analogous technique can be found in [36]. Without loss of generality, we may choose any \( X_s(c) \in C_s(X) \) so that \( \inf X_s(c) = c/\mathcal{A}_s \) and \( \sup X_s(c) = (c + 1)/\mathcal{A}_s \). In Section 4, it will appear the case when \( X \) and any \( X_s(c) \in C_s(X) \) are closed.

For each subset sum function \( G_s \) in \( \{G_s\}_s \), we embed an element in the image \( G_s(\{0, 1\}^s) \) into a set in the minimal cover \( C_s(X) \). Thus we can define the “dimensions” for a subset sum problem.

**Definition 3.1.** For some \( s \in \mathbb{Z}_{>0} \), we denote by \( P^{(s)}(\cdot) \) a probability distribution and by \( \text{supp}(P^{(s)}) = \{c \in \mathbb{Z}/\mathcal{A}_s\mathbb{Z} : P^{(s)}(c) \neq 0\} \) its support set. Then for a real number \( q \in \mathbb{R} \setminus \{1\} \),
we define the quantity

\[ D_q(P^{(s)}) := \frac{1}{1-q} \log \left( \sum_{c \in \text{supp}(P^{(s)})} P^{(s)}(c)^q \right) / \log A_s. \]

For \( q = -\infty, 1 \) and \( \infty \), we define as \( D_{-\infty}(P^{(s)}) := \lim_{q \to -\infty} D_q(P^{(s)}) \), \( D_1(P^{(s)}) := \lim_{q \to 1} D_q(P^{(s)}) \) and \( D_{\infty}(P^{(s)}) := \lim_{q \to \infty} D_q(P^{(s)}) \), respectively, i.e.

\[
D_{-\infty}(P^{(s)}) := -\log \min_{c \in \text{supp}(P^{(s)})} P^{(s)}(c)/\log A_s,
\]

\[
D_1(P^{(s)}) := -\sum_{c \in \text{supp}(P^{(s)})} P^{(s)}(c) \log P^{(s)}(c)/\log A_s,
\]

\[
D_{\infty}(P^{(s)}) := -\log \max_{c \in \text{supp}(P^{(s)})} P^{(s)}(c)/\log A_s,
\]

respectively. For any \( q \), we call \( D_q = D_q(P^{(s)}) \) with \( \mathcal{C}_s(X) \) the \( q \)-fractal dimension\(^1\).

Notice that the \( q \)-fractal dimension \( (q \geq 0) \) is the same as Rényi entropy up to the exceptions of the scale \( 1/\log A_s \) and a cover \( \mathcal{C}_s(X) \). If \( q_1 \leq q_2 \), then \( D_{q_1} \geq D_{q_2} \). If \( q \geq 0 \), then \( 0 \leq D_q \leq 1 \), i.e. \( D_q \) is a normalization of Rényi entropy in some sense. The \( q \)-fractal dimension \( D_q \) is constant for any \( q \) if and only if the probability distribution is uniform.

Now, we introduce non-classical generalized dimensions for a family of subset sum functions by using Definition 3.1.

**Definition 3.2.** We denote by \( X \) an unit interval of \( \mathbb{R} \), by \( \{ G_s \}_s \) a family of subset sum functions by \( \{ P^{(s)} \}_s \) the corresponding family of probability distributions with support sets \( \text{supp}(P^{(s)}) \), and by \( \{ A_s \}_s \subseteq \mathbb{Z}_{>0} \) a sequence such that \( A_s \to \infty \) as \( s \to \infty \). Given any \( q \)-fractal dimension \( D_q = D_q(P^{(s)}) \) for subset sum functions in a family \( \{ G_s \}_s \), we define the quantity

\[ d_q := \lim_{s \to \infty} D_q(P^{(s)}). \]

For any \( q \), we call the quantity \( d_q \) the **generalized dimension**\(^1\) for a family \( \{ G_s \}_s \) of subset sum functions.

Of course, these non-classical generalized dimensions include the box-counting dimension \( d_0 \), the information dimension \( d_1 \) and the correlation dimension \( d_2 \) as well as the classical

\(^1\)Although “\( q \)-fractal dimension” or “\( q \)-dimension” means the generalized dimension in several literatures, we shall use the \( q \)-fractal dimension of Definition 3.1 as the terminology. For \( q < 0 \) (including \( -\infty \)), the generalized dimension has no sense as a dimension since the embedding dimension is 1. However we use the generalized dimension or the \( q \)-fractal dimension as the terminology even if \( q < 0 \).
generalized dimensions. The dimensions $d_0$, $d_1$ and $d_2$ are given explicitly by
\[
d_0 := \lim_{s \to \infty} \log \left( \frac{\# \text{supp}(P^{(s)})}{\log A_s} \right),
\]
\[
d_1 := -\lim_{s \to \infty} \sum_{c \in \text{supp}(P^{(s)})} P^{(s)}(c) \log P^{(s)}(c) / \log A_s,
\]
\[
d_2 := -\lim_{s \to \infty} \log \left( \frac{\sum_{c \in \text{supp}(P^{(s)})} P^{(s)}(c)^2}{\log A_s} \right),
\]
respectively.

Recall that $1/A_s$ has the meaning as the diameter of an interval in a minimal cover $C_s(X)$. For the classical setting, although the diameter of a set in a minimal cover is not $1/A_s$, it is at most an arbitrarily small real number $\varepsilon > 0$.

If $d_q$ exists, then we will sometimes admit the existence of some limit probability distribution over a unit interval $X$. Conversely, let $\mu$ denote some Borel probability measure over the measurable space $X$ which is constructed so that $C_s(X)$ for any $s$ is measurable. Then we can take the probability distribution $P^{(s)}(\cdot)$ for any $s$ such that $P^{(s)}(c) = \mu(X_s^{(c)})$ holds for every $c$ and $X_s^{(c)}$.

In order to see a fractal structure in a family $\{G_s\}_s$ of subset sum functions, we may consider as follows. For any subset sum functions $G_{s_1}$, $G_{s_2}$ in the family $\{G_s\}_s$ with $s_1 < s_2$, suppose that the pattern of the range of $G_{s_1}$ is contained in the pattern of the range of $G_{s_2}$. Then this should imply that the family $\{G_s\}_s$ has a self-similarity in some sense. As some consequence, we suspect that the family $\{G_s\}_s$ of subset sum functions has some fractal structure.

In the rest of this paper, we use
\[
P^{(s)}(c) := \frac{\# G_{s}^{-1}(c)}{\# \{0, 1\}^s} = \frac{\# G_{s}^{-1}(c)}{2^s} \tag{3.2}
\]
for $c \in G_s(\{0, 1\}^s)$ as a probability distribution $P^{(s)}(\cdot)$ so that $G_s(\{0, 1\}^s) = \text{supp}(P^{(s)})$. Moreover, we suppose that
\[
\min_{c \in \text{supp}(P^{(s)})} P^{(s)}(c) = \frac{1}{\# \{0, 1\}^s} = \frac{1}{2^s}
\]
for simplicity. The definition of the probability distribution (3.2) gives rise to the information of multi-collisions.

Let $l$ denote any positive integer to describe any $l$-collision $G_{s}^{-1}(c)$ with $l = \# G_{s}^{-1}(c)$, where a 1-collision means a 1-element set that consists of the one-to-one element. For the aspect of multi-fractal analysis, we should consider the exponent $\alpha$ such that
\[
P^{(s)}(c) = \left( \frac{1}{A_s} \right)^\alpha
\]
for any \( c \). The exponent \( \alpha \) is called \textit{singularity exponent} in the context of multi-fractal analysis. From (3.2), \( \alpha \) is corresponding to \( l \)-collisions \( G^{-1}_s(c) \) for a fixed \( l \). So, in our situation, we may investigate \( l \)-collisions for any \( l \) instead of the strength of singularity \( \alpha \). Indeed, all of \( l \)-collisions for any fixed \( l \) yields a “mono-fractal” and a “multi-fractal” is described when \( l \) is varied arbitrarily. In Chapter 4, we will give one of possible approaches to a mono-fractal.

Hereafter, we concentrate to investigate the \( q \)-fractal dimension \( D_q \) for the subset sum function. In the following proposition, we give the relation between the density \( \rho_s \) and the \( q \)-fractal dimension \( D_q \) for the subset sum problem.

**Proposition 3.3.** Let \( \rho_s \) denote the density of the subset sum problem. Assume that the probability distribution is as described in (3.2). Then \( D_{-\infty} = \rho_s \). Moreover, if a subset sum function with density \( \rho_s \) has a collision, then the \( q \)-fractal dimension \( D_q \) is strictly decreasing for \( q \in \mathbb{R} \).

**Proof of Proposition 3.3.** It holds that

\[
D_{-\infty} = -\frac{\log(1/2^s)}{\log A_s} = \frac{s}{\log_2 A_s} = \rho_s.
\]

It follows from the general property of Rényi entropy that \( D_q \) is strongly decreasing.

The most interesting case is the case when \( \rho_s \) is bounded for any \( s \). In this case, the sequence \( \{A_s\}_s \) is strictly increasing and then the upper and lower limits of \( D_q \) as \( s \to \infty \) are bounded from above and below, respectively.

From Proposition 3.3 we can see that the quantity \( D_{-\infty} \) generalizes the density for the subset sum problem below. Consider a set \( \mathcal{M}_s \subseteq \{0, 1\}^s \) and assume that the domain of the subset sum function \( G_s \) is restricted to \( \mathcal{M}_s \), say \( G_s: \mathcal{M}_s \to \mathbb{Z}/A_s\mathbb{Z} \). Then we may define the probability distribution of \( G_s \) as

\[
P^{(s)}(c) = \frac{\#G^{-1}_s(c)}{\#\mathcal{M}_s}.
\]

With Proposition 3.3, we will call the quantity \( D_{-\infty} = \log \#\mathcal{M}_s/\log A_s \) the \textit{(generalized) density}. Let \( \mathcal{M}_s^{(k)} \) denote the set of all elements in \( \{0, 1\}^s \) of Hamming weight \( k \). The set \( \mathcal{M}_s^{(k)} \) may be regarded as the collection of all \( k \)-element subsets in the power set \( 2^U \). Assume that the Hamming weight \( k \) is fixed. Then for the set \( \mathcal{M}_s^{(k)} \), we can define the pseudo-density due to Nguyen and Stern [31] and the density due to Kunihiro [24] (which we refer to as the Kunihiro density). The Kunihiro density unifies the density \( \rho_s \) and the pseudo-density, which can be seen as follows. If \( \sum_{j=1}^s x_j \) is close to 0, then the pseudo-density is regarded as the Kunihiro density. Moreover, if \( \sum_{j=1}^s x_j \) is close to \( s/2 \), then the Kunihiro density is regarded as the density \( \rho_s \) in (2.2). The Kunihiro density has some information theoretic property such as the information rate. For CR and OTU cryptosystems, \( \mathcal{M}_s^{(k)} \) is the set of
encoded plaintexts in order to encrypt each of plaintexts. Although the density $D_{-\infty}$ has no sense as the information rate, it should have some meaning as the $q$-fractal dimensions and the generalized dimensions via any $q$. In Section 4, we describe another approach to a subset sum function with a restricted domain.

With (3.2), the definition of the $q$-fractal dimension $D_0$ at $q = 0$ is replaced by

$$D_0 = \frac{\log \# G_s\{(0, 1)^s\}}{\log A_s}.$$  (3.3)

This is regarded as a logarithmic version of “the density of solutions” to the subset sum problems in \[30, 39\].

For a subset sum function, the weak partition problem plays an essential role to find some collisions. We use the following lemma in order to find (multi-)collisions.

**Lemma 3.4.** Let $U = \{1, \ldots, s\}$, and $\{a_1, \ldots, a_s\}$ be a set of positive integers such that $1 \leq a_i \leq A_s - 1$. Let $S_1$ and $S_2$ denote subsets of $U$ such that $S_1 \cap S_2 = \emptyset$. Assume that

$$\sum_{j \in S_1} a_j \equiv \sum_{j \in S_2} a_j \pmod{A_s},$$

i.e. there is a solution to the weak partition problem. Then we can find at most $2^{\#(U \setminus (S_1 \cup S_2))}$ collisions for the subset sum function $G_s: \{0, 1\}^s \to \mathbb{Z}/A_s\mathbb{Z}$.

**Proof of Lemma 3.4.** Let $S'_1$ and $S'_2$ denote subsets of $U$. For each $i = 1, 2$ and each $j \in U$, we define $x^{(i)} = (x_1^{(i)}, \ldots, x_s^{(i)}) \in \{0, 1\}^s$ such that $x_j^{(i)} = 1$ if and only if $j \in S'_i$. For any $T \in 2^{U \setminus (S_1 \cup S_2)}$, we put $S'_1 = S_1 \cup T$ and $S'_2 = S_2 \cup T$. Then the set $\{x^{(1)}, x^{(2)}\}$ is a collision and the possible number of collisions of the function $G_s$ that are obtained from $\{S_1, S_2\}$ is at most $2^{\#(U \setminus (S_1 \cup S_2))}$. \qed

Notice that an ordered pair $(U, 2^{U \setminus (S_1 \cup S_2)})$ becomes an independence system with the ground set $U$ and the collection $2^{U \setminus (S_1 \cup S_2)}$ of independent sets. Hence, this independence system has some correspondence to the solution of the weak partition problem. For the details on the independent systems, see [23, Chapter 13].

For $s \in \mathbb{Z}_{>0}$, let $G_s: \{0, 1\}^s \to \mathbb{Z}/A_s\mathbb{Z}$ denote a subset sum function. If we consider an exact set cover of $\text{supp}(P^{(s)})$ by a family of 1-element subsets of $\mathbb{Z}/A_s\mathbb{Z}$, then this is corresponding to a minimal covering for the generalized dimension $d_q$.

**Lemma 3.5 (cf. \[39\]).** The subset sum function $G_s$ has a collision if and only if the corresponding weak partition problem has a solution.

Although a proof of Lemma 3.5 was given by Shamir in [39], we give an alternative proof.

**Proof of Lemma 3.5.** For some $c'$, let $G_s^{-1}(c') = \{S_1, \ldots, S_l\} \subseteq 2^U$ denote the $l$-collision. First, we prove the “only if” direction. We choose distinct sets $S_i, S_j \in G_s^{-1}(c')$. Then $\{S_i \setminus S_j, S_j \setminus S_i\}$ is a solution to the weak partition problem. The “if” direction follows from Lemma 3.4. \qed
Now we can estimate the lower bound of the $q$-fractal dimension $D_0$ at $q = 0$.

**Theorem 3.6.** For $\mathbf{y} = (y_1, \ldots, y_s) \in \{-1,0,1\}^s$, let $r(\mathbf{y})$ denote the number of zeros in $\mathbf{y}$, i.e. $r(\mathbf{y}) = \# \{j : y_j = 0\}$. Assume that the weak partition problem has a solution. Then

$$
\#G_s(\{0,1\}^s) \geq 2^s - \sum_{\mathbf{y}} 2^{r(\mathbf{y})},
$$

where $\mathbf{y}$ runs through all solutions of the weak partition problem with respect to $G_s$. Consequently, if the right hand side of (3.4) is positive, then we have

$$
D_0 \geq \log \left( \frac{2^s - \sum_{\mathbf{y}} 2^{r(\mathbf{y})}}{\log A_s} \right).
$$

**Proof of Theorem 3.6.** If the right hand side of (3.4) is positive, then it is clear that (3.4) implies (3.5). Hence, we prove (3.4). For some $c' \in G_s(\{0,1\}^s)$, we consider the $l$-collision $G_s^{-1}(c')$ with $l = \#G_s^{-1}(c')$. It follows from the proof of Lemma 3.3 that given an $l$-collision $G_s^{-1}(c') = \{x_1, \ldots, x_l\}$, we can find at most $\binom{2^s}{l}$ solutions to the weak partition problem. Hence, for each $i, j$ with $i < j$, $y_{i,j} \in \{-1,0,1\}^s$ is chosen from one of $x_i - x_j$ or $x_j - x_i$ so that the first component in $y_{i,j}$ is positive. Notice that $y_{i_1,j_1}$ and $y_{i_2,j_2}$ such that $(i_1, j_1) \neq (i_2, j_2)$, $i_1 < j_1$ and $i_2 < j_2$ may be equal. Hence, let $N_{c'}$ denote the set of $y_{i,j}$’s (without repetition) and assume that any two elements in $N_{c'}$ are not equivalent with respect to the weak partition problem. Then by using Lemma 3.4, there exists a non empty set $K_{c'} \subseteq G_s(\{0,1\}^s)$ such that

$$
\bigcup_{c \in K_{c'}} G_s^{-1}(c) \subseteq N_{c'}
$$

for some $c' \in G_s(\{0,1\}^s)$. Here we write

$$
2^s = \sum_{c \in G_s(\{0,1\}^s)} \sum_{x \in G_s^{-1}(c)} 1.
$$

Since (3.7) holds, we may choose $K_{c'}$ to be maximal under a given $N_{c'}$, and choose a collection $\{K_{c'}\}_{c'}$ of such sets which are pairwise disjoint. Here, we also write

$$
2^s = \#G_s(\{0,1\}^s) + \sum_{c \in G_s(\{0,1\}^s)} (\#G_s^{-1}(c) - 1).
$$

Applying (3.6) for every set in a collection $\{K_{c'}\}_{c'}$, the second term of (3.8) is bounded from above by $\sum_{\mathbf{y}} 2^{r(\mathbf{y})}$. Therefore (3.4) holds.

Related to the proof of Theorem 3.6, there is another approach to the all solutions to the weak partition problem. Let $\mathcal{G}$ denote a graph with vertex set $\{0,1\}^s$. For distinct
elements $x, x' \in \{0,1\}^s$, the set $\{x, x'\}$ is an edge in the graph $G$ if and only if there exists $c \in G_s(\{0,1\}^s)$ such that $\{x, x'\} \in G_s^{-1}(c)$. If there exists an $l$-collision $G_s^{-1}(c)$ such that $c \in G_s(\{0,1\}^s)$ and $l \geq 3$, then the $l$-collision $G_s^{-1}(c)$ has a one-to-one correspondence to some clique in the graph $G$. Especially, the maximal clique in the graph $G$ determines the value of the $q$-fractal dimension $D_\infty$ at $q = \infty$. Recall that we may consider an independence system for a solution to the weak partition problem and this independence system has some simple structure. From this, it may be used some greedy algorithm in order to find multi-collisions. Especially, maximizing $l$ subject to an $l$-collision $G_s^{-1}(c) \neq \emptyset$ for some $c$ becomes some optimization problem. Thus, the $q$-fractal dimensions $D_q$ for any $q$ are determined.

The following proposition guarantees the existence of a 4-collision for the subset sum function.

**Proposition 3.7.** Put $U = \{1, \ldots, s\}$. Let $\{a_1, \ldots, a_s\}$ be a set of integers with $1 \leq a_i \leq A_s - 1$ and let $\{S_1, S_2\}$ is a solution to the weak partition problem for this set. Suppose that there exists a non-empty set $T \subseteq U \setminus (S_1 \cup S_2)$ such that

$$\sum_{i \in S_1} a_i \equiv \sum_{i \in S_1 \cup T} a_i \pmod{A_s}.$$

Then $\{T, \emptyset\}$ is a solution to the weak partition problem. Moreover, there exists $c \in G_s(\{0,1\}^s)$ such that $\#G_s^{-1}(c) \geq 4$.

Here we consider the cases when the right hand side in (3.4) is negative. Let $\{a_1, \ldots, a_s\}$ be an arithmetic progression such that $a_j = ja$ for some positive $a \in \mathbb{Z}$ and let the notation $r(y)$ be as described in Theorem 3.6. We consider the weak partition problem for this arithmetic progression and a modulus $A_s = (s+1)a$. If $s = 3$, then $\{\{1, 3\}, \emptyset\}, \{\{1, 2\}, \{3\}\}$ and $\{\{1\}, \{2, 3\}\}$ yield the solutions $(1,0,1), (1,1,-1)$ and $(1,-1,-1)$, respectively. Hence,

$$2^s - \sum_y 2^{r(y)} = 4 > 0.$$

However, if $s = 4$, then

$$2^s - \sum_y 2^{r(y)} = -2 < 0.$$

In general, the following proposition holds.

**Proposition 3.8.** Let $\{a_1, \ldots, a_s\}$ be an arithmetic progression such that $a_j = ja$ for some positive $a \in \mathbb{Z}$. Assume that $s \geq 4$ and $A_s = (s+1)a$. Then the right hand side of (3.4) is negative.

**Proof of Proposition 3.8.** Consider each solution to the weak partition problem of the form $\{S, \emptyset\}$ for some 2-element subset $S$ of indices. From Lemma 3.4 and the assumptions, we have

$$\sum_y 2^{r(y)} \geq \binom{s}{2} 2^{s-2} > 2^s$$

12
since any 2-element subset of indices is a solution to the weak partition problem modulo \( A_s = (s + 1)a \). Hence, the right hand side of \( (3.4) \) is negative.

Notice that the (non-modular) subset sum problem is sometimes regarded as the restricted partition of a given positive integer. In order to give the exact value or better lower bound for the \( q \)-fractal dimension \( D_0 \) at \( q = 0 \), we will be able to apply several well-known techniques using generating functions and asymptotic formulae (e.g. \( [16] \)). In the case of an arithmetic progression, such techniques sometimes give rise to the exact value or a better estimate for any \( q \)-fractal dimension \( D_q \). In the other case, we omit the details.

4 Hausdorff Dimension and Similarity Dimension

In this section, we fix a positive integer \( s \). And we use the following notations. We denote by \( \mathcal{M} \) a set of \( \{0, 1\}^s \), by \( A \) a positive integer and by \( G: \mathcal{M} \to \mathbb{Z}/AZ \) a subset sum function with restricted domain \( \mathcal{M} \).

4.1 Iterated Function System and Self-Similar Set

In this subsection, we describe the results of Hutchinson \([19]\) in the only case of the complete metric space \( \mathbb{R} \) with respect to the absolute value \( |\cdot| \). For simplicity, let \( X \) denote a compact set of \( \mathbb{R} \), for which we will use a unit closed interval as \( X \) in next subsections.

**Definition 4.1** (Iterated Function System (IFS)). A family \( \Psi = \{\psi_c\}_c \) of functions is called an iterated function system (IFS) on \( X \) if it consists of a finite number of functions such that the each function \( \psi_c: X \to X \) is a contraction mapping, i.e. Lipschitz constants of functions in the IFS \( \Psi \) are less than 1.

**Definition 4.2** (Similarity Dimension). Let \( \Psi = \{\psi_c\}_c \) be an IFS on \( X \) with Lipschitz constants \( r_c \). Then a positive real number \( t \) is called the similarity dimension if \( \sum_c r_c^t = 1 \).

**Definition 4.3** (Similitude). Let \( \psi: X \to X \) a contraction mapping with Lipschitz constant \( r < 1 \). Then the mapping \( \psi \) is a similitude if
\[
|\psi(x) - \psi(y)| = r|x - y|
\]
for any \( x, y \in X \).

**Definition 4.4** (Open Set Condition). Let \( \Psi = \{\psi_c\}_c \) denote an IFS. Then the IFS \( \Psi \) satisfies the open set condition if there exists an open set \( O \subseteq \mathbb{R} \) satisfies that \( \psi(O) \subseteq O \) and \( \psi_c(O) \cap \psi_{c'}(O) = \emptyset \) \( (c \neq c') \).

It is well known that if the open set condition holds, then the Hausdorff dimension can be calculated from the similarity dimension \( \left[19\right] \).

13
Lemma 4.5 (cf. [19]). Let \( \Psi = \{ \psi_c \} \) denote an IFS of similitudes on \( X \), where each of similitudes in the IFS \( \Psi \) has Lipschitz constant \( r_c < 1 \). Assume that the IFS \( \Psi \) satisfies the open set condition. Then there exists the unique compact set \( F \) which satisfies the Hutchinson equation \( F = \bigcup_c \psi_c(F) \). Moreover, the Hausdorff dimension of \( F \), denoted by \( \text{dim}_H(F) \), is the unique solution \( t \) to the equation
\[
\sum_c r_c^t = 1,
\]
i.e. the Hausdorff dimension \( \text{dim}_H(F) \) is equal to the similarity dimension.

The above compact set \( F \) is called the self-similar set with respect to the IFS \( \Psi \).

4.2 Graph Theory and Box-Counting

In this subsection, the \( q \)-fractal dimension \( D_0 \) at \( q = 0 \) is defined by
\[
D_0 = \frac{\log \#G(M)}{\log A},
\]
which is analogous to (3.3). We suppose that \( G : M \to \mathbb{Z}/A\mathbb{Z} \) is injective, but not surjective. For some \( c_{\min}, c_{\max} \in \mathbb{Z} \), let \( A \) denote some complete residue system such that \( A = \{c_{\min}, c_{\min} + 1, \ldots, c_{\min} + A - 1\} \) with \( c_{\max} = c_{\min} + A - 1 \). We choose \( X = [c_{\min}/A, c_{\min}/A + 1] \) as a unit closed interval of \( \mathbb{R} \). For \( a \in A \), let \( X(a) = [a/A, (a + 1)/A] \) and let
\[
\mathcal{C}(X; A) := \{ X(a) : G(x) = a \mod A, \ x \in M, \ a \in A \},
\]
so that \( \bigcup \mathcal{C}(X; A) = \bigcup_{a \in A} X(a) = X \). Any set \( X(a) \) in the minimal cover \( \mathcal{C}(X; A) \) is a “box”. Put \( A' = \{ a : G(x) = a \mod A, \ x \in M, \ a \in A \} \). Hence, we have \( \bigcup \mathcal{C}(X; A') \subseteq X \). We consider the only case where both of \( \text{min} A' \) and \( \text{max} A' \) does not belong to \( A \).

Here we give some description using graph theory. For some detailed terminology, see [2]. Let \( \mathcal{H} \) denote the intersection graph of \( \mathcal{C}(X; A') \), i.e. the vertex set of the graph \( \mathcal{H} \) is \( A \) and for distinct elements \( a, a' \in A \), a set \( \{a, a'\} \) is an edge in the graph \( \mathcal{H} \) if and only if \( X(a) \cap X(a') \neq \emptyset \). Hence, a set \( \{c_{\min}, c_{\max}\} \) is not edge in the graph \( \mathcal{H} \). It can be seen that each connected component in the graph \( \mathcal{H} \) is a path since \( G : M \to \mathbb{Z}/A\mathbb{Z} \) is not surjective. If \( c \) is the smallest vertex in a connected component in the graph \( \mathcal{H} \), then we identify \( c \) with the connected component in the graph \( \mathcal{H} \).

Put \( n = \#G(M) \). Let \( n' \) denote the number of connected components in \( \bigcup \mathcal{C}(X; A') \), let \( r_c \) denote the length of each connected component in \( \bigcup \mathcal{C}(X; A') \) and let \( b_c \) denote the the number of vertices in the connected component \( c \). Notice that a connected component in a graph \( \mathcal{H} \) has the corresponding connected component in the set \( \bigcup \mathcal{C}(X; A') \). Hence \( n' \) is also the number of connected components in the graph \( \mathcal{H} \).
4.3 Hausdorff Dimension Related to A Subset Sum Function

In this subsection, let $X$ denote a unit closed interval. We combine descriptions of the previous subsections in Section 4. Now we can describe the relation between the number of connected components in the graph, the Hausdorff dimension and the $q$-fractal dimension at $q = 0$ (cf. [7]).

**Theorem 4.6.** The notations $D_0$, $\mathcal{H}$, $c$, $n$, $n'$ and $b_c$ are as described in Subsection 4.2. Let $G: \mathcal{M} \to \mathbb{Z}/\mathbb{A}$ denote a subset sum function, let $\Psi = \{\psi_c\}_{c}$ denote the IFS of similitudes on $X$ such that for each $c$, the function $\psi_c(x)$ is given by

$$\psi_c(x) = \frac{b_c}{A} \left( x - \frac{c}{A} \right) + \frac{c}{A} \quad \text{or} \quad \psi_c(x) = -\frac{b_c}{A} \left( x - \frac{c}{A} \right) + \frac{c + b_c}{A}.$$ 

and let $F$ denote the unique self-similar set with respect to the IFS $\Psi$. Then we have

$$\frac{\log n'}{\log A} \leq \dim_H(F) \leq \frac{\log n}{\log A} = D_0,$$

(4.1)

where $\dim_H(F)$ is the Hausdorff dimension of $F$.

**Proof of Theorem 4.6.** It is clear that the IFS $\Psi$ satisfies the open set condition. Put $f(t) = \sum_c t_c - 1$. Using Lemma 4.5, the function $f(t)$ satisfies that

$$f \left( \frac{\log n'}{\log A} \right) > 0, \quad f \left( \dim_H(F) \right) = 0 \quad \text{and} \quad f(D_0) < 0.$$ 

The relation (4.1) follows from the monotonicity of the function $f(t)$.

**Remark 4.7.** In [7], it is also used the intersection graph. However, the intersection graph is constructed from the intersection of a collection $\{\psi_c(F)\}_{c}$ for a self similar set $F$ with respect to a general IFS $\Psi = \{\psi_c\}_{c}$ on a compact set of a Euclidean space. However, our construction of the self-similar set $F$ is from the intersection graph of the “generator” $\mathcal{C}(X; \mathcal{A}')$.

Although $n$ and $n'$ are integers, $A^{\dim_H(F)}$ is not necessarily an integer. Indeed, if $n' = n-1$, then $A^{\dim_H(F)}$ is not an integer. The Hausdorff dimension $\dim_H(F)$ has some information on connected components. Indeed, the longer a connected component is, the smaller the Hausdorff dimension $\dim_H(F)$ is. Moreover, if some connected components are long, then there are a small number of connected components.

The structure of the self-similar set $F$ can be interpreted as the digit patterns of elements in the self-similar set $F$, which we can see as follows. Let $\mathcal{B}$ be a finite alphabet set and let $\mathcal{B}^\mathbb{N} = \{\mathbf{c} = (c_1, c_2, \ldots) : c_i \in \mathcal{B}, \ i \in \mathbb{N}\}$, where $\mathbb{N} = \{1, 2, \ldots\}$ is the set of positive integers. Assume that $\mathcal{B}$ is endowed with the discrete topology and $\mathcal{B}^\mathbb{N}$ with the product topology. Then $\mathcal{B}^\mathbb{N}$ is totally disconnected (i.e. 1-point sets are maximal connected components) in this topology. If $\mathcal{B} = \mathcal{A}$, then each element $\mathbf{c} \in \mathcal{B}^\mathbb{N}$ is regarded as a real number represented in base $A$ using the digit set $\mathcal{B}$. Moreover, if $\mathcal{B} = \mathcal{A}'$, then we can identify $\mathcal{B}^\mathbb{N}$ with the
self-similar set \( F \) by using some coordinate map (cf. \([19]\)). If an adversary can use the digit structure in \( F \), then the adversary may have some ability to cryptanalyze for a cryptosystem.

For the proof of Theorem 4.6, notice that the function \( G: \mathcal{M} \rightarrow \mathbb{Z}/A\mathbb{Z} \) may not be presumed to be the subset sum function. Let \( \mathcal{M} \) denote a set, which does not necessarily satisfy \( \mathcal{M} \subseteq \{0,1\}^s \). The analogue of this theorem holds for any algorithm \( G \) with an input element in \( \mathcal{M} \) and an output element in \( \mathbb{Z}/A\mathbb{Z} \). We omit the details.

5 Concluding Remarks

In the case of the classical correlation dimension, the number of elements in the orbit of a discrete dynamical system that visit each box can be efficiently estimated by using its neighborhoods (\([41]\)). In the case of some classical generalized dimensions, it is somewhat difficult to estimate them. Although several correlation integrals or correlation functions are used for integers \( q \geq 2 \) in the classical case (\([14,13,17]\)), our non-classical generalized dimensions required combinatorial methods instead. The future work will be to investigate detailed combinatorial structures of subset sum problems.

In Section 4, we gave the self-similar set \( F \) by using a certain method. One may generalize the techniques of this paper for several problems which are often used in cryptography. From some point of view, the technique in Section 4 will be applicable not only for a cryptosystem based on the subset sum problem but also for a cryptosystem based on mathematical problems.

A totally disconnected set in Euclidean space (in general, a set in a metric space with topological dimension 0) is sometimes called fractal dust, especially by Mandelbrot \([28]\). The fractal dust \( F \) was appropriate for the descriptions of fractal and multifractal analysis in this paper.

Mandelbrot’s definition of a fractal set, as one of the definitions, is that the topological dimension is strictly less than the Hausdorff dimension. We will also expect to describe cryptoanalysis using any other fractal set. If one admits another definition of a fractal set, then it will be accelerated.

For the construction of a self-similar set in Section 4, the several classical methods are applicable (\([13]\)). If there is some good generalization of the technique in Section 4 then it will be applicable to non-malleable cryptography \([34, 6]\).

Acknowledgements

The author would like to thank Professor Keisuke Shiromoto for helpful comments. The author would like to thank Professor Shuya Chiba for detailed advice. The author would like to thank Professor Emeritus Koichiro Naito for useful suggestions.
References

[1] M. Ajtai. “The shortest vector problem in $L^2$ is NP-hard for randomized reductions”. In: Proceedings of the 30th annual ACM symposium on Theory of computing. ACM, 1998, pp. 10–19.

[2] J.A. Bondy and U.S.R. Murty. Graph Theory. Graduate Texts in Mathematics. Springer-Verlag London, 2008.

[3] E.F. Brickell and A.M. Odlyzko. “Cryptanalysis: A survey of recent results”. In: Contemporary Cryptology. IEEE Press, 1991, pp.501–540.

[4] B. Chor and R.L. Rivest. “A knapsack-type public key cryptosystem based on arithmetic in finite fields”. In: IEEE Transactions on Information Theory 34 (1988), pp. 901–909.

[5] M.J. Coster, A. Joux, B.A. Lamacchia, A.M. Odlyzko, C.P. Schnorr, and J. Stern. “Improved low-density subset sum algorithms”. In: computational complexity 2 (1992), pp. 111–128.

[6] D. Dolev, C. Dwork, and M. Naor. “Nonmalleable cryptography”. In: SIAM Review 45 (2003), pp. 727–784.

[7] J.H. Elton and M. Piccioni. “Iterated function systems arising from recursive estimation problems”. In: Probability Theory and Related Fields 91 (1992), pp. 103–114.

[8] P. van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in a lattice. Technical Report. 81–04. Mathematics Department, University of Amsterdam, 1981.

[9] K.J. Falconer. The geometry of fractal sets. Cambridge University Press, 1986.

[10] S. Faust, D. Masny, and D. Venturi. Chosen-Ciphertext Security from Subset Sum. Cryptology ePrint Archive, Report 2015/1223. https://eprint.iacr.org/2015/1223. 2015.

[11] S. Furuya and K. Yakubo. “Multifractality of complex networks”. In: Physical Review E 84 (2011), p. 036118.

[12] M.R. Garey and D.S. Johnson. Computers and intractability: A Guide to the Theory of NP-Completeness. WH Freeman and Company, 1979.

[13] P. Grassberger. “Generalized Dimensions of Strange Attractors”. In: Physics Letters A 97 (1983), pp. 227–230.

[14] P. Grassberger and I. Procaccia. “Characterization of Strange Attractors”. In: Physical Review Letters 50 (1983), pp. 346–349.

[15] T.C. Halsey, M.H. Jensen, L.P. Kadanoff, I. Procaccia, and B.I. Shraiman. “Fractal measures and their singularities: The characterization of strange sets”. In: Physical Review A 33 (1986), pp. 1141–1151.
[16] G.H. Hardy and S. Ramanujan. “Asymptotic Formulae in Combinatorial Analysis”. In: Proceedings of the London Mathematical Society. s2-17. Wiley Online Library, 1918, pp. 75–115.

[17] H.G.E. Hentschel and I. Procaccia. “The infinite number of generalized dimensions of fractals and strange attractors”. In: Physica D 8 (1983), pp. 435–444.

[18] A. Hosoyamada, Y. Sasaki, and K. Xagawa. “Quantum Multicollision-Finding Algorithm”. In: Advances in Cryptology – ASIACRYPT 2017. Springer International Publishing, 2017, pp. 179–210.

[19] J.E. Hutchinson. “Fractals and self similarity”. In: Indiana University Mathematics Journal 30 (1981), pp. 713–747.

[20] R. Impagliazzo and M. Naor. “Efficient cryptographic schemes provably as secure as subset sum”. In: Journal of Cryptology 9 (1996), pp. 199–216.

[21] A. Joux and L. Granboulan. “A practical attack against knapsack based hash functions”. In: Advances in Cryptology – EUROCRYPT 1994. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 58–66.

[22] R.M. Karp. “Reducibility among Combinatorial Problems”. In: Complexity of Computer Computations. Boston, MA: Springer US, 1972, pp. 85–103.

[23] B. Korte and J. Vygen. Combinatorial Optimization: Theory and Algorithms. 4th ed. Springer-Verlag Berlin Heidelberg, 2007.

[24] N. Kunihiro. “New Definition of Density on Knapsack Cryptosystems”. In: Progress in Cryptology – AFRICACRYPT 2008. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 156–173.

[25] J. C. Lagarias. “The computational complexity of simultaneous Diophantine approximation problems”. In: SIAM Journal on Computing 14 (1985), pp. 196–209.

[26] J.C. Lagarias and A.M. Odlyzko. “Solving low-density subset sum problems”. In: Journal of the ACM 32 (1985), pp. 229–246.

[27] V. Lyubashevsky, A. Palacio, and G. Segev. “Public-key Cryptographic Primitives Provably As Secure As Subset Sum”. In: Proceedings of the 7th International Conference on Theory of Cryptography. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 382–400.

[28] B.B. Mandelbrot. The fractal geometry of nature. 173. WH freeman New York.

[29] J.E. Mazo and A.M. Odlyzko. “Lattice points in high-dimensional spheres”. In: Monatshefte für Mathematik 110 (1990), pp. 47–61.

[30] R.C. Merkle and M.E. Hellman. “Hiding information and signatures in trapdoor knapsacks”. In: IEEE Transactions on Information Theory 24 (1978), pp. 525–530.
[31] P.Q. Nguyen and J. Stern. “Adapting Density Attacks to Low-Weight Knapsacks”. In: Advances in Cryptology – ASIACRYPT 2005. Springer Berlin Heidelberg, 2005, pp. 41–58.

[32] A.M. Odlyzko. “The rise and fall of knapsack cryptosystems”. In: Cryptology and computational number theory 42 (1990), pp. 75–88.

[33] T. Okamoto, K. Tanaka, and S. Uchiyama. “Quantum Public-Key Cryptosystems”. In: Advances in Cryptology - CRYPTO 2000. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 147–165.

[34] R. Pass, A. Shelat, and V. Vaikuntanathan. “Relations Among Notions of Non-malleability for Encryption”. In: Advances in Cryptology – ASIACRYPT 2007. Springer Berlin Heidelberg, 2007, pp. 519–535.

[35] A. Rényi. “On Measures of Entropy and Information”. In: Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability. 1. 1961, pp. 547–561.

[36] A. Rényi. “On the dimension and entropy of probability distributions”. In: Acta Mathematica Academiae Scientiarum Hungarica 1 (1959), pp. 193–215.

[37] C.P. Schnorr and M. Euchner. “Lattice basis reduction: Improved practical algorithms and solving subset sum problems”. In: Mathematical Programming 66 (1994), pp. 181–199.

[38] A. Shamir. “A Polynomial-Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem”. In: IEEE Transactions on Information Theory 30 (1984), pp. 699–704.

[39] A. Shamir. “On the Cryptocomplexity of Knapsack Systems”. In: Proceedings of the 11th Annual ACM Symposium on the Theory of Computing. ACM, 1979, pp. 118–129.

[40] A. Shamir. “The Cryptographic Security of Compact Knapsacks (Preliminary Report)”. In: IEEE Symposium on Security and Privacy 1980. IEEE, 1980, pp. 94–94.

[41] J. Theiler. “Efficient algorithm for estimating the correlation dimension from a set of discrete points”. In: Physical Review A 36 (1987), pp. 4456–4462.

[42] S. Vaudenay. “Cryptanalysis of the Chor-Rivest Cryptosystem”. In: Journal of Cryptology 14 (2001), pp. 87–100.