A New Measure of Watermarking Security Applied on DC-DM QIM

Teddy Furon, Patrick Bas

A New Measure of Watermarking Security Applied on QIM

Teddy Furon[1] and Patrick Bas[2⋆]

[1] INRIA Research Centre Rennes Bretagne Atlantique, France
teddy.furon@inria.fr
[2] CNRS-LAGIS, Ecole Centrale de Lille, France
patrick.bas@ec-lille.fr

Abstract. Whereas the embedding distortion, the payload and the robustness of digital watermarking schemes are well understood, the notion of security is still not completely well defined. The approach proposed in the last five years is too theoretical and solely considers the embedding process, which is half of the watermarking scheme. This paper proposes a new measurement of watermarking security, called the *effective key length*, which captures the difficulty for the adversary to get access to the watermarking channel. This new methodology is applied to the Distortion Compensated Dither Modulation Quantized Index Modulation (DC-DM QIM) watermarking scheme where the dither vector plays the role of the secret key. This paper presents theoretical and practical computations of the effective key length. It shows that this scheme is not secure as soon as the adversary gets observations in the Known Message Attack context.

Keywords: watermarking, security, Quantized Index Modulation

1 Introduction

The problem: This paper deals with the evaluation of the security level of a digital watermarking scheme. The problem is that the previous methodology on this topic [1], although applied on Spread Spectrum [2] and Dither Modulated Distortion Compensated Quantized Index Modulation (DM-DC QIM) [3] watermarking schemes, is not so successful. As detailed in Sect. 2, it does not fully capture the whole watermarking scheme as it only considers the embedding process. Its assessment is mostly theoretical and difficult to apply on real-life watermarking schemes. One has important difficulties in interpreting the quantity measuring the security level by relying only on information theory.

Example: Let us take the following scenario: consider a DC-DM QIM with a cubic lattice (a.k.a. SCS, Scalar Costa Scheme [4]) for embedding bits in a signal $\mathbf{x}$, at a given DWR (Document to Watermark power Ratio) and a given expected

⋆ P. Bas' work was partly founded by the French National Research Agency program referenced ANR-10-CORD-019 under the Estampille project.

WNR (Watermark to Noise power Ratio). Denote Δ the quantization step and α the compensation parameter. Now, the security level when measured by the equivocation equals $\log((1-\alpha)\Delta)$ nats [3]. Suppose now that we watermark the scaled signal $2 * \mathbf{x}$ with the same technique and setup (DWR, WNR). Then, the quantization step is now 2Δ while α remains the same. The security level is now higher by 0.69 nats. It is counterintuitive that by doubling the amplitude of the host signal, we succeed to increase the security level. Moreover this amount is indeed hard to understand: Does 0.69 nats represent a big increase in term of security?

Our contributions: This paper proposes a new way of defining the security level of a digital watermarking scheme in Sect. 3. Sect. 4 applies this methodology to QIM watermarking schemes from a theoretical point of view, while Sect. 5 presents an experimental framework to evaluate the security level. Our contributions are the following:

- A framework for security assessment in line with the cryptographic approach,
- A theoretical derivation of the security levels for watermarking schemes based on Quantized Index Modulation (QIM) with self-similar lattices,
- Theoretical bounds of the security levels when the lattices are not self-similar,
- An experimental setup for estimating the security levels for QIM.

2 The Problem with Previous Security Measures

From the beginning, watermarking has been characterized by a trade-off between the embedding distortion and the capacity. The capacity is the theoretical amount of hidden data that can be reliably transmitted when facing an attack of a given strength. In practice, the operating point of a watermarking technique is defined by the embedding distortion (measured by a DWR for instance), a payload (measured in bits per host samples for instance) and the robustness (for instance, measured by a Symbol Error Rate SER after an attack - compression, rotation etc).

Security came as a fourth feature stemming from applications where there exist attackers willing to circumvent watermarking such as copy and/or copyright protection. The efforts of the pioneering works introducing this new concept first focused on stressing the distinction between security and robustness. An early definition was coined by Ton Kalker as *the inability by unauthorized users to have access to the raw watermarking channel* [5].

The problem we see lies in the fact that the methodology proposed so far poorly captures T. Kalker's definition. In a nutshell, the methodology of [1–3] is based on C. E. Shannon definition of security for crypto-systems. The security level is defined as the amount of uncertainty the attacker has about the secret key. This is measured by the equivocation which is the entropy of the key knowing some observations, which are for instance contents watermarked with the same technique and the same secret key. The equivocation, be it valued in nats or

bits, can be negative (if the secret key is a continuous random variable), and as illustrated in the example of the introduction, the results of this approach are sometimes hard to understand.

The main pitfall is that watermarking and symmetric cryptography strongly disagree in the following point: In symmetric cryptography, the deciphering key is the secret key which is unique. Therefore, inferring this key from the observations (here, say some cipher texts) is the main task of the attacker. The disclosure of this key grants the adversary the access to the crypto-channel.

This is not the case in watermarking for the simple reason that there is no unique key to decode the hidden messages. In many watermarking schemes, the secret is a signal lying in the same space as the host vector: the carriers for Spread Spectrum, the dither for DC-DM QIM. They are generated by a Pseudo-Random Number Generator (PRNG) fed by a secret seed. Yet, the attacker may use another generator, or use some observations to estimate these signals. Therefore, the real secret granting access to the watermarking channel is less the seed of the PRNG than these signals. In the sequel, the secret signal is denoted by $\mathbf{k}$ and we show that a close enough signal $\mathbf{k}'$ may decode the hidden messages.

Consequently, inferring the secret key $\mathbf{k}$ from the observations (here, say some watermarked contents) is not the ultimate goal of the attacker. As T. Kalker stated, it is the access to the watermarking channel that matters. The estimation of the secret key is a possible path to this goal, but not the final destination. The limit of the past articles on watermarking security is that they focus on the estimation of the secret key, but very few works deal with the impact of the estimation accuracy on the access to the watermarking channel. It is quite symptomatic that almost none of them consider the decoding of the watermarking schemes. We strongly believe that this is the reason why the outcomes of this methodology are quite difficult to understand. C. E. Shannon was right, but those who translated his theory to watermarking only capture half the problem. The only exception we are aware of is [6] which intuitively sketched the idea that is formalized in this paper.

3 Our New Approach

3.1 The Idea

The keystone of our approach is the brute force attack. In cryptanalysis, the attacker randomly draws a test key and decrypts the ciphertexts. It is assumed that a genie tells the attacker when he succeeds, ie. when the test key equals the secret key. If the secret is a N-bit word, the probability of this event is $P = 1/2^N$, ie. one single secret key over 2^N possible keys. With some observations, the attacker might reduce the key space which increases the probability of success to $P = 2^{-L}$, with $L < N$. The security level is measured by $L = -\log_2(P)$ in bits.

We use the same approach for watermarking security. The *inability by unauthorized users to have access to the raw watermarking channel* is measured by

$-\log_2(P)$, where P is the probability that the attacker finds a key granting the decoding of hidden messages embedded with the secret key. Contrary to symmetric cryptographic, there are a plurality of such a key ; and this is mainly due to the fact that the embedding has to be robust. We name them the *equivalent decoding keys*. Note that we could also consider *equivalent embedding keys*, ie. keys embedding messages in host content which are reliably decoded by the secret key. Our methodology aims at resolving the following questions:

- What is an equivalent decoding key?
- How many equivalent decoding keys do exist?
- What is the probability of picking an equivalent decoding key?
- How to improve the odds thanks to the observations?

3.2 The Setup

Before producing any watermarked content, the designer draws the secret key $\mathbf{k}$ in the key space $\mathcal{K}$ according to a given distribution $p_{\mathbf{K}}$. There is an extraction function that computes a vector $\mathbf{x} \in \mathcal{X}$ from a content. Usually, $\mathcal{X} = \mathbb{R}^{N_v}$. The embedding modifies this vector into $\mathbf{y}$ under a distortion constraint (here, given by a bound on the Euclidean distance $\|\mathbf{y} - \mathbf{x}\|^2 \leq N_v D$). There is an inverse extraction function which maps $\mathbf{y}$ back into the content. We assume that the extraction process is public, and that the secret key $\mathbf{k}$ is only used for shaping $\mathbf{x}$ into $\mathbf{y}$: The embedder creates a watermarked vector $\mathbf{y} \in \mathcal{X}$ with hidden message m using the embedding function $e(.)$: $\mathbf{y} = e(\mathbf{x}, m, \mathbf{k})$. At the decoding side, a vector is computed from the received content with the same extraction function. The message $\hat{m}$ is decoded from the watermarked vector by $\hat{m} = d(\mathbf{y}, \mathbf{k})$.

The adversary sees N_o independent observations $\mathbf{O}^{N_o} = (\mathbf{O}_1, \ldots, \mathbf{O}_{N_o})$. The nature of these observations defines the attack. In this paper, we restrict our attention to the Known Message Attack (KMA) where an observation is a pair of a watermarked content and the embedded message: $\mathbf{O}_i = \{\mathbf{y}_i, m_i\}$. The article [1] gives a list of other attacks.

We define by $\mathcal{D}_m(\mathbf{k}) \subset \mathcal{X}$ the decoding region associated to the message m and for the key $\mathbf{k}$ by:

$$\mathcal{D}_m(\mathbf{k}) \triangleq \{\mathbf{y} \in \mathcal{X} : d(\mathbf{y}, \mathbf{k}) = m\}. \tag{1}$$

The topology and location of this region in $\mathcal{X}$ depends of the watermarking scheme and of $\mathbf{k}$.

To hide message m, the encoder pushes the host vector $\mathbf{x}$ deep inside $\mathcal{D}_m(\mathbf{k})$, and this creates an embedding region $\mathcal{E}_m(\mathbf{k}) \subseteq \mathcal{X}$:

$$\mathcal{E}_m(\mathbf{k}) \triangleq \{\mathbf{y} \in \mathcal{X} : \exists \mathbf{x} \in \mathcal{X} \text{ s.t. } \mathbf{y} = e(\mathbf{x}, m, \mathbf{k})\}. \tag{2}$$

Watermarking provides robustness by pushing the watermarked vectors far away from the boundary of the decoding region. If the vector extracted from an attacked content $\mathbf{z} = \mathbf{y} + \mathbf{n}$ goes out of $\mathcal{E}_m(\mathbf{k})$, $\mathbf{z}$ might still be in $\mathcal{D}_m(\mathbf{k})$ and the correct message is decoded.

For QIM based watermarking schemes, we often have $\mathcal{E}_m(\mathbf{k}) \subseteq \mathcal{D}_m(\mathbf{k})$. Therefore, there might exist another key $\mathbf{k}'$ such that $\mathcal{E}_m(\mathbf{k}) \subseteq \mathcal{D}_m(\mathbf{k}')$, $\forall m$. A graphical illustration of this phenomenon is depicted on Fig. 1.

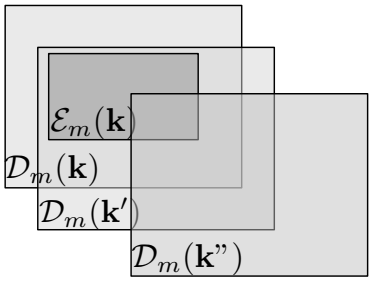

Fig. 1. Graphical representation in space $\mathcal{X}$ of three decoding regions $\mathcal{D}_m(\mathbf{k})$, $\mathcal{D}_m(\mathbf{k}')$ and $\mathcal{D}_m(\mathbf{k}'')$ and the embedding region $\mathcal{E}_m(\mathbf{k})$: $\mathbf{k}$ and $\mathbf{k}'$ belong to the equivalent decoding region $\mathcal{K}_{eq}^{(d)}(\mathbf{k}, 0)$, but $\mathbf{k}''$ does not.

3.3 The Equivalent Keys

We now define the equivalent keys and the associated equivalent region. We should make the distinction between the equivalent decoding keys and the equivalent embedding keys. But we restrict our attention to the decoding problem in this paper, and we use the term equivalent keys.

The set of equivalent keys $\mathcal{K}_{eq}(\mathbf{k}, \epsilon) \subset \mathcal{K}$ with $0 \leq \epsilon$ is defined as the set of keys that allows a decoding of the hidden messages embedded with $\mathbf{k}$ with a probability bigger than $1 - \epsilon$:

$$\mathcal{K}_{eq}(\mathbf{k}, \epsilon) = \{\mathbf{k}' \in \mathcal{K} : \mathbb{P}\left[d(e(\mathbf{X}, M, \mathbf{k}), \mathbf{k}') \neq M\right] \leq \epsilon\}. \tag{3}$$

Due to a lack of space, this paper focuses on $\epsilon = 0$ giving birth to an equivalent definition:

$$\mathcal{K}_{eq}(\mathbf{k}, 0) = \{\mathbf{k}' \in \mathcal{K} : \mathcal{E}_m(\mathbf{k}) \subseteq \mathcal{D}_m(\mathbf{k}')\}. \tag{4}$$

This set is usually not empty for QIM: if $\mathcal{E}_m(\mathbf{k}) \subseteq \mathcal{D}_m(\mathbf{k})$, $\mathbf{k}$ is then an element of $\mathcal{K}_{eq}(\mathbf{k}, 0)$.

3.4 The Effective Key Length

We introduce the notion of *effective key length* as a way to measure security. The adversary picks a key $\mathbf{k}' \in \mathcal{K}$ taking into account the set of observations $\mathbf{O}^{N_o}$ with an estimator: $\mathbf{K}' = g(\mathbf{O}^{N_o})$. The estimator $g(\cdot)$ is either deterministic or stochastic such that $\mathbf{K}' \sim p(\mathbf{k}'|\mathbf{O}^{N_o})$ for instance. A graphical example of the key space $\mathcal{K}$ is depicted in Fig. 2.

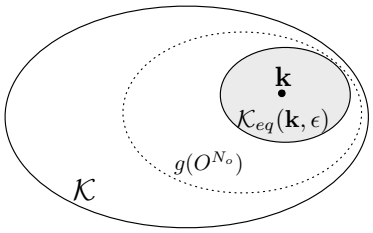

Fig. 2. Graphical representation of the key space $\mathcal{K}$ and the equivalent region $\mathcal{K}_{eq}(\mathbf{k},\epsilon)$. The dotted boundary represents the support of the estimator $g(O^{N_o})$ used to draw new test keys when the adversary has N_o observations.

The probability $P(\epsilon, N_o)$ that the adversary picks up a key belonging to the equivalent region is:

$$P^{(d)}(\epsilon, N_o) = \mathbb{E}_{\mathbf{K}}[\mathbb{E}_{\mathbf{O}^{N_o}}[\mathbb{E}_{\mathbf{K}'}[\mathbf{K}' \in \mathcal{K}_{eq}(\mathbf{K},\epsilon)|\mathbf{O}^{N_o}]]]. \tag{5}$$

Finally, to obtain an analogy with cryptography, the effective key length $\ell(\epsilon, N_o)$ translates this probability into bits as follows:

$$\ell(\epsilon, N_o) \triangleq -\log_2(P(\epsilon, N_o)) \quad \text{bits.} \tag{6}$$

The bigger the effective key length, the less likely is the attacker to find keys granting the access to the watermarking channel, and therefore, the more secure is the watermarking scheme. This measurement of the security is in line with Kalker's definition. It is easily interpretable. It doesn't rely on information theoretical element, and it takes into account the embedding and the decoding of the watermarking scheme.

4 Technical Details: Part I - Theoretical Analysis

This section applies the above methodology to DC-DM QIM watermarking. We give close form expressions for self-similar lattices and upper and lower bounds in the general case.

4.1 A Primer on DC-DM QIM Watermarking

Let us model the host signal by a vector $\mathbf{x} \in \mathbb{R}^{N_v}$. Consider a coarse Euclidean lattice $\Lambda_c \subset \mathbb{R}^{N_v}$. The origin $\mathbf{0} \in \mathbb{R}^{N_v}$ is an element of Λ_c and the Voronoi cell is defined as the set of vectors of $\mathbb{R}^{N_v}$ closer to $\mathbf{0}$ than to any other element of Λ_c: $\mathcal{V}(\Lambda_c) \triangleq \{\mathbf{v} \in \mathbb{R}^{N_v} | Q_{\Lambda_c}(\mathbf{v}) = \mathbf{0}\}$ where $Q_{\Lambda_c}(\cdot)$ is the Euclidean quantizer on Λ_c. The Voronoi cell of a lattice is a centrally symmetric, convex polytope.

For each message $m \in \mathcal{M}$ with say $\mathcal{M} = \{1, 2, \ldots, M\}$, a coset leader $\mathbf{d}_m \in \mathbb{R}^{N_v}$ is defined such that $\Lambda_f = \cup_{m=1}^{M}(\Lambda_c + \mathbf{d}_m)$ is a finer lattice. This induces the partition of Λ_f into M shifted versions of Λ_c, which implies that

$$|\mathcal{M}| = M = \text{vol}(\mathcal{V}(\Lambda_c))/\text{vol}(\mathcal{V}(\Lambda_f)), \tag{7}$$

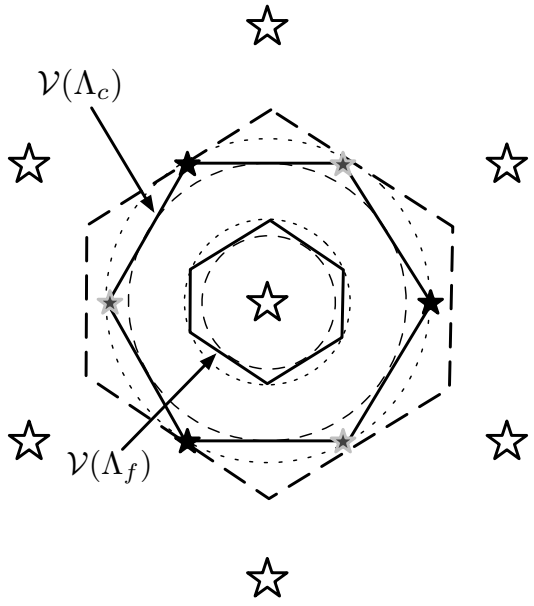

Fig. 3. 2D representation of the different elements used to compute the equivalent region. The large stars represent elements of the coarse lattice Λ_c, the small and large stars represents the fine lattice Λ_f, associated with the Voronoi cells $\mathcal{V}(\Lambda_c)$ and $\mathcal{V}(\Lambda_f)$. In this specific non-similar construction with the hexagonal lattice, $M = 3$. The dotted and dashed circles represent balls with radius of $R(\Lambda)$ and $r(\Lambda)$ respectively. The dashed hexagone is the scaled version of $\mathcal{V}(\Lambda_f)$ used to compute the lower bound in (20).

with $\mathrm{vol}(\mathcal{A})$ the volume of subset $\mathcal{A} \subset \mathcal{X}$. Define $r(\Lambda)$ the packing radius of lattice Λ as the radius of the largest hyper-ball contained in $\mathcal{V}(\Lambda)$ and $R(\Lambda)$ the covering radius of Λ as the radius of the smallest hyper-ball containing $\mathcal{V}(\Lambda)$. Denote $\mathcal{B}(\mathbf{x}, r)$ the hyperball centered on $\mathbf{x}$ of radius r (see Fig. 3). Then, $\mathcal{B}(\mathbf{0}, r(\Lambda)) \subset \mathcal{V}(\Lambda) \subset \mathcal{B}(\mathbf{0}, R(\Lambda))$. Finally, define $\rho(\Lambda)$ the effective radius of Λ such that $\mathrm{vol}(\mathcal{B}(\mathbf{0}, \rho(\Lambda))) = \mathrm{vol}(\mathcal{V}(\Lambda))$. Eq. (7) means that

$$M = (\rho(\Lambda_c)/\rho(\Lambda_f))^n. \tag{8}$$

Hiding message m in $\mathbf{x}$ with a DC-DM QIM technique yields watermarked vector $\mathbf{y}$:

$$\begin{aligned}\mathbf{y} = e(\mathbf{x}, m, \mathbf{k}) &= \mathbf{x} + \alpha(Q_{\Lambda_c}(\mathbf{x} - \mathbf{d}_m - \mathbf{k}) - \mathbf{x} + \mathbf{d}_m + \mathbf{k}) \\ &= Q_{\Lambda_c}(\mathbf{x} - \mathbf{d}_m - \mathbf{k}) + \mathbf{d}_m + \mathbf{k} + (1-\alpha)(\mathbf{x} - \mathbf{d}_m - \mathbf{k} - Q_{\Lambda_c}(\mathbf{x} - \mathbf{d}_m - \mathbf{k}))\end{aligned} \tag{9}$$

The key $\mathbf{k} \in \mathbb{R}^{N_v}$ is called the dither applying a secret shift of the quantizer. Due to the Λ_c-periodicity, the key ensemble $\mathcal{K}$ is the Voronoi cell $\mathcal{V}(\Lambda_c)$. We assume as in [3] that $\mathbf{k}$ has been uniformly drawn over $\mathcal{K} = \mathcal{V}(\Lambda_c)$. The last equation shows that the watermarked signal is an element of $\Lambda + \mathbf{d}_m + \mathbf{k}$ plus the self-inference noise $(1-\alpha)\tilde{\mathbf{x}}$, with $\tilde{\mathbf{x}} \triangleq [\mathbf{x} - \mathbf{d}_m - \mathbf{k} \mod \Lambda_c]$ and $[\mathbf{x} \mod \Lambda] \triangleq$

$\mathbf{x} - Q_\Lambda(\mathbf{x})$. Parameter α with $0 < \alpha < 1$ is the distortion compensation factor. The two lattices are scaled by a factor Δ such that the Euclidean embedding distortion is below the distortion budget: $\alpha^2 \frac{\int_{\mathcal{V}(\Lambda_c)} \|\mathbf{x}\|^2 \partial\mathbf{x}}{\mathrm{vol}(\mathcal{V}(\Lambda_c))} \leq N_v D$ (under the flat host assumption, see [3]).

The message decoded from $\mathbf{y}$ with key $\mathbf{k}'$ is given by

$$\hat{m} = d(\mathbf{y}, \mathbf{k}') = \arg\min_{m \in \mathcal{M}} \|\mathbf{y} - \mathbf{d}_m - \mathbf{k}' - Q_{\Lambda_c}(\mathbf{y} - \mathbf{d}_m - \mathbf{k}')\|, \tag{10}$$

which is m for $\mathbf{y} = e(\mathbf{x}, m, \mathbf{k})$ if:

$$[(1-\alpha)\tilde{\mathbf{x}} + \mathbf{k} - \mathbf{k}' \mod \Lambda_c] \in \mathcal{V}(\Lambda_f). \tag{11}$$

We suppose that, in the noiseless case, the self-interference doesn't give birth to decoding errors when we decode with the secret key $\mathbf{k}' = \mathbf{k}$. It implies that $(1-\alpha)\mathcal{V}(\Lambda_c) \subset \mathcal{V}(\Lambda_f)$, or more simply $(1-\alpha)R(\Lambda_c) \leq r(\Lambda_f)$. This holds if $\alpha \geq \alpha_{\min}$ with

$$\alpha_{\min} \triangleq 1 - r(\Lambda_f)/R(\Lambda_c). \tag{12}$$

If $\alpha = \alpha_{\min}$, then only $\mathbf{k}$ can decode without error: the set of equivalent keys is the singleton $\{\mathbf{k}\}$.

There are several constructions of the partition (Λ_c, Λ_f) provably good for data hiding. Their description is out of the scope of this paper (see [3]). However, we detail one in particular: We say that (Λ_c, Λ_f) are self-similar lattices if $\Lambda_f = \beta\Lambda_c$ with $0 < \beta < 1$ (ie. we exclude the case where Λ_f is a scaled rotation of Λ_c). Eq. (8) imposes that $M = \beta^{-N_v}$ which must be an integer bigger than 1. Decoding without error in the noiseless case implies $\beta \geq (1-\alpha)$ so that $\alpha \geq \alpha^{\mathrm{ss}}_{\min}$ (superscript ss means self-similar) with

$$\alpha^{\mathrm{ss}}_{\min} \triangleq 1 - \beta. \tag{13}$$

4.2 No Observation - $N_o = 0$

The attacker has no observation. He randomly picks a test key $\mathbf{k}'$ uniformly over $\mathcal{V}(\Lambda_c)$. What is the probability that $\mathbf{k}'$ is an equivalent key of $\mathbf{k}$?

Self-Similar Lattices Construction. We are able to write a close form expression of this probability for this construction thanks to the following lemma. For two sets $\mathcal{A}$ and $\mathcal{B}$ in $\mathbb{R}^{N_v}$, define $a\mathcal{A} = \{\mathbf{x} | \exists \mathbf{a} \in \mathcal{A} : \mathbf{x} = a\mathbf{a}\}$ and $\mathcal{A} \oplus \mathcal{B} = \{\mathbf{x} | \exists (\mathbf{a}, \mathbf{b}) \in \mathcal{A} \times \mathcal{B} : \mathbf{x} = \mathbf{a} + \mathbf{b}\}$.

Lemma 1. *For (a, b) two positive real numbers, $a\mathcal{V}(\Lambda) \oplus b\mathcal{V}(\Lambda) = (a+b)\mathcal{V}(\Lambda)$ for any Euclidean Lattice Λ.*

Proof. Take any $\mathbf{z} \in (a+b)\mathcal{V}(\Lambda)$, then $\mathbf{x} = a/(a+b)\mathbf{z}$ lies in $a\mathcal{V}(\Lambda)$, $\mathbf{y} = b/(a+b)\mathbf{z}$ lies in $b\mathcal{V}(\Lambda)$ while $\mathbf{z} = \mathbf{x} + \mathbf{y}$. Take now $\mathbf{x} \in a\mathcal{V}(\Lambda)$ and $\mathbf{y} \in b\mathcal{V}(\Lambda)$. Consider a codeword $\mathbf{c} \in \Lambda$ with $\mathbf{c} \neq \mathbf{0}$. Vector $\mathbf{x}$ is closer to codeword $\mathbf{0}$ than to any other codeword $a\mathbf{c}$ of $a\Lambda$. We have $\|\mathbf{x}\| \leq \|a\mathbf{c} - \mathbf{x}\|$ so that $a\|\mathbf{c}\|^2 - 2\mathbf{c}^\top\mathbf{x} \geq 0$. In the

same way, $b\|\mathbf{c}\|^2 - 2\mathbf{c}^\top\mathbf{y} \geq 0$. Then $\|(a+b)\mathbf{c} - (\mathbf{x}+\mathbf{y})\|^2 = \|\mathbf{x}+\mathbf{y}\|^2 + (a+b)((a+b)\|\mathbf{c}\|^2 - 2\mathbf{c}^\top(\mathbf{x}+\mathbf{y})) \geq \|\mathbf{x}+\mathbf{y}\|^2$. This holds for any codeword $(a+b)\mathbf{c}$ of $(a+b)\Lambda$ so that $\mathbf{x}+\mathbf{y} \in \mathcal{V}((a+b)\Lambda) = (a+b)\mathcal{V}(\Lambda)$.

If $\mathbf{k}' \in [\mathbf{k} + (\beta - (1-\alpha))\mathcal{V}(\Lambda_c) \mod \Lambda_c]$, then Eq. (11) is satisfied thanks to this lemma. Because there is no aliasing since $0 \leq \beta - (1-\alpha) \leq 1$, the volume of $\mathcal{K}_{eq}(0,\mathbf{k})$ is the same for any $\mathbf{k}$. For the sake of simplicity, we can restrict our attention to the case $\mathbf{k} = \mathbf{0}$ which makes the modulo Λ_c useless. In the end, the probability of picking an equivalent key is the ratio:

$$P^{(d)}(0,0) = \frac{\mathrm{vol}(\mathcal{K}_{eq}(0,\mathbf{k}))}{\mathrm{vol}(\mathcal{K})} = (\beta - (1-\alpha))^{N_v} \tag{14}$$

$$= \frac{1}{M}\left(1 - \frac{1-\alpha}{1-\alpha_{\min}^{\mathrm{ss}}}\right)^{N_v}, \tag{15}$$

with $\alpha_{\min}^{\mathrm{ss}}$ given in (13). This expression does not depend on factor Δ.

Bounds For a General Construction. For $\alpha = 1$, (11) states that $\mathcal{K}_{eq}(0,\mathbf{k}) = \mathbf{k} + \mathcal{V}(\Lambda_f)$ and $P^{(d)}(0,0) = 1/M$. For $\alpha < 1$, we cannot determine $\mathcal{K}_{eq}(0,\mathbf{k})$.

Upper Bound. We upper bound $\mathcal{K}_{eq}(0,\mathbf{k})$ with an hyperball. Since $\tilde{\mathbf{x}} \in \mathcal{V}(\Lambda_c)$, then $(1-\alpha)\|\tilde{\mathbf{x}}\| \leq (1-\alpha)R(\Lambda_c)$. If $\|\mathbf{k} - \mathbf{k}'\| \leq r(\Lambda_f) - (1-\alpha)R(\Lambda_c)$, then $\|(1-\alpha)\tilde{\mathbf{x}} + \mathbf{k} - \mathbf{k}'\| \leq r(\Lambda_f)$, which implies that (11) is satisfied. This means that $\mathcal{B}(\mathbf{k}, r(\Lambda_f) - (1-\alpha)R(\Lambda_c)) \subset \mathcal{K}_{eq}(0,\mathbf{k})$. Therefore,

$$P^{(d)}(0,0) \geq \frac{\mathrm{vol}(\mathcal{B}(\mathbf{0}, r(\Lambda_f) - (1-\alpha)R(\Lambda_c)))}{\mathrm{vol}(\mathcal{V}(\Lambda_c))} \tag{16}$$

$$\geq \left(\frac{r(\Lambda_f) - (1-\alpha)R(\Lambda_c)}{\rho(\Lambda_c)}\right)^{N_v} \tag{17}$$

$$\geq \frac{1}{M}\bar{r}(\Lambda_f)^{N_v}\left(1 - \frac{1-\alpha}{1-\alpha_{\min}}\right)^{N_v}, \tag{18}$$

where $\bar{r}(\Lambda) \triangleq r(\Lambda)/\rho(\Lambda) \leq 1$ is the packing efficiency of the lattice Λ and $\alpha_{\min}$ is given in (12). Equality holds however if $\mathcal{V}(\Lambda_f)$ and $\mathcal{V}(\Lambda_c)$ are both spherical:

$$\bar{R}(\Lambda_f) = \bar{r}(\Lambda_f) = \bar{R}(\Lambda_c) = \bar{r}(\Lambda_c) = 1. \tag{19}$$

This is only the case for $N_v = 1$ where the Voronoi cell are intervals of $\mathbb{R}$, and we find back the expression for self similar lattices.

Lower Bound. We lower bound $\mathcal{K}_{eq}(0,\mathbf{k})$ with a scaled Voronoi cell of Λ_f (see Fig. 3). Suppose $\mathbf{k}' \in \mathcal{K}_{eq}(0,\mathbf{k})$, then $\mathbf{k}' = \mathbf{k} + \mathbf{x}_f + (1-\alpha)\mathbf{x}_c$ with $\mathbf{x}_f \in \mathcal{V}(\Lambda_f)$ and $\mathbf{x}_c$ belonging to:

$$\mathcal{V}(\Lambda_c) \subset \mathcal{B}(\mathbf{0}, R(\Lambda_c)) = \mathcal{B}\left(\mathbf{0}, \frac{R(\Lambda_c)}{r(\Lambda_f)} r(\Lambda_f)\right) \subset \frac{R(\Lambda_c)}{r(\Lambda_f)}\mathcal{V}(\Lambda_f).$$

Therefore, $\mathcal{K}_{eq}(0,\mathbf{k}) \subset \mathbf{k} + \left(1 + (1-\alpha)\frac{R(\Lambda_c)}{r(\Lambda_f)}\right)\mathcal{V}(\Lambda_f)$ and

$$P^{(d)}(0,0) \leq \frac{1}{M}\left(1 - \frac{1-\alpha}{1-\alpha_{\min}}\right)^{N_v}, \tag{20}$$

which is the same expression as for self-similar lattices, but with the $\alpha_{\min}$ of (12). Equality holds if the lattices are self-similar.

It may surprise the reader that no figure of merit about the coarse lattice Λ_c appears in these bounds. This is not true because $\alpha_{\min}$ indeed depends on its covering efficiency. These bounds depend on the distortion compensation factor α but not on the scale Δ of (Λ_c, Λ_f). These bounds may not be tight in general. For instance, for $\alpha = 1$, $P^{(d)}(0,0) = M^{-1}$ $\forall(\Lambda_c, \Lambda_f)$, whereas the lower bound adds a scaling factor $\bar{r}(\Lambda_f)^{N_v}$. In the end, we obtain upper and lower bounds for the effective key length with a gap between the two of $N_v \log_2 \bar{r}(\Lambda_f)$ bits.

4.3 Some Observations - $N_o > 0$

In the KMA setup, the attacker observes N_o watermarked vectors together with their hidden message: $\mathbf{o}_i = \{\mathbf{y}_i, m_i\}$ with $1 \leq i \leq N_o$. We only detail the calculus for SCS: $N_v = 1$ and $\Lambda_c = \Delta\mathbb{Z}$, which can be used for self similar cubic lattices. We drop the boldface font since the host, the watermarked content and the key are now scalars. In other words, the embedding (9) simply gives:

$$y \in l\Delta + d_m + k + (1-\alpha)\mathcal{V}(\Delta\mathbb{Z}) \tag{21}$$

with $l \in \mathbb{Z}$, $d_m = (m-1)\Delta/M$ and $k \in \mathcal{V}(\Delta\mathbb{Z}) = \Delta/2.(-1,1]$. We also assume that $\alpha > 1/2$ and that the adversary knows d_m under KMA. The observations are:

$$o_i \triangleq y_i - d_{m_i} \in l_i\Delta + k + (1-\alpha)\Delta/2.(-1,1].$$

If we take these observations modulo Δ, the results may lie in a non convex set. However, there exist some r for which $[o_i - r \mod \Delta]$ are all in a convex interval of length $(1-\alpha)\Delta/2.(-1,1]$ (see [3, Prop. 2]). In other words, $\tilde{o}_i \triangleq [o_i - r \mod \Delta] + r = k + (1-\alpha)\tilde{x}_i$, and we get rid off the modulo operation. This implies in return that $k \in \tilde{o}_i + (1-\alpha)\Delta/2[-1,1)$. This holds for all the observations so that k must lie in the intersection of these intervals and we have:

$$k \in [\max \tilde{o}_i - (1-\alpha)\Delta/2, \min \tilde{o}_i + (1-\alpha)\Delta/2). \tag{22}$$

This interval is called the feasible set in [3] and we denote it by $\mathcal{K}(o^{N_o})$. In words, thanks to the observations, the attacker knows that the secret key lies into the feasible set. Therefore, he randomly picks a key k' in this set, and the probability that k' is an equivalent key is given by the ratio:

$$P^{(d)}(0,N_o) = \frac{\mathrm{vol}(\mathcal{K}_{eq}^{(d)}(k,0) \cap \mathcal{K}(o^{N_o}))}{\mathrm{vol}(\mathcal{K}(o^{N_o}))}. \tag{23}$$

Fig. 4 shows that $\mathcal{K}_{eq}^{(d)}(k,0)$ has a volume equalling $\Delta(1/M - (1-\alpha))$.

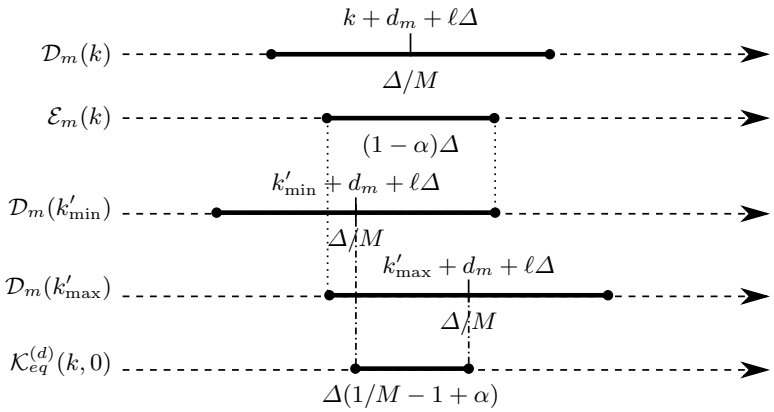

Fig. 4. Computation of $\mathrm{vol}(\mathcal{K}_{eq}^{(d)}(k,0))$ for DC-QIM.

First Study: $N_o = 1$. Denote $l_{eq} = \mathrm{vol}(\mathcal{K}_{eq}^{(d)}(k,0))/\Delta = 1/M - (1-\alpha)$ and $l_{fs} = \mathrm{vol}(\mathcal{K}(O^1))/\Delta = (1-\alpha)$ (see (22) with $\max \tilde{o}_i = \min \tilde{o}_i$ for $N_o = 1$). There are three cases depending on the values of l_{eq} and l_{fs}.

1. For $1 - 1/M \leq \alpha \leq 1 - 1/2M$, we have $l_{eq} \leq l_{fs}$.
   The probability $P^{(d)}(0,1)$ is given by $\int \mathbb{P}\left[k' \in \mathcal{K}_{eq}(k,0)|\tilde{o}_1\right] f(\tilde{o}_1)\partial\tilde{o}_1$, with $f(\tilde{o}_1) = (\Delta l_{fs})^{-1}$ and $\mathbb{P}\left[k' \in \mathcal{K}_{eq}(k,0)|\tilde{o}_1\right]$ given in Fig. 5 (left). We find:

$$P^{(d)}(0,1) = \frac{l_{eq}}{l_{fs}}\left(1 - \frac{l_{eq}}{4l_{fs}}\right) = 1 - (1-d)^2, \tag{24}$$

   with $d \triangleq \frac{1}{2M(1-\alpha)} - \frac{1}{2} \leq 1$.
2. For $1 - 1/2M \leq \alpha \leq 1 - 1/3M$, we have $l_{fs} \leq l_{eq}$.
   Although $\mathbb{P}\left[k' \in \mathcal{K}_{eq}(k,0)|\tilde{o}_1\right]$ has a different expression as shown in Fig. 5 (right), after integration, we find the same expression as (24).
3. For $1 - 1/3M \leq \alpha \leq 1$, we have $l_{eq} \leq 2l_{fs}$ and $P^{(d)}(0,1) = 1$.

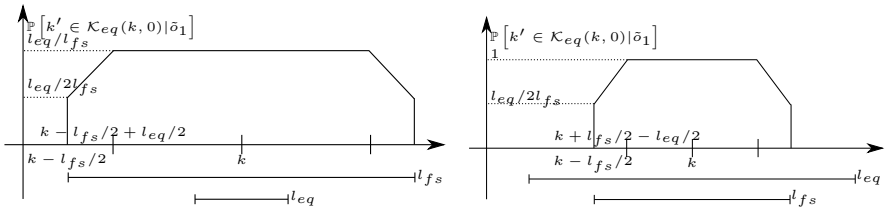

Fig. 5. SCS with $1-1/2M \leq \alpha \leq 1-1/3M$ (left) or $1-1/M \leq \alpha \leq 1-1/2M$ (right).

Second Study: $N_o > 1$: We introduce two random variables: $\underline{O} = \min \tilde{O}_i$ and $\bar{O} = \max \tilde{O}_i$ which are defined on the following interval: $-(1-\alpha)\Delta/2 \leq \underline{O} \leq (1-\alpha)\Delta/2$ and $\underline{O} \leq \bar{O} \leq (1-\alpha)\Delta/2$. The pdf of $(\underline{O}, \bar{O})$ is given by:

$$p_{\underline{O},\bar{O}}(\underline{o}, \bar{o}) = \frac{N_o(N_o-1)}{((1-\alpha)\Delta)^{N_o}}(\bar{o} - \underline{o})^{N_o-2}. \tag{25}$$

For a given couple $(\underline{o}, \bar{o})$, the probability of picking an equivalent key is as follows:

$$A(\underline{o}, \bar{o}) = 1 - \frac{|\underline{o} + (1-\alpha-1/2M)\Delta|^+ + |(1-\alpha-1/2M)\Delta - \bar{o}|^+}{(1-\alpha)\Delta + \underline{o} - \bar{o}},$$

with $|x|^+ \triangleq \max(x, 0)$. Note that if $\alpha \geq 1 - 1/3M$, then $A(\underline{o}, \bar{o}) = 1$, $\forall(\underline{o}, \bar{o})$ in the definition set, so that $P^{(d)}(0, N_o) = 1$, which is consistent with the first study. Note also that if $\alpha = 1 - 1/M$, then $A(\underline{o}, \bar{o}) = 0$ and the attacker never succeeds. Finally,

$$P^{(d)}(0, N_o) = \int_{-(1-\alpha)\Delta/2}^{(1-\alpha)\Delta/2} \int_{\underline{o}}^{(1-\alpha)\Delta/2} p_{\underline{O},\bar{O}}(\underline{o}, \bar{o}) \cdot A(\underline{o}, \bar{o}) \partial\underline{o}\partial\bar{o}. \tag{26}$$

After some cumbersome manipulations, we have for $1 - 1/M \leq \alpha \leq 1 - 1/3M$:

$$\begin{aligned} P^{(d)}(0, N_o) &= 1 - (1-d)^{N_o} \\ &\quad + dN_o(N_o-1)\left(d\ln(d) + 1 - d - \sum_{\ell=1}^{No-2} \frac{(1-d)^{\ell+1}}{\ell(\ell+1)} \right). \end{aligned} \tag{27}$$

This shows that when α increases from $1 - 1/M$ to $1 - 1/3M$, $P^{(d)}(0, N_o)$ goes from 0 to 1.

It is easy to extend these results to self similar cubic lattices: $\Lambda_c = \Delta\mathbb{Z}^{N_v}$. The probability to find an equivalent key over the block of size N_v is the product of the N_v probabilities per component. Therefore, one just has to take Eq. (24) and (27) to the power N_v, and the effective key length is N_v times the key length per component.

5 Technical Details: Part II - Experimental Setup

This section presents an experimental framework to numerically evaluate the effective key length. We assume that there exist efficient quantizers for the chosen lattices (Λ_c, Λ_f). This means that we know how to embed, decode and make modulo Λ_c operation. The subsections below explain how we overcome two difficulties.

5.1 Indicator Function of $\mathcal{K}_{eq}(0, \mathbf{k})$

Consider the case $N_o = 0$. A naive experimental protocol based on a Monte Carlo simulations would be to generate one secret key $\mathbf{k}$, and then N test keys

$\{\mathbf{k}'_i\}_{i=1}^{N}$ and to count the number of times $\mathbf{k}'_i$ is an equivalent decoding key of $\mathbf{k}$. The problem is that, if the partition is not based on self similar lattices, we do not know the shape of $\mathcal{K}_{eq}(0,\mathbf{k})$ and there is no indicator function of this set. The only thing we have is that Eq. (11) holds for any $\tilde{\mathbf{x}} \in \mathcal{V}(\Lambda_c)$ if $\mathbf{k}'_i \in \mathcal{K}_{eq}(0,\mathbf{k})$.

A first possibility is to generate N_t vectors $\{\tilde{\mathbf{x}}_i\}_{i=1}^{N_t}$ uniformly distributed over $\mathcal{V}(\Lambda_c)$. Thanks to the convexity of the Voronoi cells, we know that if Eq. (11) holds for the N_t elements, then it holds for any point in their convex hull of which is a subset of $\mathcal{V}(\Lambda_c)$. Therefore, this method is only an approximation of the indicator function, which becomes inaccurate if N_t is too small. This in turn raises a problem of complexity since we need to check (11) N_t times per test key.

A second possibility benefits from the convexity property. Since $\mathcal{V}(\Lambda_c)$ is convex, setting $\{\tilde{\mathbf{x}}_i\}_{i=1}^{N_t}$ as its vertices is sufficient. However, the dimension of the space strikes us again. For instance, there are 2^{N_v} such vertices for $\Lambda_c = \Delta\mathbb{Z}^{N_v}$ and $19,440$ for $\Lambda_c = E_8$. For the latter case, we only consider the $2,160$ deep holes of E_8, i.e. the most far away from $\mathbf{0}$ vertices [7].

5.2 Rare Event Probability Estimator

Since the probabilities to be estimated can be low, the complexity of Monte Carlo simulations is another difficulty. The number of test keys N must be in the order of $1/P^{(d)}(0,N_o)$ to achieve a reasonably low relative variance of estimation. This is the reason why we also use a rare event probability estimator[3]. Three ingredients are needed:

- A generator of test keys. The test keys are to be drawn uniformly over a convex set (e.g. $\mathcal{K} = \mathcal{V}(\Lambda_c)$ for $N_o = 0$). This is done by the rejection method: We randomly draw a vector $\mathbf{v}$ in the hypercube $R(\Lambda_c)[-1,1]^{N_v}$ and we accept it as an occurence of $\mathbf{K}' \sim U(\mathcal{V}(\Lambda_c))$ if $Q_{\Lambda_c}(\mathbf{v}) = \mathbf{0}$ indicating that $\mathbf{v} \in \mathcal{V}(\Lambda_c)$. If not, we reject it and redraw a vector $\mathbf{v}$ until the condition is checked.
- A modification process. It randomly modifies a key $\mathbf{K}'$ into $\mathbf{K}''$ so that the latter is exactly distributed like the former. One says that the process is distribution invariant. Since the law is indeed the uniform distribution over a convex set, we use the "Hit and Run" algorithm [8]. In a nutshell, from a point $\mathbf{K}'$ in the set, one uniformly draws a direction Θ is the space. Then, one seeks the 2 points A and B of this line $(\mathbf{K}', \Theta)$ that intersect with the frontier of the set. At the end, one draws a point uniformly over $[A,B]$. The process is repeated several times and the output $\mathbf{K}''$ is the last point.
- A score function $s(\cdot) : \mathcal{K} \to \mathbb{R}$. It is designed such that $s(\mathbf{k}') = 1$ implies that $\mathbf{k}' \in \mathcal{K}_{eq}(0,\mathbf{k})$. However, it must be a soft function: $s(\mathbf{k}')$ graciously tends to 1 when $\mathbf{k}'$ gets closer to $\mathcal{K}_{eq}(0,\mathbf{k})$ in some sense. We propose the following trick: We compute the difference $d_i = \|(1-\alpha)\tilde{\mathbf{x}}_i + \mathbf{k} - \mathbf{k}' \mod \Lambda_c\| - r(\Lambda_f)$. Therefore, $d_i > 0$ for the vectors violating (11). We set $s(\mathbf{k}') = 1 - \max(\{|d_i|^+\})$. If (11) holds for the N_t vectors defined in Sub. 5.1, then $s(\mathbf{k}') = 1$.

[3] available as a Matlab Toolbox at `www.irisa.fr/texmex/people/furon/src.html`

With this setting, the algorithm described in [9] estimates $\mathbb{P}[s(\mathbf{K}') = 1]$ with $\mathbf{K}'$ uniformly distributed over a convex set $\mathcal{K}$. Its properties in term of bias, relative variance and confidence interval are given in [9]. Its complexity is in $O(\log(1/P^{(d)}(0, N_o)))$. In practice, if $P^{(d)}(0, N_o)$ is lower than 10^{-3}, this algorithm runs faster than the Monte Carlo simulations.

6 Discussions

6.1 Scalar Costa Scheme

We first analyze the security of the Scalar Costa Scheme where $N_v = 1$, $\Lambda_c = \Delta\mathbb{Z}$, $\Lambda_f = M^{-1}\Delta\mathbb{Z}$, and $\alpha^{\text{ss}}_{\text{min}} = 1 - M^{-1}$. This is the only case where we have a complete picture for any value of N_o. Fig. 6 shows the effective key length in bits per component .

The embedding distortion increases with Δ and with α, and so is the robustness. However, the effective key length decreases with α and does not depend on Δ. This stems in a trade-off between robustness and security. For a given Δ, α closer to 1 provides more robustness but less security.

There is a big discrepancy w.r.t. the value of N_o. When $N_o = 0$, the effective key length is always bigger $\log_2 M$ bits per component, which is the rate of the watermarking scheme. Hiding symbols at a higher rate does increase the security, but the robustness would be much smaller.

When $N_o > 0$, the effective key length vanishes to 0 bit as $\alpha \to 1 - 1/3M$. Fig. 6 (right) shows that the effective key length quickly vanishes as N_o increases. Note the big loss between $N_o = 0$ and $N_o = 1$.

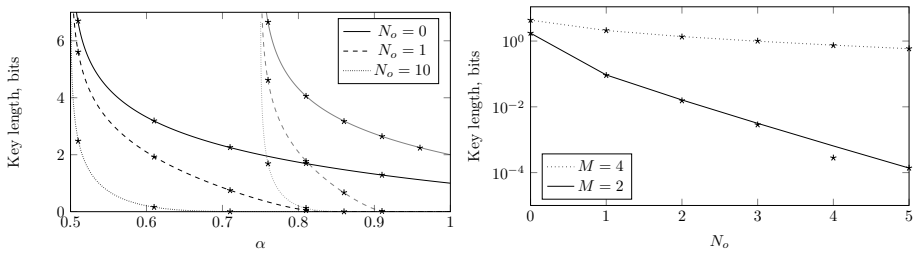

Fig. 6. Key length in bits for the SCS scheme, (left) vs. the distortion compensation factor α. (right) vs. the number of observations N_o for $\alpha = 0.8$. Stars mark experimental estimations as described in Sect. 5.1.

6.2 Lattice Embedding

The only setup where we have a full analysis is the cubic self-similar lattices: the effective key length for a block of size N_v is the effective key length of SCS times N_v. Therefore, the effective key length per component remains the same.

For any other construction, we only have results for $N_o = 0$. As above, when $\alpha = 1$, the effective key length per component equals the rate of the watermarking scheme: $\log_2(M)/N_v$ bits. Surprisingly, two self-similar constructions operating with the same β and at the same rate, share the same effective key length per component. For instance, SCS with $M = 2$ and the construction 1 detailed below share the same plot for $N_o = 0$ (Fig. 6 (left) and Fig. 7 (left)). In the same way, two non-similar constructions operating with the same $\alpha_{\min}$ and at the same rate share the same lower bound on the effective key length per component. In general, $\alpha_{\min}$ has an impact on the decay rate of the effective key length, whereas the rate of message hiding shifts the plot.

We apply the experimental benchmark detailed in Sect. 5 to two constructions for $N_v = 8$ (RE_8 denotes a rotated version of lattice E_8 [7]):

1. Self similar: $\Lambda_c = E_8$, $\Lambda_f = \beta E_8$, $\beta = 0.5$, $M = 256$, $\alpha^{\text{ss}}_{\min} = 0.5$.
2. Non similar: $\Lambda_c = RE_8$, $\Lambda_f = E_8$, $\bar{r}(\Lambda_f) = 0.842$, $M = 16$, $\alpha_{\min} = 0.5$.

Fig. 7 validates the experimental evaluation of the effective key length: for the self-similar lattices, the estimation is in line with the close form expression since it lies in the confidence interval except for the smallest value of α (see Fig. 7 (left)). This is due to the approximation of the equivalent region (see Sect. 5.1). For non similar lattices, the bounds are so close that the experimental evaluation does not bring much information. It seems that the key length is closer to the upper bound for weak α, and closer to the lower bound for strong α. The rare event estimator (see Sect. 5.2) is useful because the probabilities to be evaluated are as low as 10^{-16} for the smallest value of α. This algorithm succeeds to estimate such order of probability within two minutes on a regular computer.

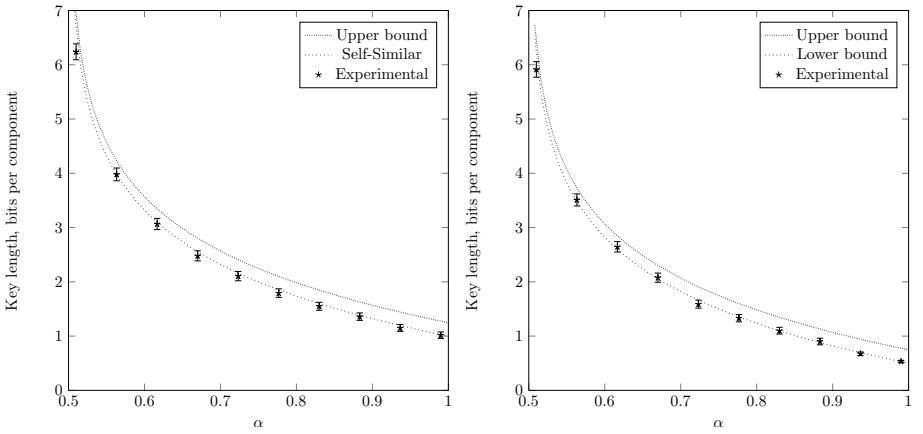

Fig. 7. Key length in bits for constructions 1 (left) and 2 (right) vs. the distortion compensation factor α. Stars mark experimental estimations as described in Sect. 5.2; the intervals are the 95% confidence intervals of these estimations.

7 Conclusion and Future Works

This paper introduces a new approach to gauge the security of watermarking schemes. The keystone is the notion of equivalent keys: there exist a plurality of keys granting access to the watermarking channel. The scheme is more secure if the attacker has greater difficulty in finding an equivalent key.

This approach is then applied to DC-DM QIM watermarking schemes. The lesson is that, as soon as the attacker observes some watermarked contents and their hidden message, the scheme is then broken if it is designed to be robust.

The paper lacks a part of the study: for lattice embedding, the computation of the effective key length is missing when the attacker has some observations. This will be done in a future work. The experimental evaluation should not be difficult: we will use Set Member Estimation technique to approximate the feasible set yielded by the observations by a bounding ellipsoid as done in [3]. Then, the attacker has to randomly pick a key inside this region. The theoretical part however seems much more difficult. Another point is that we work with $\epsilon = 0$ (perfect access to the watermarking channel), it is interesting to see how the effective key length evolves when we relax this strong constraint.

References

1. Cayre, F., Fontaine, C., Furon, T.: Watermarking security: Theory and practice. IEEE Trans. Signal Processing **53**(10) (2005) 3976 – 3987
2. Pérez-Freire, L., Pérez-González, F.: Spread-spectrum watermarking security. IEEE Transactions on Information Forensics and Security **4**(1) (2009) 2–24
3. Pérez-Freire, L., Pérez-González, F., Furon, T., Comesaña, P.: Security of lattice-based data hiding against the Known Message Attack. IEEE Trans. on Information Forensics and Security **1**((4)) (2006) 421–439
4. Eggers, J., Baüml, R., Tzschoppe, R., Girod, B.: Scalar Costa Scheme for information embedding. IEEE Trans. on Signal Processing **51**(4) (2003) 1003–1019 Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery.
5. Kalker, T.: Considerations on watermarking security. In Dugelay, J.L., Rose, K., eds.: Proc of the Fourth Workshop on Multimedia Signal Processing (MMSP), Cannes, France, IEEE (2001) 201–206
6. Cox, I., Doerr, G., Furon, T.: Watermarking is not cryptography. In Springer-Verlag, ed.: Proc. Int. Work. on Digital Watermarking, inivited talk. L.N.C.S., Jeju island, Korea (2006)
7. Conway, J.H., Sloane, N.J.A.: Sphere packings, lattices, and groups. Volume 290. Springer-Verlag, New York (1988)
8. Lovász, L., Vempala, S.: Hit-and-run is fast and fun. Technical Report MSR-TR-2003-05, Microsoft Research (2003)
9. Guyader, A., Hengartner, N., Matzner-Løber, E.: Simulation and estimation of extreme quantiles and extreme probabilities. Applied Mathematics & Optimization (2011) 1–26