Universal Optimality of Apollonian Cell Encoders

Fabrizio Biondi, Thomas Given-Wilson, Axel Legay

Universal Optimality of Apollonian Cell Encoders
DRAFT: Working Pre-Print

Fabrizio Biondi[a,*], Thomas Given-Wilson[b,*], Axel Legay[b]

[a] *CentraleSupélec Rennes, Avenue de la Boulaie, 35510 Cesson-Sévigné, France*
[b] *Inria, Campus de Beaulieu, 263 Avenue du Général Leclerc, 35042 Rennes, France*

Abstract

Preserving privacy of private communication against an attacker is a fundamental concern of computer science security. Unconditional cryptography considers the case where the attacker has unlimited computational power, hence no complexity result can be used for encryption. This paper introduces *Apollonian cell encoders*, a class of shared-key cryptosystems that are proven to be universally optimal and have a very compact representation. Conditions for the existence of Apollonian cell encoders are presented, as well as a constructive proof. Contrarily to perfectly secret cryptosytems, Apollonian cell encoders allow for unconditionally secure cryptography while supporting unlimited key reuse.

Keywords: Apollonian, unconditional security, perfect secrecy, entropy, max-equivocation, private-key cryptography, symmetric encryption

1. Introduction

Preserving privacy of private communication is a fundamental concern of computer science. Modern efforts can be divided into two categories: computational and unconditional security. Computational security of the privacy of an encrypted message depends on the assumed superpolynomial lower bound on complexity of some particular functions, e.g. factorization. Such lower-bound results are currently unproven, and may be weakened by technological progress in engineering, algorithmic theory, or quantum computing. In contrast, unconditional security is based on information-theoretic reasoning and proven independently of computational hardness. For this reason, unconditional security results are more general and robust than computational security results. However, the strict requirements to obtain unconditionally-secure cryptographic algorithms can make them often impractical.

*Corresponding author
Email addresses: fabrizio.biondi@inria.fr (Fabrizio Biondi), thomas.given-wilson@inria.fr (Thomas Given-Wilson), axel.legay@inria.fr (Axel Legay)

Recent work has presented *max-equivocation* that generalises perfect secrecy and is a measure of the best possible unconditional security achievable [4, 5]. These results showed the theoretical best possible security results (when the entropy of the message $H(M)$ is greater than the entropy of the key $H(K)$) are:

$$H(M|C) = H(K) \tag{1}$$

that the attacker's uncertainty about the message after observing the ciphertext $H(M|C)$ is equal to the attacker's uncertainty about the key (before observing the ciphertext); and

$$H(K|C) = H(K)\ . \tag{2}$$

the attacker's uncertainty about the key after observing the ciphertext $H(K|C)$ is unchanged.

These theoretical bounds are the limits of what can be achieved in practice. The rest of this paper presents an encoder achieving these theoretically optimal bounds and shows the necessary and sufficient conditions for such encoder to exist. Furthermore, the encoder itself has a compact representation that is reasonable to implement.

The first step in achieving optimality is developing a new kind of encoder called a *cell encoder*. The intuition behind a cell encoder is that given a message and key, the encoder does not have a single ciphertext, but instead a cell containing a set of ciphertexts. The choice of which ciphertext from a cell to transmit is chosen uniformly at random.

The next step is to define an *Apollonian cell encoder* that is a cell encoder that satisfies some reasonable conditions. Simplistically (details in Section 3) these can be summarised as: that the encoder is Latin [7] (no ciphertext is repeated in any row or column of the encoder's matrix representation); and the the number of ciphertexts and the sizes of the cells are derived from the distribution over the messages. From this it can be proved that an Apollonian cell encoder achieves: max-equivocation for the message, and perfect secrecy for the key.

The concluding step is to show necessary and sufficient conditions for the construction of an Apollonian cell encoder. The required conditions are that all the probabilities in the message distribution are rational numbers, and that no probability is greater than the probability of any key (key distribution is assumed uniform here). From these conditions an Apollonian cell encoder can be defined by

$$\text{encode}(k, m) \ = \ (b + kx)\%\mu \tag{3}$$

where b is derived from the message and message distribution, k is the key, and x and μ are derived (once) from the message distribution. This satisfies not only the conditions of an (universally optimal) Apollonian cell encoder, but is also compact and efficient to implement in practice.

The rest of this paper develops the above in careful detail.

The structure of the paper is as follows. Section 2 introduces notation and concepts for understanding the paper. Section 3 proves optimality of Apollonian

cell encoders. Section 4 proves existence and construction of Apollonian cell encoders. Section 5 draws conclusions.

2. Background

We recall standard definitions and concepts that will be used throughout this work.

The size of a set $\mathcal{S}$ is denoted as $|\mathcal{S}|$. A function $f : \mathcal{A} \to \mathcal{B}$ is *injective* iff $\forall a_1, a_2 \in \mathcal{A}.\ f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.

Basic concepts from probability and information theory can be found in the literature [8], including the definitions of support set $\mathcal{X}$, probability $P(E)$ of an event $E \subseteq \mathcal{X}$, random variable X on $\mathcal{X}$, entropy $H(X)$ of a random variable, and so on. We will write $\rho_{\mathcal{X}}(X)$ for a probability distribution on the random variable X on the support set $\mathcal{X}$, abbreviated to $\rho(X)$ when the support set is unambiguous.

2.1. Shared-Key Cryptosystems

We recall the definition of a shared-key cryptosystem, components, and typical use as the basis for the results and scenarios in this paper. A shared-key cryptosystem can be defined by the following components [5].

Definition 1. *A* (shared-key) cryptosystem *is a 3-tuple* $(\mathcal{M}, \mathcal{K}, \text{enc})$ *where:*

- *the* message space $\mathcal{M}$ *is a finite set of possible messages;*
- *the* key space $\mathcal{K}$ *is a finite set of possible keys;*
- *the* encoder *enc is a function* $\mathcal{M} \times \mathcal{K} \to \mathcal{C}$ *to some space* $\mathcal{C}$*.*

Note that in [5] *enc* is defined such that $\forall k \in \mathcal{K}.\ enc(\cdot, k)$ is injective, however this requirement is relaxed here.

A shared-key cryptosystem induces a ciphertext space $\mathcal{C} = enc[\mathcal{M}, \mathcal{K}]$ as the image of its encoder function and a decoder function as a function $dec : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$ such that $dec(enc(m, k), k) = m$. The existence and uniqueness of such a decoder function is ensured when $enc(\cdot, k)$ is injective.

The cloak $CLOAK(c)$ of a ciphertext c is the set of messages m such that there exists a k and $enc(m, k) = c$, i.e. $\{m \in \mathcal{M} \mid \exists k \in \mathcal{K} \text{ s.t. } enc(m, k) = c\}$.

The channel model of a cryptosystem was introduced by Shannon [13]. In this model, the sender wants to send a message $m \in \mathcal{M}$ to the receiver on a public channel that is eavesdropped by an attacker. Initially, the sender and receiver share a secret *key* $k \in \mathcal{K}$.

The sender encodes the message m with key k into the ciphertext c as $c = enc(m, k)$. The sender then sends c to the receiver via a public channel, where c is also eavesdropped by the attacker. Knowing the key k, the receiver decodes the message $m = dec(c, k)$ using the decoder function. Not knowing the key k, the attacker tries to infer m from c. The computational power available to the sender, receiver and attacker is assumed to be unlimited.

The attacker's knowledge about the elements of the communication is modeled by random variables. Let M (resp. K, C) be a random variable on the support set $\mathcal{M}$ (resp. $\mathcal{K}$, $\mathcal{C}$) representing the value of the message m (resp. key k, ciphertext c) according to the attacker.

2.2. Information Theory

Entropy is a commonly used measure of the uncertainty of a system represented by a probability distribution, since it can conveniently represent the information that the attacker has about the secret message before and after the attack and consequently quantify the information gained by the attacker thanks to the attack [2, 3, 6, 10, 11, 14]. For the application of entropy to security, many different entropy measures have been proposed, modeling different attackers and security scenarios, including Shannon entropy $\mathcal{H}(\rho(X)) = -\sum_{x\in X} \rho(x) \log \rho(x)$ [13] and min-entropy $H_\infty(X) = -\log \max_{x\in X} \rho(x)$ [14]. A generalization of many of these entropies has been proposed by Renyi [12], and more recently Khouzani and Malacaria [9] proposed a definition of entropy that generalizes Renyi entropy. This Khouzani-Malacaria entropy is defined as follows:

Definition 2. *A function $H(\rho)$ from a probability distribution ρ to a real number is a Khouzani-Malacaria entropy if it satisfies the following.*

Symmetry *$H(\rho)$ is invariant under permutation of elements of ρ (i.e. depends on the probabilities but not on their order or labeling).*

Expansibility *Adding elements with probability zero to ρ does not change $H(\rho)$.*

Core-Concavity *$H(\rho)$ can be written as $\eta(F(\rho))$ where $\eta : \mathbb{R} \to \mathbb{R}$ is a non-constant function on real numbers, F is a scalar function on probability distributions, and it holds that either*

1. *η is increasing and F is concave in ρ, or*
2. *η is decreasing and F is convex in ρ.*

Given a Khouzani-Malacaria entropy measure H, it is possible to derive the maximum amount of secrecy that a cryptosystem can preserve, following Shannon [13]:

Definition 3. *A cryptosystem satisfies* perfect message *(resp.* key*)* secrecy *for a given Khouzani-Malacaria entropy measure H when $H(M|C) = H(M)$ (resp. $H(K|C) = H(K)$). This is possible only when $H(K) \geq H(M)$ (resp. $H(M) \geq H(K)$).*

Practical cryptograpic usage requires the key to be significantly smaller than the message, making perfect message secrecy very unlikely to be achievable. Biondi et al. [5] derived maximum message equivocation bounds for the case in which $H(M) > H(K)$ and perfect secrecy is not achievable:

Definition 4. *A cryptosystem satisfies* max-equivocation on the message *iff* $H(M|C) = H(K)$.

Hence if $H(M) > H(K)$ for a given Khouzani-Malacaria entropy H, the best possible cryptosystem would have max-equivocation on the message ($H(M|C) = H(K)$) and perfect secrecy on the key ($H(K|C) = H(K)$). Note that with such a cryptosystem the key can be reused indefinitely, since the system does not leak any information about the key.

Khouzani and Malacaria call a cryptosystem *universally optimal* if it is optimal for any Khouzani-Malacaria entropy. This paper assumes that the probability distribution of the key is uniform over the key space $\mathcal{K}$, i.e. $\forall k \in \mathcal{K}.\ \rho(k) = \frac{1}{|\mathcal{K}|}$. Under this condition, a cryptosystem is universally optimal if and only if the posterior distribution of the secret is uniformly distributed on a number of elements equal to the size of the keyspace $\mathcal{K}$ [9]. Also assuming $H(M) > H(K)$ this translates to the following:

Definition 5. *A cryptosystem has* universal max-equivocation on the message *if it has max-equivocation on the message for any Khouzani-Malacaria entropy measure. This holds iff* $\forall c \in \mathcal{C}, m \in CLOAK(c).\ \rho(m|c) = \frac{1}{|\mathcal{K}|}$.

Note that trivially $\forall c \in \mathcal{C}, m \notin CLOAK(c).\ \rho(m|c) = 0$ by definition of $CLOAK$.

Definition 6. *A cryptosystem has* universal perfect key secrecy *if it has perfect key secrecy for any Khouzani-Malacaria entropy measure. This holds iff* $\forall k \in \mathcal{K}, c \in \mathcal{C}.\ \rho(k|c) = \frac{1}{|\mathcal{K}|}$.

In Section 3 an encoder with universal max-equivocation on the message and universal perfect key secrecy is presented, making it the best possible cryptosystem theoretically achievable for any Khouzani-Malacaria entropy.

3. Apollonian Cell Encoders Optimality Results

For the rest of the paper we assume that: $H_\infty(M) \geq H_\infty(K)$; $\rho(M)$ and $\rho(K)$ are independent; and the probability distribution of the key is uniform over the key space $\mathcal{K}$, i.e. $\forall k \in \mathcal{K}.\ \rho(k) = \frac{1}{|\mathcal{K}|}$.

Cell encoders. We define a function $CELL(m, k)$ that given a message m and key k returns a set of symbols (nominally a subset of the ciphertexts).

We define a new type of encoder, called *cell encoder*, which exploits a cell function when producing a ciphertext for a given message m and key k.

Definition 7. *A* cell encoder enc^{CELL} *is a function* $\mathcal{M} \times \mathcal{K} \to \mathcal{C}$ *that given a message* m *and key* k *chooses a ciphertext* c *uniformly at random from the symbols of* $CELL(m, k)$.

Observe that prior definitions of encoders [4, 5] can also be considered cell encoders by assuming that the $CELL$ function always returns a set of size 1. Thus, the rest of this paper shall assume all encoders are cell encoders and the $CELL$ function is defined implicitly and not shown in the notation.

Let $\Delta(c \in CELL(m,k))$ be the Dirac delta function for the statement $c \in CELL(m,k)$, i.e.

$$\Delta(c \in CELL(m,k)) = \begin{cases} 1 & \text{if } c \in CELL(m,k) \\ 0 & \text{otherwise} \end{cases} .$$

Then we can write the probability of each ciphertext c as:

$$\rho(c) = \sum_{m \in \mathcal{M}} \sum_{k \in \mathcal{K}} \Delta(c \in CELL(m,k)) \frac{\rho(m,k)}{|CELL(m,k)|} \tag{4}$$

and the conditional probability of each ciphertext c given a message m or a key k as

$$\rho(c|m) = \sum_{k \in \mathcal{K}} \Delta(c \in CELL(m,k)) \frac{\rho(k)}{|CELL(m,k)|} \tag{5}$$

and

$$\rho(c|k) = \sum_{m \in \mathcal{M}} \Delta(c \in CELL(m,k)) \frac{\rho(m)}{|CELL(m,k)|} \tag{6}$$

respectively.

A cell encoder is *semi-injective on the message* if $\forall k \in \mathcal{K}.\ enc(\cdot, k)$ is injective, i.e. for all messages m_i and m_j and all keys k then $m_i \neq m_j$ implies $CELL(m_i,k) \cap CELL(m_j,k) = \emptyset$.

A cell encoder is *semi-injective on the key* if $\forall m \in \mathcal{M}.\ enc(m, \cdot)$ is injective, i.e. for all keys k_i and k_j and all messages m then $k_i \neq k_j$ implies $CELL(m,k_i) \cap CELL(m,k_j) = \emptyset$.

Apollonian cell encoders. Assume that each message probability is rational, i.e. $\forall m_i \in \mathcal{M}.\ \rho(m_i) \in \mathbb{Q}$. Then each message probability $\rho(m_i)$ can be written as the quotient of a numerator n_i and a denominator d_i: $\rho(m_i) = \frac{n_i}{d_i}$. Let μ be the least common multiple of these denominators: $\mu = LCM(d_1, d_2, \ldots, d_{|\mathcal{M}|})$ and so define $n'_i = \frac{n_i \mu}{d_i}$.

A cell encoder is *Apollonian* if it is semi-injective on both the key and message, and $|\mathcal{C}| = \mu$ and each cell corresponding to message m_i has size n'_i:

Definition 8. *Let ρ be a distribution over the message space $\mathcal{M}$ such that for every $m_i \in \mathcal{M}$ then $\rho(m_i) \in \mathbb{Q}$. Let each $\rho(m_i) = \frac{n_i}{d_i}$ and $\mu = LCM(d_1, d_2, \ldots, d_{|\mathcal{M}|})$ and so define $n'_i = \frac{n_i \mu}{d_i}$. Then a cell encoder enc is* Apollonian *iff*

1. $\forall k \in \mathcal{K}.\ \text{enc}(\cdot, k)$ *is injective and*
2. $\forall m \in \mathcal{M}.\ \text{enc}(m, \cdot)$ *is injective and*
3. $|\mathcal{C}| = \mu$ *and*
4. $\forall m_i \in \mathcal{M}, k_j \in \mathcal{K}.\ |CELL(m_i, k_j)| = n'_i$.

Optimality of Apollonian cell encoders. Recall that we assume that the key is uniformly distributed, i.e. $\forall k \in \mathcal{K}.\ \rho(k) = \frac{1}{|\mathcal{K}|}$, and furthermore that $H_\infty(M) \geq H_\infty(K)$. Then an Apollonian cell encoder for the message and key space always exists and achieves the best possible theoretically achievable secrecy, i.e. perfect secrecy on the key and max-equivocation on the message. See Section 4 for necessary and sufficient conditions for the existence of Apollonian cell encoders. The following lemmata hold for Apollonian cell encoders.

Lemma 1. $\forall k_j.\ \sum_{m_i} \Delta(c \in CELL(m_i, k_j)) = 1.$

Proof. By conditions 1 and 3 of Definition 8. □

Lemma 2. $\forall m_i.\ \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) = \Delta(m \in CLOAK(c)).$

Proof. By conditions 2 and 3 of Definition 8. □

Lemma 3. $\sum_{m_i} \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) = |\mathcal{K}|.$

Proof. By conditions 1 and 3 of Definition 8. □

Lemma 4. $\forall c \in \mathcal{C}.\ \rho(c) = \frac{1}{\mu}.$

Proof.

$$
\begin{aligned}
\rho(c) &= \sum_{m_i} \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) \frac{\rho(m_i, k_j)}{|CELL(m_i, k_j)|} && \text{(by Equation (4))} \\
&= \sum_{m_i} \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) \frac{\rho(m_i, k_j)}{n'_i} \\
& && \text{(by condition 4 of Definition 8)} \\
&= \sum_{m_i} \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) \frac{\rho(m_i)\rho(k_j)}{n'_i} \\
& && \text{(since } \rho(M) \text{ and } \rho(K) \text{ are independent)} \\
&= \sum_{m_i} \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) \frac{\frac{n'_i}{\mu} \frac{1}{|\mathcal{K}|}}{n'_i} \\
& && \text{(by definition of } n'_i \text{ and uniformity of } \rho(K)) \\
&= \sum_{m_i} \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) \frac{1}{\mu|\mathcal{K}|} \\
&= \frac{1}{\mu|\mathcal{K}|} \sum_{m_i} \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) && \text{(since } \mu \text{ and } |\mathcal{K}| \text{ are constants)} \\
&= \frac{1}{\mu|\mathcal{K}|} |\mathcal{K}| && \text{(by Lemma 3)} \\
&= \frac{1}{\mu}\ .
\end{aligned}
$$

□

Lemma 5. $\forall k \in \mathcal{K}, c \in \mathcal{C}.\ \rho(c|k) = \frac{1}{\mu}$.

Proof.

$$\begin{aligned}
\rho(c|k_j) &= \sum_{m_i} \Delta(c \in CELL(m_i, k_j)) \frac{\rho(m_i)}{|CELL(m_i, k_j)|} && \text{(by Equation (6))} \\
&= \sum_{m_i} \Delta(c \in CELL(m_i, k_j)) \frac{\rho(m_i)}{n'_i} && \text{(by condition 4 of Definition 8)} \\
&= \sum_{m_i} \Delta(c \in CELL(m_i, k_j)) \frac{(\frac{n'_i}{\mu})}{n'_i} && \text{(by definition of } n'_i) \\
&= \sum_{m_i} \Delta(c \in CELL(m_i, k_j)) \frac{1}{\mu} \\
&= \frac{1}{\mu} \sum_{m_i} \Delta(c \in CELL(m_i, k_j)) && \text{(since } \mu \text{ is a constant)} \\
&= \frac{1}{\mu} \ . && \text{(by Lemma 1)}
\end{aligned}$$

□

Lemma 6. $\forall c \in \mathcal{C}, m_i \in CLOAK(c).\ \rho(c|m_i) = \frac{1}{n'_i|\mathcal{K}|}$.

Proof.

$$\begin{aligned}
\rho(c|m_i) &= \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) \frac{\rho(k_j)}{|CELL(m_i, k_j)|} && \text{(by Equation 5)} \\
&= \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) \frac{\rho(k_j)}{n'_i} && \text{(by condition 4 of Definition 8)} \\
&= \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) \frac{1}{n'_i|\mathcal{K}|} && \text{(by uniformity of } \rho(K)) \\
&= \frac{1}{n'_i|\mathcal{K}|} \sum_{k_j} \Delta(c \in CELL(m_i, k_j)) \\
& && \text{(since } n'_i \text{ is a constant for a given } m_i \text{ and } |\mathcal{K}| \text{ is a constant)} \\
&= \frac{1}{n'_i|\mathcal{K}|} \ . && \text{(by Lemma 2 since } m_i \in CLOAK(c))
\end{aligned}$$

□

Lemma 7. $\forall c \in \mathcal{C}, m \in CLOAK(c).\ \rho(m|c) = \frac{1}{|\mathcal{K}|}$.

Proof.

$$\begin{aligned}
\rho(m|c) &= \frac{\rho(c|m)\rho(m)}{\rho(c)} && \text{(by Bayes'theorem)}\\
&= \frac{\frac{1}{n_i'|\mathcal{K}|}\rho(m)}{\rho(c)} && \text{(by Lemma 6)}\\
&= \frac{\frac{1}{n_i'|\mathcal{K}|}\frac{n_i'}{\mu}}{\rho(c)} && \text{(by definition of } n_i')\\
&= \frac{\frac{1}{n_i'|\mathcal{K}|}\frac{n_i'}{\mu}}{\frac{1}{\mu}} && \text{(by Lemma 4)}\\
&= \frac{1}{|\mathcal{K}|} \quad .
\end{aligned}$$

□

The following theorems prove the optimality of Apollonian cell encoders:

Theorem 1. *An Apollonian cell encoder achieves perfect secrecy on the key, i.e.* $H(K) = H(K|C) = \log_2 |\mathcal{K}|$*, where* H *is any Khouzani-Malacaria entropy measure.*

Proof. To prove this result it suffices to show that $\forall c \in \mathcal{C}, k \in \mathcal{K} \ : \ \rho(k|c) = \rho(k)$. Observe that $\rho(k|c) = \frac{\rho(c|k)\rho(k)}{\rho(c)}$ so it suffices to show that $\rho(c) = \rho(c|k)$. The theorem then follows from Lemma 4, Lemma 5, and uniformity of $\rho(K)$. □

Observe that this does not require condition 2 of Definition 8.

Theorem 2. *An Apollonian cell encoder achieves max-equivocation on the message, i.e.* $H(M|C) = H(K) = \log_2 |\mathcal{K}|$*, where* H *is any Khouzani-Malacaria entropy measure.*

Proof. To prove this result it suffices to show that $\forall c \in \mathcal{C}, m \in CLOAK(c) \ : \ \rho(m|c) = \rho(k) = \frac{1}{|\mathcal{K}|}$. The theorem then follows from Lemma 7. □

4. Existence and Construction of Apollonian Cell Encoders

This section discusses the necessary and sufficient conditions for an Apollonian encoder to exist given a probability distribution on messages and a key space, and presents a closed form to construct an Apollonian encoder when possible.

Given a distribution ρ over the message space $\mathcal{M}$ and a key space $\mathcal{K}$ with uniform distribution, an Apollonian cell encoders exists iff $H_\infty(M) \geq H_\infty(K)$. The rest of this section formalises this.

4.1. Necessity

The following two lemmata are used in the proof of necessary conditions for an Apollonian cell encoder. The first to clarify the underlying relation between message distribution and key distribution. The second to show necessity of the condition $H_\infty(M) \geq H_\infty(K)$.

Lemma 8. $H_\infty(M) \geq H_\infty(K) \equiv max(\rho(m_i)) \leq \frac{1}{|\mathcal{K}|}$

Proof.

$$\begin{aligned} H_\infty(M) \geq H_\infty(K) &\equiv -\log(max(\rho(m_i))) \geq \log(|\mathcal{K}|) \\ &\equiv -\log(max(\rho(m_i))) \geq -\log\left(\frac{1}{|\mathcal{K}|}\right) \\ &\equiv \log(max(\rho(m_i))) \leq \log\left(\frac{1}{|\mathcal{K}|}\right) \\ &\equiv max(\rho(m_i)) \leq \frac{1}{|\mathcal{K}|} \end{aligned}$$

□

Lemma 9. *Let $H_\infty(M) < H_\infty(K)$. Then no Apollonian encoder can exist for M and K.*

Proof. As a trivial corollary of Lemma 8, it holds that $H_\infty(M) < H_\infty(K) \equiv max(\rho(m_i)) > \frac{1}{|\mathcal{K}|}$. Now consider a row of the cell encoder corresponding to the message m_j with probability $\rho(m_j) = max(\rho(m_i)) = \frac{n'_j}{\mu}$. Observe that to fill all the cells of the row corresponding to m_j requires $n'_j|\mathcal{K}|$ ciphertexts. However, since $\frac{n'_j}{\mu} > \frac{1}{|\mathcal{K}|}$ and so $n'_j|\mathcal{K}| > \mu$ it is impossible to fill the row corresponding to m_j without repeating a ciphertext. □

Thus, if $H_\infty(M) < H_\infty(K)$ holds no Apollonian cell encoder can exist for ρ and $\mathcal{M}$ and $\mathcal{K}$.

4.2. Sufficiency – Construction Proof

This section formalises how to construct an Apollonian encoder given ρ and $\mathcal{M}$ and (size of) $\mathcal{K}$.

First assign to each message m a set of n' sequential base numbers $\mathcal{B} = b_0, b_1, \ldots, b_{n'-1}$ and where $\forall i, j \;:\; m_i \neq m_j,\ \mathcal{B}_i \cap \mathcal{B}_j = \emptyset$. For simplicity this can be done by ordering the messages and then assigning to m_0 the base numbers $0, 1, \ldots, n'_0 - 1$, then to m_1 the base numbers $n'_0, n'_0 + 1, \ldots, n'_0 + n'_1 - 1$, etc. Observe that all of these base numbers can be assigned to exactly range over 0 to $\mu - 1$.

For simplicity let $x = \mu\ max(\rho(m_i)) = max(n'_i)$. Now an Apollonian cell encoder $enc(k, m)$ can be defined by

$$enc(k, m) \quad = \quad (b + kx)\%\mu$$

where the keys are represented as their index $k_j = j$ $(0 \leq j \leq |\mathcal{K}| - 1)$, also b is chosen uniformly at random from the appropriate $\mathcal{B}$ according to m, and $\%$ is the modulo operation. Note that here the natural numbers $0, 1, \ldots, \mu - 1$ are used as the ciphertexts $\mathcal{C}$.

Theorem 3. *The encoder* $enc(k, m) = (b + kx)\%\mu$ *is Apollonian.*

Proof. Observe that each cell corresponding to the message m_i has size n'_i by construction. Each column contains exactly one instance of each ciphertext since when $k = 0$ this is exactly the numbers $0, 1, \ldots, \mu - 1$, and this is stable under addition-modulo for any kx. The only non-trivial part is the proof that no ciphertext is repeated in any row. Fix some message m_i and let $b_\alpha = min(b)\ .\ b \in \mathcal{B}_i$ and $b_\omega = b_\alpha + n'_i - 1 = max(b)\ .\ b \in \mathcal{B}_i$. Observe that when $k = 0$ then the possible ciphertexts are some numbers $b_\alpha, b_\alpha + 1, \ldots, b_\omega$ that are sequential and distinct. Now consider when k_1 and k_2 are both in the range $0, \ldots, |\mathcal{K}| - 1$ inclusive and $k_1 < k_2$. Observe that the maximum ciphertext for k_1 is $b_\omega + k_1 x$ and the minimum for k_2 is $b_\alpha + k_2 x$. It is sufficient to show that $b_\omega + k_1 x < b_\alpha + k_2 x$ (since we can adjust by subtracting $(b_\omega + k_1 x)$ to avoid issues with $\%\mu$):

$$
\begin{array}{rcll}
b_\omega + k_1 x & < & b_\alpha + k_2 x & \\
b_\omega + k_1 x & < & b_\alpha + k_1 x + nx & \text{for } n \geq 1 \text{ since } k_1 < k_2 \\
b_\omega & < & b_\alpha + nx & \\
b_\alpha + n'_i - 1 & < & b_\alpha + nx & \text{by definition of } b_\omega \\
n'_i - 1 & < & nx & \\
n'_i & < & nx + 1 & \\
n'_i & < & x + 1 & \text{since } n \geq 1 \text{ by definition} \\
n'_i & \leq & x &
\end{array}
$$

which must hold since $x = max(n'_i)$. Finally, to conclude requires showing that $(b_\omega - b_\alpha) + (|\mathcal{K}| - 1)x < \mu$:

$$
\begin{array}{rcll}
(b_\omega - b_\alpha) + (|\mathcal{K}| - 1)x & < & \mu & \\
(b_\alpha + n'_i - 1 - b_\alpha) + (|\mathcal{K}| - 1)x & < & \mu & \text{by definition of } b_\omega \\
(n'_i - 1) + (|\mathcal{K}| - 1)x & < & \mu & \\
(n'_i - 1) + (|\mathcal{K}| - 1)x & < & |\mathcal{K}|x & \text{by definition of } \mu \\
n'_i - 1 & < & x & \\
n'_i & \leq & x &
\end{array}
$$

which always holds since $x = max(n'_i)$ by definition. □

This shows that when $\forall m \in \mathcal{M}\ .\ \rho(m) \in \mathbb{Q}$ and $\rho(m) \leq \frac{1}{|\mathcal{K}|}$ and then an optimal (Apollonian) encoder can be constructed.

4.3. Existence

Combining these yields the necessary and sufficient conditions for the existence of an Apollonian cell encoder given probability distribution ρ over the message space $\mathcal{M}$ and key space $\mathcal{K}$ with uniform distribution.

Theorem 4. *Let ρ be a distribution over the message space $\mathcal{M}$, let $\mathcal{K}$ be a key space with uniform distribution, and let M and K be the corresponding random variables. Then an Apollonian cell encoder for ρ and $\mathcal{M}$ and $\mathcal{K}$ exists iff $H_\infty(M) \geq H_\infty(K)$.*

Proof. By Lemma 9 and Theorem 3. □

5. Conclusions

Finding a good unconditionally secure encryption scheme has been an open problem for some time. This paper presents the necessary and sufficient conditions to construct an optional unconditional encryption scheme: an Apollonian cell encoder. Apollonian cell encoders provide the maximum possible security; max-equivocation for the message, and perfect secrecy for the key. In addition, a constructive proof that have a compact and easy to implement form is provided, that allows Apollonian cell encoders to be easily implemented in practice.

References

[1] *IEEE 29th Computer Security Foundations Symposium, CSF 2016, Lisbon, Portugal, June 27 - July 1, 2016*. IEEE Computer Society, 2016.

[2] M. S. Alvim, K. Chatzikokolakis, A. McIver, C. Morgan, C. Palamidessi, and G. Smith. Axioms for information leakage. In *IEEE 29th Computer Security Foundations Symposium, CSF 2016, Lisbon, Portugal, June 27 - July 1, 2016* [1], pages 77–92.

[3] M. S. Alvim, K. Chatzikokolakis, C. Palamidessi, and G. Smith. Measuring information leakage using generalized gain functions. In S. Chong, editor, *25th IEEE Computer Security Foundations Symposium, CSF 2012, Cambridge, MA, USA, June 25-27, 2012*, pages 265–279. IEEE, 2012.

[4] F. Biondi, T. Given-Wilson, and A. Legay. Attainable unconditional security for shared-key cryptosystems. In *14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015, Helsinki, Finland, August 20-22, 2015*, pages 1–8. IEEE, 2015.

[5] F. Biondi, T. Given-Wilson, and A. Legay. Attainable unconditional security for shared-key cryptosystems. *Inf. Sci.*, 369:80–99, 2016.

[6] F. Biondi, A. Legay, P. Malacaria, and A. Wasowski. Quantifying information leakage of randomized protocols. *Theor. Comput. Sci.*, 597:62–87, 2015.

[7] A. Bruen and M. Forcinito. *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*. Wiley, 2011.

[8] T. Cover and J. Thomas. *Elements of Information Theory*. A Wiley-Interscience publication. Wiley, 2006.

[9] M. H. R. Khouzani and P. Malacaria. Relative perfect secrecy: Universally optimal strategies and channel design. In *IEEE 29th Computer Security Foundations Symposium, CSF 2016, Lisbon, Portugal, June 27 - July 1, 2016* [1], pages 61–76.

[10] B. Köpf and D. A. Basin. An information-theoretic model for adaptive side-channel attacks. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*, pages 286–296. ACM, 2007.

[11] P. Malacaria. Algebraic foundations for information theoretical, probabilistic and guessability measures of information flow. *CoRR*, abs/1101.3453, 2011.

[12] A. Rényi. On measures of entropy and information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, pages 547–561, Berkeley, Calif., 1961. University of California Press.

[13] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28, 1949.

[14] G. Smith. On the foundations of quantitative information flow. In L. de Alfaro, editor, *Foundations of Software Science and Computational Structures, 12th International Conference, FOSSACS 2009, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2009, York, UK, March 22-29, 2009. Proceedings*, volume 5504 of *Lecture Notes in Computer Science*, pages 288–302. Springer, 2009.