Investigation of the use of finite frame theory in cryptography

by

Laura Christine Walters

A Creative Component submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Mathematics

Program of Study Committee:
Ryan Martin, Major Professor
Jennifer Davidson
Eric Weber

Iowa State University

Ames, Iowa

2008

TABLE OF CONTENTS

LIST OF NOTATION

$\mathbb{N}$	Set of all natural numbers
$\mathbb{Z}$	Set of all integers
$\mathbb{C}$	Set of all complex numbers
$\mathcal{A}$	Generic algebra
$\mathcal{L}$	Loop
L	Lower frame bound
U	Upper frame bound
G	Gram matrix
H	Generic Hilbert space
K	Generic Hilbert space
p	Plaintext vector
m	Dimension of plaintext
g	Garbage (or noise) vector
c	Ciphertext vector
$C(X)$	Set of all continuous functions on an interval X
$\langle \cdot, \cdot \rangle$	Inner product
$\overline{\langle \cdot, \cdot \rangle}$	Conjugate of the inner product
$\| \cdot \|$	Norm of an inner product space
$\| \cdot \|$	Modulus of a complex number
$L^2[-T, T]$	Set of all Lebesgue square-integrable functions on the interval [-T,T]
$L^\infty[-T, T]$	Set of all bounded measurable functions on the interval [-T,T]
$\{x_j\}_{j \in [N]}$	Finite sequence or set of vectors
$\{e_j\}_{j=1}^N$	Standard orthonormal basis for $\mathbb{C}^N$

$\{h_j\}_{j=1}^N$	Standard orthonormal basis for a Hilbert space, H
$\mathbb{X}$	Frame given by the vectors $\{x_j\}_{j=1}^N$
$\Theta_{\mathbb{X}}$	Analysis operator for the frame $\mathbb{X}$
$\Theta_{\mathbb{X}}^*$	Synthesis operator for the frame $\mathbb{X}$
$[x_i]_{i\in[N]}$	Column vector x with entries $x_1, x_2, ..., x_N$
$[x_i]_{i\in[N]}^*$	Row vector x with entries $x_1, x_2, ..., x_N$
$\mathbf{0}$	Matrix whose entries are all zero; dimension inferred from context
I	Identity matrix; dimension inferred from context
$\mathbb{A}$	Hadamard array $H[m, k, \lambda]$
$\pm a_1, \pm a_2, ..., \pm a_k$	Set of elements in a Hadamard array
λ	Number of elements of type a_j in each row and each column of a Hadamard array, $\mathbb{A}$
d_i	Dimension of a Hadamard array
$A \otimes B$	Tensor product of two matrices A and B

CHAPTER 1. INTRODUCTION

Cryptography, the art of hiding data, relies heavily on invertible mathematical functions. Mathematicians and computer scientists have explored a plethora of mathematical concepts in their quest to develop an unbreakable cryptosystem. In this paper, we investigate the use of finite frame theory in cryptography.

At first glance, finite frames seem ideal for cryptography. Although similar to a basis for a Hilbert space, frames contain redundancy that could be used to hide data. Another property is that any vector in a Hilbert space can be reconstructed using a frame and its dual frame. However, these properties can also be used to break cryptosystems that use them.

In 2004, Miotke and Rebollo-Neira published a theoretical private key encryption scheme using infinite frames and oversampling of Fourier coefficients [MRN04]. In 2005, Harkins, Weber, and Westmeyer, published a set of private key encryption schemes using finite frames and Hadamard arrays [HWW05]. Both of these schemes use the same frame theory structure.

Once a cryptosystem is developed, it is important to find out if it is vulnerable to an attack. In [HWW05], the authors showed that their system was vulnerable to a chosen ciphertext attack. Later in 2005, Bhatt, Kraus, Walters, and Weber published a paper [BKWW06] showing that the general cryptosystem used in both [MRN04] and [HWW05] was vulnerable to a known plaintext attack.

This paper begins with an introduction to cryptography and the mathematical concepts used in these cryptosystems. Then, it goes into the details of the cryptosystems and proves a few of the details left out of the published papers. Next, the vulnerabilities of these systems and two types of attack are explained. We conclude that this particular use of frame theory in cryptography is not secure and other avenues should be explored. We open the door for future research by questioning why Hadamard matrices can be used in cryptography.

CHAPTER 2. BACKGROUND ON CRYPTOGRAPHY

Cryptography is the science of disguising data so that only the sender and recipient can read the data. Suppose a student wanted to buy a textbook online from Amazon.com. The student must enter her credit card number and security code. However, many people could intercept the data as it flies through the Internet on its way to the financial department of Amazon.com. If a criminal found the student's credit card number and security code, he could buy many items online and the student may be charged. Therefore, it is important to disguise the credit card number and security code, so that only the student and the financial department at Amazon.com know the correct numbers.

Cryptographers call the data they want to send *plaintext*, usually converted into a string of integers between 0 and 255, inclusive. We think of this string as a vector in a vector space. The process of disguising the data is encryption. *Encryption* is a one-to-one mathematical function that requires a key (a unique number or set of numbers) and a plaintext as input to produce the encrypted text or *ciphertext*. The ciphertext, a new string (or vector) of integers between 0 and 255, can be converted back to the same medium as the plaintext and sent through the mail, Internet, or any other mode of data transportation. Once the receiver obtains the ciphertext, he applies a process called decryption. *Decryption* is the inverse mathematical function of encryption which takes a key and a ciphertext as input to reproduce the plaintext. The domains of the plaintext and ciphertext along with the keys, encryption function, and decryption function make up a *cryptosystem*.

A good cryptosystem is one that is computationally efficient and requires little storage space. Cryptographers are encouraged to develop systems that have a small key size, so that the keys are easy to share through covert channels; for example, short verbal communication, an encrypted email or disguised postal letter. The cryptosystem must also be secure against

attack. Most cryptographers use Kerckhoffs' Principle and knowledge of four basic attacks, described below, when creating their cryptosystems.

The following version of Kerckhoffs' Principle is quoted from Data Privacy and Security by Salomon [Sal03].

Theorem 2.1 (Kerckhoffs' Principle)**.** *One should assume that the method used to encipher data is known to the opponent, and that security must lie in the choice of the key. This does not necessarily imply that the method should be public, just that it is considered public during its creation. –Auguste Kerckhoffs*

Cryptanalysis is the art and science of decoding an encrypted message without knowing the keys. Cryptanalysis can be compared to finding the quickest and safest method of breaking into a house without the keys. Many view cryptanalysts as malicious and call them hackers, enemies, or adversaries. However, the tools, theory, and knowledge gained through cryptanalysis are essential. Law enforcement can use cryptanalysis to stop terrorism, child pornography, and fraud. If the government can decrypt emails, financial data, and other information stored on a terrorist's computer or website, then they may be able to save hundreds of lives by thwarting the terrorist's plans. Also, the information cryptanalysts discover while trying to break a cryptosystem can help cryptographers create stronger more secure systems.

There are four basic types of attacks cryptanalysts use to break a cryptosystem.

- *Ciphertext Only Attack*. In a ciphertext only attack, the adversary only has access to strings of ciphertexts. For example, suppose we have a substitution cipher, one in which we create a mapping from the English letters to a permutation of the letters. Then, one can use statistical properties of the English language to figure out what the message says. A cryptosystem is considered extremely weak if it is susceptible to this type of attack because this is the most difficult and time consuming way to discover the key used in the cryptosystem. A ciphertext only attack also usually requires extensive computational power.

- *Known Plaintext Attack*. In a known plaintext attack, the adversary has access to a set of plaintexts and their corresponding ciphertexts. For example, if it is known that the

cryptosystem is a specific linear transformation, then one can try to use mathematical properties of the linear transformation and the pairs of text to compute the key. A cryptosystem is considered weak if it is susceptible to this type of attack using current computational technologies. The RSA cryptosystem is a system that uses computations in $\mathbb{Z}_n$ where n is the product of two prime numbers. As of the writing of this paper, the largest factorable number using general purpose algorithms has 200 digits[1] and was found in 2005 according to the "General Purpose Factoring Records" [Con08]. Thus, we suspect that the RSA cryptosystem is considered secure if the cryptosystem uses a modulus n that is more than 200 digits. For more information about factoring records and large prime numbers see http://www.crypto-world.com/FactorRecords.html and http://primes.utm.edu.

- *Chosen Plaintext Attack*. In a chosen plaintext attack, the adversary obtains temporary access to the encryption machine. He can input any message he wants and see the ciphertext that it creates.

- *Chosen Ciphertext Attack*. In a chosen ciphertext attack, the adversary obtains temporary access to the decryption machine. He can input any ciphertext he chooses and see the message that produced it.

These last two attacks are more difficult to implement than the known plaintext attack or ciphertext only attack because gaining access to the encryption or decryption machine is usually more difficult than gaining a list of ciphertexts and/or plaintexts. Also, the chosen plaintext and chosen ciphertext attacks are more successful when the adversary's chosen texts are within a narrow range, so more strategic planning is usually necessary. If one can prove that a cryptosystem is secure against these four types of attacks, even if the attacker has infinite computational resources, then it is highly probable that the cryptosystem is not susceptible to attack. However, there are always other methods of attack being developed.

[1] In May 2007, an international team from EPFL, the University of Bonn, and NTT in Japan announced that they had factored a 307-digit number ($2^{1039} - 1$) using the "special number field sieve" method created in the late 1980's. For more information see the EPFL website, specifically http://actualites.epfl.ch/presseinfo-com?id=441.

For more information about cryptography and the use of mathematics in cryptography, see Stinson's Cryptography: Theory and Practice [Sti02].

CHAPTER 3. BACKGROUND ON MATHEMATICAL CONCEPTS

Cryptographers can use almost any branch or branches of mathematics to develop a cryptosystem. We are learning, however, that some branches are better suited for cryptography than others. In this chapter, we explore the definitions and theorems associated with frame theory; the specific area of math chosen by Miotke and Rebollo-Neira in [MRN04] and Harkens, Weber, and Westerner in [HWW05] to build their cryptosystems. We also explain the two areas of mathematics that these authors use to reduce the key size of their cryptosystems, namely Fourier analysis and Hadamard arrays.

3.1 Finite Frame Theory

The underlying foundation of frame theory is a Hilbert space. In order to understand what a Hilbert space is, we need to remember the definition of a Cauchy sequence. A *Cauchy sequence* is a set of vectors $\{x_j\}$ in an inner product space such that for all $\epsilon > 0$, there exists $M \in \mathbb{N}$ such that for all $k, l > M$, $||x_k - x_l|| < \epsilon$. An inner product space in which every Cauchy sequence converges is called *complete*. A *Hilbert space*, H, is a complete inner product space.

According to Folland in Real Analysis [Fol84], one of the most useful Hilbert spaces is the L^2 space because many important operations are bounded on L^2, such as the Fourier transformation. The set of all Lebesgue square-integrable functions on the interval $[-T, T] \in \mathbb{C}$ is denoted by $L^2[-T, T]$. It has the inner product, $\langle f(t), g(t)\rangle = \int_{-T}^{T} f(t)\overline{g(t)}\ dt$, and the 2-norm, $||f(t)||_2 = \sqrt{\langle f(t), f(t)\rangle}$. The Riesz-Fisher Theorem states that $H = L^2[-T, T]$ is a Hilbert space, see Royden [Roy88].

A *finite frame* is a finite sequence of vectors $\{x_j\}_{j\in[N]} \subset H$ for which there exist constants

$0 < L \leq U < \infty$ such that for all vectors $x \in H$,

$$L||x||^2 \leq \sum_j |\langle x, x_j \rangle|^2 \leq U||x||^2.$$

We call L and U the lower and upper *frame bounds*, respectively. The fact that a frame spans the Hilbert space is proven as Proposition 3.18 in Frames for Undergraduates [HKLW08].

The reason cryptographers think frame theory is an interesting mathematical tool is that frames allow any vector in the Hilbert space to be reconstructed. The following theorem states that, given any frame for a Hilbert space, there exists another frame, called the *dual frame*, such that any vector can be reconstructed by the given formula.

Theorem 3.1 ([HKLW08], Prop. 3.19)**.** *Let $\{x_j\}_{j=1}^N$ be a frame for a Hilbert space H. Then there exists a frame $\{y_j\}_{j=1}^N$ such that every $x \in H$ can be reconstructed with the formula: $x = \sum_{j=1}^N \langle x, y_j \rangle x_j = \sum_{j=1}^N \langle x, x_j \rangle y_j$.*

Proof. See [HKLW08] for a proof. □

The proof of the above theorem uses the concept of an analysis operator. Given a finite frame $\mathbb{X} = \{x_j\}_{j=1}^N \subset H$, the *analysis operator* $\Theta_{\mathbb{X}}$ is defined as a linear operator from the Hilbert space to the complex plane given by

$$\Theta_{\mathbb{X}} x = \begin{bmatrix} \langle x, x_1 \rangle \\ \vdots \\ \langle x, x_N \rangle \end{bmatrix} = \sum_{j=1}^N \langle x, x_j \rangle e_j$$

where $\{e_j\}_{j=1}^N$ is the standard orthonormal basis of $\mathbb{C}^N$. It is shown in [HKLW08] that $\Theta_{\mathbb{X}}$ is one-to-one and has a *synthesis operator*, $\Theta_{\mathbb{X}}^*$, such that $\Theta_{\mathbb{X}}^* \Theta_{\mathbb{X}} x = \sum_{j=1}^N \langle x, x_j \rangle x_j$. It is helpful to note that analysis and synthesis operators can easily be written as matrices. Let each vector $[x_j]^*$ be a row in the matrix Θ_X of an analysis operator. Then, the matrix Θ_X^* whose columns are the vectors $[x_j]$ is the matrix of the synthesis operator. Since $[x_j][x_k]^* = \langle x_j, x_k \rangle = \overline{\langle x_k, x_j \rangle} = [x_k][x_j]^*$, we know that $G = \Theta_X \Theta_X^*$ is a Hermitian matrix whose entries are given as inner products, also known as a Gram matrix. From linear algebra, we remember that Hermitian matrices have real nonnegative eigenvalues.

Two special types of frames are enticing to cryptographers because their properties make calculations easier. A *tight frame* is a frame whose upper and lower bounds are equal. If the upper and lower bounds equal one, then it is called a *Parseval frame*. The following theorem proves that if there exists a set of vectors that forms an orthonormal basis for the Hilbert space, then the set of vectors forms a Parseval frame.

Theorem 3.2 (Parseval's Identity)**.** *Let* $\{h_j\}_{j=1}^N$ *be an orthonormal basis for a Hilbert Space,* H*. Then, for all vectors* $x \in H$*,* $||x||^2 = \sum_{j=1}^{N} |\langle x, h_j \rangle|^2$*.*

Proof. See [HKLW08] for a proof (page 32). □

Another reason frames are interesting to cryptographers is that they have many of the same properties as matrices. Frames can be a basis for a linear space. However, they are usually more than a basis and allow for redundant vectors while still spanning the space. Frames can also be orthogonal to each other. Two frames $\mathbb{X}$ and $\mathbb{Y}$ are orthogonal if $\Theta_{\mathbb{X}}^* \Theta_{\mathbb{Y}} = \mathbf{0}$ where $\Theta_{\mathbb{X}}$ and $\Theta_{\mathbb{Y}}$ are the analysis operators for $\mathbb{X}$ and $\mathbb{Y}$, respectively [HKLW08].

3.2 Fourier Analysis

In [MRN04], the authors use Fourier analysis to create their cryptosystem. Before we can understand the claims they made, we need a few definitions and theorems from analysis.

From Saff and Snider in Fundamentals of Complex Analysis [SS03], we learn, that given any periodic, continuously differentiable function, $f(t)$, on an interval $[-T, T]$, we can represent $f(t)$ as a *Fourier series*, an infinite sum of complex exponentials,

$$f(t) = \sum_{-\infty}^{\infty} c_n e^{2\pi i n t/2T}$$

where the Fourier coefficients, c_n, are computed using integration,

$$c_n = \frac{1}{2T} \int_{-\infty}^{\infty} f(t) e^{-2\pi i n t/2T} \, dt.$$

It is helpful to know that these complex exponentials form an orthonormal basis for $L^2[-T, T]$. Folland [Fol84] states and proves this in a general sense. We state a version

for the set $\left\{\frac{1}{\sqrt{2T}}e^{i\pi nt/T}\right\}_{n\in\mathbb{Z}} \subset L^2[-T,T]$ and prove it here to help the reader make the connections between Hilbert spaces, frame theory, Fourier series and the cryptosystem presented in [MRN04]. Before we prove our theorem, we will prove four lemmas. The first identifies the relationship between the Hilbert space L^2 and the space of all bounded measurable functions L^∞. It shows that every element in L^∞ is also an element of L^2 and the 2-norm of an element is less than a constant times the infinity-norm of the element. The second, third, and fourth lemmas show that the set of complex exponentials $\left\{\frac{1}{\sqrt{2T}}e^{i\pi nt/T}\right\}_{n\in\mathbb{Z}} \subset L^2[-T,T]$ is normal, orthogonal, and complete.

Lemma 3.3. *$L^\infty[-T,T] \subset L^2[-T,T]$ and $||\cdot||_2 \leq \sqrt{2T}||\cdot||_\infty$.*

Proof. Let $f(t) \in L^\infty[-T,T]$. Then $||f(t)||_\infty = \inf\{M|m\{t \in (-T,T) : |f(t)| > M\} = 0\} = c$ for some constant $c \geq 0$. Note that $|f(t)| \leq c$ for all $t \in [-T,T]$ except on a set of measure zero. Thus,

$$\begin{aligned}
|f(t)| &\leq c \\
|f(t)|^2 &\leq c^2 \\
\int_{-T}^{T} |f(t)|^2 \, dt &\leq \int_{-T}^{T} c^2 \, dt \\
\left(\int_{-T}^{T} |f(t)|^2 \, dt\right)^{1/2} &\leq \left(\int_{-T}^{T} c^2 \, dt\right)^{1/2} \\
||f(t)||_2 &\leq \sqrt{2T}c \\
||f(t)||_2 &\leq \sqrt{2T}||f(t)||_\infty
\end{aligned}$$

Therefore, $f(t) \in L^2[-T,T]$ which implies $L^\infty[-T,T] \subset L^2[-T,T]$ and $||f(t)||_2 \leq \sqrt{2T}||f(t)||_\infty$.

□

Lemma 3.4. *The set $\left\{\frac{1}{\sqrt{2T}}e^{i\pi nt/T}\right\}_{n\in\mathbb{Z}} \subset L^2[-T,T]$ is normal.*

Proof. A set is normal if every element has norm 1.

$$\begin{aligned}\left\| \frac{1}{\sqrt{2T}} e^{i\pi nt/T} \right\|_2^2 &= \int_{-T}^{T} \left(\frac{1}{\sqrt{2T}} e^{i\pi nt/T} \right) \left(\frac{1}{\sqrt{2T}} e^{-i\pi nt/T} \right) \, dt \\ &= \int_{-T}^{T} \frac{1}{2T} \, dt \\ &= 1\end{aligned}$$

□

Lemma 3.5. *The set* $\left\{ \frac{1}{\sqrt{2T}} e^{i\pi nt/T} \right\}_{n\in\mathbb{Z}} \subset L^2[-T,T]$ *is pairwise orthogonal.*

Proof. Two elements are orthogonal if $\langle f(t), g(t) \rangle = 0$. Note: $n \neq m$ are integers, so $n-m \neq 0$ is also an integer. Thus, $e^{2\pi i(n-m)} = \cos(2\pi(n-m)) + i\sin(2\pi(n-m)) = 1$ and $e^{\pi i(n-m)} = \pm 1$.

$$\begin{aligned}\left\langle \frac{1}{\sqrt{2T}} e^{i\pi nt/T}, \frac{1}{\sqrt{2T}} e^{i\pi mt/T} \right\rangle &= \int_{-T}^{T} \left(\frac{1}{\sqrt{2T}} e^{i\pi nt/T} \right) \left(\frac{1}{\sqrt{2T}} e^{-i\pi mt/T} \right) \, dt \\ &= \int_{-T}^{T} \left(\frac{1}{2T} e^{i\pi t(n-m)/T} \right) \, dt \\ &= \frac{e^{2\pi i(n-m)} - 1}{2\pi i(n-m) e^{\pi i(n-m)}} \\ &= 0\end{aligned}$$

□

Lemma 3.6. *The set* $\left\{ \frac{1}{\sqrt{2T}} e^{i\pi nt/T} \right\}_{n\in\mathbb{Z}} \subset L^2[-T,T]$ *is complete.*

Proof. Let $\epsilon > 0$ and $f(x) \in L^2[-T,T]$ be given. Then, we know that $|f(x)|^2$ is integrable. By Proposition 4.14 [Roy88], we know there exists a $\delta > 0$ such that for $[T-\delta, T]$, $\int_{T-\delta}^{T} |f(x)|^2 \, dx < \left(\frac{\epsilon}{3}\right)^2$. Define $g(x) = f(x)$ for $x \in [-T, T-\delta]$ and $g(x) = 0$ for $x \in [T-\delta, T]$. Thus,

$$||f(x) - g(x)||_2 = \sqrt{\int_{T-\delta}^{T} |f(x)|^2 \, dx} < \frac{\epsilon}{3} \tag{3.1}$$

Let $X = [-T, T-\delta]$, $C(X)$ be the set of all continuous functions on X, $g_n(x) = \frac{1}{\sqrt{2T}} e^{i\pi nx/T}$ for $n \in \mathbb{Z}$, and $G(X)$ be the set of all linear combinations of g_n. Note that $G(X) \subset C(X) \subset L^2[-T, T-\delta]$ and the norm on $L^2[-T, T-\delta]$ is $||\cdot||_2$.

Claim: $G(X)$ is a closed subalgebra that separates points.

Before we begin the proof of our claim. We give a few definitions.

- *Complex Algebra.* The set $\mathcal{A}$ is said to be a complex algebra if it is a complex subspace of $C(X)$ where X is a Hausdorff space such that $fg \in \mathcal{A}$ whenever $f \in \mathcal{A}$ and $g \in \mathcal{A}$.
- *Complex Subalgebra.* A subset of a complex algebra that is itself a complex algebra.
- *Separate Points.* A set $A \in C(X)$ is said to separate points if for every $x, y \in X$ with $x \neq y$ there exists $f \in A$ such that $f(x) \neq f(y)$.

Proof of Claim. Choose any two unique functions $g_n(x), g_m(x) \in G(X)$ and any constant $c \in \mathbb{C}$. It is clear by the definition of $G(X)$ that $cg_n(x)+g_m(x)$, $g_n(x)g_m(x)$, and $\overline{g_n(x)} = g_{-n}(x)$ are elements of $G(X)$. Thus, $G(X)$ is a complex subalgebra of $C(X)$ that is closed under complex conjugation.

Now we need to show that $G(X)$ separates points. Suppose $x \neq y \in X$. Then $|x - y| < 2T$. We proceed with a proof by contradiction. Suppose $g_1(x) = g_1(y)$. Then $e^{i\pi(x-y)/T} = 1$. Thus, there exists $k \neq 0 \in \mathbb{Z}$ such that $\pi(x - y)/T = 2\pi k$ which implies $x - y = 2Tk$. This is a contradiction to the fact that $|x - y| < 2T$. Therefore, $G(X)$ is a closed subalgebra that separates points. □

By Littlewood's second principle [Roy88], there exists a continuous function $h(x) \in C(X)$ such that $||g(x) - h(x)||_2 < \frac{\epsilon}{3}$.

Let $\mathcal{A}$ be the closure of $G(X)$ with respect to the infinity norm, $||f_n(x)||_\infty = \sup_{x \in X} f_n(x)$. By the Complex Stone-Weierstrauss Theorem [Fol84], $\mathcal{A} = C(X)$ because $g_0(x) \in \mathcal{A}$ and $f_0(x) = 1$ for all $x \in X$. Therefore, there exists a polynomial $p(x) = \sum_{-N}^{N} c_n g_n(x)$ such that $||h(x) - p(x)||_\infty < \frac{\epsilon}{3\sqrt{2T}}$.

Hence,

$$\begin{aligned} ||f(x)-p(x)||_2 &= ||(f(x)-g(x))+(g(x)-h(x))+(h(x)-p(x))||_2 \\ &\leq ||f(x)-g(x)||_2+||g(x)-h(x)||_2+||h(x)-p(x)||_2 \qquad (3.2) \\ &\leq ||f(x)-g(x)||_2+||g(x)-h(x)||_2+\sqrt{2T}||h(x)-p(x)||_\infty \qquad (3.3) \\ &< \frac{\epsilon}{3}+\frac{\epsilon}{3}+\sqrt{2T}\frac{\epsilon}{3\sqrt{2T}} \qquad (3.4) \\ &= \epsilon \end{aligned}$$

The inequality (3.2) holds by the Minkowski Inequality, [Roy88]. The inequality (3.3) holds by Lemma 3.3. The inequality (3.4) holds by equation 3.1. Therefore, there exist constants $\{c_n : -N \leq n \leq N\}$ such that $||f(x)-\sum_{-N}^{N} c_n f_n(x)||_2 < \epsilon$, so $\left\{ f_n = \frac{1}{\sqrt{2T}} e^{i\pi nt/T} \right\}_{n\in\mathbb{Z}} \subset L^2[-T,T]$ is complete. □

Theorem 3.7. *The set* $E = \left\{ \frac{1}{\sqrt{2T}} e^{i\pi nt/T} \right\}_{n\in\mathbb{Z}} \subset L^2[-T,T]$ *forms an orthonormal basis for* $L^2[-T,T]$.

Proof. The set, E, is a complete orthonormal set by Lemmas 3.4, 3.5, and 3.6. Completeness implies that, given any function $f(t) \in L^2[-T,T]$, there exist constants c_n such that $\sum \frac{c_n}{\sqrt{2T}} e^{i\pi nt/T}$ converges absolutely to $f(t)$, see Theorem 5.1 in [Fol84]. In other words, the set E spans the Hilbert space $L^2[-T,T]$. Pairwise orthogonality of the elements implies that the set is linearly independent. Therefore, E is an orthonormal basis of $L^2[-T,T]$. □

3.3 Hadamard Arrays

In order to understand the cryptosystem created in [HWW05], we need to know a few definitions and theorems about Hadamard arrays and linear algebra.

A *Hadamard array*, denoted by $\mathbb{A} = H[m,k,\lambda]$, is an $m \times m$ matrix consisting of the elements $\pm a_1, \pm a_2 ... \pm a_k$ such that every row and every column has exactly λ elements of $\pm a_1$, λ elements of $\pm a_2$,..., λ elements of $\pm a_k$. Also, each pair of rows and each pair of columns must be orthogonal, i.e. their inner product is 0. Below is an example of $\mathbb{A} = H[4,4,1]$ with elements A, B, C, D.

$$\begin{bmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{bmatrix}$$

It is useful to know the following things about Hadamard arrays when $\lambda = 1$: they can only be of dimensions 1, 2, 4, or 8, their adjoint exists, and the product of a Hadamard array and its adjoint is the identity matrix multiplied by a scalar.

Theorem 3.8. *The following are properties of a Hadamard array,* $\mathbb{A} = H[m, k, 1]$*:*

1. $m = k$ *and* $m = 1, 2, 4,$ *or* 8.

2. $\mathbb{A}^*\mathbb{A} = \mathbb{A}\mathbb{A}^* = SI$ *where* $S = \sum_{j=1}^{k} |a_{1j}|^2$.

Proof. In his paper "Hadamard Designs" [Spe72], Spence uses the similarity of construction between n-letter Hadamard designs and Hadamard arrays with $\lambda = 1$. A Hadamard design is a square array of letters which commute in pairs and to which signs are attached, so that the scalar product of any two distinct rows is zero. An n-letter Hadamard design is an $n \times n$ array with n distinct elements in each row and each column. Thus, their matrix representation is similar to that of a Hadamard array. Here is a sketch of his proof.

If $\mathbb{A}$ is a Hadamard array with $\lambda = 1$, then we can use elementary matrix operations to make all elements in the first row and the first column positive and to ensure that the first row is identical to the first column.

Next, create a block matrix, M, as below

$$M = \begin{bmatrix} \mathbb{A} & -\mathbb{A} \\ -\mathbb{A} & \mathbb{A} \end{bmatrix}.$$

This matrix is a multiplication table of a loop $\mathcal{L}$ of order $2n$ with elements $A, B, ...N, -A, -B, ..., -N$. A loop is a pair $(\mathcal{L}, \cdot)$ where $\mathcal{L}$ is a nonempty set and $(a, b) \to a \cdot b$ is a closed binary operation on $\mathcal{L}$ with the property that given any $a, c \in \mathcal{L}$, there exists a unique element b such that $a \cdot b = c$. A loop also contains a two-sided identity element 1.

The loop satisfies the following:

1. The center, Z has two elements $1, -1$ such that $(-1)^2 = 1$ and $1 \neq -1$.

2. If $x \in Z$, then $x^2 = -1$.

3. If $xy \neq yx$, then $xy = -yx$ and x, y generate a quaternion group.

4. If $x(yz) = (xy)z$, then x, y, z generate a subgroup.

The only loops satisfying these conditions are the cyclic groups of order 2 and order 4, the quaternion group of order 8, and the Cayley loop of order 16. The cyclic group of order 2 can be determined by a Hadamard array $\mathbb{A} = H[1, 1, 1]$, the cyclic group of order 4 by a Hadamard array $\mathbb{A} = H[2, 2, 1]$, the quaternion group of order 8 by a Hadamard array $\mathbb{A} = H[4, 4, 1]$, and the Cayley loop of order 16 by a Hadamard array $\mathbb{A} = H[8, 8, 1]$. Therefore, the only possible values for m and k are $1, 2, 4$, or 8.

Now we can show that $\mathbb{A} = H[8, 8, 1]$, has an adjoint, and that the product of $\mathbb{A}\mathbb{A}^* = \mathbb{A}^*\mathbb{A} = SI$ where S is a scalar. The proof that the smaller Hadamard arrays also have these qualities is similar, so we will not include it here.

Let a, b, c, d, e, f, g, h be a set of distinct real numbers. Then the Hadamard array M, given in [HWW05], shown below is similar to all possible Hadamard arrays $\mathbb{A} = H[8, 8, 1]$.

$$M = \begin{pmatrix} a & b & c & d & e & f & g & h \\ -b & a & d & -c & f & -e & -h & g \\ -c & -d & a & b & g & h & -e & -f \\ -d & c & -b & a & h & -g & f & -e \\ -e & -f & -g & -h & a & b & c & d \\ -f & e & -h & g & -b & a & -d & c \\ -g & h & e & -f & -c & d & a & -b \\ -h & -g & f & e & -d & -c & b & a \end{pmatrix}$$

By definition, M^* is the conjugate transpose of M, so we can see it exists and we can show that $MM^* = M^*M = SI$ where $S = a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2$. Since the rows and columns of M are pairwise orthogonal, we know that $[r_i]^*[r_j] = 0$ for all rows $r_i \neq r_j$. Therefore,

$$MM^* = \begin{pmatrix} a & b & c & d & e & f & g & h \\ -b & a & d & -c & f & -e & -h & g \\ -c & -d & a & b & g & h & -e & -f \\ -d & c & -b & a & h & -g & f & -e \\ -e & -f & -g & -h & a & b & c & d \\ -f & e & -h & g & -b & a & -d & c \\ -g & h & e & -f & -c & d & a & -b \\ -h & -g & f & e & -d & -c & b & a \end{pmatrix} \begin{pmatrix} a & -b & -c & -d & -e & -f & -g & -h \\ b & a & -d & c & -f & e & h & -g \\ c & d & a & -b & -g & -h & e & f \\ d & -c & b & a & -h & g & -f & e \\ e & f & g & h & a & -b & -c & -d \\ f & -e & h & -g & b & a & d & -c \\ g & -h & -e & f & c & -d & a & b \\ h & g & -f & -e & d & c & -b & a \end{pmatrix}$$

$$= (a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2)\ I$$

Similarly, since $[c_i]^*[c_j] = 0$ for all columns $c_i \neq c_j$, $M^*M = (a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2)\ I$. □

Unfortunately, these matrices are rather small to use as a tool for encryption. Thankfully, we can expand them by using the tensor product. The *tensor product* of two matrices $A_{m\times m}$ and $B_{k\times k}$ is defined as follows:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{bmatrix}$$

Note that $A \otimes B$ is an $mk \times mk$ matrix. Also, if the rows (columns) of A are pairwise orthogonal and the rows (columns) of B are pairwise orthogonal, then the rows (columns) $A \otimes B$ are pairwise orthogonal.

CHAPTER 4. CRYPTOSYSTEM USING FRAME THEORY

This chapter begins with an explanation of a general cryptosystem using frame theory. Then, it goes into the details of two particular schemes. In 2004, Miotke and Rebollo-Neira published a theoretical private key encryption scheme using infinite frames and oversampling of Fourier coefficients [MRN04]. In 2005, Harkens, Weber, and Westmeyer, published a set of private key encryption schemes using finite frames and Hadamard arrays [HWW05].

In theory, this type of cryptosystem works in infinite space; however, computers and other technological tools can only perform finite calculations. Thus, the following will be presented in the finite complex space of dimension N.

4.1 General Cryptosystem

The general cryptosystem presented in [HWW05] is based on two orthogonal frames, $\mathbb{X} \subset H$ and $\mathbb{Y} \subset K$ with analysis operators (defined in Section 3.1) $\Theta_{\mathbb{X}}$ and $\Theta_{\mathbb{Y}}$, respectively. The plaintext is written as a vector which we call p and is an element of H. There is an arbitrary "garbage" vector called g, which is an element of K. The keys in this system are $\mathbb{X}$ and $\mathbb{Y}$, along with their analysis operators. However, as we will show below, the recipient of the ciphertext only needs to know the analysis operator $\Theta_{\mathbb{X}}$ to decode the message.

To encrypt the plaintext, the sender multiplies the plaintext vector, $p = [p_1, p_2, ..., p_m]$, by $\Theta_{\mathbb{X}}$ and the garbage vector, $g = [g_1, g_2, ..., g_n]$ by $\Theta_{\mathbb{Y}}$. Then, he adds the two vectors together to create the ciphertext, c. In symbols, $c = \Theta_{\mathbb{X}} p + \Theta_{\mathbb{Y}} g$.

To decrypt the ciphertext, the recipient calculates the adjoint of $\Theta_{\mathbb{X}}$, denoted by $\Theta^*_{\mathbb{X}}$, which we know exists by Theorem 3.8. He then multiples the ciphertext by $\Theta^*_{\mathbb{X}}$ to recover the

plaintext. This works because $\mathbb{X}$ and $\mathbb{Y}$ are orthogonal frames so $\Theta_{\mathbb{X}}^*\Theta_{\mathbb{Y}} = 0$. In symbols,

$$\begin{aligned}\Theta_{\mathbb{X}}^* c &= \Theta_{\mathbb{X}}^*(\Theta_{\mathbb{X}} p + \Theta_{\mathbb{Y}} g) \\ &= \Theta_{\mathbb{X}}^*\Theta_{\mathbb{X}} p + \Theta_{\mathbb{X}}^*\Theta_{\mathbb{Y}} g \\ &= Ip + 0 \\ &= p\end{aligned}$$

In [HWW05], the authors make several observations. One is that the two matrices, $\Theta_{\mathbb{X}}$ and $\Theta_{\mathbb{Y}}$, can be written and created as a single matrix, $\Theta = (\Theta_{\mathbb{X}}|\Theta_{\mathbb{Y}})$. In this case, encryption would be calculated as $c = \Theta(p \oplus g)$. Another observation is that a key consisting of two rather large orthogonal frames would be difficult to share and storage of the analysis operators is inefficient, especially if they must remain in matrix form. The following two cryptosystems make use of these observations in an attempt to create a better cryptosystem.

4.2 Miotke and Rebollo-Neira Cryptosystem

In [MRN04], Miotke and Rebollo-Neira use properties of Fourier coefficients to significantly decrease the size of the key. Their scheme consists of an arbitrary signal $f(t) \in L^2[-T, T]$, the N Fourier coefficients of $f(t)$ written in a vector g, the frame $F = \left\{\frac{1}{\sqrt{2T}} e^{i\pi ant/T}\right\}_{n\in\mathbb{Z}} \subset L^2[-T, T]$, an oversampling parameter $a \in (0, 1)$, and a message or plaintext vector of length $m \leq N$. The keys are simply the values of the variables a, T, N and m.

From Theorem 3.7, we know that $E = \left\{\frac{1}{\sqrt{2T}} e^{i\pi nt/T}\right\}_{n\in\mathbb{Z}} \subset L^2[-T, T]$ is an orthonormal basis for $L^2[-T, T]$. A similar proof shows that $F = \{\frac{1}{\sqrt{2T}} e^{i\pi ant/T}\}_{n\in\mathbb{Z}}$ is an orthogonal basis for $L^2[-\frac{T}{a}, \frac{T}{a}]$; note that it is not a normal set. Since $0 < a < 1$, the interval $[-T, T]$ is contained in the interval $[-\frac{T}{a}, \frac{T}{a}]$, so if $f(t) \in L^2[-T, T]$, then $f(t) \in L^2[-\frac{T}{a}, \frac{T}{a}]$ and can be written as a linear combination of functions in F. For our purposes, we let $F \subset L^2[-T, T]$, so F is a tight frame for the interval $[-T, T]$ with frame bounds $L = U = a^{-1}$. (The frame bound was proven in a paper by Rebollo-Neira and Constantinides, see [CRN96].) Thus, a is called the oversampling parameter because it creates a set of vectors that is not linearly independent, but spans the space $L^2[-T, T]$. This is significant because it allows us to hide a message vector in the null space of a Gram matrix as we will show below.

Both the sender and the recipient need to calculate the analysis operator of F. Since computers cannot function in an infinite domain, we limit the size of the analysis operator to a $N \times N$ matrix G where $g_{r,n} = \frac{1}{2T}\int_{-T}^{T} e^{-i\pi art/T} e^{i\pi ant/T}\ dt = \langle F_n(t), F_r(t)\rangle$. We note that G must have a null space of dimension at least m, the length of the plaintext. Since the null space is created by the oversampling parameter a, the dimension of N is depends on a. We also note that G is a Gram matrix, so from Chapter 3 we know that G has positive eigenvalues.

The sender begins the encryption process by choosing an arbitrary signal, $f(t)$ and computing the N Fourier coefficients $g_n = \frac{a}{\sqrt{2T}}\int_{-T}^{T} f(t)e^{-i\pi ant/T}\ dt$ where $n = 1, ..., N$. These coefficients create the vector $g = [g_n]_{n\in[N]}$. This is the noise or garbage vector, referred to in Section 4.1. To encrypt the plaintext, p, of length $m < N$, the sender computes the orthonormalized eigenvectors corresponding to the m smallest eigenvalues of G. Then, he creates an $N \times m$ matrix Θ whose columns are the computed eigenvectors. The ciphertext is computed by multiplying p by Θ and adding g, $c = \Theta p + g$. Since the columns of Θ correspond to the smallest eigenvalues of G, the columns of Θ are in the pseudokernel of G. Thus, Θp is also in the pseudokernel of G.

To decrypt the message, the recipient recreates the signal by taking the entries of the ciphertext, c_n and calculating $f(t) = \sum_{n=1}^{N} c_n e^{i\pi ant/T}$. Next, he calculates the garbage vector, g, that was chosen by the sender, $g = [g_n]_{n\in[N]} = \frac{a}{\sqrt{2T}}\int_{-T}^{T} f(t)e^{-i\pi ant/T}\ dt$. Then, he finds the orthonormalized eigenvectors corresponding to the m smallest eigenvalues of the matrix G (calculated previously) and creates Θ whose columns are the computed eigenvectors. Note that $\Theta^*\Theta = I$ because the columns are orthonormal. The message is decrypted by subtracting the vector g from the ciphertext vector $c = [c_n]_{n\in[N]}$ and then multiplying the resulting vector by Θ^*. Symbolically,

$$\Theta^*(c - g) = \Theta^*(\Theta p + g - g) = \Theta^*\Theta p = p$$

4.3 Harkins, Weber, and Westmeyer Cryptosystem

In [HWW05], the authors use the properties of Hadamard arrays to reduce the size of the key. Their scheme consists of a plaintext vector p of length m, an orthogonal matrix Θ of

dimension $2m \times 2m$, and a random garbage vector g of length m.

To create Θ, they choose J Hadamard arrays $\mathbb{A}_1, \mathbb{A}_2, ...\mathbb{A}_J$. These arrays can be of various sizes, so denote the dimension of $\mathbb{A}_i$ by $d_i \times d_i$. From Theorem 3.8, we know d_i can be 1, 2, 4, or 8. Then they create Θ by taking the tensor product of these arrays.

$$\Theta = \mathbb{A}_1 \otimes \mathbb{A}_2 \otimes ... \otimes \mathbb{A}_J$$

The dimension of Θ is $(d_1 d_2 \cdots d_J) \times (d_1 d_2 \cdots d_J) = 2m \times 2m$. We note that Θ can be created from just the first row of entries in each Hadamard array, $\mathbb{A}_i$. Thus, the key to this cryptosystem is a vector of size $(d_1 + d_2 + ... + d_J)$.

Encryption begins by choosing an arbitrary garbage vector of length m. The ciphertext is created by concatenating p and g and then multiplying by Θ, $c = \Theta(p \oplus g)$.

Decryption of the ciphertext is relatively straightforward. Since Θ is the tensor product of Hadamard arrays which have pairwise orthogonal rows and columns by definition, we know that Θ also has pairwise orthogonal rows and columns. Thus, Θ^* exists such that $\Theta^*\Theta = SI$ where $S = \sum_{i=1}^{2m} a_{1i}^2$ where $\Theta = [a_{ii}]$, refer to Theorem 3.8. Hence, to recover the message, the recipient multiplies the ciphertext by $\frac{1}{S}\Theta^*$ and reads the first m values to determine the message, $\frac{1}{S}\Theta^* c = \frac{1}{S}\Theta^*\Theta(p \oplus g) = p \oplus g$.

CHAPTER 5. CRYPTANALYSIS

According to Kerckhoffs' Principle, the attacker knows the design of the cryptosystem, but not the key. With this in mind, we can show that the general cryptosystem explained in Section 4.1 is vulnerable to a chosen plaintext attack and more importantly a known plaintext attack. This implies that the other two cryptosystems in Sections 4.2 and 4.3 are also vulnerable to these types of attacks. We assume the attacker knows that $c = (\Theta_{\mathbb{X}}|\Theta_{\mathbb{Y}})(p \oplus g)$. He wants to find the key, in this case the matrix $(\Theta_{\mathbb{X}}^*)$, so that he can decrypt any ciphertext encrypted with this key.

5.1 Chosen Plaintext attack

In this attack, we have temporary access to the encryption machine. We assume that the matrix $(\Theta_{\mathbb{X}}|\Theta_{\mathbb{Y}})$ is fixed and will be used during future communication. We can choose any plaintext, p, and obtain the ciphertext, c, associated with it. Since we know the length of the message, $|p|$, and the length of the ciphertext, $|c|$, we can calculate the length of the garbage vector, $|g| = |c| - |p|$. By following the steps below, we can determine $\Theta_{\mathbb{X}}$

- Determine the range of $\Theta_{\mathbb{Y}}$. First, the adversary chooses a message vector p. Second, he encrypts it twice to obtain ciphertexts, c_0 and c_1. These ciphertexts will usually not be the same, because the garbage vector used during encryption is randomly generated each time the message is encrypted. Third, he computes $y_1 = c_1 - c_0$. We know y_1 is in the range of $\Theta_{\mathbb{Y}}$ because $y_1 = (\Theta_{\mathbb{X}}|\Theta_{\mathbb{Y}})(p \oplus g_1) - (\Theta_{\mathbb{X}}|\Theta_{\mathbb{Y}})(p \oplus g_0) = (\Theta_{\mathbb{X}}|\Theta_{\mathbb{Y}})(0 \oplus (g_1 - g_0))$. Fourth, he encrypts the message a third time to obtain ciphertext c_2 and compute $y_2 = c_2 - c_0$. The adversary should continue finding vectors, y_k, until he obtains a linearly independent set of $|g|$ vectors. This set, $\mathbb{Y} = \{y_1, ..., y_{|g|}\} \subset \mathbb{C}^{|c|}$, is a basis for the range

of $\Theta_{\mathbb{Y}}$.

- Determine the range of $\Theta_{\mathbb{X}}$. First, the adversary must compute an orthonormal basis for the orthogonal complement of $\mathbb{Y}$, $\{w_1, ..., w_{|p|}\}$. Second, he encrypts a message, p_1, to obtain ciphertext, c_1'. Third, he projects c_1' onto the orthogonal complement of $\mathbb{Y}$, $v_1 = \sum_{i=1}^{|m|} \langle c_1, w_i \rangle w_i$. We note that the vector v_1 is in the range of $\Theta_{\mathbb{X}}$ because v_1 is a linear combination of the vectors in the orthonormal basis for $\mathbb{Y}^{\perp}$ and $\mathbb{Y} \oplus \mathbb{Y}^{\perp} = \mathbb{C}^{|c|}$. The adversary should make a note of the pair $\{p_1, v_1\}$ to use in the computation of $\Theta_{\mathbb{X}}$. Fourth, he encrypts a different message, p_2, and computes v_2. He continues finding vectors v_i until he has a linearly independent set of $|p|$ vectors. This set, $\mathbb{V} = \{v_1, ..., v_{|p|}\}$, is a basis for the range of $\Theta_{\mathbb{X}}$.

- Compute $\Theta_{\mathbb{X}}$. Using the pairs of messages and ciphertexts, $\{p_i, v_i\}$, collected to create $\mathbb{V}$, the adversary has a system of linear equations that he can solve to find $\Theta_{\mathbb{X}}$, $(\Theta_{\mathbb{X}}|\Theta_{\mathbb{Y}})(p_i \oplus 0) = v_i$.

We note that the matrix norm of $\Theta_{\mathbb{X}}$ may not be 1 as was the case in the cryptosystem presented in Section 4.3. Thus, the adversary must divide the entries of his future decrypted messages by a factor of $S = \sum_{i=1}^{|c|} a_{1i}^2$ where $\Theta_{\mathbb{X}} = [a_{ii}]$ is the first row of $\Theta_{\mathbb{X}}$. Therefore, the computation to decrypt future messages the adversary encounters using this encryption machine is $S^{-1}(\Theta_{\mathbb{X}}|0)^* c = S^{-1}(\Theta_{\mathbb{X}}|0)^*(\Theta_{\mathbb{X}}|\Theta_{\mathbb{Y}})(p \oplus g) = p$.

5.2 Known Plaintext attack

In this attack, we have access to an unlimited number of pairs of plaintexts and their corresponding ciphertexts. We assume that each of these pairs was created using the same matrix $(\Theta_{\mathbb{X}}|\Theta_{\mathbb{Y}})$ and that this matrix will be used in future communications. From our set of plaintext/ciphertext pairs $\{(p_i, c_i)\}$, we choose N pairs such that the vectors p_i are linearly independent and span $\mathbb{C}^N$. Using these pairs, we can solve the system of linear equations $\Theta_{\mathbb{X}}^* c_i = p_i$ to find a unique matrix $\Theta_{\mathbb{X}}^*$. This matrix will allow us to decrypt any ciphertext that is created using this particular cryptosystem.

CHAPTER 6. CONCLUSION AND FUTURE WORK

In [HWW05], they conclude that the main problem with this type of cryptosystem is the linearity. We agree; however, in the course of our research, we found that Hadamard matrices have been used in cryptography. Since Hadamard arrays are similar to Hadamard matrices, we wonder if these ideas could be combined to develop a secure cryptosystem.

In his book Hadamard Matrices [Hor06], Horadam explains that almost bent functions provide maximum possible resistance to both linear and differential cryptanalysis attacks and thus are good functions to use in cryptography. He begins with a Boolean function $f : V(n, 2) \to GF(2)$ and defines a bent function as a function whose absolute value of the Walsh-Hadamard Transform is constant. He then shows that a bent function is equivalent to a Hadamard matrix. He states a formula to calculate the resistance of f to a linear attack which translates into nonlinearity conditions on the Walsh-Hadamard Transform. We believe further exploration into this nonlinear property of Hadamard matrices may provide insight into finding a way to use frame theory and Hadamard arrays successfully in encryption.

In summary, the proposed general cryptosystem using finite frames and the cryptosystems presented in [MRN04] and [HWW05] are not secure with respect to a chosen plaintext attack or a known plaintext attack. A cryptanalyst can use the linearity of these systems to find the key, so these systems should not be used for cryptography unless someone finds a way to introduce nonlinearity into the algorithm.

BIBLIOGRAPHY

[BKWW06] Ghanshyam Bhatt, Lorraine Kraus, Laura Walters, and Eric Weber. On hiding messages in the oversampled fourier coefficients. *Journal of Mathematical Analysis and Applications*, 320:492–298, 2006.

[Con08] Scott Contini. General purpose factoring records. *http://www.crypto-world.com/FactorRecords.html*, April 2008.

[CRN96] A.G. Constantinides and L. Rebollo-Neira. Power spectrum estimation from values of noisy autocorrelations. *Signal Processing*, 50:223–231, 1996.

[Fol84] Gerald B. Folland. *Real Analysis: Modern Techniques and Their Applications*. Wiley-Interscience, September 1984.

[HKLW08] Deguang Han, Keri Kornelson, David Larson, and Eric Weber. *Frames for Undergraduates*. American Mathematical Society, 2008.

[Hor06] K. J. Horadam. *Hadamard Matrices and Their Applications*. Princeton University Press, November 2006.

[HWW05] Ryan Harkins, Eric Weber, and Andrew Westmeyer. Encryption schemes using finite frames and hadamard arrays. *Experimental Math*, 14:423–433, 2005.

[MRN04] J.R. Miotke and L. Rebollo-Neira. Oversampling of fourier coefficients for hiding messages. *Applied and Computational Harmonic Analysis*, 16:203–207, 2004.

[Roy88] Halsey Royden. *Real Analysis*. Prentice Hall, 3 edition, February 1988.

[Sal03] David Salomon. *Data Privacy and Security*. Springer-Verlag, New York, 2003.

[Spe72] Edward Spence. Hadamard designs. *Proceedings of the American Mathematical Society*, 32:29–31, 1972.

[SS03] E.B. Saff and A.D. Snider. *Fundamentals of Complex Analysis*. Prentice Hall, New Jersey, 3 edition, 2003.

[Sti02] Douglas R. Stinson. *Cryptography: Theory and Practice*. Chapman & Hall/CRC, 2 edition, February 2002.