ABSTRACT

Encrypting the Universe

Lesley Vestal, M.S.

Chairperson: Gerald B. Cleaver, Ph.D.

Layer one $\mathcal{N} = 4$ SUSY Weakly Coupled Free Fermionic Heterotic String (WCFFHS) Models that include string-scale massive gauge sectors are statistically investigated for even orders through 12 for uniqueness and gauge content. A focus is given to models containing the standard model or gauge group content with the embedded standard model. Results are compared with those of prior searches of $\mathcal{N} = 4$ models without explicit string-scale massive gauge sectors. This search revealed models with standard model gauge content at the string scale, which were not observed in prior searches.

Additionally, research regarding an image encryption algorithm is presented. The RGB values of each pixel in an image are encrypted using three intertwined Mandelbrot summations. Runtimes for decryption depend primarily on the size of the image. Modifications to increase complexity and runtime are explored. Advantages include adaptability, reasonable runtime on a typical personal computer and that it is novel, enhancing its security.

Encrypting the Universe

by

Lesley Vestal, B.S.

A Thesis

Approved by the Department of Physics

_____

Dwight Russell, Ph.D., Chairperson

Submitted to the Graduate Faculty of
Baylor University in Partial Fulfillment of the
Requirements for the Degree
of
Master of Science

Approved by the Thesis Committee

_____

Gerald B. Cleaver, Ph.D., Chairperson

_____

Anzhong Wang, Ph.D.

_____

Zhenrong Zhang, Ph.D.

_____

Klaus Kirsten, Ph.D.

Accepted by the Graduate School
August 2017

_____

J. Larry Lyon, Ph.D., Dean

Page bearing signatures is kept on file in the Graduate School.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

PREFACE

Mathematics allows for the physics of our universe and others to be encrypted. In this way, string model-building constructs many possible universes by way of encryption. It is a way of processing the physical implications of the theory and encoding this information, and is able to go beyond the current limits of experimental physics. This thesis presents two independent realizations of encryption.

ACKNOWLEDGMENTS

I am very thankful to Dr. Gerald Cleaver and everyone in the Early Universe Cosmology and Strings (EUCOS) Group for allowing me to join in this research. Dr. Cleaver, thank you for your patience, kindness, and guidance these last three years. I would not have made it this far if not for you, and I question if I would have continued to pursue physics.

I have enjoyed working on both the string model analysis as well as the encryption project, and I have learned so much from the experience. Thank you to Dr. Douglas Moore and past EUCOS members for constructing this amazing model-building framework. He, Dr. Cleaver, and Dr. Tim Renner first taught me about string theory and model-building when I was an undergraduate in 2012. More recently, Robert Gill spent hours teaching me how to use and modify the framework and built many of the models discussed here, for which I am grateful. Kameron Scott expanded my analysis program and helped me with debugging; he will also continue this work for higher orders, and I look forward to hearing his results. Thank you all for allowing me to work on this project and analyze these models.

Dr. Jeff Lee and Brandon Mattingly came up with this fascinating encryption project, which is different from anything I had ever worked on before. Thank you for letting me be a part of this research. Jacob Oost was an invaluable resource when I had programming questions or just wanted to brainstorm. He joined this project and drastically improved the work, and I learned so much from him.

Dr. Matthews and Dr. Hyde, thank you for first bringing me to Baylor for the REU, and for teaching me about research. This experience fostered my love of physics.

Thank you to my undergraduate research advisor, Dr. Welch. You drastically contributed to my education and my interest in research. I greatly appreciate all the time you spent teaching me about gravity, research, and faith.

Thank you also to Dr. Wu and Dr. Wang for your wonderful advice and conversations. Thank you to Ms. Baker and Ms. Nunn-Graves for always making me feel welcome.

Thank you to my classmates, I very much enjoyed spending innumerable meals and game nights with you all. You all mean so much to me, and I look forward to many more years of friendship. Blake, Jacob, and Jared, you have been great friends and have each had a significant impact on my life. Grace, thank you for your friendship, silliness, and perfect advice.

Thank you to my Mom, Dad, and Grandparents for being supportive on both good days and bad.

The last couple years have been some of the hardest of my life, but I am so fortunate to have had the opportunity to significantly deepen my understanding of physics and to contribute to research in a field I love.

DEDICATION

To my Memaw,

Betty Burdine

CHAPTER ONE

Introduction

Motivation

String theory presents a charming and mathematically elegant solution to unification where other theories have not. It accomplishes this fundamentally by treating particles not as point-like, but as one-dimensional, vibrating strings. String theory may be the last piece of the puzzle in unifying and explaining gravity and quantum mechanics at all scales. For very large gravitational fields as well as in the quantum realm, general relativity is not sufficient on its own and a quantum theory of gravitation is needed [1]. String theory is a modification to relativity and reduces to general relativity. In the low energy limit string theory must reduce to the Standard Model. Elementary particles are vibrational modes of the strings, and, rather than point-like particles, these vibrating strings are the smallest possible objects [1].

String theory requires ten dimensions - the four from Minkowski space plus six additional dimensions. The additional six that have not been observed are compactified. These additional six dimensions are very small, as are strings. Both are roughly on the order of the Planck scale, i.e. 10^{-35}m. Current technology does not allow for experiments precise enough to prove or disprove their existence. Strings are much smaller still, roughly on the order of the Planck length. An alternative to traditional experimental approaches is therefore necessary, and model-building research allows for progress in the field [2].

My focus is on string phenomenology, constructing and analyzing realistic string models. As there are many possible string models, roughly 10^{500}, it is of particular interest to examine those that may represent our universe [3-5]. This is accomplished in part by setting the parameters of the model-building algorithm such that only

models that match our universe's physical constraints are generated. This search utilizes the EUCOS Free Fermionic (FF) Framework and employs a systematic FF construction formalism [2, 11-47].

Mathematics allows for the physics of our universe to be encrypted; string model-building is a way of investigating many possible universes. It is a way of processing the physical implications of the theory and encoding this information, compactifying the six extra small dimensions and allowing for physical laws. The output is information in the form of gauge group content that may describe our universe, as well as others like it. The gauge content of supersymmetric (SUSY) models describes the forces through which matter interacts. This research aims to explore different types of SUSY models, analyzing in particular models containing the Standard Model, $SU(3) \times SU(2) \times U(1)$. This search considers only non-abelian content, not determining U(1) charges. The number of independent U(1)'s is equal the difference in the rank of the non-abelian gauge groups and 22.

Until recent decades, there were thought to be five distinct string theories. All five turned out to be special cases of one specific theory. However, in going from five theories to one, the number of string models rose from around one trillion to around 10^{500}. This set of10^{500} models is referred to as the string landscape [3, 4, 5].

Unification has been framed as a natural expectation, which is not an unfair jump to make after Maxwell's equations in the nineteenth century unified electricity and magnetism followed by the model of electroweak interactions by Glashow, Weinberg and Salam more recently, in the later twentieth century. The possibility of still further unifying quantum field theory with general relativity is compelling, as string theory proposes. String theory has been described as "21st century physics that fell by chance in the 20th century" [64]. However, string theory is not the only method for unifying general relativity and quantum mechanics. Alternatives include Loop Quantum Gravity, Hořava Lifshitz Gravity, Causal Dynamical Triangulation,

Causal Sets, Non-commutative Geometry, Twister Theory, and Asymptotic Freedom, as summarized in [63]. These alternatives will not be considered here as this goes beyond the scope of this thesis.

The Standard Model of Particle Physics (SM) provides a good picture of particle physics in our universe, but also leaves many questions unanswered. Chapter one starts with the SM and progresses towards a theory that may fully explain particles and field interactions. Section 1.2 begins with a review the SM, and continues in 1.3 with unanswered questions. Section 1.4 introduces SUSY as an addition to the SM, resolving many of the issues associated with the SM. String theory is again mentioned in section 1.5 as a solution to a key shortcoming of the SM and MSSM. Section 1.6 introduces the Free Fermionic (FF) approach, and 1.7 continues this discussion of FF strings.

A Brief Review of the Standard Model

Just as string theory describes fundamental forces and interactions, the Standard Model (SM) of particle physics describes these forces along with elementary particles [1]. The SM takes as fundamental objects elementary particles, fermions and bosons. These particles are the building blocks of the physics we observe.

Particles in the the SM are categorized by their spins. Bosons have integer spin values, while fermions have half-integer spin and are divided into subcategories of quarks and leptons. Quarks and leptons are then each divided into three groups called generations [51, 52]. The SM's prediction of Higgs boson's existence predated the experimental observation of the particle in 2012 [61]. Through interacting with the Higgs boson, W and Z bosons become massive at low energy scales; this is referred to as the Higgs mechanism. For high energies (and unbroken electroweak symmetry), all particles are expected to be massless.

Unanswered Questions of the SM

The SM is an important step in understanding our universe, but leaves many important questions unanswered, including explaining gravity. Some theories for explaining gravity include a theoretical particle called the graviton. The graviton is not included in the SM. Note that this particle also has not been observed.

Near the Planck energy, fine-tuning becomes necessary. The Planck energy is on the order of 10^{19} GeV, while the weak scale is around 100 GeV. The degree of normalizing required to resolve this significant difference may suggest other particles or phenomenon not included in the SM [59].

The SM makes no attempt to explain dark energy. As of yet undiscovered fundamental particles could provide an explanation for the phenomena we observe. The phenomenon responsible for the accelerating expansion of the universe is not full understood, but has been named dark energy. The SM makes no mention of dark energy nor does it address it with a theoretical particle or group of particles.

The weak force is many orders of magnitude greater than that of gravity. This is referred to as the hierarchy problem, and is also not addressed by the SM. The large difference in the Planck mass and the mass of the Higgs boson is also unexpected, and, through the SM, can only be resolved by fine-tuning.

Minimal Supersymmetric Standard Model as a Possible Answer

The Minimal Supersymmetric Standard Model (MSSM) builds off of the existing model. Each particle in the MSSM is given a supersymmetric partner, referred to as superpartners; this construct of pairing the fundamental particles roughly doubles the number of particles required and is referred to as supersymmetry. The MSSM is described as minimally supersymmetric because it introduces only the minimum number of particles necessary to give the SM particles superpartners and keep the theory consistent. Though none of these superpartners have yet been directly observed, their

Table 1.1: Particle Content of the MSSM. Reproduced in [67], originally from [60].

Superfield	Bosons		Fermions		$SU(3)_C$	$SU(2)_L$	$U(1)_Y$
Gauge							
$\mathbf{G}^a$	gluon	g^a	gluino	$\tilde{g}^a$	**8**	**1**	0
$\mathbf{V}^k$	weak	W^k $(W^{\pm}, W^0)$	wino, zino	$\tilde{w}^k$ $(\tilde{w}^{\pm}, \tilde{w}^0)$	**1**	**3**	0
$\mathbf{V}'$	hypercharge	B (γ)	bino	$\tilde{b}\,(\tilde{\gamma})$	**1**	**1**	0
Matter							
$\mathbf{L}_i$	sleptons	$\tilde{L}_i = (\tilde{\nu}, \tilde{e})_L$	leptons	$L_i = (\nu, e)_L$	**1**	**2**	-1
$\mathbf{E}_i$		$\tilde{E}_i = \tilde{e}^c_L$		$E_i = e^c_L$	**1**	**1**	2
$\mathbf{Q_i}$	squarks	$\tilde{Q}_i = (\tilde{u}, \tilde{d})_L$	quarks	$Q_i = (u, d)_L$	**3**	**2**	1/3
$\mathbf{U}_i$		$\tilde{U}_i = \tilde{u}^c_L$		$U_i = u^c_L$	$\bar{\mathbf{3}}$	**1**	$-4/3$
$\mathbf{D}_i$		$\tilde{D}_i = \tilde{d}^c_L$		$D_i = d^c_L$	$\bar{\mathbf{3}}$	**1**	2/3
Higgs							
$\mathbf{H_1}$	Higgses	$H_{\mathbf{1}}$	higgsinos	$\tilde{H}_{\mathbf{1}}$	**1**	**2**	-1
$\mathbf{H_2}$		$H_{\mathbf{2}}$		$\tilde{H}_{\mathbf{2}}$	**1**	**2**	1

addition resolves the hierarchy problem. Neither the SM nor the MSSM includes the graviton or gravitino; these two make up the theorized pair of particles linked with gravity.

Implications for the Higgs boson are of particular interest. In the SM, the Higgs is one complex particle and the predicted strength of the electroweak force does not agree with experimental evidence. SUSY requires two Higgsinos and a second Higgs; this addition of a second Higgs doublet to the model resolves the discrepancy between the weak scale and the SM's prediction. In total, there are two Higgs and two Higgsinos in the MSSM, as shown in table 1.1.

At the high energies such as the string scale, SUSY is expected to be unbroken and all particles and their superpartners massless. At our low energy scale, the physics we observe is consistent only with broken SUSY. That is, we do not observe particles characteristic of unbroken SUSY. The MSSM resolves the a discrepancy between observations and predictions of the SM, and allows for softly broken SUSY.

Experimentally, the search for SUSY and physical phenomena beyond the SM is led by the ATLAS and CMS groups at CERN. Searches conducted at CERN and and past work at colliders such as Fermilab have constrained the energy scales where superparticles could exist by ruling out areas previously searched. Similarly, constraints have also been placed on the size of the extra compact dimensions required by String Theory; as these extra dimensions have not been detected, they must be smaller than length scales observable by current experimental methods.

The SM has the characteristic gauge symmetry $SU(3)_C \times SU(2)_L \times U(1)_Y$, also written as $SU(3)_C \times [SU(2) \times U(1)]_{EW}$. The electroweak gauge content, $SU(2) \times U(1)$, breaks to $U(1)$ when the Higgs field acquires a vacuum expectation value (VEV) and symmetry is broken. This formulation is useful for research in string phenomenology as the matter sectors of a given model can be constructed from the gauge group content. For SUSY models, this is particularly useful and is discussed in section 2.1.2. However, searching for only models that contain the SM as written above is insufficient, as these groups may be embedded in other models. String models with both embedded and non-embedded SM gauge content are appealing candidates for unification. This discussion is also continued in section 2.1.2.

String Theory: Beyond the MSSM

String theory does not disagree with the SM, but goes a step beyond this in asserting that there are objects smaller than fermions and bosons - tiny, vibrating strings on the order of the Plank length [1]. The vibrational modes of the strings correspond to the particles we observe. With one of the vibrational modes of closed strings being the graviton, gravitation arises naturally out of the theory, which is to say that string theory is a natural candidate for quantum gravity. Barton Zwiebach describes string theory as the quantum mechanics of a relativistic string, but this

seemingly simple starting point leads us to a complete theory of fundamental forces and interactions [1].

Free Fermionic String Approach

In model-building research, each computing method will search a section of the string landscape, and the area searched is dictated by the construction method. Methods differ primarily in how they approach the compactification of the six extra dimensions. This survey of the string landscape utilizes the Free Fermionic (FF) formalism [6-8, 19, 58, 62]. Alternative methods include $\mathcal{Z}_n$-orbifolds, bosonic lattices, Calabi-Yau manifolds, and N = 2 minimal models [10]. This FF method has been utilized by the EUCOS group for past searches with much success [11-47]. With ten dimensions total, four of these are the observable directions and the other six are very small, i.e. on the order of the Planck length. These extra six dimensions are compactified [11-47].

The FF formalism is essentially an encryption method, and describes the behavior of world-sheet fermions. The world sheet is the path a string creates when it moves through space-time. The model-building framework used herein begins with a set of 64-component, modularly invariant basis vectors that describe these world-sheet free fermions.As these fermions are transported around a non-contractible loop in the world-sheet, they pick up a phase. The GSO (Gliozzi, Scherk, and Olive) projection matrix is then applied to eliminate non-physical particle states [55]. Information about the universe is encoded in the compactification process, captured by the phases these fermions pick up as they transform.

In this particular search, there are excitations in the six compact directions. Massive gauge particles are explicitly added in the construction of the basis set of states. At the Planck-scale, this search allows both massive and massless states, contrasting the prior $\mathcal{N} = 4$ search that is discussed for comparison in chapter 2. This

prior search [2] yielding 68 models required masslessness at the Planck-scale, on the order of 10^{19} GeV, and did not allow for excitations in the compact directions. Many gauge models here would not have been allowed in the prior search.

This implementation of the FF approach is a systematic construction method, rather than a random search method. The FF method creates many redundant models, due to the many-to-one mapping of the input to output, increasing computing time. By systematically constructing models, less redundant models are created and surveys with reasonable runtimes are possible [2].Further discussion of how these redundancies arise can be found in [2].

Models generated are output in the form of their gauge groups, which can be used to determine the matter content. In analyzing the models generated, models are discussed in terms of gauge group combinations they contain. Models are considered unique if they gauge groups content does not match entirely that of another model, and redundant models are not retained. The discussion of uniqueness is continued in Chapter 2.

U(1) charges can be calculated easily from analyzing the models generated; for this reason, U(1) charges were not considered in the model-building process for this particular investigation so as not to unnecessarily increase computation time. Abelian charges were constructed and statistically analyzed in prior investigations [53, 55]. The rank of a given model can be used to calculate the number of U(1) charges, n,

$$22 - rank = n$$

Numbers of Supersymmetry $\mathcal{N}$ in Free Fermionic strings

In Supersymmetric Yang Mills Theory (SYM), $\mathcal{N}$ ranges from zero to maximally eight, and refers to the number of spacetime symmetries [10]. For $\mathcal{N} = 4$ with parity symmetry, particles of spins -2, -3/2, -1, -1/2, 0, 1/2, 1, 3/2, and 2 are all in the same

representation. With higher numbers of symmetries, more particles are grouped into the same supersymmetric set, or multiplet. While $\mathcal{N} = 4$ only has one multiplet, $\mathcal{N} = 1$ is the smallest number of symmetries and provides for multiplets of supersymmetric pairs. $\mathcal{N} = 0$ models are not symmetric [2]. Models considered in this analysis are of $\mathcal{N} = 4$ SUSY.

$\mathcal{N} = 4$, models are of only even orders [2]. Order is defined by the integer n, such that a fermionic mode of the string picks up phrases defined by

$$2m/n = phases \text{ for a given order } n, m = 0, ..., n-1$$

when the fermionic mode goes around a non-contractible loop on the world sheet.

CHAPTER TWO

Generalized Gauge Model Investigations

Systematic Free Fermionic Model Building

Layer one Supersymmetric Weakly Coupled Free Fermionic Heterotic String (WCFFHS) models are statistically investigated for even orders through 12 for uniqueness and gauge content. After nearly a decade of FF model-building research by the EUCOS [47], this survey presents a unique addition to the statistical analysis of the string landscape. A systematic search avoids the issues associated with random sampling approaches [47], lessening the difficulty of tackling the roughly 10^{500} possible string models [3-5]. Even order $\mathcal{N} = 4$ layer one Models are built and investigated, through order 12; herein we discuss quantitatively unique models generated for increasing orders. Each unique model is associated with the order at which it first appears. This survey of the string landscape is compared with a prior $\mathcal{N} = 4$ search and trends are discussed along with differences. Models are only counted for the order at which they first occur.

Each model-building survey of the string landscape sheds light on the landscape as a whole. The vast number of models and limits on computation speed of modern computers make building all models impossible, as the runtime would be far too significant. Statistically analyzing models built by systematic construction methods allows for progress in the field despite these challenges. Redundant models are still an issue, but can be addressed.

Results are compared with those of prior searches by the EUCOS group [2, 56]. A focus is given to models containing gauge group factors representing potential GUT groups. This search revealed models with $SU(3) \times SU(2) \times U(1)$ gauge content at the

string scale, which were not observed in prior searches and represent a GUT models. Section 2.3.1 discusses gauge content found in more detail.

As there are so many different string models, it is helpful to consider uniqueness and gauge group content. Generation of redundant models may be, if anything, indicative of the model building approach, but generating a model more than once does not have physical meaning [2]. Unique models are classified by their gauge group content, as mentioned in section 1.6. Subsequent papers will consider specific, promising models from this search, paralleling those produced by previous investigations [50].

Uniqueness of Models

In a similar manner to that of prior work by the group [49], uniqueness of a model is defined by the gauge groups; the number of instances of each gauge group and the gauge groups involved are considered. Having the same gauge groups does not guarantee identical models. Only two models that have identical counts of each specific gauge group involved are considered redundant. All models built in this survey have $\mathcal{N} = 4$ spacetime SUSY, as discussed. Only gauge group content must then be checked in eliminating redundant models. The definition of uniqueness in this and prior surveys used for comparison, from ref. [2], is given as

Definition 2.1 *(Uniqueness) A model is considered* ***unique*** *if no other model has been previously generated with both the same gauge group and number of space-time supersymmetries.*

The matter content of models with identical gauge content is also identical for SUSY models. This cannot be assumed for non-SUSY models, and is thought not to be the case. However, some results have suggested non-SUSY models might behave similarly and further investigations in this area are needed [2]. A deeper investigation

of the matter content of promising models is an area of future work, and can be accomplished using the existing FF framework.

The analysis discussed in section 2 examines the statistical appearance of non-abelian gauge group factors. As U(1) charges can be determined from the output non-abelian content, they were not considered in this search in the interest of economizing on computing time [55]. Unique models are only counted for the order at which they first occur. For example, if a model appears at orders 2, 4, and 10, it is counted only for order 2 in figure 2.2. The vast majority of models from prior orders do indeed also occur at orders 4 through 10.

Subsequent work is needed to investigate relevant statistics for higher orders and layers. Higher layers may be entirely redundant of layer one [2], but more work is needed to investigate this further. Prior searches also indicated that higher orders may fail to produce new, unique models [2]. Initial investigations found that orders after 22 failed to produce unique models not found in lower order searches, for $\mathcal{N} = 4$. This trend was checked and confirmed through order 32 [2]. Future work will extend the analysis described herein through higher orders using the current framework. These results will further investigate if there are orders at which new models are no longer produced. Prior investigations preliminarily suggested no new unique models exist at higher layer, where layers relate to additional bosonic sections [2]. A clearer picture of the string landscape is gained from statistically analyzing unique models.

Analysis of Gauge Group Factors

In searching for string models with the SM, embedded gauge groups must also be considered. A simple case is the SU(5) group, which may contain the embedded SM, $SU(3) \times SU(2) \times U(1)$. Similarly, SO(10) may contain an embedded SU(5). Special unitary (SU) groups over 5 may also contain the embedded SM, and Special Ordinary (SO) groups over 10 may contain groups of SU(5) or higher. E_8 groups may

Table 2.1: Gauge group embedding for the SM.

E_8	
$\Downarrow$	
E_7	
$\Downarrow$	
E_6	
$\Downarrow$	
$SO(10)$	$SO(12+)$
$\Downarrow$	$\Downarrow$
$SU(5)$	$SU(6+)$
$\Downarrow$	$\Downarrow$
$SU(3) \times SU(2) \times U(1)$	

contain embedded E_7 groups, which may contain embedded E_6 groups, which may contain embedded SO(10)'s. Embeddings are shown in table 2.1.

Prior Results

The EUCOS group has conducted many varying searches of the string landscape. Past FF investigations of include an Extension of NAHE models and a NAHE variation [49, 53, 54]. Investigations have also considered specific, promising models [50]. The FF formalism, as discussed in section 1.6, has been utilized for a variety of searches [11-47].

A prior similar systematic investigation considered layer one $\mathcal{N} = 4$ models for even orders 2 through 22. This search was later expanded to order 32. 68 unique SUSY models and 502 non-SUSY models were found through order 22, and no new models were found later for $\mathcal{N} = 4$ through order 32. The trend of higher order models being partly or entirely redundant of those generated at lower orders peaked under order 10. Statistics for these unique SUSY models are of interest in this particular comparison and are given in table 2.3, and are also discussed comparatively in section 2.3.3 [2].

This prior survey of the landscape in ref. [56] found the most SUSY models in a given order at order 6, with 18 unique models. In this prior survey as well as the new survey discussed below, each order after the initial one, order 2, was checked to determine how many models that were found in previous orders were absent from that particular order. The count of models absent from a given order that were found at prior orders also decreased with increasing order.

This investigation did not find any SM, Reduced SM $SU(3)\times SU(2)$ or left-right symmetric $SU(3) \times SU(2) \times SU(2)$ models for $\mathcal{N} = 4$. Pati-Salam $SU(4) \times SU(2) \times SU(2)$ and $SU(5)$ models were observed. An extension of this search [2] found no new SUSY models after order 22, searching through order 32.

New Results

Statistics for Even Orders 2 through 12

This search found a large variety of models. Some gauge content was similar to that found in previous searches, while many models had interesting gauge group combinations not observed in the prior $\mathcal{N} = 4$ investigation [56]. The gauge content found is shown below in tables 2.2 and 2.3, and is statistically compared to the aforementioned prior run in the latter. As each survey is limited by the area of the string landscape being considered, statistics are given as percentages of the number of total unique models in the given survey. Appendix A contains a list of the 512 models found through order 12 by this survey.

The prior $\mathcal{N} = 4$ investigation that yielded 68 unique models found no models containing both $SU(3)$ and $SU(2)$ gauge groups. It also did not find any models with left-right symmetric $SU(3) \times SU(2) \times SU(2)$ or Pati-Salam $SU(4) \times SU(2) \times SU(2)$ groups [2, 56]. This search found multiple instances of each of these. Many models present in the prior search also appeared here. Both searches found many models with

the SM model embedded, SU(5) models, which may represent flipped SU(5) groups, and at least one occurrence of $E_6 \times E_6$.

Also of interest is what percentage of the total each gauge group comprised. There are similarities in the two surveys, though the percentages certainly differ, as shown more precisely in table 2.2. Groups that occurred often in the 68 model search also occurred often here. None of the differences in how often models occurred in the two surveys exceed 20%. As the prior survey requires Planck-scale masslessness and the more recent work does not, the two having reasonably similar gauge content was not an expectation. Notably, a 20% difference is still significant; the two are by no means identical in their gauge content makeup. Figure 2.4 shows this graphically.

Unique Models at Each Order

Figure 1 shows the number of new, unique models at each order, shown in green, along with the number of models missing from the given order. Through order 10, very few models from previous orders were not repeated in subsequent orders. A total of 512 unique models were generated from even orders though 12. Figure 2 shows a statistical comparison of these new unique models as percentages of the total unique model count. Order 12 has the highest count of absent models, varying from the trend in a prior investigation of $\mathcal{N} = 4$ models [2, 56]. The vast majority of models from prior orders do indeed also occur at orders 4 through 10. The drastic increase in the number of absent models in order 12 was unexpected.

That count of absent models in each order (that were in previous orders) is given in red in table 2.2. In green, models that appear for the first time are also considered. Unique models are counted in green for the order in which they first appear. The peak of new models per order occurred at order 10, with 151 new unique models generated. This peak occurred at order 6 for the prior search of 68 models; 26% unique models

Table 2.2: Comparison of gauge content in the 512 models from this search to a prior $\mathcal{N} = 4$ survey that explicitly excluded string-scale massive states and yielded 68 models are given as percentages of the total of unique models for each survey.

Gauge Group	$n = 512$	$n = 68$	Difference
SU(2)	55.27	44.12	11.15
SU(3)	14.06	4.41	9.65
SU(4)	34.77	16.18	18.59
(Flipped) SU(5)	15.82	5.88	9.94
SU(5+)	74.80	57.35	17.45
SO(8)	19.92	16.18	3.74
SO(10)	14.06	13.24	0.82
SO(10+)	44.14	57.36	-13.22
E_n	14.84	25.53	-10.69
$E_6 \times E_6$	0.98	2.94	-1.96

first occurred at this order[2, 56] . For this 512 model survey, 29% of the 512 unique models first occurred at this peak order.

Comparison to Prior Results/Work

Expanding on prior work, 512 unique models were found for layer one through order 12. Future work will soon add to these results to including all unique models through order 22. All models described are $\mathcal{N} = 4$ maximally SUSY. As prior orders are expected to be in part or wholly redundant of lower orders, results through order 12 are sufficient to gain a better understanding of the string landscape and are statistically significant.

Results through order 10 support the findings of the earlier 68 model survey in that very absent models occur, where an absent model is defined as one that occurred at a lower order but is not found in a given order. Order 12 of the 512 model search has a drastic increase in absent models. However, orders 14 and 16, which are in progress, will help to consider the characteristics of this set more fully, and the trend may still hold. The generation of new models follows a similar curve to that of the prior survey,

Table 2.3: Models containing specific gauge groups of interest are given as a total count and as percentages of the total count of unique models.

Gauge Content	Percent	Number of Models
$SU(3) \times SU(2) \times$ U(1)	7.6%	39
SM or Embedded SM	99.2%	508
Pati-Salam	13.1%	67
Left-Right Symmetric	$< 1\%$	24
$SU(3) \times SU(3) \times SU(3)$	$< 1\%$	1
(Flipped) $SU(5)$	15.8%	81
$E_6 \times E_6$	1.0%	5

peaking slightly later, at order 10; the peak of new unique model generation for the 68 model survey was at order 6.

Also of interest is the gauge content, particularly for GUT groups. This investigation found many types of models not present in the prior search. Most notably, a total of 39 unique models, 7.6% of the total model count, contain both $SU(2)$ and $SU(3)$ gauge groups; these were not observed to coexist in any models from the prior search. Table 2.2 gives a statistical analysis of the groups found, and these are compared to the results of the prior search. The overwhelming majority of models, 508 of the total 512 contained the SM. These models make up 99% of the landscape surveyed in this work. Section 2.1.2 discusses embedded groups. The vast majority of models containing the SM did contain it as an embedding in the 512 model survey. However, in the 68 model survey, it was only ever observed as an embedded group.

Future Work

Promising Models

More work is needed to investigate further the promising models from this run. Of interest are GUT groups, and many were observed in this 512 survey that were not in the prior. This survey included models containing both $SU(3)$ and $SU(2)$

gauge groups; these were absent from the prior $\mathcal{N} = 4$ survey [2, 56]. The prior search, differing from this one, also did not find any models with left-right symmetric $SU(3) \times SU(2) \times SU(2)$ or Pati-Salam $SU(4) \times SU(2) \times SU(2)$.

In particular, I would like to study the 39 models that contain the $SU(3) \times SU(2)$ gauge content without considering embedded gauge groups. As mentioned in previous sections, this combination represents the SM when accompanied by a $U(1)$ charge. Some models with this gauge content may be more interesting that others, depending on the additional gauge content they contain.

Increasing Orders and Layers

The existing FF framework allows for the trends discussed herein to be checked at higher orders. Modifying the framework for order 14 is already in progress. Unique models at higher orders after a certain point are expected to be entirely redundant of lower orders, as is the trend particularly for orders 2 through 10 here. This trend was shown to be true in prior searches by the EUCOS group, as discussed at length in earlier sections

Beyond the Standard Model

This survey of the string landscape is of SUSY models, but the analysis focuses primarily on those that may contain the Standard Model. Statistics for other gauge groups are presented, and the addition to the framework utilized for this analysis could be utilized to investigate interesting gauge group content not discussed herein. Simple modifications to this program would allow for statistics on any gauge group content of particular interest for the existing data as well as future orders.

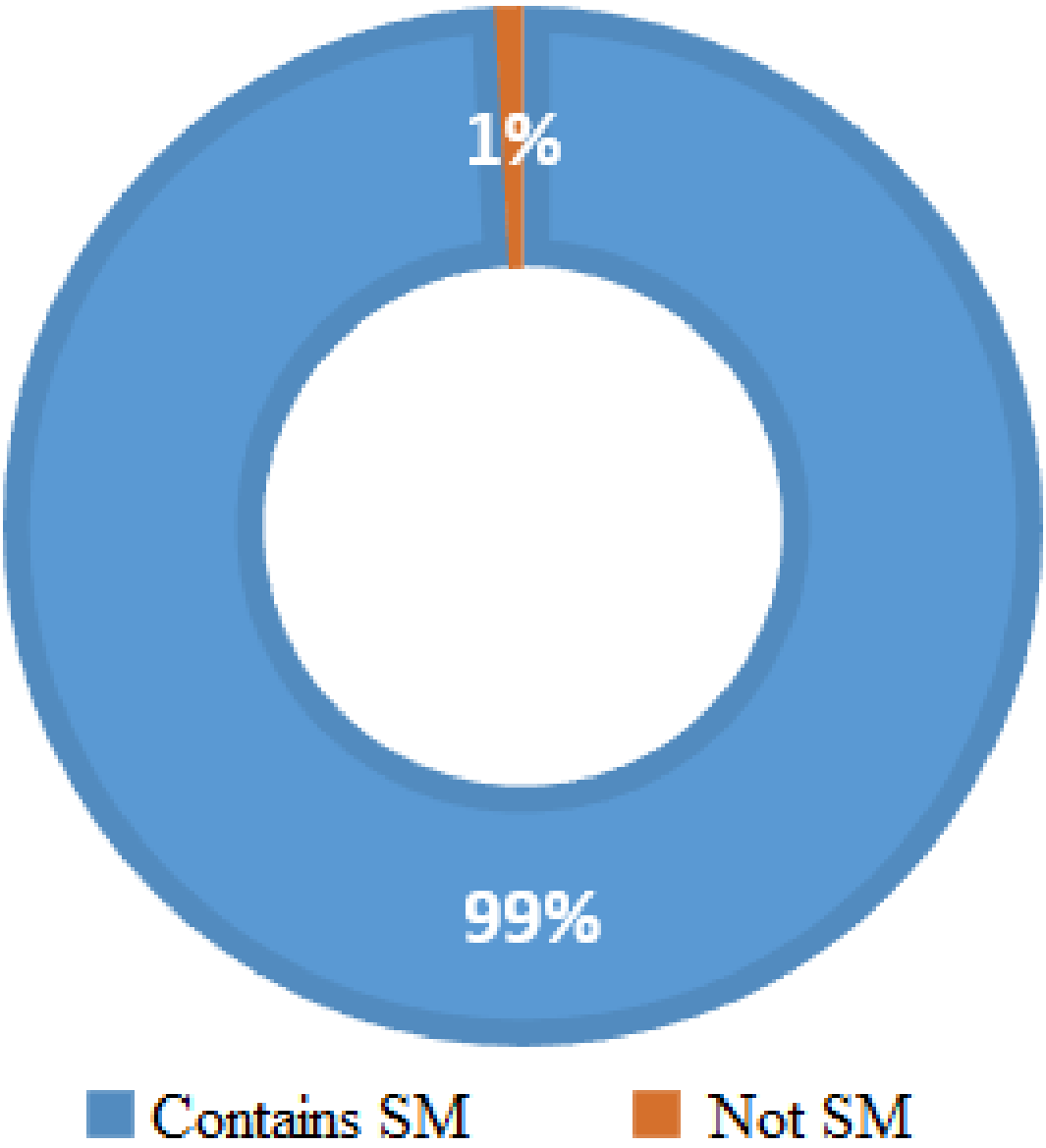

Figure 2.1: Unique new models containing the standard model are shown in blue, including those with gauge content containing the embedded standard model. Those without are shown in orange, and make up a small fraction of the survey.

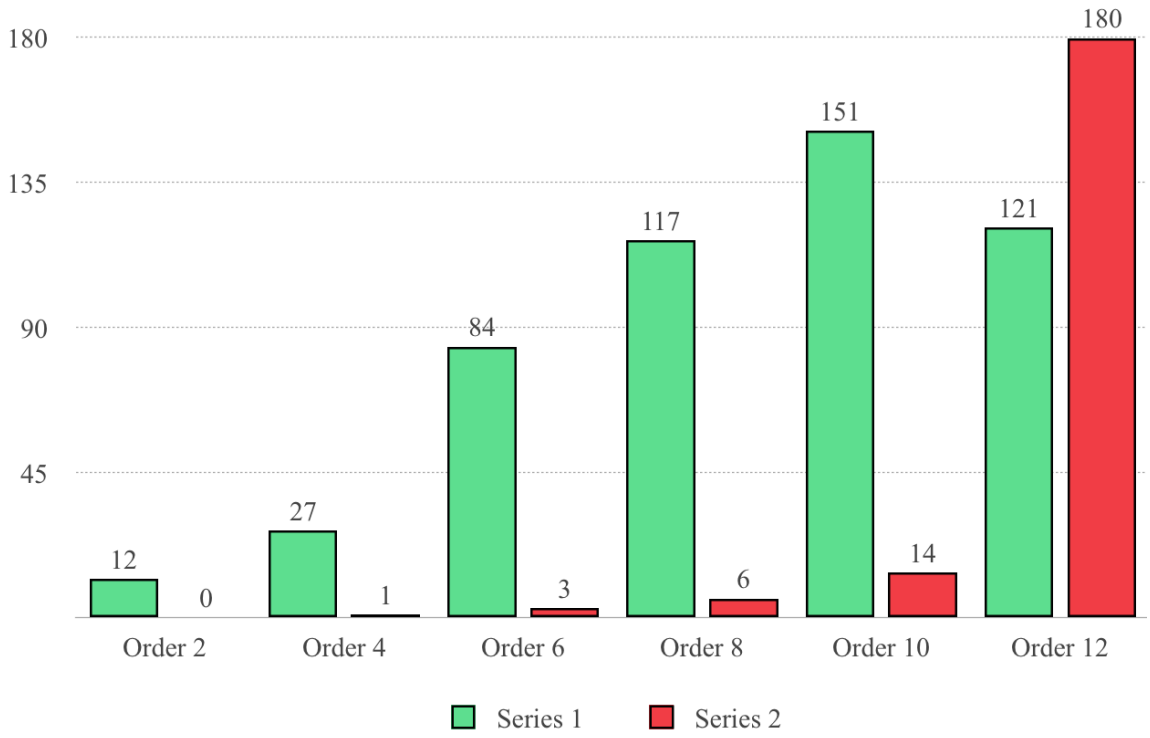

Figure 2.2: Unique new models are shown to the left, in green. The red bars are the count of models that were present in previous orders and are absent from the given order.

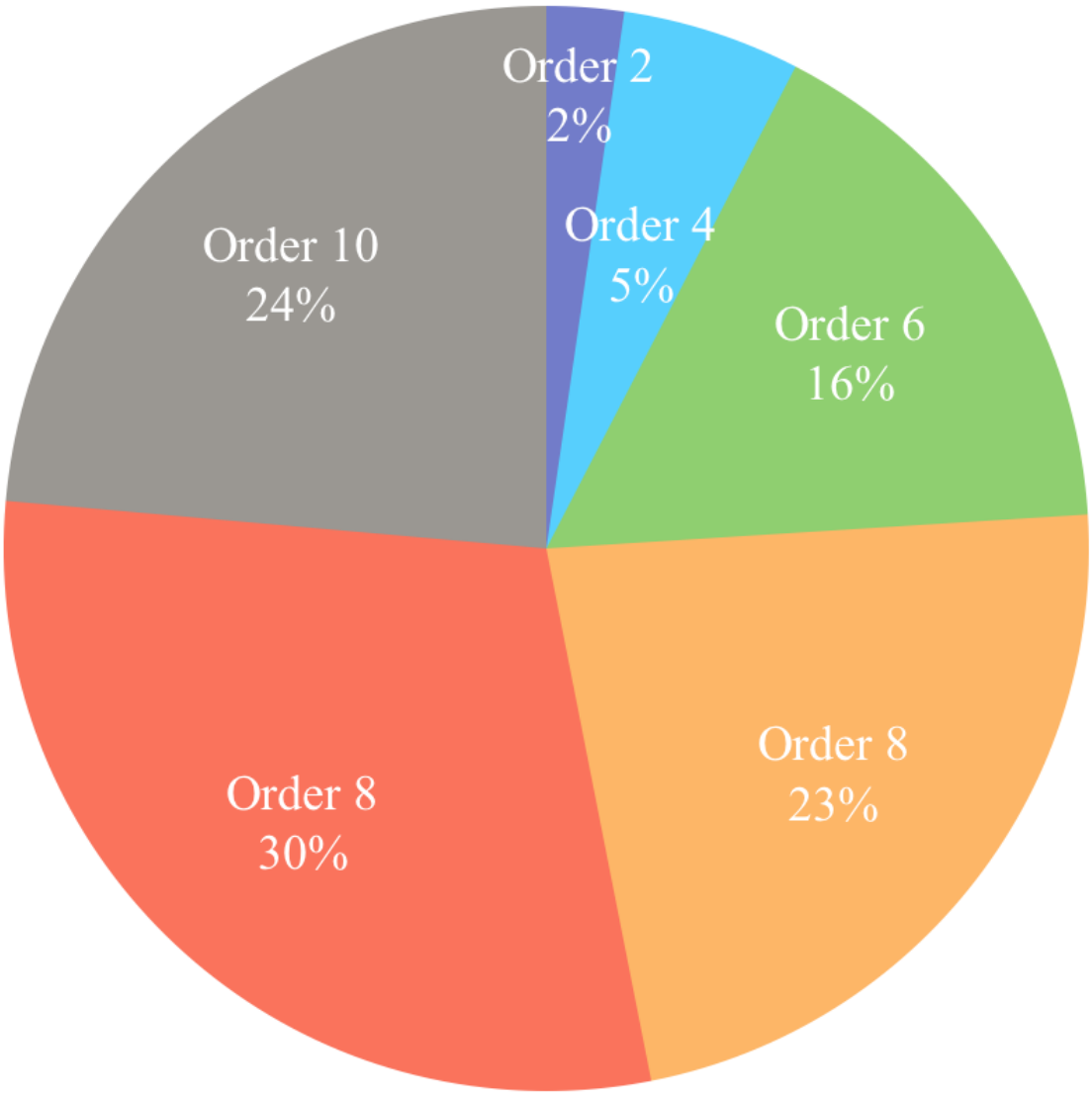

Figure 2.3: Unique models and the order at which they first appear are shown as percentages of the 512 unique total models through order 12.

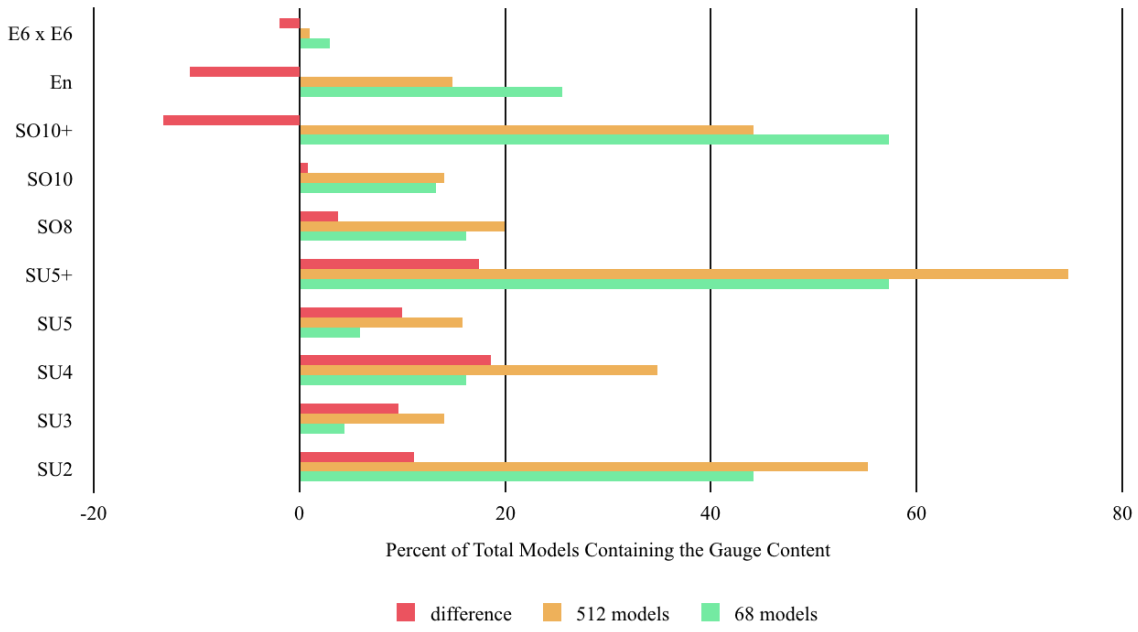

Figure 2.4: Comparison of gauge content in the 512 models from this search to a prior $\mathcal{N} = 4$ survey that explicitly excluded string-scale massive states and yielded 68 models are given as percentages of the total of unique models for each survey.

CHAPTER THREE

Mandelbrot Encryption Project

Brief Overview of Encryption

Good encryption algorithms make use of mathematics to encode the given information such that the capability of extracting said information, or decrypting, is limited severely unless one possesses certain knowledge. One of the most widely used encryption algorithms is RSA, named for its creators Ron Rivest, Adi Shamir, and Leonard Adleman [65]. RSA mathematically utilizes the difficulty of factoring two large enough prime numbers, and utilizes two keys, one public and one private. The public key is used to decrypt the message, but the private key, which is known by the intended recipient, is necessary to sufficiently decrease decryption computation time to a reasonable range (assuming the public key is chosen to be a sufficiently large number). Advantages of this method include short runtimes for encryption and decryption, ease of use, popularity, and good security. RSA encryption and decryption does not require hardware beyond that of typical personal computers, assuming reasonably small numbers are chosen for the keys. Unfortunately, due to the popularity of this method, eavesdroppers tend to expect it and methods exist for breaking RSA encryption. Another drawback of the RSA algorithm include vulnerability to fast enough computers for simple enough choices of prime numbers.

A relatively new and novel encryption scheme is a Mandelbrot summation algorithm, described herein[1] It shares traits with RSA encryption, such as ease of use, short encryption and decryption runtimes, functionality on a typical personal computer, and good security; it also has advantages over RSA. Mandelbrot encryption is

[1] Another approach to utilizing Mandelbrot summations for an encryption scheme is described in ref. [66]. The implementation described herein differs in its use of RGB values for image encryption.

relatively new and far less frequently used. Further, the particular Mandelbrot Summation encryption scheme described herein is unique to existing methods. Potential eavesdroppers are drastically less likely to expect it, and may experience a significant learning curve in decrypting sent messages. In the case of Mandelbrot summation encryption, the knowledge necessary for decryption is the choice of how the red (R), green (G), and blue (B) color values of each pixel are processed, as well as how the two intermediate images that result from the encrypted initial image are related. One of these sets of color values must solved for by the decryption program using brute force, and knowledge of this choice reduces decryption runtime to a reasonable range.

The process is discusses in terms of the common convention of Alice, who is encrypting and sending a message, Eve, and Bob. Bob is the intended recipient of the message. He has preexisting knowledge of the key from Alice. Bob's decryption time is the minimum, because he has all the required information. Note that this is for a simple case where each participant's computer is identical. Eve, being the eavesdropper, has no knowledge of the private key. The goal is for Eve's time to be sufficiently large, as she must try more possibilities to make up for lacking the information possessed by Alice and Bob, and for Bob's decryption runtime to be reasonable. This implementation is useful as intended if these requirements are met, but what may be reasonable for Bob will vary with each use. Further discussion of the implications of runtimes for Eve and Bob are discussed in section 3.7. Alice's portion of the program accounts for less than one percent of the total runtime. Due to this negligible computation time contribution, the encryption runtime is discussed in less detail.

Section 3.2 begins with a review of the underlying mathematics, Mandelbrot summations. 3.3 discusses strengths of this algorithm for utilization as an encryption scheme. Section 3.4 introduces this particular implementation. Section 3.4 described the decryption process. Section 3.5 discusses the encryption process, and decryption is

discussed in 3.6. Example runtimes are given in 3.7. Section 3.8 presents modifications to increase computation time for the decryption process and discusses advantages to implementing these changes. A couple key weaknesses are covered in 3.9, followed by a proposed solution. In Section 3.11, further applications are briefly discussed.

Review of Mandelbrot Sets

A good encryption scheme makes use of an algorithm that does not map 1:1, but has many initial combinations that might lead to the decrypted output. A Mandelbrot summation approach was chosen, as shown below,

$$z_i = z_{i-1}^2 + C, \text{ where } 0 \leq C < 1 \text{ to ensure convergence}$$

The first few iterations are then

$$z_0 = C$$

$$z_1 = C^2 + C$$

$$z_2 = (C^2 + C)^2 + C$$

For this implementation, red (R), green (G), and blue (B) values are taken into account. This is accomplished by defining C as

$$C = \alpha + i\beta$$

This allows R, G, and B to be defined as shown below. Matching R, G, and B to the right-hand sides of the equations below are purely arbitrary choices.

$$R = \alpha^2 - \beta^2 = C^2 - G$$

$$G = 2i\alpha\beta = C^2 - R$$

$$B = \alpha^2 + \beta^2$$

The resulting equations are therefore chosen as

$$R_i = R_{i-1}^2 - G_{i-1}^2 + R_0$$

$$G_i = 2R_{i-1} \times G_{i-1} + G_0$$

$$B_i = R_{i-1}^2 + G_{i-1}^2 + B_0$$

Strengths of the Mandelbrot Algorithm

A Mandelbrot summation algorithm was chosen for a few primary reasons. The runtimes for Bob are reasonable but not so much so as to be reasonable for Eve, as discussed at length in section 3.7. This particular implementation does not exist, introducing a learning curve for eavesdropping attempts. Further, the adaptability of this algorithm, discussed in more detail in section 3.10, allows users to scale the complexity when advantageous for a given application; this is particularly useful when sending images with low pixel counts or if increasing the runtime of the decryption process is desired in order to deter eavesdroppers with more powerful computers than the intended recipient. Otherwise, as computers advance, runtimes for a typical computer would decrease, resulting in decryption times becoming too low for use as an effective encryption scheme.

Implementation of the Mandelbrot Algorithm Encryption Scheme

A proposed encryption method, alternative to standard RSA encryption, employs a Mandelbrot summation algorithm and allows for images to be encrypted and decrypted. The program processes an image by converting each pixel to its integer RGB values and encrypting these using three coupled Mandelbrot summations. The output is a set of two images corresponding to the fractional and integer parts of the first image. We also discuss the subsequent decryption process of these two resulting images; the process takes roughly 15 minutes for a 300×300 pixel image on an average modern desktop computer. The encryption algorithm was tested as described and reasonable runtimes were confirmed for typical use, with knowledge of the key utilized for the decryption. For an outside interceptor, Eve, the decryption time is sufficiently long. Further, this algorithm gives the user the ability to increase the complexity of the process, increasing the runtime for Bob less so than for Eve. Advantages to this

program are its adaptability, reasonable runtime on a typical personal computer and that it is new and unique, inherently enhancing its security.

The Mandelbrot summation encryption method described herein may be used for secure transmission of images and presents an alternative to RSA encryption, where the user chooses the key using two prime numbers [65]. An eavesdropper would lack knowledge of the key, and would require significantly more time for any attempts to decrypt the sent image if intercepted. The key is what makes this encryption scheme unique, and is knowledge of how the color values of the image are summed.

The program encrypts an image by first converting it to its RGB values, which are then processed through the summation described in section 3.2. It returns two images which are components of the encrypted first image. These are sent to Bob, who has the key that specifies the order in which the R values, G values, and B values were summed. Eve, attempting to reconstruct the original image without this key, will require exponentially more time to decode the image as she tries all possible combinations. Bob, however, uses the key to direct the program and is able to reconstruct the original image Alice encrypted in a reasonable time frame.

Encryption Process

Our program takes as the input an image. It converts each pixel to its integer RGB values, with these three respective values ranging from 0 to 255. It then encrypts the RGB values using three coupled Mandelbrot summations. This is accomplished by allowing the function to run until the summations have converged to at least five decimal places. Each of the three summation values, which at this point range from 0 to 1, is then multiplied by 255 before being broken into integer and fractional parts. Two new pixels, one of the integer part and one of the fractional part multiplied by 255, will then be added to two separate encrypted images as the program loops

through each pixel in the original image. Finally, the output is the set of these two encrypted images resulting from the encryption of the initial image.

Decryption Process

The program's decryption function uses information from the encryption function to decrypt the images generated using the process above. It tries systematically tries combinations of values in an attempt to reproduce sums from the received images. Two encrypted images are input, similarly to the aforementioned process, with one image corresponding to the integer parts and the second to the fractional parts of the RGB values of the encrypted pixels. The encrypted RGB values of each pixel must then be fed into the function decrypt. The program will convert these into a key, which will be slightly less than the matching summation values from the original picture due to round off error. This round off error will, at most, result in some of the individual RGB values being reduced by one, which is inconsequential as this change in the image is unlikely to be noticeable significance.

The function utilizes a brute force algorithm to then try each possible R and G combination whose encrypted value matches the key pixel R and G values. Then, knowing the first two color values of the original pixel color, it searches through possible B values with those R and G values whose encrypted summation value matches that of the key pixel. From knowing these R and G values, the B value can be found in a very reasonable amount of time through a brute force approach. The maximum number of loops required, M, to find the B values is given by

$$M = n^2 + n \tag{3.1}$$

where n is the number of possible integer values for a color value, which is 256 (as it ranges 0 to 255). This yields a maximum of 65,792 loops for each pixel, taking a fraction of a second per pixel on most computers. In this way, the program processes the two input images pixel by pixel, yielding the decrypted image as the output.

Table 3.1: Encryption and decryption times for two 400 × 400 pixel images prior to enabling optimization futures of the compiler.

Image	Encryption Time	Decryption Time
Hat	23s	57053s
Iceland	16s	36809s

Runtimes

One key test of the encryption scheme was the time required for each step of the process. This section expands upon the factors that influence runtime, focusing on picture size, complexity, and the computer running the program. Timers were implemented and tracked time to encrypt for Alice, decrypt for Eve, and decrypt for Bob. This process assumes the typical situation for which the method is designed - Alice and Bob have discussed the key in advance and Eve has no knowledge of this at the onset. Though the program was uploaded to Baylor University's CRAY supercomputing cluster, KODIAK, as a test, here the focus is on runtime on an average computer, as this constitutes typical use. As the program is not parallelized, it cannot make use of multiple core. This was tested on a typical modern computer. Information is also included below for runtimes without using the optimization tools in the GNU C++ compiler. This data was collected first, and sheds light on how the runtimes may vary due to characteristics of the given image.

If the overall runtime was too high, this program would be referred to as a shredder. This is not its intended use. For example, for a large number of uses, one week would be too long to wait for the decryption of an image. For other uses, this limit might be much shorter for the program to be useful. Specifically, here, the runtime being investigated is that of the decryption process. The encryption process and formatting conversions from spreadsheet to image account for much less than one percent of the total runtime. Had the runtime been very small for both Eve and Bob, such as a matter of seconds for example, this would have ruled out the program

as a good encryption scheme altogether. If Bob's time is very small, Eve's is more likely to be within a reasonable range as well. Specifics will depend on the size of the image, colors involved, the computers used, etc. This would likely be too little of a delay for Eve to be useful, because decryption times for both parties are too reasonable. Alice does not require much computing time, as the image conversion and encryption processes are very straightforward. Alice's runtimes are very reasonable, as shown in the table. They are expected to remain reasonable even for very large images. Fortunately, tests of the program showed times to be within a reasonable range for Bob.

Eve might face an additional delay in converting the encrypted output to images, as she does not know the formatting of the programs Bob and Alice possess. However, this is a small fraction of the overall process, and trying a variation of configurations may add only a negligible amount to her total runtime, assuming she starts with programs for the various possibilities, such as starting with the first pixel in the left-hand corner of the image.

However, section 3.10 provides suggestions for changes to the algorithm if altered runtime is desired. The ideal situation is for Bob's decryption time to be reasonable, i.e. less than a day, but Eve's to be significant, i.e. weeks. Eve, as the eavesdropper, will struggle without the key, increasing her decryption time.

Initial runtimes for the algorithm prior to enabling optimization features of the compiler are given in table 3.2. Two pictures of the same size, 400 $\times$ 400 pixels, were encrypted and decrypted. RGB-spreadsheet conversion runtimes are not shown as they did not exceed 30 seconds and are negligible in the context of the total runtime. One picture, referred to as "hat", had a large amount of whitespace as the background and was primarily reds and pinks; the picture is of a dark pink ball-cap with a small design and very little color variety. The second picture is of a landscape in Iceland; the colors vary much more significantly, and there are no large areas of one solid

color, contrasting the first picture. An oversimplification might lead one to assume the first picture would decrypt more quickly. However, as shown, the second picture had a drastically shorter decryption runtime. The decryption function counts up, first trying each combinations of integer values for two of the colors. A different colored hat or a different colored background might drastically change these results. The program tracks time spent encrypting and decrypting and outputs this value in seconds. The hat takes about 15.8 hours to decrypt, while the landscape picture takes only 10.2. Table 3.3 shows the times with the GNU C++ complier optimization level 03 enabled.

Table 3.2: Encryption and decryption times for two 400 × 400 pixel images prior to enabling optimization futures of the compiler.

Image	Encryption Time	Decryption Time
Hat	23s	57053s
Iceland	16s	36809s

Table 3.3: Encryption and decryption times for two 400 × 400 pixel images when run utilizing optimization futures of the compiler.

Image size	Improved Encryption Time	Improved Decryption Time
Hat	8s	3412s
Iceland	6s	2232s

Table 3.4 shows the RGB to spreadsheet conversion times in addition to the data given in the prior table. An image of 323 × 323 pixels was used for table 3.4. Times used for the spreadsheet to RGB conversion process are only an estimate and are taken to be equal to the RGB to spreadsheet times for the image; this accounts for a very small fraction of the process's total runtime. This table is of the times with the C++ complier's optimization feature enabled.

As shown in the tables above, runtime is closely related to the size of the image and the computer running the program. Additional random images of various sizes

Table 3.4: Spreadsheet conversion, encryption, and decryption times for a 323 $\times$ 323 image rounded to the closest second.

Computer	Image to RGB	Encryption	Decryption	RGB to Image
Laptop	0s	3	1450	0

were run and runtimes are listed in table 3.5. High R, G, and B values may increase the decryption time, depending on the order in which these values are solved. What times are considered reasonable will vary with how the program is being used. If sending a very large image, one might consider either running the decryption process on a more advanced computer or breaking the image into smaller pieces and running each on a separate computer. Related future work includes investigating possible ways of further optimizing the decryption process by improving the program's efficiency. Parallelization of this algorithm would be advantageous for images with a very large pixel count if the decryption is run on a computing cluster or multi-core CPU.

Runtime could be decreased by taking into account which R, G, or B channel has a low, or high, value. For instance, if images sent were primarily green landscapes, this information could be used by Alice and Bob to strategically select the order in which each value is found. In this particular example, Bob might first solve for the R and B values, as they will likely be lower than the G values. In the case of the hat, the R values were much higher than the B and G values. The large amount of white space (255, 255, 255) also contributed significantly to the runtime. However, one must be careful as this choice is part of the key and unpredictability ensures that Eve's average time is much less than Bob's.

Weaknesses of the Mandelbrot Algorithm

The primary weakness of this encryption scheme is that one or both of the encrypted images tend to share characteristics of the original image. Various images

Table 3.5: Spreadsheet conversion, encryption, and decryption times for various images, rounded to the closest second.

Image size in pixels	Image to RGB	Encryption	Decryption	RGB to Image
1920×1080	0s	13s	27943s	1s
100×133	0s	4s	276s	0s
375×300	0s	6s	1507s	0s
500×480	0s	3s	2840s	0s
512×512	0s	3s	3926s	0s
720×576	0s	4s	4237s	0s

were tested, and information such as that the pictures were of people or mountains for example could be determined from the encrypted fractional and integer images. However, details like specific facial features or any information about the colors of the original images were difficult to determined. To say that the colors of the input image are merely swapped would be an oversimplification of the effect, but does capture the essence of the problem.

As is true of many encryption schemes currently in use, the Mandelbrot encryption algorithm is vulnerable to quantum computers, as well as computers with a significant amount of computing performance power throughput. Invulnerability to computers on the level of quantum computers or supercomputers is out of the scope of this project. The Mandelbrot encryption algorithm may be a good encryption scheme when used as intended, when Bob's computer is similar to or faster than an eavesdropper's. Eve could accomplish a similar or faster decryption time than Bob's if she runs her process on a computer drastically faster than Bob's. Alice's encryption process uses very little computing power, and is not relevant here.

Double-Encryption as a Possible Solution

The spreadsheets of RGB values resulting from the encryption of the image were translated to images. Unfortunately, these initial tests of roughly ten images found that encrypted pictures tested still resembled the initial images to varying degrees.

The usefulness of this algorithm is highly dependent on the specific application, but this does lessen the encryption scheme's appeal. However, to make use of the encrypted pictures if they are sent as spreadsheets, the eavesdropper must have knowledge of the dimensions of the original picture. Determining the two images (which are the encrypted version of the original image) from the spreadsheet of values without this knowledge would be difficult and tedious.

A simple approach to strengthening the encryption scheme proposed is to encrypt the image twice. Work to determine the effectiveness of this method is in progress, but preliminary tests have shown that encrypting the image a second time drastically decreases the resemblance to the original image. A second encryption results in four total images resulting from the encryption of one initial image. The first encryption results in the fractional and integer parts of the initial image. Each of these is again encrypted by simply being run through the program a second time, such that, for example, the fractional part image is broken into a fractional image and an integer image. The recipient of these images must know which ones are paired in order to reconstruct the original image.

The downside of double-encryption here is that the final decrypted image has noticeable distortions. Encrypting a second time amplifies the discoloration due to round-off, as discussed in earlier sections, noticeably. In the single-encryption process, this means that each pixel's R, G, and B values may be maximally increased by 1, which makes very little difference in the final images. Though some of the the final images (after the decryption process) and original images tested were distinguishable from one another, the differences were small. For most applications, these minor discolorations of a few pixels are expected to be acceptable. After double-encryption and processing the images twice in the decryption phase to reverse this, the distortions are significant enough that additional modifications are being considered. Modifying the program to increase the precision of the summations should result in an increased

runtime, which is acceptable. This approach is being explored as a possible way to decrease distortions and greatly improve the resulting decrypted images.

An alternative to double-encryption also being explored focuses on modifying or replacing the Mandelbrot summation algorithm. Instead of using Mandelbrot summations for encryption and decryption, another mathematical method may be used. There may be similar summation methods that fit the same constraints as the Mandelbrot summation described herein that could be utilized with little change to the overall functionality of the program.

Variations and Choices

The initial approach involved running multiple programs, all now combined in C++, to encrypt and decrypt this image. One set of programs broke each pixel into its RGB values and encoding these in an excel spreadsheet. The second program would run the Mandelbrot encryption algorithm after feeding in this excel sheet as the "image"; this outputs the encrypted image. The third program, again in C++, would take this image along with the key as inputs and decrypt, yielding an excel file with the RGB values of the original image that was fed into the second program. The final program would then take this output and process it, outputting an image. It is irrelevant for the encryption itself how the image files are translated to RGB arrays. This would combine the four programs into two - one for encryption and one for decryption; alternately, one program could be used with an option to do either.

Another option would be further complicating the process, making it more difficult for Eve, the eavesdropper, to figure out the image sent. This could be accomplished by, rather than having two agreed-upon values in the key and solving for the last, having an agreed-upon sequence of which values are solved for and which are given in the code. This might mean solving for the R values, then solving for the G values, etc., for example. This would have no effect on the decryption time for

Bob, but would make the process drastically more complex for Eve. Note that the agreed-upon switch from solving for R for example to solving for B would add further complexity to the encryption scheme. Bob's time would at maximum double, going from from time t to time t' where time t' is given as the total time to decrypt both parts. Each part, being smaller than the whole picture, would take at maximum the same amount of time to decrypt as the full picture. The total time is then given by

$$t' = m * t$$

where t' is the new time with multiple parts and m is the number of parts; $m = 2$ in the given example. Eventually, Eve might figure out when the switches occur, making this not permanently unpredictable. Bob and Alice could discuss this sequence, specifically setting and changing it, and the points at which it might change, as an additional aspect when they would usually discuss the key.

Additionally, modifying a few lines of code would allow the encryption program to store the integer and fractional RGB values in another order. Modification of the format of the stored RGB values is easily accomplished, and creates one more obstacle for Eve. The format used here was extremely straightforward, but Alice and Bob might decide that the integer and fractional spots switch places every ten rows, for example. They might complicate this additionally be switching them on every prime row or switching only blue values. This is similar to the above proposed modification in that it is something Alice and Bob could discuss prior to sending images, and would add another obstacle for Eve, slowing her further. These sequences could also change every so many lines to add additional security. As is, the code stores the values as

$$(R_{integer}, G_{integer}, B_{integer}, R_{fractional}, G_{fractional}, B_{fractional})$$

The simplest example of modifying this aspect of the program would be to switch the order to output

$$(R_{fractional}, G_{fractional}, B_{fractional}, R_{integer}, G_{integer}, B_{integer})$$

A key advantage of this algorithm is its inherent flexibility; making choices such as those described above allows the user to customize and add a layer of security, with minimal effort and at times an additional piece of information shared beforehand.

Further Applications

This program could be modified as an application for encrypted image sending between cell phones to within an order of magnitude. Many widely used image sending applications (apps) popularized as secure image sending tools do not currently offer encrypted image sending, with some allowing for owners of the app to store sent images. A cursory search yields similar apps but only one that promises image sending without the user agreeing to permissions that allow the company to access the file. While phone applications are well outside of the intended use of this program, this is a promising area of future work. As this program has a reasonable runtime on computers that are comparable to modern cell phones, runtimes are expected to be roughly similar.

Beyond functioning as an secure image sending tool, this program could be modified and made useful as a way to save information, to a computer for example, where one hard drive would only have the encrypted information and another would have the key; the information would only be accessible if the user had both. These could, for example, be stored in different locations, adding security and insuring certain files could not be read without both devices (the information and the key) together at the time of access. The algorithm described herein would be applicable for data stored as images.

Another feature could be added for this particular application in order to track when the data is accessed - the key could be set to change the data file during each interaction, where an interaction is defined as the two being used in conjunction and the data being accessed. A simple case of this might simply be a count that tracks the

interactions (accesses), and the key file would increase the count by one each time. By writing the key such that it cannot be altered (this would more so be a choice of the device the key is stored on, such as when you physically switch a floppy drive such that it cannot be written to), any time the data is ever accessed, the count would make note of this. This could be expanded to a slightly more complex case where the time of access is recorded in addition to increasing the count.

Future work could focus on this application in possible comparison to any alternatives, if these exist. Nonetheless, this program presents a new alternative to current encryption methods, the usefulness of which is not unlike a new antibiotic for penicillin-resistant illness; Eve, the illness here, may have experience with existing encryption methods (the penicillin here). However, she has never encountered the Mandelbrot summation method, and thus is not adapted to overcoming it. As the antibiotic might annihilate the illness, the Mandelbrot algorithm holds up to Eve's decryption tactics and she is unable to achieve her goal of accessing the image in a reasonable amount of time.

APPENDIX

APPENDIX A

Gauge Groups for Models through Order 12

Gauge Group	Percentage of Unique Models
$SU(2)$	55.27
$SU(3)$	14.06
$SU(4)$	34.77
$SU(5)$	15.82
$SU(6)$	18.75
$SU(7)$	11.72
$SU(8)$	19.92
$SU(9)$	8.40
$SU(10)$	12.11
$SU(11)$	3.91
$SU(12)$	8.20
$SU(13)$	1.76
$SU(14)$	3.123
$SO(8)$	20.51
$SO(10)$	14.06
$SO(12)$	13.09
$SO(14)$	6.84
$SO(16)$	7.81
$SO(18)$	2.54
$SO(20)$	3.71
$E_n(n = 6, 7, or 8)$	14.84

BIBLIOGRAPHY

1. Zwiebach, Barton. A First Course in String Theory. Cambridge University Press, 2004. Print.

2. D. G. Moore, The landscape of free fermionic gauge models. doi:10.1007/978-3-319-24618-5

3. R. Bousso, J. Polchinski, *Quantization of four-form fluxes and dynamical neutralization of the cosmological constant*. JHEP06 (2000), arXiv:hep-th/0004134v3.

4. S. K. Ashok, M. R. Douglas, *Counting flux vacua*. JHEP 01 (2004), arXiv:hep-th/0307049v3.

5. M. R. Douglas, *The statistics of string/m theory vacua*. JHEP 05 (2003), arXiv:hep-th/0303194v4

6. I. Antoniadis, C. P. Bachas and C. Kounnas, Nucl. Phys. B **289**, 87 (1987). doi:10.1016/0550-3213(87)90372-5

7. I. Antoniadis and C. Bachas, Nucl. Phys. B **298**, 86 (1988). doi:10.1016/0550-3213(88)90355-0

8. H. Kawai, D. C. Lewellen and S. H. H. Tye, Nucl. Phys. B **288**, 1 (1987). doi:10.1016/0550-3213(87)90208-2

9. J. D. Lykken, hep-th/9612114.

10. G. B. Cleaver, Nucl. Phys. B **456**, 219 (1995) doi:10.1016/0550-3213(95)00481-0 [hep-th/9505080].

11. G. B. Cleaver, A. E. Faraggi, D. V. Nanopoulos and J. W. Walker, Nucl. Phys. B **593**, 471 (2001) doi:10.1016/S0550-3213(00)00543-5 [hep-ph/9910230].

12. J. L. Lopez, D. V. Nanopoulos and K. j. Yuan, Nucl. Phys. B **399**, 654 (1993) doi:10.1016/0550-3213(93)90513-O [hep-th/9203025].

13. A. E. Faraggi, D. V. Nanopoulos and K. j. Yuan, Nucl. Phys. B **335**, 347 (1990). doi:10.1016/0550-3213(90)90498-3

14. A. E. Faraggi, Nucl. Phys. B **387**, 239 (1992) doi:10.1016/05503213(92)90160-D [hep-th/9208024].

15. I. Antoniadis, G. K. Leontaris and J. Rizos, Phys. Lett. B **245**, 161 (1990). doi:10.1016/0370-2693(90)90127-R

16. G. K. Leontaris and J. Rizos, Nucl. Phys. B **554**, 3 (1999) doi:10.1016/S0550-3213(99)00303-X [hep-th/9901098].

17. A. E. Faraggi, Phys. Lett. B **278**, 131 (1992). doi:10.1016/0370-2693(92)90723-H

18. A. E. Faraggi, Nucl. Phys. B **403**, 101 (1993) doi:10.1016/0550-3213(93)90030-S [hep-th/9208023].

19. A. E. Faraggi, Nucl. Phys. B **407**, 57 (1993) doi:10.1016/0550-3213(93)90273-R [hep-ph/9210256].

20. A. E. Faraggi, Phys. Lett. B **274**, 47 (1992). doi:10.1016/0370-2693(92)90302-K

21. A. E. Faraggi, Phys. Rev. D **47**, 5021 (1993). doi:10.1103/PhysRevD.47.5021

22. A. E. Faraggi, Phys. Lett. B **377**, 43 (1996) doi:10.1016/0370-2693(96)00310-3 [hep-ph/9506388].

23. A. E. Faraggi, Nucl. Phys. B **487**, 55 (1997) doi:10.1016/S0550-3213(96)00682-7 [hep-ph/9601332].

24. G. B. Cleaver, Nucl. Phys. Proc. Suppl. **62**, 161 (1998) doi:10.1016/S0920-5632(97)00653-1[hep-th/9708023].

25. G. B. Cleaver and A. E. Faraggi, Int. J. Mod. Phys. A 14, 2335 (1999) doi:10.1142/S0217751X99001172 [hep-ph/9711339].

26. G. Cleaver, M. Cvetic, J. R. Espinosa, L. L. Everett and P. Langacker, Nucl. Phys. B **525**, 3 (1998) doi:10.1016/S0550-3213(98)00277-6 [hep-th/9711178].

27. G. Cleaver, M. Cvetic, J. R. Espinosa, L. L. Everett and P. Langacker, Nucl. Phys. B **545**, 47 (1999) doi:10.1016/S0550-3213(98)00863-3 [hep-th/9805133].

28. G. Cleaver, M. Cvetic, J. R. Espinosa, L. L. Everett, P. Langacker and J. Wang, Phys. Rev. D **59**, 055005 (1999) doi:10.1103/PhysRevD.59.055005 [hep-ph/9807479].

29. G. Cleaver, M. Cvetic, J. R. Espinosa, L. L. Everett, P. Langacker and J. Wang, Phys. Rev. D **59**, 115003 (1999) doi:10.1103/PhysRevD.59.115003 [hep-ph/9811355].

30. G. Cleaver. 1998. *Quark masses and flat directions in string models*. pages 332-340.

31. G. B. Cleaver, A. E. Faraggi and D. V. Nanopoulos, Phys. Lett. B **455**, 135 (1999) doi:10.1016/S0370-2693(99)00413-X [hep-ph/9811427].

32. G. B. Cleaver, A. E. Faraggi and D. V. Nanopoulos, Int. J. Mod. Phys. A **16**, 425 (2001) doi:10.1142/S0217751X01001057 [hep-ph/9904301].

33. G. B. Cleaver, A. E. Faraggi, D. V. Nanopoulos and J. W. Walker, Nucl. Phys. B **593**, 471 (2001) doi:10.1016/S0550-3213(00)00543-5 [hep-ph/9910230].

34. G. Cleaver. *M fluences on string model building*. (1991).

35. G. B. Cleaver, A. E. Faraggi, D. V. Nanopoulos and J. W. Walker, Mod. Phys. Lett. A **15**, 1191 (2000) doi:10.1142/S0217732300001444 [hep-ph/0002060].

36. G. B. Cleaver, A. E. Faraggi and C. Savage, Phys. Rev. D **63**, 066001 (2001) doi:10.1103/PhysRevD.63.066001 [hep-ph/0006331].

37. G. B. Cleaver, A. E. Faraggi, D. V. Nanopoulos and J. W. Walker, Nucl. Phys. B **620**, 259 (2002) doi:10.1016/S0550-3213(01)00558-2 [hep-ph/0104091].

38. G. B. Cleaver, D. J. Clements and A. E. Faraggi, Phys. Rev. D **65**, 106003 (2002) doi:10.1103/PhysRevD.65.106003 [hep-ph/0106060].

39. G. B. Cleaver, A. E. Faraggi and S. Nooij, Nucl. Phys. B **672**, 64 (2003) doi:10.1016/j.nuclphysb.2003.09.012 [hep-ph/0301037].

40. G. Cleaver. *Parameter space investigations of free fermionic heterotic models.* (2002).

41. G. Cleaver, V. Desai, H. Hanson, J. Perkins, D. Robbins and S. Shields, Phys. Rev. D **67**, 026009 (2003) doi:10.1103/PhysRevD.67.026009 [hep-ph/0209050].

42. J. Perkins, B. Dundee, R. Obousy, E. Kasper, M. Robinson, et al.. *Heterotic string optical unification*. pages 86-93. (2003).

43. J. Perkins et al., Phys. Rev. D **75**, 026007 (2007) doi:10.1103/PhysRevD.75.026007 [hep-ph/0510141].

44. G. B. Cleaver, A. E. Faraggi, E. Manno and C. Timirgaziu, Phys. Rev. D **78**, 046009 (2008) doi:10.1103/PhysRevD.78.046009 [arXiv:0802.0470 [hep-th]].

45. J. Greenwald, K. Pechan, D. Moore, T. Renner, T. Ali and G. Cleaver, Nucl. Phys. B **850**, 445 (2011) doi:10.1016/j.nuclphysb.2011.05.001 [arXiv:0912.5207 [hep-ph]].

46. G. Cleaver, A. E. Faraggi, J. Greenwald, D. Moore, K. Pechan, E. Remkus and T. Renner, Eur. Phys. J. C **71**, 1842 (2011) doi:10.1140/epjc/s10052-011-1842-8 [arXiv:1105.0447 [hep-ph]].

47. M. Robinson, G. Cleaver and M. B. Hunziker, Mod. Phys. Lett. A **24**, 2703 (2009) doi:10.1142/S0217732309031843 [arXiv:0809.5094 [hep-th]].

48. G. B. Cleaver, A. E. Faraggi, D. V. Nanopoulos and J. W. Walker, Nucl. Phys. B **593**, 471 (2001) doi:10.1016/S0550-3213(00)00543-5 [hep-ph/9910230].

49. T. Renner, J. Greenwald, D. Moore and G. Cleaver, Eur. Phys. J. C **72**, 2167 (2012*)* doi*:*10.1140/epjc/s10052-012-2167-y [arXiv:1111.1263 [hep-ph]].

50. R. K. Obousy, M. B. Robinson and G. B. Cleaver, Mod. Phys. Lett. A **24**, 1577 (2009) doi:10.1142/S0217732309030965 [arXiv:0810.1038 [hep-ph]].

51. H. Harari, Beyond charm, in Balian, R.; Llewellyn-Smith, C.H. Weak and Electromagnetic Interactions at High Energy (Les Houches, France, 1976). Les Houches Summer School Proceedings. p. 613.

52. Harari H. Three generations of quarks and leptons, in E. van Goeler, Weinstein R. (eds.). Proceedings of the XII Rencontre de Moriond. p. 170. SLAC-PUB-1974.

53. T. Renner, J. Greenwald, D. Moore and G. Cleaver, ISRN High Energy Phys. **2013**, 595070 (2013) doi:10.1155/2013/595070 [arXiv:1111.1917 [hep-ph]].

54. J. Greenwald, K. Pechan, D. Moore, T. Renner, T. Ali and G. Cleaver, Nucl. Phys. B **850**, 445 (2011) doi:10.1016/j.nuclphysb.2011.05.001 [arXiv:0912.5207 [hep-ph]].

55. W. Hicks, L. Vestal, J. Greenwald, D. Moore, T. Renner and G. Cleaver, arXiv:1108.4082 [physics.comp-ph].

56. D. Moore et al., Mod. Phys. Lett. A **26**, 2411 (2011) doi:10.1142/S0217732311036851 [arXiv:1107.5758 [hep-ph]].

57. G. B. Cleaver, Nucl. Phys. B **456**, 219 (1995) doi:10.1016/0550-3213(95)00481-0 [hep-th/9505080].

58. H. Kawai, D. C. Lewellen, J. A. Schwartz and S. H. H. Tye, Nucl. Phys. B 299, 431 (1988). doi:10.1016/0550-3213(88)90544-5 H. Kawai, D. C. Lewellen and S. H. H. Tye, Nucl. Phys. B **288**, 1 (1987). doi:10.1016/0550-3213(87)90208-2

59. Y. Cui, Phenomenology of Hidden Sector Physics, The University of Michigan, 2008.

60. A. V. Gladyshev and D. I. Kazakov, *Supersymmetry and LHC.* (2006).

61. G. Aad et al. (ATLAS Collaboration, CMS Collaboration) Phys. Rev. Lett. **114**, 191803 (2015)

62. I. Antoniadis, C. P. Bachas and C. Kounnas, Nucl. Phys. B **289**, 87 (1987). doi:10.1016/0550-3213(87)90372-5

63. Robinson, Matthew. Symmetry and the Standard Model: Mathematics and Particle Physics. Springer, 2011. Print.

64. String Theory, at 20, Explains It All (or Not). The New York Times. The New York Times Company, December 2004. Web. 28 Jun 2017.

65 R. L. Rivest, A. Shamir, L. M. Adleman, Commun. ACM **21**, (1978). doi:10.1145/359340.359342

66 Y. y. Sun, R. q. Kong, X. y. Wang and L. c. Bi, *An Image Encryption Algorithm Utilizing Mandelbrot Set.* 2010 International Workshop on Chaos-Fractal Theories and Applications, Kunming, Yunnan, 2010, pp. 170-173. doi: 10.1109/IWCFTA.2010.70

67. B. Dundee, Grand Unified Theories in Higher Dimensions: From the Heterotic String to Randall-Sundrum, Baylor University, 2006