BOISECRYPT FALL 2013

ABSTRACTS

David Albertson, *Generalization of the Whirlpool Hash Function*

Whirlpool is a hash function developed in 2003 and accepted by the New European Schemes for Signatures, Integrity, and Encryption (NESSIE) for widespread use. Whirlpool uses a Rijndael-type block cipher in a Merkle-Damgård construction to create a hash function. This internal block cipher has a rich algebraic structure, which is vital to the security of the function. We generalize the standard version of Whirlpool and explore these algebraic properties. In particular, we investigate the conditions under which the set of encryption functions used in Whirlpool form a group under functional composition. We will give special attention to the *MixRow* function and the matrix used therein.

Rustyn Yazdanpour, *Strong Measure Zero Sets*

In this talk, we chart the history of strong measure zero sets, characterize them in relation to other sets, and present specific set theoretic statements that surface as a consequence of the existence of strong measure zero sets. We also provide plenty of examples of strong measure zero sets and give a partial compilation of others' work in relation to them.

Shehzad Ahmed, *The Borel Conjecture in the Projective Hierarchy*

In 1919, Emile Borel conjectured that all strong measure zero subsets of the real line are countable. Sierpinski later showed that this fails in ZFC+CH, while Laver was able to exhibit a model of ZFC in which the Borel Conjecture held. In this talk we show that, while the full Borel Conjecture fails in the presence of the continuum hypothesis, there are natural models of ZFC+CH in which the Borel Conjecture holds for "reasonably definable" subsets of the real line.

Kent Mussell, *Selection Principles in Metalogic*

This paper covers the most fundemental topics needed to talk about soundness and completeness in logical systems, and to understand proofs of either of these properties. The contents of this paper operate in an area of logic study that takes logic itself as the object of study: meta-logic. In meta-logic we often do three things: define our logical formulae (Grammar), define what those logical formulae

Date: December 20, 2013.

mean (Semantics), and define the rules for proofs (proof theory). In a crude sense, the semantics of a logic tell us which logical formulae are true. The proof-theory of a logic tells us which logical formulae can be deduced by proof from a set of axioms. These axioms are the objects of study in this paper. The properties studied in most depth is soundness and completeness. Basically put, soundness is the following property: Every logical formula that is provable is guaranteed to be true. Completeness is this: Every logical formula that is guaranteed to be true is provable. The selection principle that I explore is this: Given a sequence of sound and complete sets of logical formulae, can we pick one formula from each, such that the set of all of our selections is complete? As it turns out, the answer is: no. I also explore the following Ramsian property: If we take any sound and complete set of logical formulae and partition it into finitely many pieces, will one of those pieces be sound and complete? Again, the answer is: no.

Dillon Wardwell, *Selection Principles in the Zariski Topology*

We show that the prime spectrum of a Noetherian ring, when endowed with the Zariski topology, is Rothberger. In fact, we demonstrate a strategy for player TWO in the Rothberger game which results in a win for TWO in finitely many innings.

Anna Megale, *Primality Testing Using Elliptic Curves*

Primality testing is the process of taking an integer greater than one and determining whether it is prime or composite. Algorithms for primality testing have grown to be very popular since the introduction of public-key cryptography. This paper will discuss a method of primality testing using elliptic curves, along with some intermediate theorems and statements leading up to the formation of the main algorithm.

Erik Holmes, *Selection Principles and Cardinal Characteristics*

A cardinal characteristic is simply the smallest cardinal for which a statement, true of $\aleph_0$, fails. There are many examples of cardinal characteristics, one such example being $\mathbf{cov}(meager) = \mathbf{cov}(\mathcal{M}) =$ the smallest number of meager sets whose union covers $\mathbb{R}$. The selection principles that we will discuss hold for all countable sets, thus it makes sense to consider the smallest cardinality at which a certain property fails. In this talk we will introduce cardinal invariants, focusing most of our attention on $\mathfrak{b}$, $\mathfrak{d}$, and $cov(\mathcal{M})$. Then we will investigate the relation between certain selection principles and these well known invariants.

Suzanne Craig, *Simplified Version of AES*

Today the greatest challenge to the cyber world is security. Technology rapidly changes, making old methods obsolete and requiring new developments and advancements in information security. Cryptography, the science of preparing coded or protected communications, designs systems which make messages intelligible only to the person possessing a key. There are two types of key-based cryptosystems: symmetric key and asymmetric cryptosystem. Symmetric key encryption is a cryptographic technique that uses a shared secret key to encrypt and decrypt data. Symmetric encryption algorithms are very efficient in processing large amounts of information. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers, which provide bit-by-bit and block encryption respectively. The Advanced Encryption Standard (AES) is a block cipher which was approved by the U.S. Federal Information Processing Standards in 2001 and is used to secure Top Secret information by the federal government. This cryptosystem has a highly complex algebraic structure. We design a simplified version of this cryptosystem that has all the functions that AES has, but is made suitable for timely security analysis. Our simplified AES is based on a field of characteristic 3, while all other known versions of AES are based on fields of characteristic 2. We then investigate how the characteristic of the field affects the security of this cryptosystem.

William Unger, *Edwards Curves and Their Applications*

The Edwards curves is a newer type of equation that has cryptological applications. These curves have some computational advantages compared to other curves. We will explore the proprieties of the Edwards curve including the group operation of adding points on the curve. Then we will explore some of the cryptological applications that you can use with Edwards curves.

Paul Plummer, *Looking at Generators and Relations of Groups with Selection Principles*

We will be looking at groups, in particularly countably presented groups, and certain selection principles relating to the generators and relations. Similarly we will also look at selection principles and see what they imply about the groups.