AES Introduction

In October 2000, NIST announced that a Belgian submission, Rijndael, would become the Advanced Encryption Standard (AES). The AES was created as a result of the U.S. government’s National Institute of Standards’ (NIST) programme to choose a block cipher to succeed the Data Encryption Standard (DES). The DES has been a U.S. federal standard and a de facto global block cipher standard for over 20 years and it is expected that the AES will replace DES around the world. It is therefore crucial that any trust invested in the AES be well-founded.

As part of the AES selection process, security analysis of the different candidates was contributed by cryptographic researchers in an ad hoc manner. While Rijndael was a popular choice, due in great part to its versatile performance attributes, there has been a growing disquiet about whether Rijndael really is a good choice when the anticipated lifetime of the cipher is twenty years. The purpose of this grant application is to employ a post-doctoral researcher to work with the named investigators on the cryptanalysis of the AES and to explore and refine new and promising cryptanalytic techniques.

AES Recent Research

The AES is a cipher that exhibits a remarkable degree of mathematical structure. Much of this structure was introduced intentionally and results from considerations such as the implementation of the algorithm and its resistance to certain standard cryptanalytic techniques. However, some cryptographers (for example [4]) commented at an early stage that the exceptional simplicity and algebraic structure of Rijndael might be a source of concern. This speculation increased considerably in recent months following the publication of two papers about the AES.

- **Essential Algebraic Structure Within the AES** by S. Murphy and M. Robshaw [5]. This paper by two of the investigators on this proposal, forms the basis for the work proposed here. This paper was given at the CRYPTO 2002 conference and showed some remarkable properties of the AES. The AES is defined using operations over two fields $GF(2^8)$ and $GF(2)$, and the interaction between operations in these two fields is a major difficulty in the cryptanalysis of the AES. This paper outlined a new approach that avoids the conflict between these two fields. This paper defined a new
block cipher, the BES, that uses two very simple algebraic operations in $GF(2^8)$, and showed that the AES is identical to the BES with a restricted message space and key space. Thus the AES can be defined solely using two simple algebraic operations in one field, $GF(2^8)$, which allows the AES to be analyzed within a broad and rich setting. One consequence is that AES encryption can be described by a very small and extremely sparse overdetermined multivariate quadratic (MQ) system over $GF(2^8)$. The solution of such an MQ system would recover an AES key.

- Cryptanalysis of Block Ciphers with Overdefined Systems of Equations by N. Courtois and J. Pieprzyk [2]. This paper suggests a two stage process for the cryptanalysis of certain block ciphers. The first involves expressing the operation of encryption as a multivariate quadratic system over $GF(2)$. The second part of their work proposes a new technique known as extended sparse linearization (XSL) to solve the type of MQ system that naturally arises from block ciphers, thus enabling recovery of the key. This paper of Courtois and Pieprzyk has had a mixed reception. The first part of their work is not in doubt, and indeed, similar techniques for the analysis of block ciphers have been considered for many years. However, the second part of their work, namely the validity of the XSL technique, is somewhat controversial and is not universally accepted by leading cryptographers [1]. In any case, when Courtois and Pieprzyk applied the XSL technique to the MQ system over $GF(2)$ that defines an AES encryption, they obtained a work effort of around $2^{230}$ AES encryptions, far in excess of the $2^{128}$ AES encryptions required for an exhaustive key search.

The work pursued by Murphy and Robshaw [5] has very broad implications for the analysis of the AES. However, it also has some immediate implications for the work of Courtois and Pieprzyk [2]. In particular, with regard to the XSL technique, Murphy and Robshaw showed that by using their techniques, an MQ system over $GF(2^8)$ for an AES encryption would be very small and extremely sparse. Thus this system of equations would be particularly well-suited to the proposed XSL technique. Consequently, if XSL was a valid technique then applying XSL to the MQ $GF(2^8)$-system would reduce the work effort for the recovery of an AES key to $2^{100}$ AES encryptions (this is briefly discussed in [5] with further details in [6]). Whilst this would not be a practical concern for the security of the AES, it would be severe blow to its credibility.

However, the full impact of the algebraic simplification of the AES given by Murphy and Robshaw has yet to be assessed and it is clear that a full exploration of techniques for analyzing the AES is urgently required. As such, we propose a research project dedicated to exploring the effectiveness of existing techniques on the AES, to developing new cryptanalytic techniques for the analysis of the AES, and to broaden the scope of the application of this knowledge to other prominent block ciphers.
AES Research Project

The overall aim of this project is to analyse and assess the cryptanalytic strength of the AES using novel algebraic techniques. In more detail, the proposed research program would have the following major aims.

1. To understand the (true) effectiveness of the XSL technique.

2. To consider the applicability of methods of solving large sparse systems of multivariate quadratic equations over finite fields to the systems generated in the cryptanalysis of the AES and other block ciphers. Such methods might involve extensions to the XSL technique, Gröbner basis techniques such as the F4 algorithm recently proposed by Faugere [3] or new techniques.

3. To consider the further implications of the work of the algebraic simplification of the AES given by Murphy and Robshaw [5], and to extend this approach to related cryptographic primitives.

4. To develop and pursue alternative approaches to the analysis of the AES. The algebraic simplification of the AES indicates that the AES possesses considerable geometric structure [5]. A full exploration of this geometric structure has not yet been possible, some of which would require a very particular set of skills (both cryptographic and geometric) to develop fully.

5. To apply new and developing techniques for the cryptanalysis of the AES in a more general context to other block ciphers and encryption primitives.

The starting point for any such work would be to develop a sound and thorough understanding of the algebraic and geometric issues that underpin the security of the AES, rather than the ad hoc approach that appears in the public AES literature.

References


