Literature Survey

Karl Southern

October 24, 2017

1 Introduction

Project Title: Cryptanalysis of SPNs building up to AES-128
Student: Karl Southern
Supervisor: Dr Magnus Bordewich

1.1 Problem background

The aim of this project is to demonstrate the effectiveness of various methods of cryptanalysis on a simple 4 round SPN and then on a reduced round AES-128 and, if possible, the full AES-128. The effectiveness of each attack will be measured by the number of plaintext-ciphertext pairs that are required to find the key as well as the complexity of the attack. Each attack will also be measured on how effective it is as the complexity of the cryptosystem is increased, such as by increasing the size of each block or by increasing the number of rounds.

1.2 Terms

SPN: Substitution-Permutation Network, a type of cipher that encrypts text by running it through multiple rounds, where each round consists of an SBox (a substitution cipher), a permutation (a transposition cipher) and then XOR'ing the state with the round key.
Round key: The key used for that particular round, it is generated by the key schedule.
Key schedule: The method used to generate sub keys from an initial key, this is normally done by applying SBoxes and permutations to the key, and details which sub key is applied to which round.
DES: The Data Encryption Standard is a symmetric-key cryptosystem created by IBM in 1975 and became a Federal Information Processing Standard in 1977. In 1997 NIST started a competition to replace DES, with its successor becoming AES.
AES[1]: The Advanced Encryption Standard, also known as Rijndael, its original name. It is a block cipher that can be of length 128,196 or 256, which have 10,12 and 14 rounds respectively. It can also be modelled as a SPN.

2 Themes

2.1 Attacks

There are many different types of cryptanalysis that are applicable to SPN's and AES, in this project most of these will be covered. The first major cryptanalysis of a block cipher was differential cryptanalysis[2] and was detailed at the 1990 CRYPTO conference by Biham and Shamir, this was able to break DES, the precursor to AES, faster than an exhaustive search. This approach is a chosen plaintext attack, where plaintexts are chosen that have specific differences, ΔX, the cryptanalysis then exploits the probability of a corresponding difference, ΔY, existing between the outputs. At the 1993 EUROCRYPT conference, Matsui proposed another type of cryptanalysis called linear cryptanalysis[3]. Linear cryptanalysis is a known plaintext based attack in which exploits linear expressions, which involve plaintext bits, subkey bits and ciphertext bits, that have a high probability of holding.

In the years since they were proposed, both forms of cryptanalysis have been refined further and have had specialised versions developed including: higher order cryptanalysis [4] which focuses on a set of differences; truncated cryptanalysis [5] which focuses on predicting just a few bits and not a whole block; impossible differential cryptanalysis[6] which focuses on differences that can't occur and even differential-linear cryptanalysis[7] which uses both methods in tandem. The third major type of cryptanalysis is integral cryptanalysis, also known as the SQUARE attack after the cryptosystem is was first used to break, the attack was first detailed in the original paper proposing SQUARE[8], a more general method of integral cryptanalysis was explored in a paper by Knudsen and Wagner[9] in 2002. Integral cryptanalysis acts a complement to differential cryptanalysis in that it looks at how the summation of values propagate through the cryptosystem, as it looks at the summation of ciphertexts, it allows multiple ciphertexts to be considered at once instead of only considering pairs of ciphertexts.

At ASIACRYPT 2002, Courtois and Pieprzyk became the first people to announce that they had an attack that they claimed could break AES, this attack was called XSL[10]. XSL works by expressing the cryptosystem as a system of polynomial equations, these can then be solved using a very small amount of ciphertext/plaintext pairs. However it requires an unrealistic amount of preprocessing, such that it is slower than brute force. As such, until better methods are found to generate and solve these equations, this attack does not break AES in any practical sense.

The only attack so far that "breaks" AES is the Biclique attack[11] although even this is only about 4 times quicker than brute force. Biclique is a type of meet-in-the-middle attack, that starts with a standard meet-in-the-middle attack and then creates "bicliques", a key that maps internal states to ciphertexts.

This allows a standard meet-in-the-middle attack to be extended to attack every round of AES, where as a normal meet-in-the-middle attack is only able to attack a limited number of rounds.

2.2 Security

As well as looking at attacks on cryptosystems, I will also be looking at its complement, security of cryptosystems. When a cryptosystem is proposed, it is very difficult to prove that it will be secure against both current forms of cryptanalysis and against future forms of cryptanalysis, this is demonstrated with SQUARE[8], a cryptosystem that was proposed for AES and was designed to be secure against linear and differential cryptanalysis, however another form of cryptanalysis was discovered by the creators of SQUARE that cracked it.

In section 8 of the Rijndael proposal for AES[1], Daemen and Rjimen demonstrate how Rijndael is not susceptible to linear, differential or integral cryptanalysis on the full AES. The security of AES against linear and differential cryptanalysis was further discussed at ASIACRYPT 2002 [12] and was expanded to include SPN's. In 2010 Kaminsky presented a paper[13] on the security of AES, whilst it is able to show that AES is provably secure against linear, differential and integral cryptanalysis, it is only able to state that for algebraic attacks, such as XSL, AES is secure with the versions of the attacks we have now. Below is a table showing how secure AES is against various forms of cryptanalysis, looking at multiple key sizes and both full and reduced round AES.

In Transactions on Symmetric Cryptology, Kaplan looks at how classical cryptanalysis methods could be applied using quantum computers[14], whilst it hasn't broken AES yet, it does show that the quantum forms of these types of cryptanalysis will have the potential to break AES.

Key Size	No. Rounds	Data Complexity	Time Complexity	Method and Source
AES-128	7	2^{32}	2^{128}	Collision[15]
AES-128	7	$2^{128} - 2^{119}$	2^{120}	SQUARE[16]
AES-128	7	$2^{115.32}$	$2^{119.32}$	Impossible Differential[17]
AES-128	7	$2^{112.2}$	$2^{117.2}$	Impossible Differential[18]
AES-128	8	2^{88}	$2^{125.4}$	Biclique[11]
AES-128	10	2^{88}	$2^{126.1}$	Biclique[11]
AES-192	7	2^{34+n}	$2^{280-n} + 2^{82+n}$	Meet In The Middle[19]
AES-192	7	2^{32}	2^{184}	SQUARE[20]
AES-192	7	2^{92}	2^{162}	Impossible Differential[21]
AES-192	7	$19 \cdot 2^{32}$	2^{155}	SQUARE[16]
AES-192	7	$2^{109.67}$	$2^{154.67}$	Impossible Differential[17]
AES-192	7	$2^{115.5}$	2^{119}	Impossible Differential[21]
AES-192	8	$2^{128} - 2^{119}$	2^{188}	SQUARE[16]
AES-192	8	$2^{102.3}$	$2^{166.3}$	Impossible Differential[17]
AES-192	9	2^{80}	$2^{188.8}$	Biclique[11]
AES-192	9	$2^{115.89}$	$2^{180.89}$	Impossible Differential[17]
AES-192	9	$2^{125.89}$	$2^{150.89}$	Impossible Differential[17]
AES-192	12	2^{80}	$2^{189.7}$	Biclique[11]
AES-256	7	2^{32}	2^{208}	Meet In The Middle[19]
AES-256	7	2^{32}	2^{200}	SQUARE[20]
AES-256	7	$21 \cdot 2^{32}$	2^{172}	SQUARE[16]
AES-256	7	$2^{115.5}$	2^{119}	Impossible Differential[21]
AES-256	8	$2^{111.1}$	$2^{227.8}$MA	Impossible Differential[18]
AES-256	8	$2^{116.5}$	$2^{247.5}$	Impossible Differential [21]
AES-256	8	2^{32}	2^{09}	Meet In The Middle [19]
AES-256	8	$2^{128} - 2^{119}$	2^{204}	SQUARE[16]
AES-256	9	2^{120}	$2^{241.92}$	Biclique [11]
AES-256	11	$2^{122.4}$	$< 2^{254.4}$	Impossible Differentials[17]
AES-256	14	2^{40}	$2^{254.4}$	Biclique[11]

Table 1: A table comparing different methods of cryptanalysis when applied to AES

3 Direction of Project

This project will look at the forms of cryptanalysis discussed so far and will apply them, initially, to a simple SPN with the aim of comparing their complexity, it will also look at how increasing the complexity of the SPN, by increasing the key size and the number of rounds, impacts the effectiveness of the cryptanalysis. By doing this the project will try to show how these methods of increasing complexity can be used to improve security. These forms of cryptanalysis will then be applied to AES*, a SPN identical to AES proposed by Baignères [22] and then finally to reduced round AES-128.

References

[1] Joan Daemen and Vincent Rijmen. AES Proposal: Rijndael, 1999.

[2] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.

[3] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

[4] Xuejia Lai. *Higher Order Derivatives and Differential Cryptanalysis*, pages 227–233. Springer US, Boston, MA, 1994.

[5] Lars R. Knudsen. Truncated and Higher Order Differentials. In *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211. Springer, 1994.

[6] R.C.W. Phan. Generalised impossible differentials of advanced encryption standard. *Electronics Letters*, 37:896–898(2), July 2001.

[7] Susan K. Langford and Martin E. Hellman. Differential-Linear Cryptanalysis. In *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 17–25. Springer, 1994.

[8] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The Block Cipher Square. In *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer, 1997.

[9] Lars R. Knudsen and David Wagner. Integral Cryptanalysis. In *Fast Software Encryption, 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers*, volume 2365 of *Lecture Notes in Computer Science*, pages 112–127. Springer, 2002.

[10] Nicolas Courtois and Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 267–287. Springer, 2002.

[11] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique Cryptanalysis of the Full AES. In *ASIACRYPT*, volume 7073 of *Lecture Notes in Computer Science*, pages 344–371. Springer, 2011.

[12] Sangwoo Park, Soo Hak Sung, Seongtaek Chee, E-Joong Yoon, and Jongin Lim. On the Security of Rijndael-Like Structures against Differential and Linear Cryptanalysis. In *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 176–191. Springer, 2002.

[13] Alan Kaminsky, Michael Kurdziel, and Stanisław Radziszowski. An overview of cryptanalysis research for the advanced encryption standard. In *MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010*, pages 1310–1316. IEEE, 2010.

[14] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum Differential and Linear Cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(1):71–94, 2016.

[15] Henri Gilbert and Marine Minier. A Collision Attack on 7 Rounds of Rijndael. In *AES Candidate Conference*, pages 230–241, 2000.

[16] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved Cryptanalysis of Rijndael. In *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 213–230. Springer, 2000.

[17] Zheng Yuan. New Impossible Differential Attacks on AES. Cryptology ePrint Archive, Report 2010/093, 2010.

[18] Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New Impossible Differential Attacks on AES. Cryptology ePrint Archive, Report 2008/540, 2008.

[19] Hseyin Demirci and Ali Aydin Seluk. A Meet-in-the-Middle Attack on 8-Round AES. In *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*, pages 116–126. Springer, 2008.

[20] Stefan Lucks. Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys. In *AES Candidate Conference*, pages 215–229, 2000.

[21] Wentao Zhang, Wenling Wu, and Dengguo Feng. New Results on Impossible Differential Cryptanalysis of Reduced AES. In *Information Security and Cryptology - ICISC 2007, 10th International Conference, Seoul, Korea, November 29-30, 2007, Proceedings*, pages 239–250, 2007.

[22] Thomas Baignères and Serge Vaudenay. Proving the Security of AES Substitution-Permutation Network. In *Selected Areas in Cryptography*, 2005.