CRYPTANALYSIS OF SYMMETRIC CIPHERS USING ROBDDs AND SMT SOLVERS

HARISH KUMAR SAHU

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
AUGUST 2018

CRYPTANALYSIS OF SYMMETRIC CIPHERS USING ROBDDs AND SMT SOLVERS

by

HARISH KUMAR SAHU

Department of Mathematics

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi
AUGUST 2018

Dedicated To My Family

Certificate

This is to certify that the thesis titled **"Cryptanalysis of Symmetric Ciphers Using ROBDDs and SMT Solvers"** submitted by **Mr. Harish Kumar Sahu** to the Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by him under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Prof. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas
New Delhi 110 016

Acknowledgements

Any achievement, no matter how big or small, is not just an individual endeavour but the fructification of the efforts of a lot of people. This thesis is no exception. I hereby acknowledge the people whose involvement, directly or indirectly, helped in this thesis seeing the light of the day.

First and foremost, I would like to express my deep sense of respect and gratitude to supervisor Prof. R. K. Sharma, who has been a constant source of inspiration during the course of this work. He has always been patient and encouraged me to work in a better way. Without his help and support, I might have not been able to write this thesis.

I would like to give my special thanks to my SRC (Student Research Committee) members Prof. S. Dharmaraja, Prof. Ritumoni Sarma, and Prof. M.P. Gupta for their valuable time and suggestions. I would also like to thank all the faculty members and staff of Department of Mathematics, IIT Delhi for their co-operation and support. I would like to especially thank Prof. Aparana Mehra for her continuous encouragement and motivation.

I also thank all my friends at IIT Delhi Ambrish, Chirag, Rohit, Yogesh, Dinesh, Rahul, Varun, Deepchand, Meenu and Anju for their support, special thanks to Vishal who helped me in completing administrative formalities of the institute.

Now I would like to acknowledge the support from my office Scientific Analysis Group (SAG), DRDO. In particular, I would like to express special thanks and heartiest gratitude to Dr. N. R. Pillai for his supervision. He kept me motivated to remain focused in the research work whenever I got distracted. He spared time from his very busy schedule for discussion, reviewing my articles and listening me patiently.

I would like to express my sincere respect and heartiest gratitude to Dr. S.K. Tiwari, Dr. P.R.

Mishra and Dr. Indivar Gupta for their continuous guidance. All of them are very hard-working and workaholic. They spent lot of time beyond office hours with me for discussion and provided valuable suggestions.

I wish to express my sincere thanks to the current Director, Mrs. Anu Khosla, the former Directors Dr. G Athithan and Dr. P. K. Saxena for the administrative support to carry out this work.

I would like to thank all my colleagues at DRDO and specially to Mrs. Pratibha Yadav, Dr. Dhananjoy Dey, Dr. Yogesh Lather, Dr. Nupur Gupta and Mr. Avdhesh Kumar Gautam for their support and encouragement.

I am immeasurably grateful to my family who gently offered counselling and gave unconditional support at each and every point of my academic journey. It was the patience and silent sacrifice of my father and mother, which led me to complete this sojourn. My achievements are outcome of their dedication and their belief in my potentials. It is their blessings that made me reach this milestone. The contribution of my in-laws deserve my regards and heartiest gratitude as they encouraged continuously.

Last, but not the least is the dedicated sacrifice of my loving wife, Preeti Sahu who calmly and patiently did everything possible on her part, leaving aside all her comforts and ease of life, just to support me through my research work. I draw a superb and delightful stream of strength from my lovely son, Krishna, who has always made the atmosphere at my home very lively and entertaining. Most importantly, I thank almighty God for his blessings.

New Delhi *Harish Kumar Sahu*

Abstract

This dissertation is concerned with cryptanalysis of symmetric ciphers using Reduced Ordered Binary Decision Diagrams (ROBDDs) and Satisfiability Modulo Theories (SMT) solvers and demonstrate these approaches on real world symmetric ciphers. Based on the above approaches, the thesis is organized in the following two parts:

I. Cryptanalysis of Stream Ciphers using ROBDDs

II. Cryptanalysis of Block Ciphers using SMT Solvers

In the first part of thesis, we propose practical approach for ROBDDs based cryptanalysis of stream ciphers. Theoretical framework for BDD based cryptanalysis of stream ciphers has been presented first by Krause in 2002. Since then not much work has been reported in this area. ROBDD is a key variant of BDD. It has important properties of compactness and uniqueness to represent Boolean functions. So, we propose a practical approach for cryptanalysis of stream ciphers using ROBDDs. We discuss various methods for finding ordering of ANDing operation of ROBDDs, as it is a crucial step required during the process of cryptanalysis. Out of these methods, "Recursive Symmetric ANDing" (RSAND) gives optimal order of ANDing in terms of time and memory. We demonstrate our approach on E_0 and LILI-128 stream ciphers.

In the second part of the thesis, we study SMT solvers based cryptanalysis of block ciphers. SMT solvers have already been used in cryptanalysis, Martin Stanek has experimented the solvers over the shuffle block cipher, and Stefan Kolbl and Gregor Leander have used them to find both optimal differential and linear characteristics of the Simon block cipher. Here, we propose an approach for the cryptanalysis of block ciphers using SMT solvers. We show how the cryptanalysis problem of International Data Encryption Algorithm (IDEA) block cipher can be translated into SMT-LIB v2 format and then can be solved using SMT solvers. We demonstrate our attack on IDEA. An important feature of our attack is that it requires a few plaintext-ciphertext pairs to recover the key. We also use various serial and parallel SMT solvers and compare their performances in mounting the attack on IDEA. Experiments have been performed on reduced round versions of IDEA to determine full key and to obtain partial key for full IDEA cipher. We compare our results on 2-round and 3-round IDEA with some other existing attacks on it.

सार

इस शोध कार्य में सिमेट्रिक साइफर्स का रिड्यूस्ड ऑर्डरड बाइनरी डिसिशन डायग्राम (आरओबीडीडी) और सेटीस्फिएबिलिटी मॉड्यूलो थ्योरी (एसएमटी) सॉल्वर्स का प्रयोग करके क्रिप्टएनालिसिस की गई हैं तथा इन तकनीकों को व्यवहारिक साइफर्स पर भी लगाया गया है |

उपरोक्त तकनीकों के आधार पर शोध कार्य को निम्नलिखित दो भागो में विभाजित किया गया है:

१. आरओबीडीडीज का उपयोग करके स्ट्रीम साइफर्स की क्रिप्टएनालिसिस करना
२. एसएमटी सॉल्वर्स का उपयोग करके ब्लॉक साइफर्स की क्रिप्टएनालिसिस करना

शोधकार्य के प्रथम भाग में हम आरओबीडीडी का प्रयोग करके स्ट्रीम साइफर्स की क्रिप्टएनालिसिस करने के लिए एक व्यवहारिक तकनीक प्रस्तावित करते हैं | क्रॉस ने सर्वप्रथम बीडीडी आधारित स्ट्रीम साइफर्स के क्रिप्टएनालिसिस के लिए सैद्धांतिक ढांचा प्रस्तुत किया | परन्तु इसके उपरांत इस क्षेत्र में ज्यादा प्रगति नहीं हुई | आरओबीडीडी, बीडीडी का एक महत्वपूर्ण प्रकार है | आरओबीडीडी का एक महत्वपूर्ण अनुप्रयोग यह है कि इनका प्रयोग करके बुलियन फलनो को कॉम्पैक्ट और अद्वितीय तरीके से निरूपित कर सकते है | इस लिए इस कार्य में हमने आरओबीडीडी का प्रयोग करते हुए स्ट्रीम साइफर्स की क्रिप्टएनालिसिस की एक व्यवहारिक तकनीक प्रस्तावित की है| आरओबीडीडी के एंडिंग ऑपरेशन में विभिन्न तरीको का विश्लेषण किया क्योंकि यह क्रिप्टएनालिसिस के प्रक्रिया के दौरान एक अति महत्वपूर्ण चरण हैं | हम इस निस्कर्स पर पहुंचते है कि एंडिंग ऑपरेशन के सभी तरीको में से रिकर्सिव सिमेट्रिक एंडिंग (आर एस एंड) समय तथा भण्डारण के दृष्टिकोण से उत्तम हैं हम विकसित तकनीक का उपयोग करके लिली-१२८ व् इ0 स्ट्रीम साइफर की क्रिप्टएनालिसिस करके दिखाते हैं |

हम शोध कार्य के दूसरे भाग में एसएमटी सॉल्वर्स का प्रयोग करके ब्लॉक साइफर की क्रिप्टएनालिसिस करने की तकनीक प्रस्तुत करते हैं | एसएमटी सॉल्वर्स का क्रिप्टएनालिसिस के लिए अनुप्रयोग मार्टिन स्टेनक ने शफल ब्लॉक साइफर पर तथा स्टीफन कोल्बल और ग्रेगोर लिंडर ने साइमन ब्लॉक साइफर पर किया हैं | हम अपनी विकसित तकनीक का उपयोग करके आईडिया ब्लॉक साइफर का क्रिप्टएनालिसिस करते हैं | इस दौरान सर्वप्रथम हम आईडिया ब्लॉक साइफर को एसएमटी लिब प्रारूप में निरूपित करते हैं और फिर इस प्रारूप में उत्पन्न सिस्टम को एसएमटी सॉल्वर का प्रयोग करके हल करते हैं जो कि हमे वांछित गुप्त कुंजी प्रदान करती हैं | इस तकनीक का महत्वपूर्ण गुण यह है कि इसमें हमे बहुत कम प्लेन टेक्स्ट - साइफर टेक्स्ट के युग्मों की आवश्यकता होती है| हम विभिन्न सीरियल एवं सामानांतर एसएमटी सॉल्वर्स का उपयोग करते हुए आईडिया ब्लॉक साइफर की क्रिप्टएनालिसिस करते हैं साथ ही हम दोनों तरह के सॉल्वर्स की क्षमता का तुलनात्मक अध्ययन भी करते है | हम इस तकनीक का उपयोग करके रिड्यूस्ड राउंड आईडिया के लिए पूर्ण कुंजी तथा पूर्ण राउंड आईडिया की आंशिक कुंजी ज्ञात करने में करते है | हम अपने २ तथा ३ राउंड के क्रिप्टएनालिसिस के परिणामो की तुलना अन्य प्रकाशित परिणामों से करते हैं |

Contents

List of Figures

List of Tables

List of Symbols

$\mid$	OR operation
&	AND operation
$\oplus$	Ex-OR operation
$<<$	Circular left shift operator
$>>$	Circular right shift operator
$\wedge$	Conjunction
$\vee$	Disjunction
$\neg$	Complement
$\boxplus$	Addition of unsigned integers modulo 2^{16}(65536)
$\odot$	Multiplication of unsigned integers modulo 2^{16}+1 (65537)

List of Abbreviation

XOR	Exclusive OR
BDD	Binary Decision Diagram
ROBDD	Reduced Ordered BDD
LFSR	Linear Feedback Shift Register
P-C	Plaintext-Ciphertext
TMTO	Time Memory Trade Off
MITM	Meet In The Middle
IDEA	International Data Encryption Algorithm
IPES	Improved Proposed Encryption Standard
PGP	Pretty Good Privacy
SAT	Satisfiability
SMT	Satisfiability Modulo Theories
CNF	Conjunctive Normal Form
LSB	Least Significant Bit
MSB	Most Significant Bit