Towards a Combined Rotational-Differential Cryptanalytic Framework

Theodosis Mourouzis
Department of CS, University College London, WC1E 6BT

tmourouz@cs.ucl.ac.uk

Nikos Komninos

Department of CS, City University London, EC1V 0HB

nikos.komninos.1@city.ac.uk

Michalis Christofi

Department of CS, King's College, WC2R 2LS

michalis.christofi@kcl.ac.uk

Abstract

Cryptanalysis is the science of studying given encryption algorithms or any other cryptographic related mechanism in order to identify potential flaws or vulnerabilities either in the implementation and the environment or in the mathematics that underline the mathematical algorithms used. Such flaws can be used in order to dispute the level of security that the mechanism is claimed to offer and it is very important if we always enhance existing techniques.

One of the most important and powerful techniques in the area of symmetric cryptanalysis is the technique of Differential Cryptanalysis (DC). DC can be applied primarily to block ciphers but also to some extend to stream ciphers and cryptographic hash functions. Its discovery was attributed to Eli Biham and Adi Shamir in the late 1980s [2, 3], but according to Don Coppersmith this technique was already known to IBM and NSA as early as 1974 [1]. However, they decided to keep confidential the description of such powerful attack since it would be possibly able of breaking many block ciphers or other cryptography standards used in many applications.

The main task in DC is to study the propagation of certain input differences through different number of rounds and identify some input-output pairs of differences which propagate with comparatively good probability, compared to what expected in the case of a random permutation. This non-random behavior of the cipher for reduced number of rounds can sometimes be extended to a key recovery attack. Several enhancements were proposed to naive DC such as boomerang attack, impossible differentials and more importantly truncated differentials as proposed by Knudsen [6, 7]. In truncated differentials, an attacker studies the propagation of sets of differences instead of single differences. The problem in attacks involving truncated differentials is the study of the exponentially large space of differentials. Some ad-hoc heuristics of the cipher can be used to speedup the process. For example, Courtois and Mourouzis have suggested such heuristics in case of GOST block cipher which can be used in order to construct reduced round distinguishers for up to 20 rounds [8, 9]. In addition, a framework for extending a distinguisher to a possibly efficiently good key recovery attack is described in details in [10].

In addition to DC, we have plenty of other cryptanalytic techniques such as Linear Cryptanalysis [4, 5], Algebraic Attacks [11] and more recently Rotational Cryptanalysis by Khovratovich [13]. In linear cryptanalysis, the attacker constructs linear equations involving plaintext, ciphertext and key bits for a certain number of rounds which can be used to extend to an at-

tack against the full cipher. In algebraic attacks, an attacker tries to encode algebraically all cipher's operations and then using limited data such as known plaintext-ciphertext pairs tries to solve the underlying system of equations and derive some key bits. After deriving the algebraic encoding of the given cryptographic primitive, then ready open-source software can be used to derive the key in an automated way such as SAT solver.

In the other framework, that of rotational cryptanalysis, the attacker observes the propagation of pairs of inputs or intermediate states, which have some rotational symmetry towards different number of rounds. What we end up is a distinguisher in the related-key setting, since here the assumption of stochastic equivalence is not guaranteed as in case of DC. Such attacks are applicable to the ARX ciphers which are ciphers widely used in lightweight cryptography since they have very cheap implementation cost and they involve only three operations; modular additions, rotations and XOR gates [13].

All these attacks have been studied for many years and many advancements have been made. Many cryptographers combined such techniques in a cryptanalytic framework for constructing more efficient techniques. For example, we have algebraic-linear attacks, where linear equations hold with sufficiently high probability and added to the algebraic description of the cipher, increasing in this way the probability of being able to solve the underlying system. Albrecht in his PhD thesis suggested a cryptanalytic framework of combining algebraic attacks with differential attacks [12] and recently Mourouzis in his PhD thesis suggested an enhancements of algebraic attacks using truncated differentials [10].

In this report, we suggest a new cryptanalytic framework of constructing distinguishers which can be eventually extended to full attacks in the related-key scenario. We name this new paradigm as "Relational Cryptanalysis". The main idea is to exhibit the non-randomness of a given encryption algorithm by observing the propagation of specific sets of plaintexts of the form (P, P') such that these pairs satisfy some rotational and differential properties of the form $R_1(P) = P'$ and $P \oplus P' \in \Delta P$, for some rotational symmetry R_1 and fixed set of differences ΔP. Except of rotational and differential properties, we can add any other relation which seems to hold for a reduced number of rounds of the cryptographic primitive we study. Intuitively, we expect that by adding more relations we increase the observed probability of the propagation and this result to stronger statistical distinguishers.

The main idea behind our statistical distinguishers is to define two sets of relations $A = \{RI_1, RI_2, ..., RI_n\}$ and $B = \{RO_1, RO_2, ..., RO_m\}$, for some relations RI_i, RO_j and some integers n, m and then count the number of expected plaintext pairs (P_i, P_j) which are related by relations from the set A and lead to ciphertext pairs (C_i, C_j) which are related by relations from set B after some rounds r. For example, one relation RI_i may denote a specific difference or a set of differences as in truncated differentials, or a rotational symmetry of the pair of plaintexts by a fixed number of shifts or any other relation we can find based on the structure of the encryption algorithm.

We count this number by simulations over random plaintexts and keys and by repeating this procedure and considering the average number of these pairs we expect that these events are described by some Gaussian distribution with the mean and standard deviation computed after running many simulations until the limit of the probability is obtained. This is essentially a simple application of the Central Limit Theorem. Thus, it is a non-trivial optimization steps to find the best possible input-output relations which result in comparatively good probabilities of the propagation we study. For each encryption standard we need to derive some ad-hoc heuristics derived from the specific structure in order to have a speed-up in this procedure.

We formalize this new framework inspired from the work of Courtois and Mourouzis for constructing statistical distinguishers based on truncated differentials for GOST block cipher and some of its variants [8, 9]. As a proof of concept, we apply this combined framework using simple toy example ciphers and show that this combination leads to stronger statistical distinguishers. In addition, we discuss how this technique can be used in cryptanalysis of hash functions since the attack has full control over the key and thus working in a related-key scenario makes more sense.

References

[1] Don Coppersmith, *The Data Encryption Standard (DES) and its strength against attacks* , IBM Journal of Research and Development 38 (3): 243. doi:10.1147/rd.383.0243, 1994.

[2] Eli Biham and Adi Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, ISBN: 0-387-97930-1, 3-540-97930-1, 1993.

[3] Eli Biham and Adi Shamir, *Differential cryptanalysis of the full 16-round DES* , In Advances in Cryptology, CRYPTO 92, E. F. Brickel, Ed.,vol. 740 of Lecture Notes in Computer Science, pp. 487 496, 1992.

[4] Mitsuru Matsui, *The first experimental cryptanalysis of the data encryption standard*, Advances in Cryptology, CRYPTO, 1994.

[5] Mitsuru Matsui, *Linear cryptanalysis method for DES cipher*, Advances in Cryptology, EUROCRYPT, 1993.

[6] Lars Knudsen, *Truncated and higher order differentials* , In Fast Software Encryption, pp. 196-211, Springer Berlin Heidelberg, 2011.

[7] Lars Knudsen and Matthew Robshaw, *The Block Cipher Companion* , Springer Berlin Heidelberg, 1995.

[8] Nicolas T. Courtois and Theodosis Mourouzis, *Enhanced Truncated Differential Cryptanalysis of GOST*, In SECRYPT, 2013.

[9] Nicolas T. Courtois and Theodosis Mourouzis, *Propagation of Truncated Differentials in GOST* , In SECURWARE, 2013.

[10] Theodosis Mourouzis, *Optimizations in Algebraic and Differential Cryptanalysis* , PhD Thesis, University College London , 2014.

[11] Gregory Bard, *Algorithms for Solving linear and polynomial systems of equations over finite fields to cryptanalysis*, PhD Thesis, 2007.

[12] Martin R. Albrecht, *Algorithmic Algebraic Techniques and their Application to Block Cipher Cryptanalysis*, PhD Thesis Dissertation, Royal Holloway, University of London, 2010.

[13] Dmitry Khovratovich and Ivica Nikolic, *Rotational Cryptanalysis of ARX*, University of Luxembourg, 2010.