Literature Review

ADAM JOHNSTONE - GLJD44

October 2024

1 Literature Review

In this document, I will give a brief overview of my project and then discuss other work in a similar field or work that I will be directly using within my project. I will then draw some conclusions from the existing work I have found and relate it to my project.

The main aim of my project is to answer the research question 'Is the Sandwich Attack a feasible method for breaking the GOST block cipher?'. Although this is my main aim, I will take steps before answering the question to prove my understanding of the subject area. I have chosen to undertake this project as there is very little in terms of published articles implementing the Sandwich Attack and as far as I can tell there has yet to be an implementation of it on the GOST block cipher, hence I will hopefully be performing brand new research.

1.1 Term definition

Throughout this paper, I will be referring to a variety of cryptological terms that readers may be unfamiliar with. In this section, I will define some of the terms that will be mentioned later in the document.

1.1.1 Feistel Cipher

When constructing a block cipher, it is common for the 'main' encryption part of the machine to be created using a Feistel cipher [19]. Named and designed by Horst Feistel, who did pioneering research whilst working for IBM, a Feistel cipher (also called a Feistel network) is a symmetric key algorithm that splits one of its inputs in half and then performs multiple 'rounds' on it and its second input, known as the key, to encrypt the original input. Within each round half of the split input is passed through a pseudorandom function, called the round function, alongside the key to 'scramble' the bits of the input half. The other half is then XOR'ed with the output from the round function and finally, the halves are swapped (left becomes right and right becomes left). Figure 1 [19] showcases the process of performing the round function on a Feistel network.

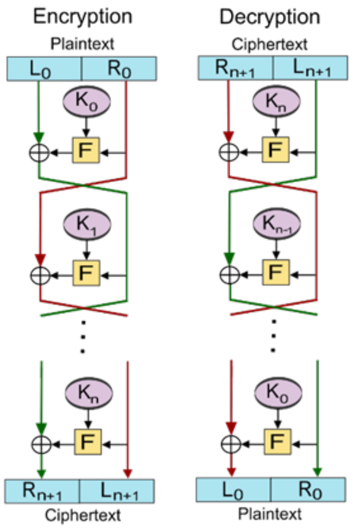


Figure 1: Feistel Network Diagram

1.1.2 S-Boxes

Used in block ciphers to help obey Shannon's property of confusion substitution boxes (S-boxes) are mathematically non-linear vectorial Boolean functions [26]. However, in general, an S-box takes some number of input bits, m, and transforms them into some number of output bits, n. In this instance m doesn't have to be equal to n for example DES takes a 6-bit input and produces a 4-bit output. S-boxes are used to help obscure the relationship between the plaintext and the ciphertext and to provide nonlinearity so that a block cipher cannot be trivially decrypted.

1.2 Block Ciphers

As part of my project, I have chosen to look at block ciphers which are a type of private key cryptosystem that operate on fixed-length groups of bits, known as blocks [14]. These block ciphers take a binary input string and then use an operation, for example, a Feistel cipher, to encrypt this input using a chosen second input called a key. In cryptography, these inputs are known as plaintexts and the outputs are called ciphertexts. In this section, I will primarily talk about three block cipher namely DES, KASUMI and GOST.

1.2.1 DES

The Data Encryption Standard (DES) (First released inn FIPS-46) is a block cipher developed in the early 1970s by IBM that utilises a balanced Feistel network of 16 rounds to encrypt 64-bit data blocks using a 56-bit key [16]. Although originally being derived from the block cipher Lucifer, developed by Horst Feistel, DES was modified by the NSA (National Security Agency) to be more resistant to differential attacks before it was accepted as a national encryption standard in 1976. Despite being more resistant to differential cryptanalysis, DES was also made to be weaker against brute force attacks by the NSA as they wanted to be able to break DES if it ever became necessary. Although upon release DES was known to not be completely secure it has since been proven that it is no longer a viable method of encryption. Notably in 1998 the EFF DES cracker (aka Deep Crack) [18] could brute force a DES key in a matter of days. Hence in 2005 it was withdrawn from the encryption standard and replaced with a new block cipher called AES (Advanced Encryption Standard) [13]. Despite this, some alternate versions of DES exist that are still considered secure such as TripleDES [27]. Although not used as an encryption standard any more DES is still an area of interest for researchers as it can give them a reliable benchmark for new attacks or potentially provide them with information about how AES will react to an attack. Although I won't directly be using DES within my project, I think that it will be useful to use as a comparative benchmark for my proposed attacks as significantly more research has been done on DES compared to KASUMI or GOST.

1.2.2 GOST

GOST is a Soviet and Russian government standard symmetric key block cipher developed in 1989 (originally called Magma) [21] but that has since had revisions and is still used today (now called Kuznyechik) [23]. GOST (an acronym derived from gosudarstvennyy standard which translates to government standard [20]) is similar to DES in that it is a 64-bit block size and utilises a Feistel network however some of the main differences between the two ciphers are listed below:

- GOST uses a key size of 256-bits
- GOST uses 32 rounds of the Feistel function
- The S-boxes of GOST take a 4-bit input and produce a 4-bit output
- The S-boxes of GOST can be changed

Despite these differing factors appearing to make GOST a more secure cipher compared to DES, it was found in 2011 that GOST could be broken quite easily and was even called a 'deeply flawed cipher' by Nicolas Courtois [7]. Although GOST has been considered broken, the attack that would perform this is infeasible. This is why I have chosen to use GOST for my project as I would like to see if the Sandwich Attack can either further break GOST or provide a more feasible attack on it. Alongside choosing GOST I am also going to choose the S-boxes defined in the original publication of GOST [8] as this should provide the best comparison to the first 'retro' version of GOST (aka Magma).

1.2.3 KASUMI

KASUMI is a Feistel network block cipher developed for use in mobile communications for 3GPP in 1995 (3rd Generation Partnership Project) [22]. Based on the MISTY1 cipher [24] KASUMI uses 128-bit keys, 64-bit blocks and generally uses 8 rounds of its Feistel function. Although it was developed to be stronger than MISTY1 (as mentioned in [4]) in 2010 Dunkleman et al. showed that it was weaker than MISTY1 [9].
The paper [9] is where I have taken a lot of the inspiration for this project as it is the first introduction of the Sandwich Attack. As such I will be trying to replicate the findings from [9] before trying to apply the Sandwich Attack to the GOST block cipher. I will go into more detail about the Sandwich Attack later in this document.

1.3 Types of Attack

Within this section, I will provide a very basic overview of some of the attacks, and their related predecessors, that I will use within my project.

1.3.1 Differential Attacks

In its broadest sense, differential attacks (or differential cryptanalysis) is the study of how differences in an input can affect the resulting differences in the output. When talking about block ciphers specifically it refers to the techniques used to trace differences through the cipher to try and discover where the cipher exhibits non-random behaviour and then exploiting those properties to retrieve the secret key [17]. The discovery of Differential cryptanalysis is generally attributed to Biham and Shamir where in [3] they proposed an attack on DES in the late 1980's. However, it was later revealed by Coppersmith that IBM had known about differential cryptanalysis since 1974 [6]. Differential cryptanalysis is usually a chosen plaintext attack meaning that an attacker must be able to obtain some ciphertext output from a set of plaintexts they have chosen. The basic version of the attack relies on pairs of plaintexts related by a constant difference (usually XOR). The attacker then computes corresponding pairs of ciphertexts and their differences hoping to discover patterns in their distributions that lead to the cipher being distinguished from random. The resulting pair of differences is called a differential. However, in the basic version of the key recovery attack, the attacker is instead trying to ascertain the secret key used in the cipher. Since its (re)discovery differential cryptanalysis has been the building block for most modern differential techniques.

1.3.2 Boomerang Attack

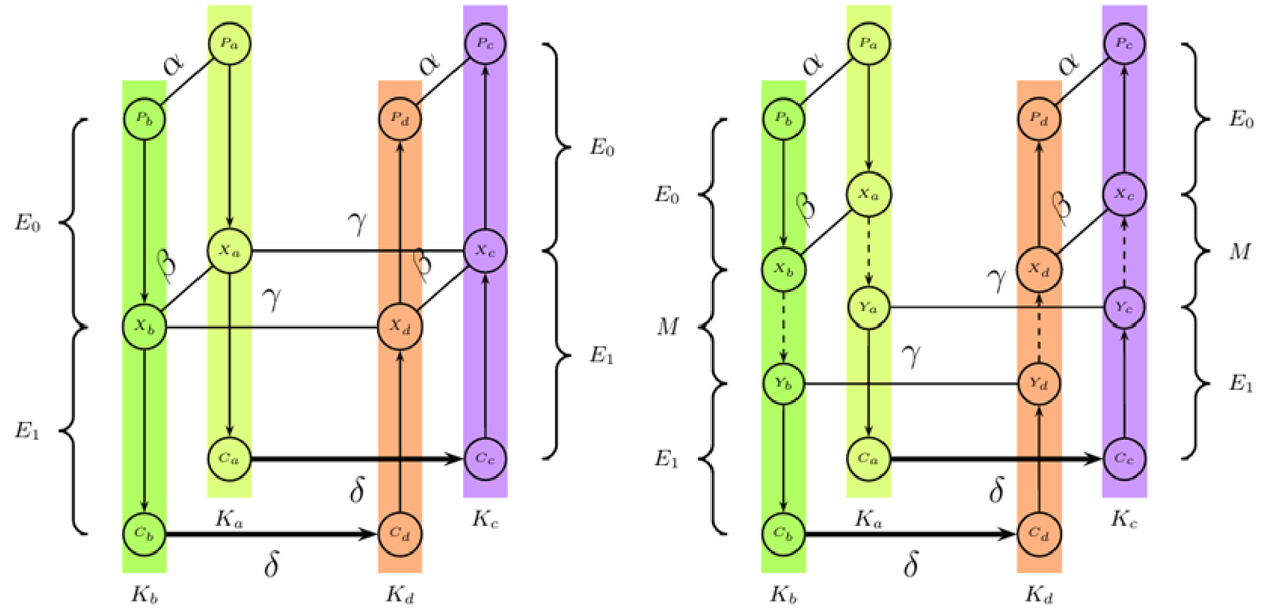
One such attack that builds upon the differential attack is known as a boomerang attack. First proposed in [12] by Wagner in 1999 the Boomerang attack splits the cipher into two consecutive stages allowing for a differential that doesn't have to cover the entire cipher and instead only needs to cover part of it [15]. During the attack, a so-called 'quartet' structure is attempted to be generated at the midpoint of the cipher. Since its release the Boomerang attack has seen lots of use and in some cases produces very good results for attacks on block ciphers as seen in [5] [2] [10]. Although most of these attacks are variants of the original Boomerang such as Rectangle attacks or amplified Boomerang attacks, they are mostly what is known as Related Key Boomerang attacks, which although similar to Boomerang are a little different.

1.3.3 Related Key Attacks

First proposed by Biham in [1] a related key attack is a form of cryptanalysis where an attacker can see how a cipher works under a set of initially unknown keys but where a mathematical relationship connecting the keys is known [25]. Generally, these attacks are applied alongside other attacks creating things such as related key differential attacks, or the previously mentioned related key boomerang attack.

1.3.4 Sandwich Attack

Although initially presented in 2010 by Dunkelman et al. [9] the Sandwich Attack has seen very little usage over the years with the only other paper being by Jana et al. [11]. As such these papers are the only source of information on how the attack works. However, the Sandwich attack is a follow-on from a Related Key Boomerang Attack so some of the workings of the attack can be ascertained from that. In [9] they initially describe the Sandwich Attack by first explaining a Boomerang attack and then advancing into the Sandwich attack. As mentioned before in a Related Key Boomerang Attack the cipher is split into two consecutive sections, however, in the Sandwich attack the cipher is now split into three cascading sub ciphers where the middle section (referred to as the filling) only operates on one round of the cipher but provides more information about the differentials than previously. The diagram below, Figure 2, (taken from [9]) shows the basic quartet structure for both a Related Key Boomerang and the (Related Key) Sandwich attacks. On the diagram to the right (Sandwich), it is clear to see where the extra middle stage has been added to the process and subsequently how it differs from the Related Key Boomerang (left).



A Related-Key Boomerang Quartet

A Related-Key Sandwich Quartet

Figure 2:

1.4 Conclusions

From the themes and papers I have mentioned above, it is clear to me that the project I have chosen will be quite complex. However, I believe that because of the distinct lack of information and usage surrounding the Sandwich Attack, I could be contributing new and potentially groundbreaking research into the field of cryptography by applying it to the GOST block cipher. However, due to its complexity and my current understanding being limited, a Sandwich Attack on GOST may be infeasible and as such my contributions to the community will be changed to be more informative about the Sandwich Attack rather than displaying its effectiveness.

References

[1] Eli Biham. New types of cryptanalytic attacks using related keys. *J. Cryptology*, 7:229–246, 1994.

[2] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. volume 3494, pages 507–525, 01 2005.

[3] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *Advances in Cryptology-CRYPTO' 90*, pages 2–21, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[4] Alex Biryukov. Block ciphers and stream ciphers: The state of the art. Cryptology ePrint Archive, Paper 2004/094, 2004.

[5] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 1–18, Tokyo, Japan, December 6–10, 2009. Springer Berlin Heidelberg, Germany.

[6] D. Coppersmith. The data encryption standard (des) and its strength against attacks. *IBM Journal of Research and Development*, 38(3):243–250, 1994.

[7] Nicolas T. Courtois. Security evaluation of GOST 28147-89 in view of international standardisation. Cryptology ePrint Archive, Paper 2011/211, 2011.

[8] Vasily Dolmatov and Dmitry Baryshkov. GOST R 34.12-2015: Block Cipher "Magma". RFC 8891, September 2020.

[9] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 393–410, Santa Barbara, CA, USA, August 15–19, 2010. Springer Berlin Heidelberg, Germany.

[10] Orr Dunkelman, Nathan Keller, and Ariel Weizman. Practical-time related-key attack on GOST with secret S-boxes. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, Part III*, volume 14083 of *Lecture Notes in Computer Science*, pages 177–208, Santa Barbara, CA, USA, August 20–24, 2023. Springer, Cham, Switzerland.

[11] Amit Jana, Mostafizar Rahman, Dhiman Saha, and Goutam Paul. Switching the top slice of the sandwich with extra filling yields a stronger boomerang for nlfsr-based block ciphers. *IACR Cryptol. ePrint Arch.*, page 1543, 2023.

[12] David Wagner. The boomerang attack. In Lars Knudsen, editor, *Fast Software Encryption*, pages 156–170, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[13] Wikipedia. Advanced Encryption Standard — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Advanced\%20Encryption\%20Standard&oldid=1254420717`, 2024. [Online; accessed 31-October-2024].

[14] Wikipedia. Block cipher — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Block\%20cipher&oldid=1251388783`, 2024. [Online; accessed 31-October-2024].

[15] Wikipedia. Boomerang attack — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Boomerang\%20attack&oldid=1180520039`, 2024. [Online; accessed 31-October-2024].

[16] Wikipedia. Data Encryption Standard — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Data\%20Encryption\%20Standard&oldid=1250616539`, 2024. [Online; accessed 31-October-2024].

[17] Wikipedia. Differential cryptanalysis — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Differential\%20cryptanalysis&oldid=1244199191`, 2024. [Online; accessed 31-October-2024].

[18] Wikipedia. EFF DES cracker — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=EFF\%20DES\%20cracker&oldid=1142041366`, 2024. [Online; accessed 31-October-2024].

[19] Wikipedia. Feistel cipher — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Feistel\%20cipher&oldid=1241213256`, 2024. [Online; accessed 31-October-2024].

[20] Wikipedia. GOST — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=GOST&oldid=1253003087`, 2024. [Online; accessed 31-October-2024].

[21] Wikipedia. GOST (block cipher) — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=GOST\%20(block\%20cipher)&oldid=1218930816`, 2024. [Online; accessed 31-October-2024].

[22] Wikipedia. KASUMI — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=KASUMI&oldid=1180505772`, 2024. [Online; accessed 31-October-2024].

[23] Wikipedia. Kuznyechik — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Kuznyechik&oldid=1253230113`, 2024. [Online; accessed 31-October-2024].

[24] Wikipedia. MISTY1 — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=MISTY1&oldid=1167898987`, 2024. [Online; accessed 31-October-2024].

[25] Wikipedia. Related-key attack — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Related-key\%20attack&oldid=1185994698`, 2024. [Online; accessed 31-October-2024].

[26] Wikipedia. S-box — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=S-box&oldid=1182341130`, 2024. [Online; accessed 31-October-2024].

[27] Wikipedia. Triple DES — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Triple\%20DES&oldid=1250575091`, 2024. [Online; accessed 31-October-2024].