Aalto University
School of Science
Degree Programme in Information and Computer Science

Md. Mohsin Ali Khan

Statistical Model of the Statistical Saturation Attack

Master's Thesis
Espoo, May 26, 2015

Supervisors: Professor Kaisa Nyberg, Aalto University
Advisor: Professor Kaisa Nyberg, Aalto University

Aalto University
School of Science
Degree Programme in Information and Computer Science

ABSTRACT OF MASTER'S THESIS

Author:	Md. Mohsin Ali Khan		
Title:	Statistical Model of the Statistical Saturation Attack		
Date:	May 26, 2015	**Pages:**	77
Major:	Foundations of Advanced Computing	**Code:**	T-79
Supervisors:	Professor Kaisa Nyberg		
Advisor:	Professor Kaisa Nyberg, Aalto University		

The statistical saturation attack (SSA) introduced by Collard and Standaert focuses on the non-uniformity of certain bits in the ciphertext space by fixing certain bits in the plaintext space. It exploits this non-uniformity by distinguishing an observed distribution among two known distributions: one is uniform and the other is non-uniform. To do so, a statistical test, based on a statistical distinguisher is required. There exists such statistical distinguishers based on the links in between SSA and other statistical cryptanalytic techniques. Instead of using such links, in this thesis we look directly in SSA and develop a statistical distinguisher and propose a statistical test based on this distinguisher. The statistical distinguisher denoted by T is primarily χ^2 distributed. Theoretical approximation of the distribution of T is derived in terms of the size and capacity of the distribution considering both of the cases of a single fixation and a set of fixations. The developed model is applied on SMALLPRESENT-[4] for the case of single fixation and the evolution of the distinguisher is observed both theoretically and experimentally as the number of encrypted plaintexts increases. In addition to this, a connection between the error probability of the statistical test and the number of required plaintexts (in other words data complexity) is also presented and showed that this theoretical data complexity is in close correspondence to the observed data complexity in the experiments on SMALLPRESENT-[4].

Keywords:	block cipher, statistical cryptanalysis, statistical saturation attack, probability distribution, capacity, statistical test, distinguishing attack
Language:	English

Acknowledgements

I would like to express my gratitude to my supervisor Professor Kaisa Nyberg for the guidance, useful comments, remarks and the way she has engaged me through the learning process of this master's thesis. She has always been very patient and quick in responding any of my query in email. Furthermore, I would like to thank my friend Jarno Niklas Alanko to help me understanding different kind of mathematics required for various courses during my studies which eventually helped me to acquire the maturity of writing a thesis.

Espoo, May 26, 2015

Md. Mohsin Ali Khan

Abbreviations and Acronyms

ML	Multidimensional Linear
TD	Truncated Differential
SS	Statistical Saturation
SSA	Statistical Saturation Attack
SPN	Substitution Permutation Network
a	A constant value at the input of an SS trail known as *fixation* of the trail input
η	A constant value at the output of an SS trail known as *output* or value at the trail output
A	Set of a
$\mathcal{F}$	Set of A
ϕ	A set of values at the non-trail input known as *sample*
Φ	Set of ϕ
μ_x	Mean of the random variable x
σ_x^2	Variance of the random variable x
$T_a : \Phi \to \mathbb{R}$	A mapping from a set of samples to the set of real numbers for a given value a used for all samples; also called as statistic T for a fixed fixation
$T_A : \Phi \to \mathbb{R}$	A mapping from a set of samples to the set of real numbers such that $T_A(\phi) = \sum_{a \in A} T_a(\phi)$. For all the samples $\phi \in \Phi$, the domain of a remains constant to A; also called as statistic T for a fixed set of fixation
$T : \Phi \times A \to \mathbb{R}$	A mapping from a set of samples and a set of fixations to the set of real numbers; also called as statistic T for a variable fixation
$T : \Phi \times \mathcal{F} \to \mathbb{R}$	A mapping from a set of samples and a set of subsets of fixations to the set of real numbers such that $T(\phi, A) = \sum_{a \in A} T(\phi, a)$; also called as statistic T for a variable set of fixation

Contents

Chapter 1

Introduction

A wide range of cryptanalytic techniques have been developed and applied on different kinds of information systems throughout the history. This thesis work focuses on a specific type of statistical cryptanalysis of symmetric key cryptosystems. More specifically, it analyses the SSA on a certain kind of block ciphers. Among the various different kinds of known statistical cryptanalysis techniques, linear and differential cryptanalysis now have been quite familiar and even taught in university courses. In addition, different variants of these techniques namely multidimensional linear (ML), truncated differential (TD) cryptanalysis have also been invented in the past decades. Statistical model of the statistics used in these cryptanalytic techniques are available including their data and time complexities in parallel with their error probabilities.

The statistics used in the linear and differential cryptanalysis are the *correlation* of a linear approximation and the *differential probability* of a plaintext-ciphertext differential, respectively [4]. Over the past few decades, different researchers have published links among the statistics of different cryptanalytic techniques. Chabaud and Vaudenay have shown that, differential probabilities and squared correlations are linked to each other by Walsh transform [8]. Blondeau and Nyberg have shown various links between TD and ML [4, 5]. Although statistical saturation (SS) is a relatively new kind of statistical cryptanalytic technique proposed by Collard and Standaert [11], few attempts have already been made by researchers to link SSA with other statistical cryptanalytic techniques so that the already known statistical models can be used to apply SSA. Blondeau and Nyberg have shown links in between TD and SS [5] attacks and have given a model for the SSA based on the existing model of the TD attack. Leander have shown that there is a mathematical link between SSA and ML cryptanalysis [13]. However, any concrete statistical model of SSA is yet to be developed. In this work, instead of using any link with other statistical cryptanalytic techniques, we look at SSA directly and develop a statistical model.

As explained in [11], in SSA, the plaintext space is partitioned into two parts. One part is fixed to a chosen value while the other part iterates over all the possible values. The ciphertext space is also partitioned into two parts. As the variable part of the plaintext space iterates over different values, the distribution of one part of the ciphertext space is observed. If the plaintext and ciphertext spaces are partitioned considering relevant weakness of the block cipher then it is possible to gain some insight of the cipher. Because of this non-uniform distribution of these chosen plaintexts, after a sufficient number of encryption of them, the one part of the corresponding ciphertexts also shows non-uniform distribution. The technique to find such a weakness is a different problem and out of scope of this thesis. Nevertheless, we have discussed the basic principles of finding such a weakness in the Chapter 2. However, we mostly focus on how to exploit such a non-uniformity extracted from the found weakness. In the original paper of Collard and Staendart [11], they have suggested two approaches to exploit this non-uniformity to reveal the secret key partially. In the first approach the attacker calculates all the ciphertext distributions for all possible keys and stores them in a table. That is, the table stores separate distributions for each key. Then it finds the distribution from this table that minimizes the distance with the distribution computed from a secret key. The corresponding key of that distribution in the table is then assumed to be the secret key. Computing this table is costly and the second approach solves the problem by introducing a distinguishing attack using last round trick. If the cipher has r rounds, then the ciphertexts are partially decrypted through the last round only by all the parital keys. The key that produces ciphertext distribution which has maximum distance from uniform distribution is assumed to be a part of the correct key. Indeed, otherwise any wrong key will make the ciphertext distribution to be more uniform. We look at this distingushing attack and find a statistic that can be used to distinguish the ciphertext distribution from random. And then we also find the model that shows the data complexity, that is, the number of required plaintext-ciphertext pairs so that the computed statistic can reach to a value that is able to distinguish the distribution from random with a significantly low error probability.

The statistic used to analyze this distribution is χ^2 distributed which is denoted in this thesis by T. Given a T computed from a sample, we apply a statistical test to identify if T is random or it follows some other known distribution of a known block cipher. The distribution of the statistic T for a cipher is then theoretically approximated considering different kinds of fixations in the plaintext space. It is approximated for any arbitrarily fixed fixation, for variable fixation, for arbitrarily fixed set of fixations, and for variable set of fixations.

In Chapter 2, the block cipher and SSA is formally defined. We have discussed the definition and properties of different kind of statistical distributions in Chapter 3. The concept of statistical tests that can distinguish an observed distribution in between two given distributions is also discussed in this chapter. In Chapter 4 we present the derivations of different T in detail. In Chapter 5, we have derived the data complexity of SSA. Chapter 6 has been dedicated to the experiments that show the validity of the models. Finally in Chapter 7, we conclude the thesis.

Chapter 2

Block Cipher Cryptanalysis

2.1 Cryptosystem

Definition 2.1.1. *[20]A cryptosystem is a five-tuple* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *where the following conditions are satisfied:*

1. $\mathcal{P}$ *is a finite set of plaintexts;*
2. $\mathcal{C}$ *is a finite set of ciphertexts;*
3. K*, the keyspace, is a finite set of keys;*
4. *For each* $K \in \mathcal{K}$ *there is an encryption rule* $e_K \in \mathcal{E}$ *and a corresponding decryption rule* $d_K \in \mathcal{D}$*. Each* $e_K : \mathcal{P} \to \mathcal{C}$ *and* $d_K \in \mathcal{D} : \mathcal{C} \to \mathcal{P}$ *are functions such that* $d_K(e_K(x)) = x$ *for every plaintext* $x \in P$*.*

That means, a cryptosystem is a set of injective mappings from a finite set of plaintexts to a finite set of ciphertexts. Each key is associated with exactly one mapping. When the plaintext and the ciphertext space are equal the injective mappings are bijective. Figure 2.1 shows a very high level picture of a cryptosystem. However, in this work, the terms *cryptosystem* and *cipher* have been used interchangeably.

From the key management point of view, cryptosystems can be classified into two categories. One is public key cryptosystem and the other is symmetric

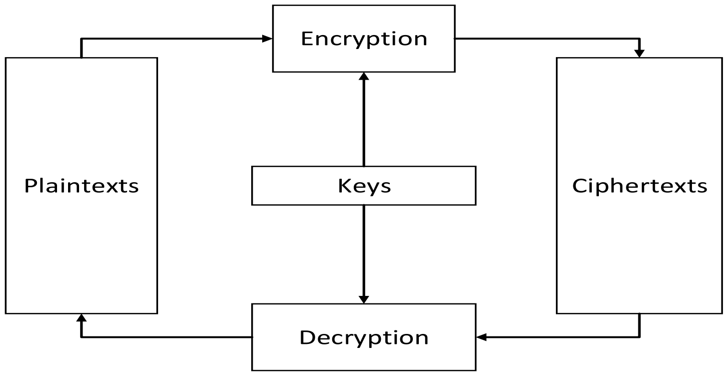

Figure 2.1: A basic cryptosystem

key cryptosystem. In public key cryptosystem, the sender encrypts the message by the receiver's public key before sending it. The encrypted message can only be decrypted by the receiver's private key. The security of a public key cryptosystem depends on some computationally hard problems. Among many others, such difficult mathematical problems include discrete logarithm and integer factoring. RSA is a widely known, studied and used public key cryptosystem that uses the hardness of integer factoring as the basis of its security. In a symmetric key cryptosystem, both of the sender and the receiver share the same key which is secret from everyone else. This secret key is used to both encrypt and decrypt the message. Figures 2.2 and 2.3 give a very high level view of a symmetric and public key cryptosystem. In both of the figures, Alice is the sender and Bob is the receiver. The security of such symmetric key cryptosystem primarily depends on its randomness, size of ciphertext space and key-length. Block ciphers and stream chiphers are examples of symmetric key cryptosystems. This thesis focuses on block ciphers.

2.2 Block Cipher

Block cipher is a symmetric key encryption system. The lowest level of granulairty of the encryption system is a block of bits. That is, the data to be encrypted is split into blocks x_i of fixed length n where $i \in \mathbb{N}$. A typical value of n is 128. And then it encrypts the whole block as a single plaintext and produce the ciphertext of the same length as the plaintext. Generally it

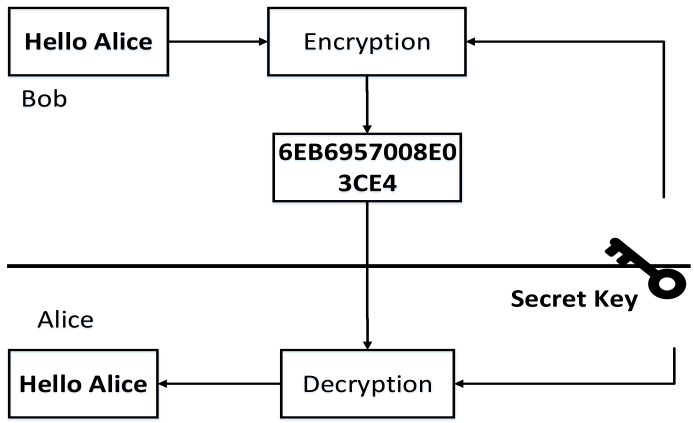

Figure 2.2: Symmetric key cryptosystem

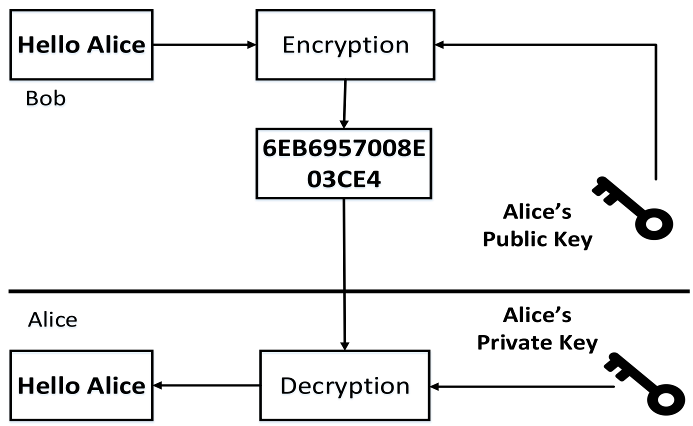

Figure 2.3: Public key cryptosystem

can be written as

$$\begin{aligned} \mathcal{P} &= \mathcal{C} = \mathbb{Z}_2^n \\ \mathcal{K} &= \mathbb{Z}_2^l \end{aligned}$$

For every $k \in \mathcal{K}$ there exists a bijective mapping $E_k : \mathcal{P} \to \mathcal{C}$. Generally, the mapping E_k consists of repetitive applications of same set of operations. Each repetition is called a round. In each round the cipher often uses a different key which is called the round key. If a block cipher has r number of rounds then there will be r number of round keys denoted by $k^1, ..., k^r$ and the list of these keys, $(k^1, ..., k^r)$ is called the key schedule. The round keys are generated from a master key k by a fixed key generation algorithm. This key generation algorithm is public. The first round of the cipher takes the plaintext as its input. The output of each round is considered as the input of the next round. The output of the final round is the ciphertext. If we

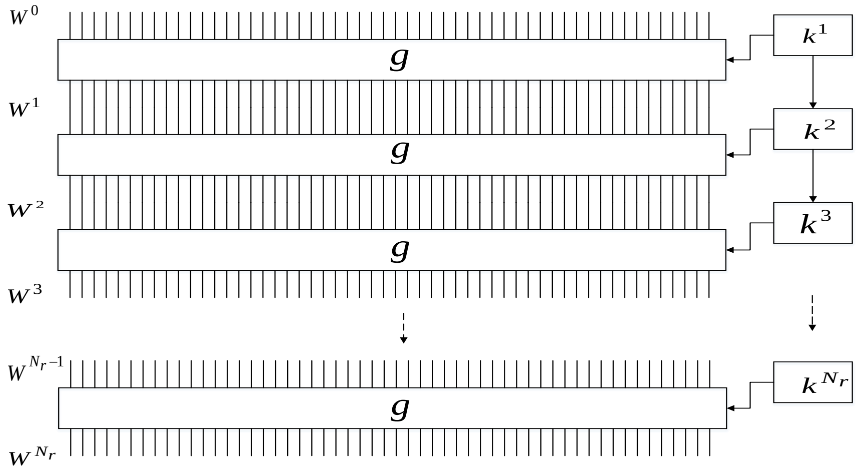

Figure 2.4: A block cipher

denote the plaintext x by W^0 and the ciphertext $E_k(x) = y$ by W^r and the round function as $g : \mathcal{P} \times \mathcal{K} \rightarrow \mathcal{C}$, then the encryption of a block cipher can be computed by the Algorithm 1. Figure 2.4 shows the operation pictorially.

Algorithm 1 : $E(x, (k^1, ..., k^r))$

$W^0 \leftarrow x$
for $i \leftarrow 1$ **to** r **do**
  $W^i \leftarrow g(W^{i-1}, k^i)$
end for
return W^r

Decryption is applying the inverse of the function g at every round. As we start from the ciphertext, we have to use the key in the reverse order. That is, we have to calculate $W^{r-1} = g^{-1}(W^r, k^r)$. Note that, g has to be an injective mapping, otherwise g^{-1} is not well defined. Using this process, we can decrypt the cipher by the Algorithm 2. However, based on the detail of function g and the data structure used to hold the states, there are different kinds of block ciphers. The simplest one among those is SPN (Substitution-

Algorithm 2 : $D(y, (k^1, ..., k^r))$

$W^r \leftarrow y$
for $i \leftarrow r$ **to** 1 **do**
  $W^{i-1} \leftarrow g^{-1}(W^i, k^i)$
end for
return W^0

Permutation Network). In this thesis, SSA is experimented on an SPN named PRESENT. In the following section SPN is discussed in detail.

2.2.1 Substitution-Permutation Networks

Definition 2.2.1. *[19] Let a, m and r be positive integers, let $\pi_s : \{0,1\}^a \rightarrow \{0,1\}^a$ be a substitution, and let $\pi_p : \{1, ..., am\} \rightarrow \{1, ..., am\}$ be a permutation. Let $\mathcal{P} = \mathcal{C} = \{0,1\}^{am}$, and let $\mathcal{K} \subseteq (\{0,1\}^{am})^{r+1}$ consist of all possible key schedules that could be derived from an initial key k using the key scheduling algorithm. For a key schedule $(k^1, ..., k^{r+1})$, the encryption of plaintext is computed as Algorithm 3*

Algorithm 3 : $SPN(x, \pi_s, \pi_p, (k^1, ..., k^{r+1}))$

$W^0 \leftarrow x$
for $r \leftarrow 1$ **to** $r-1$ **do**
  $u^r \leftarrow W^{r-1} \oplus k^r$
  for $i \leftarrow 1$ **to m do**
    $v^r_{<i>} \leftarrow \pi_s(u^r_{<i>})$
  end for
  $W^r \leftarrow (v^r_{\pi_p(1)}, ..., v^r_{\pi_p(am)})$
end for
$u^r \leftarrow W^{r-1} \oplus k^r$
for $i \leftarrow 1$ **to m do**
  $v^r_{<i>} \leftarrow \pi_s(u^r_{<i>})$
end for
$y \leftarrow v^r \oplus k^{r+1}$
return y

Given an am bit binary string, say $x = (x_1, ..., x_{am})$, can be regarded as the concatenation of m number of a-bit substrings, which can be denoted by

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Table 2.1: Substitution function $\pi_S : \{0,1\}^4 \to \{0,1\}^4$

z	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\pi_P(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Table 2.2: Permuation function:$\pi_P : \{0,1,...,15\} \to \{0,1,...,15\}$

$x_{<1>},...,x_{<m>}$. Thus

$$x = x_{<1>}||\cdots||x_{<m>}$$

and for $1 \leq i \leq m$, we have that

$$x_{<i>} = (x_{(i-1)a+1},...,x_{ia})$$

The SPN consists of r rounds. In each round (except for the last round, which is slightly different), we perform m substitutions using π_s, followed by a permutation using π_p. Prior to each substitution operation, we incorporate the round key bits via a simple XOR operation, this is called round key mixing. In Algorithm 3, u^r is the input to the S-boxes in round r, and v^r is the output of the S-boxes after round r. W^r is obtained from v^r by applying the permutation π_P, and then u^{r+1} is constructed from W^r by XOR-ing with the round key k^{r+1} . In the last round, the permutation π_P is not applied. Now, we present an SPN as an example.

Example 2.2.1. *[19] Suppose that $a = m = r = 4$. Let π_S and π_P be defined by Table 2.1 and 2.2 respectively, where the input of π_S are written in hexadecimal notation,* $(0 \leftrightarrow (0,0,0,0), 1 \leftrightarrow (0,0,0,1), ..., 9 \leftrightarrow (1,0,0,1), A \leftrightarrow (1,0,1,0), ..., F \leftrightarrow (1,1,1,1))$.

See Figure 2.5 for a pictorial representation of this particular SPN. In this diagram, we have named the S-boxes S_i^r $(1 \leq i, r \leq 4)$. All 16 S-boxes incorporate the same substitution function based on π_S.

In order to complete the description of the SPN, we need to specify a key scheduling algorithm. Here is a simple possibility: suppose that we begin with a 32-bit key $k = (k_1, ..., k_{32}) \in \{0,1\}^{32}$. For $1 \leq r \leq 5$, define k^r to consist of 16 consecutive bits of k, beginning with k_{4r-3}. This may not be a very secure way to define a key schedule; we have just chosen something easy for purposes of illustration.

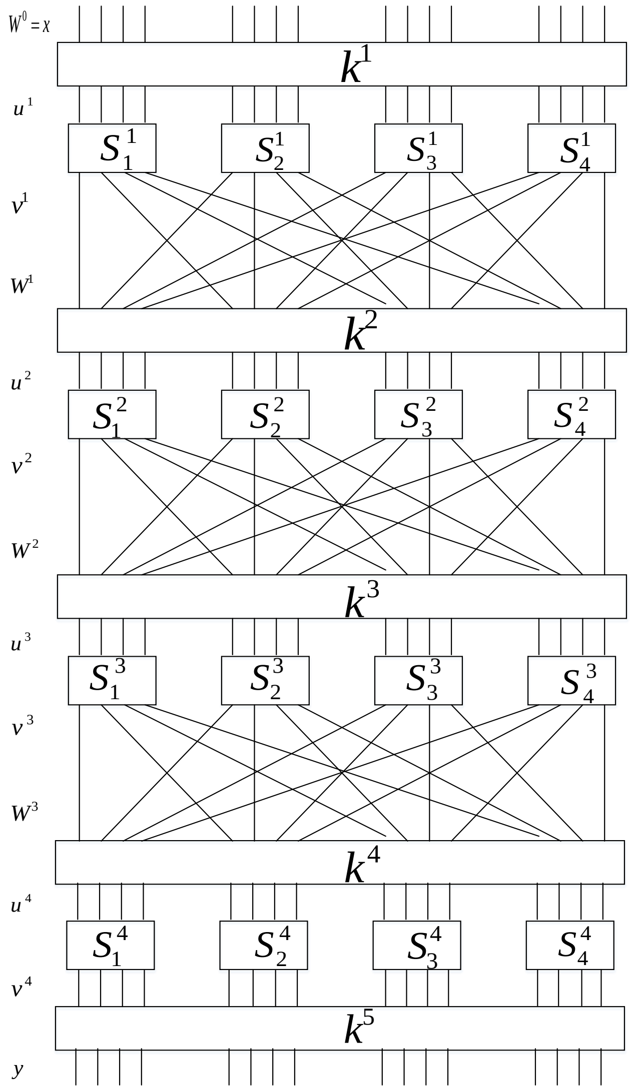

Figure 2.5: A substitution-permutation network

SPNs have simple and very efficient design, in both hardware and software. The SPN in Example 2.2.1 is not secure, if for no other reason that the key length (32 bits) is small enough that an exhaustive key search is feasible. However, "larger" SPNs can be designed that are secure against all known attacks. In this work, we use SPN as the test bed of the statistical model of SSA. As of now, we have defined cryptosystems, block ciphers and SPN. In

Section 2.3 we have discussed the general philosophy of statistical cryptnalysis of a block cipher and the state of the art in this field of research. Then we define the SSA formally. In Chapter 4, we start to derive our statistical model.

2.3 Cryptanalysis

National Security Agency (NSA) has defined cryptanalysis as the analytic investigation of an information system with the goal of illuminating hidden aspects of that system. It encompasses any systematic analysis aimed at discovering features in, understanding aspects of, or recovering hidden parameters from an information system [1].

This thesis work considers the information system to be a block cipher and the systematic analysis exploits the statistical properties of the cipher in question. The process we have followed is broadly known as statistical cryptanalysis. The process includes finding a statistic (preferably parametrized) computable from the cipher system which significantly deviates from the value of the same statistic computed in a uniformly random set up. The process also includes the task of finding the parameter that causes the statistic to deviate the most from random. As the statistic and the parameter is chosen, the cryptanalysis uses a large set of ciphertexts or plaintext-ciphertext pairs associated with the cipher in attack to compute the statistic. Comparing the value of this computed statistic with some known statistic can reveal other hidden information of the cipher. Depending on the statistic used and the way it is exploited, there are many different kinds of statistical cryptanalysis. Some of the very well known statistical cryptanalytic techniques include linear, ML, differential, TD, integral, and SS cryptanalysis.

In linear attacks, the statistic used is the correlation of a linear approximation. The linear approximation is obtained by applying a mask on the inputs and a mask on the outputs of the cipher. The correlation of the linear approximation is calculated by comparing how many times the function outputs 1 and how many times it outputs 0. Using this statistic, a cipher can be distinguished from random and the last round key can also be partially recovered. Over the years, cryptanalysts have found tricky ways to define this linear approximation. In ML attack, the linear approximation has multiple input and output masks. Based on their correlations, the theoretical distribution of partial plaintext-ciphertext pairs is computed. The input and output masks are chosen in a way so that the distribution deviates by large values from the uniform distribution.

On the other hand, in differential attacks, a different statistic is used. It considers the probability of a differential. That is, it checks the probability of pairs of plaintexts with some fixed difference to have certain fixed difference in their corresponding ciphertexts. If a differential is identified for a cipher which has a significantly different probability than in the random case, then that differential can be used to reveal other hidden information of the cipher. In general, the metric used to calculate the difference among the plaintext pairs and ciphertext pairs is bitwise XOR. Like linear cryptanalysis, differential cryptanalysis also has its variants. One such variant is truncated differential cryptanalysis. In TD attacks, the differential probability considers only certain bits of plaintexts and ciphertexts while ignoring the other bits.

In SSA, the statistic of the distribution of ciphertext or plaintext-ciphertext is considered. Certain bits of the plaintexts are kept fixed while the other bits can vary. SSA encrypts a large number of such plaintexts and exploits the distribution of certain bits of the corresponding ciphertexts. In Section 2.4, SSA is formally explained and in Chapter 4, the derivation of the statistical model of SSA is presented in detail. However, as Collard and Standaert applied this attack on the block cipher PRESENT, we also have selected PRESENT and its small versions [12] as the test bed of SSA. As a result, before discussing SSA in detail, it will be useful to discuss the specification of present PRESENT in brief.

2.4 PRESENT

PRESENT is a Substitution-Permutation Network with a block size of 64 bits designed by Bogdanov et al. [6] in 2007. The recommended key size is 80 bits, which should be sufficient for the expected applications of the cipher. However, a 128-bit key-schedule is also proposed. The encryption is composed of 31 rounds. Each of the 31 rounds consists of a non-linear substitution layer, a linear bitwise permutation layer and a bitwise XOR operation with round key K_i where $1 \leq i \leq 32$. Note that, K_{32} is used for postwhitening. The non-linear layer uses a single 4-bit S-box which is applied 16 times in parallel in each round. The linear permutation is defined by Table 2.3 where bit i of input is moved to bit position $P(i)$. The 4-bit

generateRoundKeys()
for $i = 1$ to 31 **do**
    addRoundKey(STATE,K_i)
    sBoxLayer(STATE)
    pLayer(STATE)
end for
addRoundKey(STATE,K_{32})

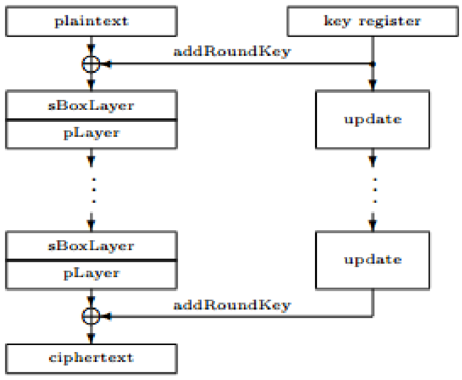

Figure 2.6: Top-level algorithmic description of PRESENT [11].

S-box is defined according to Table 2.4. We do not mention the key-schedule here as we do not make explicit use of it in our distinguishing attack. Figure 2.7 shows the substitution-permutation network pictorially for one round.

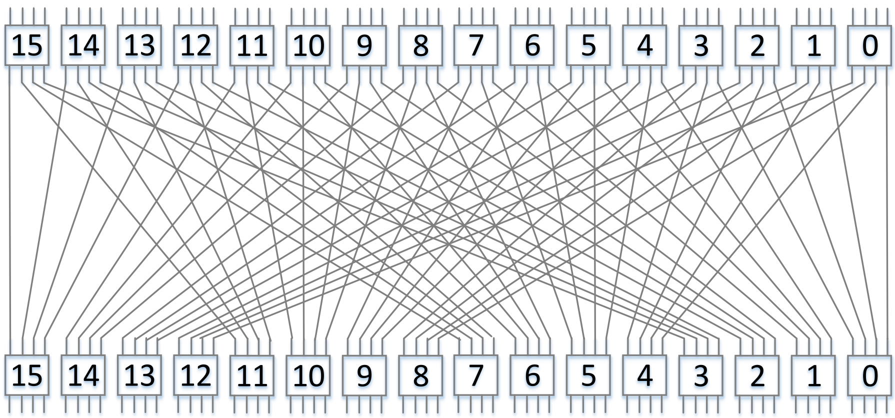

Figure 2.7: PRESENT SPN [11].

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$p(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$p(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$p(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$p(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	37	63

Table 2.3: Permutation layer of PRESENT

i	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[i]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Table 2.4: S-box of PRESENT (hexadecimal notation).

2.5 Non-linearity of the S-box in PRESENT

It is important for any block cipher to be non-linear to be immune against different kind of cryptanalytic attacks [3, 15]. PRESENT is not an exception. The S-box in PRESENT is a non-linear function. However, being non-linear is not a guarantee for the expected security. Cryptanalysts try to find out linear approximations of the non-linear function with sufficiently deviated correlation which eventually opens up a weakness of the cipher. A good S-box is the one which minimizes deviation of the correlations from zero for all the possible linear approximations. Correlation is a measure of the non-uniformity of a binary function. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a boolean function. Then the correlation of function f denoted by $\mathbf{cor}_x(f)$ is defined in [4] as its correlation with the all-zero function as following

$$\mathbf{cor}_x(f) \quad = \quad \frac{1}{2^n}\left[\#\left\{x \in \mathbb{F}_2^n \mid f(x) = 0\right\} - \#\left\{x \in \mathbb{F}_2^n \mid f(x) \neq 0\right\}\right] \tag{2.1}$$

A linear approximation $f : \mathbb{F}_2^n \to \mathbb{F}_2$ of a vectorial boolean function $\mathbf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is developed by considering an input and an output mask $\alpha, \beta \in \mathbb{F}_2^n$ in the following way

$$f_{(\alpha,\beta)}(x) \quad = \quad \alpha \cdot x \oplus \beta \cdot \mathbf{F}(x) \tag{2.2}$$

where the notation "·" represents standard inner product. The S-box used in PRESENT is a vectorial boolean function $S : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ mentioned in Table 2.1. So, given an input mask $\alpha \in \mathbb{F}_2^4$ and an output mask $\beta \in \mathbb{F}_2^4$, and a vectorial boolean function S, the correlation of the linear approximation $f_{(\alpha,\beta)} = \alpha \cdot x \oplus \beta \cdot S(x)$ is measured as follows:

$$\mathbf{cor}_x\left(f_{(\alpha,\beta)}\right) \quad = \quad \frac{1}{2^n}\left[\#\left\{x \in \mathbb{F}_2^n \mid f_{(\alpha,\beta)}(x) = 0\right\} - \#\left\{x \in \mathbb{F}_2^n \mid f_{(\alpha,\beta)}(x) \neq 0\right\}\right]$$

α/β	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	0	$\frac{1}{4}$	0	0	$-\frac{1}{2}$	0	$-\frac{1}{2}$	0	0	0	0	0	$-\frac{1}{2}$	0	$\frac{1}{2}$
2	0	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	$-\frac{1}{4}$	$\frac{1}{4}$
3	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{2}$	0	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{2}$	0	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$
; 4	0	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	$\frac{1}{2}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	$-\frac{1}{2}$	0	0	$-\frac{1}{4}$	$\frac{1}{4}$
5	0	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	0	0	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{2}$	0	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$
6	0	0	$-\frac{1}{4}$	0	0	$-\frac{1}{2}$	0	0	$-\frac{1}{2}$	0	0	$\frac{1}{2}$	0	0	0
7	0	0	$\frac{1}{4}$	$\frac{1}{2}$	0	0	0	0	$-\frac{1}{2}$	0	0	0	0	$\frac{1}{2}$	0
8	0	$\frac{1}{4}$	$-\frac{1}{4}$	0	0	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	0	0	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$
9	$\frac{1}{2}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{2}$	0	$-\frac{1}{4}$	$\frac{1}{4}$	0	0
A	0	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$-\frac{1}{4}$	$\frac{1}{4}$	0	0	$-\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$
B	$-\frac{1}{2}$	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$
C	0	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	0	0	$-\frac{1}{2}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$
D	$\frac{1}{2}$	$\frac{1}{2}$	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	0	0	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$
E	0	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0
F	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0	0

Table 2.5: Correlation table of S-box of PRESENT: $\mathbf{cor}_x\left(f_{(\alpha,\beta)}\right)$

The correlation table of the S-box of PRESENT is given in Table 2.5 [10]. We have discussed how this table helps in preparing an SSA in Section 2.7. In Chapter 6, we have shown in detail how this table helps in finding a feasible SSA attack on SMALLPESENT-$[n]$.

2.6 SSA

SSA is a chosen plaintext attack. It means the attacker has access to an encryption oracle and can encrypt any plaintext without knowing the encryption key. As the idea of SSA has already been mentioned in the introduction, we will now define it formally and discuss the basic principle of finding a weakness in a block cipher to mount an SSA.

Let the length of the input and the output block of the SPN is n. Then the set of plaintexts and ciphertexts can be considered as a set of vectors of length n defined over the field $\mathbb{F}_2$, that is $\mathbb{F}_2^n$. Let x^i denote the i-th element of the vector $x \in \mathbb{F}_2^n$. As the assumed weakness of the cipher suggests, we find four integers $s, t, q\ r$ such that $s + t = q + r = n$ and $B_s, B_t, B_q, B_r \subseteq [n]$ are subsets of all the possible bit positions. $|B_s| = s, |B_t| = t, |B_q| = q, |B_r| = r$ and $B_s \cap B_t = B_q \cap B_r = \emptyset$ and $|B_s \cup B_t| = |B_q \cup B_r| = \emptyset$.

That is, the bit positions are partitioned into two disjoint parts in possibly two different ways. Then the plaintexts are chosen in a way so that the bits in positions B_s are kept fixed while the bits in positions B_t vary. In this fashion, sufficiently large number of plaintexts are chosen and encrypted. Then from all the ciphertext achieved from this process is observed by focusing only on the bits in B_q. The distribution of the bits in B_q is supposed to be non-uniform enough to be used in a statistical test given that the plaintext and chiphertext space partition has been done based on a weakness. In this scenario, the sets B_s and B_q form what is called an SS trail. We call B_s as the input and B_q as the output of the trail.

2.7 Constructing an SS trail for PRESENT

The strenght of an SSA depends on the non-uniformity of the the distribution at the output of the trail associated with the attack. In an SPN, in every round, apart from the key mixing, there are two layers. One is the non-linear layer which is called the sBoxLayer and the other is the linear layer called pLayer. The target is to choose certain bits from the plaintext space of the cipher so that they are strongly correlated with certain other bits in the ciphertext space across the sBoxLayer and pLayer of all the rounds under consideration. Then those strongly correlated bits in the plaintext and ciphertext space will form a useful SS trail.

One way to find such correlations is to select a set of input and output bits (from the round function of the SPN) for the trail in such a way that the output bits of every round will after the permutation be the input bits of the next round.

Now if we encrypt many plaintexts by ensuring extreme non-uniformity in those input bits at the very first round (in other words, fixing those input bits in the plaintext space), then because of the bijective property of the S-box, there will be some degree of non-uniformity in the output bits of the selected S-box. In addition, because of the correlation among the selected input and output bits of the S-box, there will also be a certain level of non-uniformity in the chosen output bits of the first round. As the selection of the bits is made in a way that the selected output bits of the round function is permuted only among the input bit positions, the distribution of the input bits of the next round will also remain non-uniform. In this fashion, after r number of rounds, the output bits will remain non-uniform to certain degree. And thus the chosen input and output bits define the trail. However, the non-uniformity decreases as the number of rounds increases. So, naturally a good SS trail is the one which provides useful non-uniformity in the chosen output bits even after a significantly large value of r.

An S-box is a bijective function from a set of binary vectors to a set of binary vectors. As this is a bijection, applying non-uniformity in the inputs of an S-box will also produce non-uniformity in its output. Let the non-uniformity of the inputs of an S-box is generated by making only one specific input bit non-uniform. Let this specific input bit is x_i. Then such non-uniformity in the input will generate non-uniformity in those output bits y_j which has non-zero correlation with x_i. If for $i \neq j$, two input bits x_i, x_j has non-zero correlation with output bit y_k, then the non-uniformity of y_k achieved by the non-uniformity of both of the bits x_i and x_j is higher than the non-uniformity achieved by the non-uniformity of only one of x_i or x_j.

This suggests that, the input and output bits of the trail should be chosen in such a way that the number of input bits are maximized in one S-box. However, this also forces the number of output bits to be maximized in one S-box because the chosen output bits of one round become the chosen input bits of the next round. Note that if a chosen input bit x_i of an S-box has zero correlation with a chosen output bit y_j of the same S-box, then applying non-uniformity on x_i doesn't produce any non-uniformity on y_j. This suggests to avoid choosing any pair of input-output bits from the same S-box which have zero correlation accross that S-box.

2.7.1 SS trails in PRESENT

Let us visualize the S-box in PRESENT as shown in Figure 2.8. The leftmost input bit x_0 is considered as the least significant bit. By observing Table 2.5, we find that input bit x_0 has zero correlation with all the output bits y_i where $0 \leq i \leq 3$. We also find that input bit x_3 has zero correlation with output bit y_2. The 1 bit trails in case of zero correlations are marked using the red lines. As a result a good SS trail should include the bits from every S-box in a way that x_0 is not included at all and x_3, y_2 are not present in the trail simultaneously.

There is a weakness in the permutation layer of PRESENT as described in Figure 2.9 [11]. The size of a block is $n = 64$. Counting the plaintext bits starting from 0 from the right, the $21, 22, 25, 26, 37, 38, 41, 42$ bits are active only in 4 S-boxes. And none of these bits are x_0, x_3 or y_2. So, it is expected that if we fix these 8 bits (extreme non-uniformity) for each plaintext that we encrypt, then after encrypting sufficiently large amount of plaintexts, the ciphertexts will also have non-uniformity in the same 8

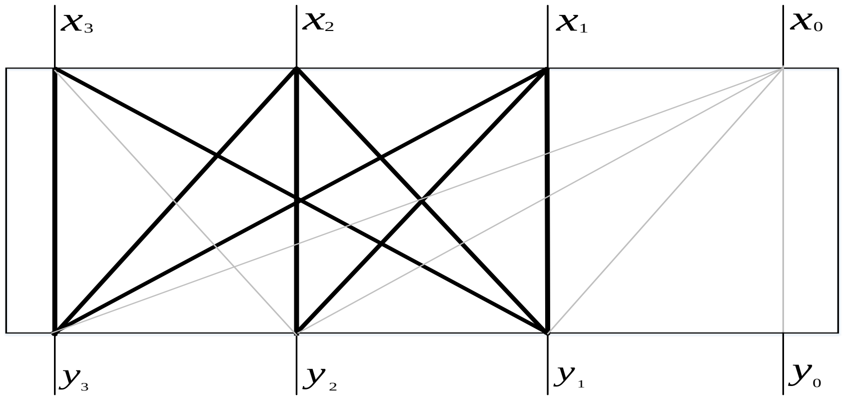

Figure 2.8: 1 bit trails in the S-box of PRESENT.

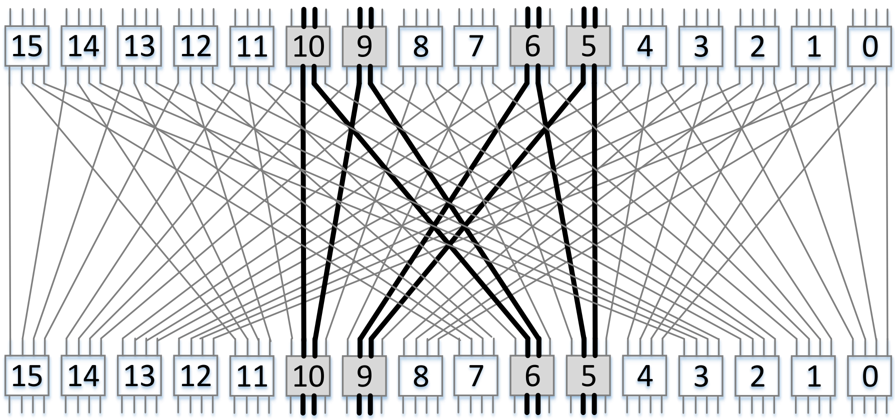

Figure 2.9: Weakness in PRESENT [11].

bits. That is, the evolution of these 8 bits are not random enough. As a result, we have a partitioning of the plaintext and ciphertext space. In the partitioning $s = q = 8$, $t = r = 56$, $B_s = B_q = \{21, 22, 25, 26, 37, 38, 41, 42\}$ and $B_t = B_r = \{0, 1, ..., 63\} \setminus B_s$.

Another interesting SS trail is mentioned in Figure 2.10. This trail has 27 bits at its input and 27 bits at its output. There are 9 active S-boxes. Every S-box has 3 input and 3 output bits. That means in every S-box there are $3 \times 3 = 9$ different 1 bit to 1 bit trail. Note that this SS trail includes x_3, y_2 simultaneously which is unlike the principle we discussed in previous section. The reason, it is still a good SS trail is, out of the 9 trails in every S-box, x_3, y_2 bits are involved in only one of them simultaneously. This results into 8 active trails in every S-box whereas by excluding both of them we could have at most $2 \times 2 = 4$ active trails in every S-box. That means, even though x_3, y_2 has zero correlation among them across the S-box, it is still useful to include them in a trail as they contribute in generating other active trails.

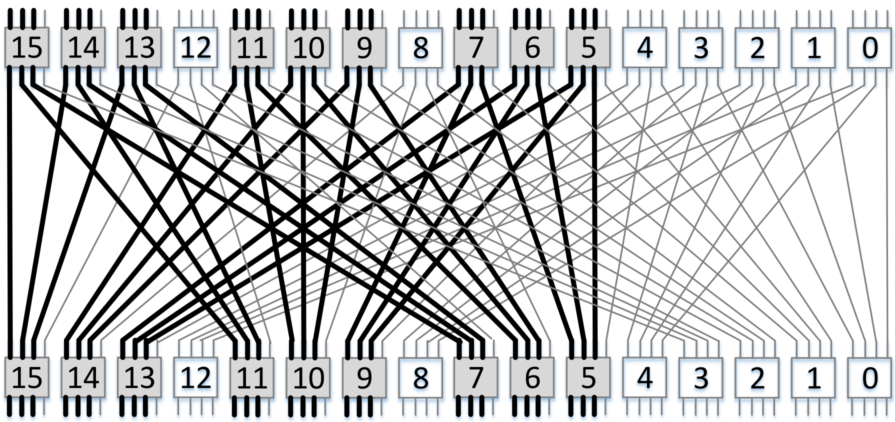

Figure 2.10: Weakness in PRESENT [11].

2.8 Exploiting the Weakness

In [11], the authors proposed two techniques to exploit the weakness. In both of the techniques a sufficient number of chosen plaintexts are encrypted where x_s part of x is fixed to a value a.

2.8.1 Comparing with Model Distribution

In order to exploit this weakness, the model distribution of y_q part of y is evaluated by Algorithm 4 for each key guess. For one key guess at each round, the work needed to compute the model distribution of the target trail after r round is equivalent to $r \cdot 2^{16}$ partial encryptions. Once the model distributions are computed, the key of the model distribution that minimizes the distance with the distribution computed from a secret key is accepted to be the correct key.

Algorithm 4 : Computing model distribution

Input: 8-bit subkey guess sk and the 8-bit input distribution $distrib\_in[256]$
Output: the 8-bit output distribution $distrib\_out[256]$

initialize $distrib\_out[256]$ to the all-zero state
for 8-bit values $text$ **do**
    for 8-bit values $rand$ **do**
        fix the 8-bit trail to $text$ and xor with sk
        fix the 8-bit non-trail to $rand$
        apply the S-boxes
        apply the permutation
        evaluate the value of the 8 bit trail out
        update $distrib\_out[out] = distrib\_out[out] + distrib\_in[text]/256$;
    end for
end for

To verify the practicability of the attack model, Collard and Standaert have conducted an experiment on reduced-round version of PRESENT. To reduce the number of key guess, they have simplified the key scheduling algorithm by using the same key in each round. They have used 2^{30} chosen plaintexts. In all those plaintexts, the 8 bits (mentioned in Figure 2.9 in bold lines) are fixed, and the other 56 bits are varied. All those plaintexts are encrypted where round keys are kept fixed in each round. Then they have computed the distribution of those fixed 8 bits at the end of $2, 4, 6$ and 8 round. These experimental distributions computed from the real cipher itself with reduced-round and modified key scheduling algorithm is compared with the model distributions computed from Algorithm 4 for $2, 4, 6$ and 8 rounds. According to this simplified experiment, both experimental and model distributions present a significant deviation from uniform as expected.

They also have made an observation on the distance in between the experimental and model distributions. First they have computed the experimental and model distributions of the concerned 8 bits at the end of $2, 4, 6$ and 8 rounds for the key byte 32 (i.e. 00100000). Then they have computed the model distributions of these 8 bits for all possible 256 sub-keys at the end of $2, 4, 6$ and 8 rounds. Finally they have plotted the distance in between the model distribution for every possible key bytes and model disribution of key byte 32. For the sake of discussion, let us call this distance to be model-model distance. They also have plotted the distance in between the model distribution for every possible key bytes and experimental disribution of key byte 32. Let us call this distance to be model-experiment distance. It has been found that the distance between the model-model and model-experiment distance is minimized at the correct key. This indicates that the model distribution captures the essence of the experimental distribution.

In both of the experiments it has been found that the deviation tends to decrease with number of rounds. So, as the number of rounds increases, to find significant deviation, the number of chosen plaintext is also needed to be increased. In other words, as the number of rounds increases, the data complexity of the attack also increases.

However, in the attack mentioned above, the effect of the key scheduling algorithm has been ignored to show that the basic idea works in principle. Now considering the key scheduling algorithm, demands more key bits to be guessed as the round key changes in every round. As for one round we need to guess at most 8 bits, we are in need of guessing at most $r \times 8$ bits after r rounds. According to Collard and Standaert, for 12 rounds of PRESENT, 63 key bits have to be guessed, meaning, there are 2^{63} different possible keys in effect. For each key guess, after r rounds, we are in need of computing $r \times 2^{16}$ partial encryptions. Which implies that we are in need of $2^{63} \times r \times 2^{16}$ partial encryptions. We see that the attack becomes quite impossible even with 12 rounds because of its time complexity. In the next section, we present a tricky way to overcome this problem. The idea is the same as in commonly used statistical linear and differential attacks. Instead of guessing key bits on the intermediate rounds, make a prediction about the behaviour of the cipher over those rounds that holds on the average over the keys.

2.8.2 Distinguishing Attack:

Computing the theoretical distribution is costly. To overcome this problem, they suggest a distinguishing attack which we will explain in brief here. The plaintexts are encrypted using r-rounds of PRESENT and record the distribution of the ciphertexts for the 16 bits at the output of the 4 active S-box in the last round. Given this experimental distribution, it is possible to compute the output distribution of the target 8-bit trail one round before by a classical partial decryption process. For one key guess, the evaluation of such $r-1$-round distribution requires 2^{16} computations. For the corect key guess, the experimental 8-bit distribution in the $r-1$-round is expected to be more non-uniform than for any other guess. This is because decrypting with a wrong guess is expected to have the same effect as encrypting one more round. Thus it is expected to distinguish the correct key from the wrong ones by computing the distance between a partially decrypted distribution and the uniform distribution. If the attack works properly, the distribution with the highest distance should correspond to the correct key.

There are extensions of this distinguishing attack. The same attack can be made by increasing the number of fixed plaintext bits or by using multiple fixations of the fixed bits or by doing partial decryption for 2 rounds instead of 1 round. However, all these extensions require to distinguish a distribution from uniform distribution. The statistical model developed in this work is a statistic T which can be used to perform a statistical test that can distinguish the computed distribution in between two known distributions. In the next sections, we have defined formally the notion of a distribution. We will also recall some known distributions and their properties as they will be useful in finding the statistical model. In the next chapter we have presented how to perform a statistical test to distinguish a distribution between two given distributions. In the next chapter we have defined the statistic T and used it to develop a SS distinguisher in Chapter 4. In Chapter 5, we have shown how the success probability of the statistical test is related with the number of plaintexts we encrypt before performing the statistical test.

Chapter 3

Statistics

3.1 Probability Distribution

Probability distribution is a function from a set of possible outcomes of an experiment to a set of real values in the range $[0, 1]$. The sum of the probabilities of occurrences of all the possible outcomes is always 1. Now if the set of possible outcomes contains only discrete values then the function that defines the probability distribution is called probability mass function (pmf). If the set of possible outcomes contains continuous value within any range, then the function that defines the probability distribution of the experiment is called probability density function (pdf).

There are different kinds of probability density and probability mass functions that describes the probability distribution of many natural events. Few of these probability distributions have been found to be very important in developing the statistical model of SSA. In this section those distributions along with their properties are discussed briefly

3.1.1 Gamma Distribution

Definition 3.1.1. *[17] A random variable X that is gamma-distributed with shape k and scale θ is denoted by*

$$X \sim \Gamma(k, \theta) \equiv Gamma(k, \theta)$$

The probability density function using the shape-scale parametrization is

$$f(x;k,\theta) = \frac{x^{k-1}e^{-\frac{x}{\theta}}}{\theta^k\Gamma(k)} \qquad \textit{for } x > 0 \textit{ and } k,\theta > 0$$

Here $\Gamma(k)$ *is the gamma function evaluated at* k*.*

Figure 3.1 provides a visualization of the gamma distribution given different shape and scale parameters.

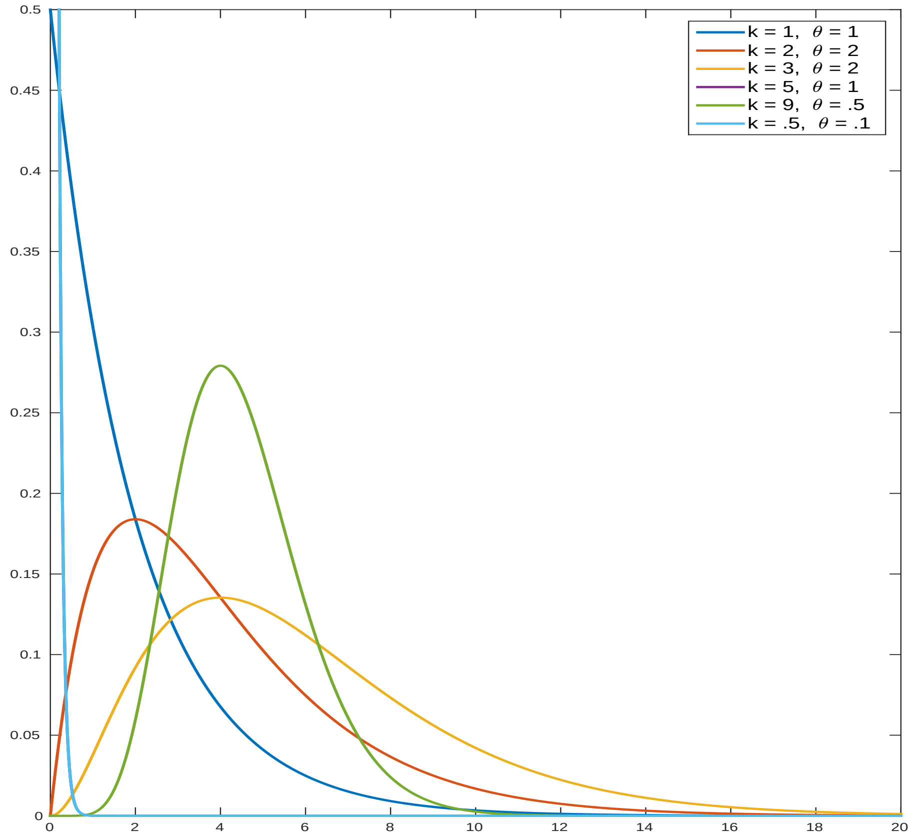

Figure 3.1: Gamma distribution with different shape and scale parameters

3.1.2 Properties of Gamma Distribution

1. Let X be a random variable which is gamma distributed with shape parameter k and scale parameter θ. Then for any constant c, the

random variable $Y = cX$ is also gamma distributed with the shape parameter $k^{'}$ and scale parameter $\theta^{'}$. Where $k^{'} = k$ and $\theta^{'} = c\theta$ [21]. In other words, we can write

$$X \sim \Gamma(k, \theta) \Rightarrow cX \sim \Gamma(k, c\theta) \tag{3.1}$$

2. Le X be a random variable which is gamma distributed with the shape parameter k and scale parameter θ. Then the mean and variance of X denoted by μ_X and σ_X^2 respectively are defined as follows [17]

$$\mu_X = k\theta \tag{3.2}$$
$$\sigma_X^2 = k\theta^2 \tag{3.3}$$

3.1.3 χ^2-Distribution

[7] In probability theory and statistics, the chi-squared distribution (also chi-square or χ^2-distribution) with k degrees of freedom is the distribution of a sum of the squares of $k+1$ independent standard normal random variables. The probability density function of the chi-squared distribution is

$$f(x;\, k) = \begin{cases} \frac{x^{(k/2-1)}e^{-x/2}}{2^{k/2}\Gamma\left(\frac{k}{2}\right)}, & x \geq 0; \\ 0, & \text{otherwise.} \end{cases} \tag{3.4}$$

where $\Gamma(k/2)$ denotes the Gamma function, which has closed-form values for integer k. In addition to these, the concept of central and non-central χ^2-distributions, their means and variances will be useful in deriving the statistical model. Figure 3.2 shows how the probability density function looks for different values of k

Definition 3.1.2. *[14] Let $X_i \sim \mathcal{N}(\mu_i, \sigma_i^2)$ where $i = 0, ..., k$. Then the random variable*

$$T_0 = \sum_{i=0}^{k} \frac{(X_i - \mu_i)^2}{\sigma_i^2} \tag{3.5}$$

has central χ^2 distribution with k degrees of freedom which is written as

$$T_0 \sim \chi_k^2 \tag{3.6}$$

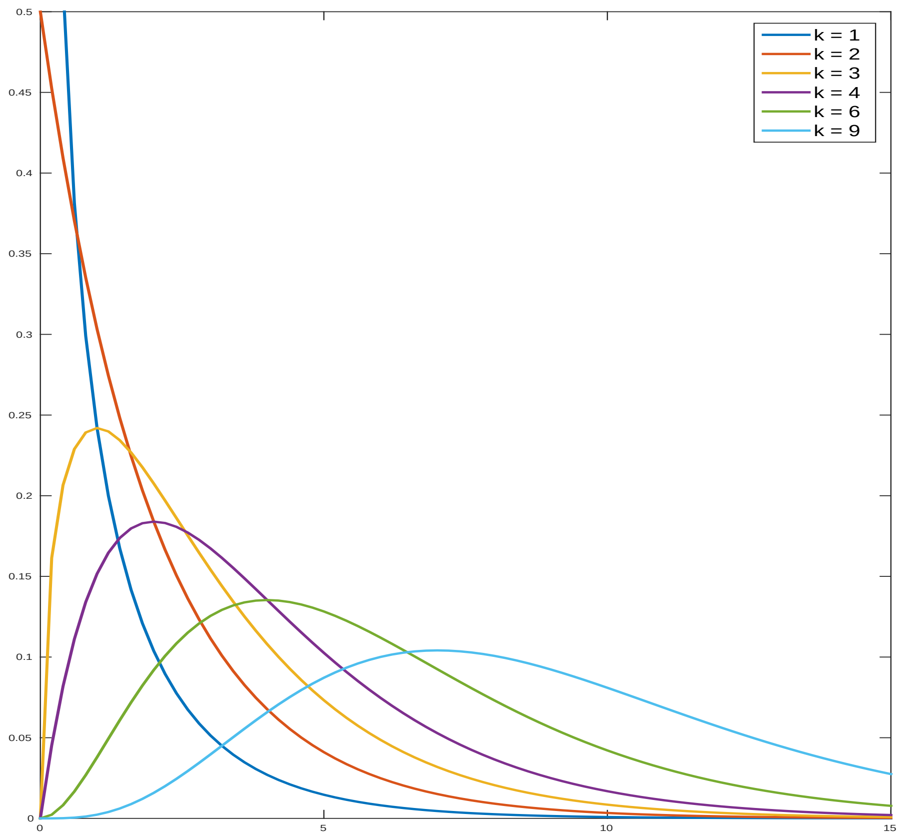

Figure 3.2: Chi-square distribution with different parameters

and the random variable

$$T_1 \;=\; \sum_{i=0}^{k} \frac{(X_i)^2}{\sigma_i^2} \tag{3.7}$$

has non-central χ^2*-distribution with* k *degrees of freedom where the non-centrality parameter is*

$$\delta \;=\; \sum_{1=0}^{k} \frac{\mu_i^2}{\sigma_i^2} \tag{3.8}$$

And this is written as:

$$T_1 \;\sim\; \chi_k^2(\delta) \tag{3.9}$$

The mean and variance of the variable T_0 which is centrally χ^2-distributed are following:

$$\mu_{T_0} = k \tag{3.10}$$
$$\sigma^2_{T_0} = 2k \tag{3.11}$$

And the mean and variance of the variable T_1 which is non-centrally χ^2-distributed with δ as non-central parameter is following:

$$\mu_{T_1} = k + \delta \tag{3.12}$$
$$\sigma^2_{T_1} = 2(k + 2\delta) \tag{3.13}$$

3.1.4 Link Between χ^2 and Γ Distribution

A χ^2 variable X of k degrees of freedom is gamma distributed with shape $\alpha = \frac{k}{2}$ and scale $\beta = 2$ [18]. That is

$$X \sim \chi^2_k \Rightarrow X \sim \Gamma\left(\alpha = k/2, \beta = 2\right) \tag{3.14}$$

3.1.5 Normal approximation of χ^2 distribution:

[23] For large number of degrees of freedom k, the chi-square distribution may be approximated by a normal distribution. Consequently we have the following two approximations.

1. For a sufficiently large value of k, a central χ^2-distributed random variable X with k degrees of freedom is approximately normally distributed

$$X \sim \mathcal{N}\left(k, 2k\right) \tag{3.15}$$

2. For a sufficiently large value of k, a non-central χ^2-distributed random variable X with k degrees of freedom and δ as non-centrality parameter is approximately normally distributed

$$X \sim \mathcal{N}\left(k + \delta, 2\left(k + 2\delta\right)\right) \tag{3.16}$$

3.1.6 Normal approximation of Γ Distribution

Let the shape and scale parameters of a gamma distribution be α and β. Asymptotically, given that for a shape parameter α, going to infinity, a gamma distribution converges towards a normal distribution with expectation $\mu = \alpha \cdot \beta$ and variance $\sigma^2 = \alpha\,\beta^2$ [22].

3.1.7 Binomial Distribution

As defined in [9], the binomial distribution with parameters n and θ is the discrete probability distribution of the number of successes in a sequence of n independent "*yes/no*" experiments, each of which yields success with probability θ. The probability of getting exactly k successes in n trials is given by the probability mass function

$$f(k; n, \theta) = \Pr(X = k) = \binom{n}{k} \theta^k (1-\theta)^{n-k} \tag{3.17}$$

for $k = 0, 1, 2, ..., n$, where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is the binomial coefficient, hence the name of the distribution.

Let N be the number of data (sample size), M be the number of cells with different probabilities $p(\eta), \eta = 1, 2, ..., M$. Now if $\omega(\eta)$ denotes the number of data in cell η, then $\omega(\eta) \sim \mathcal{B}(p(\eta))$. As mentioned in [14], for large N we have

$$\omega(\eta) \sim \mathcal{N}(Np(\eta), Np(\eta)) \approx \mathcal{N}(Np(\eta), N/M) \tag{3.18}$$

3.2 Capacity

3.2.1 Capacity of a Distribution

Given a function $f : X \to Y$, $x \in X$, $\eta \in Y$, and X is uniformly distributed, the probability of $f(x) = \eta$ is denoted by p_η defined as

$$p_\eta = |X|^{-1} \# \{x \in X \mid f(x) = \eta\} \tag{3.19}$$

The probability distribution of the function f is described by the pmf $p = (p_\eta)$. The uniformity of a distribution p is measured by its capacity, also called as Squared Euclidean Imbalance. Capacity of a distribution is computed from its squared distance from the uniform distribution. If the capacity of a distribution p is denoted by C_p, then it can be formally written as

$$C_p = |Y| \sum_{\eta \in Y} (p_\eta - |Y|^{-1})^2 \tag{3.20}$$

Let $p(a) = (p_\eta(a))$ denote a probability distribution over domain Y in a family of distributions parametrized by $a \in I$. We consider a as a uniformly distributed random variable. We assume that this family of probability distributions satisfies the following hypothesis.

Hypothesis 1. *For each fixed $\eta \in Y$, the probability $p_\eta(a)$ is a random variable and independently distributed and follow the normal distribution*

$$p_\eta(a) \sim \mathcal{N}\left(\mu, \sigma^2\right)$$

where $\mu = |Y|^{-1}$

For an arbitrarily fixed a, the capacity of $p(a) = (p_\eta\,(a))$ is denoted by $C(a)$. Then

$$C\,(a) = |Y| \sum_{\eta \in Y} (p_n\,(a) - |Y|^{-1})^2 \tag{3.21}$$

The average capacity over the parametrized probability distributions $p(a)$ is defined by

$$C = |I|^{-1} \sum_{a \in I} C(a) \tag{3.22}$$

3.2.2 Distribution of Capacity

Theorem 3.2.1. *Given a family $p(a), a \in I$ of probability distributions that satisfies Hypothesis 1, the capacity $C(a)$ is gamma distributed*

$$C(a) \sim \Gamma\left(\frac{|Y| - 1}{2}, \frac{2C}{|Y| - 1}\right)$$

with mean C and variance $\frac{2C^2}{|Y|-1}$

Proof. Let $\mu_{C(a)}$ and $\sigma^2_{C(a)}$ denote the mean and variance of $C(a)$ respectively. According to (3.22) we have $\mu_{C(a)} = C$. Let us now examine the parametrized statistic $Q(a)$ defined as

$$Q(a) = \sum_{\eta} \frac{\left(p_\eta(a) - \mu_{p_\eta(a)}\right)^2}{\sigma^2_{p_\eta(a)}} \tag{3.23}$$

From Hypothesis 1, we know that $p_\eta(a)$ is identically and independently normally distributed. As a result, using Hypothesis 1 and Definition 3.1.2, we can write

$$Q\left(a\right) = \sum_{\eta} \frac{(p_\eta(a) - |Y|^{-1})^2}{\sigma^2} \sim \chi^2_{|Y|-1} \tag{3.24}$$

Let us multiply both sides of (3.24) by the cardinality of the set Y and variance of the distribution $p_\eta(a)$. The result is following:

$$|Y|Q(a)\sigma^2 = |Y| \sum_{\eta} \left(p_\eta(a) - |Y|^{-1}\right)^2 \tag{3.25}$$

As per definition of capacity of a distribution given in (3.20), the right hand side of (3.25) is the capacity of the distribution $p(a)$, which can be denoted as $C(a)$ as per our convention. So, we get

$$C(a) = |Y|\sigma^2 Q(a)$$

Now if we plug (3.24) in (3.14), then we can write

$$Q(a) \sim \Gamma\left(\frac{|Y-1|}{2}, 2\right) \tag{3.26}$$

We see $|Y|$ is a constant and as per Hypothesis 1, σ^2 is also a constant. According to (3.26), $Q(a)$ is gamma distributed. So, as per the property of gamma distribution given in (3.1), we can write

$$C(a) \sim \Gamma\left(\frac{|Y-1|}{2}, 2|Y|\sigma^2\right) \tag{3.27}$$

Let us denote the mean of $C(a)$ over all $a \in I$ by C. As per the property of gamma distribution given in (3.2) the mean of the gamma distributed random variable is the multiplication of its shape and scale parameter. Consequently, from (3.27), the mean C is as follows

$$C = |Y-1||Y|\sigma^2$$

Which implies that

$$\sigma^2 = \frac{C}{|Y-1||Y|} \tag{3.28}$$

Now by plugging the σ^2 from (3.28) in (3.27), we obtain the following result

$$C(a) \sim \Gamma\left(\frac{|Y|-1}{2}, \frac{2C}{|Y|-1}\right) \tag{3.29}$$

The first claim of the theorem is now proven and it remains to show that the variance is $\sigma^2_{C(a)} = \frac{2C^2}{Y-1}$. As per the property of gamma distribution given in (3.3), variance of a gamma distributed variable is the multiplication of it's shape parameter and the square of scale parameter. Using this property in (3.29), we find the variance $\sigma^2_{C(a)}$ as follows

$$\begin{aligned}\sigma^2_{C(a)} &= \frac{|Y-1|}{2}\left(\frac{2C}{|Y-1|}\right)^2 \\ &= \frac{2C^2}{|Y|-1}\end{aligned}$$

□

3.3 A statistical test to distinguish distribution

In the applications of cryptanalysis, the task is to distinguish between cipher and random behavior based on an observed distribution computed from sample data. Now we present a statistical test to accomplish this task. To perform the statistical test, we are in need of a statistic computed from the cipher data distribtuion. We denote this statistic as T. For the statistical test we are presenting here, it is essential for T to be defined in a way that it is normally distributed. Suppose we already know two normal deviates T_0 and T_1 such that

$$\begin{aligned}T_0 &\sim \mathcal{N}\left(\mu_{T_0}, \sigma^2_{T_0}\right) \\ T_1 &\sim \mathcal{N}\left(\mu_{T_1}, \sigma^2_{T_1}\right)\end{aligned}$$

and assuming without loss of generality that $\mu_{T_0} < \mu_{T_1}$. Given a T computed from a sample about which we know that it follows either the distribution of

T_0 or T_1. The task is to decide which of those two it is. The test is defined by a value τ. If $T \leq \tau$ the outcome of the test is that T is drawn from the distribution of T_0 and if $T > \tau$ then T is drawn from the distribution T_1. The error probabilities are defined as

$$\begin{aligned} \alpha_0 &= \Pr(T_0 \mid T > \tau) \\ \alpha_1 &= \Pr(T_1 \mid T \leq \tau) \end{aligned}$$

That is, α_0 is the probability that the test outputs T_1 when the reality is T_0. Similarly α_1 is the probablity that the test outputs T_0 when the reality is T_1. To make the error probabilities less than α_0 and α_1, we must select τ to satisfy

$$\mu_{T_0} + \sigma_{T_0}\zeta_0 \leq \tau \leq \mu_{T_1} - \sigma_{T_1}\zeta_1 \tag{3.30}$$

where $\Phi(\zeta_i) = 1 - \alpha_i$ for $i \in \mathbb{Z}_2$ for the cumulative distribution function Φ of the standard normal distribution. That is, ζ_i indicates how many standard deviation beyond the mean is required to bound the probability of wrongly choosing T_{i-1} by at most α_i. The Figure 3.3 shows the range of feasible values of τ. In Figure 3.4 shows how to choose a single value of τ. Note that in Figure 3.4, the area on the right side of the yellow line under the red curve indicates α_0 and the area on the left side of the yellow line under the blue curve indicates α_1 In the applications of cryptanalysis the distribution of T_1 is determined by the cipher while T_0 represents random behaviour. If the cipher distribution has non-zero capacity the statistic T given above can be used. The parameters of T_1 depend on the number N of plaintexts, while the parameters of T_0 are constant with N as the distribution is uniform and its capacity is equal to zero. Then the distributions of T_0 and T_1 move apart as N grows. The phenomenon is presented in Figure 3.5. In this figure, the blue line has moved on the right along the X-axis, which has made the error areas smaller. Then the above equation allows to determine the sample size N which is sufficient to find a threshold τ that gives a test with as small non-zero error probabilities α_0 and α_1 as desired.

In Section 3.4, we have defined statistic T which we have used to develop the statistical model in the Chapter 4.

3.4 Statistic T for the statistical test

We already have mentioned that statistic T is computed from cipher data distribution. Note that the cipher data is computed from a set of chosen

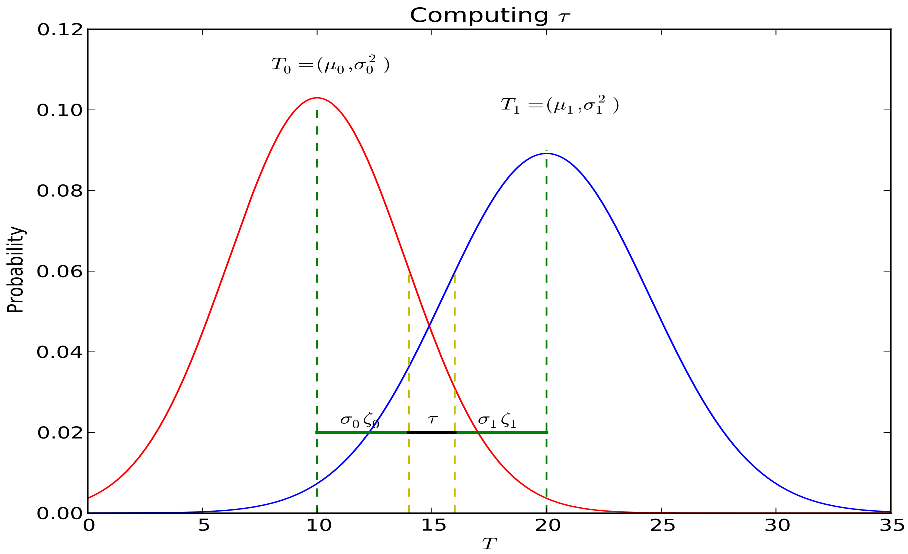

Figure 3.3: Choosing a range of feasible values of τ

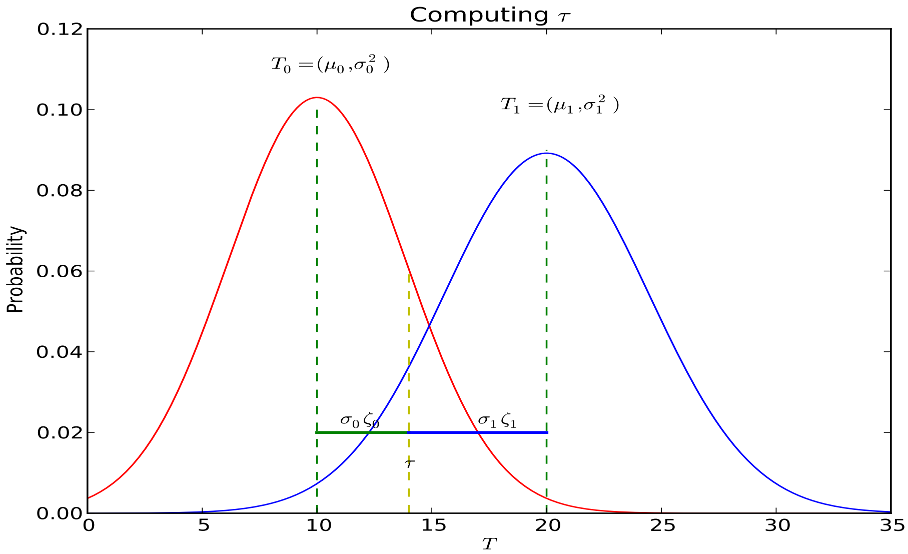

Figure 3.4: Choosing a single value of τ. That is $\mu_0 + \sigma_0\zeta_0 = \mu_1 - \sigma_1\zeta_1$

plaintexts. Let us call this set of chosen plaintexts as sample denoted by ϕ. Let us consider a fuction $\Omega : \phi \to Y$ derived from the encryption function. Let $\omega : Y \to \mathbb{Z}$ another function such that $\omega(\eta)$ is the number of times a

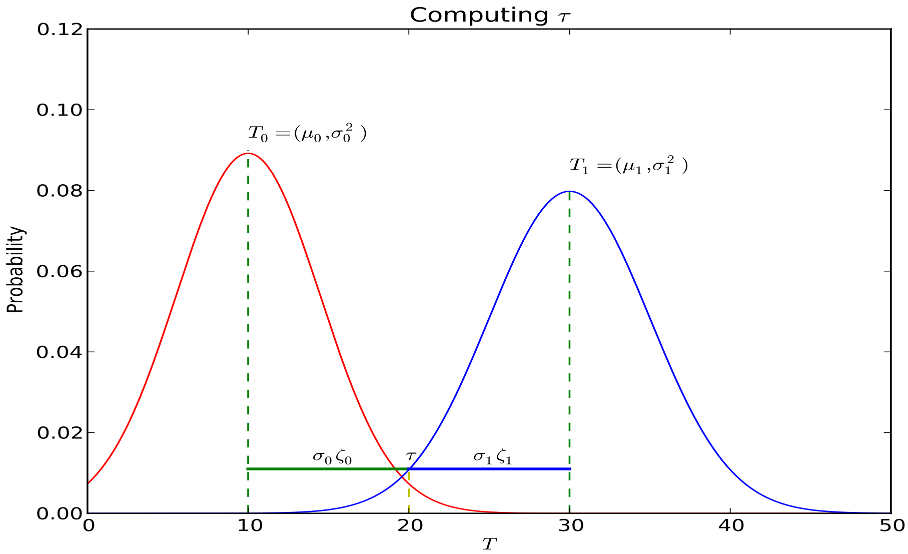

Figure 3.5: As T_0, T_1 move apart, τ can be chosen for smaller error rate

value $\eta \in Y$ is observed as the output of function Ω, that is

$$\omega(\eta) = \#\{x \in \phi \mid \Omega(x) = \eta\}, \eta \in Y$$

Now given a sample ϕ of size N, we define T as following:

$$T = \sum_{\eta \in Y} \frac{\left(\omega(\eta) - N|Y|^{-1}\right)^2}{N|Y|^{-1}}$$

In sections 3.4.1 and 3.4.2, we have discussed how the statistic T is distributed when the sample ϕ is sampled with or without replacement.

3.4.1 Sampling with replacement

Let p_η denote the expected probability of getting $\Omega(x) = \eta$ when $N = 1$. We also observe that that $\omega(\eta)$ is binomially distributed. As per property of binomial distribution given in (3.18) we can write

$$\mu_{\omega(\eta)} = Np_\eta \tag{3.31}$$

$$\sigma^2_{\omega(\eta)} = N|Y|^{-1} \tag{3.32}$$

Now, according to the definition of χ^2-distribution given in (3.9), the statistic

$$\begin{aligned} T &= \sum_{\eta\in Y}\frac{\left(\omega(\eta)-N|Y|^{-1}\right)^2}{N|Y|^{-1}} \\ &= \sum_{\eta\in Y}\frac{\left(\omega(\eta)-N|Y|^{-1}\right)^2}{\sigma^2_{\omega(\eta)}} \\ &= \sum_{\eta\in Y}\frac{\left(\omega(\eta)-N|Y|^{-1}\right)^2}{\sigma^2_{\omega(\eta)-N|Y|^{-1}}} \end{aligned}$$

is non-centrally $\chi^2_{|Y|-1}(\delta)$-distributed. To calculate the the non-central parameter δ, we need to know the mean and variance of $\omega(\eta)-N|Y|^{-1}$. Observe that $N|Y|^{-1}$ is a constant and the mean of $\omega(\eta)$ is Np_η. Consequently the mean of $\omega(\eta)-N|Y|^{-1}$ is $Np_\eta-N|Y|^{-1}$. And variance of $\omega(\eta)$ and $\omega(\eta)-N|Y|^{-1}$ are same. As a result we can calculate δ as following

$$\begin{aligned} \delta &= \sum_{\eta\in Y}\frac{\left(Np_\eta-N|Y|^{-1}\right)^2}{\sigma^2_{\omega(\eta)-N|Y|^{-1}}} \\ &= \sum_{\eta\in Y}\frac{N^2\left(p_\eta-|Y|^{-1}\right)^2}{N|Y|^{-1}} \\ &= N\sum_{\eta\in Y}\frac{\left(p_\eta-|Y|^{-1}\right)^2}{|Y|^{-1}} \\ &= NC \end{aligned}$$

Where C is the capacity of the distribution $p=(p_\eta)$. Now according to Definition 3.1.2, the mean and variance of T, denote by μ_T and σ^2_T are

$$\begin{aligned} \mu_T &= |Y|-1+NC \\ \sigma^2_T &= 2\left(|Y|-1+2NC\right) \end{aligned}$$

According to the normal approximation of χ^2-distribution as mentioned in Section 3.1.5 we can write

$$T \sim \mathcal{N}\left(|Y|-1+NC, 2\left(|Y|-1+2NC\right)\right) \tag{3.33}$$

3.4.2 Sampling without replacement

When ϕ is sampled without replacement, the number of different possible samples decreases as the size of the samples increases. The difference between those different samples also decreases as the size of the samples increases. Which implies, as the sample size grows, the value of T also differs small for different samples. As a result, the variance of T decreases. This is indeed, because when we consider the maximum sample size, there is only one possible sample and only one possible value of T resulted from this sample. Which means, in this case T has zero variance. This phenomenon has been taken into account by Blondeau and Nyberg in [2]. They have introduced a co-efficient B in the computation of the mean and variance of T using sample without replacement. When the sample size is small, B is almost one and as the sample size grows towards the maximum size, B approaches to zero and becomes zero when the sample size is maximum.

According to [2], we can define B as $\left(1 - \frac{N}{|\phi|_{max}}\right)$. Here $|\phi|_{max}$ is the largest possible size of a valid sample ϕ. And the mean and variance of T are following:

$$\mu_T = (|Y| - 1)\, B + NC \tag{3.34}$$

$$\sigma_T^2 = 2\,(|Y| - 1)\, B^2 + 4BNC \tag{3.35}$$

In the next chapter we have extended this discussion of T considering the associated trail of the attack. That is, we have defined the function Ω considering the the encryption function and the SS trail. However, we will only focus on the case of sampling with replacement in the rest of the thesis. Sampling with replacement is already good enough, in real life cryptanalysis. As shown in [2], the method of sampling without replacement offers some advantage when the sample size is close to the full codebook. In an upcoming paper [16] the statistical model developed in this work has been extended to the case of sampling without replacement.

Chapter 4

Statistical Distinguishers

In previous chapter we have discussed how to exploit the weakness of a cipher in SSA. Now we know that, to exploit the weakness of a block cipher by SSA, we need to be able to distinguish a distribution from random. It was shown how a statistical test can accomplish this task. We also have explained that we need a statistic to perform the statistical test and have defined the statistic that we have used in the test. While defining the statistic T in previous chapter we have introduced two function Ω and ω but have not exactly defined them. In this chapter we define the statistic T specifically by defining the exact mapping of Ω and ω .

In the SSA introduced by Collard and Standaert [11], a part of the plaintext is fixed and the distribution of a part of the ciphertext is observed. Let the plaintext be

$$x = (x_s, x_t) \in \mathbb{F}_2^s \times \mathbb{F}_2^t$$

and the ciphertext

$$y = E(x, K) = (y_q, y_r) \in \mathbb{F}_2^q \times \mathbb{F}_2^r$$

We fix the x_s part of the plaintexts to different values and observe the distribution of y_q part. We can define the functions Ω and ω differently based on how x_s is fixed. In the following sections we will derive different distributions of the statistics T defined differently, based on different variants of the functions Ω and ω.

4.1 Model For One Fixation

We find the distribution of the statistic depending on the way the fixation is chosen. First, we derive the distribution for a given fixation a and then we go for general case of any fixation $a \in \mathbb{F}_s^2$. For a fixed $a \in \mathbb{F}_2^s$ such that $x = (a, x_t)$ and $K \in \mathbb{F}_2^l$ the vectorial boolean function under consideration is

$$\Omega_a : \phi \to \mathbb{F}_2^q \text{ where } \Omega_a(x_t) = y_q \tag{4.1}$$

where $y = E\left((a, x_t), K\right) = (y_q, y_r)$ and $\phi \subseteq \mathbb{F}_2^t$ is sampled randomly with replacement. We also define another integer function $\omega_a : \mathbb{F}_2^q \to \mathbb{Z}$ such that for a given $\eta \in \mathbb{F}_2^q$

$$\omega_a(\eta) = \#\left\{\Omega_a(x_t) = \eta \mid x_t \in \phi\right\} \tag{4.2}$$

4.1.1 Arbitrarily Fixed Fixation

For a fixed fixation a and any sample $\phi \subseteq \mathbb{F}_2^t$ such that $|\phi| = N \leq 2^t$, the statistic T is denoted by $T_a(\phi)$ and defined as

$$T_a(\phi) = \sum_{\eta=0}^{2^q-1} \frac{\left(\omega_a(\eta) - N2^{-q}\right)^2}{N2^{-q}} \tag{4.3}$$

We see that $\omega_a(\eta)$ is binomially distributed. So, according to (3.18), we can write

$$\omega_a(\eta) \sim \mathcal{N}\left(\mu_{\omega_\eta(a)}, \sigma^2_{\omega_\eta(a)}\right)$$

where $\mu_{\omega_a(\eta)} = Np_\eta(a)$ and $\sigma^2_{\omega_a(\eta)} = N2^{-q}$. Then the random variable $X_a(\eta) = \omega_a(\eta) - N2^{-q}$ is also approximately normally distributed

$$X_a(\eta) \sim \mathcal{N}(\mu_{X_a(\eta)}, \sigma^2_{X_a(\eta)})$$

where $\mu_{X_a(\eta)} = \mu_{\omega_a(\eta)} - N2^{-q}$ and $\sigma^2_{X_a(\eta)} = \sigma^2_{\omega_a(\eta)}$. Now we can write

$$\begin{aligned} T_a(\phi) &= \sum_{\eta=0}^{2^q-1} \frac{\left(X_a(\eta)\right)^2}{N2^{-q}} \\ &= \sum_{\eta=0}^{2^q-1} \frac{\left(X_a(\eta)\right)^2}{\sigma^2_{X_a(\eta)}} \\ &= \sum_{\eta=0}^{2^q-1} \frac{\left(X_a(\eta)\right)^2}{\sigma^2_{X_a(\eta)}} \end{aligned}$$

Then by Definition 3.1.2 we can write

$$T_a(\phi) \sim \chi^2_{2^q-1}(\delta(a)) \tag{4.4}$$

where $\chi^2_{2^q-1}(\delta(a))$ is the non-central χ^2 distribution with $2^q - 1$ degrees of freedom and non-central parameter

$$\begin{aligned}
\delta(a) &= \sum_{\eta=0}^{2^q-1} \frac{(\mu_{X_a(\eta)})^2}{\sigma^2_{X_a(\eta)}} \\
&= \sum_{\eta=0}^{2^q-1} \frac{(\mu_{\omega_a(\eta)} - \sigma^2_{\omega_a(\eta)})^2}{\sigma^2_{\omega_a(\eta)}} \\
&= \sum_{\eta=0}^{2^q-1} \frac{(Np_\eta(a) - N2^{-q})^2}{N2^{-q}} \\
&= NC(a)
\end{aligned}$$

Then by Definition 3.1.2, for each fixed a the mean $\mu_{T_a(\phi)}$ and variance $\sigma^2_{T_a(\phi)}$ of $T_a(\phi)$, as the sample of size N varies, are

$$\begin{aligned}
\mu_{T_a(\phi)} &= 2^q - 1 + NC(a) \\
\sigma^2_{T_a(\phi)} &= 2(2^q - 1 + 2NC(a))
\end{aligned}$$

By the normal approximation of χ^2 distribution as given in (3.16), we can write:

$$T_a(\phi) \sim \mathcal{N}(\mu_{T_a(\phi)}, \sigma^2_{T_a(\phi)})$$

$$T_a(\phi) \sim \mathcal{N}\left(2^q - 1 + NC(a), 2(2^q - 1 + 2NC(a)\right) \tag{4.5}$$

4.1.2 Variable Fixation

By Theorem 3.2.1, for any arbitrarily fixed fixation $a \in \mathbb{F}_2^s$, the capacity of the distribution $p(a)$ denoted by $C(a)$ is

$$C(a) \sim \Gamma\left(\frac{|Y|-1}{2}, \frac{2C}{|Y|-1}\right)$$

where we have assumed that $p\,(a)$ satisfies Hypothesis 1. According to the property of gamma distribution as given in 3.2 and 3.3, the mean and variance of $C(a)$ over all possible a is C and $\frac{2C^2}{|Y|-1}$ respectively. According to the link in between gamma and normal distribution given in Section 3.1.6 we get

$$C(a) \sim \mathcal{N}\left(C, \frac{2C^2}{|Y|-1}\right) \tag{4.6}$$

We can derive the mean $\mu_{NC(a)}$ and variance $\sigma^2_{NC(a)}$ of $NC(a)$.

$$\begin{aligned}
\mu_{NC(a)} &= N\mu_{C(a)} = NC \\
\sigma^2_{NC(a)} &= N^2\sigma^2_{C(a)} = N^2\frac{2C^2}{|Y|-1} = \frac{2(NC)^2}{|Y|-1}
\end{aligned}$$

That implies

$$NC(a) \sim \mathcal{N}\left(NC, \frac{2(NC)^2}{|Y|-1}\right) \tag{4.7}$$

We denote by $T(\phi, a)$ the statistic $T_a(\phi)$ where fixation a also varies in the same way sample ϕ of size N varies. Then we have the following result.

Theorem 4.1.1. *Let us assume that sample ϕ of size $N \le 2^t$ drawn randomly with replacement with a fixed key and fixation a of s bits of the plaintext and the number q of observed bits in the ciphertext is sufficiently large. If $p(a)$ satisfies Hypothesis 1, then $T(\phi, a)$ is approximately normal with mean $\mu_{T(\phi,a)}$ and variance $\sigma^2_{T(\phi,a)}$, where*

$$\begin{aligned}
\mu_{T(\phi,a)} &= 2^{-s}\sum_{a\in\mathbb{F}_2^s}\mu_{T_a(\phi)} = 2^q - 1 + NC \\
\sigma^2_{T(\phi,a)} &= \frac{2}{2^q-1}\left(2^q - 1 + NC\right)^2
\end{aligned}$$

Proof. For each fixed a and variable sample ϕ of size N, according to (4.5) we have

$$T_a(\phi) \sim \mathcal{N}(2^q - 1 + NC(a), 2(2^q - 1 + 2NC(a)))$$

And according to (4.7) we also have

$$NC(a) \sim \mathcal{N}\left(NC, \frac{2(NC)^2}{(2^q-1)}\right)$$

Hence $T(\phi, a)$ is also a normal deviate. Now we derive the mean $\mu_{T(\phi,a)}$ and variance $\sigma^2_{T(\phi,a)}$ of $T(\phi, a)$. Let Φ be the set of all possible samples of size

N. Then with variable fixation $a \in \mathbb{F}_2^s$ and variable sample $\phi \in \Phi$ where $|\phi| = N$, we can write:

$$\begin{aligned}
\mu_{T(\phi,a)} &= \frac{1}{2^s|\Phi|} \sum_{a\in\mathbb{F}_2^s,\phi\in\Phi} T(\phi,a) \\
&= \frac{1}{2^s|\Phi|} \sum_{a\in\mathbb{F}_2^s} \sum_{\phi\in\Phi} T_a(\phi) \\
&= \frac{1}{2^s} \sum_{a\in\mathbb{F}_2^s} \frac{1}{|\Phi|} \sum_{\phi\in\Phi} T_a(\phi) \\
&= \frac{1}{2^s} \sum_{a\in\mathbb{F}_2^s} \mu_{T_a(\phi)} \\
&= \frac{1}{2^s} \sum_{a\in\mathbb{F}_2^s} 2^q - 1 + NC(a) \\
&= 2^q - 1 + \mu_{NC(a)} \\
&= 2^q - 1 + NC
\end{aligned}$$

Let $\mu_{\mu_{T_a(\phi)}}$ be the mean of $\mu_{T_a(\phi)}$ over all the fixation a. That means $\mu_{T(\phi,a)} = \mu_{\mu_{T_a(\phi)}}$. So we write

$$\begin{aligned}
T(\phi,a) - \mu_{T(\phi,a)} &= T - \mu_{T_a(\phi)} + \mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}} \\
\left(T(\phi,a) - \mu_{T(\phi,a)}\right)^2 &= \Big((T(\phi,a) - \mu_{T_a(\phi)}) + (\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}})\Big)^2 \\
\frac{1}{2^s|\Phi|} \sum_{a\in\mathbb{F}_2^s,\phi\in\Phi} \left(T(\phi,a) - \mu_{T(\phi,a)}\right)^2 &= \frac{1}{2^s|\Phi|} \sum_{a\in\mathbb{F}_2^s,\phi\in\Phi} \Big((T(\phi,a) - \mu_{T_a(\phi)}) + (\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}})\Big)^2 \\
\sigma^2_{T(\phi,a)} &= \frac{1}{2^s|\Phi|} \sum_{a\in\mathbb{F}_2^s,\phi\in\Phi} \Big((T(\phi,a) - \mu_{T_a(\phi)}) + (\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}})\Big)^2
\end{aligned}$$

Consequently we find

$$\sigma^2_{T(\phi,a)} = \frac{1}{2^s|\Phi|} \sum_{a\in\mathbb{F}_2^s} \sum_{\phi\in\Phi} \Big((T(\phi,a) - \mu_{T_a(\phi)})^2 + 2(T(\phi,a) - \mu_{T_a(\phi)})(\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}}) + (\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}})^2\Big)$$

Let MT denote the the middle term at the right side in the above equation. Now let us analyse MT. $(\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}})$ part does not depend on the variable ϕ because $\mu_{T_a(\phi)}$ is the mean of $T_a(\phi)$ over all possible ϕ and $\mu_{\mu_{T_a(\phi)}}$ is a constant. As a result we can write

$$\begin{aligned}
MT &= \frac{1}{2^s|\Phi|} \sum_{a\in\mathbb{F}_2^s} \sum_{\phi\in\Phi} 2(T(\phi,a) - \mu_{T_a(\phi)})(\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}}) \\
&= \frac{2}{2^s|\Phi|} \sum_{a\in\mathbb{F}_2^s} (\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}}) \sum_{\phi\in\Phi} (T(\phi,a) - \mu_{T_a(\phi)})
\end{aligned}$$

Observe that for a fixed a, $T_a(\phi) = T(\phi, a)$.As a result we get

$$MT = \frac{2}{2^s|\Phi|} \sum_{a \in \mathbb{F}_2^s} \left(\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}}\right) \left(\sum_{\phi \in \Phi} T_a(\phi) - \sum_{\phi \in \Phi} \mu_{T_a(\phi)}\right)$$

By the definition of mean we know that $\left(\sum_{\phi \in \Phi} T_a(\phi) = \sum_{\phi \in \Phi} \mu_{T_a(\phi)}\right)$. This implies $MT = 0$. And we can continue deriving the variance of $T(\phi, a)$ as following.

$$\begin{aligned}
\sigma^2_{T(\phi,a)} &= \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} \frac{1}{|\Phi|} \sum_{\phi \in \Phi} (T_a(\phi) - \mu_{T_a(\phi)})^2 + \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} \frac{1}{|\Phi|} \sum_{\phi \in \Phi} (\mu_{T_a(\phi)} - \mu_{\mu_{T_a(\phi)}})^2 \\
&= \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} \sigma^2_{T_a(\phi)} + \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} \frac{1}{|\Phi|} \sum_{\phi \in \Phi} (2^q - 1 + NC(a) - 2^q + 1 - NC)^2 \\
&= \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} \sigma^2_{T_a(\phi)} + \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} \frac{1}{|\Phi|} \sum_{\phi \in \Phi} (NC(a) - NC)^2 \\
&= \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} \sigma^2_{T_a(\phi)} + \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} \sigma^2_{NC(a)} \\
&= \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} 2(2^q - 1 + 2NC(a)) + \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} \frac{2(NC)^2}{2^q - 1} \\
&= 2(2^q - 1 + 2NC) + \frac{2(NC)^2}{(2^q - 1)} \\
&= \frac{2(2^q - 1 + 2NC)(2^q - 1) + 2(NC)^2}{(2^q - 1)} \\
&= \frac{2((2^q - 1)^2 + 2(NC)(2^q - 1) + (NC)^2}{(2^q - 1)} \\
&= \frac{2}{(2^q - 1)} (2^q - 1 + NC)^2
\end{aligned}$$

□

To justify Hypothesis 1 we observe that

$$2^{-s} \sum_{a \in \mathbb{F}_2^s} p_\eta(a) = 2^{-q}$$

as this probability is the probability of the event $y_q = \eta$ taken over all plaintexts. The variance $p_\eta(a)$ taken over a may not be same for all $\eta \in \mathbb{F}_2^q$.

We will see in the Experiment chapter that the variance of "variance of $p_\eta(a)$ taken over a" taken over η is nonzero for any number of rounds. And the experimental and theoretical variance of $C(a)$ taken over all the possible a also differs by large value. However, interestingly we have found that, this does not affect the distance in between the theoretical and experimental variance of the statistic T as shown in Figures 6.4, 6.5, 6.6, 6.7 for the case of SMALLPRESENT-[4]. In an upcoming research paper [16], for SMALLPRESENT-[8], we have observed that the experimental variance of T is very larger than the theoretical variance but this happens only when the distinguisher already distinguishes itself from the uniform one. As a result, such a distance in between theory and experiment does not affect our original goal significantly.

4.2 Model for Multiple Fixations

Let $A \subseteq \mathbb{F}_2^s$ be a set of fixations, $\phi \subseteq \mathbb{F}_2^t$ be the sample which is sampled randomly with replacement and Φ is the set of all possible ϕ. In this context, the functions $\Omega : A \times \phi \to \mathbb{F}_2^q$ and $\omega : A \times \mathbb{F}_2^q \to \mathbb{Z}$ are defined so that

$$\Omega(a, x_t) = y_q \tag{4.8}$$
$$\omega(a, \eta) = \#\{\Omega(a, x_t) = \eta \mid x_t \in \phi\} \tag{4.9}$$

where $y = E((a, x_t), K) = (y_q, y_r)$ and $a \in A$

4.2.1 A given set of fixations

For a given set of fixations $|A| = M$ and any sample ϕ such that $|\phi| = S \leq 2^t$, the size of the domain of the distribution to be distinguished from random is $M2^q$. The distribution of the function ω is composed of the probabilities $p_{(a,\eta)}(A)$. In this context, let the statistic T be denoted by $T_A(\phi)$ is defined as

$$T_A(\phi) = \sum_{a \in A} \sum_{\eta \in \mathbb{F}_2^q} \frac{(\omega(a, \eta) - N2^{-q}M^{-1})^2}{N2^{-q}M^{-1}} \tag{4.10}$$

For simplicity, we restrict the considerations to the case where, for each fixation, the q bits of the ciphertext is computed for equally many, say S, different $x_t \in \mathbb{F}_2^t$. Then $N = MS$, We also observe that for a given a, $w_a(\phi) = w(\phi, a)$ and $T_a(\phi) = T(\phi, a)$. Consequently, and we get

$$\begin{aligned} T_A(\phi) &= \sum_{a\in A}\sum_{\eta\in\mathbb{F}_2^q} \frac{(\omega(a,\eta) - S2^{-q})^2}{S2^{-q}} \\ &= \sum_{a\in A}\sum_{\eta\in\mathbb{F}_2^q} \frac{(\omega_a(\eta) - S2^{-q})^2}{S2^{-q}} \\ &= \sum_{a\in A} T_a(\phi) \\ &= \sum_{a\in A} T(\phi, a) \end{aligned}$$

By Theorem 4.1.1, $T(\phi, a)$ is a normal deviate. And from the above equation we see $T_A(\phi)$ is a summation of $|A| = M$ number of normally distributed random variables. As a result, according to the property of normal distribution $T_A(\phi)$ is also normally distributed and we can write

$$\begin{aligned} T_A(\phi) &\sim \mathcal{N}\left(M\mu_{T_a(\phi)}, M\sigma^2_{T_a(\phi)}\right) \\ &= \mathcal{N}\left(M(2^q - 1 + SC), M\frac{2(2^q-1+SC)^2}{(2^q-1)}\right) \\ &= \mathcal{N}\left(M(2^q - 1) + MSC, M\frac{2(2^q-1+SC)^2}{(2^q-1)}\right) \end{aligned}$$

Which implies

$$T_A(\phi) \sim \mathcal{N}\left(M(2^q - 1) + NC, \frac{2M(2^q-1+SC)^2}{(2^q-1)}\right) \qquad (4.11)$$

But the tools developed in this thesis work offer also an alternative approach to determine the distribution of $T_A(\phi)$. Instead of splitting the domain of the distribution of (a, η) as a union of subdomains of size 2^q we can investigate the distribution over the large domain directly.

Let the capacity of the distribution $p(A) = \left(p_{(a,\eta)}(A)\right)$ be denoted by $C(A)$. We can now define $C(A)$ in the same way $C(a)$ is defined for the distribution $p(a) = \left(p_{(\eta)}(a)\right)$ in 3.21 and write

$$C(A) = |A|2^q \sum_{(a,\eta)\in A\times\mathbb{F}_2^q} \left(p_{(a,\eta)}(A) - \frac{1}{|A|2^q}\right)^2$$

By plugging in the definition of probability

$$p_{(a,\eta)}\left(A\right) = \frac{\#\{x_t \in \mathbb{F}_2^t \mid x_s = a, y_q = \eta\}}{|A|2^t},$$

we can write

$$C\left(A\right) = |A|2^q \sum_{(a,\eta)\in A\times\mathbb{F}_2^q} \left(\frac{\#\{x_t \in \mathbb{F}_2^t \mid x_s = a, y_q = \eta\}}{|A|2^t} - \frac{1}{|A|2^q}\right)^2 \quad (4.12)$$

Lemma 4.2.1. *Let us denote by $C(A)$ the capacity of the distribution over the values $(a,\eta) \in A \times \mathbb{F}_2^q$ as x_t varies in $\mathbb{F}_2^t$. Then*

$$C(A) = \frac{1}{|A|}\sum_{a\in A} C(a)$$

Proof. Let us recall that $C(a)$ is defined in (3.21) as

$$C(a) \;=\; 2^q \sum_{\eta\in\mathbb{F}_2^q}\left(p_\eta\left(a\right) - \frac{1}{2^q}\right)^2 \quad (4.13)$$

According to definition $p_\eta\left(a\right) = \frac{\#\{x_t\in\mathbb{F}_2^t \mid x_s=a,y_q=\eta\}}{2^t}$. By plugging this equality in 4.13, we continue as following

$$\begin{aligned}
|A|^{-1}\sum_{a\in A} C(a) &= |A|^{-1}\sum_{a\in A} 2^q \sum_{\eta\in\mathbb{F}_2^q}\left(\frac{\#\{x_t \in \mathbb{F}_2^t \mid x_s = a, y_q = \eta\}}{2^t} - \frac{1}{2^q}\right)^2\\
&= |A|^{-1}2^q \sum_{a\in A}\sum_{\eta\in\mathbb{F}_2^q}\left(\frac{\#\{x_t \in \mathbb{F}_2^t \mid x_s = a, y_q = \eta\}}{2^t} - \frac{1}{2^q}\right)^2\\
&= |A|^{-1}2^q \sum_{\eta\in\mathbb{F}_2^q, a\in A}\left(\frac{\#\{x_t \in \mathbb{F}_2^t \mid x_s = a, y_q = \eta\}}{2^t} - \frac{1}{2^q}\right)^2\\
&= |A|^{-1}2^q \sum_{\eta\in\mathbb{F}_2^q, a\in A}\frac{|A|^2}{|A|^2}\left(\frac{\#\{x_t \in \mathbb{F}_2^t \mid x_s = a, y_q = \eta\}}{2^t} - \frac{1}{2^q}\right)^2\\
&= |A|2^q \sum_{\eta\in\mathbb{F}_2^q, a\in A}\left(\frac{\#\{x_t \in \mathbb{F}_2^t \mid x_s = a, y_q = \eta\}}{|A|2^t} - \frac{1}{|A|2^q}\right)^2
\end{aligned}$$

Now using (4.12) in the last equality above, we have

$$\begin{aligned}
|A|^{-1}\sum_{a\in A} C(a) &= C(A), \text{ that is}\\
C(A) &= \frac{1}{|A|}\sum_{a\in A} C(a)
\end{aligned}$$

□

Lemma 4.2.2. *Let A be a set of fixations such that $A \subseteq \mathbb{F}_2^s$ and $|A| = M$ and $C(A)$ be the capacity of the distribution (a, η) where $a \in A$ and $\eta \in \mathbb{F}_2^q$. The average capacity of $C(A)$ as A runs over all possible subset of $\mathbb{F}_2^s$ such that $|A| = M$ is C which is also the average capacity of $C(a)$*

Proof. Let $\mu_{C(A)}$ denote the average capacity of $C(A)$ and $\mathcal{F}$ be the set family that contains all the M-subset of $\mathbb{F}_2^s$. Then we can write

$$\mu_{C(A)} = \frac{1}{|\mathcal{F}|} \sum_{A \in \mathcal{F}} C(A)$$

Now as per the Lemma 4.2.1 we can write

$$\begin{aligned}
\mu_{C(A)} &= \frac{1}{|\mathcal{F}|} \sum_{A \in \mathcal{F}} |A|^{-1} \sum_{a \in A} C(a) \\
&= \frac{1}{|\mathcal{F}|M} \sum_{A \in \mathcal{F}} \sum_{a \in A} C(a) \\
&= \frac{1}{|\mathcal{F}|M} \sum_{A \in \mathcal{F}, a \in A} C(a) \\
&= \frac{1}{|\mathcal{F}|M} \sum_{A \in \mathcal{F}, a \in A} C(a)
\end{aligned}$$

Observe that $|\mathcal{F}| = \binom{2^s}{M}$. As A runs through $\mathcal{F}$ and a runs through each of these M-subsets, each term $C(a)$ for each $a \in \mathbb{F}_2^s$ occurs $\binom{2^s-1}{M-1}$ many times. So, we can continue with the proof as following

$$\begin{aligned}
\mu_{C(A)} &= \frac{\binom{2^s-1}{M-1}}{\binom{2^s}{M} M} \sum_{a \in \mathbb{F}_2^s} C(a) \\
&= \frac{1}{2^s} \sum_{a \in \mathbb{F}_2^s} C(a) \\
&= C
\end{aligned}$$

□

Corollary 4.2.2.1. *The capacity $C(A)$ of set A of size M is approximately a normal deviate with mean $\mu_{C(A)} = C$ and variance $\sigma^2_{C(A)} = \frac{2C^2}{M(2^q-1)}$*

Proof. We know $C\left(a\right)$ is a normal deviate. According to the definition, $C\left(A\right)$ is average of $C\left(a\right)$ over all the $a \in A$. We know that average of a collection of normally distributed random variable is also normally distributed. Consequently $C\left(A\right)$ is a normal deviate. From lemma 2 we see that the mean $\mu_{C(A)} = C$. We know $C\left(A\right) = \frac{1}{|A|}\sum_{a\in A} C\left(a\right)$. So variance of $C\left(A\right)$ will be $\frac{1}{|A|^2}$ times the variance of $\sum_{a\in A} C\left(a\right)$. And variance of $\sum_{a\in A} C\left(a\right)$ is $|A|$ times the variance of $C\left(a\right)$. As a result, we write

$$\begin{aligned}\sigma^2_{C(A)} &= \frac{1}{|A|^2}|A|\sigma^2_{C(a)} \\ &= \frac{2C^2}{M(2^q-1)}\end{aligned}$$

□

Corollary 4.2.2.2. *For each fixed set $A \subseteq \mathbb{F}_2^s$ such that $|A| = M$ and variable sample of size $N = MS$ where S is the size of the sample $\phi \subseteq \mathbb{F}_2^t$ drawn randomly with replacement for each fixation $a \in A$, the statistic $T_A(\phi)$ is χ^2-distributed with non-central parameter $\delta(A) = NC(A)$ where degree of freedom is $M2^q - 1$. That is*

$$T_A(\phi) \sim \chi^2_{M2^q-1}(NC(A))$$

Proof. Recall the definition of $T_A(\phi)$

$$T_A(\phi) = \sum_{a\in A}\sum_{\eta\in\mathbb{F}_2^q} \frac{(\omega(a,\eta) - N2^{-q}M^{-1})^2}{N2^{-q}M^{-1}}$$

Here $\omega(a,\eta)$ is non-uniformly binomially distributed. So the mean and variance of $\omega(a,\eta)$ are $\mu_{\omega(a,\eta)} = Np_{(a,\eta)}\left(A\right)$ and $\sigma^2_{\omega(a,\eta)} = \frac{N}{M2^q}$. Where $\left(p_{(a,\eta)(A)}\right)$ is the probability distribution of function ω. As a result we get

$$T_A(\phi) = \sum_{a\in A}\sum_{\eta\in\mathbb{F}_2^q} \frac{(\omega(a,\eta) - \mu_{\omega(a,\eta)})^2}{\sigma^2_{\omega(a,\eta)}}$$

Now let us assume that $X = \omega(a,\eta) - \sigma^2_{\omega(a,\eta)}$. Then the mean and variance of X are $\mu_X = Np_{(a,\eta)}(A) - \frac{N}{M2^q}$ and $\sigma^2_X = \frac{N}{M2^q}$. So we write

$$T_A(\phi) = \sum_{a\in A,\eta\in\mathbb{F}_2^q} \frac{(X)^2}{\sigma^2_X}$$

Now as per the definition of non-central χ^2 distribution we see that

$$T_A(\phi) \sim \chi^2_{|A|2^q-1}(\delta(A))$$
$$T_A(\phi) \sim \chi^2_{M2^q-1}(\delta(A))$$

where

$$\begin{aligned}
\delta(A) &= \sum_{a\in A,\eta\in\mathbb{F}_2^q} \frac{\mu_X^2}{\sigma_X^2} \\
&= \sum_{a\in A,\eta\in\mathbb{F}_2^q} \frac{(Np_{(a,\eta)}(A) - \frac{N}{M2^q})^2}{\frac{N}{M2^q}} \\
&= NM2^q \sum_{a\in A,\eta\in\mathbb{F}_2^q} \left(p_{(a,\eta)}(A) - \frac{1}{M2^q}\right)^2 \\
&= NM2^q \sum_{a\in A,\eta\in\mathbb{F}_2^q} \left(\frac{1}{|A|}p_{(\eta)}(a) - \frac{1}{M2^q}\right)^2 \\
&= NM \sum_{a\in A} 2^q \sum_{\eta\in\mathbb{F}_2^q} \left(\frac{1}{|M|}p_{(\eta)}(a) - \frac{1}{M2^q}\right)^2 \\
&= NM \sum_{a\in A} \frac{1}{M^2} 2^q \sum_{\eta\in\mathbb{F}_2^q} \left(p_{(\eta)}(a) - \frac{1}{2^q}\right)^2 \\
&= N\frac{1}{|A|} \sum_{a\in A} C\left(a\right) \\
&= NC(A)
\end{aligned}$$

The last equality is as per Lemma 4.2.1. That means:

$$T_A(\phi) \sim \chi^2_{M2^q-1}(NC(A))$$

□

So now as per the property of χ^2-distribution the mean and variance of $T_A(\phi)$ are

$$\mu_{T_A(\phi)} = M2^q - 1 + NC(A) \tag{4.14}$$
$$\sigma^2_{T_A(\phi)} = 2(M2^q - 1 + 2NC(A)) \tag{4.15}$$

And according to the normal approximation of χ^2-distribution mentioned in Section 3.1.5, we have

$$T_A(\phi) \sim \mathcal{N}\left(M2^q - 1 + NC(A), 2(M2^q - 1 + 2NC(A))\right) \tag{4.16}$$

where ϕ is sampled randomly with replacement.

4.2.2 A variable set of fixations

Lemma 4.2.3. *Now let us consider the statistic $T(\phi, A)$ where the sample ϕ of size S which is sampled randomly with replacement and the set of fixations A of size M both are variable and $N = MS$. Then the mean and variance of $T(\phi, A)$ are*

$$\begin{aligned}\mu_{T(\phi,A)} &= M2^q - 1 + NC \\ \sigma^2_{T(\phi,A)} &= 2(M2^q - 1 + 2NC) + N^2\sigma^2_{C(A)}\end{aligned}$$

Proof. Let Φ is the set of all the ϕ with $|\phi| = S$. According to the definition, the mean of $T(a, \phi)$ over all the possible value of a and ϕ is

$$\mu_{T(\phi,A)} = \frac{1}{|\mathcal{F}||\Phi|}\sum_{\phi\in\Phi, A\in\mathcal{F}} T(\phi, A) \tag{4.17}$$

It is immediate to see that for a given set of fixations A, $T(\phi, A) = T_A(\phi)$. Using this equality in (4.17), we obtain

$$\mu_{T(\phi,A)} = \frac{1}{|\mathcal{F}|}\sum_{A\in\mathcal{F}}\frac{1}{|\Phi|}\sum_{\phi\in\Phi} T_A(\phi)$$

Consequently we can write

$$\begin{aligned}\mu_{T(\phi,A)} &= \frac{1}{|\mathcal{F}|}\sum_{A\in|\mathcal{F}|}\mu_{T_A(\phi)} &(4.18)\\ &= \mu_{\mu_{T_A(\phi)}} &(4.19)\end{aligned}$$

Now, by plugging (4.14) in (4.18) we obtain

$$\begin{aligned}\mu_{T(\phi,A)} &= \frac{1}{|\mathcal{F}|}\sum_{A\in|\mathcal{F}|}(M2^q - 1 + NC(A)) \\ &= \frac{|\mathcal{F}|(M2^q-1)}{|\mathcal{F}|} + \frac{1}{|\mathcal{F}|}\sum_{A\in|\mathcal{F}|}(NC(A)) \\ &= M2^q - 1 + N\mu_{C(A)}\end{aligned}$$

By applying the Lemma 4.2.2 in the last equality above, we can write

$$\mu_{T(\phi,A)} = M2^q - 1 + NC \tag{4.20}$$

Using (4.19), we can write

$$T(\phi, A) - \mu_{T(\phi,A)} = T(\phi, A) - \mu_{T_A(\phi)} + \mu_{T_A(\phi)} - \mu_{\mu_{T_A(\phi)}} \tag{4.21}$$

Taking the average of the square of both side of (4.21) over all the possible fixations and samples we have

$$\sigma^2_{T(\phi,A)} = \frac{1}{|\mathcal{F}||\Phi|} \sum_{\phi\in\Phi, A\in\mathcal{F}} (T(\phi, A) - \mu_{T_A(\phi)} + \mu_{T_A(\phi)} - \mu_{\mu_{T_A(\phi)}})^2$$

By expanding the right side of the above equation we can write

$$\begin{aligned} \sigma^2_{T(\phi,A)} &= \frac{1}{|\mathcal{F}||\Phi|} \sum_{\phi\in\Phi, A\in\mathcal{F}} (T(\phi, A) - \mu_{T_A(\phi)})^2 \\ &+ \frac{1}{|\mathcal{F}||\Phi|} \sum (\mu_{T_A(\phi)} - \mu_{\mu_{T_A(\phi)}})^2 \\ &+ \frac{1}{|\mathcal{F}||\Phi|} \sum_{\phi\in\Phi, A\in\mathcal{F}} 2(T(\phi, A) - \mu_{T_A(\phi)})(\mu_{T_A(\phi)} - \mu_{\mu_{T_A(\phi)}}) \end{aligned}$$

Let MT denote the the third term at the right side in the above equation. Now let us analyse MT. $(\mu_{T_A(\phi)} - \mu_{\mu_{T_A(\phi)}})$ part does not depend on the variable ϕ because $\mu_{T_A(\phi)}$ is the mean of $T_A(\phi)$ over all possible ϕ and $\mu_{\mu_{T_A(\phi)}}$ is a constant. As a result we can write

$$\begin{aligned} MT &= \frac{1}{|\mathcal{F}||\Phi|} \sum_{\phi\in\Phi, A\in\mathcal{F}} 2\left(T(\phi, A) - \mu_{T_{\phi,a}(A)}\right)\left(\mu_{T_A(\phi)} - \mu_{\mu_{T_A(\phi)}}\right) \\ &= \frac{2}{|\mathcal{F}||\Phi|} \sum_{A\in\mathcal{F}} \left(\mu_{T_A(\phi)} - \mu_{\mu_{T_A(\phi)}}\right) \sum_{\phi\in\Phi} \left(T(\phi, A) - \mu_{T_A(\phi)}\right) \end{aligned}$$

Observe that for a fixed A, $T_A(\phi) = T(\phi, A)$.As a result we get

$$MT = \frac{2}{|\mathcal{F}||\Phi|} \sum_{A\in\mathbb{F}_2^s} \left(\mu_{T_A(\phi)} - \mu_{\mu_{T_A(\phi)}}\right) \left(\sum_{\phi\in\Phi} T_A(\phi) - \sum_{\phi\in\Phi} \mu_{T_A(\phi)}\right)$$

By the definition of mean we know that $\left(\sum_{\phi\in\Phi} T_A(\phi) = \sum_{\phi\in\Phi} \mu_{T_A(\phi)}\right)$. This implies $MT = 0$. And we can continue deriving the variance of $T(\phi, A)$ as following.

$$\begin{aligned}
\sigma^2_{T(\phi,A)} &= \frac{1}{|\mathcal{F}|}\sum_{A\in\mathcal{F}}\frac{1}{|\Phi|}\sum_{\phi\in\Phi}(T_A(\phi)-\mu_{T_A(\phi)})^2 \\
&+ \frac{1}{|\mathcal{F}||\Phi|}\sum_{\phi\in\Phi,A\in\mathcal{F}}(M2^q-1+NC(A)-M2^q+1-NC)^2
\end{aligned}$$

By simplifying the right side of the above equation we obtain

$$\sigma^2_{T(\phi,A)} = \frac{1}{|\mathcal{F}|}\sum_{A\in\mathcal{F}}\sigma^2_{T_A(\phi)} + \frac{1}{|\mathcal{F}||\Phi|}\sum_{\phi\in\Phi,A\in\mathcal{F}}(NC(A)-NC)^2 \quad (4.22)$$

Now by using the (4.15) in (4.22) we can continue the derivation as following

$$\begin{aligned}
\sigma^2_{T(\phi,A)} &= \frac{1}{|\mathcal{F}|}\sum_{A\in\mathcal{F}}2(M2^q-1+2NC(A)) + \frac{1}{|\mathcal{F}||\Phi|}\sum_{\phi\in\Phi,A\in\mathcal{F}}(NC(A)-NC)^2 \\
&= \frac{1}{|\mathcal{F}|}\sum_{A\in\mathcal{F}}2(M2^q-1)+4NC(A) + \frac{N^2}{|\mathcal{F}||\Phi|}\sum_{\phi\in\Phi,A\in\mathcal{F}}(C(A)-C)^2
\end{aligned}$$

The mean of $C(A)$ over all possible A is C according to Lemma 4.2.2. So, according to the definition of the variance of any statistic and using the fact that $2(M2^q-1), 4N$, and $\sigma^2_{C(A)}$ over all possible A are constant, we can write the following:

$$\begin{aligned}
\sigma^2_{T(\phi,A)} &= 2(M2^q-1) + \frac{4N}{|\mathcal{F}|}\sum_{A\in\mathcal{F}}C(A) + \frac{N^2}{|\Phi|}\sum_{\phi\in\Phi}\frac{1}{|\mathcal{F}|}\sum_{A\in\mathcal{F}}(C(A)-C)^2 \\
&= 2(M2^q-1) + \frac{4N}{|\mathcal{F}|}\sum_{A\in\mathcal{F}}C(A) + \frac{N^2}{|\Phi|}\sum_{\phi\in\Phi}\sigma^2_{C(A)} \\
&= 2(M2^q-1) + 4NC + N^2\sigma^2_{C(A)} \\
&= 2(M2^q-1+2NC) + N^2\sigma^2_{C(A)}
\end{aligned}$$

$\square$

Recall that our objective is to find the distribution of the statistic T and in this context, $T(a,\phi)$. From Lemma 4.2.3, we can find the mean and variance of $T(a,\phi)$. And from Corollary 4.2.2.1, we find the value of $\sigma^2_{C(A)}$. So, by using the corollary in the lemma, we can continue computing the variance of

$T\left(a,\phi\right)$ as following

$$\begin{aligned}
\sigma^2_{T(\phi,A)} &= 2(M2^q-1+2NC)+N^2\sigma^2_{C(A)} \\
&= 2(M2^q-1+2NC)+\frac{2(NC)^2}{M(2^q-1)} \\
&= \frac{2(M2^q-M+M-1+2NC)M(2^q-1)+2(NC)^2}{M(2^q-1)} \\
&= \frac{2(M(2^q-1)+(M-1)+2NC)M(2^q-1)+2(NC)^2}{M(2^q-1)} \\
&= \frac{2((M(2^q-1))^2+M(2^q-1)(M-1)+2NCM(2^q-1))+(NC)^2}{M(2^q-1)} \\
&= \frac{2((M(2^q-1))^2+2NCM(2^q-1))+(NC)^2}{M(2^q-1)}+\frac{2M(2^q-1)(M-1)}{M(2^q-1)} \\
&= \frac{2(M(2^q-1)+NC)^2}{M(2^q-1)}+2(M-1)
\end{aligned}$$

As mentioned in Section 3.1.6, $T_A(\phi)$-is approximately normally distributed. Now as $C(A)$ is normally distributed, so is $NC\left(A\right)$. As a result, $T\left(\phi,A\right)$ is also normally distributed. That is

$$T\left(\phi,A\right) \sim \mathcal{N}(\mu_{T(\phi,A)},\sigma^2_{T(\phi,A)})$$

And consequently

$$T\left(\phi,A\right) \sim \mathcal{N}\left(M2^q-1+NC,\frac{2(M(2^q-1)+NC)^2}{M(2^q-1)}+2(M-1)\right)$$

where ϕ is sampled randomly with replacement. We observe that for sufficiently large value of q, the term $2(M-1)$ is negligibly small in the above variance. And q is always sufficiently large. To simplify the analysis of the data complexity of the distinguisher based on the statistic $T(\phi,A)$ we have used the following approximation

$$T\left(\phi,A\right) \sim \mathcal{N}\left(M2^q-1+NC,\frac{2(M(2^q-1)+NC)^2}{M(2^q-1)}\right) \tag{4.23}$$

Chapter 5

Data Complexity of SSA

In [5], the connection in between SS an TD is used to explain the statistical behaviour of the SS attack. In this thesis, we have developed a statistical model for the SS attack using the distribution properties directly and in this section we will derive the data complexity of an SS attack directly based on the success probabilities of the statistical test described in Section 3.3.

Let us consider the statistic T computed from a set of fixations as defined in (4.10). The set of fixations is denoted by A such that $|A| = M$. And let us set $T_0 = T$ when the function ω is uniformly distributed. Otherwise $T_1 = T$. By the definition of χ^2 distribution, both the statisti T_0, T_1 is χ^2 distributed. So, accoridng to the normal approximation of χ^2 distribution we find the mean μ_{T_0} and variance $\sigma^2_{T_0}$ of the statistic T_0 as following:

$$\mu_{T_0} = M2^q - 1 \quad (5.1)$$

$$\sigma^2_{T_0} = 2(M2^q - 1) \quad (5.2)$$

On the other hand, from (4.23), we know the mean μ_{T_1} and variance $\sigma^2_{T_1}$ of the statistic T_1 are as following:

$$\mu_{T_1} = M2^q - 1 + NC \quad (5.3)$$

$$\sigma^2_{T_1} = \frac{2(M(2^q-1) + NC)^2}{M(2^q-1)} \quad (5.4)$$

Now, let us find out what is the required value of N to successfully perform the statistical test mentioned in Section 3.3. To perform the test we need to find out a value of τ so that we can succeed in the test with certain minimum success probability. If α_0, α_1 is the maximum error probability of wrongly choosing distribution T_1 and T_0, then according to inequality 3.30 and as depicted in Figure 3.5, we can choose τ as following

$$\mu_{T_0} + \sigma_{T_0}\zeta_0 = \tau = \mu_{T_1} - \sigma_{T_1}\zeta_1 \tag{5.5}$$

where $\Phi(\zeta_i) = 1 - \alpha_i$ for $i \in \mathbb{Z}_2$ for the cumulative distribution function Φ of the standard normal distribution. Without loss of generality let us assume that $\alpha_0 > \alpha_1$. Then the minimum success probability is $1 - \alpha_0$. Using (5.5), we have derived a lower bound of N to achieve the mentioned minimum probability of succeeding in the test.

According to (5.1) and (5.3) we find that

$$\mu_{T_1} = \mu_{T_0} + NC \tag{5.6}$$

Plugging the above equality in (5.5), we find

$$\begin{aligned}
\mu_{T_0} + \sigma_{T_0}\zeta_0 &= \mu_{T_0} + NC - \sqrt{\frac{2\left(M\left(2^q-1\right)+NC\right)^2}{M\left(2^q-1\right)}}\zeta_1 \\
\sigma_{T_0}\zeta_0 &= NC - \sqrt{\frac{2\left(M\left(2^q-1\right)+NC\right)^2}{M\left(2^q-1\right)}}\zeta_1
\end{aligned}$$

By setting $NC = \theta$ and $M\left(2^q - 1\right) = \Theta$, we obtain

$$\begin{aligned}
\sigma_{T_0}\zeta_0 &= \theta - \sqrt{\frac{2\left(\Theta+\theta\right)^2}{\Theta}}\zeta_1 \\
\sigma_{T_0}\zeta_0 &= \theta - \sqrt{\frac{2}{\Theta}}\left(\Theta+\theta\right)\zeta_1 \\
\sigma_{T_0}\zeta_0 &= \theta - \sqrt{2\Theta}\zeta_1 - \sqrt{\frac{2}{\Theta}}\theta\zeta_1 \\
\theta\left(1 - \sqrt{\frac{2}{\Theta}}\zeta_1\right) &= \sigma_{T_0}\zeta_0 + \sqrt{2\Theta}\zeta_1
\end{aligned}$$

By replacing back the values of θ and Θ, and plugging in the value of σ_{T_0} from 5.2, we obtain the following

$$NC\left(1 - \sqrt{\frac{2}{M\left(2^q-1\right)}}\zeta_1\right) = \sqrt{2(M2^q-1)}\zeta_0 + \sqrt{2M\left(2^q-1\right)}\zeta_1$$

We take a simple over estimate of $\sqrt{2M\left(2^q-1\right)}$ by $\sqrt{2(M2^q-1)}$ and get

$$N_{SS} \quad = \quad \frac{\sqrt{2(M2^q-1)}\,(\zeta_0+\zeta_1)}{\left(1-\sqrt{\frac{2}{M(2^q-1)}}\zeta_1\right)C}$$

Note that N_{SS} is a lower bound. That is, the statsitical test will be successfull with the considered success probabilities for any larger value of N as well.

Chapter 6

Experiment and Evaluation

In the study of this thesis, we have considered different statistics of different types of distributions. However, we will limit our experiments in the following two statistics.

1. Distribution of the capacities $C(a)$ as the fixation a varies as approximated in Theorem 3.2.1. Here C is the average of $C(a)$ over all possible a. It is also the capacity of the ML approximation.

2. The distribution of $T(\phi, a)$ as both the data sample ϕ and the fixation a vary randomly. This distribution is approximated in Theorem 4.1.1.

The objective of the experiments is to check how well the experimental distributions of the above mentioned statistics agree with the theoretical approximations. In case of the experiment for the first statistic mentioned in the above list, we have to compute the capacity of the distribution of the values at the output of the SS trail. It requires to encrypt the whole codebook. Encrypting the whole codebook is impossible for the cipher PRESENT described in Section 2.4. Because the size of the full codebook for this cipher is 2^{64} which is too large to handle with the computational capability that we have. To avoid this problem, we have considered smaller versions of PRESENT called SMALLPRESENT-[4] and SMALLPRERSENT-[8]. In principle, they are exactly the same PRESENT we have defined in section 2.4 but with only 4 and 8 S-boxes. Specifications of smaller variants of PRESENT can be found in [12]. However, we have dicussed SMALLPRESENT-[n] in general, in Section 6.1, for the sake of the continuity of our discussion.

6.1 SMALLPRESENT-$[n]$

It is a similar SPN as we have discussed in section 2.4. The differences are, in SMALLPRESENT-$[n]$, the block size is $4n$. And in the sBoxLayer, there are n copies of the same S-box which is used in the original PRESENT. The pLayer is given by the following function P. Bit at the position i of the state is moved to bit position $P(i)$, where

$$P(i) = \begin{cases} n \times i \mod 4n-1 & \text{for } 0 \leq i < 4n-1 \\ 4n-1 & \text{for } i = 4n-1 \end{cases}$$

We note that for $n = 16$, this is exactly the linear transformation used in PRESENT that we have discussed in 2.4. Figure 6.2 and 6.3 shows the pLayer of SMALLPRESENT-[4] and SMALLPRESENT-[8] respectiviely. However, as the block size is now $4n$, the key scheduling algorithm requires a modification that produces kyes of length $4n$ in every round. It is achieved by considering the $4n$ rightmost bits of the corresponding round key of the origiinial PRESENT. Which means, there is no modification in the key scheduling algorithm but there is a modification in the bits which are considered as a round key. With these specifications, it is clear that when we set $n = 16$, SMALLPRESENT-$[n]$ becomes the PRESENT that we have discussed in Section 2.4

Now as we have defined SMALLPRESENT-$[n]$, we need to find feasible SS trails in the pLayers of them, so that we can use these trails in our experiments. In Section 2.7, we have discussed the principle of choosing an SS trail from the pLayer of an SPN. Based on this principle, in the rest of the sections of this chapter, we have chosen useful SS trails for both of the SMALLPRESENT-[4] and SMALLPRESENT-[8] . However, we will limit our experiments only for the case of SMALLPRESENT-[4]. We are also experimenting on SMALLPRESENT-[8] considering sampling without replacement and the result will be published in an upcoming research paper.

6.2 SS Trails in SMALLPRESENT-$[n]$

6.2.1 SMALLPRESENT-[4]

In SMALLPRESENT-[4], there are only 4 S-boxes. That means the block size is 16 bits. Figure 6.1 shows the non-linear layer of SMALLPRESENT-[4]. The SS trail mentioned in bold lines has 8 single bit trails in each of those three S-boxes. However, we have not conducted our experiment based on this trail because there are only a few bits left to obtain a sufficiently large sample for each fixation of those 9 input bits of the trail. Fortunately, there

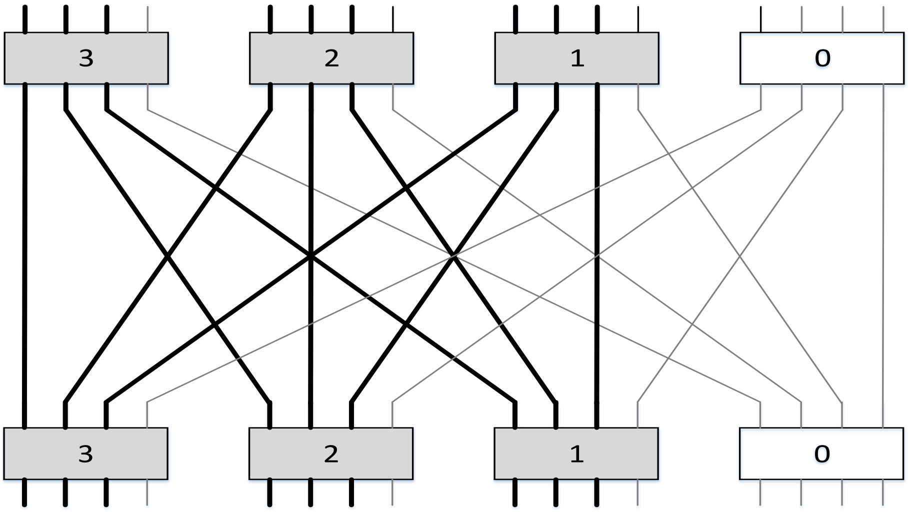

Figure 6.1: 9 bit SS trail in SMALLPRESENT-[4].

is another good trail if we consider the middle two bits of the middle two S-boxes. Because these four bits are involved only among the middle two S-boxes. That is, we have a SS trail of 4 bits with only 2 active S-boxes. Figure 6.2 shows this trail in bold lines. We have used this trail in our experiments later in this chapter.

6.2.2 SMALLPRESENT-[8]

In SMALLPRESENT-[8], there are 8 S-boxes. That means the block size is 32 bits. Figure 6.3 shows the non-linear layer of SMALLPRESENT-[8].

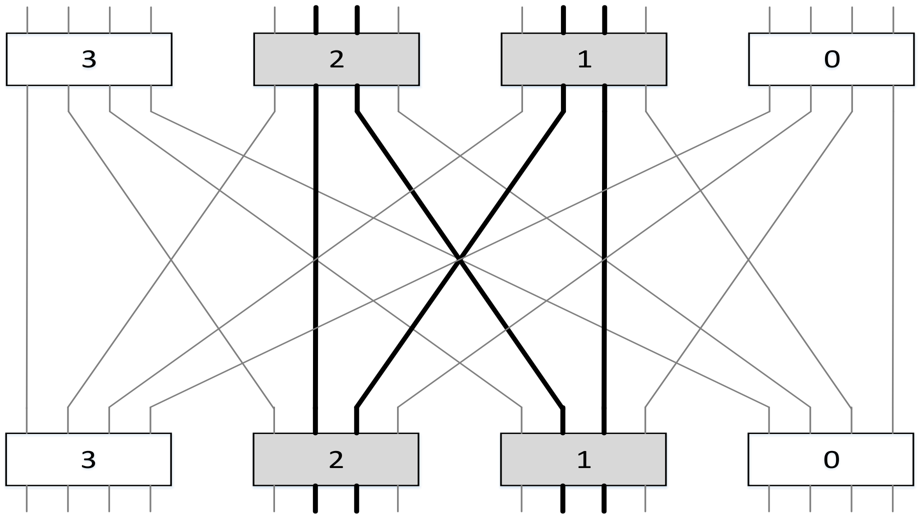

Figure 6.2: 4 bit SS trail in SMALLPRESENT-[4].

Based on the principle of choosing an SS trail, we have chosen the trail mentioned in bold lines in this figure.

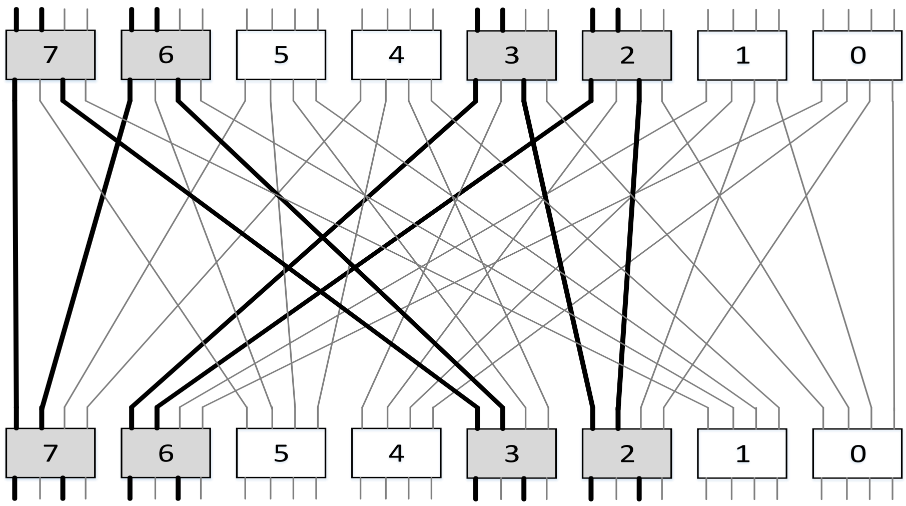

Figure 6.3: 8 bit SS trail in SMALLPRESENT-[8].

6.3 Experiments on SMALLPRESENT-[4]

The trail mentioned in bold lines in Figure 6.2 is used in these experiments. All the samples that we have used in our experiments are drawn randomly with replacement. At first we investigate the distribution of $C(a)$ as a varies. As the purpose is to investigate the distribution of $C(a)$, we do not need to consider the key. Then we investigate the distribution of the statistic T for a single fixation where both of the fixation and the sample are varible. Here a is a four bit value, and the size of the distribution is $|Y| = 2^4$. In the following sections we present the experimental results.

6.3.1 SSA Capacities $C(a)$:

Here $C(a)$ is the capacity of the distribution $p(a) = (p_\eta(a))$ where $a \in \mathbb{F}_2^4$ is the fixation at the input of the trail and $\eta \in \mathbb{F}_2^4$ is the value at the output of the trail. Which means, $C(a)$ is actually $C_{p(a)}$ as it is defined in Section 3.2.1. And it is computed according to (3.20). The experimental value of the variance of $C(a)$ is computed over all the possible fixations $a \in \mathbb{F}_2^4$. The theoretical variance is computed according to Theorem 3.2.1. The result is presented in Table 6.1.

From comparative analysis point of view, we observe that, for some numbers of rounds the practical variance is closer to the theoretical one than some other rounds. Now it would be interesting to check how this result agrees with Hypothesis 1. The question is, if the variances of $C(a)$ is comparatively far from the values predicted by the model, then, is it due to the fact that the probability distributions of $p_\eta(a)$ is also far from satisfying the hypothesis? That is, are the variances of $p_\eta(a)$ vary a lot with η? Similarly, if the variance of $C(a)$ is comparatively closer to the prediction by the model, is it also the case that $p_\eta(a)$ have smaller variances? Here $p_\eta(a)$ is calculated using the formula mentioned in (3.19). Which in our case looks like following:

$$p_\eta(a) = \frac{1}{2^{12}} \{x | E_k(x, a) = \eta\}$$

Table 6.1 also compares “Distance between theoretical and experimental $\sigma^2_{C(a)}$” with “variance of $\sigma^2_{p_\eta(a)}$ over all η”

Table 6.1

Round	$C = \frac{1}{2^4}\sum_{a\in\mathbb{F}_2^4} C(a)$	$\sigma^2_{C(a)}$ (Experimental)	$\sigma^2_{C(a)}$ (Theoretical)	Distance	Variance of $\sigma^2_{p_\eta(a)}$ (over all η)
1	1.2500000000	0.000000000000	0.208333328366	0.208333328366	0.000000000000000
2	0.0864257812	0.000053644180	0.000995922135	0.000942277955	0.000000000818545
3	0.0263200998	0.000082312916	0.000092366354	0.000010053438	0.000000001487419
4	0.0084733963	0.000012357389	0.000009573126	0.000002784263	0.000000000223686
5	0.0046606063	0.000002714300	0.000002896167	0.000000181867	0.000000000046755
6	0.0039848089	0.000002259238	0.000002117160	0.000000142078	0.000000000014765
7	0.0029691457	0.000000661685	0.000001175444	0.000000513759	0.000000000015007
8	0.0041698217	0.000001235339	0.000002318322	0.000001082983	0.000000000019639
9	0.0041134357	0.000002544029	0.000002256047	0.000000287982	0.000000000015644
10	0.0029462575	0.000001245313	0.000001157391	0.000000087922	0.000000000024034
11	0.0030920505	0.000000583181	0.000001274770	0.000000691590	0.000000000015651
12	0.0034888982	0.000002455807	0.000001622988	0.000000832819	0.000000000030971
13	0.0038551092	0.000001477955	0.000001981582	0.000000503627	0.000000000017599
14	0.0035421848	0.000001178269	0.000001672943	0.000000494674	0.000000000022411
15	0.0033624172	0.000001049226	0.000001507447	0.000000458220	0.000000000015530
16	0.0040042400	0.000001861589	0.000002137858	0.000000276270	0.000000000012828
17	0.0033563375	0.000000747953	0.000001502000	0.000000754047	0.000000000013699
18	0.0033963918	0.000001104406	0.000001538064	0.000000433658	0.000000000016437
19	0.0035276412	0.000001275685	0.000001659234	0.000000383549	0.000000000009210
20	0.0036349296	0.000002631222	0.000001761695	0.000000869527	0.000000000026018
21	0.0034182071	0.000001446692	0.000001557885	0.000000111193	0.000000000017467
22	0.0035172700	0.000004566781	0.000001649492	0.000002917289	0.000000000038211
23	0.0029666423	0.000001265739	0.000001173462	0.000000092277	0.000000000009836
24	0.0026813745	0.000000865261	0.000000958636	0.000000093375	0.000000000012813
25	0.0035705566	0.000002094620	0.000001699850	0.000000394770	0.000000000024349
26	0.0033077001	0.000000503365	0.000001458784	0.000000955419	0.000000000018401
27	0.0032589435	0.000001036276	0.000001416095	0.000000379819	0.000000000020941
28	0.0035127401	0.000002022870	0.000001645246	0.000000377624	0.000000000025578
29	0.0032626390	0.000001063931	0.000001419308	0.000000355377	0.000000000015406
30	0.0038447380	0.000002793566	0.000001970935	0.000000822632	0.000000000035005
31	0.0032460689	0.000001083049	0.000001404929	0.000000321879	0.000000000040317

Comparatively, we find that the theoretical model disagrees strongly in round 22 but agrees better in round 23. And interestingly we find that the variance of $p_\eta(a)$ over all η in round 22 is very large but comparatively small in round 23. This suggests that the smaller the distance between the theoretical model and the experimental computation, the closer the hypothesis tends to be valid.

One important thing to note here is that we do not yet have a proper understanding of what is a small difference or what is a large difference in between the theoretical and experimental values. But we know that our objective is to be a able to distinguish a distribution from random. In other words, we need to know, how useful the theoretical models are, when we use them to perform the statistical test. To visualize this effect, let us check how the theoretical and experimental values of the statistic $T(\phi, a)$ evolves as the sample size grows and when they start to distinguish from the random distribution.

6.3.2 Statistic $T(\phi, a)$

For each fixation a we draw a line for the statistic $T(\phi, a)$ computed from experimental data. We plot the size of the sample in the X-axis. The same sample is used for all the fixations. That is, For all samples ϕ_1, ϕ_2 used in the experiment, if $|\phi_1| = |\phi_2|$, then $\phi_1 = \phi_2$. And if $|\phi_1| < |\phi_2|$, then $\phi_1 \subset \phi_2$. We also draw the lines for variable fixation and variable sample calculated from theoretical distribution as in Theorem 4.1.1 and presented in gray color. The dark gray area represents 1 standard deviation around the theoretical mean. And the light gray area represents 2 standard deviation around the theoretical mean. We draw the plotting for round $3, 4, 22$ and 23 in Figures 6.4, 6.5,6.6 and 6.7. The reason to draw the plot of round 3 and 4 is to see how the evolution of the statistic happens in case of smaller number of rounds. And round 22, 23 are chosen as they were found interesting in previous section. Observe that, in all the cases of round $3, 4, 22$ and 23, they are in close accordance with the theoretical distribution. And in the cases of round 3 and 4, both of the theoretical and experimental distribution distinguishes itself from the uniformly random distribution.

These plots are also in close accordance with the theoretical data complexity N_{SS} that we have derived in previous chapter. In practice, distinguishing becomes possible when the sample size is large enough so that all the red lines are clearly above the random ($T = 15$). In theory, we can calculate the estimates of N_{SS} using (5.7). First we set the values of $\zeta_0 = \zeta_1$ to $\sqrt{2}$ which theoretically suppose to provide 85% success probability of the statistical test. Then using the values of C for the corresponding round gives the theoretical estimation of N_{SS} for that particular round. We see that using this method the theoretical values of N_{SS} for round $3, 4, 22$ and 23 are around $2^{10.20}, 2^{11.84}, 2^{13.1}$ and $2^{13.35}$ respectively. In contrast, from the experimental plots we see that the red lines start to distinguish at around the same values of $|\phi|$ in the horizontal axis for the case of round 3 and 4. From the theoretical values of N_{SS} for round 22 and 23, we also find that it distinguishes at the value of N_{SS} which is larger than the full codebook for a fixation. And this is also visible in the plots of those rounds. They do not distinguish at all.

So far, in the experiments of $T(\phi, a)$, we have used the same sample of equal

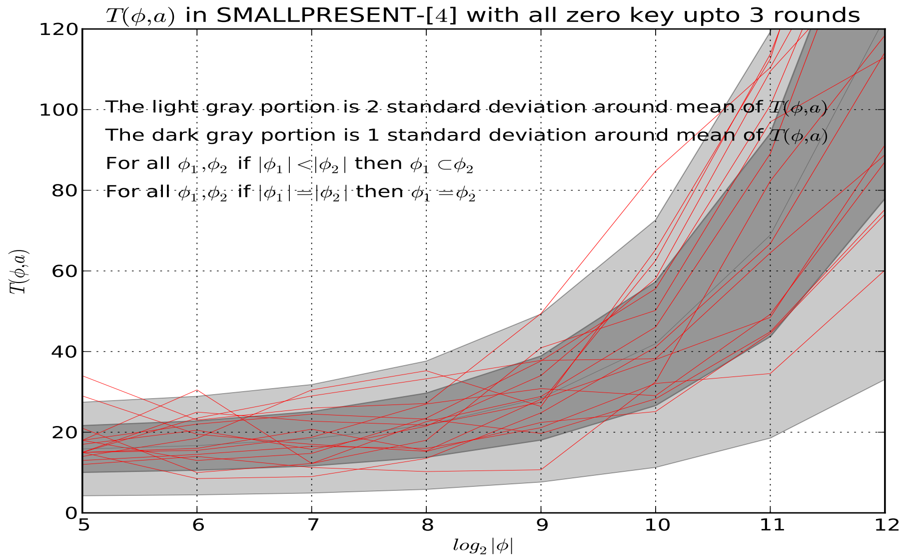

Figure 6.4: $T(\phi, a)$ with 3 rounds

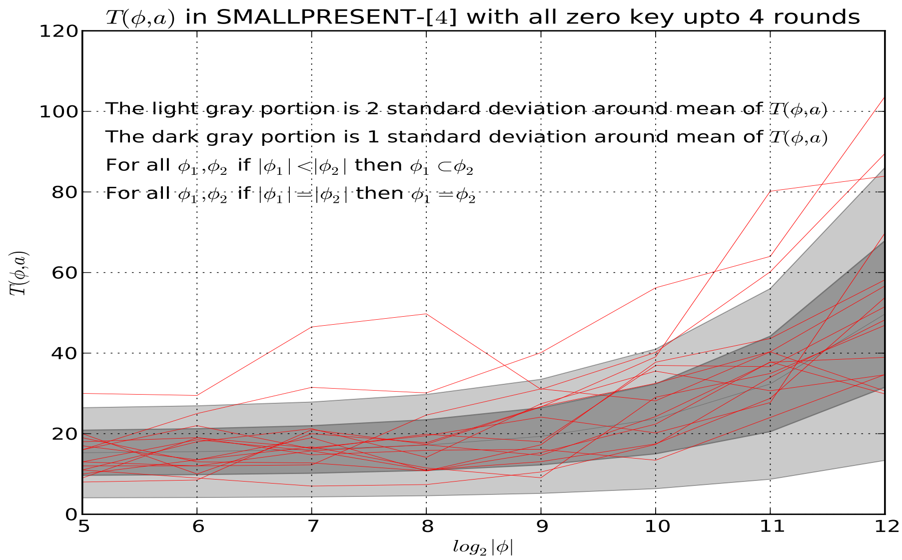

Figure 6.5: $T(\phi, a)$ with 4 rounds

size for each fixation. Now, let us do the experiment in another way. Let us look at distribution of $T(\phi, a)$ for a particular round using different fixations and samples of similar sizes. We have used all the possible fixations from 0x0 to 0xf. For each fixation, we have 10000 samples. Each sample has a size of

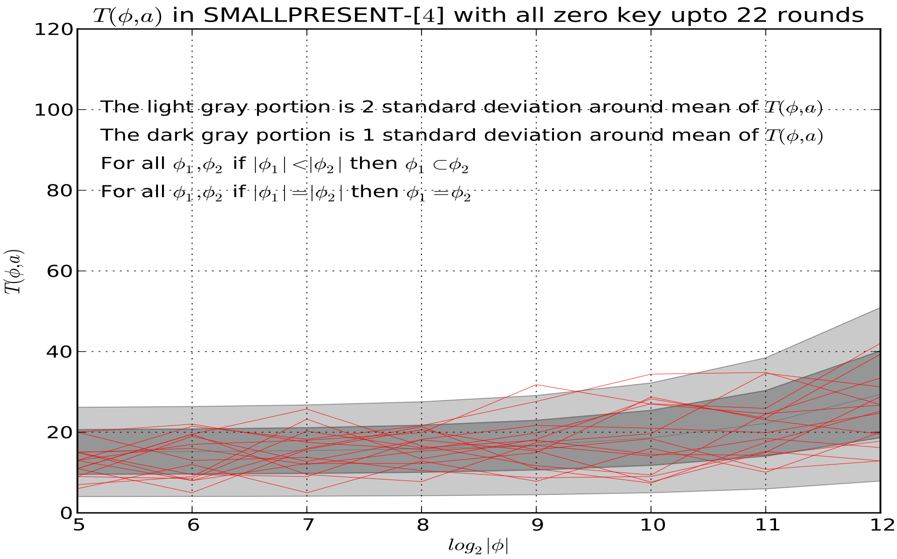

Figure 6.6: $T(\phi, a)$ with 22 rounds

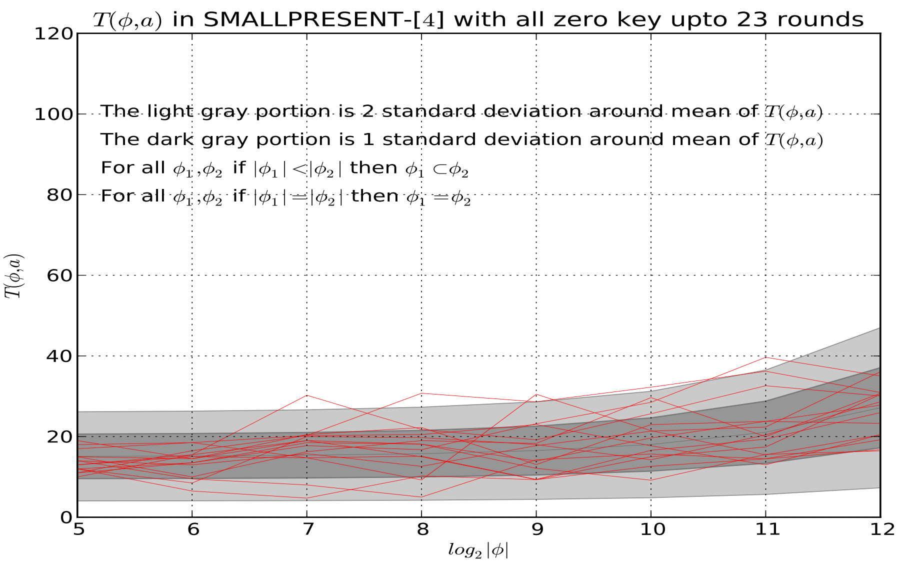

Figure 6.7: $T(\phi, a)$ with 23 rounds

2048 plaintexts and they are chosen randomly with replacement. In this way we had $10000 \times 16 = 160000$ different $T(\phi, a)$ values. We have calculated the mean and variance of these values of T. Then we have compared these with the theoretical values obtained from Theorem 4.1.1. Figures 6.8,6.9,6.10 and

6.11 shows the theoretical and experimental distribution for round $03, 04, 22$ and 23. We observe that the experimental distribution is a little skewed than the theoretical distribution. This is expected as the statistic is originally χ^2 distributed and we have used a normal approximation of χ^2 distribution. As the normal approximation of χ^2 distribution is better satisfied for higher degree of freedom, we understand that the experimental and theoretical distribution will agree better as the number of bits at the output of the SS trail grows. Note that, as like the previous visualization, we observe the same phenomenon in these plots also. For round 3 it nicely distinguishes from uniform distribution. For round 4 it looks slightly worse. Nevertheless, it is understandable that the N_{SS} for round 4 is $2^{11.84}$ and we have used sample of size 2^{11} only. And for round 22 and 23, they do not distinguishes at all.

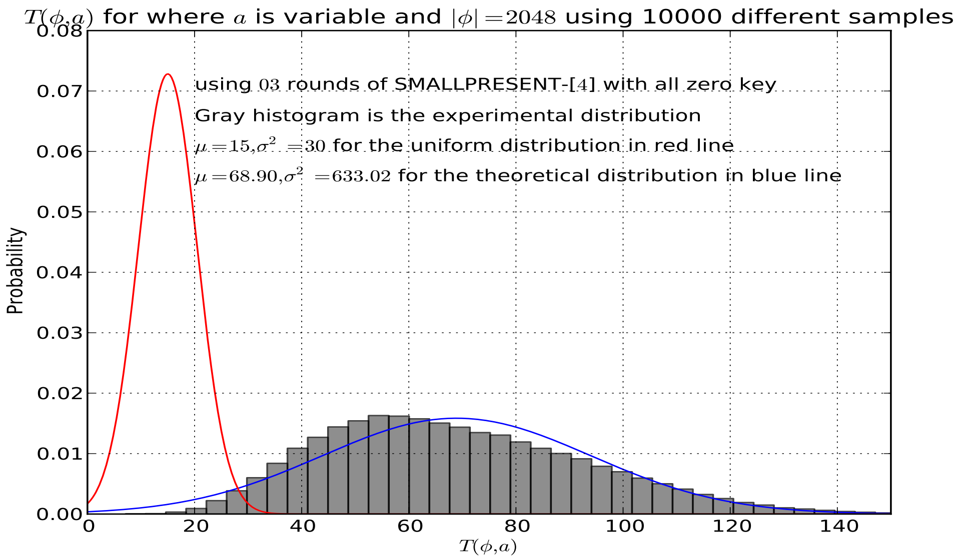

Figure 6.8: $T(\phi, a)$ with 03 rounds

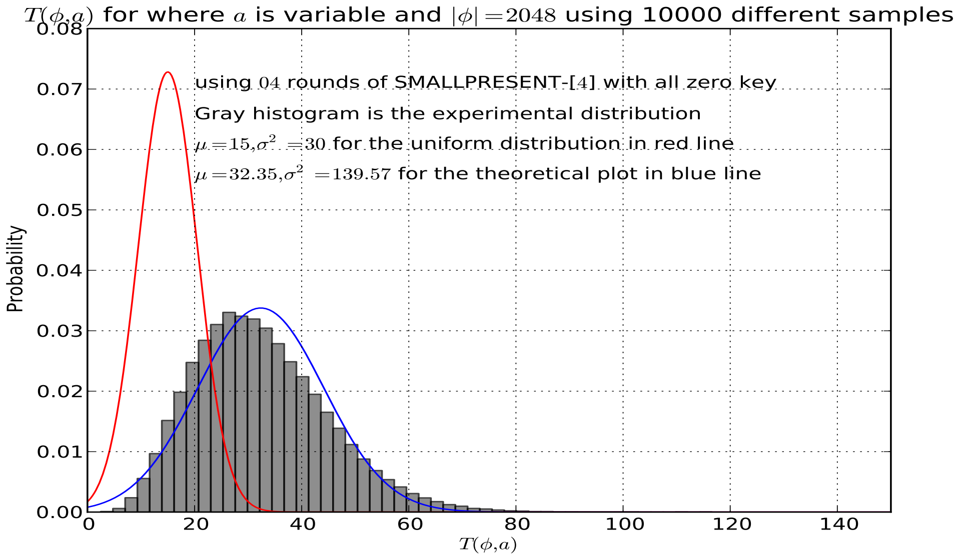

Figure 6.9: $T(\phi, a)$ with 04 rounds

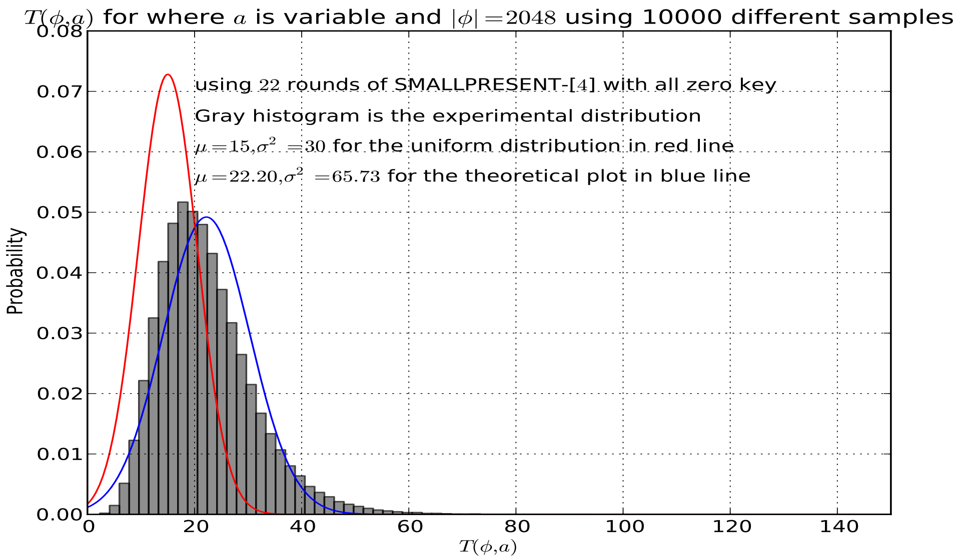

Figure 6.10: $T(\phi, a)$ with 22 rounds

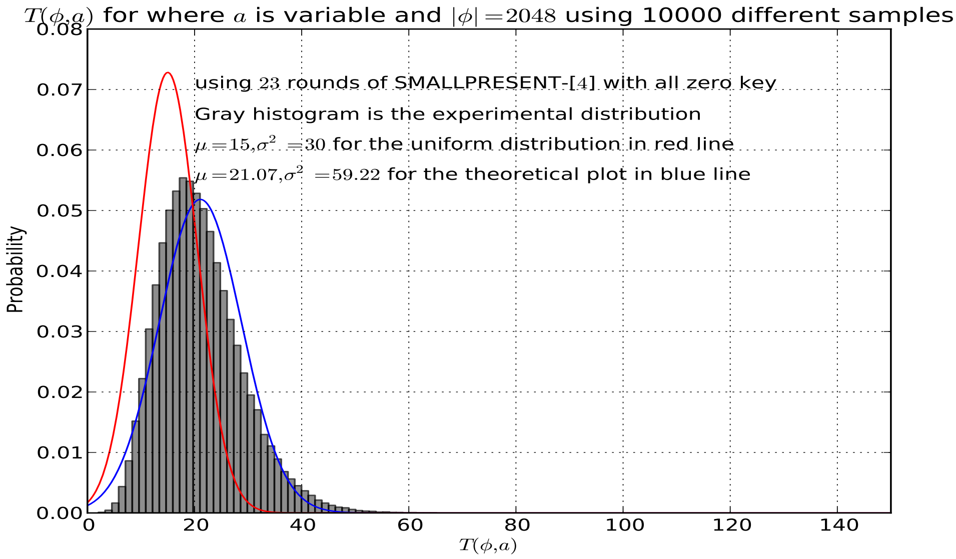

Figure 6.11: $T(\phi, a)$ with 23 rounds

Chapter 7

Conclusions

SSA is a comparatively recent statistical cryptanalytic technique among various others, as for example linear and differential cryptanalysis. Researchers have tried and established statistical links among different techniques. Blondeau and Nyberg showed one important link in between TD and SS attacks. They showed that TD attack using structures is identical to the sampling algorithm of SSA [5]. Then they used the statistical model of the TD attack to explain the behaviour of SS attack. However, there was no statistical model available which was developed based on the properties of SSA directly. In this thesis, we used the distribution at the output of an SS trail directly to develop a statistical model instead of using any link with other techniques.

If an SS trail is chosen wisely as discussed in Chapter 2, then there is a significant degree of non-uniformity in the distribution of the values at the output of the trail. As discussed in Chapter 2, to perform an SSA, we are in need of an attack that distinguishes the non-uniform distribution from uniform distribution, which eventually can be transformed into a key recovery attack. This thesis has focused only on this distinguishing attack and has not discussed the key recovery attack in detail. In Chapter 3, we have presented a statistical test that can perform this distinguishing attack. To perform the statistical test we have developed the statistic T based on the distribution of the values at the output bits of the SS trail, when the bits at the input of the SS trail are fixed and sufficiently many plaintexts are encrypted. The plaintexts differ from each other only in the non-trail input bits.

In Chapter 4, we have derived the distribution of a few different variants of this statistic T. We have shown that all of these variants of T, which are originally χ^2 distributed are also approximately normally distributed. The mean and variance of all of these variants of T are also derived in this chapter, which enables us to perform the statistical test. We also have derived a reasonable overestimation of the number of required plaintexts (in Chapter 5) to be encrypted to perform the distinguishing attack with an arbitrarily fixed success probability, which is referred as the data complexity of SSA and denoted by N_{SS}. Finally, in Chapter 6, we have verified the statistical model by experimenting on a small variant of the block cipher PRESENT called SMALLPRESENT-[4] for the case of a single fixation. The result shows that, the distinguishing attack is successful with very high success probability within the theoretical data complexity bound for smaller rounds. For large number of rounds, the theoretical data complexity is larger than the full code book excluding the fixed bits. As a result they do not distinguish at all using a single fixation. It could be the case that if we used multiple fixations, the distinguisher would distinguish itself from the uniform distribution. That is, there is a scope of more experiments based on multiple fixations.

Both in the theories and experiments it has been considered that, the sample for each fixation is chosen randomly with replacement. When the sample size approaches the full code book excluding the fixed bits, the only sensible option is to use sampling without replacement. However, in real life cryptanalysis the sample size almost never appraoches the full codebook. As a result, we recon, sampling with replacement is good enough for a successfull distinguishing attack. However, in an upcoming paper [16], the case of sampling without replacement is considered. And the experiments have also been extended to SMALLPRESENT-[8] for both of the cases of sampling with or without replacement.

Bibliography

[1] Agency, N. S. Cryptanalysis/signals analysis. `https://www.nsa.gov/careers/career_fields/cryptsiganalysis.shtml`.

[2] Blondeau, C., and Nyberg, K. On distinct known plaintext attacks. In *The Ninth International Workshop on Coding and Cryptography 2015.*

[3] Blondeau, C., and Nyberg, K. Perfect nonlinear functions and cryptography. In *Finite fields and their applications [1071-5797] Blondeau, Celine v:2015 vol:32*, pp. 120 –147.

[4] Blondeau, C., and Nyberg, K. New links between differential and linear cryptanalysis. In *Advances in Cryptology - EUROCRYPT 2013 [3-642-38347-5; 3-642-38348-3]* (2013), pp. 388–404.

[5] Blondeau, C., and Nyberg, K. Links between truncated differential and multidimensional linear properties of block ciphers and underlying attack complexites. In *Advances in Cryptology - EUROCRYPT 2014 [3-642-55219-6; 3-642-55220-X]* (2014), pp. 165 –182.

[6] Bogdanov, A., Knudsen, L. R., Leander, G., C. Paar, A. P., Robshaw, M. J. B., Seurin, Y., and Vikkelsoe, C. Present: An ultra-lightweight block cipher. vol. 4727 2007.

[7] Bowker, and Lieberman. *Engineering Statistics, Chapter: Other Probability Distribution, page: 72.*

[8] Chabaud, F., and Vaudenay, S. Links between differential and linear cryptoanalysis. In *De Santis, A. ed: EUROCRYPT-94, Vol. 950 of LNCS, Springer* (1994), pp. 356–365.

[9] Charles M. Grinstead, J. L. S. *Introduction to Probability, Chapter: Distributions and Densities, page: 184.*

[10] Cho, J. Y. Linear cryptanalysis of reduced-round present. In *Lecture Notes in Computer Science Volume 5985, 2010*, pp. 302 –317.

[11] Collard, B., and Standaert, F.-X. A atatistical saturation attack against the block cipher present. In *Lecture Notes in Computer Science Volume 5473, 2009* (2009), pp. 195–210.

[12] Leander, G. Small scale variants of the block cipher present. https://eprint.iacr.org/2010/143.pdf.

[13] Leander, G. On linear hulls, statistical saturation attacks, present and a cryptanalysis of puffin. In *Paterson, K.G. ed.: EUROCRYPT 2011. Vol. 6632 of LNCS, Springer* (2011), pp. 303–322.

[14] Nyberg, K. Distribution cryptanalysis, summer school, icebreak 2013. http://ice.mat.dtu.dk/slides/lecture2_kaisa.pdfn.

[15] Nyberg, K. Perfect nonlinear s-boxes. In *Lecture Notes in Computer Science [0302-9743] Nyberg, K v:1991 vol:547*, pp. 378 –386.

[16] Nyberg, K., and Khan, M. Statistical models for the statistical saturation distinguishers. In *Selected Areas in Cryptography 2015 (Submitted).*

[17] Scheaffer, R. L., and McClave, J. T. *Statistics for Engineers, Chapter: Common Continuous Probability Distributions, page: 102 – 104.*

[18] Scheaffer, R. L., and McClave, J. T. *Statistics for Engineers, Chapter: Satistics and Sampling Distributions, page: 140.*

[19] Stinson, D. R. *Cryptography Theory and Practice, Chapter: Block Ciphers and the Advanced Encryption Standard, page: 74 – 79*, third ed.

[20] Stinson, D. R. *Cryptography Theory and Practice, Chapter: Classical Cryptography, page: 1*, third ed.

[21] UAH. The gamma distrigution, definition: 31. http://www.math.uah.edu/stat/special/Gamma.html.

[22] UAH. The gamma distrigution, definition: 33. http://www.math.uah.edu/stat/special/Gamma.html.

[23] Walck, C. *Hand-book on STATISTICAL DISTRIBUTIONS for experimentalists, Chapter: Chi-square Distribution, page: 39.*