The Pseudorandomness of Elastic Block Ciphers

Debra L. Cook and Moti Yung and Angelos Keromytis
Department of Computer Science, Columbia University
{*dcook,moti,angelos*}@*cs.columbia.edu*

September 28, 2005

Abstract

We investigate elastic block ciphers, a method for constructing variable length block ciphers, from a theoretical perspective. We view the underlying structure of an elastic block cipher as a network, which we refer to as an elastic network, and analyze the network in a manner similar to the analysis performed by Luby and Rackoff on Feistel networks. We prove that a three round elastic network is a pseudorandom permutation and a four round network is a strong pseudorandom permutation when the round functions are independently chosen pseudorandom permutations. As a result, the elastic network allows for the creation of pseudorandom permutations and strong pseudorandom permutations with variable length inputs from PRPs with fixed length inputs.

Keywords: Elastic Network, PRP, SPRP

1 Introduction

Within this paper we analyze the elastic block cipher construction defined in [1]. This is a method for converting existing block ciphers into variable length block ciphers. The elastic block cipher construction can be viewed as a network, which we will refer to as the elastic network. We investigate the network from a theoretical perspective. We perform an analysis similar to that performed on Feistel networks by Luby and Rackoff in [2] and by Noar and Reingold in [3]. The purpose of our analysis is to capture the intrinsic properties of the network, assuming certain properties of the round functions, as Luby and Rackoff did for Feistel networks.

We first show that the elastic network with three or more rounds and round functions that are random permutations is a pseudorandom permutation (PRP). This allows us to prove that a three round elastic network is a PRP and a four round network is a strong PRP (SPRP) when the round functions are independently chosen PRPs. Our results show that the elastic network can be used to create PRPs and SPRPs with variable length inputs from PRPs with fixed length inputs. We also show that a two round elastic network and a modified three round elastic network are not PRPs, and that a three round elastic network is not a SPRP.

The remainder of the paper is organized as follows. In Section 2 we provide an overview of the elastic network structure, compare the elastic network to a Feistel network and review the concepts of a PRP and a SPRP. In Section 3 we prove that an elastic block cipher is a PRP when the original cipher contains at least two rounds and each round function is an independently chosen random permutation. In Section 4 we consider two, three and four round versions of an elastic network in terms of which ones are PRPs and which ones are SPRPs. We prove that a three round elastic network with independently chosen PRPs as round functions is a PRP and that a four round elastic network with independently chosen PRPs as round functions is a SPRP. In Section 5 we conclude the paper.

2 Background

2.1 Elastic Network

We review the elastic network from [1] and the difference between it and a Feistel network. The purpose of an elastic block cipher is to create a variable length block cipher from an existing block cipher. Given a block cipher, G, that is structured as a series of r rounds and processes b bit blocks, a variable length block cipher, G', will be created that can process block sizes of $b+y$ bits where $0 \leq y \leq b$. The number of rounds, r', in G' will be $r + \lceil yr/b \rceil$. We note that if G is a Feistel network, the round function of G will be viewed as consisting of one cycle of the Feistel network as opposed to just the function used within the Feistel network. The elastic network structure is shown in Figure 1. Using a round function which processes b bits, the elastic network processes $b+y$ bits, where $0 \leq y \leq b$, by leaving y bits out of the round function in each round. Between rounds the bits omitted from the round function are XORed with a subset of y bits output from the round function, with the subset of y bits becoming the bits omitted from the next round. The decryption function for G' consists of the network applied in reverse and the round function replaced by its inverse. If G is a Feistel network, the inverse of the round function is a cycle of G run in reverse. We omit the intial and final key dependent mixing steps present in [1] from our description because these are external to the elastic network structure and do not impact our analysis of the elastic network.

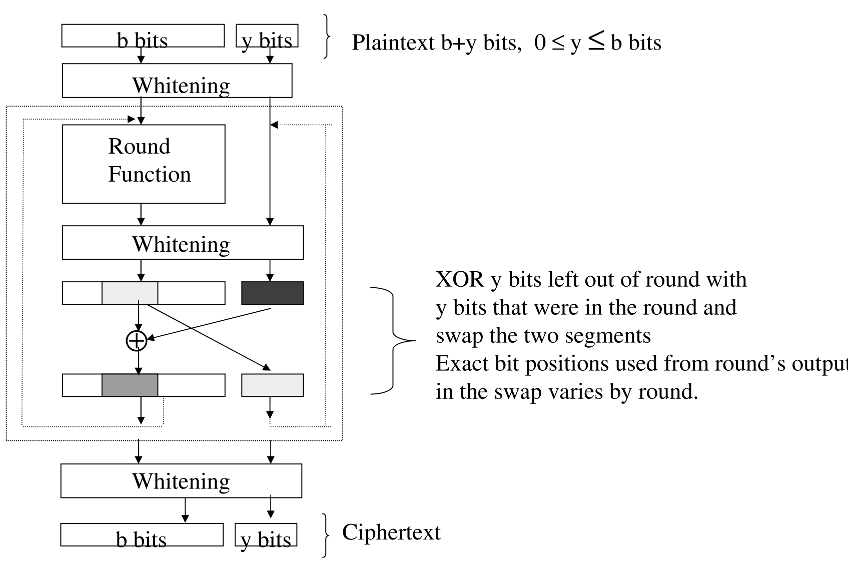

Figure 1: **Elastic Network**

The general design for elastic ciphers is similar to an unbalanced Feistel network, thus it is worth explaining the difference between the elastic network and an unbalanced Feistel network [4]. Figure 2 shows

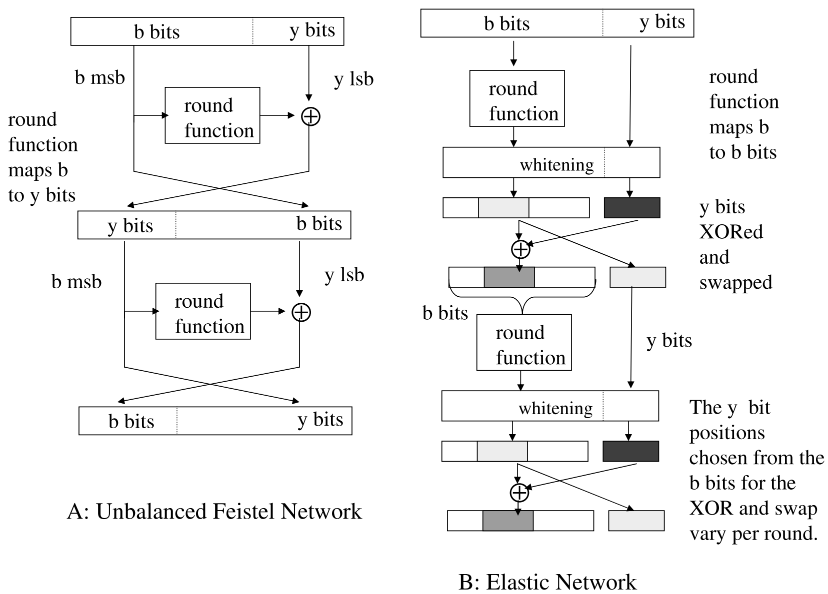

Figure 2: **Unbalanced Feistel Network Compared to Elastic Network**

the structure of an unbalanced Feistel network compared to the elastic network. In a (balanced) Feistel network, the block is split into two components of equal length; whereas, in an unbalanced Feistel network the components do not have the same length and the lengths of the round function's input differs from the length of its output. The structure of the Feistel network allows the same round function to be used for both encryption and decryption. The elastic network also involves splitting the block into two components, applying the round function to one component then XORing and swapping bits between the components to form the input to the next round. The elastic network differs from an unbalanced Feistel network in several ways. First, the round function of the elastic network must be invertible; whereas, the round function of the unbalanced Feistel network does not need to be invertible. This is because the structures differ in what bits form the input to the round function. In an unbalanced Feistel network the input to round n is XORed with the output of round $n+1$ to form the input to round $n+2$. In the elastic network, bits from the outputs of rounds n and $n+1$ are XORed when forming the input to round $n+2$. Second, the bit positions for the y bits omitted from the round function vary in the elastic block cipher; whereas, they are always the least significant bits in the unbalanced Feistel network. Third, the round function maps b bits to b bits in the elastic network and maps b bits to y bits in the unbalanced Feistel network. Fourth, $y \leq b$ in the elastic network; whereas, an unbalanced Feistel network places no restriction on the length of y in relation to b.

While the elastic network requires the inverse of the round function, the rate of diffusion is greater than that of the unbalanced Feistel network when the round functions provide the same amount of diffusion, $y \neq b$, and if all input bits to the round function do not impact all output bits. In fact, the round function in an unbalanced Feistel network must be defined very carefully; otherwise, it is possible for certain bits to have no impact on the other bits over several rounds or even over all the rounds. This results in the elastic network requiring fewer rounds to achieve complete diffusion than the number required by an unbalanced Feistel network under the conditions stated. We note that when the original block cipher is a Feistel network, an elastic version can be created without requiring the round function be invertible by using a complete cycle of the Feistel network as the round function.

2.2 PRPs and SPRPs

We informally remind the reader of the meaning of a PRP and a SPRP. We refer to a permutation on n bits that is chosen randomly from all permutations on n bits as a random permutation. A permutation, G, on n bits is a PRP if it is not possible to distinguish G from a random permutation in polynomial (in n) time. Given a black box which either contains G or a random permutation, if an attacker makes polynomial many queries to the black box and receives the output of the permutation within the box, the probability the attacker correctly guesses the contents of the box is less than $\frac{1}{2} + e$ for negligible $e \geq 0$. In terms of block ciphers, this corresponds to the attacker being able to make either adaptive chosen plaintext queries or adaptive chosen ciphertext queries (but not both) to a black box which contains either the cipher or a random permutation.

A permutation , G, on n bits is a SPRP if it is not possible to distinguish G from a random permutation in polynomial (in n) time when queries to both the permutation and its inverse are permitted. Given a black box which either contains G or a random permutation, the attacker can make polynomial many queries to the black box where the query indicates whether the permutation or its inverse is to be applied to the n bit input. The probability the attacker correctly guesses the contents of the box is less than $\frac{1}{2} + e$ for negligible $e \geq 0$. In terms of block ciphers, this corresponds to the attacker being able to make both adaptive chosen plaintext queries and adaptive chosen ciphertext queries in any order to a black box which contains either the cipher or a random permutation.

Luby and Rackoff proved that when using round functions which are independently chosen pseudo-random functions (PRFs) three rounds are required in a Feistel network to protect against known plaintext attacks and four rounds are required to protect against known plaintext, ciphertext attacks [2]. Naor and Reingold provided slightly modified constructions which achieve the same resistance to such attacks. The first round of the three round version is replaced with a permutation, and the first and last rounds of the four round version are replaced with independent permutations [3].

3 PRP from Random Permutations

In Section 4 we will prove that a three round elastic network is a PRP and that a four round elastic network is a SPRP when the round functions are independently chosen PRPs. Prior to doing so, we need to prove a property which is used as a building block for our proofs. Specifically, we claim that an elastic network is a PRP when the round function is a random permutation and there are at least 3 rounds in the elastic network. In this section, we first prove a theorem concerning the relationship between the elastic version of a block cipher and the original block cipher. We then show that our claim follows directly from the theorem's proof.

We consider a block cipher, G, operating on b bits and its elastic version, G', operating on $b + y$ bits where $0 \leq y \leq b$. We prove that G' is a PRP if each round of G is an independent random permutation and G contains at least two rounds (in order for G' to contain at least three rounds). The proof is due to the fact we are able to define the output of G' as the output of one instance of G concatenated with y bits from a second overlapping instance of G with the inputs and round keys of the two instances being related. The relationship between the pairs of inputs and between the pairs of round keys is a function of the cipher structure only and treats the key and message variables symbolically. If G contains two or more rounds that are each random permutations then each instance of G (G with a specific key) must correspond to a random permutation. Thus, two instances of G with related keys - related inputs must also each correspond to random permutations and a related key - related input attack cannot exist which distinguishes G from a random permutation. We show if there is a distinguisher for G', this distinguisher can be used to distinguish related key - related input instances of G from random permutations. From the pairs of outputs from G, $b+y$ bit strings are formed to which the distinguisher for $G\,'$ is applied and will recognize the bias bounded away from the assumed random permutation.

Before stating our theorem, we first state three obvious facts. Let $RP1$ and $RP2$ denote two random permutations, each on b bits. Let $KW1$ and $KW2$ denote b bit strings which are formed independently of the inputs and outputs of $RP1$ and $RP2$.

- Fact 1: The composition of RP1 and RP2 is a random permutation on b bits. In relation to G, this means a sequence of rounds which are each random permutations is also a random permutation; therefore, G is a random permutation if it consists solely of a series of random permutations.
- Fact 2: $KW1 \oplus RP1$, $RP1 \oplus KW2$, and $KW1 \oplus RP1 \oplus KW2$ are random permutations. In relation to G, this means that adding whitening before and/or after a round (such as when forming G') does not change the fact that the round is a random permutation, provided that the key bits used for the whitening are independent of the round function's input and output (for example, if the end of round whitening was always the output of the round, the round would always output a string of b zeroes).
- Fact 3: A function which is defined by applying $RP1$ to b bits then selecting any y bit subset of $RP1$'s output is a random function mapping b bits to y bits.

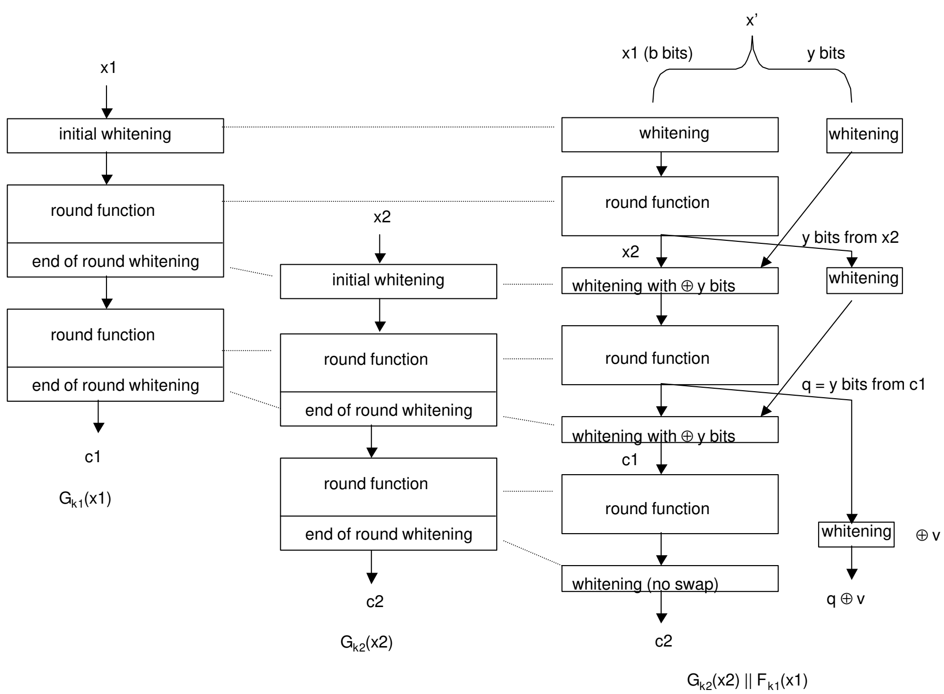

Figure 3: **Related Instances of G within G'**

Theorem I: *An elastic block cipher, G' is a PRP on $b+y$ bits, $0 \leq y \leq b$, if the original block cipher, G, is a random permutation on b bits formed from at least two rounds and each round of G is an independent random permutation on b bits.*

Before beginning the proof of Theorem I, we first formally describe how the output of $G\,'$ (when used for encryption) is the output of one instance of G concatenated with y bits from a second instance of G with the inputs and round keys of the two instances related. Without loss of generality, we describe G as if it contained initial and end of round whitening. By Fact 2, the assumption that G contains these whitening steps does not impact the condition that the round functions are random permutations. Let:

- rkj_i denote the i^{th} round key of the set of round keys rkj with rkj_0 referring to the key bits used for the initial whitening. For completeness and in order to later apply this notation to versions where each round function is not a random permutation, we define the round key to include both end of round whitening key bits and key bits used within the round function. When the round function is a random permutation, any round key bits used within the round function can be viewed as being discarded and do not impact the round function.
- $IRF_{rk_{IRF}}$ denote initial whitening and the round function, excluding the end of round whitening, of G using key material rk_{IRF}.
- x^* be a $b+y$ bit string.
- x' be the $b+y$ bit output of the $(r'-r-1)^{th}$ round of G' prior to the end of round whitening. Recall that r' and r are the number of rounds in G' and G, respectively.
- $x1, x2$ be two b bit strings such that $x1$ is the leftmost b bits of x' and $x2 = IRF_{rk_{IRF}}(x1)$.
- $k1, k2$ and $rk1, rk2$ be two keys for G and their corresponding sets of round keys, respectively, such that:
  - $rk2_i = rk1_{i+1}$ for $i = 0$ to $r-1$.
  - $rk2_0 =$ the key bits from $rk1_1$ used for the end of round whitening.
  - $rk1_0 =$ the key bits from rk_{IRF} used for the inital whitening step in IRF.
- $c1 = G_{k1}(x1)$ and $c2 = G_{k2}(x2)$
- q be the y bits from $c1$ in the same position as the y bits from the leftmost b bits which are involved in the swap in round $r'-1$ of $G\,'$ when forming the input to round r' of $G\,'$.
- $v \leftarrow \{0,1\}^y$
- G'^{-1} denotes the inverse of G', specifically G' when is used for decryption.

Define $F_{k1}(x) = q \oplus v$. The output of $G'_k(x^*)$ is $G_{k2}(x2)||F_{k1}(x1)$.

For clarity, we point out that the pair of related inputs $(x1, x2)$ to G are defined such that $x2$ is equivalent to applying a single round of G' to $x1$ using a round key which is held constant when forming multiple related message pairs of the form $(x1, x2)$. The round keys of G are related in that they are shifted one round.

We note that the variables defined in this proof are defined as if G' is being used for encryption. The same reasoning applies when G' is used for decryption by viewing the output of G'^{-1} as the b bit plaintext produced by G^{-1}_{k1} concatenated with the XOR of y bits from the plaintext produced by G^{-1}_{k2} and y pseudorandom bits. Thus we omit restating this proof in terms of decryption.

Figure 3 illustrates the relationship using a G with two rounds. The right part of the diagram reflects the initial whitening step followed by 3 rounds of $G\,'$. Thus $x1$ can be viewed as either the leftmost b bits of the input to a 3 round version of $G\,'$ or of the output of a previous round of $G\,'$ after the swap step. The "whitening with $\oplus y$ bits" and "whitening" within these 3 rounds are an equivalent representation of the end of round whitening and swap steps in $G\,'$.

We prove the following two claims to provide the intuition as to why Theorem I is true.

Claim I: If G consists of a series of two or more rounds such that each round function is an independently and randomly chosen random permutation on b bits and $y < b$ then the output of G' can be defined as the output of a random permutation concatenated with the output of a random function.

Proof: The leftmost b bits of output of G' are from an instance of G and thus are the output of a random permutation. By Fact 3, $F_{k1}(x1)$ is a random function mapping b bits to y bits. Thus the output of G' is the output of a random permutation concatenated with the output of a random function.

Claim II: If G consists of a series of two or more rounds such that each round function is an independently and randomly chosen random permutation on b bits and $y = b$ then the output of G' can be defined as the concatentation of the output of two independently chosen random permutations.

Proof: The leftmost b bits of output of G' are from an instance of G and thus are the output of a random permutation. The rightmost y bits of output of G' are from an instance of G and thus are the output of a random permutation. The two instances of G are different and thus the same random permutation is not used to form both the b and y bit portions, except for the negligible probability that the same permutation was selected randomly from all permutations when forming both instances of G.

We now prove Theorem I.

Proof of Theorem I: We will refer to the random permutation which outputs the leftmost b bits of G' as RB and to the random function (when $y < b$) or random permutation (when $y = b$) which outputs the rightmost y bits of G' as RY. In regards to the requirement that G contains at least 2 rounds, this is necessary so that it is not possible to alter the input to either RB or RY without altering the input to both. As a result, it is not possible to hold either the leftmost b bit component of the output or the rightmost y bit component of the output constant with non-negligible probability while altering the other component. It is this property of not being able to hold part of the output constant with non-negligible probability when the input changes that leads to the pseudorandomness of the output of G'. Note that RY can produce the same output with negligible probability when given different inputs and $y < b$. It is also possible through a series of rounds that the input to either RB or RY (but not both) will be identical for two different inputs to G' with negligible probability. Obviously, if it was possible to hold the output of one component constant while varying the other then G' could be distinguished from a PRP using two queries.

In order to complete our proof of Theorem I, we need to show that the concatenation of the outputs of RB and RY formed by the related key - related input pairs cannot be distinguished from random with non-negligible probability. Specifically, if $G'_k(x)$ is a PRP, we need to show the concatentation of outputs from $G_{k2}(x2)$ and $F_{k1}(x1)$ cannot be distinguished from random with nonnegligble probability using polynomial such outputs; where $k1, k2, x1, x2$ may vary to correspond to different inputs of x and fixed key k. To accomplish this, we show how a distinguisher that distinguishes $G\,'$ from a random permutation can be used to prove G is not a random permutation. Assume $G\,'$ is not a pseudorandom permutation. Then there exists a distinguisher $D\,'$ such that if polynomial many, n, inputs are given to a black box that contains either G' with a fixed, but randomly chosen key, or a random permutation, D' can determine from the outputs whether the black box contains G' or a random permutation with non-negligible probability. The n inputs to the black box can be adaptively chosen and any specific input to the black box always produces the same output. Each output from the black box is given to $D\,'$, which then outputs a 0 if it thinks the output came from an instance of $G\,'$ and outputs 1 otherwise. On n inputs, $D\,'$ will answer correctly with probability $\frac{1}{2} + \epsilon$ for some non-negligible ϵ.

D' can be used to construct a distinguisher, D, for G that distinguishes G from a random permutation.

Using the notation and relations defined previously, let G_{k1} and G_{k2} be two instances of G with keys $k1$ and $k2$ that are related, but are otherwise unknown. We consider a black box, B, that takes pairs of b bit inputs and contains either a random permutation on $2b$ bits or the two instances of G. The two instances of G are such that G_{k1} is applied to the first b bits and G_{k2} is applied to the last b bits. Without loss of generality, the outputs, $c1$ and $c2$, of the two instances of G are concatenated to form the output from B, and the random permutation treats the pairs of b bits as $2b$ bit strings and outputs $2b$ bits. It should not be possible to determine with non-negligible probability the contents of B on polynomial many queries to it if G is a random permutation. because doing so implies a related key attack on G. Furthermore, the inputs used in the queries may be adaptively chosen (we will require only that they can be chosen, not necessarily adaptively) Thus even if the pairs of b bit inputs consist of related b bit strings, $x1$ and $x2$ as defined previously, a distinguisher should not exist if G is a random permutation.

However, if G' is not a pseudorandom permutation on $b+y$ bits, we can create a D that succeeds with non-negligible probability and thus G cannot be a random permutation on b bits. Use n pairs of $(x1, x2)$ as the inputs to B (where $x1$ and $x2$ are related) and apply D to the $2b$ bit outputs of B. Let $w1||w2$ denote an output of B, where $|w1| = |w2| = b$. Define D as follows to output 0 if B contains the two instances of G and 1 otherwise:

Form a y bit random string, v, that is constant for all inputs to D: $v \leftarrow \{0,1\}^y$

$D(w1||w2)$ {

Form a y bit string, q, by taking the y bits from $w1$ that are in the same y positions used in the last swap step in G'.

$ans \leftarrow D'(w2||q \oplus v)$

Return ans.

}

We note that the bit positions chosen in each swap step of G' are part of the definition of G' and depend at most on y (they are neither dependent on the key nor on the input), thus they can be known by D. The $b+y$ bit string formed by D and given to D' is precisely $G_{k2}(x2)||F_{k1}(x1)$ when the $2b$ bits input to D are from the related key instances of G using related inputs, and thus is the output from an instance of G'. The $b+y$ bit string formed by D is random when the $2b$ bits input to D are from a random permutation. Since D' succeeds in distinguishing G' from a random permutation and D returns a 0 whenever D' returns a 0, D will succeed with non-negligible probability in determining whether B contains the two instances of G or a random permutation.

If n queries to D' are required to distinguish the output of G' from a random permutation, then n queries constructed from $2n$ outputs (n pairs) of inputs of B are required to use D to distinguish the outputs of G (with the related key - related input pairs) from outputs of a random permutation. Therefore, by using related keys and related inputs, the outputs of G can be distinguished from random with non-negligible probability on polynomial many queries. Thus if G' is not a pseudorandom permutation then G cannot be a random permutation, and if G is random permutation formed from a series of rounds of which each is a random permutation then G' is a pseudorandom permutation. This concludes our proof of Theorem I.

Our next claim follows directly from Theorem I's proof.

Claim III: A three round elastic network in which each round function is a random permutation on b bits is a pseudorandom permutation on $b+y$ bits.

Proof: In the proof to Theorem I, the only requirement regarding the number of rounds is that G' contain at least three rounds. If we define G to be the first two round functions of G' and set the number of rounds in G' to three regardless of the exact size of y ($0 \leq y \leq b$) then the proof to Theorem I still holds. We note that according to the algorithm for constructing an elastic block cipher, when G contains two rounds, the number of rounds in G' is normally set to 3 if $y \leq \frac{b}{2}$ and to 4 if $\frac{b}{2} < y \leq b$. However, 3 rounds is sufficient to create a psuedorandom permutation on $b + y$ bits when the round functions are random permutations.

4 PRP and SPRP

4.1 Overview

In Section 3 we proved that the elastic network can be used to create a PRP from random permutations. We now analyze the elastic network to determine how it may be used to construct a PRP and a SPRP from PRPs. The results are similar to the results Luby and Rackoff obtained for Feistel networks. In [2] it was shown how to construct a PRP and a SPRP from random functions using a Feistel network. We prove that a three round elastic network is a PRP and a four round network is a SPRP when the round functions are PRPs. We also show that a two round elastic network and a modified three round elastic network are not PRPs, and that a three round elastic network is not a SPRP. We note that we are using pseudorandom permutations as the round function in our constructions; whereas, pseudorandom functions are used in the analysis provided by Luby-Rackoff. This is due to the fact that the elastic network requires the round function be invertible.

4.2 Two Round and Modified 3 Round Elastic Networks

We consider two versions of the elastic network which is not a PRP. The first is a two round version. The second is a three round version in which the second and third round functions are identical, there is no whitening applied to bits omitted from the round function and $y = b$.

Claim IV: *An elastic network with exactly two rounds is not a PRP.*

Proof: This claim holds regardless of the properties of the round function. Consider the case where $y = b$. Given two $2n$ bit plaintexts of the form $B||Y1$ and $B||Y2$, let the ciphertexts be denoted by $C1||Z1$ and $C2||Z2$, respectively. As shown in Figure 4 $C1 \oplus Z1 = C2 \oplus Z2$ with probability 1. If the two round construction was a PRP, this equality would occur with probability $2^{-n} \pm e$ for negligible e instead of with probability 1. In general for any $y \leq b$, $C1 \oplus Z1$ and $C2 \oplus Z2$ will match in the y specific positions of the leftmost b bits involved in the swap after round 1. In contrast, if the two round construction was a PRP, the match would occur with probability $2^{-y} \pm e$ for negligible e.

The following claim is made regarding a modified three round version.

Claim V: *In a three round elastic network, if the round function does not change between the second and third rounds (i.e. the round keys and round function are identical) and there is no whitening applied to the bits omitted from the round function, then it is possible to distinguish the decryption function from a PRP using a chosen ciphertext when $y = b$. (If any whitening is applied to the leftmost b bits at the end of each round, this whitening step is considered to be part of the round function.)*

Proof: This is illustrated in Figure 5. Using a 3 round version of the elastic network, let β denote the $\frac{n}{2}$ bit output of the second round function prior to the XOR. Let C denote the ciphertext and let 0 denote a string of $\frac{n}{2}$ zeroes. Choose $C = 0||\beta$. Then the outputs of both the second and third round functions, prior to the XOR in each case, is β. The output of the first round function must be $\beta \oplus f2^{-1}(\beta)$. The input to the second round function is $f2^{-1}(\beta)$. Thus, the rightmost $\frac{n}{2}$ bits of the plaintext is $\beta \oplus f2^{-1}(\beta) \oplus f2^{-1}(\beta) = \beta$. If the network was a pseudorandom permutation on n bits, the probability the rightmost $\frac{n}{2}$ bits output by the inverse of the network equals β when the input is $0||\beta$ is $2^{-\frac{n}{2}} \pm e$ for negligible e.

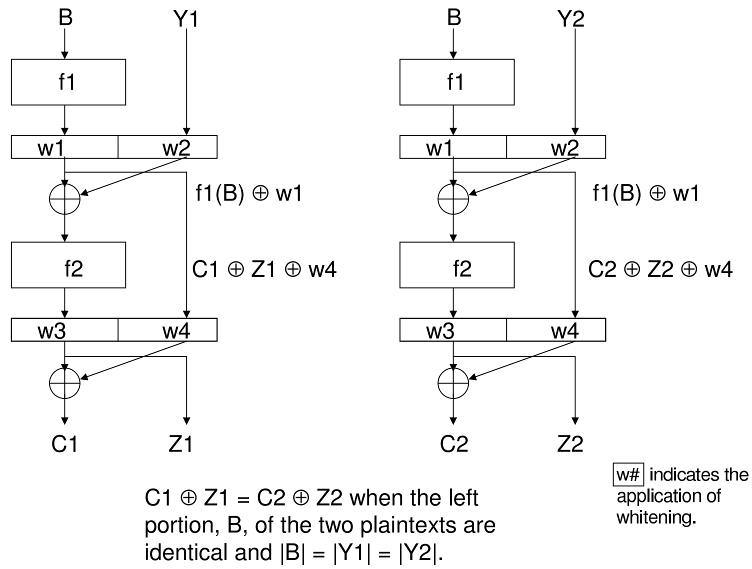

Figure 4: **Elastic Block Cipher Structure - Two Round Attack**

The network shown in Figure 5 is not the elastic network used in the elastic block cipher construction because whitening of the rightmost y bits is omitted, the round key bits do not vary between the second and third rounds, and y must equal b. If any one or more of these three conditions does not hold, the attack is no longer applicable. If the round function uses key material and the key material varies amongst rounds (which is typical of block ciphers) then the attack will not hold because $f2^{-1}(\beta)$ becomes $f_{ki}^{-1}(\beta)$ for some key material ki that varies per round and the rightmost $\frac{n}{2}$ bits of the plaintext will be $\beta \oplus f_{k3}^{-1}(\beta) \oplus f_{k2}^{-1}(\beta)$, where $k2, k3$ denote the key material used in the second and third rounds. The attack will also not hold even if the round function is identical across the second and third rounds (identical round keys, if any) but there is whitening after each round applied to the rightmost bits which were omitted from the round function. This is because the input to the second round when decrypting will be $\beta\oplus$ whitening as opposed to β (any whitening applied to the leftmost b bits output from the round function can be considered to be part of the round function). In the case where the same leftmost b whitening bits are applied in rounds 2 and 3, the attack holds. If these b whitening bits differ between rounds 2 and 3, this falls under the case of the key bits differing and the attack does not hold. Finally, the attack also does not work if $y < b$. When $y < b$, the bits input to the first two rounds of decryption will not be identical due to the specific bit positions involved in the XOR because some bits from $f2^{-1}(\beta)$ will be input to the second decryption instead of this input being exactly β.

4.3 Three Round Elastic Network is a PRP

We now show when a three round elastic network is a PRP. For simplicity, we show all of the three and four round elastic networks in the remainder of this section without the last swap step which does not impact the security of the elastic network.

Theorem II: *A three round elastic network is a PRP if the round functions are independently chosen PRPs.*

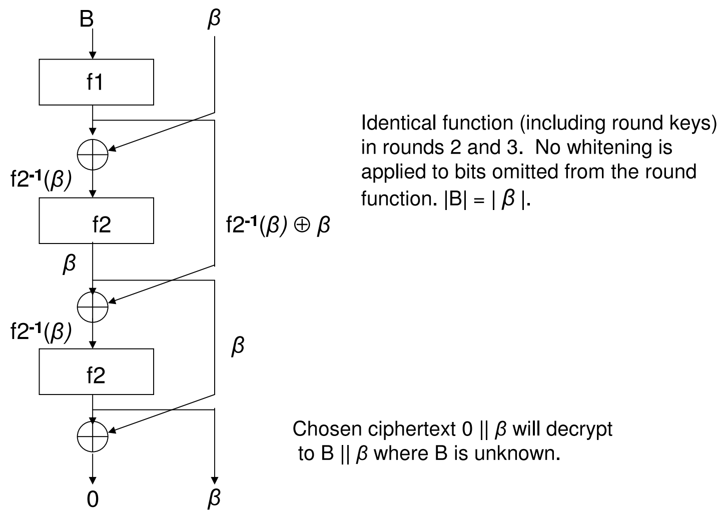

Figure 5: **Modified Three Round Elastic Network - Chosen Ciphertext Attack**

Proof: We consider the relationships between the four versions shown in Figure 6 of a three round elastic network. In each version, the round functions are chosen independently of each other and map a b bit input to a b bit output.

We define the following six permutations:

- Let $PRP1, PRP2, PRP3$ be 3 independently chosen random permutations.

- Let $RP1, RP2, RP3$ be 3 independently chosen random permutations.

Let Ni refer to a 3 round elastic network in which the first i round functions are pseudorandom permutations and the remaining round functions are random permutations, for $i = 0, 1, 2, 3$ defined as follows:

- Network 0 ($N0$): Each round function is a RP. The round functions are $RP1, RP2, RP3$.
- Network 1 ($N1$): The first round function is the PRP. The second and third round functions are RPs. The round functions are $PRP1, RP2$ and $RP3$.
- Network 2 ($N2$): The first two round functions are PRPs and the third round function is a RP. The round functions are $PRP1, PRP2$ and $RP3$.
- Network 3 ($N3$): Each round function is a PRP. The round functions are $PRP1, PRP2$ and $PRP3$.

As shown by Claim III in Section 3, $N0$ is a PRP. Therefore, if Theorem II is not true it is possible to distinquish $N3$ from $N0$ with probability $\geq \alpha$ for some non-negligible α where $0 < \alpha \leq 1$. We will show that if $N3$ can be distinquished from random then at least one of $PRP1, PRP2$ and $PRP3$ can be distinguished from random in order to derive a contradiction and thus conclude Theorem II is true.

Let D be a distinguisher that takes $b+y$ bit inputs and runs in polynomial time. D outputs a 1 if it thinks the inputs are the outputs of a random permutation and outputs a 0 otherwise. Let $Pr(Ni)$ be the probability that D outputs a 1 when given polynomial many inputs from Ni. The outputs are from Ni is applied in one

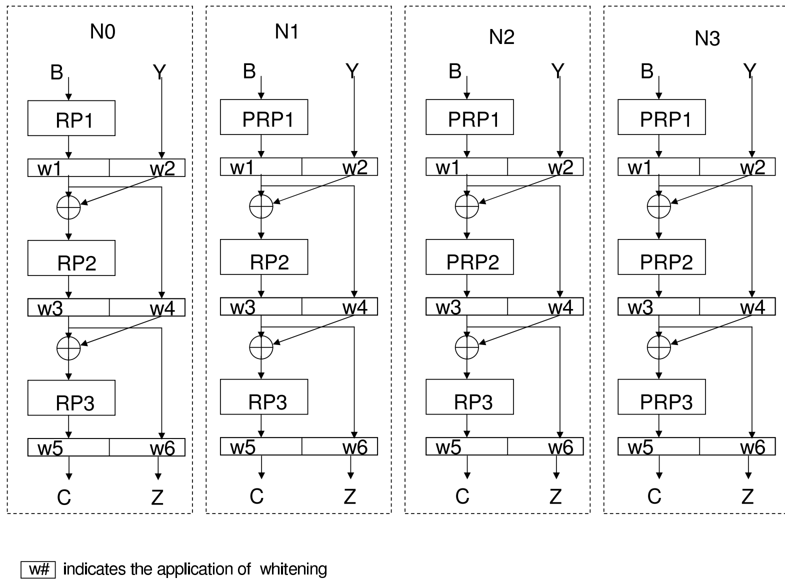

Figure 6: **3 Round Networks Consisting of RPs and PRPs**

direction only (*e.g.*, encryption or decryption). If $N3$ can be distinguished from a random permutation, then $|Pr(N0) - Pr(N3)| \geq \alpha$.
However,

$$|Pr(N0) - Pr(N3)| = |Pr(N0) - Pr(N1) + Pr(N1) - Pr(N2) + Pr(N2) - Pr(N3)|$$
$$\leq |Pr(N0) - Pr(N1)| + |Pr(N1) - Pr(N2)| + |Pr(N2) - Pr(N3)|.$$

Therefore, $\alpha \leq |Pr(N0) - Pr(N1)| + |Pr(N1) - Pr(N2)| + |Pr(N2) - Pr(N3)|$.
This implies at least one term on the right side of the inequality is $\geq \frac{\alpha}{3}$ and thus it is possible to distinguish between a three round elastic network which has i round functions which are pseudorandom permutations and one which has $i-1$ round functions which are pseudorandom permutation with non-negligible probability. Therefore, it is possible distinguish between a round function which is a random function and one which is a pseudorandom function with non-negligible probability, contradicting the definition of pseudorandom.

4.4 Three Round Elastic Network is not a SPRP

In [2], it was shown that a three round Feistel network is not a SPRP. The attack used to show this is an adaptive chosen plaintext - chosen ciphertext attack using two encryptions and one decryption. A three round elastic network is also not a SPRP. This can be shown with an adaptive attack which encrypts two chosen plaintexts then decrypts two chosen plaintexts formed from the two resulting ciphertexts.

Claim V: *A three round elastic network is not a strong PRP when $b = y$.*

Proof: The following sequence of two encryptions and two decryptions can be used to distinguish the 3 round elastic network from a SPRP when $b = y$. Each plaintext and ciphertext is of length $2b$, ı.e. $|B| = |Bi| = |Yi| = |Ci| = |Zi| = b\ \forall i$.

Encrypt two plaintexts of the form $B||Y1$ and $B||Y2$. The b bit portion is constant and the $Yi's$ may be any b bits such that $Y1 \neq Y2$. Let $C1||Z1$ and $C2||Z2$ be the resulting ciphertexts. This is depicted in Figure 7.

From the two resulting ciphertexts, form and decrypt the two ciphertexts $C1||(Z1 \oplus Z2)$ and $C2||(Z1 \oplus Z2)$. Let $B3||Y3$ and $B4||Y4$ denote the two resulting plaintexts. This is depicted in Figure 8. $Y3 \oplus Y4 = Z1 \oplus Z2$ with probability 1.

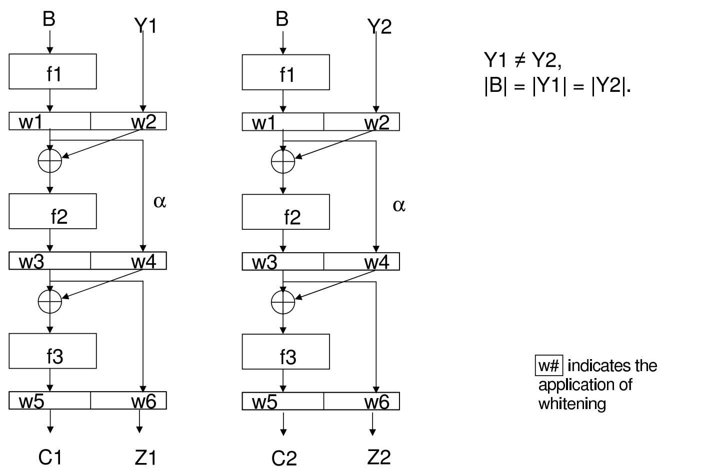

Figure 7: **Chosen Plaintexts for the Chosen Plaintext - Chosen Ciphertext Attack**

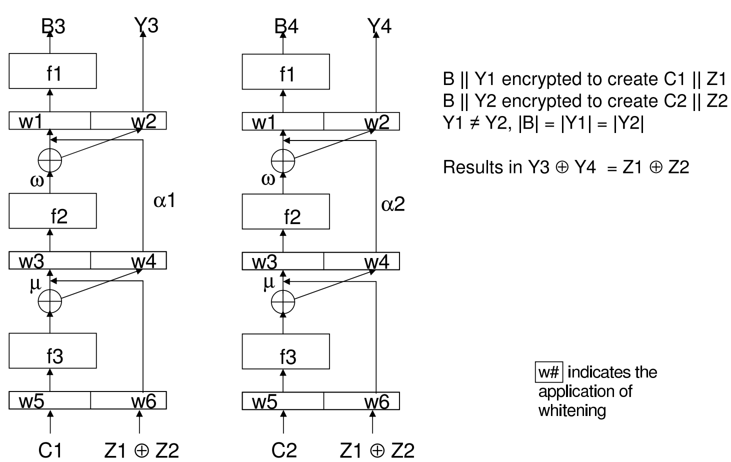

Figure 8: **Chosen Ciphertexts for the Chosen Plaintext - Chosen Ciphertext Attack**

The equality is obtained as follows:

- Let the wi values denote the whitening bits as shown in the figures.
- Let $\alpha, \alpha1$ and $\alpha2$ denote the bits left out of the second round as shown on the figures.

- Let $\mu = Z1 \oplus Z2 \oplus w6$.
- Let ω be the output from the round function in the second round of decryption when the input to the round function is $\mu \oplus w3$.
- Let $u = Z1 \oplus Z2 \oplus w6$.

Notice that:

$$\begin{aligned}
\alpha &= Z1 \oplus w6 \oplus f3^{-1}(C1 \oplus w5) \oplus w4 \\
&= Z2 \oplus w6 \oplus f3^{-1}(C2 \oplus w5) \oplus w4 \\
\alpha 1 &= f3^{-1}(C1 \oplus w5) \oplus u \oplus w4 \\
\alpha 2 &= f3^{-1}(C2 \oplus w5) \oplus u \oplus w4
\end{aligned}$$

Expanding u then substituting α in $\alpha 1$ results in:

$$\begin{aligned}
\alpha 1 &= f3^{-1}(C1 \oplus w5) \oplus Z1 \oplus Z2 \oplus w6 \oplus w4. \\
&= Z2 \oplus \alpha.
\end{aligned}$$

Likewise,

$$\alpha 2 = Z1 \oplus \alpha$$

Rewriting $Y3$ and $Y4$ in terms of $\alpha 1$ and $\alpha 2$ results in:

$$\begin{aligned}
Y3 \oplus Y4 &= \omega \oplus w2 \oplus \alpha 1 \oplus \omega \oplus w2 \oplus \alpha 2 \\
&= \alpha 1 \oplus \alpha 2 \\
&= Z2 \oplus \alpha \oplus Z1 \oplus \alpha \\
&= Z1 \oplus Z2
\end{aligned}$$

Therefore, with probability 1, $Y3 \oplus Y4 = Z1 \oplus Z2$ in this adaptive chosen plaintext - chosen ciphertext attack. If the elastic network was a SPRP, this equality would hold with probability $2^{-b} \pm e$ for negligible e.

We point out that when $y < b$ the attack does not hold because entering the second round of decryption, $Z1 \oplus Z2$ involves y bits. Since $C1 \neq C2$, the remaining $b - y$ bits are not guaranted to be equal.

4.5 Four Round Elastic Network is a SPRP

We will show that a four round elastic network in which the round functions are independently chosen random permutations is a SPRP. Before stating our theorem, we prove two claims.

By the definition of a SPRP, any random permutation is a SPRP. Let $RP1$ and $RP2$ be two independently chosen random permutations, each on n bits. Define $Perm1(p) = RP2(RP1(p))$, where x is of length n. $Perm1$ is a random permutation on n bits and is a SPRP. Now we consider what happens if we use two pseudorandom permutations instead of random permutations.

Claim VI: Let $PRP1$ and $PRP2$ be two independently chosen pseudorandom permutations, each on n bits. Define $Perm2(p) = PRP2(PRP1(p))$, where x is of length n. $Perm2$ is a SPRP.

Proof: Obviously, $Perm2$ is a pseudorandom permutation on n bits. Any change in the input to $Perm2$ results in a change to the output of $PRP1$ and thus changes the input of $PRP2$ and the output of $PRP2$. Since both $PRP1$ and $PRP2$ are pseudorandom permutations, both the input and output of the $PRP2$ portion of $Perm2$ cannot be distinguished from random.

In order for $Perm2$ to be a SPRP it must not be possible to distinguish $Perm2$ from a random permutation on polynomial many (m) queries to $Perm2$ and its inverse, $Perm2^{-1}$. For simplicity, when we say an attacker is querying $Perm1$ or $Perm2$, we mean the attacker is able to issue queries to both the permutation and its inverse.

- Let (p_i, c_i), for $i = 1$ to m be pairs of n bit strings such that $c_i = Perm2(p_i)$.
- Let $< +, p_i >$ denote a query to $Perm2$ using input p_i.
- Let $< -, c_i >$ denote a query to $Perm2^{-1}$ using input c_i.
- Let t_i be the output of the i^{th} query. $t_i = c_i$ when the query is $< +, p_i >$ and $t_i = p_i$ when the query is $< -, c_i >$.
- Let $T = (t_1, t_2, ...t_m)$ be the output of m distinct queries to $Perm2$. If the i^{th} query is $< +, p_i >$ and the j^{th} query is $< -, c_i >$, $t_j = p_i$ if and only if $t_i = c_j$, for $i \neq j$. Without loss of generality we can assume if an attacker queries with $< +, p_i >$ that he will not later query with $< -, c_i >$ since he knows the answer will be p_i regardless of whether he is querying $Perm1$ or $Perm2$.
- Let $U = (u_1, u_2, ...u_m)$ be the output of m distinct queries made to $Perm1$.

We will refer to U and T as transcripts of $Perm1$ and $Perm2$, respectively. In order for $Perm2$ to be a SPRP, it must not be possible to distinguish T from U with non-negligible probability. The probability of u_{i+1} ocurring given $(p_1, c_1), (p_2, c_2)...(p_i, c_i)$ is $\frac{1}{2^n - i}$ because $Perm1$ is a random permutation.

Since $Perm2$ is a pseudorandom permutation, it is not possible to distinguish the output, t_i, of any single query from the output of a random permutation with non-negligble probability. For any single query to $Perm2$, the output occurs with probability $\frac{1}{2^n} \pm e$ for some negligible e.

When an attacker does not issue any queries such that $(p_i, c_i) = (p_j, c_j)$ for $i \neq j$, the probability of t_{i+1} given $(p_1, c_1), (p_2, c_2)...(p_i, c_i)$ is $\frac{1}{2^n - i} \pm \hat{e}$ for some negligible $\hat{e}$. Therefore, it is not possible to distinguish T from U with non-negligble probability.

Claim VII: *A four round elastic network in which each round function is an independently chosen random permutation is a SPRP.*

Proof: We will show that the four round elastic network can be viewed as two pseudorandom permutations and then apply Claim VI. We define the following for use in the proof:

- Let $N0$ denote a four round elastic network on $b + y$ bits in which the round functions are independently chosen random permutations.
- Let RPi denote the random permutation used for the round function in round i, for $i = 1, 2, 3, 4$.
- Let $G1'$ denote the first two rounds of $N0$. $G1'^{-1}$ refers to the inverse of $G1'$.
- Let $G2'$ denote the last two rounds of $N0$. $G2'^{-1}$ refers to the inverse of $G2'$.
- Let Vb_i be a b bit string.
- Let Vy_i be a y bit string.
- Let $Vb_i || Vy_i$ denote the output of $G1'$ and of $G2'^{-1}$.
- Let $< +, p_i >$ and $< -, c_i >$ be defined in our proof of Claim VI. The lengths of p_i and c_i are both $b + y$.
- Let pb_i refer to the leftmost b bits of p_i and let py_i refer to the rightmost y bits of p_i.
- Let cb_i refer to the leftmost b bits of c_i and let cy_i refer to the rightmost y bits of c_i.
- Let wi indicate whitening bits (as shown in Figure 9). $w(2i - 1)$ is the leftmost b bit portion of the end of round whitening for round i and $w(2i)$ is the rightmost y bits of the end of round whitening for round i.
- Let $fi(x)$ be a function with a b bit input and a y bit output that extracts from x the same y bits that would be swapped out after the i^{th} round of $N0$, *e.g.,* these would be the y bits left out of round $i + 1$ if x was the output of RPi.

- Let $hbi(x4, x5)$ be a function with a b bit input, $x4$, a y bit input, $x5$, and a b bit output, $x3$, such that when $x4$ is the input to $RP(i+1)$ and $x5$ is the y bits left out of round $i+1$ in $N0$, then $x3$ is the output of $RPi \oplus w(2i-1)$. *e.g.* hbi is a function which XORs $x4$ and $x5$ in the bit positions corresponding to the swap after round i.
- Let $hyi(x4, x5)$ be a function with a b bit input, $x4$, a y bit input, $x5$, and a y bit output, $x6$, such that when $x4$ is the output of $(RP(i+1))^{-1}$ and $x5$ are the y bits left out of round $i+1$ in $N0$, then $x6 \oplus w(2i)$ are the y bits left out of round i in $N0$.

Figure 9 shows $G1'$, $G2'$, $f1, f2, hbi$ and hby as they are related to $N0$.

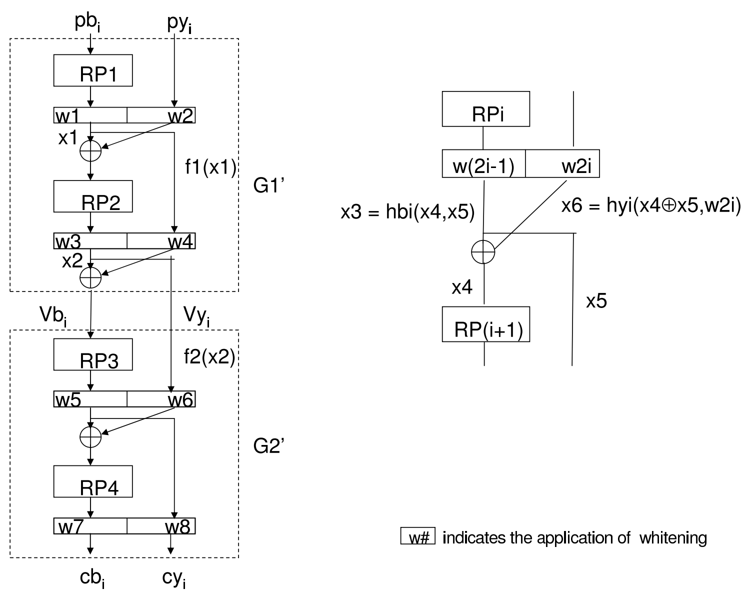

Figure 9: **4 Round N0**

We reconsider the number of rounds required in the original block cipher, G. Recall that in Theorem I we restricted the original block cipher to be one which contains at least two rounds solely to insure that the elastic version contains at least three rounds, making it impossible for an attacker to hold either the b bit or y bit portion to the last round constant while varying the other portion. A two round elastic network with independently chosen random permutations as round functions cannot be distinguished from a random permutation if the attacker is restricted to queries in which both the b bit left portion and y bit right portion must differ between any pair of queries. Under the restriction that $G1'$ can only be queried with $b+y$ bit inputs of the form $pb_i||pby_i$ such that both $pby_i \neq pbj_j$ and $pby_i \neq py_j$ for any $i \neq j$, $G1'$ cannot be distinguished from a random permutation. Likewise for $G2'$.

We now define Vb_i and Vy_i in terms of the RPi's when encrypting and when decrypting. When $N0$ is queried with $<+, p_i>$, the output, c_i, is the output of $G2'$ when $G2'$ is given input $Vb_i||Vy_i$ such that:

- $x2 = RP2(RP1(pb_i) \oplus w1) \oplus py_i \oplus w2) \oplus w3$
- $Vb_i = x2 \oplus f1(RP1(pb_i) \oplus w1) \oplus w4$
- $Vy_i = f2(x2)$

When $N0$ is queried with with $< -, c_i >$ (so the inverse of N0 is applied), the output, p_i, is the output of $G1'^{-1}$ when $G1'^{-1}$ is given input $Vb_i||Vy_i$ such that:

- $Vb_i = RP3^{-1}(hb3(RP4^{-1}(cb_i \oplus w7), cy_i \oplus w8) \oplus w5)$
- $Vy_i = hy3(RP4^{-1}(cb_i \oplus w7), cy_i \oplus w8) \oplus w6$

If any bit in the input p_i to $N0$ changes, both Vb_i and Vy_i change in the input to $G2'$, except with negligble probability. If any bit in the input c_j to $N0^{-1}$ changes, both Vb_j and Vy_j change in the input to $G1'^{-1}$, except with negligble probability. As a result, $N0$ can be viewed (per Theorem I) as two pseudorandom permutations. Therefore, Claim VI can be applied to $N0$ and we conclude that $N0$ is a SPRP.

Theorem III: *A four round elastic network in which the round functions are independently chosen PRPs is a SPRP.*

Proof: We consider the relationships between the five versions of a four round elastic network defined below. This is the same as method used in the proof to Theorem II. In each version, the round functions are chosen independently of each other and map a b bit input to a b bit output. We define the following eight permutations:

- Let $PRP1, PRP2, PRP3, PRP4$ be 4 independently chosen pseudorandom permutations.
- Let $RP1, RP2, RP3, RP4$ be 4 independently chosen random permutations.

Let Ni refer to a 4 round elastic network in which the first i round functions are pseudorandom permutations and the remaining round functions are random permutations, for $i = 0, 1, 2, 3, 4$ defined as follows:

- Network 0 ($N0$): Each round function is a RP. The round functions are $RP1, RP2, RP3, RP4$.
- Network 1 ($N1$): The first round function is the PRP. The second, third and fourth round functions are RPs. The round functions are $PRP1, RP2, RP3$ and $RP4$.
- Network 2 ($N2$): The first two round functions are PRPs, and the third and fourth round functions are RPs. The round functions are $PRP1, PRP2, RP3$ and $RP4$.
- Network 3 ($N3$): The first three round functions are PRPs and the fourth round function is a RP. The round functions are $PRP1, PRP2, PRP3$ and $RP4$.
- Network 4 ($N4$): Each round function is a PRP. The round functions are $PRP1, PRP2, PRP3$ and $PRP4$.

As we just proved, $N0$ is a SPRP. Therefore, if Theorem III is not true it is possible to distinquish $N4$ from $N0$ with probability $\geq \alpha$ for some non-negligible α where $0 < \alpha \leq 1$. We will show that if $N3$ can be distinquished from random then at least one of $PRP1, PRP2, PRP3$ and $PRP4$ can be distinguished from random in order to derive a contradiction and thus conclude Theorem III is true.

Let D be a distinguisher that takes $b+y$ bit inputs as defined previously in the proof to Theorem II, except now the inputs given to D are from both the forward and backward directions of the network. D outputs a 1 if it thinks the input is the output of a random permutation and outputs a 0 otherwise. Let $Pr(Ni)$ be the probability that D outputs a 1 when given polynomial many inputs from Ni where the inputs to D are outputs of both the forward (encryption) and backward (decryption) direction of Ni. If $N4$ is not a SPRP, then

$|Pr(N0) - Pr(N4)| \geq \alpha.$

$|Pr(N0) - Pr(N4)| = |Pr(N0) - Pr(N1) + Pr(N1) - Pr(N2) + Pr(N2) - Pr(N3) + Pr(N3) - Pr(N4)|$

$\leq |Pr(N0) - Pr(N1)| + |Pr(N1) - Pr(N2)| + |Pr(N2) - Pr(N3)| + |Pr(N3) - Pr(N4)|$.

Therefore, $\alpha \leq |Pr(N0) - Pr(N1)| + |Pr(N1) - Pr(N2)| + |Pr(N2) - Pr(N3)| + |Pr(N3) - Pr(N4)|$.

This implies at least one term on the right side of the inequality is $\geq \frac{\alpha}{4}$ and thus it is possible to distinguish between a four round elastic network which has i round functions which are pseudorandom permutations and one which has $i - 1$ round functions which are pseudorandom permutation with non-negligible probability. This implies it is possible distinguish between a round function which is a random function and one which is a pseudorandom function with non-negligible probability, contradicting the definition of pseudorandom.

5 Conclusions

We analyzed the underlying network structure of elastic block ciphers to show the network can be used to construct PRPs and SPRPs on $b + y$ bits from a round function which is a PRP on b bits, where $0 \leq y \leq b$. We proved that an elastic block cipher is a PRP when the original cipher contains at least two rounds and each round function is an independently chosen random permutation. Using this result, we proved that a three round elastic network with independently chosen PRPs as round functions is a PRP and that a four round elastic network with independently chosen PRPs as round functions is a SPRP. We showed that these are the minimum number of rounds required to obtain a PRP and a SPRP. Therefore, the number of rounds required to construct a PRP and a SPRP from PRPs using an elastic network are the same number of rounds required when using a Feistel network. Furthermore, because the elastic network works on a range of input sizes from b to $2b$ bits, our results show that the elastic network can be used to create PRPs and SPRPs with inputs ranging from b to $2b$ bits from PRPs with fixed length inputs of b bits.

References

[1] D. Cook, M. Yung, and A. Keromytis. Elastic Block Ciphers. Cryptology ePrint Archive, 2004/128, 2004. http://eprint.iacr.org/.

[2] M. Luby and C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *Siam Journal of Computing*, 17(2), April 1988.

[3] M. Naor and O. Reingold. On the Construction of Pseudo-random Permutations: Luby-Rackoff Revisited. In *Journal of Cryptology*, volume 12, pages 29–66, 1999.

[4] B. Schneier and J. Kelsey. Unbalanced Feistel Networks and Block Cipher Design. In *Proceedings of Fast Software Encryption (FSE), LNCS 1039, Springer-Verlag*, 1996.