Constructing Variable-Length PRPs and SPRPs from Fixed-Length PRPs [⋆]

Debra L. Cook[1], Moti Yung[2], Angelos Keromytis[3]

[1] Alcatel-Lucent Bell Labs, New Providence, New Jersey, USA
dcook@cs.columbia.edu
[2] Google, Inc. and Columbia University, New York, NY USA moti@cs.columbia.edu
[3] Department of Computer Science, Columbia University, New York, NY, USA
angelos@cs.columbia.edu

We create variable-length pseudorandom permutations (PRPs) and strong PRPs (SPRPs) accepting any input length chosen from the range of b to $2b$ bits from fixed-length, b-bit PRPs. We utilize the *elastic network* that underlies the recently introduced concrete design of elastic block ciphers, exploiting it as a network of PRPs. We prove that three and four-round elastic networks are variable-length PRPs and five-round elastic networks are variable-length SPRPs, accepting any input length that is fixed in the range of b to $2b$ bits, when the round functions are independently chosen fixed-length PRPs on b bits. We also prove that these are the minimum number of rounds required.

Key words: (strong) pseudorandom permutations, block ciphers, variable-length PRPs

1 Introduction

We prove that the elastic network, the underlying structure of elastic block ciphers [2], allows for the creation of variable-length PRPs and SPRPs from fixed-length PRPs, meaning it provides a PRP or SPRP for every length individually within a range of input lengths. In the abstract sense, a block cipher should be a SPRP. Feistel networks were analyzed in this manner and proven to provide fixed-length PRPs and SPRPs under certain conditions by Luby and Rackoff [7], and by Naor and Reingold [8]. This approach has also been used to justify modes of encryption. For example, the CBC-Mask-CBC mode (CMC) of encryption was proven to provide a SPRP on multiples of the block length under certain conditions on the block cipher used within the mode [5]. In general, the implementation of a block cipher can be considered a black box to applications making function calls to the cipher. This is especially true in modern computers where block cipher hardware may be included, such as Intel's plan to have AES in hardware as part of its future CPUs [4]. Understanding how to combine PRPs in theory to provide additional functionality translates into practical implementations by replacing the PRP with the black box that is the block cipher.

We consider the elastic network in an analogous manner. Elastic block ciphers are variable-length block ciphers created from existing block ciphers. The elastic version of a block cipher supports any actual block size between one and two times that of the original block size. The method consists of a substitution-permutation network, the

[⋆] This is an extended version of the paper in Inscrypt 2008.

elastic network, that uses the round function from the existing fixed-length block cipher. We prove that three and four round elastic networks provide variable-length PRPs and five round elastic networks provides a variable-length SPRP for each input length in the range of b to $2b$ bits when the round functions are independently chosen fixed-length PRPs on b-bits.

Our results assist in proving the soundness of the elastic block cipher's basic structure. The security of elastic block ciphers against practical attacks was evaluated in [3]. By proving the elastic network forms variable-length PRPs and SPRPs on inputs of b to $2b$ bits, under certain restrictions on the number of rounds and independence of the round functions as was done for Feistel networks [7, 8], our work provides further justification for the elastic block cipher approach to creating variable-length block ciphers.

We consider analysis of the elastic block cipher approach to be of value because of how the approach differs from other approaches that reuse existing block ciphers when creating a variable-length block cipher in practice. Unlike other variable-length block cipher constructions that build upon existing fixed-length block ciphers, the elastic block cipher approach does not require multiple applications of the fixed-length block cipher to encrypt $b + y$ bits, where $0 \leq y \leq b$. By using the round function of the existing fixed-length block cipher as a black box within the elastic network the computational workload of an elastic block cipher is proportional to the block size. In contrast, other methods, such as [1, 9, 10], treat a fixed-length block cipher as a black box. When encrypting $b + y$ bits, each of these methods apply a block cipher multiple times along with additional operations, resulting in a computational workload that is not proportional to the block size and which is less efficient than padding the data to two full blocks, regardless of the exact value of y.

The remainder of this paper is organized as follows. Section 2 summarizes the definitions of a PRP and SPRP, and the structure of elastic block ciphers. In Section 3, we show how to create variable-length PRPs from fixed-length PRPs with three and four round elastic networks. In Section 4, we prove that a five-round elastic network allows for the creation of a variable-length SPRP from fixed-length PRPs. In Section 5, counter-examples used to define the minimum number of rounds and independence of the round functions required for the proofs are presented. In Section 6, we summarize our results and briefly explain how the elastic network can be combined with CMC mode to extend the supported input length beyond $2b$ bits.

2 Preliminaries and Strategy

2.1 PRP and SPRP Definitions

We informally remind the reader of the definitions of a PRP and a SPRP. Refer to [6] for formal definitions. Although we are discussing permutations (as opposed to practical block ciphers), we will use the terms ”plaintext” and ”ciphertext” to refer to the inputs and outputs of the permutation. We use the following terms in the definitions of a PRP and a SPRP.

- Random permutation: A permutation on b bits that is chosen randomly from all permutations on b bits.

- Let P be a permutation on b bits. P^{-1} denotes its inverse. $P(x)$ is the output of P when given input x of length b bits.
- Chosen plaintext query: An adversary chooses an input, p_i, to a permutation, P, and receives the output, $c_i = P(p_i)$.
- Chosen ciphertext query: An adversary chooses an input, c_i, to the inverse of a permutation, P^{-1}, and receives the output, $p_i = P^{-1}(c_i)$.
- Chosen plaintext - chosen ciphertext queries: An adversary makes a series of queries to a permutation, P, and its inverse, P^{-1}, and receives the outputs.
- Adaptive queries: When making chosen plaintext, chosen ciphertext or chosen plaintext - chosen ciphertext queries to a permutation (and/or its inverse), the queries are said to be adaptive if the adversary making the queries receives the output of the i^{th} query before forming the $(i+1)^{st}$ query and can use the previous i queries and their outputs when forming the $(i+1)^{st}$ query.

The concepts of a PRP and a SPRP can be described by considering the probability with which an adversary can correctly determine whether or not a black box contains a specific permutation or a random permutation on b bits while using only polynomial (in b) many resources. Let P be a permutation on b bits. Given a black box that contains either P (or its inverse) or a random permutation, an adversary makes polynomially many adaptive queries to the black box and receives the outputs of the permutation within the box. If the probability that the adversary correctly determines (using polynomial time and memory) the contents of the box is $\frac{1}{2} + e$ for negligible $e \geq 0$, then P is a PRP. In terms of block ciphers, this corresponds to the adversary 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.

Similarly, a permutation, P, on b bits is a SPRP if it is not possible to distinguish P from a random permutation on b bits in polynomial (in b) time and memory when queries to both the permutation and its inverse are permitted. In terms of block ciphers, this corresponds to the adversary being able to make adaptive chosen plaintext - chosen ciphertext queries to a black box which contains either the cipher or a random permutation.

2.2 Elastic Network

We provide a brief review of the elastic network, which provides the underlying structure of elastic block ciphers. The elastic block cipher method was defined for creating variable-length block ciphers in practice [2]. The round function or cycle of an existing fixed-length, $b-bit$, block cipher is inserted into the elastic network, shown in Figure 1 and becomes the round function of the elastic version of the cipher. The input is $b+y$ bits, where $0 \leq y \leq b$. In each round the leftmost b bits are processed by the round function and the rightmost y bits are omitted from the round function. Afterwards, a ”swap step” is performed in which the rightmost y bits are XORed with a subset of the leftmost b bits and the results swapped when forming the input to the next round. [4]

[4] Elastic block ciphers also include initial and end-of-round whitening, and initial and final key-dependent permutations. Our analysis focuses on the basic structure and thus we omit these steps.

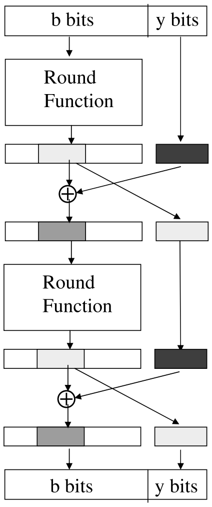


Fig. 1. Two Rounds of an Elastic Network

3 Variable-Length PRPs

As our first step, we prove that a three-round elastic network and the inverse of a four-round elastic network are variable-length PRPs when their round functions are independently chosen random permutations (RP). From these results, we can then prove that the same networks are variable-length PRPs when the round functions are independently chosen fixed-length PRPs. Figure 2 shows three-round and four-round elastic networks.

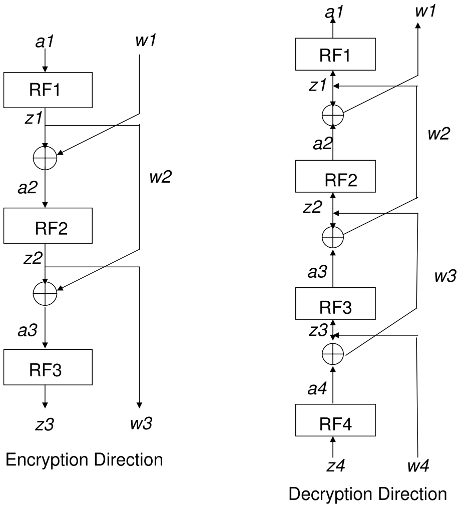


Fig. 2. Three and Four-Round Elastic Networks

We prove that if a three-round elastic network, G', with round functions that are independently chosen random permutations on b bits can be distinguished from a random permutation on $b+y$ bits, for some fixed value of $b+y$, using polynomially many queries to G' then at least one of the round functions can be distinguished from a random permutation on b bits, which is a contradiction. Therefore, we conclude that G' is a PRP. We use a black box, $B_{G'}$, that contains either G' or a random permutation on $b+y$ bits. We prove that if a distinguisher, D_3, exists that can determine whether or not $B_{G'}$ contains G' using polynomially many adaptive queries to the box then D_3 can be used to create a distinguisher for at least one of the round functions of G' to distinguish the round function from a random permutation on b bits. When we say a distinguisher for G' exists, we mean that the distinguisher, using polynomially many adaptive queries in one direction can predict or eliminate a possibility about an additional input/output pair value of the given permutation with greater certainty than that of a random guess. In contrast, with a random permutation, anything beyond the input/output pairs from the queries is known with the same probability as a random guess. We repeat the process for the inverse of a four-round elastic network.

We will refer to the components of the three and four-round networks as they are labelled in Figure 2. We use the following notation:

- $b > 0$ is an integer.
- y is an integer such that $0 \leq y \leq b$.
- $X \oplus Y$ where X is a b-bit string and Y is a y-bit string, means the bits of Y are XORed with y specific bits of X and the other $b-y$ bits of X are treated as if they are XORed with 0's. If the resulting string is stored in a variable containing only y bits instead of b bits, the result consists only of the y bits in the positions that involved both X and Y instead of X and the $b-y$ 0's. For example, consider XORing a 2-bit string with a 4-bit string such that the XOR involves the leftmost 2 bits of the 4-bit string. Let $z1$ and $a2$ be 4-bit strings. Let $w1$ and $w2$ be 2-bit strings. If $z1 =$ 0110 and $w1 =$ 11, $a2 = z1 \oplus w1 =$ 1010. $w2 = z1 \oplus w1 =$ 10.
- $n > 0$ is an integer that generically represents the number of polynomially many (in terms of the length of the input) queries made to a function.
- $|X|$ is the length, in bits, of X.
- RFi is the i^{th} round function, for $i = 1, 2, 3, 4$. Any restrictions placed on a RFi will be specified as needed. Each round function is a permutation on b-bits.
- ai is the b-bit input to the i^{th} round function for $i = 1, 2, 3, 4$.
- zi is the b-bit output of the i^{th} round function for $i = 1, 2, 3, 4$.
- wi is the y bits left out of the i^{th} round function for $i = 1, 2, 3, 4$. For any particular elastic network, $w2$ is formed from a fixed set of y-bit positions from $z1$, $w3$ is formed from a fixed set of y-bit positions of $z2$, and $w4$ is formed from a fixed set of y-bit positions of $z3$ (*i.e.,* the positions of the bits taken from $z1$ to form $w1$ do not vary amongst the inputs to a specific three-round elastic network). Likewise, when forming $w2$, $w3$ and $w4$.
- When referring to a specific value for an ai, zi or wi, a subscript will be used. For example, $a1_j$.

Theorem 1. *A three-round elastic network, G', on $b+y$ bits in which the round functions are independently chosen random permutations on b bits is a variable-length pseu-*

dorandom permutation on $b + y$ bits in the encryption direction for any fixed value of y where $0 \leq y \leq b$. Three rounds are the mininum number of rounds required.

Proof. A two-round elastic network cannot be a PRP. Refer to Section 5 for the counter-example. We define the following notation for use in proving the three round case:

- $B_{G'}$ is a black box that contains either G' or a random permutation on $b + y$ bits.
- $(a1_i, w1_i)$ is an input to $B_{G'}$. $|a1_i| = b$ and $|w1_i| = y$ as defined previously.
- $(z3_i, w3_i)$ is the output of $B_{G'}$ corresponding to the input $(a1_i, w1_i)$. $|z3_i| = b$ and $|w3_i| = y$ as defined previously.
- D_3 is a distinguisher for G', meaning D_3 can determine whether or not $B_{G'}$ contains G' with probability $\frac{1}{2} + \alpha$ for non-negligible α, $0 < \alpha \leq \frac{1}{2}$ when using only polynomially (in $b + y$) many resources. Let D_3 return a 1 if it thinks $B_{G'}$ contains G' and a 0 otherwise. D_3 makes n adaptive chosen plaintext or adaptive chosen ciphertext queries, but not both.
- $S1 = \{(a1_i, w1_i)\}$ and $S2 = \{(z3_i, w3_i)\}$, for $i = 1$ to n are the sets of n inputs and outputs D_3 uses to distinguish G' from a random permutation. When D_3 works by making queries to $B_{G'}$ in the encryption direction, $S1$ contains the inputs and $S2$ contains the resulting outputs. When D_3 works by making queries to $B_{G'}$ in the decryption direction, $S2$ contains the inputs and $S1$ contains the resulting outputs.
- B_{RFi} is a black box that contains either the i^{th} round function, RFi, of G' or a random permutation on b bits, for $i = 1, 2, 3$.
- $B_{RFi}(X)$ is the output of B_{RFi} when given input X.
- $B^{-1}_{RFi}(X)$ is the inverse of $B_{RFi}(X)$. *i.e.*, the inverse of whatever permutation is in B_{RFi} is applied to X.
- D_{RFi} is a distinguisher for RFi, meaning D_{RFi} can determine whether or not B_{RFi} contains RFi with probability $\frac{1}{2} + \alpha$ for non-negligible α, $0 < \alpha \leq \frac{1}{2}$ using polynomially (in $b + y$) resources. D_{RFi} uses either adaptive chosen plaintext or adaptive chosen ciphertext queries, but not both.
- ”plaintext query” refers to a query to G' in the encryption direction and ”ciphertext query” refers to a query to G' in the decryption direction (a query to G'^{-1}).

We note that the bit positions used in the swap steps in G' are not secret and this information can be used by any distinguisher. We define the following functions corresponding to the swap steps for use by the distinguishers:

- Let $Fi(X, Y)$ be a function that takes a b-bit input, X, and a y-bit input, Y, and returns the pair (Z, W) where Z is a b-bit string and W is a y-bit string. Fi replaces the y bits of X with the y bits of Y such that the bits in X which are replaced are in the same positions as the bits from the output of the i^{th} round function that are involved in the swap step after the i^{th} round of G'. Fi returns the updated X value in Z and returns a bit string, W, that contains the y bits of X that were removed from X XORed with the y bits inserted into X. $Fi(X, Y)$ computes the inverse of the i^{th} swap step in the elastic network.
- Let $FYi(X)$ be a function that takes a b-bit input X and returns the y bits that are in the same bit positions used to create wi from $z(i - 1)$ in G'.
- Let Oi be an oracle that contains the i^{th} round function, RFi of G'. Oi^{-1} will refer to an oracle containing RFi^{-1}.

We now prove Theorem 1. If D_3, a distinguisher for G' in the encryption direction, exists, D_3 must fall into one of the following categories:

- Category I: D_3 does not use the $z3$ portion of the output in its decision. The only part of the output used is the $w3$ portion. This means that given the n input/output pairs in $S1$ and $S2$, D_3 never uses the $z3$ portion from any of the pairs in $S2$.
- Category II: D_3 does not use the $w3$ portion of the output in its decision. The only part of the output used is the $z3$ portion. This means that given the n input/output pairs in $S1$ and $S2$, D_3 never uses the $w3$ portion from any of the pairs in $S2$.
- Category III: D_3 uses both the $z3$ and $w3$ portion of the outputs in its decision. This means that given n input/output pairs in $S1$ and $S2$, D_3 uses the $z3$ portion of the output from at least one of of the pairs in $S2$ and uses the $w3$ portion from at least one of the pairs in $S2$. Without using both portions, D_3 fails to distinguish the elastic network from a RP.

In each category, there are no restrictions on what portions of the inputs, $\{(a1_i, w1_i)\}$, are used. For each of the categories, we will show that the existence of D_3 implies a distinguisher can be formed for either the second or third round function of G', which contradicts the round functions being independently chosen random permutations.

Category I: If D_3 falls into Category I, a distinguisher, D_{RF2}, can be defined for the second round function, $RF2$. Intuitively, D_3 using only the $w3$ portion of the output of G' when $w3$ is from the output of $RF2$ whose inputs cannot be predicted with non-negligible probability implies D_3 can distinguish $RF2$ from a random permutation. The inputs to $RF2$ are distinct except with negligible probability. Therefore, the $w3$ values are distributed as if they are taken from the outputs of distinct queries to $RF2$, except with negligible probability and D_3 cannot rely on being given $w3$ values that were generated from identical inputs to $RF2$.
Define D_{RF2} as follows:

Ask D_3 what its first query (input) would be if it was querying $B_{G'}$. Populate $S1$ with this first input, so $(a1_1, w1_1)$ has been chosen and is in $S1$. $S1$ is known to D_{RF2}.

```
for $i = 1$ to $n$ {
    Take $(a1_i, w1_i)$ from $S1$ for use in subsequent steps.
    Set $z1_i = O1(a1)$.
    Set $z2_i = B_{RF2}(z1_i \oplus w1_i)$.
    Set $w3_i = FY3(z2_i)$.
    Give $a1_i, w1_i, w3_i$ to $D_3$.
    Add to $S1$ the next input $D_3$ would use when trying to distinguish $D_3$, having
    seen the inputs and partial output of the first $i$ queries. This is $(a1_{i+1}, w1_{i+1})$.
}
Let $ans$ be the value $D_3$ returns.
Return $ans$.
```

The values given to D_3 are the input and rightmost y bits of the output of a three-round elastic network with $RF1$ as the first round function and the contents of B_{RF2} as the second round function. The third round function is irrelevant here because D_3 is not using the output of the third round function. The values given to D_3 correspond to those of $S1$ and the $w3_i$ values of $S2$ when D_3 is allowed to make n adaptive chosen plaintext queries to $B_{G'}$. D_3 succeeds with non-negligible probability in determining whether or not it was given the input and partial output of G' implies D_{RF2} will succeed with non-negligible probability in determining if the n $(a2_i, z2_i)$ pairs correspond to the inputs and outputs of $RF2$. Therefore, D_{RF2} can distinguish the contents of B_{RF2} using the n queries $\{O1(a1_i) \oplus w1_i\}$. B_{RF2}, contradicting the assumption that the second round function is an RP.

Category II: If D_3 falls into Category II, a distinguisher, D_{RF3}, can be defined for the third round function, $RF3$. Intuitively, D_3 using only the $z3$ portion of the output of G' when $z3$ is from the output of $RF3$ whose inputs cannot be predicted with non-negligible probability implies D_3 can distinguish $RF3$ from a random permutation. The inputs to $RF3$ are distinct except with negligible probability. Therefore, the $z3$ values are distributed as if they are the outputs of n distinct queries to $RF3$, except with negligible probability and D_3 cannot depend on being given $z3$ values that were generated from identical inputs to $RF3$. Therefore, D_3 using only the input to G' and the $z3$ portion of the output implies D_3 can distinguish $RF3$ from a random permutation.

Define D_{RF3} as follows:

Ask D_3 what its first query (input) would be if it was querying $B_{G'}$. Populate $S1$ with this first input, so $(a1_1, w1_1)$ has been chosen and is in $S1$. $S1$ is known to D_{RF3}.

```
for $i = 1$ to $n$ {
    Take $(a1_i, w1_i)$ from $S1$ for use in subsequent steps.
    Set $z1_i = O1(a1_i)$.
    Set $z2_i = O2(z1_i \oplus w1_i)$.
    Set $w2_i = FY2(z1_i)$.
    Set $z3_i = B_{RF3}(z2_i \oplus w2_i)$.
    Give $a1_i, w1_i, z3_i$ to $D_3$.
    Add to $S1$ the next input $D_3$ would use when trying to distinguish $D_3$, having
    seen the inputs and partial output of the first $i$ queries. This is $(a1_{i+1}, w1_{i+1})$.
}
Let $ans$ be the value $D_3$ returns.
Return $ans$.
```

The values given to D_3 are the input and leftmost b bits of the output of a three-round elastic network with $RF1$ as the first round function, $RF2$ as the second round function and the contents of B_{RF3} as the third round function. The values given to D_3 correspond to those of $S1$ and the $z3_i$ values from $S2$ when D_3 is allowed to make n adaptive chosen plaintext queries to $B_{G'}$. D_3 succeeds with non-negligible probability in determining it was given the input and partial output of G' implies D_{RF3} will succeed with non-negligible probability in determining the contents of B_{RF3} by using n queries, $\{O2(O1(a1_i) \oplus w1_i) \oplus F2(O1(a1_i))\}$, contradicting the assumption that the third round function is an RP.

Category III: If D_3 falls into Category III, a second version of the D_{RF3} distinguisher we just defined can be created for the third round function, $RF3$. We call this new version D_{RF3v2}. Intuitively, D_3 using both the $z3$ and $w3$ portions of the output of

G' when $z3$ is from the output of $RF3$ whose inputs cannot be predicted with non-negligible probability, where $w3$ is from the output of $RF2$ whose inputs cannot be predicted with non-negligble probability and where $w3$ contributes to the formation of the input of $RF3$ (and thus contributes to the input to the permutation that produces $z3$) implies D_3 can distinguish $RF3$ from random. D_3 cannot depend on being given $z3$ and/or $w3$ values that were generated by holding the inputs to $RF2$ and/or $RF3$ constant since this occurs with negligible probability. Therefore, D_3 can be viewed as using some relationship between partial information (*i.e.*, $w3$) used in forming the input to $RF3$ and the output (ı.e., $z3$) of $RF3$ to distinguish the third round function from a random permutation.

D_{RF3v2} is D_{RF3} with the modification that $w3_i$ is given to D_3 along with $a1_i, w1_i$ and $z3_i$. Define D_{RFv2} as follows:

Ask D_3 what its first query (input) would be if it was querying $B_{G'}$. Populate $S1$ with this first input, so $(a1_1, w1_1)$ has been chosen and is in $S1$. $S1$ is known to D_{RF3}.

```
for $i = 1$ to $n$ {
    Take $(a1_i, w1_i)$ from $S1$ for use in subsequent steps.
    Set $z1_i = O1(a1)$.
    Set $z2_i = O2(z1_i \oplus w1_i)$.
    Set $w2_i = FY2(z1_i)$.
    Set $z3_i = B_{RF3}(z2_i \oplus w2_i)$.
    Set $w3_i = FY3(z2_i)$.
    Give $a1_i, w1_i, z3_i, w3_i$ to $D_3$.
    Add to $S1$ the next input $D_3$ would use when trying to distinguish $D_3$, having
    seen the inputs and output of the first $i$ queries. This is $(a1_{i+1}, w1_{i+1})$.
}
Let $ans$ be the value $D_3$ returns.
Return $ans$.
```

The values given to D_3 are the inputs and outputs of a three-round elastic network with $RF1$ as the first round function, $RF2$ as the second round function and the contents of B_{RF3} as the third round function. The values given to D_3 correspond to those of $S1$ and $S2$ when D_3 is allowed to make n adaptive chosen plaintext queries to $B_{G'}$. D_3 succeeds with non-negligible probability in determining it was given the input and output of G' implies D_{RF3v2} will succeed with non-negligible probability in determining the contents of B_{RF3} by using n queries, $\{O2(O1(a1_i) \oplus w1_i) \oplus F2(O1(a1_i))\}$, contradicting the assumption that the third round function is a random permutation.

For each category, we have shown that D_3 cannot exist. Therefore, a three-round elastic network cannot be distinguished from a PRP by using polynomially many plaintext queries when the round functions are independently chosen random permutations. In the decryption direction, four rounds are required to create a PRP.

Theorem 2. *The inverse of a four-round elastic network, (G'^{-1}), on $b + y$ bits in which the round functions are independently chosen random permutations on b bits is a variable-length pseudorandom permutation on $b + y$ bits for any fixed value of y where $0 \leq y \leq b$. Four rounds are the minimum number of rounds required.*

Proof. Refer to Section 5 for an example showing why three rounds are insufficient. The notation and terms are the same as in the proof to Theorem 1 unless otherwise stated. The black box, $B_{G'}$, will contain G'^{-1} or a random permutation on $b+y$ bits. The categories for the distinguisher are the same as in the three-round case. For two of the categories, three rounds are sufficient for G'^{-1} to be a PRP. We prove these cases first. Then the proof for the third category, which requires four rounds, follows directly. The inputs are of the form $(z3, w3)$ when using three rounds and $(z4, w4)$ when using four rounds. The outputs are of the form $(a1, w1)$. D_3 and D_4 will denote the distinguishers when three and four rounds are under consideration, respectively. When the number of rounds is not specified, D_r will be used to denote either D_3 or D_4. If a distinguisher exists for G'^{-1} it must fall into one of the following three categories:

- Category I: D_r does not use the $a1$ portion of the output in its decision. The only part of the output used is the $w1$ portion. This means that given the n input/output pairs in $S2$ and $S1$, D_r never uses the $a1$ portion from any of the pairs in $S1$.
- Category II: D_r does not use the $w1$ portion of the output in its decision. The only part of the output used is the $a1$ portion. This means that given the n input/output pairs in $S2$ and $S1$, D_r never uses the $w1$ portion from any of the pairs in $S1$.
- Category III: D_r uses both the $a1$ and $w1$ portion of the outputs in its decision. This means that given n input/output pairs in $S2$ and $S1$, D_r uses the $a1$ portion of the output from at least one of them and uses the $w1$ portion from at least one of them. Without using both portions, D_r fails to distinguish the elastic network from a RP.

In each category, there are no restrictions on what portions of the inputs, $\{(z3_i, w3_i)\}$ or $\{(z4_i, w4_i)\}$, are used. When D_r is restricted to Category II or III, only three rounds are needed for G^{-1} to be a PRP. These two categories will be addressed before Category I. Similar to what was done with the encryption direction, D_r can be used to create a distinguisher for one of the round functions. Since the round functions are random permutations, this results in a contradiction; therefore, D_r cannot exist.

Category II: If D_3 falls into Category II, a distinguisher, D_{RF1}, can be defined for the inverse of the first round function of G' (the last round of G'^{-1}). Intuitively, D_3 using only the $a1$ portion of the output of G'^{-1} when $a1$ is from the output of $RF1^{-1}$ whose inputs cannot be predicted with non-negligible probability implies D_3 can distinguish $RF1^{-1}$ from a random permutation. The inputs to $RF1^{-1}$ are distinct except with negligible probability. Therefore, the $a1$ values are distributed as if they are the outputs of n distinct queries to $RF1^{-1}$, except with negligible probability. Therefore, D_3 using only the input to G'^{-1} and the $a1$ portion of the output implies D_3 can distinguish $RF1^{-1}$ from a random permutation.

Define D_{RF1} as follows:

Ask D_3 what its first query (input) would be if it was querying $B_{G'}$. Populate $S2$ with this first input, so $(z3_1, w3_1)$ has been chosen and is in $S2$. $S2$ is known to D_{RF1}.

```
for $i = 1$ to $n$ {
    Take $(z3_i, w3_i)$ from $S2$ for use in subsequent steps.
    Set $a3_i = O3^{-1}(z3_i)$.
    Set $(z2_i, w2_i) = F2(a3_i, w3_i)$.
```

```
        Set $a2_i = O2^{-1}(z2_i)$.
        Set $(z1_i, w1_i) = F1(a2_i, w2_i)$.
        Set $a1_i = B_{RF1}^{-1}(z1_i)$.
        Give $a1_i, z3_i, w3_i$ to $D_3$.
        Add to $S2$ the next input $D_3$ would use when trying to distinguish $D_3$, having
        seen the inputs and output of the first $i$ queries. This is $(z3_{i+1}, w3_{i+1})$.
    }
    Let $ans$ be the value $D_3$ returns.
    $D_{RF3v2}$ returns $ans$.
```

The values given to D_3 are the inputs and outputs of the inverse of a three-round elastic network with $RF3$ as the third round function, $RF2$ as the second round function and the contents of B_{RF1} as the first round function. These values correspond to the contents of $S2$ and the $a1_i$ values of $S1$ when D_3 is allowed to make n adaptive chosen plaintext queries to $B_{G'}$. D_3 succeeds with non-negligible probability in determining it was given the input and output of G' implies D_{RF1} will succeed with non-negligible probability in determining the contents of B_{RF1}, contradicting the assumption that the first round function is a random permutation.

Category III: If D_3 falls into Category III, a distinguisher, D_{RF3}, can be defined for the inverse of the first round function, $RF1^{-1}$. Intuitively, D_3 can be viewed as using some relationship between partial information (*i.e.* $w1$) used in forming the input to $RF1^{-1}$ and the output (i.e. $a1$) of $RF1^{-1}$ to distinguish the first round function from a random permutation.

Define D_{RF1v2} to be D_{RF1} with the addition that the $w1_i$ values are also given to D_3.

Ask D_3 what its first query (input) would be if it was querying $B_{G'}$ in the decryption direction. Populate $S2$ with this first input, so $(z3_1, w3_1)$ has been chosen and is in $S2$. $S2$ is known to D_{RF1v2}.

```
    for $i = 1$ to $n$ {
        Take $(z3_i, w3_i)$ from $S2$ for use in subsequent steps.
        Set $a3_i = O3^{-1}(z3_i)$.
        Set $(z2_i, w2_i) = F2(a3_i, w3_i)$.
        Set $a2_i = O2^{-1}(z2_i)$.
        Set $(z1_i, w1_i) = F1(a2_i, w2_i)$.
        Set $a1_i = B_{RF1}^{-1}(z1_i)$.
        Give $a1_i, w1_i, z3_i, w3_i$ to $D_3$.
        Add to $S2$ the next input $D_3$ would use when trying to distinguish
        $D_3$, having seen the inputs and output of the first $i$ queries.
        This is $(z3_{i+1}, w3_{i+1})$.
    }
    Let $ans$ be the value $D_3$ returns.
    Return $ans$.
```

The values given to D_3 are the inputs and outputs of the inverse of a three-round elastic network with $RF3$ as the third round function, $RF2$ as the second round function and the contents of B_{RF1} as the first round function. These values correspond to those of $S1$ and $S2$ when D_3 is allowed to make n adaptive chosen plaintext queries to $B_{G'}$. D_3 succeeds with non-negligible probability in determining it was given the input and output of G' implies D_{RF1v2} will succeed with non-negligible probability in determining the contents of B_{RF1}, contradicting the assumption that the first round function is a random permutation.

Category I: The result for this category follows directly from the results for Categories II and III. If D_4 only uses the $w1$ portion of the outputs, since $w1 = w2 \oplus a2$, this implies D_4 is using a combination of $a2$ and $w2$ on which to base its decision. This implies D_4 is a distinguisher for the first three rounds of the network in the decryption direction that falls into Category III because the leftmost b-bit portion ($a2$) and rightmost y-bit portion ($w2$) of the three round output is used. Assume D_4 exists for the four-round network. D_4 is used to define a distinguisher, D_3, for the three rounds consisting of $RF4^{-4}$ to $RF2^{-2}$, taking inputs $(z4_i, w4_i)$ and producing outputs $(a2_i, w2_i)$. In this case, $B_{G'}$ is a black box containing either G^{-1} with four-rounds or a random permutation on $b + y$ bits. Let B_3 be a black box containing either the three-round elastic network formed from rounds $RF4^{-4}$ to $RF2^{-2}$ or a random permutation on $b+y$ bits.

Define D_3 as follows:

Ask D_4 what its first query (input) would be if it was querying $B_{G'}$ in the decryption direction. Populate $S2$ with this first input, so $(z4_1, w4_1)$ has been chosen and is in $S2$. $S2$ is known to D_3.

```
for $i = 1$ to $n$ {
    Take $(z4_i, w4_i)$ from $S2$ for use in subsequent steps.
    Give $(z4_i, w4_i)$ to $B_3$ and get back $(a2_i, w2_i)$.
    Set $w1_i = a2_i \oplus w2_i$.
    Give $w1_i, z4_i, w4_i$ to $D_4$.
    Add to $S2$ the next input $D_4$ would use when trying to distinguish $B_{G'}$, having
    seen the inputs and output of the first $i$ queries. This is $(z4_{i+1}, w4_{i+1})$.
}
Let $ans$ be the value $D_4$ returns.
$D_3$ returns $ans$.
```

The values given to D_4 are the inputs and rightmost y bits of the outputs of the inverse of a four-round elastic network. These y bits are formed from both the b-bit and y-bit portions of the output of three rounds. Therefore, by the assumption D_4 exists, D_3 will succeed with non-negligible probability in determining that the $(a2_i, w2_i)$ values were formed from the first three rounds of decryption. This contradicts the previous result from Category III.

For each of the three categories, we have shown D_r cannot exist. Therefore, the inverse of a four-round elastic network is a PRP when the round functions are independently chosen random permutations.

Using Theorems 1 and 2, we can prove that a three-round elastic network in the encryption direction and a four-round elastic network in the decryption direction is a variable-length PRP when the round functions are independently chosen fixed-length PRPs.

Theorem 3. *A three-round elastic network, G', on $b + y$ bits in which the round functions are independently chosen PRPs on b bits is a variable-length PRP on $b + y$ bits in the encryption direction for any fixed value of y where $0 \leq y \leq b$. Three rounds are the mininum number of rounds required.*

Proof. First, as noted in Theorem 1, a two-round elastic network cannot be a PRP. The result for three rounds follows directly from Theorem 1 and the triangle inequality. We consider the relationships between four versions of a three-round elastic network that differ in regards to the number of their round functions that are PRPs and RPs. We consider the relationships between the four versions shown in Figure 3 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.

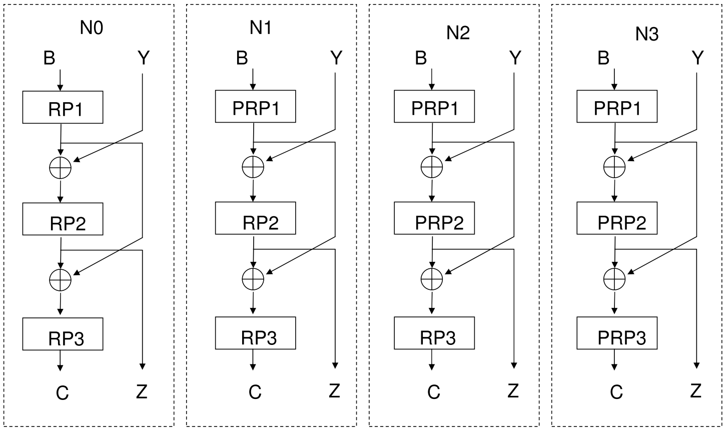


Fig. 3. Three-Round Networks Consisting of RPs and PRPs

We define the following six permutations:

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

Let Ni refer to a three-round elastic network in the encryption direction 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:

- $N0$: Each round function is a RP. The round functions are $RP1$, $RP2$ and $RP3$.
- $N1$: The first round function is the PRP. The second and third round functions are RPs. The round functions are $PRP1$, $RP2$ and $RP3$.
- $N2$: The first two round functions are PRPs and the third round function is a RP. The round functions are $PRP1$, $PRP2$ and $RP3$.

- $N3$: Each round function is a PRP. The round functions are $PRP1$, $PRP2$ and $PRP3$.

As shown by Theorem 1, $N0$ is a PRP. Therefore, if Theorem 3 is not true it is possible to distinquish $N3$ from $N0$ with probability $\geq \alpha$ for some non-negligible α where $0 < \alpha \leq 1$. However, if $N3$ can be distinquished from random then at least one of $PRP1, PRP2$ and $PRP3$ can be distinguished from random, which is a contradiction to the definition of a PRP and thus proves Theorem 3. 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 polynomially many outputs from Ni. 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 $\geq \frac{\alpha}{3}$. Therefore, it is possible to distinguish a three-round elastic network in the encryption direction that has i round functions that are pseudorandom permutations and $3 - i$ round functions that are random permutations from a three-round elastic network that has $i - 1$ round functions that are pseudorandom permutations and $4 - i$ round functions that are random permutations with non-negligible probability, where i is at least one value from $\{1, 2, 3\}$. Therefore, it is possible distinguish between a round function which is a random function and one that is a pseudorandom function with non-negligible probability, contradicting the definition of pseudorandom.

Theorem 4. *The inverse of a four-round elastic network, (G'^{-1}), on $b+y$ bits in which the round functions are independently chosen PRPs on b bits is a variable-length pseudorandom permutation on $b + y$ bits for any fixed value of y where $0 \leq y \leq b$. Four rounds are the minimum number of rounds required.*

Proof. First, as noted in Theorem 2, the inverse of a three-round elastic network cannot be a PRP. The proof uses the same method as in the proof to Theorem 3, with each network now having four rounds and Ni defined for $i = 0, 1, 2, 3, 4$, with $4 - i$ round functions being RPs and i round functions being PRPs. 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 four independently chosen pseudorandom permutations.
- Let $RP1, RP2, RP3, RP4$ be four independently chosen random permutations.

Let Ni refer to the inverse of a four-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:

- $N0$: Each round function is a RP. The round functions are $RP1$, $RP2$, $RP3$ and $RP4$.

- $N1$: The first round function is the PRP. The second to fourth round functions are RPs. The round functions are $PRP1$, $RP2$, $RP3$ and $RP4$.
- $N2$: The first two round functions are PRPs and the last two are RPs. The round functions are $PRP1$, $PRP2$, $RP3$ and $RP4$.
- $N3$: The first three round functions are PRPs and the last one is a RP. The round functions are $PRP1$, $PRP2$, $PRP3$ and $RP4$.
- $N4$: Each round function is a PRP. The round functions are $PRP1$, $PRP2$, $PRP3$ and $PRP4$.

As shown by Theorem 2, $N0$ is a PRP. Therefore, if Theorem 4 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 $N4$ 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 4 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 polynomially many outputs from Ni. If $N4$ can be distinguished from a random permutation, then $|Pr(N0) - Pr(N4)| \geq \alpha$.
However,
$|Pr(N0) - Pr(N4)| = |Pr(N0) - Pr(N1) + Pr(N1) - Pr(N2) + Pr(N2) - Pr(N3) + Pr(N3) - Pr(N4)|$
$\leq |Pr(N0) - Pr(N1)| + |Pr(N1) - Pr(N2)| + |Pr(N2) - Pr(N3)| + |Pr(N3 - Pr(N4)|$.
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 $\geq \frac{\alpha}{4}$. Therefore, it is possible to distinguish a four-round elastic network in the decryption direction that has i round functions which are pseudorandom permutations and $4 - i$ round functions that are random permutations from a four-round elastic network that has $i - 1$ round functions that are pseudorandom permutations and $5 - i$ round functions that are random permutations with non-negligible probability, where $i \in \{1, 2, 3, 4\}$. Therefore, it is possible distinguish between a round function which is a random function and one that is a pseudorandom function with non-negligible probability, contradicting the definition of pseudorandom.

4 Variable-Length SPRP from Fixed-Length PRPs

We now show how to construct variable-length SPRPs from fixed-length PRPs. First, we prove that a five-round elastic network in which the round functions are independently chosen fixed-length PRPs is a variable-length SPRP. This allows us to form SPRPs on $b + y$ bits from b-bit PRPs, where $0 \leq y \leq b$.

We note that a five-round elastic network consisting of round functions that are independently chosen PRPs is a PRP in both the encryption and decryption directions by Theorems 3 and 4. We also note that by the definition of a SPRP, any random permutation is a SPRP. Before stating the theorem regarding the $b + y$ bit SPRP, we prove a claim. Let $RP1$ and $RP2$ be two independently chosen random permutations, each on m bits. Let $Perm1(x) = RP2(RP1(x))$, where x is of length m. $Perm1$ is a random permutation on m bits and is a SPRP. Now we consider what happens if we use a combination of pseudorandom permutations and permutations in place of RP1 and RP2. We define permutations, $P1$, $P2$, $PRP1$ and $PRP2$ to satisfy the following conditions:

- $P1(x)$ and $P2(x)$ are independently chosen permutations on m bits. $P1 \neq P2$ except with negligible probability. $P1$ is not pseudorandom in that a relationship between some subset of bits in its inputs and outputs that occurs with non-negligible probability is known, but the exact permutation is unknown. Specifically, when given a black box that contains either $P1$ or a random permutation on b bits, it is possible to determine the contents of the box in polynomially many queries. However, when using $P1$ in forming PA as defined below, the exact permutation corresponding to $P1$ is unknown in that $P1$ will involve applying a PRP to the first b bits of its $(b+y)$-bit input. Likewise for $P2$, which is used to form PB as defined below. The PRPs used in $P1$ and $P2$ are not the same PRP, except with negligible probability.
- $PRP1(x)$ and $PRP2(x)$ are pseudorandom permutations on m bits whose independence is defined by the independence of $P1$ and $P2$ such that $P2(PRP2(P1(x))) = PRP1^{-1}(x)$.
- $PA(x) = PRP2(P1(x))$
- $PB(x) = PRP1(P2(x))$. Therefore, $PB = PA^{-1}$
- $Perm2$ will refer to the permutation corresponding to PA and PB. $Perm2 = PA$ and $Perm2^{-1} = PB$.

It is possible to define $P1, P2, PRP1$ and $PRP2$ that satisfy these constraints. For example, we will later show how a five-round elastic network can be viewed in this manner by defining $P1$ to be the first round, $P2$ to be the inverse of the last round, $PRP2$ to be the last four rounds and $PRP1$ to be the inverse of the first four rounds. $Perm2$ is a pseudorandom permutation on m bits (this is just $PRP2$ and $PRP1$ with the inputs selected by choosing m bits then applying a permutation, $P1$ or $P2$, to the input before giving it to the pseudorandom permutation).

Claim 1: $Perm2$ is a SPRP.

Proof. In order for $Perm2$ to be a SPRP it must not be possible to distinguish $Perm2$ from a random permutation on polynomially many (n) queries to PA and its inverse, PB. For simplicity, when we say an adversary is querying $Perm1$ or $Perm2$, we mean the adversary is able to issue queries to both the permutation and its inverse. The adversary does not have direct access to $P1$ and $P2$, meaning the adversary is not able to query $P1$ and use the output as input to $PRP2$ and/or query $P2$ and use the output as input to $PRP1$. The adversary can only give inputs to PA and PB.

- Let (p_i, c_i), for $i = 1$ to n be pairs of m bit strings such that $c_i = PA(p_i)$.
- Let $< +, p_i >$ denote a query to PA using input p_i.
- Let $< -, c_i >$ denote a query to PB 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 $T = (t_1, t_2, ...t_n)$ be the output of n distinct queries to PA. 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 that if an adversary 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 $U = (u_1, u_2, ...u_n)$ be the output of n 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 $\frac{1}{2^m - i}$ because $Perm1$ is a random permutation. The probability of a specific U occuring is $Pr_R = \prod_{i=0}^{n-1} \frac{1}{2^m - i}$.

Since PA 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-negligible probability. For any single query to PA, the output occurs with probability $\frac{1}{2^m} + e$ for some negligible e. When given i queries to PA, the $(i+1)^{st}$ such query produces an output that occurs with probability $\frac{1}{2^m - i} + e_{A_i}$ for negligible e_{A_i}. Likewise, when given i queries to PB, the $(i+1)^{st}$ such query produces an output that occurs with probability $\frac{1}{2^m - i} + e_{B_i}$ for negligible e_{B_i}. Even though PA and PB are inverses of each other, there is no non-negligible relationship between the outputs of PA and PB because these are the outputs of $PRP2$ and $PRP1$, respectively. A transcript of $n1$ distinct queries to PA will occur with probability $(\prod_{i=0}^{n1-1} \frac{1}{2^m - i}) + e_A$ for negligible e_A. A transcript of $n2$ distinct queries to PB will occur with probability $(\prod_{j=0}^{n2-1} \frac{1}{2^m - j}) + e_B$ for negligible e_B.

We consider the probability with which a transcript, T_{PA}, of $n1$ queries to PA occurs and with which a transcript, T_{PB}, of $n2$ queries to PB occurs. Suppose an adversary makes $n1$ queries to PA and that between the queries, the adversary is given (p_l, c_l) pairs that correspond to PA (ı.e., the adversary is given extra pairs for which he did not need to expend resources) such that overall, the adversary is given $n2$ such pairs. The adversary will not repeat any query or make a query for which he already been given the outcome. Let na_i be the number of (p_l, c_l) pairs the adversary has been given prior to the $(i+1)^{st}$ query to PA. $na_i \geq na_{i-1}$ for $1 \leq i \leq n1$. T_{PA} occurs with probability $Pr_A = (\prod_{i=0}^{n1-1} \frac{1}{2^m - i - na_i}) + e_{PA}$ for negligible e_{PA}. Suppose an adversary makes $n2$ queries are made to PB and that between the queries, the adversary is given (p_l, c_l) pairs that correspond to PB (ı.e., the adversary is given extra pairs for which he did not need to expend resources) such that overall, the adversary is given $n1$ such pairs. The adversary will not repeat any query or make a query for which he already been given the outcome. Let nb_j be the number of (p_l, c_l) pairs the adversary has been given prior to the $(j^+1)st$ query to PB. $nb_j \geq nb_{j-1}$ for $1 \leq j \leq n2$. T_{PB} occurs with probability $Pr_B = (\prod_{j=0}^{n2-1} \frac{1}{2^m - j - nb_j}) + e_{PB}$ for negligible e_{PB}.

When $n = n1 + n2$ queries are made to Perm2 such that $n1$ queries are made to PA and $n2$ are made to PB (the queries can be in any order), the probability of the resulting transcript, T, from Perm2 can be written as the product of Pr_A and Pr_B. Let qB_i be the number of queries made to PB between the i^{th} and $(i+1)^{st}$ queries to PA. Let qA_j be the number of queries made to PA between the j^{th} and $(j+1)^{st}$ queries to PB. By setting $na_i = \sum_{k=0}^{i} qA_k$ and $nb_j = \sum_{k=0}^{j} qB_k$, the probability of T occurring is

$(Pr_A)(Pr_B) = ((\prod_{i=0}^{n1-1} \frac{1}{2^m-i-na_i}) + e_{PA})* ((\prod_{j=0}^{n2-1} \frac{1}{2^m-j-nb_j}) + e_{PB})$
$= (\prod_{i=0}^{n1-1} \frac{1}{2^m-i-na_i}) * (\prod_{j=0}^{n2-1} \frac{1}{2^m-j-nb_j}) + (\prod_{i=0}^{n1-1} \frac{1}{2^m-i-na_i}) * e_{PA}$
$+(\prod_{j=0}^{n2-1} \frac{1}{2^m-j-nb_j}) * e_{PB} + e_{PA} * e_{PB}.$
$= \prod_{i=0}^{n-1} \frac{1}{2^m-i} + e$ for negligible e.
Therefore, it is not possible to distinguish T from U with non-negligible probability.

Theorem 5. *A five-round elastic network on $b + y$ bits in which each round function is an independently chosen PRP on b bits is a variable-length SPRP on $b + y$ bits for any fixed value of y where $0 \leq y \leq b$. Five rounds are the minimum number of rounds required.*

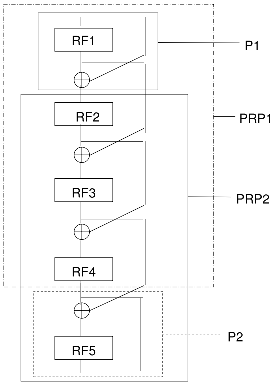


Fig. 4. Five-Round Elastic Network as Two PRPs and Two Permutations

Proof. Refer to Section 5 for an example showing why four rounds are insufficient.

G' refers to a five-round elastic network on $b + y$ bits with round functions that are independently chosen PRPs on b bits. G' can be defined in a format consistant with the four permutations used in Claim 1: $P1, P2, PRP1, PRP2$. Figure 4 shows a five-round elastic network represented in this manner. In the figure, the RFi's are independently chosen pseudorandom permutations.

- Let $P1$ refer to the first round of G', including the swap step.
- Let $P2$ refer to the inverse of the last round of G', including the swap step that precedes the round function. *i.e.,* $P2$ is the first round in G'^{-1}.
- $P1$ and $P2$ are independently chosen permutations, because each RFi is a independently chosen pseudorandom permutations. The exact permutations used for $P1$ and $P2$ are unknown because they involve $RF1$ and $RF4$, respectively. $P1$ and $P2$ are not pseudorandom because they can be distinguished from a random permutation by using queries where the b bit portion of input is held constant and the y-bit portion is varied.
- Let $PRP2$ refer to the last four rounds of G'; *i.e.,* all steps in G' after $P1$.
- Let $PRP1$ refer to the inverse of the first four rounds of G', excluding the swap step after the third round. $PRP1$ consists of all steps in G'^{-1} after $P2$.

$PRP1$ and $PRP2$ are PRPs on $b + y$ bits by Theorems 4 and 3. $PRP1 \neq PRP2^{-1}$. $P1$ and $P2$ are permutations on $b + y$ bits. By setting $PA = PRP2(P1(x))$ and $PB = PRP1(P2(x))$, $PB = PA^{-1}$. Therefore, by Claim 1, G' is a SPRP.

In our analysis for the three, four and five round cases, we required the round functions be independently chosen random permutations. It may be possible to relax the requirement that the round functions must independently chosen PRPs in a manner similar to what was done by Naor and Reingold in their analysis of Feistel networks [8]. While we have not determined to what extent the independence of the round functions can be relaxed, we know that at least two of the round functions must differ, except with negligible probability. Specifically, a three-round elastic network and the inverse of a four-round elastic network in which the round functions are identical are not PRPs. The proofs are provided in Section 5. These results indicate some independence is required of the round functions.

5 Counter-Examples

We provide a lower bound on the minimum number of rounds needed in an elastic network to create variable-length PRPs and variable-length SPRPs by providing examples of when fewer rounds are not PRPs and SPRPs. We also show that a certain level of independence is required between the round functions by considering cases when all of the round functions are identical. First, we show that at least three rounds are needed for an elastic network to be a PRP by proving that a two-round elastic network is not a PRP regardless of the round functions. Second, we show that a three-round elastic network is not a PRP when the round functions are identical. Third, we show that the inverse of a three-round elastic network is not a PRP regardless of the round functions. Fourth, we show that the inverse of a four-round elastic network is not a PRP when the round functions are identical. Fifth, we show that three and four-round elastic networks are not SPRPs, regardless of the round functions. When proving an elastic network is not a variable-length PRP or variable-length SPRP under specific conditions on the number of rounds and/or round functions, it is sufficient to provide an example for one block size. All of the counter-examples use a $2b$-bit block size ($y = b$). Each example will not hold with probability 1 when $y < b$.

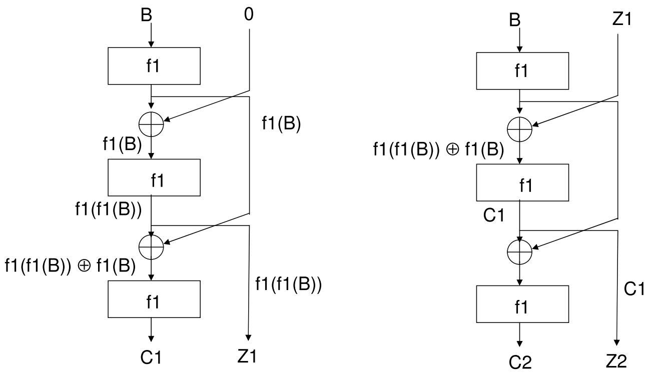
Claim 2:

An elastic network with exactly two rounds is not a PRP.

Proof. This claim holds regardless of the properties of the round functions. Consider the case where $y = b$. Given two $2b$-bit plaintexts of the form $B||Y1$ and $B||Y2$ (the b-bit portion is the same in each), let the ciphertexts be denoted by $C1||Z1$ and $C2||Z2$, respectively. $Z1 = Z2$ with probability 1. If the two-round construction was a PRP on $b + y$ bits, then for large b, this equality would occur with probability $2^{-b} \pm e$ for negligible e instead of with probability 1.

Claim 3:

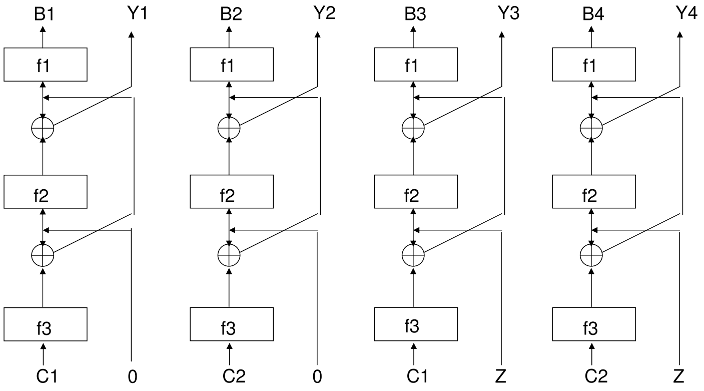
A three-round elastic network is not a PRP when the round functions are identical.



|B| = |0| = |Z1|
Encrypting B || Z1 results in Z2 = C1

Fig. 5. Three-Round Elastic Network with Identical Round Functions

Proof. Consider the case shown in Figure 5 when $y = b$. Let 0 denote a string of y zeroes. Encrypt $B||0$ and let $C1||Z1$ denote the resulting ciphertext. $Z1 = f1(f1(B))$. $C1 = f1(f1(f1(B)) \oplus f1(B))$. Then encrypt $B||Z1$ and let $C2||Z2$ denote the ciphertext. $Z2 = C1$ with probability 1. If this three-round network was a PRP on $b + y$ bits, then for large b, this equality would occur with probability $2^{-b} \pm e$ for negligible e instead of with probability 1.



|Ci| = |Z| = b, C1 ≠ C2, 0 = string of b zeroes, Z ≠ 0

Fig. 6. Three-Round Elastic Network: Chosen Ciphertext Attack

Claim 4:

The inverse of a three-round elastic network is not a PRP.

Proof. This is illustrated in Figure 6. The inputs to the round functions are defined in the directions of the arrows in the figure and correspond to the direction of decryption. This claim holds regardless of the properties of the round functions and is due to the fact that, when $y = b$, the input to the inverse of the second round function is known because it is the rightmost y bits. In contrast, in the encryption direction, the XOR after the first round prevents the input to the second round function from being chosen. Let 0 denote a string of b zeroes. When $y = b$, create four $2b$-bit ciphertexts of the form $C1||0$, $C2||0$, $C1||Z$ and $C2||Z$ where $C1 \neq C2$ and $Z \neq 0$. Let the plaintexts be denoted by $B1||Y1$, $B2||Y2$, $B3||Y3$ and $B4||Y4$. Then $Y1 = f2^{-1}(0) \oplus f3^{-1}(C1)$, $Y2 = f2^{-1}(0) \oplus f3^{-1}(C2)$, $Y3 = f2^{-1}(Z) \oplus Z \oplus f3^{-1}(C1)$ and $Y4 = f2^{-1}(Z) \oplus Z \oplus f3^{-1}(C2)$. As a result, $Y1 \oplus Y2 = Y3 \oplus Y4$ with probability 1. If the three-round network was a PRP on $2b$ bits in the decryption direction, then for large b, this equality would occur with probability $2^{-b} \pm e$ for negligible e instead of with probability 1. When $y < b$, the attack does not hold with probability 1 because the input to the second round of decryption contains $b - y$ bits of $f4^{-4}(Ci)$. These $b - y$ bits would have to be equal for $f4^{-4}(C1)$ and $f4^{-4}(C2)$.

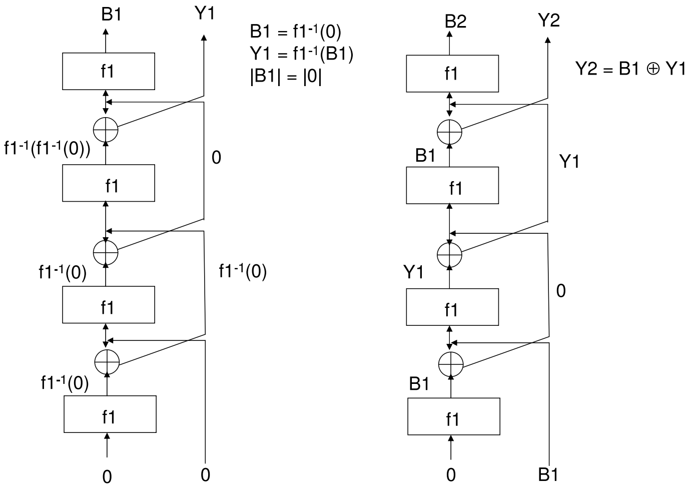


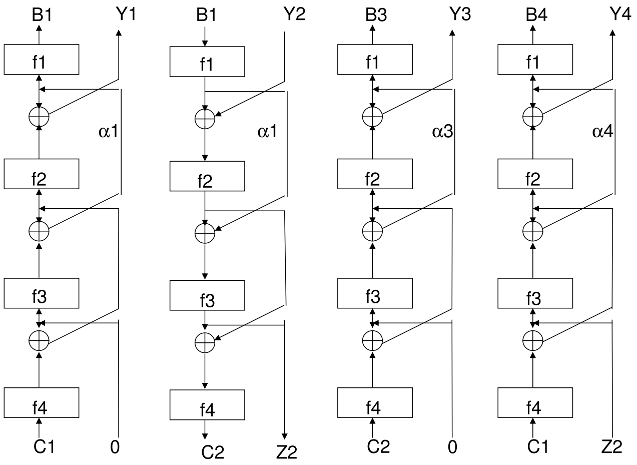
Fig. 7. Four-Round Elastic Network with Identical Round Functions

Claim 5:

The inverse of a four-round elastic network in which the round functions are identical is not a PRP.

Proof. Consider the case shown in Figure 7 when $y = b$. Let 0 denote a string of b zeroes. Decrypt $0||0$ and let $B1||Y1$ denote the resulting plaintext. $B1 = f1^{-1}(0)$. $Y1 = f1^{-1}(f1^{-1}(0)) = f1^{-1}(B1)$. Decrypt $0||B1$ and let $B2||Y2$ denote the resulting plaintext. $Y2 = f1^{-1}(B1) \oplus f1^{-1}(0) = Y1 \oplus B1$ with probability 1. If the inverse of this four-round network was a PRP on $b + y$ bits, then for large b, this equality would occur with probability $2^{-b} \pm e$ for negligible e instead of with probability 1.

Neither a three-round nor a four-round elastic network is a SPRP. In both cases, this can be shown with an adaptive chosen plaintext - chosen ciphertext attack in which two chosen plaintexts are encrypted then two chosen plaintexts formed from the two resulting ciphertexts are decrypted. We include one four-round counter-example here.



|0| = |Bi| = |Yi| = |Ci| = |Zi| Y1 ≠ Y2
Results in B3 = B4

Fig. 8. Four-Round Elastic Network: Chosen Plaintext - Chosen Ciphertext Attack

Claim 6:

A four-round elastic network is not a SPRP when $b = y$.

Proof. This claim holds regardless of the properties of the round functions and is due to the fact that a three-round elastic network in the decryption direction is not a PRP. In the three round case, using chosen ciphertexts only, a relationship can be pushed through the three rounds of decryption into the right half of the output with probability 1 when $y = b$. In the four round case, the same approach is used in that the halves of two ciphertexts are switched to form to new ciphertexts and push a relationship into the rightmost y bits of the output of the third round. When $y = b$, this becomes the entire input to the round function in the fourth round of decryption. This time, one plaintext must be encrypted to assist in providing the values from which the ciphertexts are formed. The sequence of three decryptions and one encryption shown in Figure 8 can be used to distinguish the four-round elastic network from a SPRP when $y = b$. Each plaintext and ciphertext is of length $2b$, ı.e. $|B| = |Bi| = |Yi| = |Ci| = |Zi| = b \; \forall i$. Let 0 denote a string of y zeroes. Decrypt a ciphertext of the form $C1||0$. Let $B1||Y1$ be the resulting plaintext. Encrypt a plaintext of the form $B1||Y2$ with $Y2 \neq Y1$. Let $C2||Z2$ be the resulting ciphertext. The output of the first round function, $\alpha 1$, is identical in both the decryption and encryption. Form two ciphertexts, $C2||0$ and $C1||Z2$, and decrypt them. Let $B3||Y3$ and $B4||Y4$ denote the two resulting plaintexts. $B3 = B4$ with probability 1.
Notice that: $\alpha 1 = f4^{-1}(C1) \oplus f3^{-1}(0) = Z2 \oplus f4^{-1}(C2) \oplus f3^{-1}(Z2)$

$$\alpha 3 = f4^{-1}(C2) \oplus f3^{-1}(0)$$
$$\alpha 4 = Z2 \oplus f4^{-1}(C1) \oplus f3^{-1}(Z2)$$

By rearranging the equations for $\alpha 1$:

$$f4^{-1}(C2) \oplus f3^{-1}(0) = Z2 \oplus f4^{-1}(C1) \oplus f3^{-1}(Z2).$$

Therefore, $\alpha 3 = \alpha 4$ and $B3 = B4$.

6 Conclusions and Extensions

Our analysis validates the soundness of the underlying structure used in creating elastic block ciphers. We have proven that a three-round elastic network and the inverse of a four-round elastic network are variable-length PRPs and a five-round elastic network is a variable-length SPRP when the round functions are independently chosen PRPs. These results allow for the creation of $(b+y)$-bit PRPs and SPRPs from b-bit PRPs, for each value of y where $0 \leq y \leq b$. We also proved that these are the minimum number of rounds required and that the results do not hold when all of the round functions are identical.

We can extend our PRP and SPRP constructions to cover a wider range of input sizes by using instances of CMC mode [5] as the round functions within the elastic network. CMC mode produces mb-bit SPRPs from a fixed-length b-bit PRP, where m is an integer and $2 \leq m \leq \alpha$, for some integer upper bound of α. It involves encrypting data using a block cipher in CBC mode, applying a mask, then encrypting the resulting data in a reverse CBC mode. By using a b-bit PRP in CMC mode for each of the round functions in the elastic network (the PRPs are still independently chosen across each round), we are able to create variable-length SPRPs on a larger range of input lengths, in single bit increments, then when using the elastic network by itself. This combination for supporting variable-length inputs is unique from previous designs of variable-length block ciphers that worked on any input length [1, 9]. Those constructions work by creating an IV to use with the cipher in counter mode, then create a key stream to XOR with all but one block of the data. When dealing with input lengths beyond two blocks, the use of CMC mode and the elastic network provides an alternative approach to [1, 9] that does not apply a key stream, but rather creates a permutation that results in diffusion across all of the bits.

Acknowledgments

This work was partially supported by NSF Grants ITR CNS-04-26623 and CPA CCF-05-41093. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF or the U.S Government.

References

1. M. Bellare and P. Rogaway, On the Construction of Variable Length-Input Ciphers, *Proceedings of Fast Software Encryption 1999*, LNCS 1636, Springer-Verlag, pages 231-244, 1999.

2. D. Cook, M. Yung and A. Keromytis, Elastic Block Ciphers: The Basic Design, *Proceedings of ASIACCS*, ACM, pages 350-355, 2007.
3. D. Cook, M. Yung, and A. Keromytis, The Security of Elastic Block Ciphers Against Key-Recovery Attacks. *Proceedings of ISC*, LNCS 4779, Springer-Verlag, pages 89-103, 2007.
4. S. Gueron, Advanced Encryption Standard (AES) Instructions Set. http://softwarecommunity.intel.com/articles/eng/3788.htm, 2008.
5. S. Halevi and P. Rogaway, A Tweakable Enciphering Mode, *Proceedings of Advances in Cryptology* - Crypto 2003, LNCS 2729, Springer-Verlag, 2003.
6. M. Luby, Pseudorandomness and Cryptographic Applications, Princeton University Press, 1996.
7. M. Luby and C. Rackoff, How to Construct Pseudorandom Permutations from Pseudorandom Functions, *Siam Journal of Computing*, vol. 17, no. 2, pages 373-386, April 1988.
8. M. Noar and O. Reingold, On the Construction of Pseudo-random Permutations: Luby-Rackoff Revisited, *Journal of Cryptology*, vol. 12, pages 29-66, 1999.
9. S. Patel and Z. Ramzan and G. Sundaram, Efficient Constructions of Variable-Input-Length Block Ciphers, *Proceedings of Selected Areas in Cryptography 2004*, LNCS 3357, Springer-Verlag, 2004.
10. T. Ristenpart and P. Rogaway, How to Enrich the Message Space of a Cipher, *Proceedings of Fast Software Encryption 2007*, LNCS 4593, Springer-Verlag”, pages 101-118, 2007.