The Artin-Feistel Symmetric Cipher

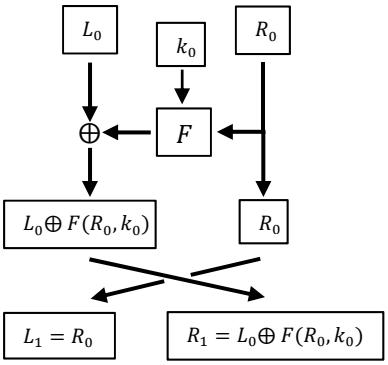
May 23, 2012

I. Anshel, D. Goldfeld

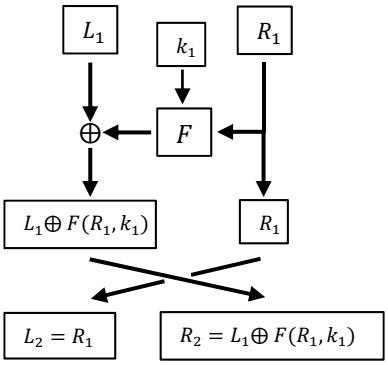
1. **Introduction.** The Feistel cipher and the Braid Group B_N

The main aim of this paper is to introduce a new symmetric cipher, which we call the Artin-Feistel cipher. The classical Feistel cipher/network (see [H]) lies at the heart of many important block ciphers, notably the Data Encryption Standard (see [C], FIPS-Pub. 46), and has been studied extensively for some time. One natural way to look at the core structure of the original cipher (and the later extensions) is from the point of view of geometric braids. In doing so a whole new level of complexity and security can be brought into the discussion and the Artin-Feistel symmetric cipher, whose underlying structure is a multi-strand geometric braid, emerges as unifying approach.

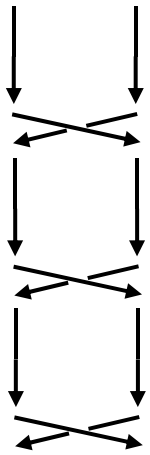
The Feistel cipher can be distilled to the following description. Let $F, k_1, k_2, \ldots, k_\ell$ denote a (round) function and a collection of sub-keys, and let $M = L_0 \cup R_0$ denote the decomposition of a plaintext block M into two equal pieces L_0, R_0. The ciphertext is obtained by concatenating a sequence of steps the first of which takes the form,



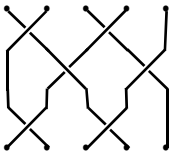
where $\oplus$ denoted the operation x/or. The output of the above step, L_1, R_1 are then input to the second step in the sequence, which takes the form.



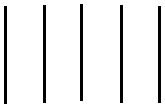
The process of evaluation of the functions F and $\oplus$ and then applying a permutation continues until the collection of sub-keys is exhausted. When viewed from a distance, the underlying skeletal structure of this concatenation of ciphering steps takes the form.



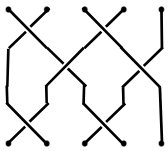
This sequence of twists is, by definition, a 2-strand geometric braid. E. Artin introduced the concept of a geometric braid, and more generally the N-stranded the Braid Group, B_N (see [A], [B]). An example of a 5-stranded braid β is given below:

$\beta =$ 

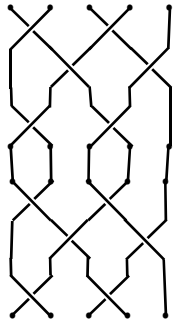
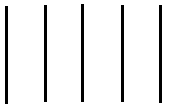
Given two N-strand braids, it is intuitively clear that concatenating them produces a third braid. This operation gives the set of N-strand braids, B_N, a group structure: continuing with the 5-strand case, the identity element of B_5 is given by,



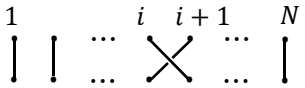
and the inverse of any braid is obtained by first vertically flipping the braid, and then reversing the crossings. In the case above, we see that

$\beta^{-1} =$ 

and we verify that $\beta\beta^{-1} = 1$:

$\beta\ \beta^{-1}=$  $=$ 

We will require one further observation. Every braid is a concatenation of elementary crossings of the strands i and $i+1$ and the inverses of said crossings: if we let $b(i)$ denote the braid



then the braid group B_N is generated by the braids $\{b(i) |\ i = 1, \dots, N-1\}$.

2. The Artin-Feistel Cipher

The core idea of the Artin-Feistel cipher is to take a braid $\beta \in B_N$, and insert Feistel steps within β prior to each crossing. The original Feistel cipher is easily recovered from the Artin-Feistel cipher by simply choosing β to be the ℓ-th power of the simple twist b_1 that generated the 2-strand braid group B_2: $\beta = b(1)^{\ell} \in B_2$. When we work with elements of the N-strand braid group, $\beta \in B_N$, the geometric braid β is transformed into an encryption mechanism.

Proceeding now to a detailed description, let $M = BL_1 \cup BL_2 \cup \cdots \cup BL_N$ denote a decomposition of a plaintext M into blocks BL_i of equal size. Let $\beta \in B_N$ be a nontrivial positive element of the N - strand braid group, i.e., an element of the form

$$\beta = b(i_1) \cdot b(i_2) \cdot \cdots \cdot b(i_\ell),$$

where ℓ is the length of β, and each $b(i_j)$ is an Artin generator, and $1 \le i_j \le N-1$ for $j = 1, \dots, \ell$. A given $b(i_j)$, which appears in β, may appear more than once in β. The number of times $b(i_j)$ appears in β, is termed the frequency of $b(i_j)$ in β, and is denoted

$$f(b(i_j), \beta).$$

For each appearance of the generator $b(i_j)$ in β, the position, denoted, $P(j,\beta)$ and defined by

$$P(j,\beta) = \text{Card}\{b(i_k) \mid b(i_k) = b(i_j), 1 \le k \le j\},$$

indicates which appearance in β it is. For example if $\beta = b(2)\cdot b(1)\cdot b(3)\cdot b(1)$, we have $f(b(1),\beta) = 2$, and $P(1,\beta) = 1$, $P(2,\beta) = 1$, $P(3,\beta) = 1$, and $P(4,\beta) = 2$.

For $i = 1, \dots, N-1$, let F_i be a sequence of (round) functions, and let $K(i)$ denote a collection of (not necessarily distinct) sub-keys which take the form,

$$K(i) = \{k(i,1), k(i,2), \dots, k(i, f(b(i),\beta))\}.$$

Setting

$$M(0,1) = BL_1,\ M(0,2) = BL_2,\ \dots\ , M(0,N) = BL_N,$$

the cipher will produce a sequence of $\ell = \text{length}(\beta)$ outputs, each of which has the same length as the plaintext: the output of the first step of the cipher will take the form,

$$M(1,1), M(1,2), \dots, M(1,N).$$

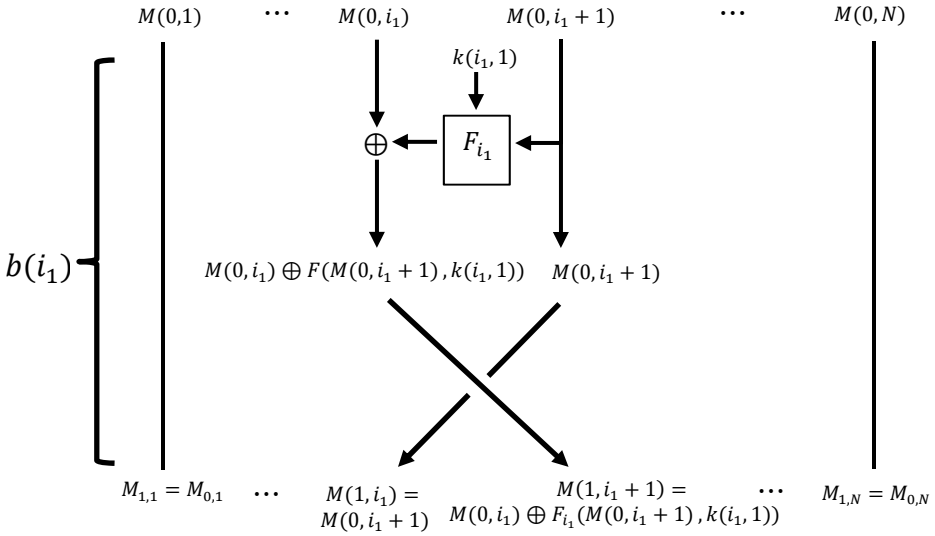
The output of the second step will take the form,

$$M(2,1), M(2,2), \dots, M(2,N),$$

and, continuing in this manner, the output of the final step,

$$M(\ell,1), M(\ell,2), \dots, M(\ell,N),$$

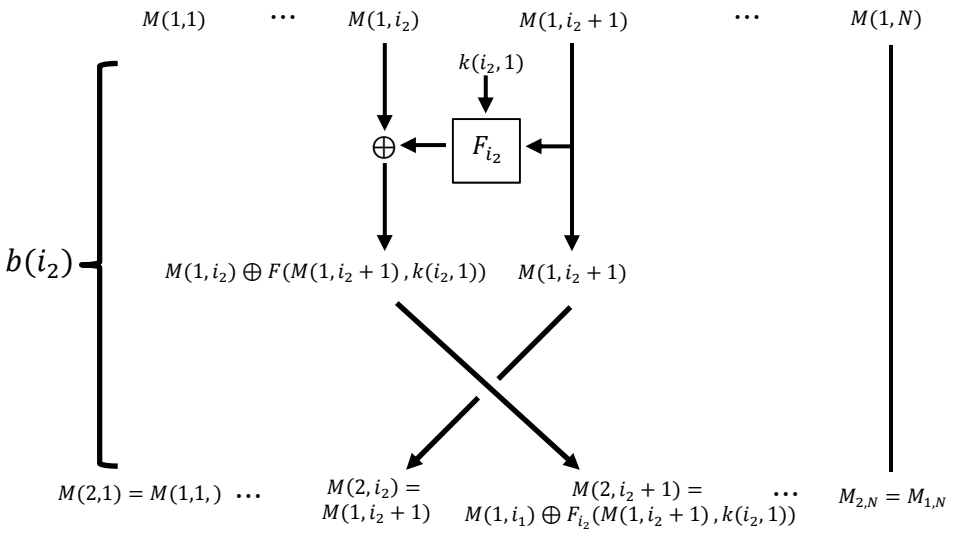
will be the ciphertext. Since the first crossing in the braid β is given by $b(i_1)$, we have $P(1,\beta) = 1$, and the first step in the cipher is dictated by the diagram below.



Thus the output of the first step of the cipher is given by,

$$M(1,q) = \begin{cases} M(0,q) & if\ q \neq i_1, i_1+1 \\ M(0,i_1+1) & if\ q = i_1 \\ M(0,i_1) \oplus F_{i_1}\big(M(0,i_1+1), k(i_1,1)\big) & if\ q = i_1+1 \end{cases}$$

This output sequence, $M(1,1), M(1,2), \dots, M(1,N)$, then becomes the input of the second diagram:



Note we are assuming that $b(i_2) \neq b(i_1)$, and hence $k(i_2,1)$ is the sub-key used in the above diagram. Were $b(i_2) = b(i_1)$, then $k(i_1,2)$ would be the sub-key used. Continuing in this manner we obtain the identities: for $j = 1, 2, \dots, \ell$

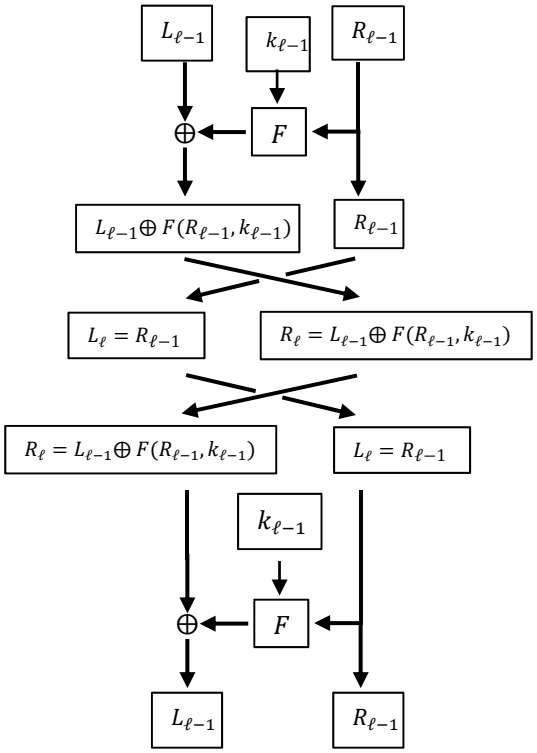
$$M(j,q) = \begin{cases} M(j-1,q) & if\ q \neq i_j, i_j+1 \\ M\big(j-1,i_j+1\big) & if\ q = i_j \\ M\big(j-1,i_j\big) \oplus F_{i_j}\Big(M\big(j-1,i_j+1\big), k\big(i_j, PV(j,\beta)\big)\Big) & if\ q = i_j+1 \end{cases}$$

The ciphertext, $M(\ell,1), M(\ell,2), \dots, M(\ell,N)$, is thus obtained after ℓ incremental steps of the Artin-Feistel cipher are performed.

In order to reverse the Artin-Feistel cipher we will takes the inverse braid, which takes the form

$$\beta^{-1} = b(i_\ell)^{-1} \cdot b(i_{\ell-1})^{-1} \cdot \cdots \cdot b(i_1)^{-1},$$

and inserting Feistel steps *after* each crossing (recall Feistel steps are inserted *before* each crossing during ciphering). In the case of a 2-stranded braid, this is precisely the classical method of recovering the plaintext from the ciphertext, i.e., this reverses the Feistel cipher. To see this note that by concatenating the final Feistel step with a reverse of the last crossing followed by the Feistel step associated with said crossing the ciphering is reversed.

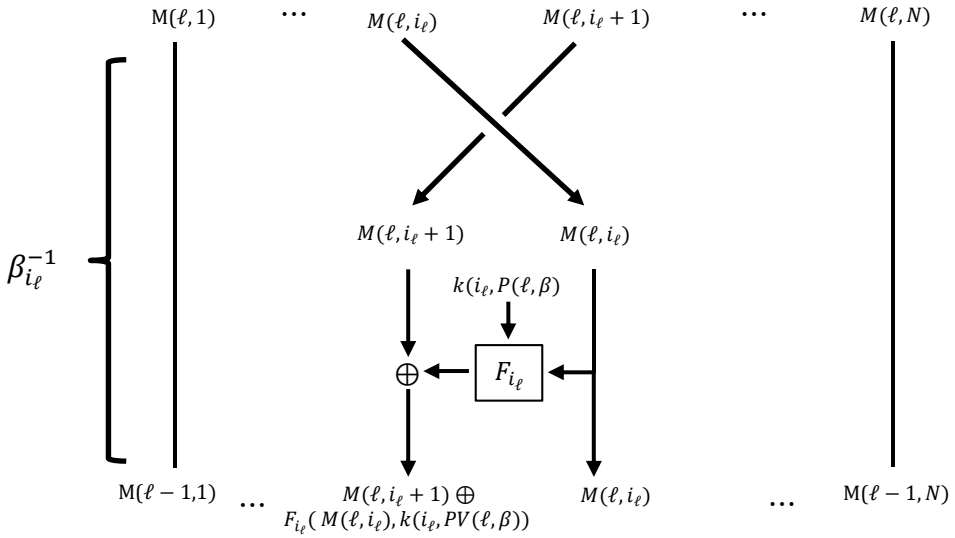


Reversing the Artin-Feistel cipher, although more complex, works in much the same way. Due to that intrinsic structure of the inverse of the braid, $\beta^{-1} = b(i_\ell)^{-1} \cdot b(i_{\ell-1})^{-1} \cdot \cdots \cdot b(i_1)^{-1}$, the order of the crossings is reversed. This implies that in the deciphering process both the sequence of functions used in the Feistel steps and the sequence of sub-keys inputted into those functions will be the reverse of the sequences used to cipher. Just as the ciphering process required $\ell = \text{length}(\beta)$ steps, the deciphering will likewise require the same number.

The output of the final step of the Artin-Feistel cipher is given by

$$M(\ell,1), M(\ell,2), \ldots, M(\ell,N),$$

will be the input of the first step of the deciphering process, which is given in the diagram below.



Recall that, by construction,

$$M(\ell,q) = M(\ell-1,q) \text{ if } q \neq i_\ell, i_\ell+1,$$

$$M(\ell,i_\ell) = M(\ell-1,i_\ell+1),$$

and

$$M(\ell,i_\ell+1) = M(\ell-1,i_\ell) \oplus F_{i_\ell}\big(M(\ell-1,i_\ell+1), k(i_\ell, PV(\ell,\beta))\big).$$

Hence the i_ℓ and $i_\ell+1$ entries in the output of the first step in the deciphering process can be simplified:

$$M(\ell,i_\ell+1) \oplus F(\, M(\ell,i_\ell), k\big(i_\ell, P(\ell,\beta)\big)$$

$$= M(\ell-1,i_\ell) \oplus F_{i_\ell}\big(M(\ell-1,i_\ell+1), k(i_\ell, PV(\ell,\beta))\big) \oplus F_{i_\ell}(\, M(\ell,i_\ell), k\big(i_\ell, P(\ell,\beta)\big)$$

$$= M(\ell-1,i_\ell) \oplus F_{i_\ell}\big(M(\ell-1,i_\ell+1), k(i_\ell, P(\ell,\beta))\big) \oplus F_{i_\ell}(\, M(\ell-1,i_\ell+1), k\big(i_\ell, P(\ell,\beta)\big)$$

$$= M(\ell-1,i_\ell),$$

and

$$M(\ell,i_\ell) = M(\ell-1,i_\ell+1).$$

We thus conclude that the output of the first step in the deciphering process is given by

$$M(\ell - 1,1), M(\ell - 1,2), \dots, M(\ell - 1, N),$$

which is the input to the ℓ^{th} step of the ciphering process, i.e., we have reversed the last step of the Artin-Feistel cipher. Continuing in this way the original Plaintext is recovered.

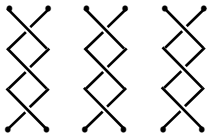
3. Security Discussion.

Any specific instance of the Artin-Feistel cipher depends on the precise knowledge of the braid β being used, which will be part of the secret key. In general, the number of possible positive braids of length ℓ, in the braid group B_N, is given by $(N-1)^{\ell}$. Not every braid is a good candidate for a secure cipher: each generator of B_N must appear sufficiently often to insure the entire plaintext is thoroughly obscured.

Observe that it is easy to choose a braid which reduces the Artin-Feistel cipher to a sequence of classical Feistel ciphers running in parallel: if for example $N = 6$, take the braid

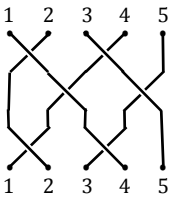
$$\beta = b(1)^{r_1} \cdot b(3)^{r_2} \cdot b(5)^{r_3}.$$

Visually, if $r_1 = r_2 = r_3 = 3$, then β is given by



To break a cipher based on such a braid would require each of the Feistel ciphers being run in parallel to be broken. Observe that in the classical Feistel cipher with $2r$ rounds, each plaintext block is obscured every time it moves to the right, and remains unchanged if it moves to the left. Thus each plaintext block is obscured r times. Given that the Artin-Feistel cipher can reduce to a sequence of classical Feistel ciphers running in parallel, it is clear that when choosing the braid β on which to base a cipher, each of the N plaintext blocks should be obscured by the cipher r times.

In order to produce a braid whose cipher will satisfy this condition consider the following example of a braid β:



Observe that the path emanating from the point labeled 1 on the top row (and ending at the point labeled 4 on the bottom row), moves to the right three times. The path starting at 2 only moves to the right one time on its way to the bottom row. The paths emanating from point 4 and 5 on the top row don't move to the right at all. An Artin-Feistel cipher based on the above braid would leave the plaintext blocks BL_4, BL_5 untouched in the final ciphertext, which may be undesirable.

The above discussion is the motivation for the following definition. Given an $i \in \{1, 2, \dots, N\}$, we define the total right displacement of i in the braid β, denoted

$$D(i, \beta),$$

to be the total number of times the path emerging from i moves to the right. Observe that if $D(i, \beta) = r$, then an Artin-Feistel cipher based on β obscures each block of plaintext r times as required. Thus we consider the following subset of B_N, which will serve as our search space:

$$B(N, r) = \{\beta \in B_N | D(i, \beta) = r \text{ for } i = 1,2, \dots, N\}.$$

A brute force search on the Artin-Feistel cipher based on a braid in the search space $B(N, r)$, is bounded below by

$$\text{Card}\big(B(N, r)\big).$$

We note that the length of any braid β, which is the Artin-Feistel equivalent to the number of rounds in a classical cipher, is given by the sum,

$$\text{length}(\beta) = \sum_{i=1}^{N} D(i, \beta) = N \cdot r,$$

each braid in $\beta \in B(N, r)$.

4. The Search Space: $B(N,r)$.

It is possible to obtain a lower bound for the size of the search space by explicitly constructing a large class of elements within it. Suppose we have two elements

$$\beta_1, \beta_2 \in B(N,1),$$

and we consider their product, $\beta_1 \cdot \beta_2$. Since each path commencing at $i = 1, 2, \dots, N$ moves to the right once in β_1, and then once in β_2, each path commencing at i will move to the right twice in the product $\beta_1 \cdot \beta_2$, i.e.,

$$\beta_1 \cdot \beta_2 \in B(N,2).$$

More generally, the product of r braids in $B(N,1)$, $\beta_1, \beta_2, \dots, \beta_r \in B(N,1)$, will be an element of the search space $B(N,r)$:

$$\beta_1 \cdot \beta_2 \cdot \cdots \cdot \beta_r \in B(N,r).$$

Observe that the number of such products $\beta_1 \cdot \beta_2 \cdot \cdots \cdot \beta_r$ is given by

$$\mathrm{Card}\big(B(N,1)\big)^r.$$

Thus we are reduced to identifying a collection braids lie in the set $B(N,1)$. To begin, observe that the collection of $N-1$ braids, which we will refer to as basic elements,

$$b(N-1)^2 \cdot b(N-2) \cdot \cdots \cdot b(1),$$

$$b(N-1) \cdot b(N-2)^2 \cdot \cdots \cdot b(1)$$

$$\vdots$$

$$b(N-1) \cdot b(N-2) \cdot \cdots \cdot b(1)^2$$

all have the required property that each path commencing at$i = 1, 2, \dots, N$ moves to the right once. Now suppose we express N as the sum

$$N = N_1 + N_2,$$

where $N_1, N_2 \geq 2$. Then by taking basic elements $\gamma_1 \in B(N_1,1)$, $\gamma_2 \in B(N_2,1)$ and juxtaposing them (γ_1 left, γ_2 to the right), we obtain an element in $B(N,1)$.

For example, 7 = 3 + 4, $b(2)^2 \cdot b(1) \in B(3,1)$, and $b(3) \cdot b(2)^2 \cdot b(1) \in B(4,1)$ juxtaposing them we obtain,

$$b(2)^2 \cdot b(1) \cdot b(6) \cdot b(5)^2 \cdot b(4) \in \ B(7,1).$$

This method produces various braids: since $B(3,1)$ contains 2 basic elements, and $B(4,1)$ contains 3 basic elements, this one decomposition of $N = 7$ as a sum yields 6 elements in $B(7,1)$. More generally, we have found a connection between braids in $B(N,1)$ and ordered partitions (i.e., $N_1 + N_2 + N_3$ is considered distinct from $N_2 + N_3 + N_1$) of the number N which do not involve either 0 or 1. Each partition of N

$$N = N_1 + N_2 + \cdots + N_k,$$

will produce

$$(N_1 - 1) \cdot (N_2 - 1) \cdot \cdots \cdot (N_k - 1)$$

elements in $B(N,1)$.

The number of ordered partitions of N grows rapidly. In the case $N = 12$, the number of elements of $B(N,1)$ that the above method generates is given by

$$2^{10} = 1024.$$

Recalling the above discussion, the size of the search space $B(N,r)$ is bounded below by

$$\mathrm{Card}\big(B(N,1)\big)^r$$

Thus, in the case $N = 12$, the search space $B(12,r)$ is bounded below by

$$2^{10 \cdot r},$$

and, hence, we see that it is possible to encrypt 12 blocks with a 2^{80} security level using a braid of length 8 ·12 = 96. Observe that the length of the braid is the number of rounds in the encryption process. In contrast triple DES requires 48 rounds to encrypt 2 blocks. It follows that, in this case, Artin –Feistel is a fast as single DES.

5. References.

Artin, Emil (1947), "Theory of braids", *Annals of Mathematics*, 2nd Ser. **48** (1): 101–126

Birman, Joan S. (1974), *Braids, links, and mapping class groups*, Annals of Mathematics Studies, **82**, Princeton, N.J.: Princeton University Press

Coppersmith, Don. (1994). The data encryption standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, **38**(3), 243–250.

Horst Feistel, "Cryptography and Computer Privacy." *Scientific American*, Vol. 228, No. 5, 1973.

FIPS-Pub.46, National Bureau of Standards, Data Encryption Standard. National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

6. Author Contact Information.

Iris Anshel
ianshel@securerf.com

Dorian Goldfeld
goldfeld@optonline.net

This material is based upon work supported by the National Science Foundation under Grant No. 0924363.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.