3-round Feistel is Not Superpseudorandom Over Any Group

Hector B. Hougaard

Abstract

Luby and Rackoff used a Feistel cipher over bit strings to construct a pseudorandom permutation from pseudorandom functions in 1988 and in 2002, Patel, Ramzan, and Sundaram generalized the construction to arbitrary abelian groups. They showed that the 3-round Feistel cipher is not superpseudorandom over abelian groups but left as an open problem a proof for non-abelian groups. We give this proof.

Keywords: Feistel, non-abelian group, pseudorandom.

1 Introduction

In cryptography, perhaps the most important question is how to create randomness. The best answer is to create something that looks random, which we call "pseudorandom". One way to create such pseudorandomness, is to start from one-way functions, functions that are easy to compute but hard to reverse. From these one-way functions, Håstad et al [HILL99] showed how to construct a generator of pseudorandomness, a so-called pseudorandom generator (PRG). Using PRGs, Goldreich, Goldwasser, and Micali [GGM86] showed how to create a pseudorandom function. Finally, Luby and Rackoff [LR88] showed how to turn pseudorandom functions into pseudorandom permutations, using the Feistel cipher [Fei73].

In their seminal paper, Luby and Rackoff showed how to use pseudorandom functions as *round functions*. What they showed was that depending on the amount of round functions used, one could achieve different levels of pseudorandomness. For example, a single round has pseudorandomness level 0 and so does a two-round Feistel cipher, but once we use three rounds, we achieve a pseudorandom permutation, and using four rounds gives us a super(!)pseudorandom permutation.

We will first give explicit definitions of pseudorandom permutations over arbitrary groups. The definitions are not explicitly needed for our proofs but are added for completeness. Second, we show that even for non-abelian groups, the one- and two-round Feistel ciphers are not pseudorandom. Finally, we answer an open problem posed by Patel, Ramzan, and Sundaram [PRS02] and show that for non-abelian groups, the three-round Feistel cipher is indeed not a super pseudorandom permutation.

1.1 Prior Work

Many Feistel cipher variants exist, with different relaxations on the round functions, see for example [NR99] and [PRS02], the latter of which considered Feistel ciphers over abelian groups among others. Vaudenay [Vau98] considered Feistel ciphers over groups other than the bit strings in order to protect them against differential analysis attacks by what he called decorrelation.

2 General Definitions

In the following, we work in the Random Oracle Model such that we may assume the existence of a random permutation oracle on group elements. We let $\mathcal{G}$ be the family of all finite groups, e.g. a group $G \in \mathcal{G}$ is a pair of the set G and operation $\cdot$ satisfying the group axioms.

On notation, we write $x \in_R X$ for an element chosen uniformly at random from a set X. In the following, we consider the positive integer λ to be the security parameter, specified in unary per convention. We assume that for each λ there exists a uniquely specified group $G(\lambda) = G_\lambda \in \mathcal{G}$ with size $|G_\lambda| \geq 2^\lambda$.

The following is taken *ad verbum* from [PRS02]. "The adversary $\mathcal{A}$ is modeled as a program for a Random Access Machine (RAM) that has black-box access to some number k of oracles, each of which computes some specified function. The adversary $\mathcal{A}$ will have a one-bit output. If $(f_1, \ldots, f_k)$ is a k-tuple of functions, then $A^{f_1,\ldots,f_k}$ denotes a k-oracle adversary who is given black-box oracle access to each of the functions $f_1, \ldots, f_k$. We define $\mathcal{A}$'s "running time" to be the number of time steps it takes plus the length of its description (to prevent one from embedding arbitrarily large lookup tables in $\mathcal{A}$'s description)." We define $A^{f_1,\ldots,f_k}(\lambda) = 1$ to denote that an adversary having access to k oracles outputs 1 when given the security parameter λ.

We can now use this to define pseudorandomness in all its needed flavours.

Definition 1. *Let $F_{m,n} : G_\lambda \times G_m \to G_n$, for $G_m, G_n \in \mathcal{G}$, be an efficient, keyed function. $F_{m,n}$ is a **pseudorandom function (PRF)** if for all probabilistic distinguishers $\mathcal{A}$, limited to only polynomially many queries to the function-oracle, there exists a negligible function $negl(\cdot)$, such that*

$$\left| \underset{k \in_R G_\lambda}{Pr} \left[\mathcal{A}^{F_{m,n}(k,\cdot)}(\lambda) = 1 \right] - \underset{\pi \in_R \mathfrak{F}_{G_m \to G_n}}{Pr} \left[\mathcal{A}^{\pi(\cdot)}(\lambda) = 1 \right] \right| \leq negl(\lambda),$$

where $\mathfrak{F}_{G_m \to G_n}$ is the set of functions from G_m to G_n.

If $F : G \times G \to G$ is a pseudorandom function, we say that it is a **pseudorandom function on** G.

Definition 2. *Let $P : G_\lambda \times G \to G$ be an efficient, keyed permutation. P is a **pseudorandom permutation (PRP)** if for all probabilistic distinguishers $\mathcal{A}$, limited to only polynomially many queries to the permutation-oracle, there exists a negligible function $negl(\cdot)$, such that*

$$\left| \underset{k \in_R G_\lambda}{Pr} \left[\mathcal{A}^{P(k,\cdot)}(\lambda) = 1 \right] - \underset{\pi \in_R \mathfrak{P}_{G \to G}}{Pr} \left[\mathcal{A}^{\pi(\cdot)}(\lambda) = 1 \right] \right| \leq negl(\lambda),$$

where $\mathfrak{P}_{G \to G}$ is the set of permutations on G.

Definition 3. *Let $P : G_\lambda \times G \to G$ be an efficient, keyed permutation. P is said to be a **super pseudorandom permutation (SPRP)** if for all probabilistic distinguishers $\mathcal{A}$, limited to only polynomially many queries to the permutation- and inverse permutation-oracles, there exists a negligible function $negl(\cdot)$, such that*

$$\left| \underset{k \in_R G_\lambda}{Pr} \left[\mathcal{A}^{P(k,\cdot),P^{-1}(k,\cdot)}(\lambda) = 1 \right] - \underset{\pi \in_R \mathfrak{P}_{G \to G}}{Pr} \left[\mathcal{A}^{\pi(\cdot),\pi^{-1}(\cdot)}(\lambda) = 1 \right] \right| \leq negl(\lambda),$$

where $\mathfrak{P}_{G \to G}$ is the set of permutations on G.

A (super) pseudorandom permutation $P : G \times G \to G$ is said to be a **(super) pseudorandom permutation on** G.

3 Feistel Ciphers

We now consider the Feistel cipher over arbitrary groups, which we will call the Group Feistel cipher. The following is a compliment to [PRS02] who treat the Group Feistel cipher construction with great detail. Our main accomplishment in this section is the settling of the open problem posed by them.

3.1 Definitions

We define a Feistel cipher over a group $(G, \cdot)$ as a series of round functions on elements of $G \times G = G^2$.

Definition 4. *Given an efficiently computable but not necessarily invertible function $f : G \to G$, called a* ***round function****, we define the* ***1-round Group Feistel cipher*** *$\mathcal{F}_f$ to be*

$$\begin{aligned} \mathcal{F}_f : G \times G &\longrightarrow G \times G, \\ (x, y) &\longmapsto (y, x \cdot f(y)). \end{aligned}$$

In the case where we have multiple rounds, we index the round functions as f_i, and denote the ***r-round Group Feistel cipher*** *by $\mathcal{F}_{f_1,\dots,f_r}$. We concurrently denote the input to the i'th round by (L_{i-1}, R_{i-1}) and having the output $(L_i, R_i) = (R_{i-1}, L_{i-1} \cdot f_i(R_{i-1}))$, where L_i and R_i respectively denote the left and right parts of the i'th output.*

Note that if (L_i, R_i) is the i'th round output, we may invert the i'th round by setting $R_{i-1} := L_i$ and then computing $L_{i-1} := R_i \cdot (f_i(R_{i-1}))^{-1}$ to get (L_{i-1}, R_{i-1}). As this holds for all rounds, regardless of the invertibility of the round functions, we get that an r-round Feistel cipher is invertible for all r.

Let $F : G_\lambda \times G \to G$ be a pseudorandom function. We define the keyed permutation $F^{(r)}$ as

$$F^{(r)}_{k_1,\dots,k_r}(x, y) \stackrel{\text{def}}{=} \mathcal{F}_{F_{k_1},\dots,F_{k_r}}(x, y).$$

We sometimes index the keys as $1, 2, \dots, r$, or omit the key index entirely.

3.2 Results

For completeness, we show some of the preliminary results for Group Feistel ciphers, not considered in [PRS02].

We first note that $F^{(1)}$ is *not* a pseudorandom permutation as

$$F^{(1)}_{k_1}(L_0, R_0) = (L_1, R_1) = (R_0, L_0 \cdot F_{k_1}(R_0)),$$

such that any distinguisher $\mathcal{A}$ need only compare R_0 to L_1.

Also $F^{(2)}$ is *not* a pseudorandom permutation: Consider a pseudorandom function F on G. Pick $k_1, k_2 \in_R G_\lambda$. Distinguisher $\mathcal{A}$ sets $(L_0, R_0) = (1, g)$ for some $g \in G$, where 1 is the identity element of G, then queries (L_0, R_0) to its oracle and receives,

$$L_2 = L_0 \cdot F_{k_1}(R_0) = F_{k_1}(g) \text{ and } R_2 = R_0 \cdot F_{k_2}(L_0 \cdot F_{k_1}(R_0)) = g \cdot F_{k_2}(F_{k_1}(g)).$$

On its second query, the distinguisher $\mathcal{A}$ lets $L'_0 \in G \setminus \{1\}$ but $R'_0 = g = R_0$, such that it receives

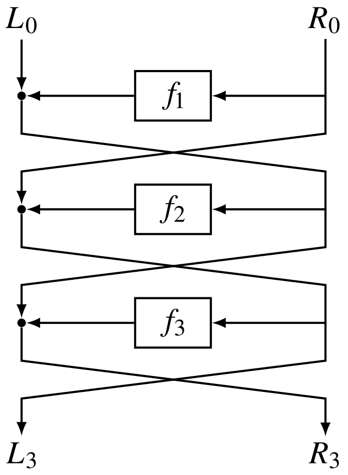

Figure 1: 3-round Group Feistel cipher.

$$L_2' = L_0' \cdot F_{k_1}(R_0) = L_0' \cdot F_{k_1}(g) \text{ and } R_2' = g \cdot F_{k_2}(L_0' \cdot F_{k_1}(g)).$$

As $\mathcal{A}$ may find the inverse to elements in G, $\mathcal{A}$ acquires $L_2^{-1} = (F_{k_1}(g))^{-1}$, and by so doing, may compute $L_2' \cdot (F_{k_1}(g))^{-1} = L_0'$. If $F^{(2)}$ were random, this would only occur negligibly many times, while $\mathcal{A}$ may query its permutation-oracle polynomially many times such that if L_0 is retrieved non-negligibly many times out of the queries, $\mathcal{A}$ is able to distinguish between a random permutation and $F^{(2)}$ with non-negligible probability.

As one would expect, the 3-round Group Feistel cipher (see Figure 1) is indeed a pseudorandom permutation.

Theorem 5. *If F is a pseudorandom function on G, then $F^{(3)}$ is a pseudorandom permutation on G.*

The proof of this proposition can be generalized from the proof given in Katz and Lindell [KL15] of the analogous result over bit-strings with XOR, with no difficulties. We therefore omit it here.

Among the considerations in [PRS02], they showed that the 3-round Feistel cipher over abelian groups was not super pseudorandom, but left as an open problem a proof over non-abelian groups. We present such a proof now.

Proposition 6. *The* 3*-round Group Feistel cipher is not super pseudorandom.*

Proof. The proof is a counter-example using the following procedure:

1. Choose two oracle-query pairs in $G \times G$: (L_0, R_0) and (L_0', R_0) where $L_0 \neq L_0'$.

2. Query the encryption oracle to get (L_3, R_3) and (L_3', R_3').

3. Query $(L_3'', R_3'') = (L_3', L_0 \cdot (L_0')^{-1} \cdot R_3')$ to the decryption oracle.

4. If $R_0'' = L_3' \cdot (L_3)^{-1} \cdot R_0$, guess that the oracle is $F^{(3)}$, else guess random.

For $F^{(3)}$, this algorithm succeeds with probability 1. For a random permutation, this algorithm succeeds negligibly often. □ □

For super pseudorandomness of the 4-round Group Feistel cipher, we refer the reader to [PRS02]. In the paper, they show a strong result using certain hash functions as round functions, from which the following is a corollary.

Corollary 7. *Let G be a group, with characteristic other than 2, and let $f, g : G_\lambda \times G \to G$ be pseudorandom functions. Then, for any adversary $\mathcal{A}$ with polynomially many queries to its E/D-oracles, the family $\mathcal{P}$ of permutations on $G \times G$ consisting of permutations of the form $F^{(4)} = \mathcal{F}_{g,f,f,g}$ are indistinguishable from random, i.e. super pseudorandom permutations (SPRPs).*

4 Conclusion

We generalized the Feistel cipher to work over arbitrary groups and proved that classical results pertain to non-abelian groups.

References

[Fei73] Horst Feistel. Cryptography and computer privacy. *j-SCI-AMER*, 228(5):15–23, may 1973.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792–807, August 1986.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, March 1999.

[KL15] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. CRC Press, 2 edition, 2015.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[NR99] Moni Naor and Omer Reingold. On the construction of pseudo-random permutations: Luby-rackoff revisited. *Journal of Cryptology*, 12:29–66, 1999. Preliminary version in: *Proc. STOC 97*.

[PRS02] Sarvar Patel, Zulfikar Ramzan, and Ganapathy S. Sundaram. Luby-rackoff ciphers: Why XOR is not so exclusive. In *Selected Areas in Cryptography, 9th Annual International Workshop, SAC 2002, St. John's, Newfoundland, Canada, August 15-16, 2002. Revised Papers*, pages 271–290, 2002.

[Vau98] Serge Vaudenay. *Provable security for block ciphers by decorrelation*, pages 249–275. Springer Berlin Heidelberg, Berlin, Heidelberg, 1998.