A Filter Bank View of Block and Stream Ciphers

G. R. Blakley and A. Klappenecker

Department of Mathematics, Texas A&M University
College Station, TX, 77843-3368, USA
{blakley|andreask}@math.tamu.edu

Abstract

Vaidyanathan suggested the use of filter banks with coefficients in finite fields as stream ciphers. We show how to break those ciphers. A more general class of ciphers is introduced, which includes many well-known block ciphers, like DES, IDEA, etc. These ciphers are derived from filter banks over group rings.

1. Introduction

Multirate filter banks have been used in numerous signal and image processing applications. More recently, such filter banks have been defined for signals with coefficients in finite fields. Lossless compression seems to be a natural application. However, it turns out that the decomposition of the input signal with such a filter bank will increase the entropy in most cases, that is, the entropy of the output sequence will be higher than the entropy of the input sequence. In fact, the output of the channels can be downright confusing. Perhaps it was this property that prompted Vaidyanathan to suggest the use of such filter banks as stream ciphers [2], [3].

In the first part of the paper we show how to break the Vaidyanathan ciphers. In the following parts we show how to generalize and strengthen them.

2. Vaidyanathan Ciphers

Let $\mathbf{F}_q$ be a finite field with q elements. A message is represented by a Laurent polynomial $m(z)$ in $\mathbf{F}_q[z, z^{-1}]$. The following cipher was suggested by Vaidyanathan in [2], [3]. Take the message $m(z)$ and split it into n submessages $m_i(z)$, representing the original message by $m(z) = \sum_{i=0}^{n-1} m_i(z^n)z^i$. Encrypt the message vector $(m_0(z), \dots, m_{n-1}(z))^t$ by left multiplication with an invertible matrix $H(z) \in \mathrm{GL}_n(\mathbf{F}_q[z, z^{-1}])$. The resulting vector

$$(c_0(z), \dots, c_{n-1}(z))^t = H(z)(m_0(z), \dots, m_{n-1}(z))^t$$

is the ciphertext. We call this encryption method a Vaidyanathan cipher with n channels. The ciphertext can be decrypted by multiplication with the inverse $H(z)^{-1}$.

Remark: Vaidyanathan confined the key space to so-called paraunitary encryption matrices $H(z)$. Our choice can be interpreted as the larger set of all keys allowing decryption (of arbitrary plaintexts encrypted with this method).

Theorem 1: A chosen plaintext attack with n messages is sufficient to completely reveal the encryption key $H(z)$ of a Vaidyanathan cipher with n channels.

Proof: Take a complete set of coset representatives $k_1, \dots, k_n$ of $n\mathbf{Z}$ in $\mathbf{Z}$. The impulse responses of the messages $z^{k_1}, \dots, z^{k_n}$ completely reveal the key $H(z)$. □

Theorem 2: A known plaintext attack with $m \geq n$ message/ciphertext pairs is possible whenever the matrix of message vectors has rank n.

Proof: Suppose we are given $m \geq n$ message/ciphertext pairs. Write the message vectors as columns of a matrix $M \in \mathrm{Mat}_{n,m}(\mathbf{F}_q[z, z^{-1}])$ and the corresponding ciphertexts as columns of a matrix $C \in \mathrm{Mat}_{n,m}(\mathbf{F}_q[z, z^{-1}])$.

Since $\mathbf{F}_q[z, z^{-1}]$ is a Euclidean domain, the matrix M can be reduced by row and column operations to diagonal form. In other words, we can find invertible matrices D, E (products of elementary transvections, really) such that $DME = \mathrm{diag}(d_1, \dots, d_n, 0, \dots, 0) \in \mathrm{Mat}_{n,m}(\mathbf{F}_q[z, z^{-1}])$. Note that the d_i's are nonzero by assumption.

The encryption of the m messages may be described by $H(z)M = C$, hence we obtain $H(z)D^{-1}DME = CE$ as a consequence. Multiplying CE by $R = \mathrm{diag}(d_1^{-1}, \dots, d_n^{-1}) \in \mathrm{Mat}_{m,n}(\mathbf{F}_q(z))$ on the right, yields $H(z)D^{-1}$. Thus the secret key $H(z)$ is given by the product $CERD$. □

Remark: In most cases, it will be enough to have merely n different message/ciphertext pairs, for n generic vectors span a module of rank n.

Theorem 3: All Vaidyanathan ciphers with n channels generate the same set $\mathcal{C}$ of ciphertexts. In fact, any ciphertext can occur: $\mathcal{C} = \prod_{i=0}^{n-1} \mathbf{F}_q[z, z^{-1}]$.

This theorem suggests that a ciphertext-only attack is not possible. However, the secrecy depends heavily on the entropy of the plaintext. Namely, if the plaintext

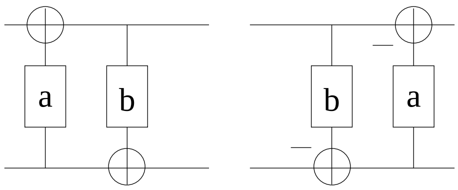

Fig. 1. A simple encryption network is shown on the left, the corresponding decryption network is shown on the right.

source is of low entropy (*e.g.*, a row in a binary fax image), then part of the key might be visible in the ciphertext.

3. Key Space

In Theorem 2, we exploited the fact that the ring $\mathbf{F}_q[z, z^{-1}]$ is a Euclidean domain. More precisely, we used the fact that a matrix of rank n can be reduced to a diagonal form by elementary row and column operations. Applying this procedure to the encryption matrix shows that $H(z)$ factors into a product of elementary transvections[1] and a diagonal matrix in $\mathrm{GL}_n(\mathbf{F}_q[z, z^{-1}])$. Thus, each Vaidyanathan cipher can be implemented by a network of convolution operations.

It is remarkable that the elementary transvections translate into operations which resemble the confusion steps in classical block ciphers. For example, the following encryption matrix of a two-channel cipher

$$H(z) = \begin{pmatrix} 1 & 0 \\ b(z) & 1 \end{pmatrix} \begin{pmatrix} 1 & a(z) \\ 0 & 1 \end{pmatrix}$$

can be implemented as shown in Fig. 1.

An encryption by such a network of filter operations has some nice features, namely, the decryption is done by running the network backwards and changing the sign of each filter output.

A simple, but crucial, observation is that each convolution operation in such a filter network can be replaced by essentially any nonlinear function $\mathbf{F}_q[z, z^{-1}] \to \mathbf{F}_q[z, z^{-1}]$. Since the argument is left unchanged in each step, the decryption is again done by running the network backwards and changing the sign of each nonlinear function.

The nonlinear versions of these ciphers are no longer vulnerable to the attacks described in the previous section. However, a few arbitrarily selected nonlinear functions will not ensure that one obtains a strong cipher. A careful analysis is required in any case.

Remark: Sweldens [1] introduced the idea of using nonlinear ladder or lifting steps for real-valued signals. This technique from wavelet analysis is basically the same as the one used here.

[1] Recall that an elementary transvection differs from the identity matrix in at most one off-diagonal entry.

4. From Stream to Block Ciphers

The Vaidyanathan ciphers are expanding, in the sense that the ciphertext is in general longer than the plaintext. This can be avoided by periodizing the cipher, that is, by replacing all 'linear' convolutions by cyclic convolutions of plaintext length. In other words, the calculations are done in the truncated polynomial ring $\mathbf{F}_q[z]/\langle 1 - z^K \rangle$ instead of $\mathbf{F}_q[z, z^{-1}]$.

We generalize Vaidyanathan ciphers to group rings in this section. This allows us to deal with nonexpanding ciphers, since $\mathbf{F}_q[z]/\langle 1 - z^K \rangle$ is isomorphic to $\mathbf{F}_q[\mathbf{Z}/K\mathbf{Z}]$. However, we do not confine ourselves to the case of a cyclic group. We allow a group ring $R[G]$ instead, where R is a finite ring, and G is a group. We will assume that G contains a normal subgroup N of finite index $n = [G\!:\!N]$ in G.

We start again with linear ciphers which basically work in the same way as the ciphers described in Section 2, and then derive the corresponding nonlinear variants.

Let t_i, $0 \leq i < n$, be a complete set of coset representatives of N in G. Take a message $m \in \sum_{g \in G} s_g g$ and split it into n submessages $m_i = \sum_{h \in N} s_{t_i h} h$, representing the original message by

$$m = \sum_{i=0}^{n-1} t_i m_i = \sum_{i=0}^{n-1} \sum_{h \in N} s_{t_i h}\, t_i h.$$

Encrypt the message vector $(m_1, \ldots, m_{n-1})^t$ by left multiplication with an invertible matrix $H \in \mathrm{GL}_n(R[N])$. The resulting vector

$$(c_0, \ldots, c_{n-1})^t = H\, (m_0, \ldots, m_{n-1})^t$$

is the ciphertext.

The more general linear ciphers have the same flaw as the Vaidyanathan ciphers. For example, a chosen plaintext attack with the coset representatives $t_0, \ldots, t_{n-1}$ as messages will again reveal all components of the encryption matrix H. We need to derive nonlinear ciphers to make this kind of attack more difficult.

If N is a finite group, then it is easy to see that every matrix in $\mathrm{GL}_n(R[N])$ can be factored into a product of elementary transvections and diagonal matrices. Indeed, $R[N]$ is an Artinian ring, since it is finite, and hence is a generalized Euclidean ring. The transvections give a network of convolutions, and we may as well replace these convolution operations by some nonlinear functions $R[N] \to R[N]$. We give an example in the next section.

5. Block Ciphers

If the group G is finite, then we can choose N to be the trivial subgroup $N = 1$. We obtain a block cipher in this case. In the linear case, one implements a network of operations which realizes a left multiplication by a matrix in $\mathrm{GL}_n(R[1]) \cong \mathrm{GL}_n(R)$.

At this point it might be instructive to have a look at a few examples. We start with a linear block cipher.

Linear Cipher. Take the group G with two elements $G = \mathbf{Z}/2\mathbf{Z}$ and the ring $R = \mathbf{F}_2^4$. The data type $R[G]$ describes bit vectors of 8 bits length. The input message is decomposed into two subwords of length 4, corresponding to the decomposition of $R[G]$ according to the cosets of the normal subgroup $N = 1$.

An elementary transvection operates in this case simply by adding certain bits in one channel to the same bit positions in the other channel (addition in $\mathbf{F}_2$ can be realized by an `xor` operation). For example, the transvection

$$\begin{pmatrix} (1,1,1,1) & (1,0,0,1) \\ (0,0,0,0) & (1,1,1,1) \end{pmatrix}$$

adds the least and the most significant bit of one channel to the corresponding bits in the other.

The elementary transvections simply do not provide enough diffusion and confusion. For example, no matter how many transvection are applied, if the most significant bits are 0 in both channels, then the most significant output bits will also be 0 in both channels.

DES. Consider the ring $R = \mathbf{F}_2^{32}$, and the group $G = \mathbf{Z}/2\mathbf{Z}$. Let $N = 1$, then a 64 bit message block in $\mathbf{R}[\mathbf{G}]$ is split into two subwords of 32 bits. One channel is used as an argument to a nonlinear function f_k and the result of this function is added (in R) to the other channel. This kind of operation is repeated sixteen times, alternating the input and output channels. The basic structure is similar to the preceding example. One can choose from a certain set of nonlinear functions $f_k : R \mapsto R$ by selecting a key k.

Remark: We observe that for the nonlinear version only the operations from the additive group $(R, +)$ are indispensable, since the multiplication operations might be replaced by other operations. In fact, one might as well replace $(R, +)$ by a finite group (or a quasi-group).

6. Conclusions

A further method to enhance confusion is to switch from one ring structure to another (or, following the preceding remark, from one quasi-group to another). For example, the IDEA cipher switches between three different groups. One can generate rather strong ciphers by concatenating simple filter bank ciphers and switching between different rings or quasi-groups. In should be emphasized, however, that only a judicious choice of nonlinearities and switching operations will lead to a strong filter bank cipher. A careful cryptanalysis is necessary in any case.

References

[1] I. Daubechies and W. Sweldens. Factoring wavelet transforms into lifting steps. *J. Fourier Anal. Appl.*, 4(3):245–267, 1998.

[2] S.-M. Phoong and P. P. Vaidyanathan. Paraunitary filter banks over finite fields. *IEEE Trans. on Signal Processing*, 45(6):1443–1457, 1997.

[3] P. Vaidyanathan. Unitary and paraunitary systems in finite fields. In *Proc. 1990 IEEE Int. Symp. on Circuits and Systems*, pages 1189–1192. IEEE, 1990.