Research Article

Information Leakage of VGF2 Structure

Ting Cui, Chen-hui Jin, and Ke-feng Huang

Information Science and Technology Institute, Zhengzhou 450000, China

Correspondence should be addressed to Ting Cui; cuiting_1209@hotmail.com

Received 9 January 2013; Accepted 5 April 2013

Academic Editor: Kwok-Wo Wong

Copyright © 2013 Ting Cui et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The block cipher VGF2 was designed at Inscrypt 2009. It was based on a new variant of generalized Feistel structure. By checking the property of the linear permutation, we find a full round differential in VGF2 with probability 1. Since this differential cannot distinguish the correct unknown key from the wrong keys, we fail in launching a key-recovery attack on this structure. However, we may guess half part of the plaintext without calculating the key. And we notice that this weakness may cause insecurity in some special environments.

1. Introduction

The architecture is one of the most important parts of block ciphers. It will directly affect the implementation performance and the choice of round number. Architectures of block ciphers could be roughly classified by SP structure [1] and Feistel family structure [2, 3]. The SP structure can provide a fast diffusion, but usually its decryption and encryption processes cannot be similar. Feistel family structures is another important structure, and it provides flexibility in the design of round function and decryption-encryption similarity; however, since only part of the input data goes through the round function in each round, these structures need more rounds to achieve enough diffusion.

Reference [4] proposed a new block cipher called VGF2. Its architecture can be considered as an extension of combining the SPN structure and generalized Feistel network together. It keeps the advantages of both SPN structure and the generalized Feistel network. It can achieve full diffusion very quickly, and decryption-encryption processes of this structure are similar.

In the design of VGF2, the original idea to achieve better diffusion is to use an involutory transformation with good branch number to replace the switch transformation. In [4], security levels of the structure against many cryptanalysis such as differential, linear, impossible differential, and integral cryptanalysis are also estimated.

In this paper, we find some information leakage in VGF2 structure. For arbitrary rounds VGF2 structure, we obtain two differentials with probability 1. Since these differentials cannot distinguish the correct key from the wrong keys, we fail in launching a key-recovery attack on this structure. However, we may guess half part of the plaintext without calculating the key.

The rest of this paper is organized as follows. Section 2 provides a description of VGF2, Section 3 presents the differential properties of VGF2 structure, and Section 4 introduces the information leakage of VGF2 cipher. As an application, Section 5 launches an attack on VGF2-based CMAC whose underlying block cipher is VGF2; in this attack, we can find a fake “familiar” message within 2^{64} CMAC operations, and the successful rate reaches 0.393. In Section 6, we conclude this paper.

2. Description of VGF2 Structure

Throughout this paper, $\oplus$ denotes the bitwise XOR and $+$ denotes the addition over real number space.

Now we will give a brief description of VGF2 structure.

All the states in VGF2 are split into 4 subblocks of equal size, and then the input and output blocks of each round can be denoted as $X = (X_0, X_1, X_2, X_3)$, and $Y = (Y_0, Y_1, Y_2, Y_3)$ respectively. For the sake of convenience, we will introduce two transformations as follows:

FIGURE 1: One round of VGF2 structure.

(i) R layer: $R(X_0, X_1, X_2, X_3) = (Z_0, Z_1, Z_2, Z_3) = (X_0, F_k(X_0) \oplus X_1, X_2, F_k(X_2) \oplus X_3)$, where F_k is the round function;

(ii) Q layer:

$$\begin{aligned} Q(Z_0, Z_1, Z_2, Z_3) &= \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} \\ &= Q_{4 \times 4} \cdot \begin{pmatrix} Z_0 \\ Z_1 \\ Z_2 \\ Z_3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} Z_0 \\ Z_1 \\ Z_2 \\ Z_3 \end{pmatrix}. \end{aligned} \quad (1)$$

One round VGF2 structure is composed of two layers (see Figure 1); that is,

$$\text{round}_{\text{VGF2}}(X_0, X_1, X_2, X_3) = Q \circ R(X_0, X_1, X_2, X_3). \quad (2)$$

3. Differential Properties of VGF2 Structure

In this section, we will introduce the differential properties of VGF2 structure.

Lemma 1. Let $R(X_0, X_1, X_2, X_3) = (X_0, F(X_0) \oplus X_1, X_2, F(X_2) \oplus X_3)$, where F is a bijection. Then, both differentials are with probability 1 of the following:

- (1) $(\alpha, \beta, 0, \alpha) \rightarrow (\alpha, \gamma, 0, \alpha)$,
- (2) $(0, \alpha, \alpha, \beta) \rightarrow (0, \alpha, \alpha, \gamma)$.

Proof. Let (x_0, x_1, x_2, x_3) and $(x_0 \oplus \alpha, x_1 \oplus \beta, x_2, x_3 \oplus \alpha)$ be inputs of the R layer. Then, output differential of the R layer is calculated by

$$\begin{aligned} &R(x_0, x_1, x_2, x_3) \oplus R(x_0 \oplus \alpha, x_1 \oplus \beta, x_2, x_3 \oplus \alpha) \\ &= (x_0, F(x_0) \oplus x_1, x_2, F(x_2) \oplus x_3) \\ &\quad \oplus (x_0 \oplus \alpha, F(x_0 \oplus \alpha) \oplus x_1 \oplus \beta, x_2, F(x_2) \oplus x_3 \oplus \alpha) \\ &= (\alpha, F(x_0) \oplus F(x_0 \oplus \alpha) \oplus \beta, 0, \alpha). \end{aligned} \quad (3)$$

Assume that $F(x_0) \oplus F(x_0 \oplus \alpha) \oplus \beta = \gamma$, and we conclude that differential $(\alpha, \beta, 0, \alpha) \rightarrow (\alpha, \gamma, 0, \alpha)$ is with probability 1. The second differential can be obtained in a similar way. $\square$

It is well known that if $f(x)$ is a linear transformation over F_2^n , then $f(\Delta x \oplus x) \oplus f(x) = f(\Delta x)$. Base on this rule, we have.

Theorem 2. For the VGF2 structure, there exists 1-round differential whose probability is equal to 1 as follows:

- (1) $(a, b, 0, a) \rightarrow (0, c, c, d)$,
- (2) $(0, c, c, d) \rightarrow (a, b, 0, a)$.

Proof. Since 1-round VGF2 structure can be expressed by $Q \circ R$, by Lemma 1, we have $(a, b, 0, a) \xrightarrow{\text{1st R layer}} (a, e, 0, a)$ with probability 1; hence, the output of the first round is

$$Q \cdot \begin{pmatrix} a \\ e \\ 0 \\ a \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ e \\ 0 \\ a \end{pmatrix} = \begin{pmatrix} 0 \\ e \oplus a \\ e \oplus a \\ e \end{pmatrix}. \quad (4)$$

Let $e \oplus a = c$ and $e = d$, then we obtain this theorem. Similarly, we can prove the second case. $\square$

Obviously, we have the following.

Theorem 3. For the VGF2 structure, if $r \equiv 0 \pmod{2}$, then r -round differential $(x, y, 0, x) \xrightarrow{(Q \circ R)^r} (u, v, 0, u)$ and $(0, x, x, y) \xrightarrow{(Q \circ R)^r} (0, u, u, v)$ are both with probability 1. If $r \equiv 1 \pmod{2}$, then r -round differential $(x, y, 0, x) \xrightarrow{(Q \circ R)^r} (0, u, u, v)$ and $(0, x, x, y) \xrightarrow{(Q \circ R)^r} (u, v, 0, u)$ are both with probability 1.

4. Information Leakage of VGF2 Structure

Base on the VGF2 structure, [4] proposed a 16-round and 256-bit block cipher VGF2 with the last Q layer omitted.

Since traditional differential cryptanalysis [5] uses high-probability characteristics or differentials to distinguish the correct unknown keys from the wrong keys. When a correct key is used to decrypt the last few rounds of many pairs of ciphertexts, it is expected that the difference predicted

FIGURE 2: CMAC algorithm.

FIGURE 3: The CBC core.

by the differential appears frequently, while when a wrong key is used, the difference occurs less frequently. However, differentials detected in this paper expose equal probability under any key; thus, we cannot launch a differential attack on this structure. But we may still conclude the following observation.

Observation 1. For VGF2 cipher, if we get a plain/ciphertext pair (m_0, m_1, m_2, m_3) and (c_0, c_1, c_2, c_3) , then for any ciphertext in set $\{(c_0 \oplus u, v, c_2, c_3 \oplus u) : u, v \in F_{2^{64}}\}$, we can predict that the plaintext is in the set $\{(m_0, x \oplus m_1, x \oplus m_2, y) : x, y \in F_{2^{64}}\}$. When ciphertext is chosen from the set $\{(c_0, c_1 \oplus u, c_2 \oplus u, v) : u, v \in F_{2^{64}}\}$, we can affirm that the plaintext is from set $\{(x \oplus m_0, y, m_2, x \oplus m_0) : x, y \in F_{2^{64}}\}$.

This weakness may bring insecurity under some special environments, and in next section, we will provide an example.

5. An Example Attack on VGF2-Based CMAC

MAC functions based on block ciphers are of great practical significance. And it is a well-known method to generate a Message Authentication Code (MAC) based on a block cipher in CBC-like mode. In this section, we will attack VGF2-based CMAC [6], which is recommended by NIST. This way of implementing a block cipher is independent of the actual block cipher being used, and so we can restrict this mode of use on VGF2 cipher. The CMAC algorithm divides message P into $(P_1, \dots, P_{n-1}, P_n^*)$, where each P_i is 256 bits length, and if the length of P_n^* is 256 bit, then $P_n = k_1 \oplus P_n^*$; else, $P_n = k_2 \oplus (P_n^* \oplus 10^j)$, where $j = 256 \times n - (\text{length of message } P) - 1$ (see Figure 2).

Since the remaining part of CMAC does not affect the attack procedure, we just focus on the CBC core (see Figure 3). Our target is to fake a similar message of

$(P_1, \dots, P_{n-1}, P_n^*)$. In fact, the attack below can be extended to most CBC-like MACs.

Step 1. Choose any $1 \leq i < j \leq n - 1$, and replace P_i by $P'_i = P_i \oplus (x, y, 0, x)$, where x, y are randomly chosen from $\{0, 1\}^{64}$ and $(x, y) \neq (0, 0)$.

Step 2. If $j - i \equiv 0 \pmod{2}$, we replace P_j by $P'_j = P_j \oplus (u, v, 0, u)$; otherwise, replace P_j by $P'_j = P_j \oplus (0, u, u, v)$, where u, v are randomly chosen from $\{0, 1\}^{64} \setminus \{0\}$.

Step 3. Compute $\text{CMAC}(P_1, \dots, P'_i, \dots, P'_j, \dots, P_n^*)$; if

$$\text{CMAC}(P_1, \dots, P'_i, \dots, P'_j, \dots, P_n^*) = \text{CMAC}(P_1, \dots, P_n^*), \quad (5)$$

the program output $(P_1, \dots, P'_i, \dots, P'_j, \dots, P_n^*)$.

When we introduce a randomly chosen difference $(x, y, 0, x)$ in the i th block, then by Observation 1, we may conclude that for any integer $k \geq 0$, output difference of the $(i + 2k - 1)$ th and the $(i + 2k)$ th blocks are $(0, x', x', y')$ and $(x'', y'', 0, x'')$, respectively, where x', y', x'', y'' are randomly picked up from $\{0, 1\}^{64}$. Consider $j = (i + 2k)$ case; only when $P_j \oplus (u, v, 0, u) = P'_j = P_j \oplus C'_{j-1} = P_j \oplus (x'', y'', 0, x'')$, that is, $u = x''$ and $v = y''$, we can obtain a collision.

We choose 2^{64} pairs of $((x, y), (u, v))$. And the successful rate is calculated by the birthday paradox; that is,

$$\begin{aligned} 1 - \prod_{i=0}^{2^{64}-1} \frac{2^{128} - i}{2^{128}} &= 1 - \prod_{i=0}^{2^{64}-1} \left(1 - \frac{i}{2^{128}}\right) \\ &\approx 1 - e^{-2^{128}/2^{129}} \\ &= 1 - e^{-0.5} \\ &\approx 0.393. \end{aligned} \quad (6)$$

We can analyze $j = (i + 2k - 1)$ case similarly.

Since all but two of the original message blocks are reserved, the fake message may probably be a meaningful message. And this may increase the risk of CMAC.

6. Conclusion

In this paper, we find two differentials in VGF2 structure whose probability is 1. Since these differentials cannot distinguish the correct key from wrong ones, we failed in launching a key-recovery attack on VGF2 structure. However, this property causes a significant information leakage; it allows us to obtain half part of the plaintext without calculating the key, and this may lead to some weakness in special environments.

In spite of the weakness presented in this paper, VGF2 structure retains some attractive features such as high diffusion and similarity in both decryption and encryption processes. And we believe that all these good features are caused by properties of matrix Q ; since its branch number reaches 4 [4], the whole structure can provide high diffusion, and also the involutory choice of matrix Q ensures the structure involutory. However, the binary matrix is not a good choice, which makes our attacks succeed. This motivates us to explore the possibility of improving Q that retains all the good properties of the VGF2 structure and yet is secure against our attacks. The best beneficial way to achieve this goal is to propose a new nonbinary matrix Q , which can retain both *large branch number* and *involution*, for example, involutory MDS matrix. Then, the proof will be invalid for this case.

Acknowledgment

The work in this paper is supported by the Natural Science Foundation of China (Grant no. 61272488, 61272041, and 61202491).

References

- [1] J. Daemen and V. Rijmen, *The Design of Rijndael—AES—The Advanced Encryption Standard*, Springer, Berlin, Germany, 2002.
- [2] Data Encryption Standard (DES), *Federal Information Processing Standards Publication FIPS-46-3*, National Bureau of Standards, 1999.
- [3] K. Nyberg, “Generalized Feistel networks,” in *Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT ’96)*, K.-C. Kim and T. Matsumoto, Eds., vol. 1163 of *Lecture Notes in Computer Science*, pp. 91–104, Springer, Kyongju, Korea, November 1996.
- [4] L. Zhang, W. Wu, and L. Zhang, “Proposition of two cipher structures,” in *Proceedings of the 5th China International Conference on Information Security and Cryptology (Inscrypt ’09)*, F. Bao, M. Yung, D. Lin, and J. Jing, Eds., vol. 6151 of *Lecture Notes in Computer Science*, pp. 215–229, Springer, Beijing, China, December 2009.
- [5] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” in *Proceedings of the 10th Annual International Cryptology Conference*, A. Menezes and S. A. Vanstone, Eds., vol. 537 of *Lecture Notes in Computer Science*, pp. 2–21, Springer, August 1990.
- [6] NIST, “Recommendation for block cipher modes of operation: the CMAC mode for authentication,” NIST Special Publication 800-38B, 2005.