An Observation on the Key Schedule of Twofish

Fauzan Mirza* Sean Murphy

Information Security Group, Royal Holloway,
University of London, Egham, Surrey TW20 0EX, U.K.

January 26, 1999

Abstract

The 16-byte block cipher Twofish was proposed as a candidate for the Advanced Encryption Standard (AES). This paper notes the following two properties of the Twofish key schedule. Firstly, there is a non-uniform distribution of 16-byte whitening subkeys. Secondly, in a reduced (fixed Feistel round function) Twofish with an 8-byte key, there is a non-uniform distribution of any 8-byte round subkey. An example of two distinct 8-byte keys giving the same round subkey is given.

1 Brief Description of Twofish

Twofish is a block cipher on 16-byte blocks under the action of a 16, 24 or 32-byte key [1]. For simplicity, we consider the version with a 16-byte key. Twofish has a Feistel-type design. Suppose we have a 16-byte plaintext $P = (P_L, P_R)$ and a 16-byte key $K = (K_L, K_R)$ considered as row vectors. Let $\mathbb{F} = GF(2^8)$ be the finite field defined by the primitive polynomial $x^8 + x^6 + x^3 + x^2 + 1$.

Twofish uses an invertible round function

$$g_{S_0,S_1} : \mathbb{F}^4 \times \mathbb{F}^4 \to \mathbb{F}^4 \times \mathbb{F}^4,$$

parameterised by two $\mathbb{F}^4$ quantities $S_0 = K_L \cdot RS^\mathsf{T}$ and $S_1 = K_R \cdot RS^\mathsf{T}$, where $RS = (T^\mathsf{T}|(T^\mathsf{T})^2)$ is a 4×8 matrix and the matrix T is given by

$$T = \begin{pmatrix} \texttt{01} & \texttt{A4} & \texttt{02} & \texttt{A4} \\ \texttt{A4} & \texttt{56} & \texttt{A1} & \texttt{55} \\ \texttt{55} & \texttt{82} & \texttt{FC} & \texttt{87} \\ \texttt{87} & \texttt{F3} & \texttt{C1} & \texttt{5A} \end{pmatrix}.$$

*This author is supported by an EPSRC award and completed part of the work whilst visiting the Department of Informatics, University of Bergen, Norway.

If $K_L = (W, X)$ and $K_R = (Y, Z)$, we have

$$\begin{aligned} S_0 &= K_L \cdot RS^{\mathsf{T}} \\ &= (W, X)\left(\frac{T}{T^2}\right) \\ &= W \cdot T \oplus X \cdot T^2 \\ &= (W \oplus X \cdot T) \cdot T \end{aligned}$$

Thus,

$$\begin{aligned} W &= X \cdot T \oplus S_0 \cdot T^{-1} &\Rightarrow\quad K_L &= (X \cdot T \oplus S_0 \cdot T^{-1}, X) \\ Y &= Z \cdot T \oplus S_1 \cdot T^{-1} &\Rightarrow\quad K_R &= (Z \cdot T \oplus S_1 \cdot T^{-1}, Z). \end{aligned}$$

The 4-byte round subkeys K_i ($i = 0, \cdots, 39$) are defined by a key scheduling function

$$h^{(i)} : \mathbb{F}^8 \times \mathbb{F}^8 \to \mathbb{F}^4 \times \mathbb{F}^4 \qquad (i = 0, \cdots, 19),$$

so we have $(K_{2i}, K_{2i+1}) = h^{(i)}(K_L, K_R)$ for $i = 0, \cdots, 19$.

The functions $q_0, q_1 : \mathbb{Z}_{2^8} \to \mathbb{F}$ are (key-independent) bijective S-boxes with one byte inputs. These give constants $A_i, B_i \in \mathbb{F}^4$ $(i = 0, \cdots, 19)$ defined by

$$\begin{aligned} A_i &= (q_0(2i), q_1(2i), q_0(2i), q_1(2i)) \\ B_i &= (q_0(2i+1), q_1(2i+1), q_0(2i+1), q_1(2i+1)). \end{aligned}$$

These constants are used to define

$$\begin{aligned} C_i &= Q(A_i \oplus Y) \oplus W \\ D_i &= Q(B_i \oplus Z) \oplus X \\ (K_{2i}, K_{2i+1}) &= H(C_i, D_i), \end{aligned}$$

where Q and H are permutations of $\mathbb{F}^4$ and $\mathbb{F}^8$ respectively. Note that $h^{(i)}$ has the property that

$$h^{(i)}(x, y) \neq h^{(j)}(x, y), \qquad \text{for any } x, y \in \mathbb{F}^8, \quad \text{and } i \neq j.$$

Suppose we define $+$ to denote a pair of modulo 2^{32} additions, and $\theta = (e, \rho)$ and $\theta' = (\rho^{-1}, e)$, where e is the identity transformation on 32 bits and ρ is a left rotation by one place of 32 bits. A Twofish encryption of $P = (P_L, P_R)$ under key $K = (K_L, K_R)$ to give ciphertext $C = (C_L, C_R)$ is then given by

$$\begin{aligned} L_0 &= P_L \oplus (K_0, K_1) \\ R_0 &= P_R \oplus (K_2, K_3) \\ L_{i+1} &= (R_i\theta \oplus (g_{S_0,S_1}(L_i) + (K_{2i+8}, K_{2i+9})))\theta' && [i = 0, \cdots, 15] \\ R_{i+1} &= L_i && [i = 0, \cdots, 15] \\ C_L &= R_{16} \oplus (K_4, K_5) \\ C_R &= R_{16} \oplus (K_6, K_7). \end{aligned}$$

2 Whitening Subkeys

The subkeys (K_0, K_1, K_2, K_3) and (K_4, K_5, K_6, K_7) XORed before the first and after the last round are known as *whitening subkeys*. They have been used in many block ciphers, for example FEAL [3] and DES-X [2]. For a 16-byte Twofish key there are less than 2^{128} possibilities for the pre-whitening subkeys (K_0, K_1, K_2, K_3). For example, $(0, 0, 0, 0)$ is not a valid pre-whitening subkey, for if it were then $h^{(0)}(x, y) = h^{(1)}(x, y)$ for some (x, y). The number of times a 16-byte pre-whitening key occurs would seem to follow a Poisson distribution with mean 1, so only $1 - e^{-1} = 0.632$ of 4-byte values occur as pre-whitening subkeys. A similar argument applies to post-whitening keys.

3 Reduced Twofish with (S_0, S_1) fixed

Consider a reduced version of Twofish in which S_0 and S_1 are fixed. Then K_L and K_R are uniquely defined by their values on four bytes respectively. We can thus define an 8-byte key $\hat{K} = (X, Z)$ and key scheduling functions

$$H^{(i)}_{(S_0,S_1)} : \mathbb{F}^4 \times \mathbb{F}^4 \to \mathbb{F}^4 \times \mathbb{F}^4 \qquad i = 0, \cdots, 19,$$

given by

$$H^{(i)}_{(S_0,S_1)}(X, Z) = h^{(i)}((X \cdot T \oplus S_0 \cdot T^{-1}, X), (Z \cdot T \oplus S_1 \cdot T^{-1}, Z)).$$

Reduced Twofish is a Feistel cipher with a known fixed invertible round function

$$g_{S_0,S_1} : \mathbb{F}^4 \times \mathbb{F}^4 \to \mathbb{F}^4 \times \mathbb{F}^4,$$

on 16-byte blocks under an 8-byte key.

Without loss of generality, we now consider the reduced Twofish in which $(S_0, S_1) = (0, 0)$. Thus $K_L = (W, X)$ and $K_R = (Y, Z)$ are elements of the kernel of RS and so $W = X \cdot T$ and $Y = Z \cdot T$.

We show how to find subkey collisions in reduced Twofish. We wish to find $((W', X'), (Y', Z'))$ such that

$$\begin{aligned} C_i &= Q(A_i \oplus Y) \oplus W &&= Q(A_i \oplus Y') \oplus W' \\ D_i &= Q(B_i \oplus Z) \oplus X &&= Q(B_i \oplus Z') \oplus X'. \end{aligned}$$

Using the kernel condition $W = X \cdot T$ etc, we have

$$\begin{aligned} X \cdot T \oplus X' \cdot T &= Q(A_i \oplus Z \cdot T) \oplus Q(A_i \oplus Z' \cdot T) \\ X \oplus X' &= Q(B_i \oplus Z) \oplus Q(B_i \oplus Z'). \end{aligned}$$

On applying T to the second equation we obtain

$$\begin{aligned} (X \oplus X') \cdot T &= Q(A_i \oplus Z \cdot T) \oplus Q(A_i \oplus Z' \cdot T) \\ (X \oplus X') \cdot T &= Q(B_i \oplus Z) \cdot T \oplus Q(B_i \oplus Z') \cdot T. \end{aligned}$$

Adding these two equations and re-arranging gives

$$Q(A_i \oplus Z \cdot T) \oplus Q(B_i \oplus Z) \cdot T = Q(A_i \oplus Z' \cdot T) \oplus Q(B_i \oplus Z') \cdot T.$$

Thus searching for subkey collisions is equivalent to finding collisions of the function $R_i : \mathbb{F}^4 \rightarrow \mathbb{F}^4$ defined by

$$R_i(Z) \quad = \quad Q(A_i \oplus Z \cdot T) \oplus Q(B_i \oplus Z) \cdot T.$$

This function behaves like a "random" function on $\mathbb{F}^4$, so we would expect to find a collision after about 2^{16} evaluations of R. For example, the pair of 8-byte reduced Twofish keys, with $(S_0, S_1) = (0, 0)$, defined by

$$\begin{aligned} (X, Z) &= (\texttt{00000000}, \texttt{000006F5}) \\ (X', Z') &= (\texttt{0015FB5C}, \texttt{000311C3}) \end{aligned}$$

cause $(K_8, K_9) = (\texttt{C82616C0}, \texttt{9FB7D001})$ by the Twofish key schedule.

The number of times an 8-byte round subkey (K_{2i}, K_{2i+1}) occurs would seem to follow a Poisson distribution with mean one, so only $1 - e^{-1} = 0.632$ of 8-byte values occur as round subkeys (K_{2i}, K_{2i+1}). This is inconsistent with the statement in Section 8.6 of [1] where it is claimed that guessing the key input (S_0, S_1) to the round function "*provides no information about the round subkeys* K_i".

The key scheduling of reduced Twofish thus means that an 8-byte round subkey (K_{2i}, K_{2i+1}) derived from an 8-byte key cannot take all possible values. This could speed up certain types of cryptanalysis.

4 Conclusion

The key scheduling of Twofish has two properties that are contrary to claims implicit in [1], and could potentially be exploited in any of the usual applications of a block cipher (e.g. hashing).

Twofish can be regarded as a collection of "reduced" Twofish encryption algorithms, each of which has its own Feistel round function and its own key schedule that is a non-uniform mapping to the round subkeys. The key to Twofish consists of two separate parts which have distinct functions. One part selects a reduced Twofish encryption algorithm from the collection. The other part is used as input to the unbalanced reduced Twofish key schedule. The use of a key which has two such separate parts offers the possibility of a divide-and-conquer attack of the key space.

References

[1] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-Bit Block Cipher". AES Submission, 15 June 1998.
http://csrc.nist.gov/encryption/aes/round1/AESAlgs/Twofish/twofish-doc.zip

[2] J. Kilian and P. Rogaway, "How to Protect DES against Exhaustive Search". In *Advances in Cryptology—Proceedings of CRYPTO '96*, pp267–278, Springer-Verlag, 1996.

[3] A. Shimuzu and S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL". In *Advances in Cryptology—Proceedings of EUROCRYPT '87*, pp267–278, Springer-Verlag, 1988.