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 15, 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. 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 $K = (K_L, K_R)$. 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 4-byte quantities $S_0 = RS \cdot K_L$ and $S_1 = RS \cdot K_R$, where RS is a 4×8 matrix given by

$$RS = \begin{pmatrix} \texttt{01} & \texttt{A4} & \texttt{55} & \texttt{87} & \texttt{5A} & \texttt{58} & \texttt{DB} & \texttt{9E} \\ \texttt{A4} & \texttt{56} & \texttt{82} & \texttt{F3} & \texttt{1E} & \texttt{C6} & \texttt{68} & \texttt{E5} \\ \texttt{02} & \texttt{A1} & \texttt{FC} & \texttt{C1} & \texttt{47} & \texttt{AE} & \texttt{3D} & \texttt{19} \\ \texttt{A4} & \texttt{55} & \texttt{87} & \texttt{5A} & \texttt{58} & \texttt{DB} & \texttt{9E} & \texttt{03} \end{pmatrix}.$$

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 $i = 0, \cdots, 19$.

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

The key scheduling function $h^{(i)}$ operates as follows. Let $A_i = (q_0(2i), q_1(2i), q_0(2i), q_1(2i))$ and $B_i = (q_0(2i+1), q_1(2i+1), q_0(2i+1), q_1(2i+1))$, where q_0 and q_1 are key-independent bijective S-boxes acting on one byte inputs. Then

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

where $(W, X) = K_L$, $(Y, Z) = K_R$, and 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]. It turns out that 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 the two halves of the key $K = (K_L, K_R)$ are constrained to lie in 4-byte $GF(2^8)$-subspaces defined by the pre-images of S_0 and S_1 respectively, so $K_L \in RS^{-1}(S_0)$ and $K_R \in RS^{-1}(S_1)$. The kernel of RS, N, is the row space of the matrix $(T|I)$, given by

$$(T|I) = \begin{pmatrix} \texttt{01} & \texttt{A4} & \texttt{02} & \texttt{A4} & \texttt{01} & \texttt{00} & \texttt{00} & \texttt{00} \\ \texttt{A4} & \texttt{56} & \texttt{A1} & \texttt{55} & \texttt{00} & \texttt{01} & \texttt{00} & \texttt{00} \\ \texttt{55} & \texttt{82} & \texttt{FC} & \texttt{87} & \texttt{00} & \texttt{00} & \texttt{01} & \texttt{00} \\ \texttt{87} & \texttt{F3} & \texttt{C1} & \texttt{5A} & \texttt{00} & \texttt{00} & \texttt{00} & \texttt{01} \end{pmatrix}.$$

Fixing (S_0, S_1) forces K_L and K_R to be in specific cosets of N. If K_L is in the kernel, so $K_L = (Y, Z) \in N$, then $Y = Z \cdot T$, so if K_L is in a coset of the kernel, say $K_L = (Y, Z) \in N + (Y^*, Z^*)$, then $Y = Z \cdot T + Y^* + Z^* \cdot T$. Thus if S_0 and S_1 are fixed, then K_L and K_R are uniquely defined by their values on four bytes. Using these transformations, we can 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, for any $(W^*, X^*, Y^*, Z^*) \in RS^{-1}(S_0, S_1)$,

$$H^{(i)}(X, Z) = h^{(i)}((X \cdot T \oplus W^* \oplus X^* \cdot T, X), (Z \cdot T \oplus Y^* \oplus Z^* \cdot T, Z)).$$

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, N, 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

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

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 $R_i : \mathbb{F}^4 \to \mathbb{F}^4$ defined by

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

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 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. Firstly, both the pre- and post-whitening subkeys of Twofish occur with a non-uniform distribution, which gives information about the key. Secondly, the round subkeys of every reduced version of Twofish (i.e., a version of Twofish with (S_0, S_1) fixed) occur with a non-uniform distribution, which gives information about the key. An attack on any reduced version of Twofish would have cryptographic consequences for the full version of Twofish (for example, the unbalanced key schedule described in reduced Twofish may aid an attacker in deriving collisions if Twofish is used in a Davies-Meyer hash).

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://www.counterpane.com/twofish-paper.html*

[2] J. Kilian and P. Rogaway. How to Protect DES against Exhaustive Search, *CRYPTO '96*, pp267–278, Springer-Verlag, 1996.

[3] A. Shimuzu and S. Miyaguchi. Fast Data Encipherment Algorithm FEAL, *EUROCRYPT '87*, pp267–278, Springer-Verlag, 1988.