The Key Separation of Twofish

Sean Murphy

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

March 15, 2000

Abstract

This paper considers the discussion of Whiting *et al* that the key separation of the AES candidate Twofish, noted by Mirza and Murphy at AES2, does not lead to cryptographic weaknesses. This paper shows that that this discussion is flawed and does not address the issue of Twofish key separation and cryptographic weaknesses.

Key Words: Cryptography, AES, Block Ciphers, Twofish, Key Separation.

1 Introduction

Twofish [1] was submitted as a candidate algorithm for the Advanced Encryption Standard (*AES*), and has subsequently been selected as one of the five finalists. Some observations about the structure of the key schedule of Twofish [2] were presented at the 2nd AES conference in Rome, March 1999. The observation that is of most interest to the cryptanalyst is the *key separation* property of Twofish.

We now explain the key separation property for the 128-bit key version of Twofish, though the property is general. The Twofish key is used to provide subkeys and a 64-bit S-Box parameter. We term a Twofish encryption in which the 64-bit S-Box parameter is fixed a *Reduced Twofish* encryption algorithm. The key schedule of Twofish means that each Reduced Twofish algorithm has a fixed structure with a 64-bit key, whose subkeys are introduced solely using group operations [2]. Thus the 128-bit Twofish key can be regarded as two separate halves (complementary subspaces) of 64 bits, the *selector* and *generator*. The 64-bit selector chooses one of the 2^{64} Reduced Twofish algorithms, and the 64-bit generator is the key for the 64-bit Reduced Twofish.

A key separation such as this of the key into two parts with independent functions always allows the possibility of a divide-and-conquer attack. If there is a cryptanalytic attack *of any type* for some or all of the 2^{64} Reduced Twofish encryption algorithms, then there is a divide-and-conquer attack on Twofish. Firstly, guess the selector, that is guess a Reduced Twofish algorithm. Secondly, use the cryptanalytic attack to find the Reduced Twofish key, that is find the generator. The extent of analysis particular to the Reduced Twofish algorithms is unclear.

An unusual property (with respect to other well-regarded block ciphers) of the Reduced Twofish algorithms is also noted in [2]. The 64-bit key of the Reduced Twofish algorithms is not mapped uniformly to the 64-bit round subkeys. *One* consequence of this property is that there is an additional small loss of key entropy (beyond the minumum) when a round subkey is given. This property of non–uniform subkeys is not intrinsically related to the key separation of Twofish.

2 Discussion of Key Separation

The Twofish Designers' comments on [2] are given in [3]. The discussion of the key separation is given in Sections 3.2 (*Implications*) and 4 (*Conclusions*). This discussion attempts to establish why the key separation gives no cryptographic weaknesses by comparing Twofish to DES. Without loss of generality, we consider this discussion in the case when a round subkey is guessed for DES and for Twofish. This discussion can be summarised in terms of the following properties and assertions (H is the entropy function).

- *Property* $P1$: $H(\text{Key}) - H(\text{Subkey})$ is large.
- *Property* $P2$: $H(\text{Key}) - H(\text{Subkey}) - H(\text{Key}|\text{Subkey})$ is very small.
- *Property* $P3$: Key Separation Property.
- *Assertion* $A0$: Property $P1$ is not a cryptographic weakness.
- *Assertion* $A1$: Property $P1$ is cryptographically weaker than Property $P2$.
- *Assertion* $A2$: Properties $P2$ and $P3$ are equivalent.
- *Assertion* $A3$: Property $P2$ is not a cryptographic weakness.
- *Assertion* $A4$: Property $P3$ is not a cryptographic weakness.

The logical structure of the discussion to establish that key separation does not give a cryptographic weakness is as follows.

$$\begin{gathered} A0 \text{ AND } A1 \text{ implies } A3 \\ A2 \text{ AND } A3 \text{ implies } A4 \\ \text{Therefore } A0 \text{ AND } A1 \text{ AND } A2 \text{ implies } A4 \end{gathered}$$

This attempt to establish that the key separation of Twofish gives no cryptographic weaknesses is flawed for the following three reasons.

- *Invalid Comparison.* Property $P1$ arises in the 2nd paragraph of Section 3.2, when the key entropy lost given a DES subkey is considered.

Property $P2$ arises in the 3rd paragraph, when only the additional entropy beyond that merely lost given a Twofish round subkey is considered. Properties $P2$ and $P1$ are considering quite different quantities, and they are clearly not comparable. Yet, in assertion $A1$, properties $P2$ and $P1$ are compared. *Assertion* $A1$ *is not justified.*

- *Non–Equivalence.* Properties $P2$ and $P3$ are not equivalent. It is easy to design a block cipher which is cryptographically weak because of a key separation but has no loss of entropy in the sense of property $P2$. *Assertion* $A2$ *is not justified.*

- *Fundamental Irrelevance.* This discussion about why the key separation does not lead to weaknesses of Twofish is based on entropy of a key given various subkeys. In any attack with minimal plaintext and ciphertext, the key entropy is zero. Finding the key is "merely" a computational problem. This discussion does not demonstrate that key separation cannot help solve this computational problem. This discussion is thus fundamentally irrelevent as to whether key separation is a weakness of Twofish.

3 Conclusions

The key separation of Twofish described in [2] may or may not be of use in the cryptanalysis of Twofish. However, the attempt to establish that the key separation leads to "no cryptographic weaknesses" given in [3] is based on unjustified assertions and is fundamentally irrelevent. Certainly, both the statement in the abstract that "it is *shown* that other block ciphers, notably DES and Triple DES, achieve far less uniform subkey distribution than Twofish over similarly constructed sets of keys", and the statement at the end of Section 3.2 that "it seems likely that any attack based on this approach [key separation] could probably be readily applied to DES and Triple DES" are unsustainable.

References

[1] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. *Twofish: A 128-Bit Block Cipher*, AES Submission, 1999. `http://www.counterpane.com/twofish-paper.html`,

[2] F. Mirza and S. Murphy *An Observation on the Key Schedule of Twofish*, Proceedings of the 2nd AES Conference, pp151-154, Rome, 1999. `http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm`

[3] D. Whiting, J. Kelsey, B. Schneier, D. Wagner, C. Hall, and N. Ferguson. *Further Observations on the Key Schedule of Twofish*, 1999. `http://www.counterpane.com/twofish-ks2.html`