Comments on Twofish as an AES Candidate

Bruce Schneier* John Kelsey† Doug Whiting‡ David Wagner§ Niels Ferguson¶

March 24, 2000

1 Introduction

In 1996, the National Institute of Standards and Technology initiated a program to choose an Advanced Encryption Standard (AES) to replace DES. Four years later, NIST is about to choose that standard. We, the authors of the Twofish algorithm, would like to express our continued support for Twofish.

2 Twofish

Twofish is our submission to the AES process. Since first proposing the algorithm in 1998, we have continued to perform extensive analysis of the cipher: both cryptanalysis and performance analysis. We believe that Twofish is the best AES candidate of the five finalist algorithms.

Security: Twofish was designed primarily with security in mind. To date the Twofish round function has proven to be the strongest round function of any of the finalists, with the best known attack being on 6 rounds of Twofish compared to at least 9 rounds for any of the other finalists.

Performance: Twofish is routinely one of the fastest AES candidates; it was designed to have good performance on a variety of hardware and software platforms, instead of being optimized for a single platform. Although Twofish is not the easiest algorithm to implement or optimise, it is amongst the fastest algorithms on virtually every platform when properly implemented.

Flexibility: Twofish is unique in its implementation flexibility. The algorithm can be optimized for bulk encryption, key agility, low gate count, high gate count, or any combination of factors. All of these implementations are completely interoperable.

More interesting than these individual measures is the security/performance ratio of Twofish. Looking at the five algorithms in this manner—normalizing to the largest number of rounds cryptanalyzed is a good metric—Twofish far surpasses the other four finalists.

3 Discussion

The AES process has worked even better than expected. Today we have five good algorithms, and any of the designs would make a good AES standard. (We would recommend increasing the number of rounds for RC6 from 20 to 32, and the number of rounds in Rijndael from 10/12/14 to 18, to get at least a 2x security

*Counterpane Internet Security, Inc., 3031 Tisch Way, 100 Plaza East, San Jose, CA 95128, USA; schneier@counterpane.com.
†Counterpane Internet Security, Inc. kelsey@counterpane.com.
‡Hi/fn, Inc., 5973 Avenida Encinas Suite 110, Carlsbad, CA 92008, USA; dwhiting@hifn.com.
§University of California Berkeley, Soda Hall, Berkeley, CA 94720, USA; daw@cs.berkeley.edu.
¶Counterpane Internet Security, Inc. niels@counterpane.com.

margin—number of rounds greater than the maximum number of rounds that can be cryptanalyzed—as recommended by Lars Knudsen.)

Two of the finalists, MARS and RC6, are not well-suited certain applications, most notably small-memory implementations (e.g., smart cards) and highly key-agile systems (e.g., IPsec). Any one of the other three algorithms—Rijndael (with the extra rounds), Serpent, or Twofish would make an *excellent* standard.

Of the five finalists, Twofish has the best speed/security-margin tradeoff, as well as the most flexibility. With security and speed being the most important criteria (certainly the most talked-about), we believe that Twofish is the best single finalist.

4 More Information

More information on Twofish can be found on the Twofish Web site, at `http://www.counterpane.com/twofish.html`.