Comment on Selecting the Ciphers for the AES Second Round

Eli Biham

Computer Science Department
Technion – Israel Institute of Technology
Haifa 32000, Israel
Email: biham@cs.technion.ac.il
WWW: http://www.cs.technion.ac.il/∼biham/

Abstract. In this comment the author writes his views on the selection of the AES second-round ciphers and proposes a smaller set of ciphers which should be considered for the second round.

1 Importance of the Various Criteria

The AES selected cipher will serve many decades as a worldwide standard. It is expected to secure financial transactions and other very valuable information. It will also secure privacy information which must be kept secure for many decades after encryption (or even for eternity).

As the AES selected cipher (which will be referred shortly as the AES) is expected to serve as a standard at least 30 years, and as most existing systems will not be immediately changed when a newer standard will be selected, it is expected that the AES will still be used in some systems even after 50–60 years. Therefore, information encrypted using systems developed in the lifetime of the AES will have to be kept secret even in the year Y2.1K (2100). We conclude that the cipher should be very secure and should be able to protect data for at least a century.

Therefore, the security of the AES should be the main criteria, and should not be underestimated. It is the best interest of the AES to have the most secure cipher.

The only criterion that may interfere with security is implementability. It is the best interest of the AES to make sure that the cipher is implementable on all expected platforms, including hardware, software, smartcards, etc.

Other criteria, including the speed on the various platforms, the code and memory sizes required for the implementations, should be taken to consideration only as fourth, fifth, etc., order criteria after

1. security,
2. security, and
3. implementability.

2 Confidence

The bottom line is confidence. In order for the cipher to be adopted and widely used there should be a high confidence in its design and security. There are several factors which affect confidence:

1. The designers' experience, and knowledge in the design and analysis of ciphers
2. The high level design, and the mixture of the used operations
3. The ability to analyze the cipher by known techniques
4. The probability that the particular cipher might lead to the design of new cryptanalysis techniques (this is good for the study of the theory of cryptanalysis, but bad for a standard cipher)
5. What is the margin of safety in terms of security that the designers put into the cipher
6. The already known cryptanalysis and evidence

3 Security and Number of Rounds

Security should be the major factor in selecting the AES. In the author's opinion the cipher should be designed very secure in a way that will give some hope that even new kinds of attacks will fail against the cipher, even if it will succeed much better than the known attacks. Therefore, large security margins are very important. The author believes that the number of rounds of the AES should be considerably larger (for example twice) than the current known kinds of attacks propose. As the cryptanalytic knowledge will advance, it is expected that new attacks are found, and some of them might attack a larger number of rounds than the currently known attacks. In such a case, if the cipher will not have sufficient security margins, somebody might use this attack. The consequences of such an improved attack can be between a bad press and a disaster. Both such consequences can easily be avoided (or their probability be reduced) by selecting a more secure cipher *now*, for example by adding rounds to the cipher.

4 Provable Security of Blockciphers

The designers of all (or almost all) candidates give evidence that standard cryptanalysis techniques are not useful against their cipher. In most cases the evidence consist of computing upper bounds on the probabilities p of characteristics and linear approximations, and conclude that the cipher cannot be analyzed by these types of analysis with less than $1/p$ chosen or known plaintexts and complexity.

This is the standard way of giving evidence for security of ciphers nowadays, but none of the designers claimed that this forms a full proof of security of their cipher, even when only differential and linear cryptanalysis are considered. Indeed, some differential and linear attacks can use differentials or linear hulls whose probability might be higher, but their existence is very difficult to find, and other attacks might use impossible differentials which use differentials with the lowest possible probability (zero) which is always smaller than any of the bounds p.

There are other kinds of attacks, taking into considerations other properties of ciphers, such as related-key attacks, Davies' attack on DES, partitioning attacks, and combinations of attacks such as differential-linear attacks.

Since the introduction of differential cryptanalysis, the research community is working on design techniques to ensure security against it. There were several attempts to prove security against differential cryptanalysis usually by means of bounding the maximal differential probability. However, many of the proposed provably secure ciphers were later broken by other techniques, sometimes by the original designers themselves. The search for provable security is still in progress, but it is not expected that a full proof of security of any cipher will be found in the next decades, as this proof is closely related to proving lower bounds of computational complexity, and to the problem of the relation of the classes P and NP.

Some designers decided to claim provable security of their cipher. Although they do not claim full proofs, but only proofs against several known kinds of attacks, their claims are too broad.

In fact, they actually bound the probabilities of characteristics as everybody do but using a new different technique. Their proof holds for restricted kinds of attacks, in particular those that require only a small amount of known of plaintexts, because their technique decorrelates a small number of encryptions. And in particular, there are example for ciphers that can be proven secure by the similar kinds of proofs that are totally insecure and have characteristics with high probabilities (e.g., probability 1). To summarize, their security proofs do not give more evidence on the security of the cipher than the evidence given by various other submitters.

5 Speed

The speed of the candidates on various platforms is studied to death, especially on platforms which will never be used in the lifetime of the AES standard. Therefore, the speed figures studied already by various parties are only approximations for the platforms on which AES will be used. Improvements in hardware chips might change the speed of various candidates considerably, for example by adding additional registers to processors, reducing the number of loads and stores currently required by many ciphers, or by adding very simple additional instructions to the processors.

Moreover, the original AES call required a cipher "with a strength equal to or better than that of Triple-DES and significantly improved efficiency". This can be interpreted as a cipher being at least twice faster than Triple-DES, i.e., about as fast as DES, or even slightly slower than DES, which is very secure and which has a high level of confidence not be broken in the next century. However, most AES candidates are actually faster than DES, and meet the speed requirements better than NIST had thought in advance. Between such ciphers, comparison by speed should only be a minor consideration.

6 Simplicity

Simplicity should be a bonus, but certainly ciphers that are far from being simple should not be selected.

Simplicity is a highly related to science. If we wish to have any kind of security proofs sometime in the future, we must have simple designs which can be studies scientifically. As simpler as the design of a cipher the more the probability that it can be studied scientifically, and its (hopefully good) properties will become known.

Moreover, complex ciphers (an extreme but not only example is HPC) will never be studied or analyzed, and even the designers of such ciphers cannot give sufficient evidence for their strengths or weaknesses.

Selection of too complex ciphers will also have a bad effect of the scientific community in this field, which always try to find simple design criteria and simple analyzable (secure) designs.

Finally, simplicity is a major reason why DES is mentioned in all the cryptographic textbooks, mentioned in classes, and influenced research in a wider field, even before most of the current knowledge about cryptanalysis and the strength of ciphers was (publicly) known. If AES is selected as a too complex cipher, it will not be mentioned in the books, and even when mentioned, nobody will show its details in classes. In the best case, lecturers will still teach DES in classes and say that there is some newer very complex cipher called AES. Alternatively, they will just teach something else. In both cases, the public and scientific interest in this field might be reduced significantly, as opposed to the current trend.

7 Multiple Ciphers?

I believe that there should be only one standard. NIST should decide on one standard in order to ensure that the standard is accepted and adopted as soon as possible. However, NIST can publish the choice of a backup cipher which will replace the standard in case it is broken or in case other circumstances (such as intellectual property problems) will prevent it from being used by the public.

8 Ranking of Ciphers

It is evident that very weak and already broken ciphers should be removed from the AES process. In addition very slow ciphers which are much slower than DES on all the platform can be removed as well. Fortunately (or unfortunately) the broken ciphers are also slow. They are LOKI97, Magenta, Frog, and Deal (which is already broken in the paper describing it with an attack whose complexity is 2^{120}).

In addition to this list the cipher HPC is relatively slow and complex, and whose security will probably never be studied unless it is accepted as the AES. However, without any study, it is better not to select it as the AES.

The ciphers Safer+, DFC, and CAST-256 are relatively slow. They may be fine from a pedagogical point of view, but some may require changes (e.g., DFC has too few rounds).

Rijndael and Crypton are very new (similar) designs based on the Square structure. As such, they should wait a few years till more cryptanalytic evidence will give us more knowledge on their security. At this stage it might be too early to select them as the standard. On the other hand, leaving one of them in the next round of the AES process might make them more visible, and may lead to new insights on their structure. Both these ciphers are faster than DES. It seems to me that between these two ciphers Rijndael is preferred at this stage.

The rest of the ciphers are faster than DES. E2, RC6, and Twofish are Feistel ciphers; Mars is an extended Feistel cipher, and Serpent is an SP network. Not all these ciphers are created equal, but all of them deserve being in the next round of the AES process. Some examples of drawbacks of these ciphers include that Mars is relatively complicated and thus difficult to analyze and verify, and RC6 bases it security on variable rotations which introduced previously only in RC5 relatively recently.

Therefore, the author proposes to select the ciphers for the next round of the AES process from the ciphers E2, Mars, RC6, Rijndael, Serpent, and Twofish.

9 Preclude

It is evident that since the author of this comment is one of the submitters of Serpent, the design of Serpent fits the above criteria.

Together with this comment the author also sends updated copies of his paper *A Note on Comparing the AES Candidates* from AES2, and an updated copy of the slides he presented in his talk.