

NESSIE Phase I: Selection of Primitives [†]

B. Preneel¹, B. Van Rompay¹,
L. Granboulan², G. Martinet²,
S. Murphy³, R. Shipsey³, J. White³,
M. Dichtl⁴, P. Serf⁴, M. Schafheutle⁴,
E. Biham⁵, O. Dunkelman⁵,
M. Ciet⁶, J-J. Quisquater⁶, F. Sica⁶,
L. Knudsen⁷, H. Raddum⁷.

23 September 2001

<http://www.cryptonessie.org>
NES/DOC/RHU/WP3/017/1

[†]The work described in this report has been supported by the Commission of the European Communities through the IST program under contract IST-1999-12324. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

¹K. U. Leuven, Dept. Elektrotechniek, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium.

²École Normale Supérieure, Département d'Informatique, 45 Rue d'Ulm, Paris 75230, France.

³Royal Holloway, Information Security Group, Egham, Surrey TW20 0EX, UK.

⁴Siemens AG, Otto-Hahn-Ring 6, München 81732, Germany.

⁵Technion, Computer Science Dept., Haifa 32000, Israel.

⁶U. C. Louvain, Département ELEC, PO Box 3, Place du Levant, B-1348 Louvain-la-Neuve, Belgium

⁷U. Bergen, Dept. of Informatics, PO Box 7800 Thormoehleensgt. 55, Bergen 5020, Norway.

1 Introduction

The NESSIE project is a three year project (2000-2002) that is funded by the European Union's *Fifth Framework Programme*. The main objective of the NESSIE project is to put forward a portfolio of strong cryptographic primitives of various types. Further details about the NESSIE project can be found at the NESSIE website <http://www.cryptonessie.org>. The start of the NESSIE project was an open call [3] for the submission of cryptographic primitives as well as for evaluation methodologies for these primitives. This call includes a request for the submission of block ciphers (as for the AES call), but also of other cryptographic primitives including hash functions, stream ciphers, and digital signature algorithms. The call also asked for evaluation methodologies for these primitives. The scope of the call was defined in conjunction with the project industry board, and was published in March 2000. This call resulted in forty submissions. The NESSIE project aims to assess these submissions with the goal of producing a portfolio of cryptographic primitives for use in different environments. The NESSIE project proposes to disseminate the project results widely and to build consensus based on these results by using the appropriate bodies: a project industry board, NESSIE workshops, the 5th Framework programme, and various standardisation bodies.

The NESSIE project has been divided into two phases. All primitives are evaluated in Phase I. At the end of Phase I, a subset of primitives is selected for further evaluation in Phase II. At the end of Phase II, a portfolio of primitives for possible standardisation will be chosen. To facilitate the open evaluation process, there are three NESSIE workshops. Submitted primitives were presented at the first NESSIE workshop, which took place on 13-14 November 2000 at K.U. Leuven (Belgium). Early results concerning the primitives were presented at the second NESSIE workshop, which took place on 12-13 September 2001 at Royal Holloway (U.K.). This workshop took place at the end of Phase I. The third workshop will take place at the end of Phase II (autumn 2002). In Phase I, both a security evaluation and a performance evaluation of the submitted primitives were undertaken by the NESSIE partners. The NESSIE partners have also received many external comments about the submitted primitives. Reports on both the Phase I Security Evaluation [5], which also contains methodological comments, and the Phase I Performance Evaluation [4] are available on the NESSIE website. An overview of the methodology used by the NESSIE project is given in the Phase I Security review [5]

This document gives the selection of primitives made by the NESSIE project for further evaluation in Phase II. The NESSIE project will also consider relevant standards or proposed standards in Phase II, such as AES, CBC-MAC, HMAC, DSS, SHA-1, SHA-256, SHA-384 and SHA-512.

2 Block Ciphers

We divide the discussion about block ciphers into normal-legacy (64-bit key) block ciphers and normal (128-bit key) or high (256-bit key) block ciphers.

2.1 Legacy Block Ciphers

- Legacy Block Ciphers selected for Phase II Evaluation
 - IDEA
 - Khazad
 - MISTY1
 - SAFER++₆₄
- Legacy Block Ciphers not selected for Phase II Evaluation
 - CS-Cipher
 - Hierocrypt-L1
 - Nimbus
 - NUSH

No security problems have been reported for IDEA, MISTY1, Khazad and SAFER++. IDEA benefits from having been scrutinised publicly for a decade without the detection of any serious weaknesses. MISTY1 has been in the public domain for five years, and the best attack breaks five of the suggested eight rounds. Khazad borrows elements from the AES, which makes it an attractive candidate for a 64-bit block cipher. Similarly SAFER++₆₄ is a minor modification of the 128-bit block cipher SAFER++₁₂₈.

CS-Cipher has no reported security problems, though it is the slowest of all the 64-bit submissions. Hierocrypt-L1 is slow, has problems with its key schedule and 3.5 out of its 6 rounds can be attacked. Nimbus has been broken in a chosen plaintext attack with 2^8 texts and 2^{10} time complexity. NUSH has an extremely low security margin, and it seems that a linear attack is faster than an exhaustive key search in the case of 256-bit keys.

2.2 Normal and high level Block Ciphers

- Normal and High Level Block Ciphers selected for Phase II Evaluation
 - SAFER++₁₂₈
 - Camellia
 - RC6
 - SHACAL
- Normal and High Level Block Ciphers not selected for Phase II Evaluation
 - NUSH
 - Grand Cru
 - Noekeon
 - Q

- Hierocrypt-3
- SC2000
- Anubis

No security problems have been reported for SAFER++₁₂₈, Camellia, RC6, and SHACAL. NUSH has an extremely low security margin, as described above. Grand Cru is based on AES, but is one of the slowest block ciphers submitted to NESSIE. Q can be attacked faster than an exhaustive key search. For Noekeon, there are many related keys for either of the two submitted key schedules. Hierocrypt-3 also has key schedule problems, and there are attacks for up to 3.5 rounds out of 6. SC2000 has a mix of Feistel rounds and SP-network rounds; the benefits of and justification for this design are unclear. Anubis is very similar to the AES. Any advantages that Anubis might offer over the AES would not seem sufficient to suggest that Anubis would ever be selected as an alternative standard to the AES.

3 MAC and Hash Functions

- MAC and Hash Functions selected for Phase II Evaluation
 - Two-Track-MAC
 - UMAC
 - Whirlpool

There have been no security problems reported for any of the submitted MAC and Hash Function primitives Two-Track-MAC, UMAC and Whirlpool. All three have been selected for further evaluation in Phase II of the NESSIE process.

4 Stream ciphers

- Stream Ciphers selected for Phase II Evaluation
 - SOBER-t16 and SOBER-t32
 - SNOW
 - BMGL
- Stream Ciphers not selected for Phase II Evaluation
 - LILI-128
 - LEVIATHAN

No security problems have been reported for the stream cipher submissions SOBER-t16, SOBER-t32, SNOW and BMGL.

LEVIATHAN possesses severe statistical problems, which have been verified experimentally. For LILI-128, there are attacks that are very much faster than brute force key space search.

5 Asymmetric Primitives

Primitives are selected for Phase II evaluation as detailed below. Phase II evaluation will take note of ongoing standardisation activities such as ISO and P1363.

5.1 Asymmetric Encryption

- Asymmetric Encryption Schemes selected for Phase II Evaluation
 - ACE Encrypt (revised version named ACE-KEM)
 - EPOC-2 (revised version)
 - PSEC-2 (revised version named PSEC-KEM)
 - ECIES
 - RSA-OAEP (if revised)
- Asymmetric Encryption Schemes not selected for Phase II Evaluation
 - EPOC-1 and EPOC-3
 - PSEC-1 and PSEC-3

Primitives based on finite field discrete logarithm

ACE Encrypt is proven to be secure without using the random oracle model but is not as flexible as the other schemes in that the only symmetric cipher it can be based on is MARS. ACE-KEM is a variant of ACE Encrypt with similar security, better performance, and also working in an elliptic curve group. ACE-KEM is supported by the submitters of ACE Encrypt.

Primitives based on elliptic curve discrete logarithm

PSEC-1 is not selected because it has worse security than PSEC-2 and similar performance. PSEC-2 as submitted to NESSIE has weaknesses. PSEC-KEM, a revised version of PSEC-2, is being considered by ISO and will be submitted to NESSIE. PSEC-KEM will be considered in Phase II. PSEC-KEM has an efficient reduction to a better asymmetric assumption, at the cost of a slower decryption, than PSEC-3. Furthermore, PSEC-3 is no longer supported by its submitters. Thus, PSEC-3 is not selected for Phase II.

ECIES and PSEC-3 are the schemes with the most efficient security reduction submitted in this category. Whilst the asymmetric component of ECIES is at least as secure as PSEC-3, it has stronger requirements for its symmetric components. ECIES is selected for Phase II. There is also an ECIES-KEM variant that will be compared to ECIES.

Primitives based on the factorisation problem

EPOC-1 is not selected for Phase II because it has worse security than EPOC-2 and similar performance. EPOC-2 has been revised in P1363 to fix some parameters and encoding methods. Compared to EPOC-3, EPOC-2 has an efficient reduction to a better asymmetric assumption, at the cost of a slower decryption. Furthermore, EPOC-3 is no longer supported by its submitters. Thus EPOC-3 is not selected for Phase II. EPOC-2 is selected for Phase II because it is the only submitted primitive based on factoring and it has efficient and convincing security.

RSA-OAEP is selected for Phase II. However, the OAEP padding has weaknesses and the submission should be modified to use another technique with a better security proof. We are aware of four techniques in the literature that reduce RSA encryption to the RSA problem: OAEP+ [6] and SAEP+ [1] have a bad reduction, REACT [2] and KEM [7] have a tight reduction. Recent results have shown that a Rabin-SAEP scheme [1] has better properties than the RSA-based schemes, as its security has a very efficient reduction to factoring instead of RSA inversion, and it has better performance than RSA-based schemes, though a bad implementation can reveal the secret key.

5.2 Digital Signature Schemes

- Digital Signature Schemes selected for Phase II Evaluation
 - ECDSA
 - ESIGN (revised version)
 - RSA-PSS
 - SFLASH
 - QUARTZ (depending on application)
- Digital Signature Schemes not selected for Phase II Evaluation
 - ACE Sign
 - FLASH

Primitives based on the RSA problem.

ACE Sign and RSA-PSS are both based on the difficulty of factorisation. While both are secure in the random oracle model if the RSA problem is hard (with a much tighter reduction for RSA-PSS), ACE Sign is also secure if the Strong-RSA problem is hard without any random oracle assumption. This additional security property has a high performance cost, which implies that ACE Sign with a 1024-bit modulus has similar performance to RSA-PSS with a 3000-bit modulus. Thus RSA-PSS is selected for Phase II, and ACE Sign is not selected for Phase II.

Primitives based on elliptic curve discrete logarithm problem

ECDSA is selected for Phase II. There have been no reported security problems, and ECDSA creates shorter signatures than RSA-PSS with a shorter signing time with an equivalent verification time.

Primitives based on the approximate e -th root modulo p^2q

The security of ESIGN is based on a similar but stronger assumption than RSA. It has similar performance to ECDSA, and its security also seems to be similar. ESIGN has been revised in P1363 to change some parameters and encoding methods so that signature generation for long messages requires only one pass through a hash function. ESIGN is selected for Phase II.

Primitives based on multivariate quadratic polynomials

FLASH and SFLASH are both C^{*--} schemes targeted to a smart card environment. SFLASH is selected for Phase II and FLASH is not. SFLASH has similar security and similar performance as FLASH, but with a much smaller public key. QUARTZ has very slow signature generation but the resulting signature is only 128 bits long. If such short signatures are considered useful in standardised applications, then QUARTZ should be selected for Phase II. We note that the less convincing security of these schemes is a less significant problem for applications which need signatures with only a short validity period.

5.3 Digital Identification Schemes

- Digital Identification Schemes selected for Phase II Evaluation
 - GPS

GPS, the only primitive submitted to NESSIE in this category, has good performance with high security. The submitted documents contain some minor flaws in the specification, but these have been corrected. GPS is selected for further evaluation in Phase II.

References

- [1] Dan Boneh. Simplified OAEP for the RSA and Rabin functions. In *Advances in Cryptology – CRYPTO 2001*, August 2001. Available at <http://crypto.stanford.edu/~dabo/abstracts/saep.html>.
- [2] Tatsuaki Okamoto and David Pointcheval. RSA-REACT: An alternative to RSA-OAEP. In *Proceedings of the Second Open NESSIE Workshop*, September 2001. Available at <http://www.di.ens.fr/~pointche/>.
- [3] NESSIE Project. NESSIE call for cryptographic primitives, March 2000. Available at <http://www.cryptoneessie.org>.

- [4] NESSIE Project. Deliverable D14 – report on the performance evaluation of the NESSIE candidates. Available at <http://www.cryptonessie.org>, September 2001.
- [5] NESSIE Project. Security evaluation I. Available as Deliverable D13 at <http://www.cryptonessie.org>, September 2001.
- [6] Victor Shoup. OAEP reconsidered. Available at <http://www.shoup.net>, August 2001.
- [7] Victor Shoup. A proposal for an ISO standard for public key encryption (version 2.0). Available at <http://www.shoup.net>, September 2001.