



Project Number	IST-2000-12324
Project Title	NESSIE
Deliverable Type	Report
Security Class	Public
Deliverable Number	D18
Title of Deliverable	Update on the selection of algorithms for further investigation during the second round
Document Reference	NES/DOC/ENS/WP5/D18/1
Contractual Date of Delivery	Y3 M2
Actual Date of Delivery	Y3 M3
Editors	ENS
Abstract	A preliminary selection of primitives was published at the end of the first round of evaluation. This is an update of the selection, which determines which primitives will be further evaluated during the second round. This report includes rationale for all the primitives considered by the NESSIE consortium.
Keywords	NESSIE, Selected primitives.

Version 1.0

March 11, 2002

Update on the selection of algorithms for further investigation during the second round[†]

B. Preneel¹, A. Bosselaers¹, S. B. Örs¹, A. Biryukov¹,
L. Granboulan², E. Dottax²,
S. Murphy³, A. Dent³, J. White³,
M. Dichtl⁴, S. Pyka⁴, P. Serf⁴,
E. Biham⁵, E. Barkan⁵, O. Dunkelman⁵,
M. Ciet⁶, F. Sica⁶,
L. Knudsen^{7,8}, H. Raddum⁷.

March 11, 2002

Version 1.0

[†]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.

¹Katholieke Universiteit Leuven, Dept. Elektrotechniek-ESAT/COSIC, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium

²École Normale Supérieure, Département d'Informatique, 45 rue d'Ulm, Paris 75230 Cedex 05, 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

⁶Université Catholique de Louvain, Dept. ELEC, Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium

⁷Universitetet i Bergen, Dept. of Informatics, PO Box 7800 Thormoehlensgt. 55, Bergen 5020, Norway

⁸Tech. Univ. of Denmark, Dept. of Mathematics, Building 303, DK-2800 Lyngby, Denmark

Executive Summary

Evaluation Phase II

(NESSIE Deliverable D18)

NESSIE (New European Schemes for Signature, Integrity, and Encryption) is a research project within the Information Societies Technology (IST) Programme of the European Commission. Detailed and up to date information on the NESSIE project is available at the project web site: <http://cryptonessie.org>. The participants of the project are:

- Katholieke Universiteit Leuven (Belgium), coordinator;
- Ecole Normale Supérieure (France);
- Royal Holloway, University of London (U.K.);
- Siemens Aktiengesellschaft (Germany);
- Technion - Israel Institute of Technology (Israel);
- Université Catholique de Louvain (Belgium); and
- Universitetet i Bergen (Norway).

NESSIE is a 3-year project which started on 1st January 2000. The main objective of the project is to put forward a portfolio of strong cryptographic primitives obtained after an open call and evaluated using a transparent and open process. The evaluation concerns both the security and the performance aspects of the primitives.

An open call [14] for the submission of cryptographic primitives was published at the start of the NESSIE project. The submitted primitives have been studied during the Phase I of the project, along with existing standards. Reports on both the Phase I Security Evaluation [17] and the Phase I Performance Evaluation [16] were published. A workshop was held in September 2001 at Royal Holloway at which early results concerning the primitives were presented.

At the end of Phase I a subset of the primitives was selected that was believed to have the most potential to be recommended by NESSIE for inclusion in future standards. This list was published in [15] for further evaluation during Phase II. Submitters had the opportunity to propose minor changes (alterations or ‘tweaks’) to their submissions before the beginning of Phase II of the evaluation.

New results have been found on some primitives and the submitters’ comments have been taken into account. The present report presents an updated selection of primitives based on these and gives the rationale behind the choice.

Status of the primitives considered by NESSIE

Selected primitives are marked by an X.

64-bit block ciphers

CS-cipher		not selected
Hierocrypt-L1		not selected
IDEA	X	selected
Khazad	X	tweaked version selected
Misty1	X	selected
Nimbus		not selected
Nush		not selected
Safer++ ₆₄	X	selected
Triple-DES	X	NIST standard considered

128-bit block ciphers

Anubis		tweaked version not selected
Camellia	X	selected
Grand Cru		not selected
Hierocrypt-3		not selected
Noekeon		not selected
Nush		not selected
Q		not selected
RC6	X	selected
Safer++ ₁₂₈	X	selected
SC2000		not selected
Rijndael	X	NIST standard considered

160-bit block ciphers

SHACAL-1	X	selected
----------	---	----------

256-bit block ciphers

RC6	X	selected
Rijndael-256	X	variant of NIST standard is considered
SHACAL-2	X	selected

Stream ciphers and pseudo-random numbers generators

BMGL	X	tweaked version (adding IV) selected
LEVIATHAN		not selected
LILI-128		not selected
SNOW	X	128-bit key selected. 256-bit key not selected.
SOBER-t16		selected, but eliminated during first part of Phase II
SOBER-t32		selected, but eliminated during first part of Phase II
RC4		existing de facto standard is not selected

Hash functions

Whirlpool	X	selected
SHA-1	X	NIST standard considered
SHA-2/256	X	NIST standard considered
SHA-2/384	X	NIST standard considered
SHA-2/512	X	NIST standard considered

Message authentication codes

HMAC	X	NIST standard considered
UMAC	X	selected
Two-Track-MAC	X	selected

Asymmetric encryption

ACE-KEM	X	tweaked version of ACE-Encrypt selected
ECIES	X	selected (ECIES-KEM tweak will also be studied)
EPOC-1		not selected
EPOC-2	X	tweaked version selected
EPOC-3		not selected
PSEC-1		not selected
PSEC-KEM	X	tweaked version of PSEC-2 selected
PSEC-3		not selected
RSA-OAEP		not selected
RSA-OAEP+	X	possible future ISO standard considered
RSA-KEM	X	possible future ISO standard considered

Digital signature schemes

ACE Sign		not selected
ECDSA	X	selected
ESIGN	X	tweaked version selected
FLASH		not selected
SFLASH	X	tweaked version selected
QUARTZ	X	tweaked version selected
RSA-PSS	X	selected

Digital identification schemes

GPS	X	tweaked version selected
-----	---	--------------------------

Note that there have been some changes in the way the primitives have been categorised. Block ciphers are now divided by block length with the three levels of security (high, normal and legacy) still taken into consideration where relevant. Stream ciphers and pseudorandom number generators have been merged in one category in spite of their different uses.

Contents

Executive Summary	i
1 64-bit block ciphers	1
1.1 CS-cipher	1
1.2 Hierocrypt-L1	1
1.3 IDEA	1
1.4 Khazad	1
1.5 Misty1	1
1.6 Nimbus	1
1.7 Nush	1
1.8 Safer++ ₆₄	2
1.9 Triple-DES	2
2 128-bit block ciphers	3
2.1 Anubis	3
2.2 Camellia	3
2.3 Grand Cru	3
2.4 Hierocrypt-3	3
2.5 Noekeon	3
2.6 Nush	3
2.7 Q	3
2.8 RC6	3
2.9 Rijndael	4
2.10 Safer++ ₁₂₈	4
2.11 SC2000	4
3 160-bit block ciphers	5
3.1 SHACAL-1	5
4 256-bit block ciphers	6
4.1 RC6	6
4.2 Rijndael-256	6
4.3 SHACAL-2	6
5 Stream ciphers and pseudo-random numbers generators	7
5.1 BMGL	7
5.2 LEVIATHAN	7
5.3 LILI-128	7
5.4 SNOW	7
5.5 SOBER-t16	7
5.6 SOBER-t32	7
5.7 RC4	7

6	Hash functions	8
6.1	Whirlpool	8
6.2	SHA-1	8
6.3	SHA-2/256, SHA-2/384 and SHA-2/512	8
7	Message authentication codes	9
7.1	HMAC	9
7.2	UMAC	9
7.3	Two-Track-MAC	9
8	Asymmetric encryption	10
8.1	ACE-KEM	10
8.2	ECIES	10
8.3	EPOC-1	10
8.4	EPOC-2	10
8.5	EPOC-3	10
8.6	PSEC-1	10
8.7	PSEC-KEM	10
8.8	PSEC-3	11
8.9	RSA-OAEP	11
8.10	RSA-OAEP+	11
8.11	RSA-KEM	11
9	Digital signature schemes	12
9.1	ACE Sign	12
9.2	ECDSA	12
9.3	ESIGN	12
9.4	FLASH	12
9.5	SFLASH	12
9.6	QUARTZ	12
9.7	RSA-PSS	12
10	Digital identification schemes	13
10.1	GPS	13

1 64-bit block ciphers

1.1 CS-cipher

No security flaws have been found but the performance of CS-Cipher is significantly worse than its competitors on common desktop computers. Therefore it has not been selected.

1.2 Hierocrypt-L1

Hierocrypt-L1 has a very slow key schedule with possible security flaws. Attacks significantly reducing the security margin have been found that the submitters were not aware of [3]. Therefore it has not been selected.

1.3 IDEA

IDEA has been widely studied for a decade and no security flaws have been found. With the exception of a rather slow key schedule, its performance is acceptable on most desktop platforms. Therefore it has been selected.

1.4 Khazad

The tweak to Khazad proposed by the submitters corrects a small security flaw. Its performance is good and it is similar to Rijndael which has been well-studied. Therefore it has been selected.

1.5 Misty1

Misty1 has been widely studied for five years and no serious security flaws have been found. Its performance is good and it has a very fast key schedule. Therefore it has been selected.

1.6 Nimbus

There is a very practical attack on Nimbus [4] and the justifications for its design are not sufficiently convincing for it to be worth considering a tweaked variant. Therefore it has not been selected.

1.7 Nush

Nush has no security margin [16] and its performance is no better than Misty1 or Khazad. Therefore it has not been selected.

1.8 Safer++₆₄

The performance of Safer++₆₄ is similar to that of CS-Cipher but its key schedule is faster. No security flaws have been found and it has many similarities to Safer++₁₂₈ which has been selected, so it has also been selected.

1.9 Triple-DES

The security of Triple-DES is significantly less than the 128 bits required for this cipher category and its performance on workstations is rather bad. However Triple-DES will still be considered as a benchmark for other algorithms.

2 128-bit block ciphers

2.1 Anubis

No security flaws have been found in the tweaked version of Anubis. Anubis is very similar to Rijndael and any advantage that it might offer over AES would not be sufficient to select it as an alternative. Therefore it has not been selected.

2.2 Camellia

No security flaws have been found. Its performance on common desktop computers is close to that of the AES finalists and it has an interesting design. Therefore it has been selected.

2.3 Grand Cru

Grand Cru is the slowest cipher submitted to NESSIE and there is no reason to believe that this is compensated for by stronger security. Therefore it has not been selected.

2.4 Hierocrypt-3

Hierocrypt-3 has a very slow key schedule with possible security flaws. Attacks significantly reducing the security margin have been found that the submitters were not aware of [3]. Therefore it has not been selected.

2.5 Noekeon

Both key schedules of Noekeon are too susceptible to related key attacks [12], so it has not been selected.

2.6 Nush

Nush has no security margin [16] and its performance is no better than Rijndael. Therefore it has not been selected.

2.7 Q

There is an attack on Q faster than exhaustive search [5], so it has not been selected.

2.8 RC6

No security flaws have been found and it has resisted cryptanalysis during and after the AES process. Therefore, although its performance is bad on some architectures, it has been selected.

2.9 Rijndael

Rijndael has been selected by the NIST as the new AES. No security flaws have been found, its performance is very good on most architectures, and the justifications for its design are convincing. Therefore it will serve as a benchmark for other submissions.

2.10 Safer++₁₂₈

No security flaws have been found, and its performance is relatively good. Its design has many interesting properties. Therefore it has been selected.

2.11 SC2000

No security flaws have been found, and its performance is relatively good. However the justifications for its design are not convincing, so it has not been selected.

3 160-bit block ciphers

3.1 SHACAL-1

No security flaws have been found, and its performance is good. It also has the interesting property of being able to share most of the code of the SHA-1 hash function. Therefore it has been selected.

4 256-bit block ciphers

4.1 RC6

No security flaws have been found and the 128-bit block variant of RC6 on which the 256-bit variant is based has been well studied. Therefore it has been selected.

4.2 Rijndael-256

No security flaws have been found, and the 128-bit block variant on which it is based was selected at the AES and has been well-studied. Therefore it has been selected.

4.3 SHACAL-2

No security flaws have been found and its performance is quite good. It also has the interesting property of being able to share most of the code of the SHA-2 hash function. Therefore it has been selected.

5 Stream ciphers and pseudo-random numbers generators

5.1 BMGL

BMGL has been tweaked to allow rekeying. No flaws have been found in the security proof. The performance of BMGL is quite bad for a stream cipher, but it is still interesting as a pseudorandom number generator, so it has been selected.

5.2 LEVIATHAN

There is a distinguishing attack on LEVIATHAN faster than exhaustive key search [6]. Therefore it has not been selected.

5.3 LILI-128

The key of LILI-128 can be recovered faster than exhaustive key search [2, 11, 18]. Therefore it has not been selected.

5.4 SNOW

The internal state of SNOW can be recovered faster than exhaustive 256-bit key search [1]. Therefore 256-bit SNOW has not been selected. The tweaked version (adding IV) of 128-bit SNOW is selected.

5.5 SOBER-t16

There is a distinguishing attack on SOBER-t16 faster than exhaustive key search [7]. Therefore it has been selected, but eliminated during first part of Phase II

5.6 SOBER-t32

There is a distinguishing attack on SOBER-t32 without stuttering much faster than exhaustive key search [7]. The submitters claimed that the stuttering was not necessary for security. Therefore it has been selected, but eliminated during first part of Phase II

5.7 RC4

RC4 is the de facto standard for stream ciphers. The second output byte of RC4 can be easily distinguished from a random one [13]. Although this can be easily overcome, the keystream still can be distinguished from a random output [9] and the key schedule has severe weaknesses [8]. There is also no form of rekeying defined for RC4. Therefore RC4 will not be considered by NESSIE.

6 Hash functions

6.1 Whirlpool

No security flaws have been found and its performance is reasonable considering its 512-bit output size. Therefore it has been selected.

6.2 SHA-1

SHA-1 has been the NIST hash function standard for a long time. Its performance is very good, partly since it has a 160-bit output size. Therefore it will be considered as a benchmark for the submission in this category.

6.3 SHA-2/256, SHA-2/384 and SHA-2/512

SHA-2 has recently been published as the new NIST hash function standard, generating 256-bit, 384-bit or 512-bit hash values. It will also serve as a benchmark for the hash functions for the submission in this category.

7 Message authentication codes

7.1 HMAC

The SHA-1 based HMAC has recently been published as the new future NIST MAC standard. It will be considered as benchmark for the submissions.

7.2 UMAC

No flaws have been found in the security proof of UMAC and the cipher on which it is based (AES) seems to meet the security requirements claimed. Therefore it has been selected.

7.3 Two-Track-MAC

No security flaws have been found, and its performance is good. Therefore it has been selected.

8 Asymmetric encryption

8.1 ACE-KEM

ACE-KEM is the tweaked version of the ACE-Encrypt submission, following the ISO proposal [19]. It is based on the discrete logarithm problem, and its security proof does not require the random oracle model, possibly an important issue in the long term. The performance of ACE-KEM is better than ACE-Encrypt, and it can be defined on either a multiplicative modular group or on an elliptic curve, making its performance competitive. Therefore it has been selected.

8.2 ECIES

ECIES is the most efficient submission with respect to encryption and decryption. Therefore it has been selected. However some tweaks have been proposed by Shoup [19] to change this scheme to ECIES-KEM. These will be considered.

8.3 EPOC-1

EPOC-1 has worse security and similar performance to EPOC-2. It is no longer supported by its submitters. Therefore it has not been selected.

8.4 EPOC-2

EPOC-2 is the only submitted scheme that relies on the factorisation problem, and has an efficient security proof and reasonable performance. It has been tweaked, mostly in the key generation algorithm. Some parameters have also been defined more precisely. It is vulnerable to side-channel attacks, probably more so than similar schemes such as Rabin-SAEP, and it should be studied further. It has been selected.

8.5 EPOC-3

EPOC-3 is no longer supported by its submitters. Therefore it has been rejected.

8.6 PSEC-1

PSEC-1 has worse security and similar performance to PSEC-2. It is no longer supported by its submitters. Therefore it has been rejected.

8.7 PSEC-KEM

PSEC-KEM is the tweaked version of the PSEC-2 submission, following the ISO proposal [19]. Compared to ECIES, it has an efficient reduction to a better asymmetric assumption (at the cost of slower decryption). Therefore it has been selected.

8.8 PSEC-3

PSEC-3 has similar performance to ECIES and slightly different security. It is no longer supported by its submitters. Therefore it has not been selected.

8.9 RSA-OAEP

The OAEP padding for RSA is proven to be secure but with an inefficient security reduction. Some other constructions have been proposed with better security. Therefore OAEP has not been selected.

8.10 RSA-OAEP+

This variant of RSA-OAEP with a more efficient security reduction has been proposed as a possible future ISO standard [19]. Therefore it will be considered, in particular for direct encryption.

8.11 RSA-KEM

This RSA based scheme has an efficient security reduction but can only be used in hybrid mode. It has been proposed as a possible future ISO standard [19]. Therefore it will be considered for hybrid encryption.

9 Digital signature schemes

9.1 ACE Sign

Despite its security proof not requiring the random oracle model, the performance cost of this additional security makes ACE Sign an unsuitable choice. Therefore it has not been selected.

9.2 ECDSA

No flaws have been found in the security proof which gives an efficient reduction. ECDSA creates shorter signatures than RSA-PSS and has a shorter signing time. Therefore it has been selected.

9.3 ESIGN

The submission has been tweaked to correct some security flaws. No flaws have been found in the security proof. Its performance and security are similar to ECDSA. Therefore it has been selected.

9.4 FLASH

FLASH and SFLASH are very similar so it seems necessary to consider only one of them and FLASH has larger keys sizes and signatures. Therefore it has not been selected.

9.5 SFLASH

The submitted version of SFLASH has been broken [10] so it has been tweaked to be more similar to FLASH. Its performance is similar to ESIGN or ECDSA on common workstations but it has no security proof. It may be much faster on low cost smart cards however, so is selected for further investigation.

9.6 QUARTZ

Despite the very long signing time, Quartz is the only scheme to produce very short signatures. The tweaked version improves the speed marginally. No security flaws have been found and it has been selected.

9.7 RSA-PSS

No flaws have been found in the security proof which gives an efficient reduction. RSA-PSS relies on the well-studied RSA problem, and allows fast verification. It has been selected.

10 Digital identification schemes

10.1 GPS

A flaw was discovered in the submitted GPS, but this can be easily overcome. The security and performance of the scheme are good, so it has been selected.

References

- [1] anonymous. Guess-and-determine attacks on SNOW. In *submitted to Crypto '02*, 2002.
- [2] S. Babbage. Cryptanalysis of the LILI-128 stream cipher. Technical report, NESSIE report, 2001.
- [3] P. Barreto, V. Rijmen, J. Nakahara Jr., B. Preneel, J. Vandewalle, and H. Y. Kim. Improved SQUARE attacks against reduced-round HIEROCRYPT. In *Proceedings of Fast Software Encryption '01*, 2001.
- [4] E. Biham and V. Furman. Differential cryptanalysis of Nimbus. In *Proceedings of Fast Software Encryption '01*, 2001.
- [5] E. Biham, V. Furman, M. Misztal, and V. Rijmen. Differential cryptanalysis of Q. In *Proceedings of Fast Software Encryption '01*, 2001.
- [6] P. Crowley and S. Lucks. Bias in the LEVIATHAN stream cipher. In *Proceedings of Fast Software Encryption '01*, 2001.
- [7] P. Ekdahl and T. Johansson. Distinguishing attacks on SOBER-t16 and t32. In *Proceedings of Fast Software Encryption '02*, 2002.
- [8] S. R. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key scheduling algorithm of RC4. In *Proceedings of SAC '01*, 2001.
- [9] S. R. Fluhrer and D. A. McGrew. Statistical analysis of the alleged RC4 stream cipher. In *Proceedings of Fast Software Encryption '00*, 2000.
- [10] H. Gilbert and M. Minier. Cryptanalysis of SFLASH. In *Proceedings of Eurocrypt '02*, 2002.
- [11] F. Jönsson and T. Johansson. A fast correlation attack on LILI-128. Technical report, Lund University report, 2001.
- [12] L. R. Knudsen and H. Raddum. On Noekeon. In *Proceedings of the second NESSIE Workshop*, 2001. NES/DOC/UIB/WP3/009/1.
- [13] I. Mantin and A. Shamir. A practical attack on broadcast RC4. In *Proceedings of Fast Software Encryption '01*, 2001.
- [14] NESSIE partners. NESSIE call. Technical report, NES/DOC/KUL/WP1/001/2, 2000.
- [15] NESSIE partners. NESSIE Phase I: Selection of Primitives. Technical report, NES/DOC/RHU/WP3/017/1, 2001.

- [16] NESSIE partners. Report on the Performance Evaluation of NESSIE Candidates I. Technical report, NES/DOC/UCL/WP4/D14/1, 2001.
- [17] NESSIE partners. Security Evaluation I. Technical report, NES/DOC/RHU/WP3/D13/1, 2001.
- [18] M.-J. O. Saarinen. A time-memory trade-off attack against LILI-128. In *Proceedings of Fast Software Encryption '02*, 2002.
- [19] V. Shoup. A proposal for an ISO standard for public key encryption (version 2.0). Technical report, <http://eprint.iacr.org/2001/112/>, 2001.