New European Schemes for Signature, Integrity and Encryption (NESSIE): A Status Report[*]

Bart Preneel

Katholieke Univ., Leuven, Dept. Electrical Engineering-ESAT,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium

bart.preneel@esat.kuleuven.ac.be

Abstract

In February 2000 the NESSIE project has launched an open call for the next generation of cryptographic algorithms. These algorithms should offer a higher security and/or confidence level than existing ones, and should be better suited for the constraints of future hardware and software environments.The NESSIE project has received 39 algorithms, many of these from major players. In October 2001, the project completed the first phase of the evaluation and has selected 24 algorithms for the second phase. The goal is to recommend a complete portfolio of algorithms by the end of 2002. This article presents the status of the NESSIE project after two years.

1 Introduction

NESSIE (New European Schemes for Signature, Integrity, and Encryption) is a research project within the Information Societies Technology (IST) Programme of the European Commission. 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 January 1, 2000. This paper presents the state of the project after two years, and it is organized as follows. Section 2 discusses the NESSIE call and its results. Section 3 discusses the tools which the project is developing to support the evaluation process. Sections 4 and 5 deal with the security and performance evaluation respectively, and Sect. 6 discusses the selection of algorithms for the 2nd phase. Section 7 raises some intellectual property issues. The NESSIE approach towards dissemination and standardization is presented in Section 8. Finally, conclusions are put forward in Section 9.

Detailed and up to date information on the NESSIE project is available at the project web site http://cryptonessie.org/.

[*] To appear in Springer Verlag LNCS, Proc. PKCS 2002.

2 NESSIE Call

In the first year of the project, an open call for the submission of cryptographic algorithms, as well as for evaluation methodologies for these algorithms has been launched. The scope of this call has been defined together with the project industry board (PIB) (cf. Sect. 8), and it was published in February 2000. The deadline for submissions was September 29, 2000. In response to this call NESSIE received 40 submissions, all of which met the submission requirements.

2.1 Contens of the NESSIE Call

The NESSIE call includes a request for a broad set of algorithms providing date confidentiality, data authentication, and entity authentication. These algorithms include block ciphers, stream ciphers, hash functions, MAC algorithms, digital signature schemes, and public-key encryption and identification schemes (for definitions of these algorithms, see [14]). In addition, the NESSIE call asks for evaluation methodologies for these algorithms. While key establishment protocols are also very important, it was felt that they should be excluded from the call, as the scope of the call is already rather broad.

The scope of the NESSIE call is much wider than that of the AES call launched by NIST [16], which was restricted to 128-bit block ciphers. It is comparable to that of the RACE Project RIPE (Race Integrity Primitives Evaluation, 1988-1992) [22] (confidentiality algorithms were excluded from RIPE for political reasons) and that of the Japanese CRYPTREC project [4] (which also includes key establishment protocols and pseudo-random number generation). Another difference is that both AES and CRYPTREC intend to produce algorithms for government standards. The results of NESSIE will not be adopted by any government or by the European commission. However, the intention is that relevant standardization bodies will adopt these results. As an example, algorithms for digital signature and hash functions may be included in the EESSI standardization documents which specify algorithms recommended for the European Electronic Signature Directive.

The call also specifies the main selection criteria which will be used to evaluate the proposals. These criteria are long-term security, market requirements, efficiency, and flexibility. Primitives can be targeted towards a specific environment (such as 8-bit smart cards or high-end 64-bit processors), but it is clearly an advantage to offer a wide flexibility of use. Security is put forward as the most important criterion, as security of a cryptographic algorithm is essential to achieve confidence and to build consensus.

For the *security requirements* of symmetric algorithms, two main security levels are specified, named *normal* and *high*. The minimal requirements for a symmetric algorithm to attain either the normal or high security level depend on the key length, internal memory, or output length of the algorithm. For block ciphers a third security level, *normal-legacy*, is specified, with a block size of 64 bits compared to 128 bits for the normal and high security level. The motivation for this request are applications such as UMTS/3GPP, which intend to use 64-bit block ciphers for the next 10-15 years. For the asymmetric algorithms, a varying security level is accepted, with as minimum about 2^{80} 3-DES encryptions.

If selected by NESSIE, the algorithm should preferably be available royalty-free. If this is not possible, then access should be non-discriminatory. The submitter should state the position concerning intellectual property and should update it when necessary.

The submission requirements are much less stringent than for AES, particularly in terms of the requirement for software implementations (only `portable C' is mandatory).

2.2 Response to the NESSIE Call

The cryptographic community has responded very enthusiastically to the call. Thirty nine algorithms have been received, as well as one proposal for a testing methodology. After an interaction process, which took about one month, all submissions comply with the requirements of the call. There are 26 symmetric algorithms:

- seventeen block ciphers, which is probably not a surprise given the increased attention to block cipher design and evaluation as a consequence of the AES competition organized by NIST. They are divided as follows:
  - six 64-bit block ciphers: CS-Cipher, Hierocrypt-L1, IDEA, Khazad, MISTY1, and Nimbus;
  - seven 128-bit block ciphers: Anubis, Camellia, Grand Cru, Hierocrypt-3, Noekeon, Q, and SC2000 (none of these seven come from the AES process);
  - one 160-bit block cipher: Shacal; and
  - hree block ciphers with a variable block length: NUSH (64, 128, and 256 bits), RC6 (at least 128 bits), and SAFER++ (64 and 128 bits).
- six synchronous stream ciphers: BMGL, Leviathan, LILI-128, SNOW, SOBER-t16, and SOBER-t32.
- two MAC algorithms: Two-Track-MAC and UMAC; and
- one collision-resistant hash function: Whirlpool.

Thirteen asymmetric algorithms have been submitted:

- five asymmetric encryption schemes: ACE Encrypt, ECIES, EPOC, PSEC, and RSA-OAEP (both EPOC and PSEC have three variants);
- seven digital signature algorithms: ACE Sign, ECDSA, ESIGN, FLASH, QUARTZ, RSA-PSS, and SFLASH; and
- one identification scheme: GPS.

Approximately[1] seventeen submissions originated within Europe (6 from France, 4 from Belgium, 3 from Switzerland, 2 from Sweden), nine in North America (7 USA, 2 from Canada), nine in Asia (8 from Japan), three in Australia and three in South America (Brazil). The majority of submissions originated within industry (27); seven came from academia, and six are the result of a joint effort between industry and academia. Note however that the submitter of the algorithm may not be the inventor, hence the share of academic research is probably underestimated by these numbers.

On November 13-14, 2000 the first NESSIE workshop was organized in Leuven (Belgium), where most submissions were presented. All submissions are available on the NESSIE web site [15].

3 Tools

It is clear that modern computers and sophisticated software tools cannot replace human cryptanalysis. Nevertheless, software tools can play an important role in modern cryptanalysis. In most cases, the attacks found by the cryptanalyst require a large number of computational steps, hence the actual computation of the attack is performed on a computer. However, software and software tools can also be essential to find a successful way to attack a symmetric cryptographic algorithm; examples include differential and linear cryptanalysis, dependence tests, and statistical tests.

Within NESSIE, we distinguish two classes of tools. The general tools are not specific for the algorithms to be analyzed. Special tools, which are specific for the analysis of one algorithm, are implemented when, in the course of the cryptanalysis of an algorithm, the need for such a tool turns up.

For the evaluation of the symmetric submissions, a comprehensive set of general tools is available within the project. These tools are in part based on an improved version of the tools developed by the RIPE (RACE Integrity Primitives Evaluation) [22]. These test include: the frequency test, the collision

[1] Fractional numbers have been used to take into account algorithms with submitters over several continents/countries -- the totals here are approximations by integers, hence they do not add up to 40.

test, the overlapping *m*-tuple test, the gap test, the constant runs test, the coupon collector's test, Maurer's universal test [13], the poker test, the spectral test, the correlation test, the rank test, the linear, non-linear, and dyadic complexity test, the Ziv-Lempel complexity test, the dependence test, the percolation test, the linear equation, linear approximation and correlation immunity test, the linear factors test, and a cycle detection tool.

The NESSIE project is also developing a new generic tool to analyze block ciphers with differential [1] and linear cryptanalysis [12]. This tool is based on a general description language for block ciphers.

In September 2000, the US NIST published a suite of statistical tests for the evaluation of sequences of random or pseudo-random bits; this document has been revised in December 2000 [18]. A careful comparison has been made between the RIPE and NIST test suites.
The software for these tools will not be made available outside the project, but all the results obtained using these tools will be made public in full detail.

4 Security Evaluation

We first describe the internal process within NESSIE used to assess submissions. Initially each submission was assigned to a NESSIE partner, who performed basic checks on the submission, such as compliance with the call, working software, obvious weaknesses etc. The aim of this initial check was mainly to ensure that submissions were specified in a consistent and cogent form in time for the November 2000 workshop. It is vital for proper security assessments that the algorithms are fully and unambiguously described. This process required interaction with some submitters to ensure that the submissions were in the required form.

The next internal stage (November 2000) was to assign each submission to a pair of NESSIE partners for an initial detailed evaluation. Each submission has then been subject to two independent initial assessments. After the two initial assessments of a submission have taken place, the two NESSIE partners have produced a joint summary of their assessments concerning that submission. Based on this initial evaluation, algorithms were dismissed or subjected to further dedicated analysis.

Next, an open workshop was organized in Egham (UK) on September 12-13, 2001 to discuss the security and performance analysis of the submissions. The presenters include both researchers from the NESSIE project, but also submitters, members from the NESSIE PIB, and members from the cryptographic community at large.

Following this workshop, a comprehensive security evaluation report has been published [19]. The document gives an overview of generic attacks on the different type of algorithms. Moreover, for each symmetric algorithm it presents a short description, the security claims by the designers, and the reported weaknesses and attacks. The part on asymmetric algorithms contains a discussion of security assumptions, security models, and of the methodology to evaluate the security. For each algorithm, a short description is followed by a discussion of the provable security (which security properties are proved under which assumptions) and of the concrete security reduction.

5 Performance Evaluation

Performance evaluation is an essential part in the assessment of a cryptographic algorithm: efficiency is a very important criterion in deciding for the adoption of an algorithm.

The candidates will be used on several platforms (PCs, smart cards, dedicated hardware) and for various applications. Some applications have tight timing constraints (e.g., payment applications, cellular phones); for other applications a high throughput is essential (e.g., high speed networking, hard disk encryption).

First a framework has been defined to compare the performance of algorithms on a fair and equal basis. It will be used for all evaluations of submitted candidates. First of all a theoretical approach has been established. Each algorithm is dissected into three parts: setup (independent of key and data), precomputations (independent of data, e.g., key schedule) and the algorithm itself (that must be repeated for every use). Next a set of four test platforms has been defined on which each candidate may be tested. These platforms are smart cards, 32-bit PCs, 64-bit machines, and Field Programmable Gate Arrays (FPGAs).

Then rules have been defined which specify how performance should be measured on these platforms. The implementation parameters depend on the platform, but may include RAM, speed, code size, chip area, and power consumption. On smart cards, only the following parameters will be taken into account, in decreasing order of importance: RAM usage, speed, code size. On PCs, RAM has very little impact, and speed is the main concern. On FPGAs, throughput, latency, chip area and power consumption will be considered. Unfortunately, the limited resources of the project will not allow for the evaluation of dedicated hardware implementations (ASICs), but it may well be that teams outside the project can offer assistance for certain algorithms.

The project will also consider the resistance of implementations to physical attacks such as timing attacks [9], fault analysis [2, 3], and power analysis [10]. For non constant-time algorithms (data or key dependence, asymmetry between encryption and decryption) the data or key dependence will be analyzed; other elements that will be taken into account include the difference between encryption and decryption, and between signature and verification operation. For symmetric algorithms, the key agility will also be considered.

This approach will result in the definition of a platform dependent test and in several platform dependent rekeying scenarios. Low-cost smart cards will only be used for block ciphers, MACs, hash functions, stream ciphers, pseudo-random number generation, and identification schemes.

In order to present performance information in a consistent way within the NESSIE project, a performance `template' has been developed. The goal of this template is to collect intrinsic information related to the performance of the submitted candidates. A first part describes parameters such as word size, memory requirement, key size and code size. Next the basic operations are analyzed, such as shift/rotations, table look-ups, permutations, multiplications, additions, modular reduction, exponentiation, inversion… Then the nature and speed of precomputations (setup, key schedule, etc.) are described. Elements such as the dependence on the keys and on the inputs determine whether the code is constant-time or not. Alternative representations of the algorithms are explored when feasible.

The result of the preliminary performance evaluation are presented in [21]. This document contains an overview of the performance claimed by the designers, a theoretical evaluation, and performance measurements of optimized C-code on a PC and a workstation. However, due to limited resources and the large number of algorithms, it was not possible to guarantee full optimization for all algorithms. Nevertheless, it was felt that these results provide sufficient information to make a selection of algorithms for the 2nd phase of the project.

6 Selection for the 2nd Phase

On September 24, 2001, the NESSIE project has announced the selection of candidates for the 2nd phase of the project. Central to the decision process has been the project goal, that is, to come up with a portfolio of strong cryptographic algorithms. Moreover, there was also a consensus that every algorithm in this portfolio should have a unique competitive advantage that is relevant to an application.

It is thus clear that an algorithm could not be selected if it failed to meet the security level required in the call. A second element could be that the algorithm failed to meet a security claim made by the designer. A third reason to eliminate an algorithm could be that a similar algorithm exists with better security (for comparable performance) or with significantly better performance (for comparable security). In retrospect, very few algorithms were eliminated because of performance reasons. It should also be noted that the selection was more competitive in the area of block ciphers, where many strong contenders were considered. The motivation for the decisions is given in [20].

Designers of submitted algorithms were allowed to make small alterations to their algorithms; the main criterion to accept these alterations is that they should improve the algorithm and not substantially invalidate the existing security analysis. More information on the alterations can be found on the NESSIE webpages [15].

The selected algorithms are listed below; altered algorithms are indicated with a *. Block ciphers:

- IDEA: MediaCrypt AG, Switzerland;
- Khazad*: Scopus Tecnologia S.A., Brazil and K.U.Leuven, Belgium;
- MISTY1: Mitsubishi Electric Corp., Japan;
- SAFER++64, SAFE++128: Cylink Corp., USA, ETH Zurich, Switzerland, National Academy of Sciences, Armenia;
- Camellia: Nippon Telegraph and Telephone Corp., Japan and Mitsubishi Electric, Japan;
- RC6: RSA Laboratories Europe, Sweden and RSA Laboratories, USA;
- Shacal: Gemplus, France.

Here IDEA, Khazad, MISTY1 and SAFER++64 are 64-bit block ciphers. Camellia, SAFER++128 and RC6 are 128-bit block ciphers, which will be compared to AES/Rijndael [5, 7]. Shacal is a 160-bit block cipher based on SHA-1 [6]. A 256-bit version of Shacal based on SHA-256 [17] has also been introduced in the second phase; this algorithm will be compared to an RC-6 and a Rijndael [5] variant with a block length of 256 bits (note that this variant is not included in the AES standard). The motivation for this choice is that certain applications (such as the stream cipher BMGL and certain hash functions) can benefit from a secure 256-bit block cipher.

Synchronous stream ciphers:

- SOBER-t16, SOBER-t32: Qualcomm International, Australia;
- SNOW*: Lund Univ., Sweden;
- BMGL*: Royal Institute of Technology, Stockholm and Ericsson Research, Sweden.

MAC algorithms and hash functions:

- Two-Track-MAC: K.U.Leuven, Belgium and debis AG, Germany;
- UMAC: Intel Corp., USA, Univ. of Nevada at Reno, USA, IBM Research Laboratory, USA, Technion, Israel, and Univ. of California at Davis, USA;
- Whirlpool*: Scopus Tecnologia S.A., Brazil and K.U.Leuven, Belgium.

The hash function Whirlpool will be compared to the new FIPS proposals SHA-256, SHA-384 and SHA-512 [17].

Public-key encryption algorithms:

- ACE-KEM*: IBM Zurich Research Laboratory, Switzerland (derived from ACE Encrypt);
- EPOC-2*: Nippon Telegraph and Telephone Corp., Japan;
- PSEC-KEM*: Nippon Telegraph and Telephone Corp., Japan (derived from PSEC-2);
- ECIES*: Certicom Corp., USA and Certicom Corp., Canada
- RSA-OAEP*: RSA Laboratories Europe, Sweden and RSA Laboratories, USA.

Digital signature algorithms:

- ECDSA: Certicom Corp., USA and Certicom Corp., Canada;

- ESIGN*: Nippon Telegraph and Telephone Corp., Japan;
- RSA-PSS: RSA Laboratories Europe, Sweden and RSA Laboratories, USA;
- SFLASH*: BULL CP8, France;
- QUARTZ*: BULL CP8, France.

Identification scheme:

- GPS*: Ecole Normale Supérieure, Paris, BULL CP8, France Télécom and La Poste, France.

Many of the asymmetric algorithms have been updated at the beginning of phase2. For the asymmetric encryption schemes, these changes were driven in part by the recent cryptanalytic developments, which occurred after the NESSIE submission deadline [8, 11, 23]. A second reason for these changes is the progress of standardization within ISO/IEC JTC1/SC27 [24]. The standards seem to evolve towards defining a hybrid encryption scheme, consisting of two components: a KEM (Key Encapsulation Mechanism), where the asymmetric encryption is used to encrypt a symmetric key, and a DEM (Data Encapsulation Mechanism), which protects both secrecy and integrity of the bulk data with symmetric techniques (a "digital envelope"). This approach is slightly more complicated for encryption of a short plaintext, but it offers a more general solution with clear advantages. Three of the five NESSIE algorithms (ACE Encrypt, ECIES and PSEC-2) have been modified to take into account this development. At the same time some other improvements have been introduced; as an example, ACE-KEM can be based on any abstract group, which was not the case for the original submission ACE Encrypt. Other submitters decided not to alter their submissions at this stage. For further details, the reader is referred to the extensive ISO/IEC draft document authored by V. Shoup [24]. The NESSIE project will closely monitor these developments. Depending on the progress, variants such as RSA-KEM defined in [24] may be studied by the NESSIE project.

For the digital signature schemes, three out of five schemes (ESIGN, QUARTZ and SFLASH) have been altered. In this case, there are particular reasons for each algorithm (correction for the security proof to apply, improve performance, or preclude a new attack). The other two have not been modified. It should also be noted that PSS-R, which offers very small storage overhead for the signature, has not been submitted to NESSIE.

7 Intellectual Property

An important element in the evaluation is the intellectual property status. While it would be ideal for users of the NESSIE results that all algorithms recommended by NESSIE were in the public domain, it is clear that this is for the time being not realistic. The users in the NESSIE PIB have clearly stated that they prefer to see royalty-free algorithms, preferably combined with open source implementations. However, providers of intellectual property typically have different views.

One observation is that in the past, there has always been a very large difference between symmetric and asymmetric cryptographic algorithms. Therefore it is not so surprising that NIST was able to require that the designers of the block cipher selected for the AES would give away all their rights, if their algorithm was selected; it is clear that this is not a realistic expectation for the NESSIE project. In this section we will attempt to summarize the intellectual property statements of the submissions retained for the 2nd phase. Note however that this interpretation is only indicative; for the final answer the reader is referred to the intellectual property statement on the NESSIE web page [15], and to the submitters themselves.

Twelve out of 24 algorithms are in the public domain, or the submitters indicate that a royalty-free license will be given. These are the block ciphers Khazad, Misty1, Shacal, Safer++, the stream ciphers BMGL, SNOW, Sober-t16 and Sober-t32, the MAC algorithms Two-Track-MAC and UMAC, the hash function Whirlpool, and the public-key algorithms RSA-OAEP[2] (public-key encryption) and

RSA-PSS[2] This statement does not hold for the variants of RSA with more than two primes.} (digital signature scheme).

Royalty-free licenses will be given for the block cipher Camellia, for the public-key encryption algorithms EPOC-2 and PSEC-KEM, and for the digital signature scheme ESIGN, provided that other companies with IPR to the NESSIE portfolio reciprocate.

The block cipher IDEA is free for non-commercial use only; for commercial applications a license is required.

Licenses under reasonable and non-discriminatory terms will be given for ACE-KEM (the detailed license conditions are rather complex). Additions to the `reasonable and non-discriminatory' terms are required for the public-key algorithms ECDSA and ECIES; it is required that the license holder reciprocates some of his rights.

For the digital signature schemes SFLASH and QUARTZ the licensing conditions are expected to be non-discriminatory, but no decision has been made yet. A similar statement holds for the identification scheme GPS, but in this case certain applications in France may be excluded from the license.

Finally, the submitters of RC6 are willing to negotiate licenses on reasonable terms and conditions.

It is clear that intellectual property is always a complex issue, and it will not be possible to resolve this completely within the framework of NESSIE. However, IPR issues may play an important role in the final selection process.

8 Dissemination and Standardization

8.1 An Open Evaluation Process

The NESSIE project intends to be an open project, which implies that the members of the public are invited to contribute to the evaluation process. In order to facilitate this process, all submissions are available on the NESSIE website, and comments are distributed through this website. In addition, three open workshops are organized during the project: the first two workshops have taken place in November 2000 and September 2001; the third one has been scheduled for November 2002.

8.2 The Project Industry Board

The Project Industry Board (PIB) was established to ensure that the project addresses real needs and requirements of industry dealing with the provision and use of cryptographic techniques and cryptographic products. The goals for the Board may be summarized as follows:

- contribute to dissemination: outwards through a member's contacts with industry and users, and also through passing NESSIE information into the member's own organization influencing products and directions;
- collaboration with the Project in formulation of the call and its goals and requirements;
- contribution to consensus building through influence and contacts in the industry and marketplace;
- identification of industry requirements from market needs and corporate strategies;
- guidance and judgment on the acceptability and relevance of submissions and evaluation results;
- support in standardization of NESSIE results;

[2] This statement does not hold for the variants of RSA with more then two primes.

- contribution to Project workshops;
- practical contributions to analysis and evaluation of submissions;
- identification of gaps in the scope of the submissions;
- ongoing guidance during the evaluation of the processes and validity of results.

Two meetings are held per year, but the PIB may request additional meetings to address specific issues or concerns that may arise. Membership was originally by invitation, but subsequently a number of additional companies have requested and obtained membership. Currently the PIB consists of about twenty leading companies which are users or suppliers of cryptology.

8.3 Standardization

Together with the NESSIE PIB, the project will establish a standardization strategy. It is not our intention to establish a new standardization body or mechanism, but to channel the NESSIE results to the appropriate standardization bodies, such as, ISO/IEC, IETF, IEEE and EESSI. We believe that the NESSIE approach of open evaluation is complementary to the approach taken by standardization bodies. Indeed, these bodies typically do not have the resources to perform any substantial security evaluation, which may be one of the reasons why standardization in security progresses often more slowly than anticipated.

The NESSIE project will also take into account existing and emerging standards, even if these have not been formally submitted to the NESSIE project. Two recent examples in this context come from the standardization efforts run by NIST: AES/Rijndael [5, 7] will be used as a benchmark for the other 128-bit block ciphers, and the NESSIE project will study the security and performance of the new SHA variants with results between 256 and 512 bits [17].

9 Conclusion

We believe that after two years, the NESSIE project has made important steps towards achieving its goals. This can be deduced from the high quality submissions received from key players in the community, and by the active participation to the workshops.

The first two years of the NESSIE project have also shown that initiatives of this type (such as AES, RIPE, CRYPTREC) can bring a clear benefit to the cryptographic research community and to the users and implementors of cryptographic algorithms. By asking cryptographers to design concrete and fully specified schemes, they are forced to make choices, to think about real life optimizations, and to consider all the practical implications of their research. While leaving many options and variants in a construction may be very desirable in a research paper, it is often confusing for a practitioner. Implementors and users can clearly benefit from the availability of a set of well defined algorithms, that are described in a standardized way.

The developments in the last years have also shown that this approach can result in a better understanding of the security of cryptographic algorithms. We have also learned that concrete security proofs are an essential tool to build confidence, particularly for public key cryptography (where constructions can be reduced to mathematical problems believed to be hard) and for constructions that reduce the security of a scheme to other cryptographic algorithms. At the same time, we have learned that it is essential to study proofs for their correctness and to evaluate the efficiency of such reductions.

Finally, the NESSIE project is inviting the community at large to further analyze the candidates for the 2nd phase, and to offer comments on their security, performance and intellectual property status. The project is accepting comments until mid November 2002, and the final selection will be announced by December 2002.

9.1 Acknowledgments

I would like to thank all the members of and the contributors to the NESSIE project. The work described in this paper has been supported by the Commission of the European Communities through the IST Programme under Contract IST-1999-12324.

References

[1] E. Biham, A. Shamir, "*Differential Cryptanalysis of the Data Encryption Standard*," Springer-Verlag, 1993.

[2] E. Biham, A. Shamir, "Differential fault analysis of secret key cryptosystems", *Advances in Cryptology, Proceedings Crypto'97, LNCS 1294*, B. Kaliski, Ed., Springer-Verlag, 1997, pp. 513-525.

[3] D. Boneh, R. A. DeMillo, R. J. Lipton, "On the importance of checking cryptographic protocols for faults", *Advances in Cryptology, Proceedings Eurocrypt'97, LNCS 1233*, W. Fumy, Ed., Springer-Verlag, 1997, pp. 37-51.

[4] CRYPTREC project, http://www.ipa.gov.jp/security/enc/CRYPTREC/index-e.html.

[5] J. Daemen, V. Rijmen, "*AES proposal Rijndael*," September 3, 1999, available from http://www.nist.gov/aes.

[6] FIPS 180-1, "*Secure Hash Standard*", Federal Information Processing Standard (FIPS), Publication 180-1, National Institute of Standards and Technology, US Department of Commerce, Washington D.C., April 17, 1995.

[7] FIPS XXX "*Advanced Encryption Standard (*AES)", Washington D.C.: NIST, US Department of Commerce, Draft, February 28, 2001.

[8] E. Fujisaki, T. Okamoto, D. Pointcheval, J. Stern, "RSA-OAEP is secure under the RSA assumption", *Advances in Cryptology, Proceeding Crypto'01, LNCS 2139*, J. Kilian, Ed., Springer-Verlag, 2001, pp. 260-274.

[9] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", *Advances in Cryptology, Proceedings Crypto'96, LNCS 1109,* N. Koblitz, Ed., Springer-Verlag, 1996, pp. 104-113.

[10] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis", *Advances in Cryptology, Proceedings Crypto'99, LNCS 1666,* M.J. Wiener, Ed., Springer-Verlag, 1999, pp. 388-397.

[11] J. Manger, "A chosen ciphertext attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as standardized in PKCS #1 v2.0", *Advances in Cryptology, Proceeding Crypto'01, LNCS 2139*, J. Kilian, Ed., Springer-Verlag, 2001, pp. 230-238

[12] M. Matsui, "The first experimental cryptanalysis of the Data Encryption Standard", *Advances in Cryptology, Proceeding Crypto'94, LNCS 839*, Y. Desmedt, Ed., Springer-Verlag, 1994, pp. 1-11.

[13] U. M. Maurer, "An universal statistical test for random bit generators", *Advances in Cryptology, Proceeding Crypto'90, LNCS 537*, S. Vanstone, Ed., Springer-Verlag, 1991, pp. 409-420.

[14] J. Menezes, P.C. van Oorschot, S. A. Vanstone, "*Handbook of Applied Cryptography*", CRC Press, 1997.

[15] NESSIE, http://www.cryptonessie.org.

[16] NIST, AES Initiative, http://www.nist.gov/aes.

[17] NIST, *"SHA-256, SHA-384, SHA-512,"* Washington D.C.: NIST, US Department of Commerce, Draft, 2000.

[18] NIST, *"A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications"*, NIST Special Publication 800-22, National Institute of Standards and Technology, US Department of Commerce, Washington D.C., December 2000.

[19] B. Preneel, B. Van Rompay, L. Granboulan, G. Martinet, S. Murphy, R. Shipsey, J. White, M. Dichtl, P. Serf, M. Schafheutle, E. Biham, O. Dunkelman, V. Furman, M. Ciet, J.-J. Quisquater, F. Sica, L. Knudsen, and H. Raddum, "*Security Evaluation I*", NESSIE Deliverable D13, September 2001, available from [15].

[20] B. Preneel, B. Van Rompay, L. Granboulan, G. Martinet, S. Murphy, R. Shipsey, J. White, M. Dichtl, P. Serf, M. Schafheutle, E. Biham, O. Dunkelman, V. Furman, M. Ciet, J.-J. Quisquater, F. Sica, L. Knudsen, and H. Raddum, "*NESSIE Phase I: Selection of Primitives*", NESSIE Report, September 2001, available from [15].

[21] B. Preneel, B. Van Rompay, L. Granboulan, G. Martinet, M. Dichtl, M. Schafheutle, P. Serf, A. Bibliovicz, E. Biham, O. Dunkelman, M. Ciet, J.-J. Quisquater, and F. Sica, "*Report on the Performance Evaluation of the NESSIE Candidates*", NESSIE Deliverable D14, October 2001, available from [15].

[22] RIPE, "*Integrity Primitives for Secure Information Systems. Final Report of RACE Integrity Primitives Evaluation (RIPE-RACE 1040)*"*, LNCS 1007*, A. Bosselaers, B. Preneel, Eds., Springer-Verlag, 1995.

[23] V. Shoup, "OAEP reconsidered", *Advances in Cryptology, Proceedings Crypto'01, LNCS 2139, J. Kilian, Ed., Springer-Verlag, 2001, pp.* 239-259.

[24] V. Shoup, "*A Proposal for an ISO Standard for Public Key Encryption*", Version 2.0, September 17, 2001, available from http://www.shoup.net.

About the author

Bart Preneel is a professor in the Electrical Engineering Department of the Katholieke Universiteit Leuven in Belgium, and is also a visiting professor at the Ruhr-Universitaet Bochum in Germany and at the University of Ghent in Belgium. His main research interests are cryptology and information security. Since 1987, he has been involved in a large number of projects and security studies on banking and telecommunications systems. He is a Director of the International Association of Cryptologic Research (IACR). He has been program chair of the RSA Security Cryptographer's Track 2002, Eurocrypt 2000, FSE'94 and CMS'99. Homepage: http://www.esat.kuleuven.ac.be/~preneel