NESSIE: A European Approach to Evaluate Cryptographic Algorithms

Bart Preneel

Katholieke Univ. Leuven, Dept. Electrical Engineering-ESAT,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
bart.preneel@esat.kuleuven.ac.be

Abstract. The NESSIE project (New European Schemes for Signature, Integrity and Encryption) intends to put forward a portfolio containing the next generation of cryptographic primitives. These primitives will offer a higher security level than existing primitives, and/or will offer a higher confidence level, built up by an open evaluation process. Moreover, they should be better suited for the constraints of future hardware and software environments. In order to reach this goal, the project has launched an open call in March 2000. In response to this call, 39 primitives have been submitted by September 29, 2000, many of these from major players. Currently, the NESSIE evaluation process is under way; it considers both security and performance aspects. This article presents the status of the NESSIE project after 15 months.

1 Introduction

NESSIE 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 1st January 2000. This paper intends to present the state of the project in April 2000. It is organised as follows. Section 2 presents 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. Section 6 raises some intellectual property issues. The NESSIE approach towards dissemination and standardisation is presented in Sect. 7. Finally, conclusions are put forward in Sect. 8.

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

M. Matsui (Ed.): FSE 2001, LNCS 2355, pp. 267–276, 2002.

2 NESSIE Call

In the first year of the project, an open call for the submission of cryptographic primitives, as well as for evaluation methodologies for these primitives has been launched. The scope of this call has been defined together with the project industry board (PIB) (cf. Sect. 7), and it was published in March 2000. The deadline for submissions was 29 September 2000. In response to this call NESSIE received 40 submissions, all of which met the submission requirements.

2.1 Contents of the NESSIE Call

The NESSIE call includes a request for a broad set of primitives providing confidentiality, data integrity, and authentication. These primitives include block ciphers, stream ciphers, hash functions, MAC algorithms, digital signature schemes, and public-key encryption and identification schemes (for definitions of these primitives, see [17]). In this respect the NESSIE call is very similar to the two calls of RIPE (Race Integrity Primitives Evaluation, 1988-1992) [20]. In addition, the NESSIE call asks for evaluation methodologies for these primitives.

It has been stressed that not only block ciphers are needed, but also several other primitives such as stream ciphers, MACs, etc. (since there are many block ciphers around but far fewer other primitives even though they are required in many applications). Thus the scope of this call is much wider than that of the AES call launched by NIST in 1997.

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 primitive is essential to achieve confidence and to build consensus.

For the *security requirements* of symmetric primitives, two main security levels are specified, named *normal* and *high*. The minimal requirements for a symmetric primitive to attain either the normal or high security level depend on the key length, internal memory, or output length of the primitive. 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. Remark that the AES call only specifies a 128-bit block size. For the asymmetric primitives the security level is specified in terms of the computational effort of the most efficient attack.

If selected by NESSIE, the primitive 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 primitives 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. The results of the call seem promising, and will lead to a very interesting and challenging evaluation process. There are 26 symmetric primitives:

- 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 organised 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
  - three 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 primitives have been submitted:

- five asymmetric encryption schemes: ACE Encrypt, ECIES, EPOC, PSEC, and RSA-OAEP;
- 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 13–14 November 2000 the first NESSIE workshop was organised in Leuven (Belgium), where 35 submissions were presented. All submissions are available on the NESSIE web site.

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

3 Tools

It would be rather naive to believe that modern computers and sophisticated software tools can replace human cryptanalysis. Nevertheless, software plays 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 execution of the attack is done on a computer. However, software and software tools can also be essential to find a successful way to attack a 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 analysed. Special tools, which are specific for the analysis of one algorithm, will be implemented when, in the course of the cryptanalysis of an algorithm, the need for such a tool turns up.

For the evaluation of the NESSIE 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) project [20]. These test include: the frequency test, the collision test, the overlapping m-tuple test, the gap test, the constant runs test, the coupon collector's test, Maurer's universal test [16], 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 analyse block ciphers with differential [5] and linear cryptanalysis [15]. This tool is based on a general description language for block ciphers. Other tools under development comprise tools for related key attacks [3] and tools for χ^2 cryptanalysis [21].

In September 2000, the US NIST published a suite of statistical tests for the evaluation of sequences of random or pseudorandom bits; this document has been revised in December 2000 [19]. A careful comparison will be 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

4.1 Methodology

We first describe the internal process within NESSIE used to assess submissions. Initially each submission was assigned to a NESSIE partner. The NESSIE partner 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

did require 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. Clearly, any future assessment of a submission will depend on this joint summary, but it is generally anticipated that the two NESSIE partners would then further jointly assess the submission.

It is anticipated that the report published at the end of the first phase of the security evaluation (August 2001) will contain a security assessment of the primitives against standard cryptanalytic techniques, the results of statistical testing (where appropriate) and an indication of types of future assessment to be carried out. This preliminary assessment will include a rationale for submissions rejected at this stage.

4.2 First Results

In the short time available for analysis so far, there have been significant results concerning some submissions. The analyses of the block ciphers Q [4] and Nimbus [12] and of the next bit testing methodology already indicate that they are not suitable for recommendation by the NESSIE project. The 'SQUARE' type attack on Hierocrypt-3 and Hierocrypt-L1 described by the designers has been improved [2]. There are also some external preliminary results concerning Leviathan [8], LILI-128 [1], and NUSH. However, it should be stressed that at the time of writing of this paper (March 2001), the assessment process is at a very early stage.

5 Performance Evaluation

5.1 Background and Motivation

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., banking applications, cellular phones); for other applications a high throughput is essential (e.g., high speed networking, hard disk encryption).

5.2 The Methodology

First a framework has been defined to compare the performance of primitives on a fair and equal basis. It will be used for all evaluations of submitted candidates or asymmetric primitives, for block ciphers as well as stream ciphers, hash functions, etc.

First of all a theoretical approach has been established. For each candidate we will dissect the algorithm into three parts: setup (independent of key and data), precomputations (independent of data, e.g., key schedule) and the primitive 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 PCs, smart cards, 64-bit machines and FPGAs. The implementations 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 primitives.

The project will also consider the resistance of implementations to physical attacks such as timing attacks [13], fault analysis [6,7], and power analysis [14].

For non constant-time algorithms (data or key dependence, asymmetry between encryption and decryption) the data or key dependence will be analysed; other elements that will be taken into account include the difference between encryption and decryption, and between signature and verification operation. For symmetric primitives, the key agility will also be considered.

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

5.3 Template for Performance Evaluation

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. It is presented as a questionnaire, which can be completed by analyzing the primitive and the software for the primitive. A first part describes parameters such as word size, memory requirement, key size and code size. Next the basic operations are analysed, 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.) is described. Elements such as the dependence on the keys and on the inputs determine whether the code is constant-time or not.

6 Intellectual Property

An important element of the call is the intellectual property statement of the submitters. While it were 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 primitives, preferably combined with open source implementations. However, providers of intellectual property, who are also represented in the PIB, typically have different opinions.

One observation is that in the past, there has always been a very large difference between symmetric and asymmetric cryptographic primitives. 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 summarise the intellectual property statements of the submitters. 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, and to the submitters themselves.

Nineteen out of 39 submissions are in the public domain, or the submitters indicate that a royalty-free license will be given. These are the block ciphers Anubis, CS-Cipher, Grand Cru, Khazad, Misty1, Nimbus, Noekeon, Nush, Q, Shacal, Safer++, the stream ciphers BMGL, LILI-128 and SNOW, the MAC algorithms Two-Track-MAC and UMAC, the hash function Whirlpool, and the public-key primitives RSA-OAEP[2] (public-key encryption) and RSA-PSS[2] (digital signature scheme).

The block cipher IDEA is free for non-commercial use only; for commercial applications a license is required. The stream ciphers SOBER-t16 and SOBER-t32 are royalty-free in non-embedded applications, but licenses are required for embedded applications.

Licenses under reasonable and non-discriminatory terms will be given for the block ciphers Camellia, Hierocrypt-L1, Hierocrypt-L3 and SC2000, the stream cipher Leviathan[3], and for the public-key encryption algorithms EPOC and PSEC and the digital signature scheme ESIGN. Similar conditions hold for ACE Crypt and ACE Sign, but in this case the detailed license conditions are rather complex (that is, they cannot be summarised in a few words). Additions to the 'reasonable and non-discriminatory' terms are required for the public-key primitives ECDSA and ECIES; it is required that the license holder reciprocates some of his rights.

For the digital signature schemes FLASH, 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. The call

[2] This statement does not hold for the variants of RSA with more than two primes.
[3] If this algorithm is recommended by NESSIE.

for papers for the second NESSIE workshop will definitely invite comments on this issue.

7 Dissemination and Standardisation

7.1 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. The NESSIE website contains an open forum where everyone can post contributions on the primitives and on the process. In addition, three open workshops are organised during the project; the first one has taken place in November 2000. The second workshop has been scheduled for September 12-13, 2001 (University of London, Egham, UK), and the third one for the Fall of 2002.

7.2 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. Two meetings are planned per year, but additional meetings may be held to address specific issues or concerns that may arise.

Membership was originally by invitation, but there have been a number of subsequent requests to join the PIB. Currently it consists of about twenty-five leading companies which are users or suppliers of cryptology. During the first year, the PIB has provided very useful input to all aspects of the NESSIE project.

7.3 Standardisation

Together with the NESSIE PIB, the project will establish a standardisation strategy. It is not our intention to establish a new standardisation body or mechanism, but to channel the NESSIE results to the appropriate standardisation bodies, such as, ISO/IEC, IETF, IEEE and EESSI (European Electronic Signature Standardisation Initiative). We believe that the NESSIE approach of open evaluation is complementary to the approach taken by standardisation bodies. Indeed, these bodies typically do not have the resources to perform any substantial security evaluation, which may be one of the reasons why standardisation 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 standardisation efforts run by NIST. The NESSIE project has contributed to the AES process, and one of the designers of the AES algorithm 'Rijndael' [9,11] is a member of the NESSIE project team. It is therefore clear that in the evaluation of block ciphers, the

Rijndael algorithm will be used as a benchmark. The NESSIE project will also study the security and performance of SHA-2 [18], the new hash algorithm proposed by NIST to extend the result of SHA-1 [10] to hash results between 256 and 512 bits.

8 Conclusion

We believe that the approach of the NESSIE project provides an interesting approach to provide the users with the next generation of cryptographic algorithms, and to stimulate further research on cryptographic algorithms.

The NESSIE evaluation process will be delicate and complex, but we are confident that the project will be able to live up to the expectations. In the first months of the evaluation, several research papers have been written by project members describing cryptanalytic results of the NESSIE project, and several comments were received from other cryptographers.

We invite the readers of this article to contribute towards the NESSIE project by sending comments on individual algorithms, on the evaluation process, and on their expectations towards the project results.

Acknowledgments. I would like to thank all the members of the NESSIE project, and more in particular the contributors to the first annual report, on which this text is largely based: Eli Biham, Antoon Bosselaers, Mathieu Ciet, Markus Dichtl, Louis Granboulan, Keith Howker, Lars Knudsen, Sean Murphy, François Koeune, and Francesco Sica.

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.

Disclaimer

The information in this paper is provided as is, and no guarantee or 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.

References

1. S. Babbage, "Cryptanalysis of LILI-128," Preprint, 2001.
2. P. Barreto, V. Rijmen, J. Nakahara Jr., B. Preneel, J. Vandewalle, H. Kim, "Improved Square attacks against reduced-round Hierocrypt," *Preproceedings Fast Software Encryption 2001*, M. Matsui, Ed.
3. E. Biham, "New types of cryptanalytic attacks using related keys," *Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765*, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 398–409.
4. E. Biham, V. Furman, M. Misztal, V. Rijmen, "Differential Cryptanalysis of Q," *Preproceedings Fast Software Encryption 2001*, M. Matsui, Ed.

5. E. Biham, A. Shamir, *"Differential Cryptanalysis of the Data Encryption Standard,"* Springer-Verlag, 1993.
6. 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.
7. 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.
8. P. Crowley, S. Lucks, "Bias in the Leviathan stream cipher," *Preproceedings Fast Software Encryption 2001*, M. Matsui, Ed.
9. J. Daemen, V. Rijmen, "AES proposal Rijndael," September 3, 1999, available from `http://www.nist.gov/aes`.
10. 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.
11. FIPS XXX *"Advanced Encryption Standard (AES),"* Washington D.C.: NIST, US Department of Commerce, Draft, February 28, 2001.
12. V. Furman, "Differential cryptanalysis of Nimbus," *Preproceedings Fast Software Encryption 2001*, M. Matsui, Ed.
13. 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.
14. 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.
15. M. Matsui, "The first experimental cryptanalysis of the Data Encryption Standard," *Advances in Cryptology, Proceedings Crypto'94, LNCS 839*, Y. Desmedt, Ed., Springer-Verlag, 1994, pp. 1–11.
16. U.M. Maurer, "A universal statistical test for random bit generators," *Advances in Cryptology, Proceedings Crypto'90, LNCS 537*, S. Vanstone, Ed., Springer-Verlag, 1991, pp. 409–420.
17. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *"Handbook of Applied Cryptography,"* CRC Press, 1997.
18. NIST, *"SHA-256, SHA-384, SHA-512,"* Washington D.C.: NIST, US Department of Commerce, Draft, 2000.
19. 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.
20. 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.
21. S. Vaudenay, "An experiment on DES – statistical cryptanalysis," *Proceedings 1996 ACM Conference on Computer and Communications Security*, March 14-15, New Delhi, India, 1996, pp. 139–147.