Portfolio of recommended cryptographic primitives

NESSIE consortium[⋆]

February 27, 2003

1 Introduction

This document presents and motivates the NESSIE portfolio of recommended cryptographic primitives. Further technical information supporting these decisions can be found in the NESSIE security [1] and performance [2] evaluation documents.

The information in this document 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.

2 Block Cipher Encryption Schemes

2.1 64-bit Block Ciphers

NESSIE portfolio. The 64-bit block cipher included in the NESSIE portfolio is MISTY1.

- The NESSIE project did not find an attack on MISTY1. Furthermore, MISTY1 is similar to the block cipher KASUMI, so much of the analysis for KASUMI would also be applicable to MISTY1. KASUMI has been scrutinised prior to its adoption as a 3GPP standard. However, many NESSIE partners are concerned that the simple algebraic structure of MISTY1 may lead to future breakthroughs in the analysis of MISTY1.

Comments on the other 64-bit block ciphers studied in Phase II.

- No attacks were found on Khazad and in the opinion of the NESSIE project it is an interesting primitive for future research. However, concerns were expressed with regard to the structural symmetry of Khazad.
- The NESSIE project did not find an attack on IDEA. However, it was not selected because of Intellectual Property Rights issues and some concerns about its key schedule.
- The NESSIE project did not find an attack on SAFER$_{++64}$. However, SAFER$_{++64}$ was not selected because there were some concerns about certain structural properties of SAFER$_{++64}$, as discussed in the NESSIE Security Evaluation Report. It was also found to be slower than the other ciphers except in smart cards.
- The NESSIE project considers 3-DES to be a secure but slow block cipher.

[⋆] `http://www.cryptonessie.org`

2.2 128-bit Block Ciphers

NESSIE portfolio. The 128-bit block ciphers included in the NESSIE portfolio are the AES and Camellia.

- The AES has been scrutinised by the U.S. National Institute of Standards and Technology as a secure block cipher and adopted as a U.S. Federal Information Processing Standard. Camellia has many similarities to the AES, so much of the analysis for the AES is also applicable to Camellia. It is also the case that the NESSIE project did not find an attack on either the AES or Camellia. However, the NESSIE partners, as well as the wider cryptographic community, have a wide range of views about the AES and Camellia. Many NESSIE partners have significant concerns that the simple algebraic structure of the AES, and to a somewhat lesser extent Camellia, may lead to future breakthroughs in the analysis of these block ciphers.

Comments on the other 128-bit block ciphers studied in Phase II.

- The NESSIE partners felt unable to consider the selection of RC6 owing to ongoing serious Intellectual Property Rights issues.
- The NESSIE project did not find an attack on SAFER$_{++128}$. However, the NESSIE project did not select SAFER$_{++128}$ because of some concerns, both about certain structural properties of SAFER$_{++128}$ and about the low security margin of SAFER$_{++128}$, as discussed in the NESSIE Security Evaluation Report.

2.3 256-bit Block Ciphers

NESSIE portfolio. The 256-bit block cipher included in the NESSIE portfolio is SHACAL-2.

Comments on the other block ciphers with block length larger than 128 bits studied in Phase II.

- The NESSIE partners felt unable to consider the selection of RC6 owing to ongoing serious Intellectual Property Rights issues.
- The NESSIE project did not select SHACAL-1 because of concerns about its key schedule.

3 Stream Ciphers and Pseudorandom Number Generators

NESSIE portfolio. The NESSIE portfolio in this category is empty.

Comments on the stream ciphers studied in Phase II.

- NESSIE does not recommend SNOW for encryption, because there are distinguishing attacks and guess and determine attacks faster than exhaustive key search.
- For SOBER-t16 and SOBER-t32 there are distinguishing attacks faster than exhaustive key search. Owing to the irregular decimation of SOBER-t16 and SOBER-t32 there are certain reservations with respect to the vulnerability of implementations of these algorithms with respect to side-channel attacks. NESSIE, therefore, does not recommend either primitive.

- The first drawback of BMGL is its small internal state, which makes it vulnerable to a time-memory tradeoff attack. In addition, BMGL is too slow for encryption, so NESSIE does not recommend BMGL.

4 Collision-Resistant Hash Functions

NESSIE portfolio. The collision-resistant hash functions included in the NESSIE portfolio are Whirlpool, SHA-256, SHA-384 and SHA-512.

- The NESSIE project selects Whirlpool as a collision-resistant hash function, with an output length of 512 bits. The design of Whirlpool is based on an underlying 512-bit block cipher that is used in Miyaguchi-Preneel mode. This block cipher has a structure similar to Rijndael. The best known attack on Whirlpool finds non-random properties when the compression function is reduced to six rounds or less (out of ten); this gives a good security margin. The performance of Whirlpool is acceptable, though on most platforms it is slightly slower than SHA-512.
- The NESSIE project selects SHA-256, SHA-384 and SHA-512 as collision-resistant hash functions, with an output length of 256, 384 or 512 bits. These primitives have recently been added to the NIST standard for hash functions. In contrast to the AES process this was not an open standardisation process and the design strategy was not made public. These primitives are rather new designs that have some similarities to SHA-1 but there are important differences in the structure. They were not submitted to NESSIE and owing to a lack of resources only limited evaluation has been performed. Current results indicate no security problems and these primitives seem to have a large security margin against known attacks. The performance of these primitives is acceptable, SHA-512 and SHA-384 being slightly faster than Whirlpool on most platforms. SHA-256 is about twice as fast on most platforms.

No security weaknesses were found for these primitives. However, Whirlpool, SHA-256, SHA-384 and SHA-512 are newly designed primitives which have undergone only limited evaluation by the cryptographic community so far.

NESSIE comments on “legacy” hash functions. The standard primitives SHA-1 and RIPEMD-160 do not meet the NESSIE security requirement for symmetric primitives, because their output is only 160 bits, but they can be recommended for applications where this security level is sufficient.

5 Message Authentication Codes

NESSIE portfolio. The message authentication codes included in the NESSIE portfolio are UMAC, TTMAC, EMAC and HMAC.

- For the authentication of long message streams UMAC is by far the fastest of the MAC primitives considered by NESSIE (at the cost of greater complexity and worse key-agility compared to the other primitives). UMAC is based on universal hash function families and has provable security: a break of the primitive would imply a break of the block cipher that is used by the scheme as a pseudo-random function (the current specification chooses AES as block cipher).

– TTMAC (also known as Two-Track-MAC) has the highest security level of the MAC primitives considered by NESSIE. The design of TTMAC is based on the hash function RIPEMD-160 (with small modifications). The security can be proven on the assumption that the underlying compression function is pseudo-random. TTMAC has specific performance advantages: it is especially efficient in the case of short messages, and has optimal key-agility.

– EMAC (also known as DMAC) has the advantage that it allows the reuse of an existing block cipher implementation (in CBC-mode with an extra encryption as output transformation). The security can be proven on the assumption that the underlying block cipher is pseudo-random. The performance and key-agility are reasonable (EMAC is preferable for short messages because the block length is smaller compared to the schemes based on a hash function). NESSIE recommends the use of this construction with a 128-bit block cipher included in the NESSIE portfolio.

– HMAC has the advantage that it allows the reuse of an existing hash function implementation. The security can be proven on the following assumptions: the underlying hash function is collision-resistant for a secret initial value; the compression function keyed by the initial value is a secure MAC primitive (for messages of one block); the compression function is a weak pseudorandom function. These assumptions are weaker than the assumptions required for TTMAC and EMAC. The performance and key-agility are reasonable. NESSIE recommends the use of this construction with a collision-resistant hash function included in the NESSIE portfolio.

No security weaknesses were found for any of these primitives. NESSIE makes a broad recommendation in this area because every primitive has its own specific advantages.

6 Asymmetric encryption schemes

NESSIE portfolio. The asymmetric encryption schemes included in the NESSIE portfolio are PSEC-KEM, RSA-KEM and ACE-KEM.

– The primary recommendation is PSEC-KEM. Its security is based on the Computational Diffie-Hellman assumption with an efficient proof of security. From a performance point of view, it compares favourably with other schemes that offer a similar security level. The elliptic curve should be carefully chosen and the base field should be at least of size 160 bits, which should be sufficient for medium term security (5 to 10 years). A prime field is preferable, unless implementation constraints favour a field of characteristic 2.

– A secondary recommendation is RSA-KEM with exponent at least 65537 and public keys of at least 1536 bits, which should be sufficient for medium term security (5 to 10 years). Exponent 3 can be used if fast encryption is important. Its security is based on the RSA assumption with an efficient proof, but it has a relatively slow decryption and longer keys than PSEC-KEM. It may be more difficult to protect implementations of RSA-KEM against side-channel attacks than implementations of PSEC-KEM.

– ACE-KEM is recommended where performance is not critical. It has several provable security arguments, and therefore its security is better than that of the other encryption schemes. Depending on the application, either a 160-bit (or more) elliptic curve or a 1536-bit (or more) prime field can be used.

Comments on the other asymmetric encryption schemes studied in Phase II.

- ECIES and ECIES-KEM have slightly better performance than PSEC-KEM, but the Gap Diffie-Hellman security assumption makes the security proof less convincing than PSEC-KEM.
- EPOC-2 compares unfavourably with Rabin-based schemes such as HIME(R) and Rabin-SAEP.

NESSIE recommendation if very long term security is important. For very high level security we note that double encryption using ACE-KEM and RSA-KEM with different DEMs gives a good range of security, based on various different assumptions. Triple encryption that also uses a public-key scheme not based on number-theoretical assumptions might increase the security against future breakthrough.

7 Digital signature schemes

NESSIE portfolio. The digital signature schemes included in the NESSIE portfolio are RSA-PSS, ECDSA and SFLASH.

- The primary recommendation is a digital signature scheme based on the RSA-PSS submission to NESSIE with exponent at least 65537 and public keys of at least 1536 bits, which should be sufficient for medium term security (5 to 10 years). Exponent 3 can be used if fast verification is important.
- A secondary recommendation is ECDSA. This scheme is well suited to applications where the signing time or the appendix length are important. The elliptic curve should be carefully chosen and the base field should be at least of size 160 bits, which should be sufficient for medium term security (5 to 10 years). A prime field is preferable, unless implementation constraints favour a field of characteristic 2.
- SFLASH is not recommended for general use but this signature scheme is very efficient on low cost smart cards, where the size of the public key is not a constraint.

If this causes no interoperability problems, a tweak of the submitted schemes is strongly recommended. One should include some certification data in the inputs of the hash functions. This would bind the scheme parameters, public key and expiration time, to a particular signature. (This was a proposal of the KCDSA scheme.)

Comments on the other digital signature schemes studied in Phase II.

- The ESIGN family of digital signature schemes has convincing security and some performance advantages, but RSA-PSS and ECDSA have more convincing security and cover most common applications. Both ESIGN-D and ESIGN-R may be suited to specific uses.
- QUARTZ does not meet our security requirements for the submitted parameters. A modification of the parameter d might be sufficient, but is not fully evaluated. Still, if a digital signature scheme with appendix shorter than 250 bits is needed, QUARTZ with a larger d can be used.

NESSIE recommendation if very long term security is important. Use simultaneously different digital signature schemes, based on different mathematical assumptions and distinct hash functions.

8 Asymmetric Identification Schemes

NESSIE portfolio. The asymmetric identification scheme included in the NESSIE portfolio is GPS.

- GPS is the only primitive submitted to NESSIE in the category of asymmetric identification schemes and has good performance with high security. It compares favourably with the other zero-knowledge identification schemes that have been described in the literature. For medium term security (5 to 10 years) the modulus should have at least 1536 bits and the other parameters as recommended by the submitters of the scheme. The flexibility of GPS allows this scheme to be used in a variety of situations, and different security parameters might be appropriate.
  A trivial protocol flaw was found in the original submitted version, and was corrected. Implementations of GPS should not forget any item of the protocol, as a mistake may have serious security implications.

References

1. NESSIE consortium, “Security Report,” Version 2.0, February 19, 2003.
2. NESSIE consortium, “Performance Report,” Version 2.0, February 19, 2003.