Race Integrity Primitives Evaluation (RIPE): A status report

B. Preneel*
ESAT Lab, K.U.Leuven

D. Chaum
C.W.I., Amsterdam

W. Fumy
Siemens AG, Erlangen

C.J.A. Jansen
Philips Crypto B.V., Eindhoven

P. Landrock
Århus University

G. Roelofsen
PTT Research, The Netherlands

Abstract

Early in 1989, a call for integrity primitives was disseminated within the cryptographic community by the RIPE consortium. The goal of this consortium is to put forward an ensemble of techniques to meet the anticipated requirements of the future Integrated Broadband Communication Network in the European Community. The aim of this paper is to describe the status of the RIPE project.

1 Integrated Broadband Communication for Europe

The European Community plans to set up a unified European market of about 300 million customers by 1993. In view of this market Integrated Broadband Communication (IBC) is planned for commercial use in 1996. This communication network will provide high speed channels and will support a broad spectrum of services. In order to pave the way towards commercial use of IBC, the Commission of the European Communities has launched the RACE program (Research and Development in Advanced Communications Technologies in Europe) [RACE88]. Under this RACE program pre-competitive and pre-normative work is going on.

*NFWO aspirant navorser, sponsored by the National Fund for Scientific Research (Belgium).

D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 547-551, 1991.

It is clear that the majority of the services offered as well as the management of the network are crucially dependent on the use of cryptographic techniques for their security.

Within RACE, the RIPE project (RACE Integrity Primitives Evaluation) will put forward a portfolio of techniques to meet the anticipated security requirements of IBC. Consensus on integrity primitives is essential for interoperability. The members of the RIPE project are: Centre for Mathematics and Computer Science, Amsterdam (prime contractor); Siemens AG; Philips Crypto BV; PTT Research, The Netherlands; Katholieke Universiteit Leuven and Århus Universitet.

2 An open call for integrity primitives

The project's motivation is the unique opportunity to attain consensus on openly available integrity primitives. In order to achieve wide acceptance for a collection of algorithms, the RIPE consortium decided to disseminate an open call [VdW89]. The scope of the project and the evaluation procedure were fixed after having reached consensus with the main parties involved.

The scope includes any digital integrity primitive, except data confidentiality. In this context it is important to note that in some documents (e.g. [ISO7498]) integrity is *not* the complement of confidentiality, but has a very restricted meaning.

In response to the call, that was announced at Eurocrypt'89 and Crypto'89 and was published in the Journal of Cryptology and the IACR Newsletter, fifteen submissions were received. Most types of primitives were represented, but three additional primitives were invited for more comprehensive coverage. In fact, many well known primitives were ultimately submitted, as well as proprietary submissions from major suppliers, thus demonstrating the widespread acceptance and perceived need for the project.

From the eighteen submissions, ten came from academic submitters and eight from industry. The division over different countries was as follows: West Germany 5; U.S.A. 4; Denmark 3; Canada and Japan 2; Belgium and Australia 1. In October 1989, many of the submitters attended special meetings to clarify the submissions.

3 Evaluation results

The evaluation was carried out following a fixed procedure. In view of the potential use in IBC the submissions were evaluated with respect to three aspects: functionality, modes of use, and performance. The evaluation comprised computer simulation, statistical verification and analysis of mathematical structures, particularly to verify the integrity properties. Because of the limited resources and time period, it was decided that if any flaw was identified, the submitter would not be allowed to patch the flaw, thus preventing a moving target.

The submissions can roughly be divided into four categories: identification protocols, digital signatures, hash functions and keyed hash functions. Note that a single submission can contain primitives in more than one category. Five submissions could be rejected in a preliminary screening. After the main phase of the evaluation and after taking into account deficiencies implied by work done in the cryptographic community (external work), seven submissions remained. The reader is referred to table 1 that indicates how the different categories evolved through the evaluation process.

	Identification Protocols	Digital Signatures	Hash Functions	Keyed Hash Functions
Total number	6	3	14	8
After first phase	6	3	9	3
After main phase	3	2	4	1
External work	3	2	2	0

Table 1: Evolution of the number of submissions in different categories.

The remaining submissions show significant potential, but each requires modification and/or further specification by the submitters. Five of these seven show minor functional problems. In most of the cases, it is clear how these problems can be avoided. It was however decided to stick to the agreed policy and perform further evaluation together with the new submissions from the second call. One primitive was incompletely specified and one primitive needs more analysis before it can be recommended. More details on the promising submissions are given in table 2.

For six submissions permission was obtained from the submitters to publish the

	Identification Protocols	Digital Signatures	Hash Functions	Keyed Hash Functions
Total remaining	3	2	2	0
Minor functional problems	3	1	1	0
Incomplete specification	0	1	0	0
More analysis required	0	0	1	0

Table 2: Problems concerning submissions showing significant potential.

evaluation or attack by the RIPE consortium. Preprints of the reports [RIPE91-1, RIPE91-2, RIPE91-3, RIPE91-4, RIPE91-5, dRo91] are available from: Gert Roelofsen, PTT Research, P.O.Box 421, NL-2260 AK Leidschendam, The Netherlands. Telephone +31(70)332 64 10; Fax +31(70)332 64 77; Telex 311236 rnl nl; email g_roelofsen@pttrnl.nl. Note also that the version of MD4 submitted to the RIPE consortium differs in some details from the published version [Riv90].

4 Second call for integrity primitives

In 1989, it was already foreseen that some first round submissions would require fixing of functional problems. Moreover, the period of 9 months between announcement of the call and the deadline for submission was relatively short. A final argument for a second call is that work on functional specifications for security within RACE had started only in 1989.

In order to assure that the recommended integrity primitives result in a comprehensive coverage of IBC requirements, following sources for primitives will be taken into account in the second evaluation phase: the responses to the second call, the revised versions of the first round primitives believed to be promising after the first evaluation and other primitives proposed in open literature and in the international standards community. Finally, if necessary, some submissions might be invited.

5 Conclusion

The first call for primitives and the subsequent evaluation process was certainly successful. On one hand, important flaws were identified in several submitted

schemes, and on the other hand a selection of seven submissions showing significant potential survived. The need for a second call for integrity primitives has been demonstrated. The results of the second evaluation phase will be available by July 1992.

References

[ISO7498] *"Information Processing - OSI Reference Model - Part 2: Security architecture*, International Standard ISO 7498/2, International Organisation for Standardisation, 1988.

[VdW89] J. Vandewalle, D. Chaum, W. Fumy, C.J.A. Jansen, P. Landrock and G. Roelofsen, "A European call for cryptographic algorithms: RIPE; Race Integrity Primitives Evaluation", *Proceedings Eurocrypt'89, Lecture Notes in Computer Science 434*, Springer Verlag, 1990, p. 267-271.

[RACE88] *"RACE Workplan"*, Commission of the European Communities, 1988, Rue de la Loi 200, B-1049, Brussels, Belgium.

[RIPE91-1] *"Evaluation of N-HASH"*, RIPE Internal Report 1991-1, 1991.

[RIPE91-2] *"Evaluation of a hash function based on modular squaring"*, RIPE Internal Report 1991-2, 1991.

[RIPE91-3] *"Evaluation of a hash function based on 32-bit arithmetic"*, RIPE Internal Report 1991-3, 1991 (can not be published before March 1992).

[RIPE91-4] *"Evaluation of LOKI"*, RIPE Internal Report 1991-4, 1991.

[RIPE91-5] *"Evaluation of MD4 (as submitted to RIPE)"*, RIPE Internal Report 1991-5, 1991.

[dRo91] Peter J.N. de Rooij, "On the Security of the Schnorr scheme using preprocessing", *these proceedings.*

[Riv90] R.L. Rivest, "The MD4 Message Digest Algorithm", *Abstracts Crypto'90*, pp. 281-291.