How to Use RSA; or How to Improve the Efficiency of RSA Without Loosing its Security (Extended Abstract)

[Published in U. Schulte, Ed., *ISSE 2002*, on CD-ROM, Paris, France, October 2–4, 2002.]

Marc Joye and Pascal Paillier

Gemplus Card International, France
{marc.joye, pascal.paillier}@gemplus.com
http://www.gemplus.com/smart/

Abstract. It is striking to observe the progressive explosion of RSA key lengths. Although this trend clearly corresponds to a (legitimate) ever-increasing need for a guaranteed security level, this paper considers alternative, more efficient, secure implementations of RSA with respect to industrial constraints.

Keywords. RSA cryptosystem, factorization, NFS, ECM, key sizes.

1 Better RSA Moduli without Security Loss

The RSA cryptosystem [14] is still a de-facto standard in all branches of public-key cryptography. However, it is rapidly loosing its attractiveness. This is mainly due to the enormous key lengths necessary to make RSA secure.

Recently, following a report by Lenstra and Verheul (now published in [11]), several organizations suggested to increase the key size of an RSA modulus up to 2048 bits. Even though hardware-enhanced programmable devices such as smart card cryptographic processors are becoming more and more efficient over time, our feeling is that considerable research efforts in the field could be saved by the simple fact of allowing several prime factors to appear in the factorization of RSA moduli. For example, one can envision to perform an RSA exponentiation with a 2048-bit modulus of the form $N = pqrs$ where p, q, r, s are 512-bit primes. Another possible choice is a modulus of the form $N = p^k q$ (see [17]).

We stress that the security level of RSA in such a case remains completely unchanged unless major scientific discoveries (new factoring algorithms) are carried out in the field of integer factorization. Indeed, the current state of the art includes two main families of factorization algorithms. The first family presents a running time which depends on the total length of the number to be factored while the running time of algorithms belonging to the second family only depends on the length of the factors. The most popular representative of the first family is the number field sieve (NFS). The second family includes the elliptic curve method (ECM). The main threat for RSA comes from the first family of factorization algorithms and more particularly NFS and its variants. A factor of 512 bits is really beyond the scope of ECM.

2 Better RSA Public Exponents without Security Loss

For historical reasons, there is a confusion between the *RSA primitive* (that is, the modular exponentiation function) and an *RSA encryption/signature scheme* (that is, a particular way to use the RSA primitive to encrypt or to sign a message). In the original paper ([14]), the RSA primitive is used to encrypt or to sign messages. This is definitely not a reasonable way to use RSA. As observed by Goldwasser and Micali [5], an encryption scheme had better to be probabilistic. The same conclusion holds for signature schemes [6]. The now recommended ways to use RSA rely on the Optimal Asymmetric Encryption Padding (OAEP) for encryption [1] and the Provable Secure Scheme (PSS) for signature [2]. This is supported by the RSA Laboratories [9, 10] and will be followed by the IEEE and ANSI X9 standards.

Numerous attacks are reported on the bad use of small public exponents in the RSA *primitive* (see the survey paper by Boneh [4] and the references therein). There are no known such attacks on a provable secure version of RSA (e.g., OAEP or PSS): such a scheme with a small public exponent is no less secure than a scheme with a large exponent. However, as small exponents lead to much better performances, they are no reasons to use large public[1] exponents.

3 Better RSA Primes without Security Loss

Another reminiscence of history is the use of so-called safe, strong or X9.31 RSA primes. The reason of using such primes was to prevent some classes of attacks. In particular, they were introduced to better resist the cycling attacks [16] (see also [20, 7, 3]) and the $(p-1)$ and $(p+1)$ factoring attacks [13, 19]. We refer the reader to [15] for an account concerning the recommendations of special RSA primes. The lesson is that they are now obsolete owing to new factorization algorithms (more particularly ECM). More importantly, they offer a negligible increase of security over random primes of the same size [15, 8].

4 Conclusion

We believe it is important that standardization committees (and standards through them) recognize that RSA signature (or decryption) performances could

[1] For private exponents, this is another story ... See [18].

be significantly improved at no cost at all provided that secret prime factors remain out of the reach of ECM-like factoring algorithms. A second improvement consists in choosing a small public exponent as the popular values $e = 3$ or $e = 2^{16} + 1$. Finally, we recommend random primes in the RSA key generation.

References

1. Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In A. De Santis, editor, *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111. Springer-Verlag, 1995.
2. Mihir Bellare and Phillip Rogaway. The exact security of digital signatures - How to sign with RSA and Rabin. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 399–416. Springer-Verlag, 1996.
3. Shimshon Berkovits. Factoring via superencryption. *Cryptologia*, 6(3):229–237, July 1982.
4. Dan Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203–213, February 1999.
5. Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.
6. Shafi Goldwasser, Silvio Micali, and Ronald Rivest. A digital signature scheme secure against adaptive chosen message attacks. *SIAM Journal of Computing*, 17(2):281–308, 1988.
7. Tor Herlestam. Critical remarks on some public-key cryptosystems. *BIT*, 18:493–496, 1978.
8. Marc Joye, Jean-Jacques Quisquater, and Tsuyoshi Takagi. How to choose secret parameters for RSA and its extensions to elliptic curves. *Designs, Codes and Cryptography*, 23(3):297–316, 2001.
9. RSA Laboratories. PKCS #1 v2.0: RSA cryptography standard, October 1998. Available at `http://www.rsasecurity.com/rsalabs/pkcs/`.
10. RSA Laboratories. PKCS #1 v2.1: RSA cryptography standard. Draft 2, January 2001. Available at `http://www.rsasecurity.com/rsalabs/pkcs/`.
11. Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology*, 14(4):255–293, 2001.
12. Andrew Odlyzko. The future of integer factorization. *Cryptobytes*, 1(2):5–12, 1995.
13. J.M. Pollard. Theorems on factorization and primality testing. *Proc. Camb. Phil. Soc.*, 76:521–528, 1974.
14. Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.
15. Ronald L. Rivest and Robert D. Silverman. Are 'strong' primes needed for RSA. Report 2001/007, Cryptology ePrint Arhive, 2001. Available at `http://eprint.iacr.org/2001/007/`. A preliminary version appears in *1997 RSA Laboratories Seminar Series*, Seminar Proceedings, 1997.
16. Gustavus J. Simmons and Michael J. Norris. Preliminary comment on the M.I.T. public-key cryptosystem. *Cryptologia*, 1:406–414, 1977.
17. Tsuyoshi Takagi. Fast RSA-type cryptosystem modulo $p^k q$. In H. Krawczyk, editor, *Advances in Cryptology – CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 318–326. Springer-Verlag, 1998.

18. Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553–558, May 1990.
19. Hugh C. Williams. A $p+1$ method of factoring. *Mathematics of Computation*, 39(159):225–234, July 1982.
20. Hugh C. Williams and B. Schmid. Some remarks concerning the M.I.T. public-key cryptosystem. *BIT*, 19:525–538, 1979.
21. ANSI X9.31. Public-key cryptography using RSA for the financial services industry. Draft, 1995.

About the Authors

Marc Joye received his PhD degree in applied sciences (cryptography) from the Université catholique de Louvain, Belgium, in 1997. In 1998 and 1999, he was a post-doctoral fellow of the National Science Council, Republic of China. Since Sept. 1999, he has been with Gemplus Card International. His research interests include cryptography, computer security, computational number theory, and smart-card implementations. He is a member of the IACR.

Pascal Paillier is a public key specialist. His main research topics cover the design of new encryption and signature schemes, provable security and efficient implementations. Member of IEEE and IACR, he served in various program committees of cryptographic conferences. In 1999, he obtained his PhD thesis which focused on the applications of high order residues in public key design.