Cryptography and the Methodology of Provable Security

Jacques Stern

Dépt d'Informatique, ENS – CNRS, 45 rue d'Ulm, 75230 Paris Cedex 05, France.
E-mail : Jacques.Stern@ens.fr
URL : http ://www.di.ens.fr/users/stern

1 Introduction

Public key cryptography was proposed in the 1976 seminal article of Diffie and Hellman [6]. One year later, Rivest, Shamir and Adleman introduced the RSA cryptosystem as a first example. From an epistemological perspective, one can say that Diffie and Hellman have drawn the most extreme consequence of a principle stated by Auguste Kerckhoffs in the XIXth century : "le mécanisme de chiffrement doit pouvoir tomber sans inconvénient aux mains de l'ennemi [1]". Indeed, Diffie and Hellman understood that only the deciphering operation has to be controlled by a secret key : the enciphering method may perfectly be executed by means of a publicly available key, provided it is virtually impossible to infer the secret deciphering key from the public data.

Today, algorithms have replaced mechanisms and the wording "virtually impossible" has been given a formal meaning using the theory of complexity. This allows a correct specification of the security requirements, which in turn can be established by means of a *security proof*.

2 The RSA cryptosystem

In modern terms, a public-key encryption scheme on a message space $\mathcal{M}$ consists of three algorithms $(\mathcal{K}, \mathcal{E}, \mathcal{D})$:

- the key generation algorithm $\mathcal{K}(1^k)$ outputs a random pair of private/public keys $(\mathsf{sk}, \mathsf{pk})$, relatively to a security parameter k
- the encryption algorithm $\mathcal{E}_{\mathsf{pk}}(m; r)$ outputs a ciphertext c corresponding to the plaintext $m \in \mathcal{M}$, using random coins r
- the decryption algorithm $\mathcal{D}_{\mathsf{sk}}(c)$ outputs the plaintext m associated to the ciphertext c.

We will occasionnally omit the random coins and write $\mathcal{E}_{\mathsf{pk}}(m)$ in place of $\mathcal{E}_{\mathsf{pk}}(m; r)$. Note that the decryption algorithm is deterministic.

The famous RSA cryptosystem has been proposed by Rivest, Shamir and Adleman [14]. The key generation algorithm of RSA chooses two large primes p, q of equal size and issues the so-called modulus $n = pq$. The sizes of p, q are set in such a way that the binary length $|n|$ of n equals the security parameter k. Additionally, en exponent e, relatively prime to $\varphi(n) = (p-1)(q-1)$ is chosen,

[1] The enciphering mechanism may fall into the enemy's hands without drawback

so that the public key is the pair (n, e). The private key d is the inverse of e modulo $\varphi(n)$. Variants allow the use of more than two prime factors.

Encryption and decryption are defined as follows :

$$\mathcal{E}_{n,e}(m) = m^e \bmod n \qquad \mathcal{D}_{n,d}(c) = c^d \bmod n.$$

Note that both operations are deterministic and are mutually inverse to each other. Thus, the RSA encryption function is a permutation. It is termed a *trapdoor permutation* since decryption can only be applied given the private key.

The basic security assumption on which the RSA cryptosystem relies is its *one-wayness* (OW) : using only public data, an attacker cannot recover the plaintext corresponding to a given ciphertext. In the general formal setting provided above, an encryption scheme is one-way if the success probability of any adversary $\mathcal{A}$ attempting to invert $\mathcal{E}$ (without the help of the private key), is negligible, i.e. asymptotically smaller than the inverse of any polynomial function of the security parameter. Probabilities are taken over the message space $\mathcal{M}$ and the randoin coins Ω. These include both the random coins r used for the encryption scheme, and the internal random coins of the adversary. In symbols :

$$\mathsf{Succ}^{\mathsf{ow}}(\mathcal{A}) = \Pr[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^k), m \stackrel{R}{\leftarrow} \mathcal{M} : \mathcal{A}(\mathsf{pk}, \mathcal{E}_{\mathsf{pk}}(m)) = m].$$

Formally, the assumption that RSA is one-way is stronger than the hardness of factoring. Still, it is widely believed and the only method to assess the strength of RSA is to check whether the size of the modulus n outreaches the current performances of the various factoring algorithms.

3 From Naive RSA to OAEP

The "naive" RSA algorithm defined in the previous section cannot be used as it stands : in particular, it has algebraic multiplicative properties which are highly undesirable from a security perspective. Accordingly, it was found necessary to define formatting schemes adding some redundancy. For several years, this worked by trials and errors, as shown by the subtle attack against the PKCS #1 v1.5 encryption scheme devised by Bleichenbacher [4]. In this attack, the adversary discloses the secret key of an SSL server based on the information coming form the error messages received when an incorrectly formatted ciphertext is submitted to the server. Thus, a more formal approach appeared necessary.

The starting point of the new appraoch is semantic security, also called *polynomial security/indistinguishability of encryptions*, introduced by Goldwasser and Micali [9] : an encryption scheme is *semantically secure* if no polynomial-time attacker can learn any bit of information about the plaintext from the ciphertext, except its length. More formally, an encryption scheme is semantically secure if, for any two-stage adversary $\mathcal{A} = (A_1, A_2)$ running in polynomial time, the advantage $\mathsf{Adv}^{\mathsf{ind}}(\mathcal{A})$ is negligible, where $\mathsf{Adv}^{\mathsf{ind}}(\mathcal{A})$ is formally defined as

$$2 \times \Pr\left[\begin{array}{l}(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^k), (m_0, m_1, s) \leftarrow A_1(\mathsf{pk}), \\ b \stackrel{R}{\leftarrow} \{0,1\}, c = \mathcal{E}_{\mathsf{pk}}(m_b) : A_2(m_0, m_1, s, c) = b\end{array}\right] - 1,$$

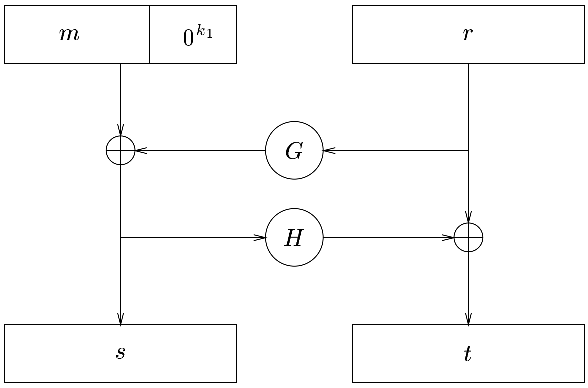

Fig.1. Optimal Asymmetric Encryption Padding

where the probability space includes the internal random coins of the adversary, and m_0, m_1 are two equal length plaintexts chosen by A_1 in the message-space $\mathcal{M}$.

The above definition only covers passive adversaries. It is a *chosen–plaintext* or CPA attack since the attacker can only encrypt plaintext. In extended models, the adversary is given access to a decryption oracle which returns the decryption of any ciphertext c, with the only restriction that it should be different from the challenge ciphertext c. This scenario is is termed the *adaptive chosen-ciphertext attack* ($\mathsf{CCA2}$) [13].

The OAEP padding scheme (optimal asymmetric encryption padding) was proposed by Bellare and Rogaway [3] in 1994. It is depicted on figure 1 . For a long time it was believed that OAEP achieved $\mathsf{CCA2}$ security, based on an almost mathematical proof relying on the one-wayness of the RSA function. The word "almost" here refers to the use of the so-called *random oracle model* which models G and H in figure 1 as functions which return random independant values, which is not formally correct.

4 Rise, Fall and Repair of OAEP

In 2001, Victor Shoup [16] showed by means of a subtle counter-example, the the proof of Bellare and Rogaway only applied in the restricted attack setting where the adversary can query the decryption oracle before it receives the challenge ciphertext c (sometimes referred as $\mathsf{CCA1}$. It did not necessarily mean that OAEP was itself flawed. In any case, a new proof was needed.

Surprisingly, the repaired proof appeared shortly afterwards in [8]. Albeit based on the same methodology, it is significantly different and uses additional algebraic tools, notably two-dimensional lattices, which did not appear in the earlier proof. Thus, the multiplicative properties of RSA, which motivated the quest for formatting schemes, help for the security proof. It should also be noted that alternative formatting schemes, with a more direct security proof have been recently designed. However, OAEP is a widely used standard [15] and it is unclear whether it will be replaced by these challengers.

5 Conclusion

The lesson to learn from the above is that cryptography should proceed with care. Twenty-five centuries were needed before the discovery of public key cryptography by Diffie and Hellman. It took twenty-five more years to understand how RSA could be correctly practiced. No cryptographic algorithm can be designed and validated in twenty-five minutes or twenty-five hours, not even twenty-five days.

Références

1. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among Notions of Security for Public-Key Encryption Schemes. In *Crypto '98*, LNCS 1462, pages 26–45. Springer-Verlag, Berlin, 1998.
2. M. Bellare and P. Rogaway. Random Oracles Are Practical : a Paradigm for Designing Efficient Protocols. In *Proc. of the 1st CCS*, pages 62–73. ACM Press, New York, 1993.
3. M. Bellare and P. Rogaway. Optimal Asymmetric Encryption – How to Encrypt with RSA. In *Eurocrypt '94*, LNCS 950, pages 92–111. Springer-Verlag, Berlin, 1995.
4. D. Bleichenbacher. A Chosen Ciphertext Attack against Protocols based on the RSA Encryption Standard PKCS #1. In *Crypto '98*, LNCS 1462, pages 1–12. Springer-Verlag, Berlin, 1998.
5. D. Coppersmith. Finding a Small Root of a Univariate Modular Equation. In *Eurocrypt '96*, LNCS 1070, pages 155–165. Springer-Verlag, Berlin, 1996.
6. W. Diffie and M.E. Hellman. New Directions in Cryptography, IEEE Transactions on Information Theory, v. IT-22, 6, Nov 1976, pages 644-654.
7. D. Dolev, C. Dwork, and M. Naor. Non-Malleable Cryptography. *SIAM Journal on Computing*, 30(2) :391–437, 2000.
8. E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA–OAEP is Secure under the RSA Assumption. In *Crypto '2001*, LNCS 2139, pages 260–274. Springer-Verlag, Berlin, 2001.
9. S. Goldwasser and S. Micali. Probabilistic Encryption. *Journal of Computer and System Sciences*, 28 :270–299, 1984.
10. C. Hall, I. Goldberg, and B. Schneier. Reaction Attacks Against Several Public-Key Cryptosystems. In *Proc. of ICICS'99*, LNCS, pages 2–12. Springer-Verlag, 1999.
11. M. Naor and M. Yung. Public-Key Cryptosystems Provably Secure against Chosen Ciphertext Attacks. In *Proc. of the 22nd STOC*, pages 427–437. ACM Press, New York, 1990.
12. T. Okamoto and D. Pointcheval. REACT : Rapid Enhanced-security Asymmetric Cryptosystem Transform. In *CT – RSA '2001*, LNCS 2020, pages 159–175. Springer-Verlag, Berlin, 2001.
13. C. Rackoff and D. R. Simon. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In *Crypto '91*, LNCS 576, pages 433–444. Springer-Verlag, Berlin, 1992.
14. R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, 21(2) :120–126, February 1978.
15. RSA Data Security, Inc. Public Key Cryptography Standards – PKCS. Available from `http ://www.rsa.com/rsalabs/pubs/PKCS/`.
16. V. Shoup. OAEP Reconsidered. In *Crypto '2001*, LNCS 2139, pages 239–259. Springer-Verlag, Berlin, 2001.