REACT: Rapid Enhanced-security Asymmetric Cryptosystem Transform

Tatsuaki Okamoto[1] and David Pointcheval[2]

[1] NTT Labs, 1-1 Hikarinooka, Yokosuka-shi 239-0847 Japan.
~okamoto@isl.ntt.co.jp.
[2] Dépt d'Informatique, ENS – CNRS, 45 rue d'Ulm, 75230 Paris Cedex 05, France.
David.Pointcheval@ens.fr http://www.di.ens.fr/~pointche.

Abstract. Seven years after the optimal asymmetric encryption padding (OAEP) which makes chosen-ciphertext secure encryption scheme from any trapdoor one-way permutation (but whose unique application is RSA), this paper presents REACT, a new conversion which applies to any weakly secure cryptosystem, in the random oracle model: it is optimal from both the computational and the security points of view. Indeed, the overload is negligible, since it just consists of two more hashings for both encryption and decryption, and the reduction is very tight. Furthermore, advantages of REACT beyond OAEP are numerous:

1. it is more general since it applies to any partially trapdoor one-way function (a.k.a. weakly secure public-key encryption scheme) and therefore provides security relative to RSA but also to the Diffie-Hellman problem or the factorization;
2. it is possible to integrate symmetric encryption (block and stream ciphers) to reach very high speed rates;
3. it provides a key distribution with session key encryption, whose overall scheme achieves chosen-ciphertext security even with weakly secure symmetric scheme.

Therefore, REACT could become a new alternative to OAEP, and even reach security relative to factorization, while allowing symmetric integration.

1 Introduction

For a long time many conversions from a weakly secure encryption scheme into a chosen-ciphertext secure cryptosystem have been attempted, with variable success. Such a goal is of greatest interest since many one-way encryption schemes are known, with variable efficiency and various properties, whereas chosen-ciphertext secure schemes are very rare.

1.1 Chosen-Ciphertext Secure Cryptosystems

Until few years ago, the description of a cryptosystem, together with some heuristic arguments for security, were enough to convince and to make a scheme to be

D. Naccache (Ed.): CT-RSA 2001, LNCS 2020, pp. 159–174, 2000.

widely adopted. Formal semantic security [18] and further non-malleability [13] were just seen as theoretical properties. However, after multiple cryptanalyses of international standards [7,10,9], provable security has been realized to be important and even became a basic requirement for any new cryptographic protocol. Therefore, for the last few years, many cryptosystems have been proposed. Some furthermore introduced new algebraic problems, and assumptions [25,1,2,19,26, 29,31,34], other are intricate constructions, over old schemes, to reach chosen-ciphertext security (from El Gamal [20,41,40,11], D-RSA [33] or Paillier [32]), with specific security proofs.

Indeed, it is easy to describe a one-way cryptosystem from any trapdoor problem. Furthermore, such a trapdoor problems is not so rare (Diffie-Hellman [12], factorization, RSA [37], elliptic curves [22], McEliece [24], NTRU [19], etc). A very nice result would be a generic and *efficient* conversion from any such a trapdoor problem into a chosen-ciphertext secure encryption scheme.

1.2 Related Work

In 1994, Bellare and Rogaway [5] suggested such a conversion, the so-called OAEP (Optimal Asymmetric Encryption Padding). However, its application domain was restricted to trapdoor one-way *permutations*, which is a very rare object (RSA, with a few variants, is the only one application). Nevertheless, it provided the most efficient RSA-based cryptosystem, the so-called OAEP-RSA, provably chosen-ciphertext secure, and thus became the new RSA standard – PKCS #1 [38], and has been introduced in many world wide used applications.

At PKC '99, Fujisaki and Okamoto [15,17] proposed another conversion with further important improvements [16,35]. Therefore it looked like the expected goal was reached: a generic conversion from any one-way cryptosystem into a chosen-ciphertext secure encryption scheme. However, the resulting scheme is not optimal, from the computational point of view. Namely, the decryption phase is more heavy than one could expect, since it requires a re-encryption.

As a consequence, with those conversions, one cannot expect to obtain a scheme with a fast decryption phase (unless both encryption and decryption are very fast, which is very unlikely). Nevertheless, decryption is usually implemented on a smart card. Therefore, cryptosystem with efficient decryption process is a challenge with a quite practical impact.

1.3 Achievement: A New and Efficient Conversion

The present work provides a new conversion in the random oracle model [4] which is optimal from the computational point of view in both the encryption and decryption phases. Indeed, the encryption needs an evaluation of the one-way function, and the decryption just makes one call to the inverting function. Further light computations are to be done, but just an XOR and two hashings. Moreover, many interesting features appear with integration of symmetric encryption schemes.