Efficient CCA-Secure Public-Key Encryption Schemes from RSA-Related Assumptions

Jaimee Brown, Juan Manuel González Nieto, and Colin Boyd

Information Security Institute
Queensland University of Technology, Australia
{j2.brown, j.gonzaleznieto, c.boyd}@qut.edu.au

Abstract. We build new RSA-based encryption schemes secure against adaptive chosen-ciphertext attack (CCA-secure) without random oracles. To do this, we first define a new general RSA-related assumption, the Oracle RSA-type assumption, and give two specific instances of this assumption. Secondly, we express RSA-based encryption schemes as tag-based encryption schemes (TBE), where the public exponent is the tag. We define selective-tag weak chosen-ciphertext security for the special RSA-based case and call it selective-exponent weak chosen-ciphertext security. RSA-based schemes secure in this sense can be used as a building block for the construction of chosen-ciphertext secure encryption schemes using a previous technique. We build two concrete CCA-secure encryption schemes whose security is based on the two concrete Oracle RSA-type assumptions respectively, and whose efficiency is comparable to the most efficient CCA-secure schemes known.

Keywords: chosen-ciphertext security, public key encryption, RSA assumptions.

1 Introduction

Indistinguishability against adaptive chosen ciphertext attack (IND-CCA), where an adversary is given the capability to decrypt ciphertexts of his choice, with the exception of a target ciphertext, is considered to be the correct notion of security for general-purpose public key encryption schemes. We refer to such schemes as CCA-secure schemes. In the literature, there are a number of approaches for obtaining encryption schemes that are CCA-secure. Much of this work, however, has been only achieved with proofs in the random oracle model, the most famous being OAEP [3]. When, in practice, these random oracles are replaced by hash functions, the security argument becomes heuristic only and does not guarantee security against all attacks under the standard assumptions.

In the standard model three main techniques have been proposed for constructing CCA-secure encryption schemes. The first approach, from Naor and Yung [21] and subsequently Dolev, Dwork and Naor [14], builds CCA-secure schemes from any chosen-plaintext secure scheme (CPA-secure) and any non-interactive zero knowledge (NIZK) proof system. The resulting schemes, however, are too inefficient for practical use, since they use expensive NIZK proofs.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 176–190, 2006.

Cramer and Shoup [11] proposed the first encryption scheme that was simultaneously practical and CCA-secure in the standard model. Cramer and Shoup [12] later generalised their encryption scheme by defining *hash proof systems* (HPS) and giving a framework for constructing CCA-secure encryption schemes using a HPS constructed from a general subset membership problem. Kurosawa and Desmedt [18] later showed how to obtain CCA-secure hybrid encryption schemes using a HPS as a building block, and in particular described an efficient hybrid encryption scheme based on the Cramer-Shoup cryptosystem.

More recently, Canetti, Halevi and Katz [8] proposed a framework (CHK) for constructing chosen-ciphertext secure encryption schemes from ID-based encryption (IBE) schemes secure against selective-identity chosen-plaintext attack. Boneh and Katz [7] improved the efficiency of the CHK construction, and the two related works were combined in a later paper [6]. The resulting schemes are both simple and efficient, with proofs of security in the standard model. Interestingly, the authors note that the resulting schemes seem to achieve chosen-ciphertext security using a different approach to the two previous techniques that use NIZK proofs and HPS. More precisely, the schemes do not use a *proof of well-formedness* as in the two previous approaches and hence do not fall within the general paradigm for chosen-ciphertext encryption described by Elkind and Sahai [15]. Kiltz [17] showed that tag-based encryption (TBE) is a more general case of IBE and can in fact be used as the building block for the CHK framework in place of the IBE. Kiltz defined selective-tag security for TBE and showed that a TBE secure in this sense is a sufficient building block for the CHK transformation and then proposed a new TBE that can be used to construct a reasonably efficient CCA-secure scheme from the Decisional Linear Assumption [5].

It is worth noting that despite these three approaches to building provably CCA-secure encryption schemes, there has yet to emerge an efficient CCA-secure encryption scheme based on RSA or related assumptions in the standard model.

1.1 Our Contributions

New RSA-related assumption. We define a new general RSA-related assumption, namely the *Oracle RSA-type assumption*, which will be used to prove the security of the new schemes we introduce later in the paper. The Oracle RSA-type assumption is a variant of the general *Decisional RSA-type assumption* which is a decisional RSA-based assumption of a specific form. The Oracle RSA-type assumption can be viewed as the analog of the Oracle Diffie-Hellman assumption [2] for an RSA context. We give concrete examples of Oracle RSA-type assumptions derived from previously studied decisional RSA-based assumptions.

Selective-exponent security for RSA-based encryption. We observe that an RSA-based encryption scheme can be considered as a TBE where the exponent e is the tag. We redefine the notion of selective-tag weak CCA security [17] for this special case of RSA-based TBEs, and call it *selective-exponent weak chosen-ciphertext security*, or more simply *selective-exponent security*. In a selective-exponent attack, an adversary is given access to a decryption oracle