Concrete Chosen-Ciphertext Secure Encryption from Subgroup Membership Problems

Jaimee Brown, Juan Manuel González Nieto, and Colin Boyd

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

Abstract. Using three previously studied subgroup membership problems, we obtain new concrete encryption schemes secure against adaptive chosen-ciphertext attack in the standard model, from the Cramer-Shoup and Kurosawa-Desmedt constructions. The schemes obtained are quite efficient. In fact, the Cramer-Shoup derived schemes are more efficient than the previous schemes from this construction, including the Cramer-Shoup cryptosystem, when long messages are considered. The hybrid variants are even more efficient, with a smaller number of exponentiations and a shorter ciphertext than the Kurosawa-Desmedt Decisional Diffie-Hellman based scheme.

Keywords: public key encryption, chosen ciphertext security, Cramer-Shoup framework, subgroup membership problems, hybrid encryption.

1 Introduction

The underlying security goal for a public key encryption scheme is to guarantee that no partial information about a plaintext message is revealed from its ciphertext, a notion often called indistinguishability of encryptions. 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 shall refer to schemes that achieve this level of security as CCA-secure schemes.

We present several practical, concrete encryption schemes that are proven CCA-secure in the standard model each based on the difficulty of a particular subgroup membership problem. Several of these schemes are more efficient than previous CCA-secure schemes, and all schemes rely on different problems than have previously been used for CCA-schemes. We have used three subgroup membership problems previously studied in the literature: the subgroup membership problem discussed by González-Nieto, Boyd and Dawson [6], the r-th residue problem [8], and Okamoto and Uchiyama's [9] p-subgroup problem.

Cramer and Shoup [1] proposed the first encryption scheme that was simultaneously practical and CCA-secure under standard intractability assumptions. Cramer and Shoup [3] later generalised their encryption scheme to give a

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 1–18, 2006.

framework for constructing CCA-secure encryption schemes from general subgroup membership problems and *hash proof systems* (HPS). Accompanying their framework, Cramer and Shoup also described three instantiations of the framework using three subgroup membership problems, namely Decisional Diffie-Hellman, Decisional Composite Residuosity [10] and the classical Quadratic Residuosity problem. Kurosawa and Desmedt [7] later presented an efficient hybrid encryption scheme based on the Cramer-Shoup cryptosystem, as well as a generalised construction of CCA-secure hybrid encryption schemes from the HPS primitive introduced by Cramer and Shoup.

Motivation and Contribution. The Cramer-Shoup construction is an important development in the area of chosen-ciphertext security for public key encryption. However, their general construction is quite complicated, and developing schemes requires a strong understanding of how the construction works, and the steps involved applying it concretely. We believe that understanding in this case is best achieved through example, and our hope is that by applying the construction to a number of different subgroup membership problems, and detailing the steps taken, the process of deriving new schemes will become clearer.

Of independent interest are the actual schemes obtained by applying both the Cramer-Shoup and Kurosawa-Desmedt to the three previously proposed subgroup membership problems. For the Cramer-Shoup construction, the resulting encryption schemes are in fact more efficient than the schemes presented by Cramer and Shoup, including the Cramer-Shoup cryptosystem, when the encryption of long messages is considered. The hybrid schemes obtained by applying the Kurosawa-Desmedt construction to the same subgroup membership problems, are even more efficient. In fact, the number of exponentiations and the size of the ciphertexts are smaller than the previous DDH-based hybrid scheme.

Related Work. Gjøsteen [5] discussed symmetric subgroup membership (SSM) problems and described an instantiation of the Cramer-Shoup framework specific for such problems. A symmetric subgroup membership problem considers a group X and non-trivial subgroups L and $\tilde{L}$ such that $X = L\tilde{L}$, $L \cap \tilde{L} = \{1\}$. It is said to be hard if distinguishing elements of L from elements of $X \backslash L$, and elements of $\tilde{L}$ from elements of $X \backslash \tilde{L}$ are both hard problems. Gjøsteen also showed that the decisional Diffie-Hellman (DDH) problem and the symmetric subgroup membership problem are related such that SSM is not harder than DDH. In other words, the difficulty of SSM implies the difficulty of DDH. Although Gjøsteen showed the general encryption scheme for SSMs, we analyse instances of subgroup membership problems and the resulting concrete schemes obtained.

2 Preliminaries

If x is an integer, we denote the bit length of x as $|x|$. For a set S, we denote the order of S as $|S|$. We denote by $x \in_R S$ the act of sampling x from S uniformly at random. The notation G_α is used to denote a group of order α.