Homomorphic Cryptosystems Based on Subgroup Membership Problems

Kristian Gjøsteen

Department of Telematics,
Norwegian University of Science and Technology, 7491 Trondheim, Norway
kristian.gjosteen@item.ntnu.no

Abstract. We define an abstract subgroup membership problem, and derive a number of general results for subgroup membership problems. We define an homomorphic public key cryptosystem based essentially on a subgroup membership problem, and show that this abstract construction gives a uniform description of many famous cryptosystems, such as ElGamal, Goldwasser-Micali and Paillier. We show that the abstract theory gives new insights into older results, and allows us to derive new results.

Keywords: public key encryption, homomorphic cryptosystems, subgroup membership problem.

1 Introduction

A cryptosystem is *homomorphic* with respect to some operation $*$ on the message space if there is a corresponding operation $*'$ on the ciphertext space such that for encryptions c, c' of messages m, m', $c *' c'$ is an encryption of $m * m'$.

Goldwasser and Micali [9] introduced the concept of semantic security and described a semantically secure cryptosystem based on the quadratic residue assumption. It was later remarked that this cryptosystem really was homomorphic with respect to addition in $\mathbb{Z}_2$.

ElGamal [8] introduced an homomorphic cryptosystem based on the Diffie-Hellman key exchange protocol [7]. It has later been remarked that this cryptosystem is semantically secure under the Decision Diffie-Hellman assumption.

Naccache and Stern [11] introduced an homomorphic cryptosystem based on "higher residues" in $\mathbb{Z}_n^*$, where n was a product of two primes of a special form. Okamoto and Uchiyama [13] described an homomorphic cryptosystem over $\mathbb{Z}_n^*$ using a modulus of the form $n = p^2q$. Paillier [14] introduced an homomorphic cryptosystem based on the ring $\mathbb{Z}_{n^2}$, where n was simply an RSA modulus.

It turns out that all of these cryptosystems are simply special cases of a cryptosystem based on a general subgroup membership problem [5]. We discuss some general theory for subgroup membership problems in Sect. 2, then we describe the cryptosystem in Sect. 3. We give a catalogue of known subgroup membership problems in Sect. 4, and describe some new results in Sect. 5.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 314–327, 2005.

The main achievement in this paper is an abstract construction for a homomorphic cryptosystem. From this construction, we derive as special cases many famous cryptosystems. The use of abstract descriptions to focus on the interesting points of a cryptosystem is a common technique, see for example [3]. The novel arguments in Sect. 2.1 and in Sect. 5 show that our abstract constructions gives us new insights into old results, and can reduce the analysis of new constructions to the analysis of older, simpler constructions.

2 Subgroup Membership Problems

A *subgroup membership problem* consists of a finite abelian group G along with a proper, non-trivial subgroup K. The problem is to decide if a group element $x \in G$ is in K or in $G \setminus K$. We denote this subgroup membership problem by $\mathcal{SM}_{(G,K)}$, and the advantage of an adversary A is

$$\mathrm{Adv}_A^{\mathcal{SM}_{(G,K)}} = |\Pr[A(G,K,x) = 1 \mid x \xleftarrow{r} K] - \Pr[A(G,K,x) = 1 \mid x \xleftarrow{r} G \setminus K]|.$$

When we leave out the adversary, we consider the maximal advantage of all algorithms using less than some fixed amount of resources.

An alternative description of the subgroup membership problem is that given a representative x of a residue class in the factor group G/K, the adversary must decide if this residue class is the neutral element in G/K. (Note that the residue class $xK = 1K$ if and only if $x \in K$.)

We note some general facts about subgroup membership problems.

Let $\mathcal{SM}_{(G,K)}$ be such that the factor group G/K is cyclic. If $|G/K|$ is a known prime ℓ, sampling a uniformly from $\{1, \ldots, \ell - 1\}$ gives us a random automorphism $x \mapsto x^a$ on G/K.

If $|G/K|$ contains no small primes, then an element chosen uniformly at random from G/K is, except with negligible probability, a generator. Sampling a uniformly from $\{1, \ldots, 2^N\}$ (for some sufficiently large N) therefore gives us, except with negligible probability, a representative x^a for a residue class in G/K chosen uniformly at random.

If we are given an element x, we sample a as above and x' uniformly from K to get $x^a x'$. If x is in K, then $x^a x'$ is an element of K chosen uniformly at random. If x is in $G \setminus K$, then $x^a x'$ is (except with at most negligible probability) a random representative of a random non-neutral element in G/K, that is, $x^a x'$ is a random element in $G \setminus K$.

Therefore, $\mathcal{SM}_{(G,K)}$ is random self-reducible.

Note the following useful extension of this idea. Let $\mathcal{SM}_{(G,K)}$ and $\mathcal{SM}_{(G',K')}$ be subgroup membership problems. If there is a probabilistic algorithm that on input of x sampled uniformly from K outputs an element of K', and on input of x sampled uniformly from $G \setminus K$ outputs an element of $G' \setminus K$, with the output distribution in both cases uniform, then

$$\mathrm{Adv}^{\mathcal{SM}_{(G',K')}} \leq \mathrm{Adv}^{\mathcal{SM}_{(G,K)}}.$$

The following theorem will be useful for the analysis in Sect. 4 and 5.