Unification Modulo Homomorphic Encryption

Siva Anantharaman[1], Hai Lin[2], Christopher Lynch[2],
Paliath Narendran[3], and Michaël Rusinowitch[4]

[1] Université d'Orléans (Fr.)
siva@univ-orleans.fr
[2] Clarkson University, Potsdam, NY, USA
{linh,clynch}@clarkson.edu
[3] University at Albany-SUNY, USA
dran@cs.albany.edu
[4] Loria-INRIA Lorraine, Nancy (Fr.)
rusi@loria.fr

Abstract. Encryption 'distributing over pairs' is a technique employed in several cryptographic protocols. We show that unification is decidable for an equational theory HE specifying such an encryption. The method consists in transforming any given problem in such a way, that the resulting problem can be solved by combining a graph-based reasoning on its equations involving the homomorphisms, with a syntactic reasoning on its pairings. We show HE-unification to be NP-hard and in NEXPTIME.

1 Introduction

Several methods based on rewriting have been proposed with success, for the formal analysis of cryptographic protocols. The following Dolev-Yao (DY) system underlies many of them:

$$\text{(DY)} \qquad \begin{array}{ll} p_1(x.y) \to x & dec(enc(x,y),y) \to x \\ p_2(x.y) \to y & enc(dec(x,y),y) \to x \end{array}$$

The '.' here is the 'pairing' operation on messages, p_1, p_2 are the respective projections from pairs, and '*dec*' (resp. '*enc*') stands for decryption (resp. encryption); the second argument of these latter functions are referred to as keys.

The so-called *public collapsing* theories, used in some works (e.g., [7]), are presented by rewrite systems where the rhs of every rule is a ground term or a variable. Some other results assume that the rhs of any rule is a proper subterm of the lhs. A general procedure for protocol security analysis has been given in [3] for such systems, extensively using equational unification and narrowing. Rewrite systems with such a 'subterm' property have been called *dwindling* in [1], where a decision procedure was given for passive deduction (i.e., detecting secrecy attacks by an intruder *not* interacting actively with the protocol sessions). The technique used is one that combines unification and narrowing with the notion of *cap closure* modeling the evolution of the intruder knowledge. The algorithm presented was also shown to be complete for passive deduction, for a class of rewrite systems strictly including the dwindling systems, and in particular the following

S. Ghilardi and R. Sebastiani (Eds.): FroCoS 2009, LNAI 5749, pp. 100–116, 2009.

convergent, non-dwindling system, that we shall refer to as HE; it extends DY with the requirement that '*encryption distributes over pairs*':

$$\text{(HE)} \quad \begin{array}{ll} p_1(x.y) \to x & \\ p_2(x.y) \to y & enc(x.y, z) \to enc(x, z).enc(y, z) \\ enc(dec(x, y), y) \to x & dec(x.y, z) \to dec(x, z).dec(y, z) \\ dec(enc(x, y), y) \to x & \end{array}$$

We shall refer to the equational theory defined by this system HE as *Homomorphic Encryption*, or just as HE. On protocols implementing encryption with the so-called ECB (Electronic Code Book) block chaining – performed sequentially on a block decomposition of the plain text, and under the assumption that message fields are assigned a round number of blocks – encryption can be modeled as an homomorphism on pairs; examples of such protocols can be found in e.g., [5]. As mentioned above, passive deduction is known to be decidable for protocols employing HE; but the problem of *active deduction* for such protocols, i.e., when the intruder is allowed to interact with the protocol steps (for instance, to forge the identity of some honest agent), has not been studied yet. Now, the decidability of unification modulo any given intruder theory E is known to be a necessary condition for deciding active deduction modulo E, cf. e.g., [5]; that motivated our interest in HE-unification. Note that the homomorphism $enc(-, y)$ defined on terms for any given y, admits an inverse homomorphism $dec(-, y)$ modulo HE; as a consequence, HE-unification cannot be reduced directly to unification modulo one-sided distributivity [12].

This paper is structured as follows: The needed preliminaries are given in Section 2. Unification modulo HE is shown to be decidable in Section 3. The main idea consists in reducing any given HE-unification problem into one of solving a set of 'simple' equations of the form $Z = enc(X, V)$ or $Z = dec(X, V)$, where none of the 1st arguments under *enc* get split into pairs by the other equations. Solving such a set of 'simple' equations is essentially the unification problem modulo the two rules for encryption and decryption:

$$\begin{array}{c} dec(enc(x, y), y) \to x \\ enc(dec(x, y), y) \to x \end{array}$$

which form a confluent, dwindling system, so has a decidable unification problem, cf. [10]. The method we propose in this work actually combines a graph-based algorithm reasoning modulo the group structure on homomorphisms – that is specific to 'simple' HE-unification problems – with one that reasons modulo a theory for pairings. We show that *even solving 'simple' HE-unification problems* (i.e., without pairings) *is NP-complete*. A couple of examples illustrating the method are given in Section 4.

2 Notation and Preliminaries

As usual, Σ will stand for a ranked signature, and $\mathcal{X}$ a countably infinite set of variables. $\mathcal{T} = \mathcal{T}(\Sigma, \mathcal{X})$ is the algebra of terms over this signature; terms in $\mathcal{T}$ will be denoted as $s, t, \ldots$, and variables as $u, v, x, y, z, \ldots$, all with possible suffixes.