Sound Approximations to Diffie-Hellman Using Rewrite Rules
(Extended Abstract)

Christopher Lynch[1,⋆] and Catherine Meadows[2]

[1] Department of Mathematics and Computer Science
Clarkson University
Potsdam, NY 13699
clynch@clarkson.edu
[2] Naval Research Laboratory
Center for High Assurance Computer Systems
Code 5543
Washington, DC 20375
meadows@itd.nrl.navy.mil

Abstract. The commutative property of exponentiation that is necessary to model the Diffie-Hellman key exchange can lead to inefficiency when reasoning about protocols that make use of that cryptographic construct. In this paper we discuss the feasibility of approximating the commutative rule for exponentiation with a pair of rewrite rules, for which in unification-based systems, the complexity of the unification algorithm changes from at best exponential to at worst quadratic in the number of variables. We also derive and prove conditions under which the approximate model is sound with respect to the original model. Since the conditions make the protocol easier to reason about and less prone to error, they often turn out to be in line with generally accepted principles for sound protocol design.

1 Introduction

It is not always easy to tell what is the right level of detail to model a system for formal analysis. This is particularly the case for cryptographic protocols, which rely on cryptographic assumptions involving statistical and complexity-theoretic constructs that can't easily be captured by existing formal analysis tools. Even when the properties we wish to model are algebraic identities that *can* easily be captured, their use still might present problems for efficient analysis. For this reason, many formal systems for cryptographic analysis model the systems they are analyzing as free algebras, with operations such as encryption and decryption being modeled as constructors and destructors, respectively. When this is done properly, it is often possible to guarantee soundness. For example, Backes et al. [1] have developed a composable cryptographic library that can be reasoned

⋆ This work was done while the author was visiting the Naval Research Laboratory

J. López, S. Qing, and E. Okamoto (Eds.): ICICS 2004, LNCS 3269, pp. 262–277, 2004.

about in terms of a free algebra. On an intermediate level, Millen [13] and the authors of this paper [9] have developed criteria for protocols so that theorems proved under the free algebra model remain true under more faithful models that model the actions of encryption and decryption as cancellation rules. An advantage of all the systems described above is that most of the restrictions correspond well to what it commonly considered to be principles of sound protocol design. This makes sense, since one of the goals of sound cryptographic protocol design is to reduce the risk of cryptographic features having unintended side effects.

There are, however, limits to this approach. Although the free algebra model seems to be able to capture much of the needed functionality of cryptosystems, there are some places where it clearly fails to do so. One of the most prominent of these is the Diffie-Hellman key exchange protocol. This makes use of the difficulty of finding discrete logarithms modulo large primes to achieve a shared secret as follows:

1. $A \rightarrow B : x^{N_A} \bmod P$. B computes ${x^{N_A}}^{N_B} = x^{N_A \cdot N_B}$
2. $B \rightarrow A : x^{N_B} \bmod P$. A computes ${x^{N_B}}^{N_A} = x^{N_B \cdot N_A} = x^{N_A \cdot N_B}$

At the end of this exchange, assuming the absence of an active attacker, A and B share a secret with each other.

There appears to be no clear way of modeling the properties of exponentiation used here in terms of a free algebra with constructors and destructors. It is possible to utilize a destructor only when one has a means of telling that a constructor has previously been applied. In the case of encryption and decryption this can be accomplished by formatting data to be encrypted so that it can be recognized when properly decrypted. If the decryption operator is applied to an unencrypted message, or a message encrypted with the wrong key, then the results will be discarded, and the operation can be ignored. On the other hand, there is no way a principal can tell a generator raised to a random power from any other random number. Thus, it makes no sense to reason about Diffie-Hellman in terms of destructors.

One might conclude then that the most efficient solution would be to augment the free algebra with a commutative rule for exponentiation. But even modeling only the commutative property has its costs. For example, suppose that we are using a system based on unification, as in [2, 11, 14]. Then, as we shall see in this paper, it is possible to construct terms containing only n variables that have 2^n most general unifiers. Thus the running time of any unification algorithm must be at least exponential.

The approach we follow in this paper is to take a middle ground. We define an approximation in terms of rewrite rules. The approximation does not capture the full behavior of commutative exponentiation, but it is enough to describe the derivation of a Diffie-Hellman key. The next step is to show that the approximation is rich enough to allow us to reason about possible attacks. We achieve this, as in [9, 13], by defining a set of conditions that a cryptographic protocol must satisfy in order for the approximation to be sound with respect to the more