Chapter X

A Summary of Recent and Old Results on the Security of the Diffie–Hellman Key Exchange Protocol in Finite Groups

Ionuț Florescu
Stevens Institute of Technology, USA

ABSTRACT

Regarding fundamental protocols in cryptography, the Diffie-Hellman (Diffie and Hellman, 1976) public key exchange protocol is one of the oldest and most widely used in today’s applications. Consequently, many specific cryptographic implementations depend on its security. Typically, an underlying (finite dimensional) group is selected to provide candidates for the key. The study of the security of the exchange as depending on the structure of the underlying group is even today poorly understood, with the most common approaches relying on the security of the Discrete Logarithm problem or on the size of the group. Recent developments bring to attention that the relationship is not necessarily valid and that more research is needed that will relate the underlying structure of the group and the security of the Diffie-Hellman exchange. In this chapter, we describe the problem in detail, we present the relationship with the previously studied Discrete Logarithm and Computational Diffie-Hellman problems, we expose the various concepts of security, and we introduce a new statistical concept specifically designed to serve the assessment of the security of the exchange.

INTRODUCTION

A key exchange protocol is any algorithm through which two parties A and B agree on a common key $K_{AB}$. Once the key is established, any further information shared between the parties is encoded, transmitted and decoded using the key $K_{AB}$. The protocol is secure if any third party $C$ finds it extremely hard (impossible in practice) to identify the key.

In a public key exchange protocol the two parties agree on a common key pooled from
A Summary of Recent and Old Results on the Security of the Diffie-Hellman Key Exchange Protocol

...of the exchange. We give a brief introduction to the discrete logarithm problem and the computational Diffie-Hellman problem, for more on these a reader can look at Koblitz and Menezes (2004) or Stinson (2005).

In the present work we are concerned with the practical security of this protocol. We investigate the various concepts of security and the known relationships between them. We interpret security in a probabilistic manner and devise a statistical test that will “assess” the security of the exchange in a given group. Our main objective is to find a test that would determine given two cyclic groups $G_1$ and $G_2$ with similar orders but perhaps different structures whether or not the security of the key exchange is the same using either group.

BACKGROUND

Traditionally the study of the security of the exchange was restricted to the verification of the following assumptions:

**The Discrete Logarithm Assumption (DL):** For a cyclic group $G$, generated by $g$, we are given $g$ and $g^a$, $a \in \mathbb{Z}_n$, the challenge is to compute $g^b$.

**The Computational Diffie-Hellman Assumption (CDH):** Given $g$, $g^a$, $g^b$ it is hard to compute $g^{ab}$.

Whether or not these assumptions are true in a given group generate the respective problems. For example we say that the Discrete Logarithm problem is hard in a given group if the DL assumption is satisfied in that group.

Clearly, if these assumptions are not satisfied then $C$, an adversary, can gain access to the key $g^{ab}$. The relationship between these two assumptions has been extensively studied. It is clear that the CDH assumption will not be satisfied in a group where finding the solution to the discrete logarithm problem is easy. In Maurer and Wolf (1999), Boneh...