PUBLIC KEY CRYPTOGRAPHY BASED ON SEMIGROUP ACTIONS

GÉRARD MAZE
Department of Mathematics
University of Zürich, Winterthurerstr 190
CH-8057 Zürich, Switzerland

CHRIS MONICO
Department of Mathematics and Statistics
Texas Tech University
Lubbock, TX 79409-1042, USA

JOACHIM ROSENTHAL
Department of Mathematics
University of Zürich, Winterthurerstr 190
CH-8057 Zürich, Switzerland

(Communicated by Andreas Stein)

ABSTRACT. A generalization of the original Diffie-Hellman key exchange in $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ found a new depth when Miller [27] and Koblitz [16] suggested that such a protocol could be used with the group over an elliptic curve. In this paper, we propose a further vast generalization where abelian semigroups act on finite sets. We define a Diffie-Hellman key exchange in this setting and we illustrate how to build interesting semigroup actions using finite (simple) semirings. The practicality of the proposed extensions rely on the orbit sizes of the semigroup actions and at this point it is an open question how to compute the sizes of these orbits in general and also if there exists a square root attack in general.

In Section 5 a concrete practical semigroup action built from simple semirings is presented. It will require further research to analyse this system.

1. INTRODUCTION

The (generalized) discrete logarithm problem is the basic ingredient of many cryptographic protocols. It asks the following question:

**Problem 1.1.** (see e.g. [26]). Given a finite group $G$ and elements $g, h \in G$, find an integer $n \in \mathbb{N}$ such that $g^n = h$.

Problem 1.1 has a solution if and only if $h \in \langle g \rangle$, the cyclic group generated by $g$. If $h \in \langle g \rangle$ then there is a unique integer $n$ satisfying $1 \leq n \leq \text{ord}(g)$ such that $g^n = h$. We call this unique integer the discrete logarithm of $h$ with base $g$ and we denote it by $\log_g h$.

2000 Mathematics Subject Classification: Primary: 94A60, 11T71; Secondary: 16Y60.

Key words and phrases: Public key cryptography, Diffie-Hellman protocol, one-way trapdoor functions, semigroup actions, simple semirings.

This work has been supported in part by the Swiss National Science Foundation under grant no. 107887.