Properties of certain semigroups and their potential as platforms for cryptosystems

P.H. Kroholler · S.J. Pride · W.A.M. Othman · K.B. Wong · P.C. Wong

Dedicated to the memory of Walter Douglas Munn.

Received: 30 December 2009 / Accepted: 15 April 2010 / Published online: 16 July 2010 © Springer Science+Business Media, LLC 2010

Abstract In this paper, we study some properties of semigroups with presentation \(<a, b : a^p = b^q, a^q = b^r>\). We will also study their potential as platforms for the Diffie-Hellman key exchange protocol.

Keywords Semigroups · Diffie-Hellman · Discrete logarithm problem · Key exchange protocol · Cryptosystems

1 Introduction

In the last ten or more years, there has been a lot of on-going research work to find more secure and efficient public key cryptosystems based on objects like non-abelian


P.H. Kroholler · S.J. Pride (✉)
Department of Mathematics, University of Glasgow, University Gardens, Glasgow G12 8QW, Scotland, UK
e-mail: stephen.pride@glasgow.ac.uk

P.H. Kroholler
e-mail: peter.kroholler@glasgow.ac.uk

W.A.M. Othman · K.B. Wong · P.C. Wong
Institute of Mathematical Sciences, University of Malaya, 50603 Kuala Lumpur, Malaysia
W.A.M. Othman
e-mail: wamanian@um.edu.my
K.B. Wong
e-mail: kbwong@um.edu.my
P.C. Wong
e-mail: wongpe@um.edu.my