Cryptology ePrint Archive: Report 2011/383

A representation of the p-sylow subgroup of $\perm(\F_p^n)$ and a cryptographic application

Stefan Maubach

Abstract: This article concerns itself with the triangular permutation group, induced by triangular polynomial maps over $\F_p$, which is a p-sylow subgroup of $\perm(\F_p^n)$. The aim of this article is twofold: on the one hand, we give an alternative to $\F_p$-actions on $\F_p^n$, namely $\Z$-actions on $\F_p^n$ and how to describe them as what we call ``$\Z$-flows". On the other hand, we describe how the triangular permutation group can be used in applications, in particular we give a cryptographic application for session-key generation. The described system has a certain degree of information theoretic security. We compute its efficiency and storage size.

To make this work, we give explicit criteria for a triangular permutation map to have only one orbit, which we call ``maximal orbit maps". We describe the conjugacy classes of maximal orbit maps, and show how one can conjugate them even further to the map $z\lp z+1$ on $\Z/p^n\Z$.

Category / Keywords: cryptographic protocols / Diffie-Hellmann session key exchange

Date: received 14 Jul 2011

Contact author: stefan maubach at gmail com