

Cryptology ePrint Archive: Report 2011/383

A representation of the p -Sylow subgroup of $\text{Perm}(\mathbb{F}_p^n)$ and a cryptographic application

Stefan Maubach

Abstract: This article concerns itself with the triangular permutation group, induced by triangular polynomial maps over \mathbb{F}_p , which is a p -Sylow subgroup of $\text{Perm}(\mathbb{F}_p^n)$. The aim of this article is twofold: on the one hand, we give an alternative to \mathbb{F}_p -actions on \mathbb{F}_p^n , namely \mathbb{Z} -actions on \mathbb{F}_p^n and how to describe them as what we call " \mathbb{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 $z \mapsto z+1$ on $\mathbb{Z}/p^n\mathbb{Z}$.

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

Date: received 14 Jul 2011

Contact author: stefan maubach at gmail com

Available formats: [PDF](#) | [BibTeX Citation](#)

Note: 21 pages

Version: 20110715:112914 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]