The Sidelnikov-Shestakov's Attack applied to the Chor-Rivest Cryptosystem

Sylvain Colin & Gaspard Férey

February 12, 2014

Contents

Abstract

In this article, we discuss about the Sidelnikov-Shestakov Attack on cryptosystems based on Reed-Solomon codes. Then we describe how this algorithm can be used to attack the Chor-Rivest Cryptosystem.

1 Introduction

sec:intro

1.1 Our Work

2 Preliminaries

sec:defnot

2.1 Generalized Reed-Solomon codes

3 Attack of Sidelnikov-Shestakov

4 Application to the Chor-Rivest Cryptosystem

5 Conclusions