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 A cryptosystem based on Reed-Solomon codes

We study here the public-key cryptosystem introduced by Niederreiter [1] applied to the generalized Reed-Solomon codes. Let $\mathbb{F}_q$ be a finite field with $q = p^h$ elements and $\mathbb{F} = \mathbb{F}_q \cup \{\infty\}$, where ∞ has natural properties ($1/\infty = 0$, etc). We call $\mathfrak{A}$ the following matrix:

$$\mathfrak{A}(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_n) := \begin{pmatrix} z_1\alpha_1^0 & z_2\alpha_2^0 & \cdots & z_n\alpha_n^0 \\ z_1\alpha_1^1 & z_2\alpha_2^1 & \cdots & z_n\alpha_n^1 \\ & & \ddots & \\ z_1\alpha_1^{k-1} & z_2\alpha_2^{k-1} & \cdots & z_n\alpha_n^{k-1} \end{pmatrix} \in \mathcal{M}_{\mathbb{F}_q}(k, n)$$

2.2 Equivalence between Reed-Solomon codes

Sidelnikov and Shestakov show [2] that for all $a \in \mathbb{F}_q - \{0\}$ and $b \in \mathbb{F}_q$, there exists $H_1, H_2, H_3 \in \mathcal{M}_{F_q}(k, k)$ invertible such that

$$\begin{aligned} H_1\mathfrak{A}(a \cdot \alpha_1 + b, \ldots, a \cdot \alpha_n + b, c_1z_1, \ldots, c_nz_n) &= \mathfrak{A}(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_n) \\ H_2\mathfrak{A}\left(\frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_n}, d_1z_1, \ldots, d_nz_n\right) &= \mathfrak{A}(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_n) \\ H_3\mathfrak{A}(\alpha_1, \ldots, \alpha_n, a \cdot z_1, \ldots, a \cdot z_n) &= \mathfrak{A}(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_n) \end{aligned}$$

This means that for any cryptosystem $M = H\mathfrak{A}(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_n)$, for any birationnal transformation

$$\phi : x \mapsto \frac{ax + b}{cx + d}$$

$M = H_\phi\mathfrak{A}(\phi(\alpha_1), \ldots, \phi(\alpha_n), z'_1, \ldots, z'_n)$ and by using the unique transformation ϕ that maps $(\alpha_1, \alpha_2, \alpha_3)$ to $(0, 1, \infty)$, we get that for any cryptosystem $M = H\mathfrak{A}(\alpha_1, \ldots, \alpha_n, z_1, \ldots, z_n)$, M can be uniquely written

$$M = H'\mathfrak{A}(0, 1, \infty, \alpha'_4, \ldots, \alpha'_n, 1, z'_2, \ldots, z'_n)$$

with H' invertible, $z'_i \neq 0$ and α_i distincts elements of $\mathbb{F}_q - \{0, 1, \infty\}$.

3 Attack of Sidelnikov-Shestakov

4 Application to the Chor-Rivest Cryptosystem

5 Conclusions

References

NiederH86 [1] H. Niederreiter. Knapstack-type cryptosystems and algebraic coding theory. *Probl. Control and Inform. Theory*, 15:19–34, 1986.

SidelShes92 [2] V. M. Sidelnikov and S. O. Shestakov. On insecurity of cryptosystems based on generalized reed-solomon codes. *Discrete Math. Appl.*, 2(4).