Some weak keys in McEliece public-key cryptosystem

Pierre Loidreau
INRIA, Projet CODES, B.P. 105
78153 Le Chesnay , FRANCE
Email Pierre.Loidreau@inria.fr

Nicolas Sendrier
INRIA, Projet CODES, B.P. 105
78153 Le Chesnay , FRANCE
Email Nicolas.Sendrier@inria.fr

Abstract — **We show that the Goppa codes $\Gamma(L, g)$ where g is a binary polynomial constitute a recognizable family of weak keys for McEliece cryptosystem, thus inducing naturally a structural attack against the system.**

I. Introduction

In this paper we identify a set of weak keys of McEliece system - Goppa codes generated by binary polynomials - thanks to a polynomial time algorithm which recovers part of the automorphism group of a code. Such codes indeed have a non trivial automorphism group which in general is the group of automorphism of the field used as support of the code.

II. Goppa codes and idempotents

Let $GF(2^m)$ denote the field with 2^m elements. We will denote $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ an ordered subset of distinct elements of $GF(2^m)$ of cardinality n used to index the elements of $GF(2)^n$. For any $c \in GF(2)^n$ and any $\beta \in L$, we will denote c_β the position indexed by β and $c = (c_\beta)_{\beta \in L} = (c_{\alpha_1}, c_{\alpha_2}, \ldots, c_{\alpha_n})$.

We consider binary codes of length $n = 2^m$ and of support $L = GF(2^m) = \{\alpha_1, \ldots, \alpha_n\}$. Two such codes C and C' are equivalent if there exists a permutation τ of L such as
$C' = \tau(C) = \{(c_{\alpha_1}, \ldots, c_{\alpha_n}) \mid (c_{\tau(\alpha_1)}, \ldots, c_{\tau(\alpha_n)}) \in C\}$

Definition 1 *The Goppa code $\Gamma(L, g)$ is the set of words $c = (c_{\alpha_i})_{i=1}^n \in GF(2)^n$ such as*
$\sum_{i=1}^n c_{\alpha_i}/(z + \alpha_i) \equiv\ 0 \bmod\ g(z)$

Proposition 2 *If the coefficients of $g(z)$ are in $GF(2)$ then the automorphism group of $\Gamma(L, g)$ contains the Frobenius field automorphism of $GF(2^m)$. That is*
$(c_{\alpha_1}, c_{\alpha_2}, \ldots, c_{\alpha_n}) \in \Gamma(L, g) \Leftrightarrow (c_{\alpha_1^2}, c_{\alpha_2^2}, \ldots, c_{\alpha_n^2}) \in \Gamma(L, g)$

McEliece public-key cryptosystem can be described as follows:

Let Γ be a binary Goppa code. The procedure Φ_Γ used below can be easily derived from the decoding procedure of Γ.

Secret key: The code Γ, a $k \times k$ non-singular matrix S, a $n \times n$ permutation matrix P.

Public key: $G' = SGP$,
where G is a generating matrix of Γ.

Encryption: $m \longmapsto mG' + e$,
where e is a random vector of weight t.

Decryption: $y \longmapsto \Phi_\Gamma(yP^{-1})S^{-1}$,
$\Phi_\Gamma(xG + e) = x$ whenever the weight of e is t or less.

The code of generating matrix G' is equivalent to the secret Goppa code. In its original paper [4], McEliece uses the family of binary Goppa codes of length 1024 with Goppa polynomials of degree 50.

We will consider a particular subclass of Goppa codes; those defined by a polynomial with binary coefficients. In these codes, the codewords whose supports are invariant under the action of the Frobenius field automorphism are called idempotents. A word $c \in GF(2)^n$ is an *idempotent* if any of the following statement is true:

1. the support of c is invariant under the Frobenius,
2. the support of c is the union of conjugation cosets of L,
3. the locator polynomial of c has its coefficients in $GF(2)$.

Note also that the subset of all idempotents is a subspace of $GF(2)^n$, we will call its intersection with $\Gamma(L, g)$ the *idempotent subcode* of $\Gamma(L, g)$, denoted $\mathcal{I}(L, g)$.

III. Weak keys in McEliece cryptosystem

A *signature* is a mapping taking as argument a code C and an element β of L such as for any permutation τ of L, we have $S(C, \beta) = S(\tau(C), \tau(\beta))$. It is said to be *discriminant* for a given code C if there exist $\beta \neq \gamma$ such as $S(C, \beta) \neq S(C, \gamma)$.

The support splitting algorithm takes a code with a trivial automorphism group as an argument and returns with high probability the most discriminant signature for the code, and thus the conjugation cosets of the support of the code through its automorphism group. Provided the hull of the code is not too large, it is a polynomial time algorithm.

We will denote $\mathcal{SA}(C)$ the signature returned by the algorithm for the input C. The automorphism group of a Goppa codes using a binary polynomial contains the group generated by the Frobenius automorphism.

Thus, the exhaustive attack can be described as follows: Given a code C' used as public key in an instance of McEliece cryptosystem,

1. Compute $S = \mathcal{SA}(C')$,
2. If the partition associated to S and C' is not “conjugation cosets like” then EXIT else —
3. For all $g(z)$ in $GF(2)[z]$ relatively prime to $z^{1024} - z$ and square-free, compute $S_g = \mathcal{SA}(\Gamma(L, g))$, if $S_g = S$ then RETURN$(g(z))$

References

[1] E. Bombieri, Exponential Sums in Finite Fields, *Am. J. Math.*, vol. 88, pp.71-105, 1966.

[2] A. Canteaut, F. Chabaud, A New Algorithm for Finding Minimum-Weight words in a Linear Code: Application to McEliece's Cryptosystem and to Narrow-Sense BCH Codes of length 511, *IEEE Trans. Inf. Theo*, vol 44-1, pp 367-378, 1998.

[3] V .D Goppa, A new class of linear error-correcting codes, *Probl. Peredach. Inf*, vol 6, pp 24-30, 1971.

[4] R.J. McEliece, A public-key cryptosystem based on algebraic coding theory, *DSN Progress Report*, pp. 114-116, 1978.

[5] H. Niederreiter, Knapsack-type cryptosystems and algebraic coding theory, *Prob. Cont. Info. Theo*, vol 15. pt. 2, 1986.

[6] N. Sendrier, Finding the permutation between equivalent binary codes, *IEEE Conference, ISIT'97, Ulm Germany.*

[7] N. Sendrier, On the dimension of the hull, *SIAM J. App. Math*, vol 10, pp. 282-293, 1997.