Large Weight Patterns Decoding in GOPPA codes and Application to Cryptography

Pierre Loidreau
Project CODES, INRIA
Rocquencourt
Domaine de Voluceau, B.P. 105
78 153 Le Chesnay CEDEX, France
e-mail: Pierre.Loidreau@inria.fr

Abstract — **By using the action of the FROBENIUS group it is possible to decode far beyond the error-correcting capability of GOPPA codes provided the error-vector has a definite structure. In particular cases the generation of these patterns can be easily described and gives a number of decodable patterns numerous enough to avoid enumeration. We show that it is possible to use this property to strengthen the MCELIECE-type cryptosystems against attacks based on random decoding.**

I. INTRODUCTION

We present a method to decode error-patterns of large weight in GOPPA codes by using a subgroup of the automorphism group of the GOPPA codes. Namely, we use the group generated by the FROBENIUS automorphism. By its action on the large weight error-patterns one obtains error-patterns of weight less than the error-correcting capability of the code.

The efficiency of this method and the number of decodable patterns depend on the nature of the FROBENIUS group. In a well chosen case we show that it is possible to decode a large number of patterns with weight one and a half larger than the error-correcting capability of the code. These patterns being easily generated, they can be used to improve the work factor of the random decoding attack on the MCELIECE public-key cryptosystem without increasing the size of the public-key.

II. AUTOMORPHISM GROUP OF GOPPA CODES

GOPPA codes are a subfamily of alternant codes generated by a polynomial g of degree t over a finite field $\mathrm{GF}(2^m)$. The set $L = (\alpha_1, \dots, \alpha_n)$ of elements in L that are not roots of g is denoted generating vector. The GOPPA code $\Gamma(L, g)$ of length $n = |L|$ is the set of binary words $a = (a_{\alpha_1}, \dots, a_{\alpha_n})$ such that

$$\mathrm{H}.^t a = 0$$

where $\mathrm{H} = \left(\alpha_j^i / g(\alpha_j)\right)_{i=0,j=1}^{t-1,n}$.

Generally, the automorphism group of a GOPPA code is trivial. However, we showed that when the generating polynomial g has coefficients over a subfield $\mathrm{GF}(2^s)$ of $\mathrm{GF}(2^m)$, the automorphism group contains the group generated by the FROBENIUS automorphism σ of $\mathrm{GF}(2^m)/\mathrm{GF}(2^s)$. [2]

III. TOWER DECODABLE PATTERNS

Suppose one receives the word

$$c = m + e$$

where m is a word in $\Gamma(L, g)$, g is taken over $\mathrm{GF}(2^s)$ and e is an error-vector. If the weight of e is less than the error-correcting capability t of the code then one recovers m easily. Since the automorphism group of the code contains the group generated by the FROBENIUS automorphism σ of $\mathrm{GF}(2^m)/\mathrm{GF}(2^s)$, any linear combination $\sum_{i=0}^{m/s-1} \epsilon_i^{(u)} \sigma^i(m)$ of the transformed of m through the FROBENIUS is in $\Gamma(L, g)$. The transform of the error pattern e becomes $\sum_{i=0}^{m/s-1} \epsilon_i^{(u)} \sigma^i(e)$ and we say that

Definition 1 *e is tower decodable in $\Gamma(L, g)$ if*

1. *There exists linear combinations indexed by u*

$$\mathcal{E}^{(u)} = \sum_{i=0}^{m/s-1} \epsilon_i^{(u)} \sigma^i(e)$$

of the $\sigma^i(e)$ such that the $\mathcal{E}^{(u)}$ can be decoded in the GOPPA code $\Gamma(L, g)$,

2. *the knowledge of some of the $\mathcal{E}^{(u)}$ enables the receiver to recover the error-pattern e with a certain probability.*

IV. APPLICATION TO MCELIECE CRYPTOSYSTEM

We take the MCELIECE parameters [3] that is, the private key is a generating matrix of a GOPPA code $\Gamma(L, g)$ where L is an indexation of $\mathrm{GF}(2^{10})$ and g is irreducible over $\mathrm{GF}(2^{10})$ of degree 50. The error-correcting capability of the code is 50. The public key is the scrambled private key. The best known work factor for the attack by random decoding is 2^{64} [1].

In our scheme we take g over $\mathrm{GF}(2^2) \subset \mathrm{GF}(2^{10})$. Hence, the Frobenius group has cardinality 5. The public-key is the scrambled private key reordered according to the orbits of the Frobenius group. By randomly chosing a number of 25 orbits out of 204 and placing randomly 3 bits on every chosen orbit we construct tower decodable patterns of weight 75. The number of such patterns is 2^{188}. For the decoding, we need to decode at most two words. The size of the public-key is the same as in the original scheme whereas the work factor of the attack by random decoding becomes 2^{90}.

REFERENCES

[1] A. CANTEAUT and 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 Transactions Information Theory*, 44(1):367–378, January 1998.

[2] P. LOIDREAU. Codes derived from binary GOPPA codes. *S*ixth International workshop on Algebraic and Combinatorial Coding Theory, sept. 1998, Pskov, Russia

[3] R. J. MCELIECE. A public-key cryptosystem based on algebraic coding theory. Technical report, Jet Propulsion Lab. DSN Progress Report, 1978.