Equivalent Goppa Codes and Trapdoors to McEliece's Public Key Cryptosystem

J. K. Gibson

Department of Computer Science, Birkbeck College,
Malet Street, London WC1E 7HX, England

Abstract

We show that contrary to a published statement, any instance of McEliece's Public Key Cryptosystem always has many trapdoors. Our proof leads to a natural equivalence relation on monic polynomials over a finite field F such that any two irreducible Goppa codes over F whose Goppa polynomials are equivalent under this relation are equivalent as codes.

1. Introduction

McEliece [7] introduced the idea of using an error correcting code as the basis of a Public Key Cryptosystem, which we abbreviate to PKC. Let C be a linear code which corrects t errors and for which a fast decoder is known, and let G be a generator matrix for C such that it is hard to find any fast decoder for C from knowledge of G. To encipher a message M, introduce t random errors and encode the result with G. In the McEliece PKC, C is an irreducible binary Goppa code. Since for an arbitrary linear code finding the nearest codeword to a given received word is an NP-complete problem, it can be expected that only the holder of the decoder for C will be able to decrypt messages. Thus the decoder acts as a trapdoor to the decipherment function and is the secret key of the system, while G is the public key. Experience with the knapsack PKC has shown however that the NP-completeness of a problem used to construct a PKC in this way is no guarrantee of security, since only special cases of the problem are used [2]. Part of the difficulty lies in the fact that there may be many

D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 517-521, 1991.

trapdoors to a given decipherment function. Adams and Meijer [1] state that for the McEliece system there is usually only one. We show that their statement is incorrect, although there are probably sufficiently few that finding one by brute force is out of the question. A more serious cloud has been cast on the security of the McEliece PKC by the announcement by Korzhik and Turkin [5] of an algorithm for decoding a linear code that succeeds for received words whose distance from the nearest codeword is strictly less than half the minimum distance of the code, and which is polynomial in the length of the code. They do not find a trapdoor for the McEliece PKC, and indeed they estimate a time of 60 hours on a personal computer to decipher one block of ciphertext. Their algorithm assumes the usual Hamming metric, so Gabidulin [3] has suggested using codes that employ a non-Hamming metric instead.

There are two main thrusts to this paper. The first is an examination of just what is involved in finding a fast decoder for an irreducible binary Goppa code when its generator matrix G is given. We show there are many fast decoders, each corresponding to a permutation of the columns of G. Each such permutation may be regarded as a trapdoor to the instance of the McEliece PKC with public key G. The second thrust is the introduction of an equivalence relation ~ on the set P of monic polynomials of degree t over $F = GF(2^m)$. We define $g \sim h$ if some affine transformation over F composed with some automorphism of F maps roots of g to roots of h, and show that any two irreducible Goppa codes over F with equivalent Goppa polynomials are equivalent as codes. Although the converse is not true, this does suggest that it would be worthwhile to count and classify the equivalence classes of P, which has not to our knowledge been previously attempted. Some results in this direction have been obtained, and will appear in a forthcoming paper. Certainly it can be hoped that this kind of detailed study of the structure of Goppa codes will lead eventually to a determination of whether or not the problem of finding a trapdoor to an instance of the McEliece PKC is NP-complete.

There is not a large body of literature on the McEliece PKC. Several authors [1] [6] [9] show how to reduce the work needed to decipher messages without finding a trapdoor. Heiman [4] is the only previous author to address the problem of finding a trapdoor. Goppa codes are a special case of the class of Alternant codes [8], and Heiman shows how to find a fast decoder for any Alternant code

from its generator matrix. Fortunately the irreducible binary Goppa codes used in the McEliece PKC have fast decoders that will correct more errors, twice as many in fact, as Heiman's decoders will, and they are the only Alternant codes known with this property! The papers [3] [5] already referred to complete the current picture.

2. Finding a fast decoder from the generator matrix

Let F = GF(n), $n = 2^m$, and let $\alpha = (\alpha_0, \alpha_1 \ldots \alpha_{n-1})$ be any vector of all the n members of F. Let g be an irreducible monic polynomial of degree t over F. The irreducible binary Goppa code of degree t with field vector α and Goppa polynomial g is the code $\Gamma(\alpha, g)$ whose codewords are the binary vectors $c = (c_0, c_1 \ldots c_{n-1})$ with $\sum_{i=0}^{n-1} c_i/(x-\alpha_i) = 0 \mod g(x)$. $\Gamma(\alpha, g)$ is determined up to equivalence by g, and knowledge of α and g provides a fast decoder correcting up to t errors. More details can be found in [8].

To create an instance of the McEliece PKC from a k × n generator matrix G for Γ, a designer chooses at random a non-singular k × k binary matrix S, and an n × n permutation matrix P, and uses K = SGP as the public key. Let C denote the code whose generator matrix is K. We examine in this section the task that a cryptanalyst faces in finding a fast decoder for C that corrects t errors, and show in the next that there are many such decoders.

An important point, first noted by Heiman [4], is that the matrix S has no cryptographic significance, though it may be useful in hiding any obvious structure of G. The reason is simply that S does not change the set of codewords of C, and messages can be recovered from codewords using K without knowing what S is. We now show that in a sense, P has no cryptographic significance either. We show that if α permuted with P can be found then a fast decoder for C correcting t errors can be obtained easily. In other words, a trapdoor is just a suitable field vector.

The cryptanalyst first chooses a representation of F, and any vector $\rho = (\rho_0, \rho_1 \ldots \rho_{n-1})$ of all the n members of F. He then seeks a permutation of the coordinates of ρ that transforms ρ into $\omega = (\omega_0, \omega_1 \ldots \omega_{n-1})$ for which $C = \Gamma(\omega, h)$ for some h. (An entirely equivalent procedure is to keep ρ fixed and look for a suitable permutation of the columns of K). g and α permuted with P are known to be possible values for h and ω, but there are many others. Once ω is found, h, and consequently a fast decoder for C, can be found

quickly by a method described in [8] p341 in a different context. The rows of K are codewords of C. Let $c = (c_0, c_1 \ldots c_{n-1})$ be any codeword of C, and let $p(x) = \prod_{i=0}^{n-1} c_i(x-\omega_i)$. Then the formal derivative p' of p is a multiple of h^2. Thus the cryptanalyst has only to find ω for which the polynomials p' obtained using each row of K have non-trivial greatest common divisor.

We will show that there are at least mn(n-1) permutations that work, and each may be regarded as a trapdoor to the instance of the McEliece PKC with public key K. McEliece suggested m = 10, giving the cryptanalyst over 10 million permutations to choose from, though since they have to be selected from all 1024! permutations of the coordinates of ρ he will not find one by brute force.

3. The equivalence of codes and polynomials

Let F = GF(n), $n = 2^m$. Let $\alpha = (\alpha_0, \alpha_1 \ldots \alpha_{n-1})$ be any vector of all the n members of F. Let g be an irreducible monic polynomial of degree t over F. Let $a, b \in F$, $a \neq 0$. We use the same symbol b to denote the n-vector (b,b ... b). Let j be an integer, $0 \leq j < m$. Let h be the be the monic polynomial of degree t over F for which $a^t[g(x)]^{2^j} = h(ax^{2^j}+b)$, and let $\rho = (\rho_0, \rho_1 \ldots \rho_{n-1}) = a\alpha^{2^j}+b$, powers of a vector being taken coordinatewise. It is not difficult to show that if $c = (c_0, c_1 \ldots c_{n-1})$ is any binary n-vector then $\sum_{i=0}^{n-1} c_i/(x-\alpha_i) = 0 \bmod g(x)$ if and only if $\sum_{i=0}^{n-1} c_i/(x-\rho_i) = 0 \bmod h(x)$, ie. $\Gamma(\alpha,g) = \Gamma(\rho,h)$. This prompts what follows.

Let P be the set of monic polynomials of degree t over F. Define the equivalence relation ~ on P by $g \sim h$ if for some $a, b \in F$, $a \neq 0$, and some integer j, $0 \leq j < m$, $a^t[g(x)]^{2^j} = h(ax^{2^j}+b)$. Equivalently $g \sim h$ if, in the splitting field of g, some affine transformation over F composed with some automorphism of F maps roots of g to roots of h. In terms of coefficients, $\sum_{i=0}^{t} g_i x^i \sim \sum_{i=0}^{t} a^{t-i} g_i^{2^j} (x+b)^i$.

It is clear that any two irreducible Goppa codes over F with equivalent Goppa polynomials are equivalent as codes. Indeed this is true for any two codes of the same length and degree, whether irreducible or not. The converse is not true. The irreducible Goppa codes over GF(32) with Goppa polynomials $x^6 + x + 1$ and $x^6 + x^5 + 1$ are equivalent codes with inequivalent polynomials.

Let L denote the group generated under composition by affine

transformations over F and automorphisms of F. Then the order of L is mn(n-1), and each member of L applied to the coordinates of a vector α of all the n members of F maps α to a different vector, justifying the assertion made in the last section that there are at least mn(n-1) successful permutations available to a cryptanalyst of an instance of the McEliece PKC of degree t over F with given public key K. There may be far more. If eg. two columns of K are equal, any successful permutation composed with the appropriate interchange will be successful, though it will not in general be a permutation induced by any member of L. This happens when m = 3 and t = 2.

Summarising, let α,ρ be vectors of all the n members of F, and let g,h be irreducible monic polynomials of the same degree over F. If a member of L maps α to ρ and roots of g to roots of h then $\Gamma(\alpha,g) = \Gamma(\rho,h)$. There will always be more than one polynomial describing $\Gamma(\alpha,g)$ up to equivalence, but there may be fewer than mn(n-1). The exact number will be discussed in a forthcoming paper.

References

[1] ADAMS C.M. and MEIJER H. 'Security Related Comments Regarding McEliece's Public-Key Cryptosystem'. Lecture Notes in Computer Science vol 293, Eurocrypt 87. Springer-Verlag 1987.

[2] BRICKELL E.F. 'Breaking Iterated Knapsacks'. Lecture Notes in Computer Science vol 196, Crypto 84. Springer-Verlag 1984.

[3] GABIDULIN E.M. 'Ideals over a Non-Commutative Ring and their Applications in Cryptography'. These Proceedings.

[4] HEIMAN R. 'On the Security of Cryptosystems Based on Linear Error Correcting Codes'. MSc. Thesis, Feinberg Graduate School of the Weizmann Institute of Science. August 1987.

[5] KORZHIK V.I. and TURKIN A.I. 'Cryptanalysis of McEliece's Public Key Cryptosystem'. These Proceedings.

[6] LEE P.J. and BRICKELL E.F. 'An Observation on the Security of McEliece's Public Key Cryptosystem'. Lecture Notes in Computer Science vol 330, Eurocrypt 88. Springer-Verlag 1988.

[7] McELIECE R.J. 'A Public Key Cryptosystem Based on Algebraic Coding Theory'. DSN Progress Report (Jan,Feb), Jet Propulsion Lab., Calif. Inst. Tech. 1978.

[8] McWILLIAMS F.J.and SLOANE N.J. 'The Theory of Error Correcting Codes'. North Holland Publishing Co. 1977.

[9] Van TILBURG J. 'On the McEliece Public Key Cryptosystem.' Lect. Notes in Comp. Sc. vol 403, Crypto 88. Springer-Verlag 1988.