Problems of Control and Information Theory, Vol. 15 (2), pp. 159—166 (1986)

KNAPSACK-TYPE CRYPTOSYSTEMS AND ALGEBRAIC CODING THEORY

H. NIEDERREITER

(*Vienna*)

(Received April 16, 1985)

Recently Chor and Rivest proposed a knapsack-type public-key cryptosystem for low-weight message vectors. We introduce cryptosystems of this type involving public keys with fewer bits and yielding a higher information rate than the Chor–Rivest cryptosystem. The design of these cryptosystems is based on techniques from algebraic coding theory.

1. Introduction

In the last decade the field of cryptography, which is concerned with the design of systems for the communication of secret information, has undergone a dramatic development stimulated by the introduction of public-key cryptosystems in the fundamental paper of Diffie and Hellman [3]. In a *public-key cryptosystem*, the encryption keys of all correspondents are available in a public directory, whereas each correspondent keeps his decryption key secret. If correspondent B wants to send a confidential message to correspondent A, he looks up A's encryption key in the directory, uses this key to encipher the message, and transmits the resulting ciphertext to A. If the cryptosystem is well designed, then only A can recover the original message in a reasonable amount of time by applying his decryption key.

Various types of public-key cryptosystems are known today. The principles of most of them can be traced back to the RSA cryptosystem of Rivest, Shamir, and Adleman [13] and the knapsack cryptosystem of Merkle and Hellman [11]. As a representative sample of recent proposals we mention the Massey–Omura lock (see [18]), the public-key cryptosystem of ElGamal [4], the FSR cryptosystems of the author [12], and the knapsack-type cryptosystem of Chor and Rivest [2]. Knapsack-type cryptosystems are based on the difficulty of recovering the summands from the value of their sum. Information on cryptosystems can be found in the books of Beker and Piper [1] and Lidl and Niederreiter [8].

In this paper we introduce a class of knapsack-type public-key cryptosystems that are based on devices from algebraic coding theory. We recall that a *linear* (n, k) *code*

Akadémiai Kiadó, Budapest
Pergamon Press, Oxford

C over the finite field F_q of order q is a k-dimensional linear subspace of the n-dimensional vector space F_q^n over F_q, where $1 \leqq k < n$. Thus C contains exactly q^k code words. For a row vector $\mathbf{y} \in F_q^n$ we define the *weight* $w(\mathbf{y})$ to be the number of nonzero coordinates of $\mathbf{y}$, and for $\mathbf{x}, \mathbf{y} \in F_q^n$ we let $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$ be the Hamming distance. The *minimum distance* of C is defined as the smallest weight of a nonzero code word of C. If t is a positive integer, then C is called *t-error-correcting* if for any $\mathbf{y} \in F_q^n$ there is at most one $\mathbf{c} \in C$ such that $d(\mathbf{y}, \mathbf{c}) \leqq t$. If C has minimum distance d, then the largest error-correcting capability of C is $t = \lfloor (d-1)/2 \rfloor$. For a general background on algebraic coding theory we refer to the books of MacWilliams and Sloane [9] and van Lint [17].

We will compare our cryptosystems with the recent knapsack-type cryptosystem of Chor and Rivest [2], and so we briefly describe the latter cryptosystem. Let F_q be a publicly known finite field with $q = p^t$, p prime, $t \geqq 2$, and choose a primitive element β of F_q at random. The field F_q should be such that it is feasible to calculate the discrete logarithm ind (α) of any nonzero element α of F_q, where $a = \text{ind}\,(\alpha)$ is the unique integer with $\alpha = \beta^a$ and $0 \leqq a \leqq q-2$. For well-chosen (but secret) elements $\alpha_1, \ldots, \alpha_p$ of F_q calculate the integers $a_i = \text{ind}\,(\alpha_i)$, $1 \leqq i \leqq p$, and scramble them by applying a random permutation and a random shift. The resulting integers $c_1, \ldots, c_p$ form the public key, the random data are kept secret. With this cryptosystem we encipher binary messages $\mathbf{m} = (m_1, \ldots, m_p) \in F_2^p$ of length p and weight $< t$. The ciphertext corresponding to $\mathbf{m}$ is the integer $E(\mathbf{m})$ with $0 \leqq E(\mathbf{m}) \leqq p^t - 2$ and

$$E(\mathbf{m}) \equiv \sum_{i=1}^{p} m_i c_i \bmod (p^t - 1) .$$

A crucial lemma (in a corrected form given in Lidl and Niederreiter [8, Ch. 9]) shows that distinct message vectors of the type above are mapped into distinct ciphertexts. The decryption of ciphertexts is possible on the basis of the secret information (compare with [2], [8, Ch. 9]).

2. The cryptosystems

We first describe a *conventional cryptosystem* which is a prototype of our public-key cryptosystem. Choose a t-error-correcting linear (n, k) code C over F_q. Good choices for C will be discussed in Section 3. Let H be a parity-check matrix of C, i.e. H is an $(n-k) \times n$ matrix over F_q of rank $n-k$ such that C consists exactly of all $\mathbf{c} \in F_q^n$ with $H\mathbf{c}^T = \mathbf{0}$, where $\mathbf{c}^T$ denotes the transpose of $\mathbf{c}$. The cryptosystem depends on the simple but crucial fact that the matrix H yields a mapping from F_q^n to F_q^{n-k} that is one-to-one when restricted to vectors of weight $\leqq t$.

Lemma. If $H\mathbf{y}^T = H\mathbf{z}^T$ for some $\mathbf{y}, \mathbf{z} \in F_q^n$ with $w(\mathbf{y}) \leqq t$ and $w(\mathbf{z}) \leqq t$, then $\mathbf{y} = \mathbf{z}$.

Proof. From $H\mathbf{y}^T = H\mathbf{z}^T$ we get $H(\mathbf{y}-\mathbf{z})^T = \mathbf{0}$, hence $\mathbf{y}-\mathbf{z} = \mathbf{c}$ for some $\mathbf{c} \in C$. Now $d(\mathbf{y}, \mathbf{0}) = w(\mathbf{y}) \leqq t$ and $d(\mathbf{y}, \mathbf{c}) = w(\mathbf{y}-\mathbf{c}) = w(\mathbf{z}) \leqq t$, and so we must have $\mathbf{c} = \mathbf{0}$ by the definition of a t-error-correcting code. Therefore $\mathbf{y} = \mathbf{z}$.

In the conventional cryptosystem we keep H secret and encipher a plaintext message $\mathbf{y} \in F_q^n$ of weight $\leqq t$ as the ciphertext $H\mathbf{y}^T$. Upon receipt of this ciphertext, we can recover $\mathbf{y}$ uniquely. Note that in the language of algebraic coding theory $H\mathbf{y}^T$ is the syndrome of $\mathbf{y}$ with respect to the code C. Since $d(\mathbf{y},\mathbf{0}) = w(\mathbf{y}) \leqq t$, we may view $\mathbf{y}$ as an error vector relative to the code word $\mathbf{0}$. Therefore, an application of the decoding algorithm of C to the syndrome $H\mathbf{y}^T$ will yield the error vector $\mathbf{y}$.

To obtain a *public-key cryptosystem* from this conventional cryptosystem, we form a scrambled version of the matrix H and take it as a public key. This can be done in various ways. For instance, we may use the following scrambling device employed in the Goppa-code cryptosystem (see [8, Ch. 9]): premultiply H by a randomly chosen nonsingular $(n-k) \times (n-k)$ matrix M over F_q and postmultiply by a randomly chosen $n \times n$ matrix P over F_q that is obtained by permuting the rows of a nonsingular diagonal matrix. The matrices M, H, and P are kept secret, whereas the $(n-k) \times n$ matrix $K = MHP$ serves as the public key. A plaintext message $\mathbf{y} \in F_q^n$ of weight $\leqq t$ is now enciphered as $K\mathbf{y}^T$. Thus the ciphertexts are column vectors over F_q of length $n-k$. Upon receipt of the ciphertext $K\mathbf{y}^T = MHP\mathbf{y}^T$, we premultiply it by M^{-1} to get $HP\mathbf{y}^T = H(\mathbf{y}P^T)^T$. Note that $\mathbf{y}P^T$ is again a vector of weight $\leqq t$. Therefore we can obtain $\mathbf{y}P^T$ by the same method as in the conventional cryptosystem, namely by applying the decoding algorithm of C. Postmultiplying by $(P^T)^{-1}$, we recover the original message $\mathbf{y}$.

In the binary case $q = 2$ this cryptosystem is of the classical knapsack type. The ciphertext $K\mathbf{y}^T$ is then just a sum of at most t column vectors of the public-key matrix K, and determining $\mathbf{y}$ is equivalent to deciding which column vectors of K yield the given sum $K\mathbf{y}^T$. For general q, the ciphertext $K\mathbf{y}^T$ is a linear combination of at most t column vectors of K with coefficients from F_q, and finding $\mathbf{y}$ is equivalent to determining this linear combination explicitly.

3. The choice of codes

A brief inspection of the construction of our cryptosystems shows that a code C suitable for our purposes should satisfy the following requirements: (i) C should have a relatively large error-correcting capability (or equivalently a large relative distance d/n) so that a reasonable number of message vectors can be used; (ii) C should allow an efficient decoding algorithm so that the decryption can be carried out with a short run time. Further analysis reveals that the dimension k of C should be in a medium range relative to the length n. For if k is too small, then there are relatively few good codes of

dimension k, which makes it easier to break the cryptosystem. On the other hand, if k is too close to n, this results in short ciphertexts, which again imperils the security of the cryptosystem.

There are various classes of linear codes that satisfy the criteria above. A benchmark for the quality of a code is provided by the Gilbert–Varshamov bound (see [9, Ch. 17], [17, Ch. 5]). A family of good codes should meet this bound, at least asymptotically. A well-known family of codes that meet this bound is given by alternant codes, and these codes also allow an efficient decoding algorithm (see [9, Ch. 12]). An important subclass of alternant codes is formed by Goppa codes, which have the advantage that they can be described quite easily in terms of a suitable polynomial. Goppa codes still meet the Gilbert–Varshamov bound (see [17, Ch. 8]). According to a result of Sarwate [14], a t-error-correcting Goppa code of length n can be decoded in $0(n \log^2 n)$ arithmetic operations for fixed t/n. For a detailed description of the decoding algorithm for Goppa codes see Lidl and Niederreiter [8, Ch. 8] and McEliece [10, Ch. 8]. There is another family of good linear codes introduced recently by Goppa [5], namely his algebraic geometry codes. This family contains codes that even go beyond the Gilbert–Varshamov bound for sufficiently large q (see [15], [16]), but on the other hand the decoding problem has not yet been solved satisfactorily.

Another suitable class of codes is given by Reed–Solomon codes (see [9, Ch. 10]). These codes are of interest since they are maximum distance separable, i.e. they achieve equality in the Singleton bound $d \leqq n-k+1$ for linear codes. A Reed–Solomon code is a cyclic code of length $n=q-1$ over F_q with generator polynomial

$$g(x)=(x-\beta^b)(x-\beta^{b+1}) \ldots (x-\beta^{b+d-2}),$$

where the integer $b \geqq 0$ is arbitrary, β is a primitive element of F_q, and any d with $2 \leqq d \leqq n$ may be prescribed. The minimum distance of this code is d and its dimension is $k=n-d+1$. Reed–Solomon codes belong to the well-known family of BCH codes and thus allow an efficient decoding algorithm. In fact, Justesen [6] has shown that a t-error-correcting Reed–Solomon code of length n can be decoded in $0(n \log^2 n)$ arithmetic operations for fixed t/n. Reed–Solomon codes are also instrumental in building concatenated codes of excellent quality, such as the Justesen codes (see [9, Ch. 10]).

4. Discussion

The most desirable property of a public-key cryptosystem is of course its ability to withstand attempts at breaking it. Possible attacks can be directed against two targets, either the deciphering of a specific ciphertext without knowledge of the secret keys, or the more ambitious goal of determining the secret keys M, H, and P. The latter task is complicated by the fact that the "factorization" $K=MHP$ of the public key is by

no means unique. This is in marked contrast to the RSA cryptosystem, where one can at least rely on the unique factorization of integers.

Even if k and $n-k$ are only moderately large, a brute-force attack on the secret keys based on trying all possibilities is hopeless. Note that the number of possibilities for M is equal to the number of nonsingular $(n-k)\times(n-k)$ matrices over F_q, which is

$$q^{(n-k)^2}\prod_{j=1}^{n-k}(1-q^{-j})$$

by a well-known formula (see [7, p. 401]). The number of possibilities for the code C is equal to the number of k-dimensional linear subspaces of F_q^n, which is

$$\prod_{j=0}^{k-1}(q^{n-j}-1)(q^{k-j}-1)^{-1}$$

by [7, p. 456]. The number of possibilities for P is $n!\,(q-1)^n$. A brute-force attack on deciphering a specific ciphertext would be based on trying all possible message vectors $\mathbf{y}\in F_q^n$ of weight $\leq t$. The number of such vectors is

$$\sum_{j=0}^{t}\binom{n}{j}(q-1)^j.$$

Our public-key cryptosystem shares a common feature with that of Chor and Rivest in Section 1, namely that it works with low-weight message vectors. A comparison with the Chor–Rivest cryptosystem immediately shows one drawback of this cryptosystem, namely a longer setup time due to time-consuming calculations of discrete logarithms. Another aspect which favors our cryptosystem is the information rate. Let S be the number of possible messages and T the number of possible ciphertexts in a cryptosystem. Then the *information rate* of the cryptosystem is defined by

$$R=\frac{\log_2 S}{\log_2 T},$$

where $\log_2$ denotes the logarithm to the base 2. Thus R may be viewed as the amount of information contained per bit of ciphertext. To have a fair comparison, we consider both the Chor–Rivest cryptosystem and our cryptosystem for binary message vectors of length n and weight $\leqq t$. For the Chor–Rivest cryptosystem we have then

$$S=\sum_{j=0}^{t}\binom{n}{j}\leqq 2^n,\quad T=n^{t+1}-1\geqq n^t.$$

Let $t=\theta n$ with $0<\theta<1$. Then

$$R\leqq\frac{n}{\theta n\log_2 n},$$

so that asymptotically (i.e. as $n\to\infty$) the information rate R tends to 0.

The information rate of our cryptosystem shows a completely different behavior. In the binary case $q=2$ we have here

$$S=\sum_{j=0}^{t}\binom{n}{j}, \quad T=2^{n-k}.$$

Choose a family of codes that meet the Gilbert–Varshamov bound. According to [9, p. 557, Theorem 30] this means that for given $0<\delta<\frac{1}{2}$ we can achieve relative distance $d/n\geqq\delta$ and asymptotically

$$\frac{k}{n}\gtrsim 1-H_2\left(\frac{d}{n}\right),$$

where $H_2(x)=-x\log_2 x-(1-x)\log_2(1-x)$ is the binary entropy function. Let again $t=\theta n$. Then

$$\log_2 S=\log_2\sum_{j=0}^{\theta n}\binom{n}{j}\geqq H_2(\theta)n-\frac{1}{2}\log_2 n-\log_2 c(\theta)$$

for some constant $c(\theta)>0$ by [9, p. 310, Corollary 9]. Since $\log_2 T=n-k$, we get

$$R\gtrsim\frac{H_2(\theta)}{1-(k/n)}\gtrsim\frac{H_2(\theta)}{H_2(d/n)}.$$

Since $t=\lfloor(d-1)/2\rfloor$, we have $d\sim 2\theta n$ asymptotically, hence

$$R\gtrsim\frac{H_2(\theta)}{H_2(2\theta)}.$$

This means that asymptotically R stays above a positive lower bound. If for instance $\theta\to\frac{1}{4}$, then

$$R\gtrsim H_2\left(\frac{1}{4}\right)\approx 0.81.$$

To have some concrete examples, consider first the binary concatenated code mentioned in [9, p. 308] with parameters $n=104$, $k=24$, $d=32$, $t=15$. This code is obtained by concatenation of the (8, 4) binary extended Hamming code of minimum distance 4 with a (13, 6) punctured Reed–Solomon code over F_{16} of minimum distance 8. In this case the public key K contains $80\cdot 104=8320$ bits. This compares favorably with the Chor–Rivest cryptosystem where for the suggested parameters the key requires about 36 000 bits. With this binary concatenated code, the number of possible

message vectors is about $5 \cdot 10^{17}$, and this yields an information rate $R \approx 0.73$. For the parameters $n = 104$ and $k = 24$, the number of possible binary linear codes is greater than 10^{570} and the number of nonsingular $(n-k) \times (n-k)$ matrices over F_2 is greater than 10^{1900}.

As a second example, consider a Reed–Solomon code over F_{31} with $n = 30$, $k = 12$, $d = 19$, $t = 9$. The number of bits in the public key K is then $18 \cdot 30 \cdot \lceil \log_2 30 \rceil = 2700$. This is comparable to the size of the RSA public key, which according to current recommendations requires about 1200 bits. With this Reed–Solomon code, the number of possible message vectors is about $3 \cdot 10^{20}$, and this yields an information rate $R \approx 0.76$. For the parameters $n = 30$ and $k = 12$, the number of possible linear codes over F_{31} is greater than 10^{320} and the number of nonsingular $(n-k) \times (n-k)$ matrices over F_{31} is greater than 10^{480}.

References

1. *Beker, H., Piper, F.*, Cipher Systems. The Protection of Communications, Northwood, London, 1982.
2. *Chor, B., Rivest, R. L.*, A knapsack type public key cryptosystem based on arithmetic in finite fields, Proc. CRYPTO '84, to appear.
3. *Diffie, W., Hellman, M. E.*, New directions in cryptography, IEEE Trans. Information Theory **22,** 644–654 (1976).
4. *ElGamal, T.*, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Information Theory, to appear.
5. *Goppa, V. D.*, Algebraic-geometric codes (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **46,** 762–781 (1982).
6. *Justesen, J.*, On the complexity of decoding Reed–Solomon codes, IEEE Trans. Information Theory **22,** 237–238 (1976).
7. *Lidl, R., Niederreiter, H.*, Finite Fields, Encyclopedia of Math. and Its Appl., Vol. **20,** Addison-Wesley, Reading, Mass., 1983.
8. *Lidl, R., Niederreiter, H.*, Introduction to Finite Fields and Their Applications, Cambridge Univ. Press, Cambridge, 1985.
9. *MacWilliams, F. J., Sloane, N. J. A.*, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
10. *McEliece, R. J.*, The Theory of Information and Coding, Encyclopedia of Math. and Its Appl., Vol. **3,** Addison-Wesley, Reading, Mass., 1977.
11. *Merkle, R. C., Hellman, M. E.*, Hiding information and signatures in trapdoor knapsacks, IEEE Trans. Information Theory **24,** 525–530 (1978).
12. *Niederreiter, H.*, A public-key cryptosystem based on shift register sequences, Proc. EUROCRYPT '85, to appear.
13. *Rivest, R. L., Shamir, A., Adleman, L.*, A method for obtaining digital signatures and public-key cryptosystems. Comm. Assoc. Comput. Mach. **21,** 120–126 (1978).
14. *Sarwate, D. V.*, On the complexity of decoding Goppa codes, IEEE Trans. Information Theory **23,** 515–516 (1977).
15. *Tsfasman, M. A.*, Goppa codes that are better than the Varshamov–Gilbert bound (Russian), Problemy Peredači Informacii **18,** *3*, 3–6 (1982).
16. *Tsfasman, M. A., Vlădut, S. G., Zink, T.*, Modular curves, Shimura curves, and Goppa codes, better than Varshamov–Gilbert bound, Math. Nachr. **109,** 21–28 (1982).
17. *van Lint, J. H.*, Introduction to Coding Theory, Springer, New York, 1982.
18. *Wah, P. K. S., Wang, M. Z.*, Realization and application of the Massey–Omura lock, Proc. Internat. Seminar on Digital Communications (Zürich, 1984), pp. 175–182.