Authentication via algebraic-geometric codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, MI 49931

February 6, 1997

Abstract

In this primarily expository paper we exhibit a close connection between the concepts of universal hash classes and error-correcting codes. We derive the properties that an algebraic curve must enjoy in order to yield codes which are well-suited for this application.

1 Introduction

The concept of **universal hashing** was introduced by Carter and Wegman in 1979 (see [8]). It has since found a plethora a very diverse applications in computer science and mathematics. We mention the following:

1. complexity theory
2. cryptography and authentication
3. The static and dynamic dictionary problems
4. probabilistic and random algorithms: partial and complete derandomization of randomized algorithms.
5. public vs. private coins in interactive proofs

More on applications is to be found in [17, 19].

2 Definitions and direct constructions

Definition 1 (universal hash classes) *Let X, Y be sets of cardinality n and m, respectively, and $\mathcal{H}$ a family of N functions*

$$f : X \longrightarrow Y.$$

Let $0 < \epsilon < 1$.
*$\mathcal{H}$ is $\epsilon-$***universal** *(short ϵ -***U***) if for any two distinct elements $x_1, x_2 \in X$ at most $N \cdot \epsilon$ functions $f \in \mathcal{H}$ satisfy $f(x_1) = f(x_2)$.*
We denote the parameters as $\epsilon - U(N, n, m)$.

It is sometimes advantageous to visualize such a hash class as a matrix with N rows, n columns and m different entries, where each function $f \in \mathcal{H}$ contributes a row. The idea in the applications is to choose one of the functions at random. If the distinct elements x_1, x_2 are given, then the probability that $f(x_1) = f(x_2)$ (the probability of a **collision**) is limited by ϵ. We see that the number ϵ plays the role of a probability. This is paradigmatic for all applications. Here is an $(1/3) - U(3, 9, 3)$:

0	1	2	0	1	2	0	1	2
0	1	2	1	2	0	1	2	0
0	1	2	2	0	1	1	2	0

We give a direct construction: Let $Y = \mathbb{F}_q, X$ the set of all q^k polynomials $p(X)$ of degree $< k$ with coefficients in $\mathbb{F}_q$. The rows (mappings) are indexed by the elements $u \in \mathbb{F}_q$, the entry in row u and column $p(X)$ being defined as $p(u)$. This is an $\epsilon - U(q, q^k, q)$ for which ϵ? Two different polynomials of degree $< k$ can agree in at most k values. This shows $\epsilon = 1 - \frac{k}{q}$. Naturally we should choose $k < q$.

Example 1 *Let $k < q$. Put $Y = \mathbb{F}_q, k < q$,*
$X = \{p(X) | p(X) = \sum_{i=0}^{k-1} a_i X^i \in \mathbb{F}_q[X]\}$, and $\mathcal{H} = \{f_u | u \in \mathbb{F}_q\}$, where

$$f_u(p(X)) = p(u).$$

Then $\mathcal{H}$ is an $\frac{k}{q} - U(q, q^k, q)$.

We define the second fundamental class of hash functions:

Definition 2 (strongly universal hash classes) *Let X, Y be sets of cardinality n and m, respectively, and $\mathcal{H}$ a family of N functions*

$$f : X \longrightarrow Y.$$

Let $0 < \epsilon < 1$.
*$\mathcal{H}$ is $\epsilon-$***strongly universal** *(short ϵ -***SU***) if the following hold:*

1. *For every $x \in X$ and $y \in Y$ the number of $f \in \mathcal{H}$ satisfying $f(x) = y$ is N/m.*

2. *For any two distinct elements $x_1, x_2 \in X$ and any two $y_1, y_2 \in Y$ the number ν of functions $f \in \mathcal{H}$ mapping $f(x_1) = y_1, f(x_2) = y_2$ satisfies $\frac{\nu}{N/m} \leq \epsilon$.*

The parameters are denoted as $\epsilon - SU(N, n, m)$.

In matrix notation the first requirement states that in every column every entry occurs equally often. The second condition is more involved. In order to understand it let us digress and consider an application of SU-classes as authentication systems.

2.1 SU-classes as authentication systems

Let $\mathcal{A}$ be an $\epsilon - SU(N, n, m)$. We want to show in this section how to use $\mathcal{A}$ as an authentication system. Identify $\mathcal{A}$ with the corresponding array. Assume a source produces messages, to be sent from the originator (here called **transmitter**), to a remote **receiver**, via a public channel. In order to be able and distinguish two types of messages, those produced by the source and those (possible encrypted or otherwise changed) sent via the channel, we denote the messages produced by the source as **source states**, those sent over the channel as **messages**. We identify X with the set of source states. Our concern is here not with secrecy (protecting the knowledge as to which source state is being transmitted) nor with error-correction (the channel may be noisy and we may wish to use an error-correcting code), but rather with **authentication**. This means that we want to device schemes which enable the receiver to verify if the message really originated from the proper transmitter and has not been altered under way. This is where the

defining properties of an $\epsilon - SU$ family come in. We use the mappings $f \in \mathcal{H}$ as **keys**. The elements $y \in Y$ are also called **authenticators**. Assume $x \in X$ is the source state to be transmitted. Transmitter and receiver will agree, via a secure private channel, on a key $f \in \mathcal{H}$ to be used. Then the message (consisting of x, possibly in encrypted form, possibly encoded for error-correction purposes,...) will contain the **authentication tag** $f(x) = y$. Upon receiving a message which decodes to $x' \in X$, with authentication tag $y' \in Y$, the receiver will accept it as authentic if and only if $f(x') = y'$. Observe that if no problems occured, then $x' = x, y' = y = f(x)$, and the message will be accepted as authentic. We imagine an opponent has access to the communication channel. His aim is to disturb the system, more precisely to have non-authentic messages accepted as authentic. Everything hinges upon the assumptions concerning the power of this opponent. Assume the opponent is able not only to read messages but also to alter them and send the altered version to the receiver. Knowledge of the message gives him some information on the key used. Assume he knows the source state x (we do not want to assume anything concerning secrecy). Then the secret key is one of the mappings f satisfying $f(x) = y$. How can the opponent use this knowledge to improve his chances of cheating? He wishes to have a different message, corresponding to a source state $x' \neq x$, accepted as authentic. He has to choose an authentication tag y' such that with high probability $y' = f(x')$. However, the definition of an $\epsilon - SU$ family shows that his probability of success will always be $\leq \epsilon$. Observe that when $x' \neq x$ has been chosen, then the opponent's probability of success can be written as a conditional probability: $Pr(f(x') = y' \mid f(x) = y)$. Here x, x', y, y' are given ($x' \neq x$), and the probability refers to the choice of $f \in \mathcal{H}$.
We give a direct construction:

Theorem 1 *Let q be a prime-power, a, b, k natural integers, $a \geq b$. Then there is a $\frac{k}{q^b} - SU(q^{a+b}, q^{ka}, q^b)$ hash family.*

Proof: Fix a surjective $\mathbb{F}_q-$linear mapping

$$\Phi : \mathbb{F}_{q^a} \longrightarrow \mathbb{F}_{q^b}.$$

X is identified with the set of polynomials $p(X)$, defined over $\mathbb{F}_{q^a}$, of degree $\leq k$, without constant term. The rows are indexed by pairs (u, v), where

$u \in \mathbb{F}_{q^a}, v \in \mathbb{F}_{q^b}$. The entry in row (u,v) and column $p(X)$ is defined as

$$\Phi(p(u)) + v.$$

It is clear that every column contains each element of $\mathbb{F}_{q^b}$ exactly $N/m = q^a$ times. Fix two different columns $p_1(X), p_2(X)$ and two not necessarily different elements $y_1, y_2 \in \mathbb{F}_{q^b}$. We have to count the rows (u,v) satisfying

$$\Phi(p_1(u)) + v = y_1$$

$$\Phi(p_2(u)) + v = y_2.$$

By subtracting and using the linearity of Φ we get the equivalent equation

$$\Phi((p_1 - p_2)(u)) = y_1 - y_2.$$

Every solution u of this equation will yield a unique row (u,v). Let $M = \Phi^{-1}(y_1 - y_2)$. We have $|M| = q^{a-b}$. Observe that $p_1(X) - p_2(X)$ is a nonconstant polynomial of degree $\leq k$. We conclude that the number of solutions (u,v) is $\leq k \cdot q^{a-b}$, hence $\epsilon = kq^{a-b}/q^a = k/q^b$, as claimed.$\blacksquare$

3 Relation with other combinatorial objects

Error-correcting codes are among the most intensively studied combinatorial objects. Their study originated in the needs of transmitting information reliably over noisy channels.

Definition 3 *Let $x, y \in A^N$ be sequences of length N with entries in a finite set A. The* **Hamming distance** *$d(x,y)$ is defined as the number of coordinates, where x and y differ. This defines a metric on A^N.*
Let $\mathcal{C} \subseteq A^N$ be a family of such tuples. The **minimum distance** *$d(\mathcal{C})$ is the smallest Hamming distance between different elements from $\mathcal{C}$.*

Coding theory is the study of the minimum distance. It is then custumary to call the family $\mathcal{C}$ an (error-correcting) **code** of **length** N. The code $\mathcal{C}$ is q-ary if $|A| = q$. Elements of $\mathcal{C}$ are also called **code words.** The number d/N is known as the **relative distance** of $\mathcal{C}$.

It is not enough known in the coding-theoretic community that codes have a very wide range of different applications and are certainly not restricted to the traditional use for the transmission of messages via noisy channels. We want to discuss here one facet, thus demonstrating the malleability of the concept.
When thinking about U hash families one cannot help observing that the columns of an $\epsilon - U(N, n, m)$ form the words of a code with relative distance $1-\epsilon$, and this obviously is an equivalent description of universal hash families:

Theorem 2 *The following are equivalent:*

- *An $\epsilon - U(N, n, m)$ hash family, and*
- *An m ary code of length N, with n code words and relative minimum distance $1 - \epsilon$.*

This observation is in [4]. It had been made independently by the present author and the remaining authors of [4]. This was one of the reasons why the organizers of Crypto 93 urged us to join forces and submit a joint paper. We conclude that the theory of universal hash classes simply coincides with coding theory. The situation is not as simple what strongly universal hash classes are concerned. If we go back to Definition 2 and demand that any pair of entries appears in any pair of different columns the same number ν of times we arrive at the definition of an **orthogonal array.** It is easy to see that this is the case precisely when $\epsilon = 1/m$ in Definition 2. As orthogonal arrays have a long history in design theory and statistics one may imagine that it would be a good idea to forget about the more general strongly universal classes and use orthogonal arrays for authentication purposes. There is however an argument, which shows that this is impractical. In fact, it follows from an old result of Plackett and Burman [16] that in an $1/m - SU(N, n, m)$ the inequality $N > n$ must hold (for a direct proof of a more general bound see [1]). In the situation of subsection 2.1 this means that the number of keys is larger than the number of source states. We would have to send more information over the private channel than over the public channel. Obviously this does not make sense. We will therefore have to come up with constructions for $\epsilon - SU(N, n, m)$ families in situations when ϵ is somewhat bigger than $1/m$ and N is very much smaller than n. In the following sections two types of constructions will be exhibited, both involving codes.

4 From codes to SU families: a direct way

Definition 4 *A code $\mathcal{C}$ is* **linear** *if its alphabet is a finite field $\mathbb{F}_q$ and $\mathcal{C}$ forms an $\mathbb{F}_q$-linear vector space. If k is the dimension of this space, then the parameters of $\mathcal{C}$ are recorded as*

$$[l, k, d]_q, \text{ where } l \text{ is the length.}$$

Observe that the minimum distance of a linear code equals its minimum weight, which is defined as the minimum distance between any nonzero word and the zero word. Assume now the linear code $\mathcal{C}$ has in addition the following property: for every nonzero code word $x \in \mathcal{C}$ and every $\alpha \in \mathbb{F}_q$ the frequency $\nu(\alpha)$ of α as an entry in x satisfies $\nu(\alpha)/l \leq \epsilon$. Define the expanded code word $\tilde{x}$ as the concatenation of the words $x + \beta\mathbf{1}$, where β varies in $\mathbb{F}_q$. It is easy to check that the $\tilde{x}$ from the columns of an

$$\epsilon - SU(lq, q^k, q).$$

This is essentially the q-**twisted construction** as detailed in [15]. These authors observe that the condition will be satisfied in the following situation: $\mathcal{C}$ has minimum distance d, does not contain the all-1 vector $\mathbf{1}$, and the code generated by $\mathcal{C}$ and $\mathbf{1}$ still has minimum distance d. In this situation we can choose $\epsilon = 1 - \frac{d}{l}$.

5 From codes to SU families: Stinson's way

Stinson's composition construction is best visualized using the language of mappings. Let X, Y be given as in Definition 2. We choose a set U of cardinality u, where $m \leq u < n$, and families $\mathcal{H}_1$ of mappings : $X \longrightarrow U, \mathcal{H}_2$ of mappings : $U \longrightarrow Y$. The family $\mathcal{H} = \mathcal{H}_2 \circ \mathcal{H}_1$ is the set of all compositions $f = f_2 \circ f_1$, where $f_i \in \mathcal{H}_i$.

Theorem 3 (Stinson composition) *The composition of an $\epsilon_1 - U(N_1, n, u)$ and an $\epsilon_2 - SU(N_2, u, m)$ is an $\epsilon - SU(N_1N_2, n, m)$, where $\epsilon = \epsilon_1 + \epsilon_2 - \epsilon_1\epsilon_2$.*

This is best understood when the defining properties of universal and strongly universal hash classes are expressed in terms of probabilities. Let

$x_1, x_2 \in X$ be different elements, $\mathcal{H}$ the family of mappings : $X \longrightarrow Y$. The defining property of an $\epsilon - U$ class is $Pr(f(x_1) = f(x_2)) \leq \epsilon$. In the case of an $\epsilon - SU$ class the main axiom from Definition 2 can be expressed in terms of a conditional propability as

$$Pr(f(x_1) = y_1, f(x_2) = y_2 | f(x_1) = y_1) \leq \epsilon$$

for any $y_1, y_2 \in Y$. Here the probabilities are with respect to the choice of the mapping f from $\mathcal{H}$, according to the uniform distribution.
Proof of Theorem 3: Here $f = f_2 \circ f_1$. It is clear that the first axiom from Definition 2 is satisfied and that the strongest condition for the second axiom occurs when $y_1 = y_2 = y$. Let $Pr(f_1(x_1) = f_1(x_2)) = \alpha$ and recall $\alpha \leq \epsilon_1$. We have $Pr(f(x_1) = f(x_2) = y | f(x_1) = y) \leq Pr(f_1(x_1) = f_1(x_2)) \cdot 1 + Pr(f_1(x_1) \neq f_1(x_2)) \cdot \epsilon_2 = \epsilon_2 + \alpha(1 - \epsilon_2) \leq \epsilon_2 + \epsilon_1(1 - \epsilon_2)$. ■

In our applications of Theorem 3 we are going to use the special case $k = 1$ of Theorem 1 as the SU-class. This is an $\frac{1}{q^b} - SU(q^{a+b}, q^a, q^b)$ for $a \geq b$ and is in fact an orthogonal array (see section 3). The first ingredient, the universal hash class, is equivalent with a code, by Theorem 2. We want to find sources for linear codes, which yield good SU classes after application of Theorem 3. The U class constructed in Example 1 is equivalent to a family of linear codes known as **Reed-Solomon codes.** If they are used in the way we just described we obtain the following:

Theorem 4 *For every prime-power q and natural numbers a, b, k, where $a \geq b$ we can conctruct*

$$\epsilon - SU(q^{2a+b}, q^{ak}, q^b), \;\; \textit{where } \epsilon < \frac{k}{q^a} + \frac{1}{q^b}.$$

In the next section we consider algebraic-geometric codes for use as universal hash classes in Stinson composition.

6 Algebraic-geometric codes and universal hashing

Let K be a function field of transcendence-degree 1 defined over the field $\mathbb{F}_q$ of constants, $P_0, P_1, \ldots P_N$ rational points of K. Consider the divisors

$D = P_1 + P_2 \ldots + P_N, G = uP_0$. Let $u_1 = 0, u_2, \ldots, u_l, \ldots$ be the pole-orders of P_0 in ascending order. Consider the code

$$\mathcal{C}_l = \mathcal{C}(D, u_l P_0)$$

of functions which are everywhere holomorphic except for a pole of degree $\leq u_l$ at P_0, evaluated at $P_1, \ldots P_N$ (this is the L-construction of [20]). Most of the material in this section is from [3]. Assume $u_l < N$. Then $\mathcal{C}_l$ has dimension l and minimum distance $\geq N - u_l$. In the language of universal hashing this construction takes on the following form:

Theorem 5 *Assume there is an algebraic curve C defined over $\mathbb{F}_q$ with $N+1$ rational points. Let P be one of these rational points, with pole orders u_i, where $u_0 = 0 < u_1 < \ldots$. Then we can construct a hash family*

$$\epsilon - U(N, q^i, q), \ \textit{where } \epsilon \leq u_i/N.$$

In the special case of the projective line this reverts to the Reed-Solomon codes and thus to the construction of Example 1. It transpires that the underlying curve has to meet the following requirements in order to yield codes that are well-suited for our hashing purposes:

1. The number of rational points is large, and
2. There is a rational Weierstraß point whose gaps are as large as possible, in other words for given i the i-th pole order u_i should be small.

The **Hermitian curve** over $\mathbb{F}_{q^2}$ has $q^3 + 1$ rational points. Its rational points are precisely the Weierstraß points, and the semigroup of pole orders is generated by q and $q + 1$. It is an easy combinatorial exercise that for every $w \leq q$ we have $u_{\binom{w+1}{2}+1} = w \cdot q$. This yields the following:

Theorem 6 *For every prime-power q and $w \leq q$ the Hermitian curve over $\mathbb{F}_{q^2}$ yields an*

$$\frac{w}{q^2} - U(q^3, q^{w^2+w+2}, q^2).$$

The projective line and the Hermitian curves belong to the family of **Deligne-Lusztig curves,** together with Suzuki curves and Ree curves (see [7, 9, 11]). We observe next that Suzuki curves also yield good universal hash classes. Let $q = 2^{2f+1}, q_0 = 2^f$. The Suzuki curve is defined over $\mathbb{F}_q$. It has $q^2 + 1$ rational points. These are the Weierstraß points. The semigroup of pole-orders of each Weierstraß point is

$$q\mathbb{N}_0 + (q + q_0)\mathbb{N}_0 + (q + 2q_0)\mathbb{N}_0 + (q + 2q_0 + 1)\mathbb{N}_0.$$

Put $s_i = 1^2 + 2^2 + \ldots + i^2 = (2i + 1)(i + 1)i/6$. If $w \leq q_0 = 2^f$, then

$$u_{s_w+1} = w \cdot q$$

This leads to the following:

Theorem 7 *Let $q = 2^{2f+1}, q_0 = 2^f$. For every $w \leq q_0$ the Suzuki curve yields an*

$$\frac{w}{q} - U(q^2, q^{1+(2w+1)w(w+1)/6}, q).$$

Let us use the Hermitian codes and Suzuki codes in Theorem 3 together with Theorem 1, as described above. We simplify and choose parameters such that ϵ is at most double as large as the theoretical minimum. We cover also Theorem 4:

Theorem 8 *Let q be a prime-power, a, b natural numbers. Then the following exist:*

1. $$\frac{2}{q^b} - SU(q^{2a+b}, q^{aq^{a-b}}, q^b) \text{ if } b \leq a.$$

2. $$\frac{2}{q^b} - SU(q^{5a/2+b}, q^{aq^{2(a-b)/2}}, q^b)$$
   if $b \leq a \leq 2b, q^a$ a square.

3. $$\frac{1}{2^{b-1}} - SU(2^{3a+b}, 2^{a2^{3(a-b)/3}}, 2^b)$$
   if $b \leq a \leq 2b - 1, a$ odd.

7 New directions

Recently Garcia and Stichtenoth [10] have given an effective construction of a family of codes, based on Artin-Schreier extensions, which attain the asymptotic Drinfeld-Vladut bound. The second level of this family are Hermitian codes. The codes on the third level have been studied in [21]. These authors determine the Weierstraß points and their pole-orders. It may be expected that this leads eventually to new authentication codes.
Finally we mention a new direction in coding theory. The present author has, in joint work with Yves Edel, introduced the notion of **Twisted BCH-codes** (see [5]). The same concept has been developed independently by a group of researchers around McEliece and Gus Solomon (see [13, 14]), under the name **subfield subcodes of Reed-Solomon codes.** We have used this concept for the construction of optimal binary linear codes in [5] and for the construction of a large family of two-weight codes related to maximal arcs in [6]. A completely different application has been given by the authors of [13]. They have used a code from this family to increase the data rate of transmission from the spacecraft Galileo. They also make a comparison with the performance of algebraic-geometric codes and demonstrate that the new codes can compete with Hermitian codes in a wide range of parameters. A very attractive line of research would be a generalization of the "twisted" mechanism to algebraic-geometry codes in general. In our context this raises the question if twisted BCH-codes can be used for our purposes of universal hashing and authentication. In the next section we will include a rather arbitrary example indicating that this is indeed possible.

8 Examples

If the source has 400 bits, we use 21 authenticator bits and are willing to accept a deception probability of $\epsilon = 2^{-20}$, then the

$$2^{-20} - SU(2^{71}, 2^{400}, 2^{21})$$

from Theorem 8 works best. It makes use of a Reed-Solomon code $[Q, 16, Q-15]$ defined over $\mathbb{F}_Q$, where $Q = 2^{25}$.
If we increase the size of the source to 2^{34} bits, the second case of Theorem 8

yields

$$2^{-20} - SU(2^{111}, 2^{2^{34}}, 2^{21}).$$

This makes use of a Hermitian code of length 2^{54}, defined over the field with 2^{36} elements.
Consider a source of 2^{57} bits. The third case of Theorem 8, with $a = 39$, yields

$$2^{-20} - SU(2^{138}, 2^{2^{57}}, 2^{21}).$$

This is based on a Suzuki code defined over $\mathbb{F}_Q$, where $Q = 2^{39}$, of length 2^{78}.
Imagine we insisted on a deception probability reaching the theoretical lower bound of 2^{-21}. As pointed out in section 3 we would need more than 2^{57} key bits in that case, compared to the 138 key bits which are needed for our system.
Finally we wish to give an example where twisted BCH-codes work better than Reed-Solomon, Hermitian or Suzuki codes. There is a twisted BCH-code of length 2^{25}, with 2^{224} code words and minimum distance $2^{25} - 16$, defined over an alphabet of size 2^{24}. This code is not linear over its alphabet, but it is **additive** meaning that the alphabet may be considered as an elementary abelian group and sums of code words are code words again. By Theorem 2 this yields an $2^{-21} - U(2^{25}, 2^{224}, 2^{24})$ hash class. Application of Theorem 3 yields

$$2^{-20} - SU(2^{70}, 2^{224}, 2^{24}).$$

It is easily seen that this is not reachable by Theorem 2. The Reed-Solomon method, when used such that the remaining parameters are unchanged, covers a source of 216 bits.

References

[1] J.Bierbrauer: *Bounds on orthogonal arrays and resilient functions, Journal of Combinatorial Designs* **3**(1995),179-183.

[2] J.Bierbrauer: *Construction of orthogonal arrays,* to appear in *Journal of Statistical Planning and Inference.*

[3] J.Bierbrauer: *Universal hashing and geometric codes,* to appear in *Designs, Codes and Cryptography.*

[4] J.Bierbrauer,T.Johansson,G.Kabatianskii,B.Smeets: *On families of hash functions via geometric codes and concatenation,* Advances in *Cryptology-CRYPTO 93, Lecture Notes in Computer Science 773 (1994),331-342.*

[5] J.Bierbrauer,Y.Edel:*Twisted BCH-codes,* to appear in *Journal of Combinatorial Designs.*

[6] J.Bierbrauer,Y.Edel: *A family of 2-weight codes related to BCH-codes,* to appear in *Journal of Combinatorial Designs.*

[7] R.W.Carter: *Finite groups of Lie type,* Wiley 1985.

[8] J.L.Carter,M.N.Wegman: *Universal Classes of Hash Functions, J.Computer and System Sci. 18(1979), 143-154.*

[9] P.Deligne,G.Lusztig: *Representations of reductive groups over finite fields,* Annals of Mathematics *103(1976),103-161.*

[10] A.Garcia,H.Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound,* Inventiones Mathematicae **121**(1995),211-222.

[11] J.P.Hansen: Group codes on Deligne-Lusztig varieties, *Coding Theory and Algebraic Geometry, Proceedings Luminy 1991, Springer LNM 1518,1992.*

[12] J.P.Hansen,H.Stichtenoth: *Group Codes on Certain algebraic curves with many rational points,* AAECC 1(1990),67-77.

[13] M.Hattori, R.J.McEliece,G.Solomon: *Subspace subcodes of Reed-Solomon codes,* submitted for publication in *IEEE Transactions on Information Theory.*

[14] M. Hattori, *Subspace subcodes of Reed-Solomon codes,* Ph.D. dissertation at Caltech, 1995.

[15] G. Kabatianskii, B. Smeets, T. Johansson: *On the Cardinality of Systematic Authentication Codes via Error-Correcting Codes, IEEE Transactions on Information Theory* **42**(1991),583-602.

[16] R.L.Plackett, J.P.Burman: *The design of optimum multi-factorial experiments, Biometrika* **33** (1945),305-325.

[17] D.R.Stinson: *Combinatorial techniques for universal hashing,* Journal *of Computer and Systems Science* **48**(1994),337-346.

[18] D.R.Stinson: *Universal Hashing and Authentication Codes, Designs, Codes and Cryptography* **4**(1994),369-380. A preliminary version appeared in the *Proceedings of CRYPTO 91, Lecture Notes in Computer Science 576 (1992), 74-85.*

[19] D.R.Stinson: *On the connections between universal hashing, combinatorial designs and error-correcting codes,* Congressus Numerantium **114**(1996),7-27.

[20] M.A.Tsfasman,S.G.Vladut : *Algebraic-Geometric codes,* Kluwer Dordrecht/Boston/London 1991.

[21] C.Voss, T.Høholdt, *An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps, IEEE Transactions on Information Theory* **43**(1997),128-135.

[22] M.N.Wegman,J.L.Carter: *New hash functions and their use in authentication and set equality,* J.Computer and System Sci. *22(1981),265-279.*