A^2 -codes from universal hash classes

Jürgen Bierbrauer

Department of Mathematical Sciences

Michigan Technological University

HOUGHTON, MI 49931 (USA)

Abstract

We describe a general method to construct codes for unconditional authentication with arbitration (A^2 -codes), which protect not only against outside opponents but also against certain types of frauds from the receiver and transmitter. The constructions are based on orthogonal arrays and universal hash classes. The idea is to construct A^2 -codes out of pairs of A -codes. The hitherto known examples are special cases of the construction. Along the way we also construct new universal hash classes.

1 Introduction

It is the purpose of the traditional theory of unconditional authentication (A -codes) to protect the *transmitter* and *receiver* from deception by an outside opponent. It is assumed that transmitter and receiver trust each other. Simmons [9, 10] extended this model to include protection against certain frauds by transmitter and receiver. This model uses an *arbiter*, who distributes partial keys to transmitter and receiver and decides in cases of controversy between transmitter and receiver. It is assumed that the arbiter is trustworthy. The corresponding systems have been termed A^2 -codes by Simmons [10].

Let us first consider A -codes: The basic ingredients in their construction are universal hash classes, in particular $\epsilon - ASU_2$ classes.

Definition 1 Let $\epsilon > 0$. A multiset $\mathcal{A}$ of b functions from a k -set S to a v -set E is ϵ -almost strongly universal₂ (short: ASU_2) if

1. for every $u \in S$ and $x \in E$ the number of elements of $\mathcal{A}$ mapping $u \mapsto x$ is b/v ,
2. for every pair $u_1, u_2 \in S, u_1 \neq u_2$, and every pair $x_1, x_2 \in E$ the number of elements of $\mathcal{A}$ affording the operation $u_1 \mapsto x_1, u_2 \mapsto x_2$ is $\leq \epsilon \cdot b/v$.

It is easy to see that $\epsilon \geq 1/v$. The special case $\epsilon = 1/v$ is known as an orthogonal array of strength 2, denoted as $OA_\lambda(2, k, v)$. Here $b = \lambda \cdot v^2$.

In *authentication without secrecy* it is the case that secrecy either cannot be tolerated or is provided by different means. Technically this means that every message sent through the public channel has to correspond to a unique source state. An A -code may be described as an array $\mathcal{A}$ whose columns correspond to the source states, whose entries are the messages sent through the channel, and whose rows correspond to the keys. We may describe $\mathcal{A}$ equivalently as a set of mappings (the rows) : $S \rightarrow M$ from source states to messages. The mappings f have to be injective. If secrecy has to be excluded, then this translates into the property that no entry occurs in more than one column. In particular, if $|S| = k$ and v different entries occur in each column, then $|M| = k \cdot v$. Simmons [10] uses the term *Cartesian* in this case, Stinson [11] calls these structures *perfectly disclosed*. In the opposite case, when the set of entries is the same for each column, let us speak of a (*perfectly*) *enclosed* array. Universal hash classes are perfectly enclosed arrays. We shall come back to the relation between enclosed and disclosed arrays in the next section.

We describe the setup of A^2 -codes: The transmitter has a set E_T of mappings : $S \rightarrow M$. These are injective and form a perfectly disclosed array. We can therefore write $M = S \times E$ and write each $F \in E_T$ in the form $F(s) = (s, f(s))$. The mappings f form then the perfectly enclosed array $en(E_T)$ of mappings : $S \rightarrow E$. Put $|S| = k, |E| = v$. The receiver has a set E_R of mappings $G : M \rightarrow \{0, 1\}$. The set of admissible pairs $E_R \circ E_T$ is chosen such that for every $(G, F) \in E_R \circ E_T$ and every source state $s \in S$ we have $G(F(s)) = 0$. The receiver, upon seeing the message m , will accept it as authentic if $G(m) = 0$. At each unit of time the arbiter distributes a pair of encoding rules F to the transmitter and G to the receiver. Here the pair $(G, F) \in E_R \circ E_T$ is chosen according to the uniform distribution. The threats against which the system yields protection (in probability) are the following: impersonation by the opponent, substitution by the opponent, impersonation by the receiver, substitution by the receiver, impersonation by the transmitter. Let $p_I, p_S, p_{R_0}, p_{R_1}, p_T$ be the corresponding probabilities of success with the corresponding attacks when using an optimal strategy. Bounds on these probabilities are obtained from (and are in fact equivalent to) combinatorial properties of $en(E_T)$, E_R and $E_R \circ E_T$. For a detailed discussion see for example [6]. Our construction is based on the idea of choosing $en(E_T)$ as a pair $(\mathcal{A}_1, \mathcal{A}_2)$ of ASU_2 universal hash classes (A -codes, that is) and of letting E_R be determined by another such universal hash class, which is closely related to $\mathcal{A}_2$ (in fact by $E_R = \overline{\mathcal{A}_2}$ in the notation of Lemma 1). The choice of $E_R \circ E_T$ will be more or less forced. Our A^2 -codes are thus obtained from pairs $(\mathcal{A}_1, \mathcal{A}_2)$ of A -codes. This construction contains earlier examples given by T.Johansson and K.Kurosawa as special cases ([6, 8]).

2 Enclosed and disclosed arrays

We wish to point out in this section that the distinction between enclosed and disclosed arrays is mathematically meaningless. This is illustrated by showing that a famous geometrical authentication code as constructed by Gilbert, McWilliams and Sloane [4] is simply the extended 2-dimensional Reed-Solomon code in disguise.

Definition 2 *Let $\mathcal{A}$ be a multiset of mappings from the k -set S to the set M of entries. Alternatively we use the array notation introduced above. For each column $s \in S$ let $\mathcal{A}(s)$ be the set of different entries in column s . Assume that $|\mathcal{A}(s)| = v$ for every s .*

- *Fix a v -set E and bijections $\phi_s : \mathcal{A}(s) \longrightarrow E$ for every column s and define $\mathcal{A}' = \{f' | f \in \mathcal{A}\}$, where*

$$f'(s) = \phi_s(f(s)).$$

Call $\mathcal{A}'$ an enclosure of $\mathcal{A}$ and write $\mathcal{A}' = \text{en}(\mathcal{A})$.

- *Fix a family E_s of pairwise disjoint v -sets, fix bijections $\phi_s : \mathcal{A}(s) \longrightarrow E_s$ for every column s and define an array $\mathcal{A}'' = \{f'' | f \in \mathcal{A}\}$, where*

$$f''(s) = \phi_s(f(s)).$$

Call $\mathcal{A}''$ a disclosure of $\mathcal{A}$ and write $\mathcal{A}'' = \text{dis}(\mathcal{A})$.

It is an elementary but important fact that the set of probabilities of deception is not changed if the entries in some column of $\mathcal{A}$ are permuted or even replaced by different entries. In this sense every array $\mathcal{A}$ is equivalent to $\text{en}(\mathcal{A})$ and to $\text{dis}(\mathcal{A})$. We find it more natural to handle and to construct enclosed A -codes. In case of authentication without secrecy one should simply use the corresponding disclosure. $\epsilon - ASU_2$ classes are A -codes in enclosed form.

There is a vast literature on so-called *geometric authentication systems*. They come by construction in disclosed form. If one considers the corresponding (and, as we know, formally equivalent) enclosed arrays, it turns out that these are either well-known or uninteresting. We give just one example:

The first geometric authentication scheme was proposed in [4]: Let q be a prime-power, $\mathcal{P}$ a projective plane of order q . Fix a line g_0 of $\mathcal{P}$. Construct a perfectly disclosed array $\mathcal{A}$ with q^2 rows in the following way:

- the columns are indexed by the points on g_0 .
- the entries are indexed by the lines $\neq g_0$.
- the rows are indexed by the affine points ($\in \mathcal{P} - g_0$).

If P is the source state, Q the key, then the corresponding message is the line PQ . We see that $\mathcal{A}$ is perfectly disclosed. In fact $\mathcal{A}(P)$ is the set of all lines $\neq g_0$ through P . As lines of $\mathcal{P}$ intersect in precisely one point, it is clear that the enclosure $en(\mathcal{A})$ is an array with only q different entries and the property that every ordered pair of entries occurs in every ordered pair of different columns precisely once. Thus $en(\mathcal{A})$ is an orthogonal array $OA_1(2, q+1, q)$. We have rediscovered the 2-dimensional extended Reed-Solomon codes.

3 JK -systems

We present a method of construction for A^2 -codes based on $\epsilon - ASU_2$ -classes of hash functions (A -codes). We call these structures JK -systems in honour of Thomas Johansson and Kaoru Kurosawa who first studied special cases of this construction. We need the following recursive construction for $\epsilon - ASU_2$ classes of hash functions:

Lemma 1 *Let q be a prime-power, $\mathcal{A}$ an $\epsilon - ASU_2$ class of b hash functions $: S \rightarrow \mathbb{F}_q$. We define a class $\overline{\mathcal{A}}$ of $q \cdot b$ hash functions $: S \times \mathbb{F}_q \rightarrow \mathbb{F}_q$ as follows: The functions of $\overline{\mathcal{A}}$ are pairs (f, z) , $f \in \mathcal{A}$, $z \in \mathbb{F}_q$, the value of (f, z) at (s, u) is $f(s) + z \cdot u$. Then $\overline{\mathcal{A}}$ is an $\epsilon - ASU_2$ class of hash functions.*

This is easily proved. Consider the special case when $\mathcal{A}$ is an orthogonal array of strength 2 (equivalently $\epsilon = 1/q$). Then $\mathcal{A}$ has parameters $OA_\lambda(2, k, q)$, where $|S| = k$, $b = q^2 \cdot \lambda$. Repeated application of the lemma yields orthogonal arrays $OA_{\lambda \cdot q^i}(2, k \cdot q^i, q)$ for every natural number i . Let in particular $\mathcal{A}$ be the 2-dimensional extended Reed-Solomon code. This is an $OA_1(2, q+1, q)$. Our construction yields $OA_{q^{n-1}}(2, q^n + q^{n-1}, q)$ for every n . This is not an achievement however as the simplex code (the dual of the Hamming code) is an $OA_{q^{n-1}}(2, q^n + q^{n-1} + \dots + q + 1, q)$. More interesting is an application to the $\frac{k}{q} - ASU_2$ classes of hash functions as constructed in [7]. In [2] we generalized this to $\frac{k}{q^m} - ASU_2$ classes of q^{n+m} hash functions from a q^{kn} -set to a q^m -set, whenever $n \geq m$. Here we obtain a generalization in a different direction:

Proposition 1 *For every prime-power q and natural numbers k, i there is a $\frac{k}{q} - ASU_2$ class of q^{2+i} hash functions from a q^{k+i} -set to a q -set.*

We come to our basic construction:

Definition 3 Let q be a prime-power, let $\mathcal{A}_i$ be an ϵ_i - ASU_2 -class of hash functions: $S \rightarrow \mathbb{F}_q$, $i = 1, 2$. Assume that $\mathcal{A}_2$ is a vector space over $\mathbb{F}_q$ and $\mathcal{A}_1 \subseteq \mathcal{A}_2$. The JK -system $JK(\mathcal{A}_1, \mathcal{A}_2, q)$ consists of $\mathcal{A}_1, \mathcal{A}_2$ and the set T of admissible triples. Here a triple (f_1, f_2, g) , where $f_i \in \mathcal{A}_i, g = (f'_2, z) \in \overline{\mathcal{A}_2}$ is admissible if

$$f_2 = f'_2 + z \cdot f_1.$$

JK -systems are thus constructed using pairs $\mathcal{A}_1, \mathcal{A}_2$ of ϵ_i - ASU_2 -class of hash functions. As discussed in the Introduction each such universal hash class is equivalent to a traditional authentication code, yielding security against intruders but no protection against frauds by insiders. The JK -system uses the properties of $\mathcal{A}_1$ to protect against certain frauds by the receiver. The properties of $\mathcal{A}_2$ yield protection against frauds by the outside opponent. Finally, the choice of admissible triples guarantees protection against the transmitter using a signature different from his own. All this will be discussed in greater detail below.

We remark that the construction is not as flexible as it might appear. In fact, as $\mathcal{A}_2$ is linear, we have $\epsilon_2 = 1/q$. Its generator matrix consists of k projectively inequivalent columns. This means that $\mathcal{A}_2$ is a shortened simplex code. Given $k = |S|$, an $\mathcal{A}_2$ of minimum dimension may be obtained as follows: Let n be minimal such that $k \leq q^n + q^{n-1} + \dots + q + 1 = (q^{n+1} - 1)/(q - 1)$. Then $\mathcal{A}_2$ may be chosen as a shortening of the $(n + 1)$ -dimensional Simplex code.

The system $JK(\mathcal{A}_1, \mathcal{A}_2, q)$ is used as an A^2 -code in the following way: at each unit of time the arbiter chooses an admissible triple $(f_1, f_2, g = (f'_2, z))$ at random (according to the uniform distribution on the set of admissible triples). He distributes the partial keys: (f_1, f_2) to the transmitter, $g = (f'_2, z)$ to the receiver, via secure channels. The following is the legitimate use of the system by transmitter and receiver: the transmitter, wishing to send source state $s \in S$, encodes it into the message $m = (s, f_1(s), f_2(s)) = F(s)$ and sends this via the public channel. The receiver, upon seeing a message (s, x, y) , accepts it as authentic if $g(s, x) = y$. Thus $G(s, x, y) = g(s, x) - y$ in the notation of the introduction. If $m = (s, f_1(s), f_2(s))$ is unaltered, then $g(s, f_1(s)) = f'_2(s) + z \cdot f_1(s) = f_2(s)$ as the triple was admissible. We determine the basic parameters of this A^2 -code:

Theorem 1 If $JK(\mathcal{A}_1, \mathcal{A}_2, q)$ is used as an A^2 -code as above, where $\mathcal{A}_1$ is an ϵ_1 - ASU_2 class of b_1 hash functions and $\mathcal{A}_2$ is obtained by shortening the $(n + 1)$ -dimensional Simplex code, where $k \leq (q^{n+1} - 1)/(q - 1)$, then the sizes of the transmitter's and receiver's key space are $|E_T| = b_1 \cdot q^{n+1}$, $|E_R| = q^{n+2}$, the number of admissible triples is $|E_R \circ E_T| = q^{n+2} b_1$. The probabilities of deception are

$$p_I = p_{R_0} = p_T = 1/q, p_S \leq 1/q, p_{R_1} \leq \epsilon_1.$$

proof: The statements concerning the sizes of the key spaces are obvious. We concentrate on the more interesting of the probabilities of deception: p_S (substitution by the opponent), p_{R_1} (substitution by the receiver) and p_T (impersonation by the transmitter):

Substitution by the opponent: The opponent observes a legitimate message $(s, f_1(s), f_2(s))$, changes this into (s', x, y) for some $s' \neq s$. He succeeds if this is accepted as authentic by the receiver. Security is based on the properties of $\mathcal{A}_2$ only. So let us assume that the opponent guessed correctly the values of $x = f_1(s')$ and of z . He has to guess the value of $f_2(s', f_1(s')) = f'_2(s') + z \cdot f_1(s')$, equivalently of $f'_2(s')$, based on the knowledge of $f_2(s) = f'_2(s) + z \cdot f_1(s)$, equivalently of $f'_2(s)$. As $s \neq s'$ and as f'_2 is chosen from $\mathcal{A}_2$ according to the uniform distribution, we have $p_S \leq 1/q$.

Substitution by the receiver: The receiver R , upon seeing a legitimate message $(s, f_1(s), f_2(s))$, claims having received (s', x, y) instead for some $s' \neq s$. He succeeds if $x = f_1(s')$. Clearly he will use $y = g(s', x)$. Security is based on the properties of $\mathcal{A}_1$. It follows from the basic rule $f_2 = f'_2 + z \cdot f_1$ that knowledge of the partial key (f'_2, z) will give R no information on f_1 . He thus has to guess $f_1(s')$ on the basis of his knowledge of $f_1(s)$ only. It follows $p_{R_1} \leq \epsilon_1$.

Impersonation by the transmitter: The transmitter T sends a message (s, x, y) , where $x \neq f_1(s)$ (i.e. using a signature different from his own). In order to succeed he has to guess the value of $g(s, x) = f'_2(s) + z \cdot x$. As T does know $f'_2(s) + z \cdot f_1(s) = f_2(s)$ we see that T has to guess equivalently the value of $z \cdot (x - f_1(s))$. However, as $x \neq f_1(s)$, this is equivalent to guessing z . As T has no a priori information on z , this shows $p_T = 1/q$. ■

The A^2 -codes which have hitherto been proposed are special cases of this construction: Johansson's construction I is $JK(\mathcal{A}, \mathcal{A}, q^m)$, where $\mathcal{A} = OA_1(2, q^n, q^m)$, $n \leq m$ is a shortened Reed-Solomon code. His construction II is $JK(\mathcal{A}, \mathcal{A}, q)$, where $\mathcal{A} = OA_{q^n-1}(2, q^n, q)$ is a member of a well-known family of OA of strength 2. We have seen above that the number of columns can be further increased. Kurosawa's first construction coincides with Johansson's construction II. Kurosawa's second construction is much more interesting. Here $\mathcal{A}_2$ is $OA_{q^n-1}(2, q^n, q)$ as before, but $\mathcal{A}_1$ is the (non linear) $t/q - ASU_2$ class of q^2 functions considered above.

4 The Wegman&Carter-effect

It is a fundamental observation, due to Wegman and Carter (see [3, 12]) that the number of rows (functions) of an $\epsilon - ASU_2$ class of functions from a k -set into a v -set may be dramatically decreased if ϵ , instead of equaling the theoretical minimum $1/v$ (this is the case of orthogonal arrays of strength 2), is allowed to be slightly larger. The latest developments in this area may be

found in [2]. We use JK -systems $JK(\mathcal{A}_1, \mathcal{A}_2, q)$ to show that the same effect occurs for A^2 -codes. Unfortunately this is only partially true. We remarked already that $\mathcal{A}_2$ has to be an orthogonal array of strength 2. We can however reduce b_1 by choosing $\mathcal{A}_1$ to be an $\epsilon_1 - ASU_2$ class of hash functions with ϵ slightly bigger than $1/q$. Kurosawa's second system is a first example. In his case $\epsilon_1 = t/q$ for an integer $t > 1$. We present a large class of JK -systems, where $\mathcal{A}_1$ is obtained by *Stinson-composition* from a Reed-Solomon code and an orthogonal array (see [1]). The technical problem is to choose the $\mathcal{A}_i$ such that $\mathcal{A}_1 \subseteq \mathcal{A}_2$.

Let $\mathbb{F}_Q$ be the ground field, where $Q = q^m$ for some prime-power q . Let $|S| = q^{nt}$ for some t and $n \geq m$. Assume further that $m \mid nt$. An explicit description of the $\epsilon_1 - ASU_2$ class of hash functions $: S \rightarrow \mathbb{F}_Q$ obtained via Stinson composition as promised above is the following (see [1]):

We have $b_1 = q^{2n+m}$. Write the elements (functions) of $\mathcal{A}_1$ as triples (α, β, γ) , where $\alpha, \beta \in \mathbb{F}_{q^n}, \gamma \in \mathbb{F}_{q^m}$. Write the elements of $\mathbb{F}_{q^{nt}}$ as polynomials $p(X)$ of degree $\leq t-1$, with coefficients in $\mathbb{F}_{q^n}$. Function (α, β, γ) maps $p(X)$ into $\Phi(p(\alpha) \cdot \beta) + \gamma$, where $\Phi : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^m}$ is a surjective $\mathbb{F}_q$ -linear mapping. We have seen in [1] that $\mathcal{A}_1$ is an $\epsilon_1 - ASU_2$ class, where $\epsilon_1 < \frac{1}{q} + \frac{t-1}{q^n}$.

Let $q^{nt} = Q^l$. We claim that $\mathcal{A}_1 \subseteq \mathcal{A}_2$, where $\mathcal{A}_2 = OA_{Q^l-1}(2, Q^l, Q)$ is one of the aforementioned orthogonal arrays: its functions are given by pairs $(x, z), x \in \mathbb{F}_{Q^l}, x \in \mathbb{F}_Q$, mapping $u \in \mathbb{F}_{Q^l}$ into $\phi(u \cdot x) + z$. Here $\phi : \mathbb{F}_{Q^l} \rightarrow \mathbb{F}_Q$ is a surjective $\mathbb{F}_Q$ -linear mapping. The reader can easily convince himself that this does define an orthogonal array with the given parameters. We want to show that each function (α, β, γ) of $\mathcal{A}_1$ also is a function $(x, z) \in \mathcal{A}_2$. This means that x, z have to be chosen such that

$$\Phi(p(\alpha) \cdot \beta) + \gamma = \phi(p(X) \cdot x) + z$$

for every element $p(X) = u \in \mathbb{F}_{Q^l} = \mathbb{F}_{q^{nt}}$. Naturally we will choose $z = \gamma$. Consider an $\mathbb{F}_{q^n}$ -linear surjective mapping $\rho : \mathbb{F}_{q^{nt}} \rightarrow \mathbb{F}_{q^n}$ (for example the trace) such that ϕ is the concatenation of ρ and Φ . It suffices then to find x such that the following is satisfied:

$$p(\alpha) \cdot \beta = \rho(p(X) \cdot x).$$

The left side defines an $\mathbb{F}_{q^n}$ -linear mapping from $\mathbb{F}_{q^{nt}}$ to $\mathbb{F}_{q^n}$. It can therefore be represented in the required fashion. We arrive at the following:

Theorem 2 *Let q be a prime-power, t, n, m natural numbers such that $m \leq n$ and $m \mid nt, |S| = q^{nt}$. Then there is $JK(\mathcal{A}_1, \mathcal{A}_2, q^m)$ such that $\epsilon_1 < q^{-m} + \frac{k-1}{q^n}, b_1 = q^{2n+m}, b_2 = q^{nt+m}$.*

In particular we have $\epsilon_1 < 2/q^m$ provided $t \leq q^{n-m} + 1$.

We see that it would be very desirable to find a more general construction such that $\mathcal{A}_2$ could be chosen as an $\epsilon_2 - ASU_2$ class of hash functions for arbitrary ϵ_2 . This would allow us to also reduce the value of b_2 .

References

- [1] J.Bierbrauer: *Universal hashing and geometric codes*, to appear in *Designs, Codes and Cryptography*.
- [2] J.Bierbrauer, T.Johansson, G.Kabatianskii,B.Smeets: *On families of hash functions via geometric codes and concatenation*, Proceedings of CRYPTO'93, Lecture Notes in Computer Science 773(1994),331-342.
- [3] J.L.Carter,M.N.Wegman: *Universal Classes of Hash Functions*, J.Computer and System Sci. 18(1979), 143-154.
- [4] E.N.Gilbert,F.J.MacWilliams,N.J.A.Sloane: *Codes which detect deception*, Bell System Technical Journal 53(1974),405-424.
- [5] T.Johansson:*Lower bounds on the probability of deception in authentication with arbitration*, in *Proceedings of the 1993 IEEE International Symposium on Information Theory*, San Antonio, USA, page 231.
- [6] T.Johansson: *On the construction of perfect authentication codes that permit arbitration*, Proceedings of CRYPTO'93, Lecture Notes in Computer Science 773(1994), 343-354.
- [7] T.Johansson,G.Kabatianskii,B.Smeets: *On the relation between A-codes and codes correcting independent errors*, Proceedings Eurocrypt 93, 1-11.
- [8] K.Kurosawa: *New bound on authentication code with arbitration*, Proceedings of CRYPTO'94, Lecture Notes in Computer Science 839(1994), 140-149.
- [9] G.J.Simmons: *Message authentication with arbitration of transmitter/receiver disputes*, Proceedings Eurocrypt 87, 151-165.
- [10] G.J. Simmons: *A cartesian product construction for unconditionally secure authentication codes that permit arbitration*, Journal of Cryptology 2 (1990),77-104.
- [11] D.R.Stinson: The combinatorics of authentication and secrecy codes, Journal of Cryptology 2 (1990),23-49.
- [12] 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.