Spectral Methods for Cross-Correlations of Geometric Sequences

Andrew Klapper, *Member, IEEE,* and Claude Carlet

***Abstract*— Families of sequences with low pairwise shifted cross-correlations are desirable for applications such as CDMA communications. Often such sequences must have additional properties for specific applications. Several ad hoc constructions of such families exist in the literature, but there are few systematic approaches to such sequence design. In this paper we introduce a general method of constructing new families of sequences with bounded pairwise shifted cross-correlations from old families of such sequences. The bounds are obtained in terms of the maximum cross-correlation in the old family and the Walsh transform of certain functions.**

***Index Terms*— Autocorrelation, CDMA, Cross-correlation, Sequences, Walsh Transform.**

I. Introduction

To build efficient CDMA communications systems one needs large families of easily generated sequences with low pairwise shifted cross-correlations. It is often desirable that these sequences have various additional properties. It is thus useful to have many families of sequences whose pairwise cross-correlations are known to be low.

Several classes of sequences whose correlation properties have been studied are described by applying a function g on a finite field to successive powers of a primitive element. In several cases the function is best described as a composition of functions, $g = f\circ h$, where h maps from a large field to an intermediate subfield, and f maps from the intermediate field to a subfield of the intermediate field. Sometimes h is a trace function and f is arbitrary [13]. In other cases f is a trace function and h is chosen from a suitable family [9], [11], [17]. In the case of GMW sequences, h is a power of a trace function [9]. In the case of generalized GMW sequences f is the trace of $Ax + Bx^{p+1}$ for some A and B [20]. In the case of No sequences and d-form sequences, h is a homogeneous function of degree d over the intermediate field [11], [17]. In this paper we generalize this setting and describe a spectral method of transferring bounds on cross-correlations for one family to another.

Let p be prime and let $q = p^n$ be a power of p. Let $\mathcal{H}$ be a set of functions from F_{q^e} to F_q such that if $a \in F_q^*$ and $h(x) \in \mathcal{H}$, then there exist $B \in F_{q^e}$ and $h' \in \mathcal{H}$ such that $ah(x) = h'(Bx)$ for all $x \in F_{q^e}$. Let $\mathcal{F}$ be a set of functions from F_q to F_p and let α be a primitive element in F_{q^e}. For any $f \in \mathcal{F}, h \in \mathcal{H}$, let $S^{f,h} = s_0, s_1 \cdots$ with $s_i = f(h(\alpha^i))$. Its period divides $q^e - 1$. We are interested in the maximum cross-correlations within such a family $\mathcal{S}^{\mathcal{F},\mathcal{H}} = \{S^{f,h} : f \in \mathcal{F}, h \in \mathcal{H}\}$.

II. Main Results

Let $S = s_0, s_1, \cdots$ and $T = t_0, t_1, \cdots$ be sequences over F_p with period L and τ be an integer. Let ζ be a complex primitive pth root of unity. The cross-correlation of S and T with shift τ is

$$C_{S,T}(\tau) = \sum_{i=0}^{L-1} \zeta^{s_i - t_{i+\tau}}.$$

It is more convenient to work with functions on finite fields. Thus if $g_1, g_2 : F_{p^r} \to F_p$, then for $a \neq 0$ we define

$$C_{g_1,g_2}(a) = \sum_{z\in F_{p^r}} \zeta^{g_1(z)-g_2(az)}.$$

If $\alpha \in F_{p^r}$ is primitive and $S = s_0, s_1, \cdots$ and $T = t_0, t_1, \cdots$ with $s_i = g_1(\alpha^i)$ and $t_i = g_2(\alpha^i)$, then

$$C_{g_1,g_2}(\alpha^\tau) = C_{S,T}(\tau) + \zeta^{g_1(0)-g_2(0)}.$$

Functions g_1 and g_2 are *equivalent* if for some $a \in F_{p^r}$ we have $g_1(x) = g_2(ax)$ for all x. If $\mathcal{G}$ is a set of pairwise inequivalent functions on F_{p^r}, then we say that $\mathcal{G}$ has *shifted correlations bounded by* K if for every $g_1, g_2 \in \mathcal{G}$, we have $|C_{g_1,g_2}(a)| < K$ unless $g_1 = g_2$ and $a = 1$.

Let $\mathcal{H}$ and $\mathcal{F}$ be families of functions as in the introduction. For $h_1, h_2 \in \mathcal{H}$ and $f_1, f_2 \in \mathcal{F}$ let

$$\Gamma_{f_1,h_1,f_2,h_2} = C_{f_1\circ h_1, f_2\circ h_2}(1).$$

For $u, v \in F_q$, let

$$N_{h_1,h_2}(u,v) = |\{z \in F_{q^e} : h_1(z) = u, h_2(z) = v\}|.$$

Then

$$\begin{aligned}\Gamma_{f_1,h_1,f_2,h_2} &= \sum_{z\in F_{q^e}} \zeta^{f_1(h_1(z))-f_2(h_2(z))}\\ &= \sum_{u,v\in F_q} \zeta^{f_1(u)-f_2(v)} N_{h_1,h_2}(u,v).\end{aligned}$$

We can express this in terms of matrices. Let N_{h_1,h_2} be the p^{2n} by 1 matrix whose (u,v)th entry is $N_{h_1,h_2}(u,v)$. Let B_{f_1,f_2} be the 1 by p^{2n} matrix whose (u,v)th entry is $\zeta^{f_1(u)-f_2(v)}$. Then

$$\Gamma_{f_1,h_1,f_2,h_2} = B_{f_1,f_2} N_{h_1,h_2}. \quad (1)$$

A. Klapper is with the University of Kentucky. Project sponsored by the National Science Foundation under grant #9980429.

C. Carlet is with INRIA.

Now let tr be the trace function from F_q to F_p. We want to relate Γ_{f_1,h_1,f_2,h_2} to the set of $\Gamma_{tr,h_1',tr,h_2'}$ where h_1' and h_2' vary in $\mathcal{H}$. In particular, for $x,y \in F_q$, let

$$\begin{aligned}\Phi_{h_1,h_2}(x,y) &= \sum_{z\in F_{q^e}} \zeta^{tr(xh_1(z))-tr(yh_2(z))}\\ &= \sum_{u,v\in F_q} \zeta^{tr(xu-yv)} N_{h_1,h_2}(u,v).\end{aligned}$$

Let A be the p^{2n} by p^{2n} matrix whose $((x,y),(u,v))$th entry is $\zeta^{tr(xu-yv)}$ and let P_{h_1,h_2} be the p^{2n} by 1 matrix whose (x,y)th entry is $\Phi_{h_1,h_2}(x,y)$. Then we have $P = AN_{h_1,h_2}$. Furthermore, A is invertible and

$$A^{-1} = \frac{1}{p^{2n}}\overline{A}$$

where $\overline{A}$ denotes the complex conjugate. Thus

$$N_{h_1,h_2} = \frac{1}{p^{2n}}\overline{A}P_{h_1,h_2}$$

and by equation (1),

$$\Gamma_{f_1,h_1,f_2,h_2} = \frac{1}{p^{2n}} B_{f_1,f_2}\overline{A}P_{h_1,h_2}. \tag{2}$$

Also, we have

$$\begin{aligned}&\frac{1}{p^{2n}}(B_{f_1,f_2}\overline{A})_{(x,y)}\\ &\quad= \frac{1}{p^{2n}}\sum_{u,v\in F_q}\zeta^{f_1(u)-f_2(v)-tr(xu-yv)}\\ &\quad= \frac{1}{p^{2n}}\sum_{u\in F_q}\zeta^{f_1(u)-tr(xu)}\sum_{v\in F_q}\zeta^{-(f_2(u)-tr(yv))}\\ &\quad= \frac{\widehat{f_1}(x)\overline{\widehat{f_2}(y)}}{q^2},\end{aligned}$$

where $\widehat{f}(x) = \sum_{u\in F_q}\zeta^{f(u)-tr(xu)}$ is the Walsh transform of the function f.

Theorem 1: If h_1 and h_2 are functions from F_{q^e} to F_q and f_1 and f_2 are functions from F_q to F_p, then

$$\Gamma_{f_1,h_1,f_2,h_2} = \frac{1}{q^2}\sum_{x,y\in F_q}\widehat{f_1}(x)\overline{\widehat{f_2}(y)}\Gamma_{tr,xh_1,tr,yh_2}. \tag{3}$$

When $x = y = 0$, we have $\Gamma_{tr,xh_1,tr,yh_2} = q^e$. Thus we want this term to vanish. This happens if we assume that $\widehat{f}(0) = 0$ for every $f \in \mathcal{F}$. When this happens we say that f is a balanced function. It follows that the terms where $x = 0$ or $y = 0$ vanish as well.

Now let $\mathcal{T} = \{tr\}$. We want the remaining nonzero terms to be nontrivial correlations of functions in the family $\{tr\circ h : h \in \mathcal{H}\}$. If $h_1 = ch_2$, then $\Gamma_{tr,xh_1,tr,xch_2} = \Gamma_{tr,xch_2,tr,xch_2}$ is the cross-correlation of a function with itself, and all such $\Gamma_{tr,xh_1,tr,xch_2}$ equal q^e. Thus we must know that the sum of the coefficients of all such terms in equation (3) is zero. That is,

$$\begin{aligned}0 &= \sum_{x\in F_q}\widehat{f_1}(x)\overline{\widehat{f_2}(xc)}\\ &= \sum_{x\in F_q}\sum_{u\in F_q}\zeta^{f_1(u)-tr(ux)}\sum_{v\in F_q}\zeta^{-(f_2(v)-tr(vxc))}\\ &= \sum_{u,v\in F_q}\zeta^{f_1(u)-f_2(v)}\sum_{x\in F_q}\zeta^{tr((-u+cv)x)}\\ &= q\sum_{v\in F_q}\zeta^{f_1(cv)-f_2(v)}.\end{aligned}$$

This must hold as long as $f_1 \neq f_2$ or $c \not\equiv 0, 1 \bmod q^e - 1$. This amounts to saying that f_1 and f_2 have ideal shifted cross-correlations. But it follows from Welch's bound that this is only possible if $\mathcal{F}$ consists of a single function with ideal autocorrelation.

Finally, we must assume that this is the only way that $tr(xh_1(z))$ and $tr(xh_2(z))$ can be equivalent.

Corollary 1: Suppose that

1) if $h_1, h_2 \in \mathcal{H}$, and h_2 is not a nonzero scalar multiple of h_1 and x and y are nonzero, then $tr(xh_1(z))$ and $tr(yh_2(z))$ are inequivalent;
2) $\{tr\circ h : h \in \mathcal{H}\}$ has shifted cross-correlations bounded by K;
3) $\mathcal{F} = \{f\}$ where f is balanced and has ideal autocorrelations.

Let

$$M = \sum_{x\in F_q}|\widehat{f}(x)|.$$

Then $\{f\circ h : h \in \mathcal{H}\}$ has shifted correlations bounded by $(M/q)^2K \leq qK$.

Proof: According to relation (3), it remains to see that $M \leq q^{3/2}$. We can think of the Walsh transform of f as a point in real q dimensional space. Parseval's theorem says that

$$\sum_{x\in F_q}|\widehat{f}(x)|^2 = q^2.$$

Thus the point defined by the Walsh transform is on the sphere with radius q. We can take absolute values of the coordinates and thus assume the point is in the positive hyper-quadrant. Thus we want to find the maximum z such that the hyperplane $x_1 + \cdots + x_q = z$ has nonempty intersection with the sphere of radius q. This must be the z such that the corresponding hyperplane is tangent to the sphere, and thus the (unique) intersection point satisfies $x_1 = x_2 = \cdots x_q \overset{\text{def}}{=} x$. Thus $qx^2 = q^2$, $x = q^{1/2}$, and $M = q^{3/2}$ as needed. ■

There are many families of sequences that arise from functions of the form $tr\circ h$ whose correlations are known. Corollary 1 can be applied immediately to these sequences for any appropriate function f. For example, for $f(x) = tr(Ax^{1+p^j})$, the rank of f has been fully analyzed (see, e.g., [10], [12]). Such known results can now be used to obtain new families with known bounds on their shifted correlations.

The new results can also be used to improve existing bounds for some families. For example, Sun, Klapper, and Yang [20] studied sequences of the form in the current paper with $\mathcal{H} = \{tr_q^{q^e}(Ax+Bx^{1+p}) : A, B \in F_{q^e}, B \neq 0\}$, where $tr_q^{q^e}$ denotes the trace function from F_{q^e} to F_q. When p is odd and f is an arbitrary balanced function, they showed that the set $\{f \circ h : h \in \mathcal{H}\}$ has maximum shifted correlations bounded by $(q^2-1)q^{e/2}$ if ne is odd and bounded by $(q^2-q)q^{e/2}$ if ne is even.

However, if we take $f = tr$, then the correlations are of form

$$S(A,B) = \sum_{x \in F_{q^e}} \zeta^{tr_p^{q^e}(Ax+Bx^{1+p})}.$$

Such exponential sums were studied by Carlitz [6] and were used by Sun, Klapper, and Yang to obtain their results. It follows from Carlitz's work that

$$S(A,B) \leq \begin{cases} pq^{e/2} & \text{if } ne \text{ is even} \\ q^{e/2} & \text{if } ne \text{ is odd} \end{cases}$$

Therefore the family $\{tr_p^{q^e}(Ax+Bx^{1+p}) : A, B \in F_{q^e}, B \neq 0\}$ has correlations bounded by the same values. It follows from Corollary 1 that the family $\{f \circ h : h \in \mathcal{H}\}$ has maximum shifted correlations bounded by $pq^{e/2+1}$ if ne is even, and by $q^{e/2+1}$ if ne is odd, an improvement by a factor of about q over the previous bound.

For some choices of f we may have further improvements. The bound in Corollary 1 is strongest if M is small. Recall that the Holder-Schwartz inequality says that for any real vectors $(a_1, \cdots, a_r)$ and $(b_1, \cdots, b_r)$ we have

$$|\sum_{i=1}^{r} a_i b_i| \leq \left(\sum_{i=1}^{r} a_i^2\right)^{1/2} \left(\sum_{i=1}^{r} b_i^2\right)^{1/2}.$$

By Parseval's theorem (see the proof of Corollary 1) and the Holder-Schwartz inequality with $a_x = 1$ if $\widehat{f}(x) \neq 0$, $a_x = 0$ if $\widehat{f}(x) = 0$, and $b_x = \widehat{f}(x)$, we have

$$\begin{aligned} q^2 &= \sum_{x \in F_q} |\widehat{f}(x)|^2 \\ &\leq q \sum_{x \in F_q} |\widehat{f}(x)| \\ &= qM \\ &\leq q^2 N_f^{1/2} \end{aligned}$$

where $N_f = |\{x : \widehat{f}(x) \neq 0\}|$. Thus

$$q \leq M \leq q N_f^{1/2}. \tag{4}$$

Alternatively, we can use the Weil's bound: if a polynomial $f(x)$ in one variable $x \in F_q$ has degree r relatively prime to q, then [21]

$$\left| \sum_{x \in F_q} (-1)^{f(x)} \right| \leq (r-1)\ q^{1/2}.$$

The condition on r can in fact be relaxed [5], [14]. If f is not affine, this leads to the bound

$$M \leq (r-1)\ q^{1/2}\ N_f. \tag{5}$$

This gives a better bound than equation (4) when $(r-1)^2 N_f < q$.

Suppose M is minimal. That is $M = q$. Then

$$\sum_{x \in F_q} |\widehat{f}(x)|^2 = q \sum_{x \in F_q} |\widehat{f}(x)|.$$

Thus for every x we have $|\widehat{f}(x)|^2 = q|\widehat{f}(x)|$. That is, $\widehat{f}(x) = 0$ or $|\widehat{f}(x)| = q$. But by Parseval's theorem, $|\widehat{f}(x)| = q$ for at most one value of x. It follows from the inversion formula that $f(z) = tr(az) + c$ for some constants a and c, which gives us essentially the original family.

III. Constructions of Good Families

We can obtain nearly optimal bounds if we can choose f so it has few nonzero Walsh coefficients $\widehat{f}(x)$. However, despite the inversion formula these coefficients cannot be chosen arbitrarily. For example, Parseval's theorem must hold. One way to obtain good examples is to choose f to be linearly equivalent to a k-resilient (that is, balanced and kth order correlation immune [19]) function for large k. This is equivalent to saying that for all x with Hamming weight at most k, $\widehat{f}(x) = 0$ [22]. This guarantees that the sum of the absolute values of the Walsh coefficients is small. It follows that for such f

$$M \leq q|\{x : \widehat{f}(x) \neq 0\}|^{1/2} \leq q \left(\sum_{i=0}^{n-k-1} \binom{n}{i} \right)^{1/2}.$$

Corollary 2: Suppose that

1) if $h_1, h_2 \in \mathcal{H}$, h_2 is not a nonzero scalar multiple of h_1, and x and y are nonzero, then $tr(xh_1(z))$ and $tr(yh_2(z))$ are inequivalent;
2) $\{tr{\circ}h : h \in \mathcal{H}\}$ has shifted cross-correlations bounded by K;
3) f has ideal autocorrelations and is k-resilient.

Then $\{f{\circ}h : h \in \mathcal{H}\}$ has shifted correlations bounded by $(\sum_{i=0}^{n-k-1} \binom{n}{i})K$.

Unfortunately, while there are several constructions of k-resilient functions (see for example the constructions due to Siegenthaler [19], Camion, Carlet, Charpin, and Sendrier [1], Carlet [4], and Maitra and Sarkar [18]), it remains as an open problem to find k-resilient functions with ideal shifted autocorrelations and $k > 2$. It may very well be that no such functions exist, which would render Corollary 2 uninteresting.

Another approach is to use functions known to have ideal autocorrelations and to find a bound on the sum of the absolute values of their Walsh coefficients. In what follows, let K be a bound on the pairwise cross-correlations in a family of functions $\{tr{\circ}h : h \in \mathcal{H}\}$, and let C denote the bound we obtain on the pairwise cross-correlations in a family of functions $\{f{\circ}h : h \in \mathcal{H}\}$ by bounding M.

As a first method, choose ν such that $gcd(\nu, q-1) = 1$ and $\gamma \in F_q$. If $a \neq 1$, then we have

$$\sum_{x \in F_q} \zeta^{tr(x^\nu - (ax)^\nu)} = \sum_{x \in F_q} \zeta^{tr((1-a^\nu)x^\nu)} = 0.$$

Thus the Boolean function $f(x) = tr(\gamma x^\nu)$ has ideal autocorrelations. In the binary case, the support of f is a *Singer cyclic difference set*. There are several cases that can be considered.

Suppose n is odd. If ν is chosen so that $\sum_{x\in F_q}\zeta^{tr(x^\nu+ax)}\in\{0,\pm p^{(n+1)/2}\}$ (in the binary case this means f is *almost bent*), then by Parseval's relation we have

$$p^{2n}=\sum_{a\in F_q}\widehat{f}(a)^2=N_f p^{n+1}.$$

Thus $N_f=p^{n-1}$, and $M=N_f\cdot p^{(n+1)/2}=p^{(3n-1)/2}$. For such a function f, we obtain a family of functions with pairwise cross-correlations bounded by $C\le p^{n-1}K=(q/p)K$. The cases $\nu=2^i+2^j$, $\nu=2^{(n-1)/2}+3$ and $\nu=2^{2k}-2^k+1$ ($gcd(k,n)=1$) give almost bent functions (cf. e.g. [2], [3]).

When $p=2$, there is a method for constructing the functions we need due to Maschietti [15]. Let κ be an integer such that $gcd(\kappa,2^n-1)=1$ and the map $h:x\mapsto x+x^\kappa$ is 2 to 1. Then $F_q\setminus\{x+x^\kappa;x\in F_q\}$ is the support of a function f with ideal auto-correlation. Singer sets with $\nu=\gamma=1$ correspond to $\kappa=2$. For $n\ge 5$ odd we can take $\kappa=6$ (the so-called Segre case). For $n\ge 7$ odd we can take $\kappa=\sigma+\tau$ or $\kappa=3\sigma+4$, where $\sigma=(n+1)/2$ and $\tau=2^{(n+1)/4}$ if $n\equiv 3 \bmod 4$ and $\tau=2^{3(n-1)/4+1}$ if $n\equiv 1 \bmod 4$.

Such a function f is balanced by the fact that h is 2 to 1. We also have, for every nonzero a

$$\widehat{f}(a)=\sum_{x\notin S_f}(-1)^{tr(ax)}-\sum_{x\in S_f}(-1)^{tr(ax)}=2\sum_{x\notin S_f}(-1)^{tr(ax)}$$

where S_f is the support of f. Thus, again by the fact that h is 2 to 1,

$$\widehat{f}(a)=\sum_{x\in F_q}(-1)^{tr(a(x+x^\kappa))}=\widehat{g}(b),$$

where $g(x)=tr(x^\kappa)$ and $b=a^{(\kappa-1)/\kappa}$. So the functions this method produces give the same values for $\sum_{a\in F_q}|\widehat{f}(a)|$ as for Singer sets.

Again, if $p=2$, there is a method due to No et al. [16]. The function f is the indicator of the set $\{x^d+(x+1)^d;\ x\in F_q\}$, where $gcd(d,2^n-1)=1$ and where the map $x\mapsto x^d+(x+1)^d$ is 2 to 1. The function f is then balanced and, for every nonzero a

$$\widehat{f}(a)=\sum_{x\in F_q}(-1)^{tr(a(x^d+(x+1)^d))}=\sum_{x\in F_q}(-1)^{tr(x^d+(x+b)^d)},$$

where $a=b^d$.

Let n be even and let k be such that $3k\equiv 1 \bmod n$ and $d=2^{2k}-2^k+1$ (called a Kasami exponent). Then, as was shown by Dillon and Dobbertin [8], f has ideal autocorrelation and its Walsh transform is zero outside the set $U=\{x^3;\ x\in F_{2^n}^*\}$ whose cardinality is $(2^n-1)/3$. By equation (4), we obtain

$$\sum_{a\in F_q}|\widehat{f}(a)|\le 2^n\sqrt{\frac{2^n-1}{3}}<\frac{2^{3n/2}}{\sqrt{3}}.$$

A final method arises from a theorem proved by Dillon.

Theorem 2 (Dillon [7]): Let $d=4^k-2^k+1$ (a so-called Kasami exponent) where $1\le k<n$ and $n/\gcd(k,n)$ is odd. Let $f(x)=tr(x^d)$. Then $\widehat{\chi_f}(a)$ equals 0 (with multiplicity 2^n-2^{n-e}) or $\pm 2^{(n+e)/2}$ where $e=gcd(n,k)$.

It is well known (and easy to see) that 2^r+1 is relatively prime to 2^n-1 if $n/\gcd(r,n)$ is odd. Under the hypotheses of Dillon's theorem (also called Welch's theorem), $d=(2^{3k}+1)/(2^k+1)$. Also, $n/\gcd(3k,n)$ divides $n/\gcd(k,n)$, so $n/\gcd(3k,n)$ is odd and $2^{3k}+1$ is relatively prime to 2^n-1. It follows that d is relatively prime to 2^n-1, so $f(x)$ has ideal autocorrelations. It follows from Dillon's theorem that $M=2^{(3n-e)/2}$. For such a function f, we obtain a family of functions with pairwise cross-correlations bounded by $C\le 2^{n-e}K=(q/2^e)K$. This can be made as small as possible by taking $n=3\cdot 2^r$ for some r. In this case we have a family of functions with pairwise cross-correlations bounded by $C=2^{2^{r+1}}K$.

ACKNOWLEDGEMENTS

The authors are grateful to Harald Niedereitter and the Institute for Mathematical Sciences at the National University of Singapore for bringing them together during the summer of 2001. Their visit was supported by the Institute and by a grant from DSTA of Singapore.

REFERENCES

[1] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in *Advances in Cryptology: Crypto '91, Proceedings, Lecture Notes in Computer Science*, vol. 576, 1991, pp. 86–100.

[2] A. Canteaut, P. Charpin and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture," *IEEE Trans. Info. Theory,* vol. 46, pp. 4–8, 2000.

[3] A. Canteaut, P. Charpin and H. Dobbertin, "Weight divisibility of cyclic codes, highly nonlinear functions on F_{2^m} and crosscorrelation of maximum-length sequences," *SIAM J. Discrete Math.*, vol. 13, pp. 105–138, 2000.

[4] C. Carlet, "More correlation-immune and resilient functions over Galois fields and Galois rings," in *Advances in Cryptology, EUROCRYPT' 97, Lecture Notes in Computer Science,* vol. 1233, Springer Verlag, 1997, pp. 422-433.

[5] L. Carlitz and S. Uchiyama, "Bounds for exponential sums," *Duke Math. J.,* vol. 24, pp. 37-41, 1957.

[6] L. Carlitz, "Evaluation of some exponential sums over finite fields," *Math. Nachr.*, pp. 319-339, 1980.

[7] J. Dillon, "Multiplicative difference sets via additive characters," *Designs, Codes and Cryptography,* vol. 17, pp. 225-235, 1999.

[8] J. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters," preprint, 1998.

[9] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canad. J. Math.*, vol. 14, pp. 614–625, 1962.

[10] A. Klapper, "Cross-correlations of geometric sequences in characteristic two," *Designs, Codes, and Cryptography,* vol. 3, pp. 347–377, 1993.

[11] A. Klapper, "Large families of sequences with low correlations and large linear span," *IEEE Trans. Info. Theory,* vol. 42, pp. 1241–1248, 1996.

[12] A. Klapper, "Cross-correlations of quadratic form sequences in odd characteristic," *Designs, Codes, and Cryptography,* vol. 11, pp. 1–17, 1997.

[13] A. Klapper, A. H. Chan, and M. Goresky, "Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences," *Discrete Appl. Math.*, vol. 46 pp. 1–20, 1993.

[14] R. Lidl and H. Niederreiter, *Finite Fields, Second Edition*. Cambridge, UK: Cambridge University Press, 1997.

[15] A. Maschietti, "Difference sets and hyperovals," *Designs, Codes, and Cryptography*, vol. 14, pp. 89-98, 1998.

[16] J. No, H. Chung, and M. Yun, "Binary pseudorandom sequences of period 2^m-1 with ideal autocorrelation generated by the polynomial $z^d+(z+1)^d$," *IEEE Trans. Info. Theory,* vol. 44, pp. 1278-1282, 1998.

[17] J. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Info. Theory,* vol. 35, pp. 371–379, 1989.

[18] P. Sarkar, and S. Maitra, "Nonlinearity Bounds and Constructions of Resilient Boolean Functions," in *Advances in Cryptology, CRYPTO 2000, Lecture Notes in Computer Science,* vol. 1880, 2000, pp. 515–532.

[19] T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic applications,” *IEEE Trans. Info. Theory,* vol. IT-30, pp. 776–780, 1984.

[20] W. Sun, A. Klapper, and Y. Yang, “On correlations of a family of generalized geometric sequences” *IEEE Trans. Info. Theory,* vol. 47, pp. 2609–2618, 2001.

[21] A. Weil, “On some exponential sums,” *Proc. Nat. Acad. Sci. U.S.A.,* vol. 34 pp. 204-207, 1948.

[22] Guo-Zhen Xiao and J. Massey, “A Spectral Characterization of Correlation-Immune Combining Functions,” *IEEE Trans. Info. Theory,* vol. 34, pp. 569–571, 1988.

Andrew Klapper received the A.B. degree in mathematics from New York University, New York, NY, in 1974, the M.S. degree in applied mathematics from SUNY at Binghamton, Binghamton, NY, in 1975, the M.S. degree in mathematics from Stanford University, Stanford, CA, in 1976, and the Ph.D. degree in mathematics from Brown University, Providence, RI, in 1982. His thesis, in the area of arithmetic geometry, concerned the existence of canonical subgroups in formal grouplaws.

From 1981 to 1984 he was a Postdoc in the Department of Mathematics and Computer Science at Clark University. From 1984 to 1991 he was an Assistant Professor in the College of Computer Science at Northeastern University. From 1991 to 1993 he was an Assistant Professor in the Computer Science Department at the University of Manitoba. Currently he is a Professor in the Department of Computer Science at the University of Kentucky. He was awarded a University Research Professorship for 2002-03. His past research has included work on algebraic geometry over p-adic integer rings, computational geometry, modeling distributed systems, structural complexity theory, and cryptography. His current interests include statistical properties of pseudo-random sequences with applications in cryptography and CDMA; covering properties of codes; and morris dancing.

Dr. Klapper is a member of the IEEE Information Theory Society and the International Association for Cryptologic Research. He was the general chair of the Crypto ’98 conference and was been the Associate for Sequences for the IEEE Transactions on Information Theory from 1999 until 2002.

Claude Carlet Claude CARLETClaude CARLET **received the Ph.D. degree from the University of Paris 6 in 1990 and the Habilitation to Direct theses from the University of Amiens in 1994.**

He was with the department of Computer Science of Amiens from 1990 to 1994 and with the department of Computer Science of Caen from 1994 to 2000.

He is currently Professor of Mathematics at the University of Paris 8, and associate researcher at the “Projet Codes” of INRIA. He is also associate editor for coding theory of IEEE Transactions on Information Theory.

His research interests include coding theory, Boolean functions and cryptology.