Resilient $PC(l)$ of Order k Boolean Functions from AG-Codes

Hao Chen
Department of Computing and
Information Technology
Fudan University
Shanghai 200433
People's Republic of China
Liang Ma
Institute of Systems Science
University of Shanghai for Science and Technology
Shanghai 200093, P.R.China
and
Jianhua Li
Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai 200030, P.R.China

August, 2006

Abstract

Propagation criterion of degree l and order k ($PC(l)$ of order k) and resiliency of vectorial Boolean functions are important for cryptographic purpose (see [1, 2, 3,6, 7,8,10,11,16]. Kurosawa , Stoh [8] and Carlet [1] gave a construction of Boolean functions satisfying $PC(l)$ of order k from binary linear or nonlinear codes in. In this paper, algebraic-geometric codes over $GF(2^m)$ are used to modify Carlet and

Kurosawa-Satoh's construction for giving vectorial resilient Boolean functions satisfying $PC(l)$ of order k. The new vectorial Boolean functions are compared with previously known results.

Index Terms—Cryptography, Boolean functions, algebraic-geometric codes

I. Introduction and Preliminaries

In cryptography vectorial Boolean functions are used in many applications (see [2]). Propagation criterion of degree l and order k is one of the most general properties of Boolean functions which have to be satisfied for their use in block ciphers. It was introduced in Preneel et al [11], which extends the property strictly avalanche criterion SAC in [16]. For a Boolean function $f(x) = (x_1, ..., x_n)$ of n variables, set $\frac{Df}{D\alpha} = f(x) + f(x + \alpha)$, f satisfies $PC(l)$ if $\frac{Df}{D\alpha}$ is a balanced Boolean function for any α with $1 \leq wt(\alpha) \leq l$. When any function obtained from f by keeping any k variables fixed satisfies $PC(l)$, we say f have the property $PC(l)$ of order k. For a vectorial Boolean function $\mathbf{f} = (f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))$ it is called $(n, m) - PC(l)$ of order k if any nonzero linear combination of $f_1, ..., f_m$ satisfies $PC(l)$ of order k. A vectorial Boolean function $\mathbf{f} = (f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))$ is called k-resilient if all the sets $f^{-1}(c), c \in GF(2)^m$ have the same cardinality. Equivalently $\mathbf{f}$ is k-resilient if any nonzero linear combination $\Sigma_i a_i f_i$ is a k-resilient. Resiliency of vectorial Boolean functions are relevant to quantum key distribution and pseudo-random sequence generators for stream ciphers (see [1] and [2]).

We recall the Maiorana-MacFarland construction of (vectorial) functions. Let $\phi_i : GF(2)^s \longrightarrow GF(2)^s$ be vectorial Boolean functions for $i = 1, ..., m$, the class of Maiorana-MacFarland $(r+s, m)$ Boolean functions is the set of the functions $F(x, y)$ of the form $F(x, y) = (x \cdot \phi_1(y) + h_1(y), ..., x \cdot \phi_m(y) + h_m(y)) : GF(2)^{r+s} \longrightarrow GF(2)^m, (x, y) \in GF(2)^r \times GF(2)^s$. It is well known that $F(x, y)$ is at least t-resilient if $a_1\phi_1(y) + \cdots + a_m\phi_m(y), (a_1, ..., a_m) \in GF(2)^m$ has its Hamming weight at least $t + 1$ for any $y \in GF(2)^s$ (see [1] and [2]).

It was known that $PC(n)$ Boolean functions of n variables are just the perfect nonlinear functions introduced by W.Meier and O.Staffebach [10].

They exist only when n is even. Bent functions are example of this kind of functions (see [10] and [16]). People only have few constructions of $PC(l)$ of order k Boolean functions. In [1] and [8] $PC(l)$ of order k (vectorial) Boolean functions were constructed from binary linear or nonlinear codes. For satisfying the conditions of these constructions the minimum distances of the binary codes and its dual have to be lower bounded. Some lower bounds on the minimum length (which is the half of the number of the Boolean functions in Kurosawa-Satoh construction) of these binary linear codes was studied in [9].

From [1, 8] we know the following results.

Kurosawa-Satoh Theorem ([8]). *Let C_1 be a linear binary code of length s and minimum distance d_1 and dual distance d_1', C_2 be a linear binary code of length t with minimum distance d_2 and dual distance d_2'. Set $l = min\{d_1', d_2'\} - 1$ and $k = min\{d_1, d_2\} - 1$. Then the Boolean functions of $s + t$ inputs satisfying $PC(l)$ of order k can be explicitly given.*

Corollary 1 ([8] and [9]). *Let C be a linear binary code with minimum distance at least $k+1$ and dual distance at least $l+1$. Then Boolean functions of $2n$ inputs satisfying $PC(l)$ of order k can be explicitly given.*

Carlet Theorem ([1]). *For a Boolean function $f(x, y) = x\phi(y) + g(y)$ from $GF(2)^{r+s}$ to $GF(2)$, f satisfies $PC(l)$ of order k if the following two conditions are satified.*
1) the sum of at least 1 and at most l coordinates of ϕ is k-resilient;
2) if $b \in GF(2)^s$ is nonzero and has its weight smaller than or equal to l, at least $k + 1$ coordinates of the words $\phi(y + b)$ and $\phi(y)$ differ.

In this paper the functions ϕ_i's in the Mairana-MacFarland construction are of the form $A_i y + v_i$, where A_i is a fixed $r \times s$ matrix over $GF(2)$ and v_i is a fixed vector in $GF(2)^r$, for $i = 1, ..., m$.

Let us now recall some basic facts about algebraic-geometric codes (see [12],[13] and [14]). Let X be an absolutely irreducible, projective and smooth curve defined over $GF(q)$ with genus g, $D = \{P_1, ...P_n\}$ be a set of $GF(q)$-rational points of X and G be a $GF(q)$-rational divisor satisfying $supp(G) \bigcap D = \emptyset$, $2g - 2 < deg(G) < n$. Let $L(G) = \{f : (f) + G \geq$

$0\}$ is the linear space (over $GF(q)$) of all rational functions with its divisor not smaller than $-G$ and $\Omega(B) = \{\omega : (\omega) \geq B\}$ be the linear space of all differentials with their divisors not smaller than B. Then the functional AG(algebraic-geometric)code $C_L(D,G) \in GF(q)^n$ and residual AG(algebraic-geometric) code $C_\Omega(D,G) \in GF(q)^n$ are defined. $C_L(D,G)$ is a $[n, k = deg(G) - g + 1, d \geq n - deg(G)]$ code over $GF(q)$ and $C_\Omega(D,G)$ is a $[n, k = n - deg(G) + g - 1, d \geq deg(G) - 2g + 2]$ code over $GF(q)$. We know that the functional code is just the evaluations of functions in $L(G)$ at the set D and the residual code is just the residues of differentials in $\Omega(G - D)$ at the set D.

We also know that $C_L(D,G)$ and $C_\Omega(D,G)$ are dual codes. It is known that for a differential η that has poles at $P_1, ...P_n$ with residue 1 (there always exists such a η, see [12]) we have $C_\Omega(D,G) = C_L(D, D - G + (\eta))$, the function f corresponds to the differential $f\eta$. This means that functional codes and residue code are essentially the same. It is clear that if there exist a differential η such that $G = D - G + (\eta)$, then $C_L(P,G) = C_\Omega(P,G) = C_L(P, P - G + (\eta))$ is a self-dual code over $GF(q)$. For many examples of AG codes, including these self-dual AG-codes, we refer to [12],[13] and [14].

It is well-known in the theory of algebraic curves over finite fields that there exists algebraic curves $\{X_t\}$ defined over $GF(q^2)$ with the property $lim\frac{N(X_t)}{g(X_t)} = q - 1$ (Drinfeld-Vladut bound)(see [4] and [5]), where $N(X_t)$ is the number of $GF(q^2)$ rational points on the curve X_t and $g(X_t)$ is the genus of the curve X_t. Actually for this family of curve $N(X_t) \geq (q-1)q^t + 1$, $g(X_t) = q^t - 2q^{\frac{t}{2}} + 1$ for t even and $g(X_t) = q^t - q^{\frac{t+1}{2}} - q^{\frac{t-1}{2}} + 1$ for t odd (see [4] and [5]).

For a AG-code over $GF(2^m)$ its expansion to some base B of $GF(2^m)$ over $GF(2)$ will be used in our construction. Let $\{e_1, .., e_m\}$ be a base of $GF(2^m)$ as a linear space over $GF(2)$. For a $[n,k,d]$ linear code $C \subseteq GF(2^m)^n$, the expansion with respect to the base B is the binary code $B(C) \subseteq GF(2)^{mn}$ consists of all codewords $B(x) = (B(x_1), ..., B(x_n)), x = (x_1, .., x_n) \in C$. Here $B(x_i)$ is a length m binary vector $(x_i^1, ..., x_i^m)$, where $x_i = \Sigma_{j=1}^m x_i^j e_j \in GF(2^m)$. It is easy to verify that the binary linear code $B(C)$ is $[mn, mk, \geq d]$ code. It is well-known that there exists a self-dual base B for any finite field

$GF(2^m)$. The following result is useful in our construction.

Proposition 1 (see [6]). *Let B be a self-dual base of $GF(2^m)$ over $GF(2)$ and C be a linear code over $GF(2^m)$. Then the dual code $B(C)^{\perp}$ is just $B(C^{\perp})$.*

A divisor G on the curve X is called effective if the coefficients of all points in the support G is non-negative. We say $G_1 \geq G_2$ if $G_1 - G_2$ is an effective divisor. This gives a partial order relation on the set of all divisors. Let $U_1 =, ..., U_m$ be divisors on the curve X, set $max\{U_1, ..., U_m\}$ be the smallest divisor U such that $U - U_i$ is effective for all $i = 1, ..., m$ and $min\{U_1, ..., U_m\}$ be the biggest divisor U' such that $U_i - U'$ is effective for all $i = 1, ..., m$. For m divisors $U_1, ..., U_m$ and it is clear the intersection $\bigcap_i L(U_i) = L(max\{U_1, ..., U_m\})$, $\bigcap_i \Omega(U_i) = \Omega(max\{U_1, ..., U_m\})$, the linear span of $L(U_1), ..., L(U_m)$ is contained in $L(min\{U_1, ..., U_m\})$.

II. Main Result

The following Theorem 1 and Corollary 2 are the main results of this paper.

Theorem 1. *Let X (resp. X') be a projective, absolutely irreducible smooth curve of genus g (resp. g') defined over $GF(2^w)$ (resp. $GF(2^{w'})$). We denote $N(X)$(resp. $N(X')$) the number of $GF(2^w)$(resp. $GF(2^{w'})$) rational points on X(resp. X'). Let P (resp. P') be a set of n $GF(2^w)$(resp. n', $GF(2^{w'})$) rational points on X(resp. X'), $U_1, ..., U_m$(resp. $U'_1, ..., U'_m$) be $GF(2^w)$(resp. $GF(2^{w'})$-rational effective divisors on X(resp. X') with degree satisfying $2g-2 < deg(max\{U_1, ..., U_m\}) < n$ and $supp(max\{U_1, ..., U_m\}) \bigcap P = \emptyset$ (resp. $2g'-2 < deg(max\{U'_1, ..., U'_m\}) < n'$, $supp(max\{U'_1, ..., U'_m\}) \bigcap P' = \emptyset$). Suppose $deg(U_i) = deg(U'_i)$ for $i = 1, ..., n$. We have another $GF(2^{w'})$-rational effective divisor H on X' satisfying $deg(H)+deg(max\{U'_1, .., U'_m\}) < n'$ and $w'(deg(H) - g' + 1) \geq m$. It is assumed that $U'_1, ..., U'_m, H$ are disjoint divisors (that is their supports are dishoint). Then we have $(wn + w'n', m)$ vectorial t-resilient $PC(l)$ of order k Boolean functions with $wn + w'n'$ variables, where*

$$l = min\{deg(max\{U_1, ..., U_m\}) - 2g + 1, deg(max\{U'_1, ..., U'_m\}) - 2g' + 1\}$$
$$k = min\{n - deg(max\{U_1, ..., U_m\}) - 1, n' - deg(max\{U'_1, ..., U'_m\}) - 1\}$$
$$t = n' - deg(max\{U'_1, ..., U'_m, H\}) - 1.$$

If the curves, the bases of the linear space $L(U_i)$'s and $\Omega(U_i)$'s(resp. $L(U'_i)$'s, $L(H)$ and $\Omega(U'_i)$'s) are explicitly given, the $(wn+w'n', m)$ vectorial t-resilient $PC(l)$ of order k Boolean functions can be explicitly given.

Proof. We consider the $D_1^i = C_L(P, U_i), D_2^i = C_L(P', U'_i)$, then $(D_1^i)^\perp = C_\Omega(P, U_i), (D_2^i)^\perp = C_\Omega(P', U'_i)$. Let B and B' be self dual bases of $GF(2^w)$ and $GF(2^{w'}$ over $GF(2)$. We consider the linear binary codes $C_1^i = B(D_1^i), C_2^i = B'(D_2^i)$. From Proposition 1 $(C_1^i)^\perp = B(C_\Omega(P, U_i)), (C_2^i)^\perp = B'(C_\Omega(P', U'_i))$. The code parameters of C_1^i and C_2^i are $[wn, w(deg(U_i - g + 1), n - deg(U_i)]$ and $[w'n', m'(deg(U'_i) - g' + 1), n' - deg(U'_i)]$. The code parameters of $(C_1^i)^\perp$ and $(C_2^i)^\perp$ are $[wn, w(n - deg(U_i) + g - 1), deg(U_i) - 2g + 2]$ and $[w'n', w'(n' - deg(U'_i) + g' - 1), deg(U'_i) - 2g' + 2]$.

Let Q_i and R_i are the generator matrices of the binary linear code C_1^i and C_2^i respectively, for $i = 1, ..., m$. Here we note that Q_i's (resp R_i's) are $w(deg(U_i) - g + 1) \times wn$ matrices (resp. $w'(deg(U'_i) - g' + 1) \times w'n'$ matrices. Since $w'(deg(H) - g' + 1) \geq m$, we can find m linear independent vectors $v_1, ..., v_m$ in the binary linear code $B(C_L(H, P')$. Set $\phi_i(y) = (R_i)^\tau Q_i(y) + v_i, y \in GF(2)^{wn}$ for $i = 1, ..., m$, in Maiorana-MacFarland construction we get our $(wn + w'n', m)$ Boolean function $\mathbf{f} = (f_1, ..., f_m)$. Here ϕ_i's are mappings from $GF(2)^{wn}$ to $GF(2)^{w'n'}$. The image of ϕ_i is in the coset $v_i + C_2^i$ for $i = 1, ..., m$.

For any nonzero linear combination $a_1 f_1 + ... + a_m f_m$, we set $\phi(y) = \Sigma_i a_i \phi_i(y) + \Sigma_i a_i v_i$. Then it is clear that $\Sigma_i a_i \phi_i(y)$ is in the binary linear code $B(C_L(P', max\{U'_1, ..., U'_m\}))$ and $\Sigma_i a_i v_i$ is in the binary linear code $B(C_L(P', H))$. Because $max\{U'_1, ..., U'_m\}$ and H are disjoint, so $\Sigma_i a_i \phi_i(y) + \Sigma_i a_i v_i$ is not zero. On the other hand this is a nonzero code word in $B(C_L(P', max\{U'_1, ..., U'_m, H\}))$, its weight is at least $n' - deg(max\{U'_1, ..., U'_m, H\})$. Hence $\mathbf{f}$ is t-resilient.

From the above argument it is also known that $\phi(y) = \Sigma_i a_i \phi_i(y) + \Sigma_i a_i v_i$ takes over all codewords in the coset of the binary linear code

$B(C_L(P', max\{U'_1, ..., U'_m\}))$, when y takes over all vectors in $GF(2)^{wn}$. Thus the sum of arbitrary j (where, $1 \leq j \leq l$) coordinates of this function $\phi(y)$ is a nonzero function, since l is less than the Hamming distance of the code $B(C_\Omega(P', max\{U'_1, ..., U'_m\})) = (B(C_L(P', max\{U_1, ..., U_m\})))^\perp$. We can check that $\phi^{-1}(c)$ has the same cardinality for all $c \in GF(2)^{w'n'}$ since it is an affine mapping and it is a subcode of the coset code of $B(C_L(P', max\{U'_1, ..., U'_m\}))$. Thus dual distance of ϕ^{-1} is at least $k+1$. From Corollary 14 in [1], $\phi(y)$ is a k-resilient function. The 1st condition of Carlet Theorem is satisfied.

For any $b \in GF(2)^{wn}$, $\phi(y+b) + \phi(y) = \phi(b)$. If the weight of b has its weight smaller than or equal to l, it is not in $B(C_\Omega(P, max\{U_1, ..., U_m\}))$, thus $Q_i b$ can not be zero for all $i = 1, ..., m$. Thus at least one $(R_i)^\tau Q_i b$ is not zero. From the condition $U'_1, ..., U'_m$ are disjoint effective divisors on X', we know that $\phi(b) = \Sigma_i a_i (R_i)^\tau Q_i b$ is a nonzero codeword in $B(C_L(P', max\{U'_1, ..., U'_m\}))$. Thus $\phi(b)$ has its weight at least $k+1$. The 2nd condition of Carlet Theorem is satisfied. The conclusion is proved.

It is well-known in the theory of algebraic curves over finite fields, there are many curves over $GF(2^w)$ (see [12], [13] and [14]) with various number of rational points and genuses. Thus when we use Theorem 1 for constructing vectorial t-resilient $PC(l)$ of order k functions, we have very flexible choices of parameters on l, k and the number of variables $wn + w'n'$. This is quite similar to the role of the algebraic curves in theory of error-correcting codes. Therefore the algebraic-geometric method offer us numerous vectorial t-resilient $PC(l)$ of order k functions. Moreover the supports of the divisors $U_1, ..., U_m, U'_1, ..., U'_m, H$ need no to be the $GF(2^w)$ (or $GF(2^{w'})$) rational points, it is sufficient for the constructions in Theorem 1 that the divisors are $GF(2^w)$ (or $GF(2^{w'})$ rational. Thus we can easily choose the sets of points P, P' and divisors to construct vectorial resilient $PC(l)$ of order k Boolean functions.

III. Constructions

In the following part some examples of vectorial t-resilient $PC(l)$ of order k Boolean functions are constructed by Theorem 1 . Comparing our constructions with the previously-known $PC(l)$ of order k functions in [1,8], it seems our constructed vectorial t-resilient $PC(l)$ of order k functions are quite good.

We take $X = X'$ genus g curve which is defined over $GF(2^w)$, $U_i = U_i'$, $i = 1, ..., m$ are m disjoint effective divisors rational over $GF(2^w)$, in the case m is small and $deg(U_i) = deg(U_i') = t$ is not 1, we can always choose the supports of U_i's outside all $GF(2^w)$ rational points on X, for example, we can choose their supports $GF(2^{2w})$-rational points of X. In the following example, $P = P'$ are n $GF(2^w)$ points of X. So the only restriction is the upper bound of $n \leq N(X)$, the number of $GF(2^w)$-rational points of X. In this construction we have $(2wn, m)$ vectorial $n - mt - 1$-resilient Boolean functions satisfying $PC(mt - 2g + 1)$ of order $n - mt - 1$.

Example 1. We use genus 0 curve over $GF(4)$ in the construction. Then $(20, 2)$ vectorial $PC(5$ function is constructed if we take $m = 2, t = 2, n = 5$.

Example 2. We use genus 1 curve over $GF(4)$ in the construction, then $n \leq 9$. We have $(4n, m)$ vectorial $n - mt - 1$-resilient functions satisfying $PC(mt - 1)$ of order $n - mt - 1$. Thus $(36, 4)$ vectorial $PC(7)$ Boolean functions are constructed, $(36, 3)$ vectorial 1-resilient Boolean functions satisfying $PC(5)$ of order 1 are constructed, $(24, 2)$ vectorial 1-resilient Boolean functions satisfying $PC(3)$ of order 1 are constructed.

When $m = 1, t = 2$ we have $n - 3$-resilient $SAC(n - 3)$ functions of $4n$ variables for $n = 4, 5, 6, 7, 8, 9$.

Example 3 We use genus 4 curve over $GF(4)$ in the construction, then $n \leq 15$ (see [14]). The $(4n, m)$ vectorial $n - mt - 1$-resilient Boolean functions satisfying $PC(mt - 7)$ of order $n - mt - 1$ are constructed. Thus we have $(60, 7)$ vectorial $PC(7)$ and $(44, 5)$ vectorial $PC(3)$ Boolean functions, $(48, 5)$ vectorial 1-resilient Boolean functions satisfying $PC(3)$ of order 1, $(60, 6)$ vectorial 2-resilient Boolean functions satisfying $PC(5)$ of order 2.

When $m = 4, t = 2$ we have $(4n, 4)$ vectorial $n - 9$-resilient $SAC(n - 9)$ Boolean functions. For example, $(60, 4)$ vectorial 6-resilient $SAC(6)$ Boolean functions are constructed.

Corollary 2.*Let X be an algebraic curve over $GF(2^w)$ with genus g and n $GF(2^w)$ rational points and there are at least g $GF(2^{2w})$-rational points on*

X. Then we have $(2wn, g)$ vectorial $n-2g-1$)-resilient $SAC(n-2g-1)$ Boolean functions.

III. Conclusion

In this paper we presented a method for constructing vectorial t-resilient Boolean functions satisfying $PC(l)$ of order k functions with less than 100 variables. The number of variables, t, k, l can be chosen quite flexibly.

Acknowledgment. The work of the first author was supported by the Distinguished Young Scholar grant 10225106 and grant 90607005 of NSF China. The work of the second author is supported by Shanghai Leading Academic Discipline Project(No.T0502).

e-mail: chenhao@fudan.edu.cn

REFERENCES

[1] C.Carlet, On the propagation criterion of degree l and order k, Advances in Cryptology, Eurocrypt'98, LNCS 1403, pages 462-474.

[2] C.Carlet, Vectorial Boolean functions for cryptography, "Boolean Methods and Models" (Eds Y.Crama and P.Hammer), Cambridge Press.

[3] Jung Hee Cheon, Nonlinear vector Boolean functions, Advances in Cryptology, Crypto 2001, LNCS 2139, pages 458-469.

[4] A.Garcia and H.Stichtenoth, A tower of Artin-Schreier extension of function fields attaining Drinfeld-Vladut bound, Invent. Math., 121(1995), no.1, pages 211-222.

[5] A.Garcia and H.Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, J.Number Theory, 61, pages 248-273, 1996.

[6] M.Grassl, W.Geiselmann and T.Beth, Quantum Reed-Solomon codes, in Proc. AAECC 13, LNCS 1719, eds., M. Fossoreier, H.Imai, S.Lin and

A.Poli, Springer-Verlag, pages 231-244, 1996.

[7] T.Johansson and E.Pasalic, A construction of resilient functions with high nonlinearity, IEEE Trans. Inf. Theory, vol. 49(2002), no. 2, pages. 494-501, Feb.2000.

[8] K.Kurosawa and T.Satoh, Design of SAC/PC(l) of order k Boolean functions and three other cryptographic criteria, Advances in Cryptology, Eurocrypt,97, LNCS 133, pages 434-449.

[9] R.Matsumoto, K.Kurosawa, T.Itoh,T.Konno and T.Uyematsu, Primal-dual distance bounds of linear codes with applications to cryptography, Cryptology e-print 194/2005, to appear in IEEE Trans. Inf. Theory.

[10] W.Meier and O.Staffelbach, Nonlinearity criteria for cryptographic functions, Advances in Cryptology, Eurocrypt'89, LNCS 434, pages 549-562.

[11] B.Preneel, R.Govaerts and J.Vandevalle, Boolean functions satisfying high order propagation criteria, Advances in Cryptology, EuroCrypto'90, LNCS 473, pages 161-173.

[12] H.Stichtenoth, Algebraic function fields and codes, Springer, Berlin, 1993.

[13] M.A.Tsfasman and S.G.Vladut, Algebraic-geometric codes, Kluwer, Dordrecht, 1991

[14] G. van der Geer and M. van der Vludgt, Tables of curves with many points, [Online] Available: http://www.science.uva.nl/∼geer/.

[15] J.H.van Lint, Introduction to coding theory (3rd Edition), Springer-Verlag, 1999.

[16] A.Webster and S.Tavares, On the design of S-boxes, Advances in Cryptology, Crypto'85, LNCS 218, pages 523-534.