Chin. Ann. Math.
32B(1), 2011, 99–104
DOI: 10.1007/s11401-010-0621-4

Chinese Annals of Mathematics, Series B

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

Hao CHEN[1] Liang MA[2] Jianhua LI[3]

Abstract Propagation criteria and resiliency of vectorial Boolean functions are important for cryptographic purpose (see [1–4, 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 this paper, the algebraic-geometric codes over GF(2^m) are used to modify the Carlet and Kurosawa-Satoh's construction for giving vectorial resilient Boolean functions satisfying PC(l) of order k criterion. This new construction is compared with previously known results.

Keywords Cryptography, Boolean function, Algebraic-geometric code
2000 MR Subject Classification 94B05

1 Introduction

In cryptography, vectorial Boolean functions are used in many applications (see [2, 3]). Propagation criterion of degree l and order k is one of the most general properties of Boolean functions, which has to be satisfied for cryptographic purpose. It was introduced in Preneel et al [11], which extends the property strictly avalanche criterion SAC in [16]. The weight of a Boolean function f of n variables is the number of vectors in $v \in \mathrm{GF}(2)^n$ such that $f(v) = 1$. A Boolean function f of n variables is called balanced if $\mathrm{wt}(f) = 2^{n-1}$. For a Boolean function $f(x) = (x_1, \cdots, x_n)$ 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 $1 \le \mathrm{wt}(\alpha) \le l$. When the function obtained from f by keeping any k variables fixed satisfies PC(l), we say that f has the property PC(l) of order k. For a vectorial Boolean function $\mathbf{f} = (f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n))$ it is called $(n, m)-$PC(l) of order k if any nonzero linear combination of $f_1, \cdots, f_m$ satisfies PC(l) of order k. We say that $\mathbf{f}$ satisfies SAC(k) if it has PC(1) of order k property. A Boolean function f of n variables is called k-resilient if it is balanced and $\mathrm{wt}(f') = \frac{\mathrm{wt}(f)}{2^k}$ where f' is the $n-k$ variable Boolean function obtained from f by substituting constants for any k variables in $f(x_1, \cdots, x_n)$. A vectorial Boolean function $\mathbf{f} = (f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n))$ is called k-resilient, if any nonzero linear combination $\sum_i a_i f_i$ is a k-resilient Boolean function. Resiliency of vectorial Boolean functions are relevant to quantum key distribution and pseudo-random sequence generators for stream ciphers (see [1–4, 17]).

Manuscript received February 13, 2009. Revised May 12, 2010. Published online December 28, 2010.
[1]Software Engineering Institute, East China Normal University, Shanghai 200062, China.
E-mail: haochen@sei.ecnu.edu.cn
[2]Institute of Systems Science, University of Shanghai for Science and Technology, Shanghai 200093, China.
[3]Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200030, China.
*Project supported by the National Natural Science Foundation of China (No. 10871068), the joint grant of the Danish National Research Foundation and the National Natural Science Foundation of China and the Shanghai Leading Academic Discipline Project (No. S30504).

We recall the Maiorana-MacFarland construction of vectorial Boolean functions. Let $\phi_i : \mathrm{GF}(2)^s \to \mathrm{GF}(2)^r$ be vectorial Boolean functions for $i = 1, \cdots, m$, the class of Maiorana-MacFarland $(r+s, m)$ Boolean functions is the set of the functions $F(x, y)$ of the form $F(x, y) = (x \cdot \phi_1(y) + h_1(y), \cdots, x \cdot \phi_m(y) + h_m(y)) : \mathrm{GF}(2)^{r+s} \to \mathrm{GF}(2)^m, (x, y) \in \mathrm{GF}(2)^r \times \mathrm{GF}(2)^s$, where $h_1, \cdots, h_m$ are Boolean functions of s variables. It is well-known that $F(x, y)$ is at least t-resilient if $a_1\phi_1(y) + \cdots + a_m\phi_m(y)$, for any nonzero $(a_1, \cdots, a_m) \in \mathrm{GF}(2)^m$ and any $y \in \mathrm{GF}(2)^s$, has its Hamming weight at least $t + 1$ (see [1–3]).

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 $\mathrm{GF}(2)$ and v_i is a fixed vector in $\mathrm{GF}(2)^r$ for $i = 1, \cdots, m$.

$\mathrm{PC}(n)$ Boolean functions of n variables are just the perfect nonlinear functions introduced by Meier and Staffebach [10]. They exist only when n is even. Bent functions are the examples of this kind of functions (see [10, 16]). People only have few constructions of $\mathrm{PC}(l)$ of order k Boolean functions. In [1, 8], $\mathrm{PC}(l)$ of order k (vectorial) Boolean functions were constructed from binary linear or nonlinear codes. For satisfying the conditions of the construction 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 variable number in the Kurosawa-Satoh construction) of these binary linear codes were studied in [9].

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

Theorem 1.1 (Kurosawa-Satoh Theorem) (see [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 $s+t$ variables satisfying $\mathrm{PC}(l)$ of order k can be explicitly given.*

Corollary 1.1 (see [8, 9]) *Let C be a linear binary code with length n, minimum distance at least $k+1$ and dual distance at least $l+1$. Then Boolean functions of $2n$ variables satisfying $\mathrm{PC}(l)$ of order k can be explicitly given.*

Theorem 1.2 (Carlet Theorem) (see [1]) *For a Boolean function $f(x, y) = x \cdot \phi(y) + g(y)$ from $\mathrm{GF}(2)^{r+s}$ to $\mathrm{GF}(2)$, where ϕ and g are (vectorial) Boolean functions of the forms $\phi : \mathrm{GF}(2)^s \to \mathrm{GF}(2)^r$ and $g : \mathrm{GF}(2)^s \to \mathrm{GF}(2)$, f satisfies $\mathrm{PC}(l)$ of order k if the following two conditions are satisfied:*

(1) *the sum of at least 1 and at most l coordinates of ϕ is k-resilient;*

(2) *if $b \in \mathrm{GF}(2)^s$ 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.*

Let us now recall some basic facts about AG-codes (algebraic-geometric codes, see [12–14]). Let X be an absolutely irreducible, projective and smooth curve defined over $\mathrm{GF}(q)$ with genus g, $P = \{P_1, \cdots, P_n\}$ be a set of $\mathrm{GF}(q)$-rational points of X, and G be a $\mathrm{GF}(q)$-rational divisor satisfying $\mathrm{supp}(G) \cap P = \emptyset$, $2g - 2 < \deg(G) < n$. Let $L(G) = \{f : (f) + G \geq 0\}$ be the linear space (over $\mathrm{GF}(q)$) of rational functions associated with the divisor G, and $\Omega(B) = \{\omega : (\omega) \geq B\}$ be the linear space of differentials associated with the divisor B. Then the functional AG-code $C_L(P, G) \subset \mathrm{GF}(q)^n$ and residual AG-code $C_\Omega(P, G) \subset \mathrm{GF}(q)^n$ can be defined (see [12]). $C_L(D, G)$ is a linear $[n, k = \deg(G) - g + 1, d \geq n - \deg(G)]$ code over $\mathrm{GF}(q)$ and $C_\Omega(P, G)$ is a linear $[n, k = n - \deg(G) + g - 1, d \geq \deg(G) - 2g + 2]$ code over $\mathrm{GF}(q)$. We know that the functional code is just the evaluations of functions in $L(G)$ at the points in P and the residual code is just the residues of differentials in $\Omega(G - P)$ at the points in P.

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

From the theory of algebraic curves over finite fields, there exist algebraic curves $\{X_t\}$

defined over $\mathrm{GF}(q^2)$ with the property $\lim \frac{N(X_t)}{g(X_t)} = q-1$ (Drinfeld-Vladut bound) (see [5, 13]), where $N(X_t)$ is the number of $\mathrm{GF}(q^2)$ rational points on the curve X_t and $g(X_t)$ is the genus of the curve X_t. Actually for this family of curves $N(X_t) \geq (q-1)q^t + 1$, $g(X_t) = q^t - 2q^{\frac{t}{2}} + 1$ for t even and $g(X_t) = q^t - q^{\frac{t+1}{2}} - q^{\frac{t-1}{2}} + 1$ for t odd (see [5]).

For an AG-code over $\mathrm{GF}(2^m)$, its expansion to some base B of $\mathrm{GF}(2^m)$ over $\mathrm{GF}(2)$ will be used in our construction. Let $\{e_1, \cdots, e_m\}$ be a base of $\mathrm{GF}(2^m)$ as a linear space over $\mathrm{GF}(2)$. For an $[n, k, d]$ linear code $C \subseteq \mathrm{GF}(2^m)^n$, the expansion with respect to the base B is a binary linear code $B(C) \subseteq \mathrm{GF}(2)^{mn}$ consisting of all codewords $B(x) = (B(x_1), \cdots, B(x_n)), x = (x_1, \cdots, x_n) \in C$. Here $B(x_i)$ is a length m binary vector $(x_i^1, \cdots, x_i^m)$, where $x_i = \sum_{j=1}^{m} x_i^j e_j \in \mathrm{GF}(2^m)$. 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 $\mathrm{GF}(2^m)$ of characteristic 2. The following result is useful in our construction.

Proposition 1.1 (see [6]) *Let B be a self-dual base of $\mathrm{GF}(2^m)$ over $\mathrm{GF}(2)$ and C be a linear code over $\mathrm{GF}(2^m)$. 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 are 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 $U_1, \cdots, U_m$ be divisors on the curve X, set $\max\{U_1, \cdots, U_m\}$ the smallest divisor U such that $U - U_i$ is effective for all $i = 1, \cdots, m$. It is clear that the linear span of $L(U_1), \cdots, L(U_m)$ is in $L(\max\{U_1, \cdots, U_m\})$. The following lemma is useful in our construction.

Lemma 1.1 (1) *Let X be an absolutely irreducible, projective and smooth curve defined over $\mathrm{GF}(q)$ with genus g, $G = G' - G''$ and $H = H' - H''$ be two $\mathrm{GF}(q)$ rational divisors on X, where G', G'', H', H'' are nonzero effective divisors satisfying $\mathrm{supp}(G') \cap \mathrm{supp}(G'') = \emptyset$ and $\mathrm{supp}(H') \cap \mathrm{supp}(H'') = \emptyset$. Suppose $\mathrm{supp}(G) \cap \mathrm{supp}(H) = \emptyset$. Then $L(G) \cap L(H) = 0$.*

(2) *For any positive integer t and any set P of points on X, there exists a $\mathrm{GF}(q)$ rational divisor G of degree t with the form $G = G' - G''$, where G' and G'' are $\mathrm{GF}(q)$ rational effective divisors, such that $\mathrm{supp}(G) \cap P = \emptyset$.*

Proof Let f be a function in $L(G) \cap L(H)$. Then f has no pole, since $\mathrm{supp}(G') \cap \mathrm{supp}(H') = \emptyset$. Thus f is a constant function. On the other hand, f has to be zero at G'' and H''. Thus $f = 0$. The first conclusion is proved.

The second conclusion follows from Weak Approximation Theorem directly (see [12]).

2 Main Results

The following Theorem 2.1 and Corollary 3.2 are the main results of this paper.

Theorem 2.1 *Let X (resp. X') be a projective, absolutely irreducible smooth curve of genus g (resp. g') defined over $\mathrm{GF}(2^w)$ (resp. $\mathrm{GF}(2^{w'})$), P (resp. P') be a set of n $\mathrm{GF}(2^w)$ (resp. n', $\mathrm{GF}(2^{w'})$) rational points on X (resp. X'), $U_1, \cdots, U_m$ (resp. $U_1', \cdots, U_m'$) be $\mathrm{GF}(2^w)$ (resp. $\mathrm{GF}(2^{w'})$) rational divisors on X (resp. X') satisfying $2g - 2 < \deg(U_i) < n$, for $i = 1, \cdots, m$ and $\mathrm{supp}(\max\{U_1, \cdots, U_m\}) \cap P = \emptyset$ (resp. $2g' - 2 < \deg(\max\{U_i'\} < n'$, for $i = 1, \cdots, m$, $\mathrm{supp}(\max\{U_1', \cdots, U_m'\}) \cap P' = \emptyset$). Suppose that U_i and U_i' $(i = 1, \cdots, m)$ are divisors of the form $T_1 - T_2$ where T_1 and T_2 are nonzero effective rational divisors satisfying $\mathrm{supp}(T_1) \cap \mathrm{supp}(T_2) = \emptyset$. We also assume $w(\deg(U_i) - g + 1) = w'(\deg(U_i') - g' + 1)$ for $i = 1, \cdots, m$. H is another $\mathrm{GF}(2^{w'})$-rational divisor on X' satisfying $\deg(H) + \deg(\max\{U_1', \cdots, U_m'\}) < n'$ and $w'(\deg(H) - g' + 1) \geq m$. Suppose that H is of the form $H_1 - H_2$ where H_1 and H_2 are effective rational divisors. It is assumed that $U_1, \cdots, U_m$ and $U_1', \cdots, U_m', H$ are disjoint divisors (that is, their supports are disjoint). Then we have $(wn + w'n', m)$ vectorial t-resilient $\mathrm{PC}(l)$ of order*

k Boolean functions with $wn + w'n'$ variables, where

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

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 linear codes $D_1^i = C_L(P, U_i),\ D_2^i = C_L(P', U'_i)$. Then $(D_1^i)^\perp = C_\Omega(P, U_i),\ (D_2^i)^\perp = C_\Omega(P', U'_i)$. Let B and B' be the self dual bases of GF(2^w) and GF($2^{w'}$ over GF(2). We use the linear binary codes $C_1^i = B(D_1^i),\ C_2^i = B'(D_2^i)$. From Proposition 1.1, we have $(C_1^i)^\perp = B(C_\Omega(P, U_i)),\ (C_2^i)^\perp = B'(C_\Omega(P', U'_i))$. The code parameters of C_1^i and C_2^i are $[wn, w(\deg(U_i - g + 1), \geq n - \deg(U_i)]$ and $[w'n', m'(\deg(U'_i) - g' + 1), \geq n' - \deg(U'_i)]$. The code parameters of $(C_1^i)^\perp$ and $(C_2^i)^\perp$ are $[wn, w(n - \deg(U_i) + g - 1), \geq \deg(U_i) - 2g + 2]$ and $[w'n', w'(n' - \deg(U'_i) + g' - 1), \geq \deg(U'_i) - 2g' + 2]$.

Let Q_i and R_i be the generator matrices of the binary linear codes C_1^i and C_2^i respectively, for $i = 1, \cdots, m$. 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 $v_1, \cdots, v_m$ in the binary linear code $B(C_L(H, P'))$. Set $\phi_i(y) = (R_i)^\tau Q_i(y) + v_i,\ y \in \mathrm{GF}(2)^{wn}$ for $i = 1, \cdots, m$. In Maiorana-MacFarland construction, we get our $(wn + w'n', m)$ Boolean function $\mathbf{f} = (f_1, \cdots, f_m)$. Here ϕ_i's are mappings from GF$(2)^{wn}$ to GF$(2)^{w'n'}$. The image of ϕ_i is the coset $v_i + C_2^i$ for $i = 1, \cdots, m$.

For any nonzero linear combination $a_1 f_1 + \cdots + a_m f_m$, we set $\phi(y) = \sum\limits_i a_i\phi_i(y) + \sum\limits_i a_i v_i$. Then it is clear that $\sum\limits_i a_i\phi_i(y)$ is in the binary linear code $B'(C_L(P', \max\{U'_1, \cdots, U'_m\}))$ and $\sum\limits_i a_i v_i$ is in the binary linear code $B'(C_L(P', H))$. Because $\max\{U'_1, \cdots, U'_m\}$ and H are disjoint, $\sum\limits_i a_i\phi_i(y) + \sum\limits_i a_i v_i$ is not zero from Lemma 1.1. On the other hand, this is a nonzero code word in $B'(C_L(P', \max\{U'_1, \cdots, U'_m, H\}))$, its weight is at least $n' - \deg(\max\{U'_1, \cdots, U'_m, H\})$. Hence $\mathbf{f}$ is t-resilient.

From the above argument, it is also known that $\phi(y) = \sum\limits_i a_i\phi_i(y) + \sum\limits_i a_i v_i$ is in the coset of the binary linear code $B'(C_L(P', \max\{U'_1, \cdots, U'_m\}))$, for any $y \in \mathrm{GF}(2)^{wn}$. Thus the sum of arbitrary j (where, $1 \leq j \leq l$) coordinates $\gamma \cdot \phi(y)$ (here $\gamma \in \mathrm{GF}(2)^{w'n'}, 1 \leq \mathrm{wt}(\gamma) \leq l$) of this function $\phi(y)$ is a nonzero function, since l is less than the Hamming distance of the code $B'(C_\Omega(P', \max\{U'_1, \cdots, U'_m\})) = (B'(C_L(P', \max\{U'_1, \cdots, U'_m\})))^\perp$. On the other hand, $\gamma \cdot \phi(y)$ is of the form $u \cdot y + 1$ or $u \cdot y$ $\Big($depending on $\gamma \cdot \Big(\sum\limits_i a_i v_i\Big) = 1$ or $0\Big)$, where u is a nonzero codeword in $B(C_L(P, \max\{U_1, \cdots, U_m\}))$ with weight at least $k + 1$. Thus $\gamma \cdot \phi(y)$ is a k-resilient function. The 1st condition of the Carlet Theorem is satisfied.

For any $b \in \mathrm{GF}(2)^{wn}$, $\phi(y + b) + \phi(y) = \sum\limits_i a_i(R_i)^\tau Q_i b$. If b has its weight smaller than or equal to l, it is not in $B(C_\Omega(P, \max\{U_1, \cdots, U_m\}))$, thus $Q_i b$ can not be zero for all $i = 1, \cdots, m$. Thus at least one $(R_i)^\tau Q_i b$ is not zero. From the conditions on $U'_1, \cdots, U'_m$ and Lemma 1.1, we know that $\sum\limits_i a_i(R_i)^\tau Q_i b$ is a nonzero codeword in $B(C_L(P', \max\{U'_1, \cdots, U'_m\}))$. Thus $\phi(b)$ has its weight at least $k + 1$. The 2nd condition of the Carlet Theorem is satisfied. The conclusion is proved.

It is well-known that in the theory of algebraic curves over finite fields, there are many curves over GF(2^w) (see [12–14]) with various numbers of rational points and genuses. Thus when we use Theorem 2.1 for constructing vectorial t-resilient PC(l) of order k functions, we have very

flexible choices of parameters $l, k, wn + w'n'$. This is quite similar to the role of algebraic curves in the 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 $U_1, \cdots, U_m, U'_1, \cdots, U'_m, H$ need not to be the GF(2^w) (or GF($2^{w'}$)) rational points from Lemma 1.1. It is sufficient that the divisors are GF(2^w) (or GF($2^{w'}$) rational. Thus we can easily choose the sets P and P' of points and the divisors to construct vectorial resilient PC(l) of order k Boolean functions.

3 Constructions

In this section, some examples of vectorial t-resilient PC(l) of order k Boolean functions are constructed from Theorem 2.1. Comparing our constructions with the previously known PC(l) of order k functions in [1, 8], it seems that our constructed vectorial t-resilient PC(l) of order k functions are quite good.

When $X = X'$ is the genus g curve which is defined over GF(2^w), $\deg(U_i) = \deg(U'_i) = t$ ($i = 1, \cdots, m$) are m divisors with disjoint supports which are rational over GF(2^w) and satisfying the conditions in Theorem 2.1. From Lemma 1.1 we can find such divisors. 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. Set H another degree t' divisor which is GF(2^w)-rational divisor satisfying $2g-2 < \deg(H) < n$, $w(t'-g+1) \geq m$ and the conditions in Theorem 2.1 (from Lemma 1.1). Moreover it is assumed that its support is the set of GF(2^{2w})-rational points and disjoint to the supports of $U_1, \cdots, U_m$ from Lemma 1.1. In this construction, we have $(2wn, m)$ vectorial $(n - mt - t' - 1)$-resilient Boolean functions satisfying PC($mt - 2g + 1$) of order $n - mt - 1$.

Example 3.1 We use the 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 3.2 We use the genus 1 curve over GF(4) in the construction. Then $n \leq 9$ (see [12, 14]). We have $(4n, m)$ vectorial $(n-mt-t'-1)$-resilient PC($mt-1$) of order $n-mt-1$ Boolean functions, where $2t' \geq m$. Thus $(36, 4)$ vectorial PC(7) Boolean functions are constructed, $(36, 3)$ vectorial PC(5) of order 1 Boolean functions are constructed, $(24, 2)$ vectorial PC(3) of order 1 Boolean functions are constructed.

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

Example 3.3 We use the genus 4 curve over GF(4) in the construction. Then $n \leq 15$ (see [14]). Suppose $t > 6,\ t' > 6$, then $(4n, m)$ vectorial $(n - mt - t' - 1)$-resilient PC($mt - 7$) of order $n - mt - 1$ Boolean functions are constructed, where $2(t' - 3) \geq m$. Thus we have $(60, 2)$ vectorial PC(7) Boolean functions.

Example 3.4 We use the Klein quartic X, an algebraic curve over GF(8) of genus 3, then $n \leq 24$. Suppose $t > 4, t' > 4$, from the construction $(6n, m)$ vectorial $(n-mt-t'-1)$-resilient PC($mt-5$) of order $n-mt-1$, Boolean functions are constructed for $n = 7, 8, \cdots, 24$, where $3(t'-2) \geq m$. Thus we have $(96, 3)$ vectorial PC(10) Boolean functions. When $n = 16, \cdots, 24$, we have $(6n, 3)$ vectorial $(n-21)$-resilient PC(10) of order $n-16$ Boolean functions.

Corollary 3.1 *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* $2g$ GF(2^{2w})*-rational points on X. Then we have* $(2wn, g)$ *vectorial* $(n - \lceil \frac{7g}{2} \rceil - 1)$*-resilient* SAC($n - 2g - 1$) *Boolean functions.*

Applying Theorem 2.1 to Garcia-Stichtenoth curves [5] over GF(2^{2w}), we have the following result.

Corollary 3.2 *For positive integers $w \geq 2$ and $h \geq 1$, we have* $(4wn, m)$ *vectorial Boolean*

functions satisfying $\mathrm{PC}(mt-2^{2wh+1}+1)$ *of order* $(n-mt-1)$ *for* m *and* n *satisfying* $2^{2wh+1}+1 \leq n \leq (2^w-1)2^{2wh}$ *and* $m \leq n$.

Comparing with the constructions in [1, 8], we can see that our method based on AG-codes offers more flexibilities for the parameters $wn + w'n', m, t, k$ and l. The main result is more suitable for constructing vectorial resilient Boolean functions satisfying propagation criteria, because there are many $\mathrm{GF}(2^w)$-rational divisors on the algebraic curves.

4 Conclusion

In this paper, we present a method based on AG-codes for constructing (n, m) vectorial t-resilient Boolean functions satisfying $\mathrm{PC}(l)$ of order k functions. The parameters n, m, t, k and l in our constructions can be chosen quite flexibly. Many such functions of less than 100 variables have been given in our examples. The constructed Boolean functions in our paper can be given explicitly and simply implemented.

Acknowledgement The authors are grateful to the anonymous referees for their helpful comments.

References

[1] Carlet, C., On the propagation criterion of degree l and order k, Advances in Cryptology, Lecture Notes in Computer Science, **1403**, Springer-Verlag, Berlin, Heidelberg, New York, 1998, 462–474.

[2] Carlet, C., Boolean Functions for Cryptography and Error Correcting Codes, Boolean Methods and Models, Y. Crama and P. Hammer (eds.), Cambridge University Press, Cambridge, 2010, in press.

[3] Carlet, C., Vectorial Boolean functions for cryptography, Boolean Methods and Models, Y. Crama and P. Hammer (eds.), Cambridge University Press, Cambridge, to appear.

[4] Cheon, J. H., Nonlinear vector Boolean functions, Advances in Cryptology, Lecture Notes in Computer Science, **2139**, Springer- Verlag, Berlin, Heidelberg, New York, 2001, 458–469.

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

[6] Grassl, M., Geiselmann, W. and Beth, T., Quantum Reed-Solomon codes, Proc. AAECC 13, Lecture Notes in Computer Science, **1719**, M. Fossoreier, H. Imai, S. Lin and A. Poli (eds.), Springer-Verlag, New York, 1996, 231–244.

[7] Johansson, T. and Pasalic, E., A construction of resilient functions with high nonlinearity, *IEEE Trans. Inf. Theory*, **49**(2), 2002, 494–501.

[8] Kurosawa, K. and Satoh, T., Design of SAC/PC(l) of order k Boolean functions and three other cryptographic criteria, Advances in Cryptology, Lecture Notes in Computer Science, **1233**, Springer-Verlag, Berlin, Heidelberg, New York, 1997, 434–449.

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

[10] Meier, W. and Staffelbach, O., Nonlinearity criteria for cryptographic functions, Advances in Cryptology, Lecture Notes in Computer Science, **434**, Springer-Verlag, Berlin, Heidelberg, New York, 1989, 549–562.

[11] Preneel, B., Govaerts, R. and Vandevalle, J., Boolean functions satisfying high order propagation criteria, Advances in Cryptology, Lecture Notes in Computer Science, **473**, Springer-Verlag, Berlin, Heidelberg, New York, 1990, 161–173.

[12] Stichtenoth, H., Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.

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

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

[15] van Lint, J. H., Introduction to coding theory, 3rd ed., Springer-Verlag, Berlin, 1999.

[16] Webster, A. and Tavares, S., On the design of S-boxes, Advances in Cryptology, Lecture Notes in Computer Science, **218**, Springer-Verlag, Berlin, Heidelberg, New York, 1985, 523–534.

[17] Zhang, X. M. and Zheng, Y., Cryptographically resilient functions, *IEEE Transactions on Information Theory*, **43**(5), 1997, 1740–1747.