Constructing $PC(l)$ of order k Boolean Functions from Algebraic-Geometric 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

May.2006

Abstract

Propagation criterion of degree l and order k ($PC(l)$ of order k) for Boolean functions is important for the design of block ciphers. In [1-2] Kurosawa , Stoh and Carlet give several constructions of Boolean functions satisfying $PC(l)$ of order k from binary linear or nonlinear codes.

Matsumoto, Kurosawa and Itoh get some lower bounds and an non-constructive upper bound on the input length the Boolean functions in Kurosawa-Satoh construction. In this paper, algebraic-geometric codes over $GF(2^m)$ are inserted in Kurosawa-Satoh construction for giving explicit constructions of Boolean functions satisfying $PC(l)$ of order k by this AG-construction. This method give some constructive upper bound on the minimum input length of Boolean functions satisfying $PC(l)$ of order k in Kurosawa-Satoh construction.

Index Terms—Cryptography, block cipher, Boolean functions, algebraic-geometric codes, Garcia-Stichtenoth curves

I. Introduction and Preliminaries

In cryptography bolck ciphers are used in many applications. 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 is introduced in Preneel et al [4], which extends the property strictly avalanche criterion SAC in [5]. For a Boolean function $f(x) = (x_1, ..., x_n)$ of n inputs, set $\frac{Df}{D\alpha} = f(x) + f(x + \alpha)$, f satisfies $PC(l)$ of degree 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 inputs fixed satisfies $PC(l)$, we say f have the property $PC(l)$ of order k. It is known that $PC(n)$ Boolean functions of n inputs are just the perfect nonlinear functions introduced by W.Meier and O.Staffebach [6]. They exist only when n is even. Bent functions are example of this kind of functions (see [2,6]). People only have few constructions of $PC(l)$ of order k Boolean functions. In [1-2] $PC(l)$ of order k Boolean functions are 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 of the binary linear codes with their minimum distance and dual distance specified are proved in [3]. They also give a non-constructive upper bound by Gilbert-Varshamov type argument in [3]. Algebraic-geometric codes are well-known for their dual distances are lower bounded by Goppa bound. Thus it is natural to use algebraic-geometric codes in Kurosawa-Satoh construction for giving $PC(l)$ of order k Boolean functions.

From [1] we know the following result.

Kurosawa-Satoh Theorem (see [1]) *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 (see [1] and [3]) *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.*

We also need recall some basic facts about algebraic-geometric codes (see [7],[8] and [9]). Let $\mathbf{X}$ be an absolutely irreducible, projective and smooth curve defined over $GF(q)$ with genus g, $\mathbf{D} = \{P_1, ...P_n\}$ be a set of $GF(q)$-rational points of $\mathbf{X}$ and $\mathbf{G}$ be a $GF(q)$-rational divisor satisfying $supp(\mathbf{G}) \bigcap \mathbf{D} =$, $2g - 2 < deg(\mathbf{G}) < n$. 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 $\mathbf{C_L}(\mathbf{D}, \mathbf{G}) \in GF(q)^n$ and residual AG(algebraic-geometric) code $\mathbf{C_\Omega}(\mathbf{D}, \mathbf{G}) \in GF(q)^n$ are defined. $\mathbf{C_L}(\mathbf{D}, \mathbf{G})$ is a $[n, k = deg(\mathbf{G}) - g + 1, d \geq n - deg(\mathbf{G})]$ code over $GF(q)$ and $\mathbf{C_\Omega}(\mathbf{D}, \mathbf{G})$ is a $[n, k = n - deg(\mathbf{G}) + g - 1, d \geq deg(\mathbf{G}) - 2g + 2]$ code over $GF(q)$. We know that the functional code is just the evaluations of functions in $L(G)$ at the set $\mathbf{D}$ and the residual code is just the residues of differentials in $\Omega(G - D)$ at the set $\mathbf{D}$ (see [7-9]).

We also know that $\mathbf{C_L}(\mathbf{D}, \mathbf{G})$ and $\mathbf{C_\Omega}(\mathbf{D}, \mathbf{G})$ 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[18]) we have $\mathbf{C_\Omega}(\mathbf{D}, \mathbf{G}) = \mathbf{C_L}(\mathbf{D}, \mathbf{D} - \mathbf{G} + (\eta))$, 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 $\mathbf{G} = \mathbf{D} - \mathbf{G} + (\eta)$, then $\mathbf{C_L}(\mathbf{P}, \mathbf{G}) = \mathbf{C_\Omega}(\mathbf{P}, \mathbf{G}) = \mathbf{C_L}(\mathbf{P}, \mathbf{P} - \mathbf{G} + (\eta))$ is a self-dual code over $GF(q)$. For many examples of AG codes, including these self-dual AG-codes, we refer to [7],[8] and [9].

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 [10-11]), where $N(X_t)$ is the number of $GF(q^2)$ rational points on the curve X_t and $g(X_t)$ is genus of the curve X_t. Actually for this family of curve we have $N(X_t) \leq (q-1)q^t+1$ and $g(X_t) = q^t - 2q^{\frac{t}{2}} + 1$ for t even and $g(X_t) = q^t - q^{\frac{t+1}{2}} - q^{\frac{t-1}{2}} + 1$ for t odd (see [10-11]).

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 code $C \subseteq GF(2^m)^n$, 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 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 [11]). *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 $B(C^\perp)$.*

II Main Result and Constructions

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

Theorem 1. *Let $\mathbf{X}$ (resp. $\mathbf{X}'$) be a projective, absolutely irreducible smooth curve of genus g (resp. g') defined over $GF(2^m)$ (resp. $GF(2^{m'})$). We denote $N(X)$(resp. $N(X')$) the number of $GF(2^m)$(resp. $GF(2^{m'})$) rational points on $\mathbf{X}$(resp. $\mathbf{X}'$). Let $\mathbf{P}$ (resp. $\mathbf{P}'$) be a set of n $GF(2^m)$(resp. n', $GF(2^{m'})$) rational points on $\mathbf{X}$(resp. $\mathbf{X}'$), G(resp. G') a $GF(2^m)$(resp. $GF(2^{m'})$) divisor on $\mathbf{X}$(resp. $\mathbf{X}'$) with degree satisfying $2g-2 < deg(G) < n$ and $supp(G) \bigcap \mathbf{P} = \emptyset$ (resp. $2g'-2 < deg(G') < n'$, $supp(G') \bigcap \mathbf{P}' = \emptyset$). Then we have $PC(l)$ of order k Boolean functions with $mn+m'n'$ bits inputs, where*

$$\begin{matrix} l = min\{deg(G) - 2g + 1, deg(G') - 2g' + 1\} \\ k = min\{n - deg(G) - 1, n' - deg(G') - 1\} \end{matrix} \quad (1)$$

. If the curves and the bases of the linear space $L(G), \Omega(G)$ (resp. $L(G'), \Omega(G')$) are explicitly given, the $PC(l)$ of order k Boolean functions can be explicitly given.

Let $N(d, d')$ be the minimum length of the linear binary codes with its minimum distance at least d and dual distance at least d' (see [3]), it is clear that the minimum input length $W(l, k)$ of $PC(l)$ of order k Boolean functions, where $l = d' - 1, k = d - 1$ in Kurosawa-Satoh construction can achieve $W(l, k) \leq 2N(k + 1, t + 1)$. We have the following constructive upper bound for $N(d, d')$ by combining Kurosawa-Satoh construction and the curve family given in [10] attaining Drinfeld-Vladut bound.

Corollary 2.*Let m be an arbitrary positive integer greater than 2. Then for any positive integers i and k, t satisfying $2^{mi+1} - 2^{\frac{mi}{2}+2} < k < t \leq (2^m - 1)2^{mi}$, we have $N(t - k, k - 2^{mi+1} + 2^{\frac{mi}{2}+2}) \leq 2mt$ and $W(k - 2^{mi+1} + 2^{\frac{mi}{2}+2} - 1, t - k - 1) \leq 4mt$.*

Proof of Theorem 1. We consider the $C_1' = C_L(P, G), C_2' = C_L(P', G')$, then $C_1'^{\perp} = C_\Omega(P, G), C_2'^{\perp} = C_\Omega(P'G')$. Let B and B' be self dual bases of $GF(2^m)$ and $GF(2^{m'}$ over $GF(2)$. Consider the linear binary codes $C_1 = B(C_1'), C_2 = B'(C_2')$, from Proposition 1 $C_1^{\perp} = B(C_\Omega(P, G)), C_2^{\perp} = B'(C_\Omega(P'G'))$. The code parameters of C_1 and C_2 are $[mn, m(deg(G - g + 1), n - deg(G)]$ and $[m'n', m'(deg(G') - g + 1), n' - deg(G')]$. The code parameters of $C_1^{\perp}$ and $C_2^{\perp}$ are $[mn, m(n - deg(G) + g - 1), deg(G) - 2g + 2]$ and $[m'n', m'(n' - deg(G') + g' - 1, deg(G') - 2g' + 2]$. From Kurosawa-Satoh Theorem the conclusion is proved.

Proof of Corollary 2. By using the curve family of Garcia-Stichtenoth described in section 1,we take $P = P'$ a set of t ($t \leq (2^m - 1)2^{mi}$) $GF(2^{2m})$ rational points, and $G = G'$ a $GF(2^{2m})$ rational divisor of $deg(G) = deg(G') = k$ .The conclusion is proved.

It is well-known in the theory of algebraic curves over finite fields, there are many curves over $GF(2^m)$ (see [13]) with various number of rational points and genus. Thus when we use Theorem 1for constructing $PC(l)$ of order k functions, we have very flexible choices of parameters on l, k and the input length $mn + m'n'$. This is quite similar to the role of AG-codes in the theory of error-correcting codes, algebraic-geometric method offer us $PC(l)$ of order k functions of $mn+m'n'$ inputs with very few restrictions on parameters.

In the following part we give some examples and compare our construction with the previously-known $PC(l)$ of order k functions in [1-2].

Example 1. We use the Reed-Solomon codes as AG-codes over genus 0 curve (over $GF(2^m)$) in the construction Theorem 1. We take $n = n' = 2^m$ a divisor of degree $deg(G) = deg(G') = t-1$. Then $l = t, k = 2^m - t$ and $mn + m'n' = m \cdot 2^{m+1}$, $PC(t)$ of order $2^m - t$ of $m \cdot 2^{m+1}$ inputs Boolean functions are constructed for each positive integer $m \geq 2$ and t satisfying $1 \leq t \leq 2^m - 1$. We have $PC(1)$ of order 3 with 16 inputs Boolean functions, $PC(2)$ of order 2 with 16 inputs Boolean functions, $PC(t)$ of order $8-t$ with 48 inputs Boolean functions for each $1 \leq t \leq 7$, etc. The cases of $m = 4, 5, 6, 7$ of various code lengths n are listed in the following Table 1.

Table 1 $PC(t)$ of order $n-t$ Boolean Functions of W Inputs

$n, d, d^{\perp}$	$m, t, n-t, W$
11,4,9	4,8,3,88
11,7,6	4,5,6,88
22,11,12	5,11,11,220
32,11,23	5,22,10,320
32,15,19	5,18,14,320
64,34,34	6,33,33,768
64,27,39	6,38,26,768
128,65,65	7,64,64,1792
128,50,80	7,79,49,1792
128,43,87	7,86,42,1792
128, 86,42,	7,41,85, 1792

Example 2. The AG-codes over a curve of genus 4 defined over $GF(4)$ is used in this example. From 13 it is known this curve have 15 $GF(4)$ rational points. Thus we have $n = n' = 14, deg(G) = deg(G') = 10, m = m' = 2$ in Theorem 1 and $PC(3)$ of order 3 Boolean functions with 56 inputs are constructed.

Example 3. We use AG-codes over elliptic curves (that is the genus g is 1) defined over $GF(8), GF(16), GF(32), GF(64), GF(128)$ in this example. From Table [13], we have such curves with $N = 14, 25, 44, 81, 150$ rational points. Thus we have AG-codes over $GF(2^m)$ with lengths $N - 1$ and distance $d = N - 1 - t$ and dual distance $d^\perp = t$, $PC(t)$ of order $N - 1 - t$ Boolean functions with $W = 2m(N-1)$ inputs are constructed. The resulted functions are summarized in the following Table II.

Table 2 $PC(t)$ of order $N - t - 3$ Boolean Functions of W Inputs

$n, d, d^\perp$	$m, t, N - t - 3, W$
13,7,6	3,5,6,78
24,18,6	4,5,17,112
24,5,19	4,4,18,112
43,20,23	5,22,19,430
80,40,40	6,39,39,768
149,89,60	7,59,88,1792

Example 4. The AG-codes over Klein quartic (defined over $GF(8)$) of genus $g = 3$ is used in this example. The Klein quartic have 24 $GF(8)$ rational points. We have $m = m' = 3$. The resulted $PC(t)$ of order k Boolean functions with W inputs are listed in the follow Table III.

Table 3 $PC(t)$ of order $18 - l$ Boolean Functions of W Inputs

$n, d, d^\perp$	$m, l, 18 - l, W$
23,9,11	3,10,8,138
23,18,2	3,1,17,138
23,5,15	3,14,4,138
23,10,10	3,9,9,138
23,2,18	3,17,1,138

Example 5. Let $\mathbf{X}$ be the genus 0 curve defined over $GF(8)$ and $\mathbf{X}'$ be the elliptic curve defined over $GF(8)$ of 14 $GF(8)$ rational points (see [13]), P be a set of 8 ration points on $\mathbf{X}$ and P' be a set of 13 rational points on $\mathbf{X}'$, $deg(G) = 4, deg(G') = 5$. From Theorem 1 we have $PC(4)$ of order 4 Boolean functions of 63 inputs.

Example 6. Hermitian curves are $C : y^q + y = x^{q+1}$ defined over $GF(q^2)$ with genus $g = \frac{q(q-2)}{2}$. There are $q^3 + 1$ $GF(q^2)$ rational points on C. Here we take $q = 2^m$. In Theorem 1, if we can find a algebraic curve such that $n - 2g \geq k + l$ it is obvious the linear binary codes needed in Theorem 1 can be constructed by the expansions of AG-codes over this curve. Thus if $q^3 - 2g = q^3 - q^2 + 2q > (q-1)^3 \geq k + l$, we have $PC(l)$ of order k Boolean functions from Hermitian codes. The input length of the constructed functions is at most $4\lceil log_2(k+l)\rceil((k+l)^{\frac{1}{3}} + 1)^3$. We have the following result.

Corollary 3. *For any positive integer l and k, we have $PC(l)$ of order k Boolean functions with $4\lceil log_2(k+l)\rceil((k+l)^{\frac{1}{3}} + 1)^3$ inputs.*

In Table 4 we summarize some Boolean functions from Hermitian curves, it is noted when k and l becomes large, we have to use some curves with high genus as Hermitian curves.

Table 4 $PC(t)$ of order $N - l - 48$ Boolean Functions of W Inputs

$n, d, d^{\perp}$	$m, l, 18 - l, W$
150,102,3	6,2,101,1800
150,17,134	6,86,16,1800
150,62,42	6,41,61,1800
200,53,101	6,100,52,2400
200,57,97	6,96,56,2400
250,102,102	6,101,101,3000
300,127,127	6,126,126,3600

From Corollary 2 we have the following constructive upper bound on the minimum input length of $PC(l)$ of order k Boolean functions.

Corollary 3. Corollary 3. *For any positive integer l and k, we have $PC(l)$ of order k Boolean functions with* $42 \cdot 8^{\lceil log_6(k+l) \rceil - 1}$ *inputs.*

Proof. We use the i-th member in Garcia-Stichtenoth curve family over $GF(q^2)$ for $q = 8$. We need $N - 1 - 2g \geq k + l$ in Theorem 1. Thus if we have $(q-3)q^i > (q-2)^i \geq k + l$, the desired AG-codes can be constructed on this curve. The conclusion follows directly from a simple computation.

Comparing the constructions of $PC(l)$ of order k Boolean functions in this paper with the lower bounds and non-constructive upper bounds in the Table of [3], we can some Boolean functions in our Tables are near the optimal possibility.

III Conclusion

We give constructive method for giving $PC(l)$ of order k functions explicitly from algebraic-geometric codes over various algebraic curves. The constructive upper bounds on the existence of $PC(l)$ of order k Boolean functions are proved and the method for giving the explicit form of these Boolean functions is suggested.

Acknowledgment: The work of the first author was supported by the Distinguished Young Scholar grant 10225106 and grant 60542006 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] K.Kurosawa and T.Satoh, Design of SAC/PC(l) of order k Boolean functions and three other cryptographic criteria, Advances in Cryptology, Eurocrypto,97, LNCS 133, pages 434-449

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

[3] R.Matsumoto, K.Kurosawa and T.Itoh, Primal-dual distance bounds of linear codes with applications to cryptography, arXiv:cs.IT/0506087, preprint 2005

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

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

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

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

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

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

[10] A.Garcia and H.Stichtenoth, A tower of Artin-Schreier extension of function fields attaining Drinfeld-Vladut bound, Invent. Math., 121(1995), no.1, pp211-222

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

[12] 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 1996, pages 231-244

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