<table>
<thead>
<tr>
<th>Title</th>
<th>Generalization of Steane's enlargement construction of quantum codes and applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Ling, San; Luo, Jinquan; Xing, Chaoping</td>
</tr>
<tr>
<td>Date</td>
<td>2010</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/7714">http://hdl.handle.net/10220/7714</a></td>
</tr>
<tr>
<td>Rights</td>
<td>© 2010 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: <a href="http://dx.doi.org/10.1109/TIT.2010.2050828">http://dx.doi.org/10.1109/TIT.2010.2050828</a></td>
</tr>
</tbody>
</table>
The work of J. Q. Luo is also partially supported by the NSF of Jiangsu Province under Grant BK2009182.

C. P. Xing is the corresponding author.

San Ling, Jinquan Luo and Chaoping Xing

II. ENLARGEMENT CONSTRUCTION

Before stating our results, we introduce some definitions and notations.

Let $q$ be a prime power and let $\mathbb{F}_q$ be the finite field of cardinality $q$. For $u \in \mathbb{F}_q^n$, denote by $wt_H(u)$ the Hamming weight of $u$. Now for $(u|v) \in \mathbb{F}_{q^2}^2$ with $u = (u_1, \cdots, u_n), v = (v_1, \cdots, v_n) \in \mathbb{F}_q^n$, define the symplectic weight by

$$wt_s(u|v) := \#\{i : u_i \neq 0 \text{ or } v_i \neq 0\}.$$ 

For two vectors $(u|v), (u'|v') \in \mathbb{F}_{q^2}^2$, define the symplectic inner product by

$$((u|v), (u'|v'))_s = u \cdot v' - u' \cdot v \in \mathbb{F}_q,$$

where $\cdot$ stands for the usual Euclidean inner product.

For a $q$-ary classical linear block code $C \subseteq \mathbb{F}_q^{2n}$, the symplectic dual code of $C$ is defined as

$$C^\perp_s = \{a \in \mathbb{F}_q^n \mid (a, b)_s = 0 \text{ for all } b \in C\}.$$ 

It is easy to verify that $C = (C^\perp_s)^\perp_s$.

A code $C \subseteq \mathbb{F}_q^{2n}$ is said self-orthogonal with respect to the symplectic inner product if $C \subseteq C^\perp_s$.

The following construction of quantum codes from classical block codes was presented by Ashikhmin and Knill in [2].

**Proposition 2.1:** If $C$ is a $q$-ary self-orthogonal $[2n, k]$ code with respect to the symplectic inner product, then there exists a $q$-ary $[[n, n-k, d]]$ quantum code with

$$d = wt_s(C^\perp_s \setminus C) = \min\{wt_s(v) \mid v \in C^\perp_s \setminus C\}.$$ 

In particular, if $C$ is a $q$-ary classical $[n, k, d]$-linear code which contains its Euclidean dual $C^\perp$, then it is easy to see that the code

$$C := \{(u|v) : u, v \in C^\perp\}$$

is self-orthogonal with respect to the symplectic inner product.

It is clear that the dimension of $C$ is $2n - 2k$. Thus, by Proposition 2.1, we obtain a $q$-ary $[[n, 2k-n, d]]$-quantum code.

The idea of Steane’s enlargement is to find a $q$-ary linear code $A$ that contains $B$ so that the dimension of the resulting quantum code is increased, while its distance remains unchanged. Steane worked out the enlargement construction only for the binary case [9], which is stated below.

**Proposition 2.2:** (see [9]) Given a classical binary error-correcting code $C_1$, of parameters $[n, k_1, d_1]$, which contains its Euclidean dual, and which can be enlarged to an $[n, k_2 > k_1 + 1, d_2]$-code $C_2$ (i.e., $C_1 \subseteq C_2$), a pure binary quantum code of parameters $[[n, k_1 + k_2 - n, \min(d_1, [3d_2/2])]]$ can be constructed.
Before generalizing Steane’s enlargement construction to the q-ary case, we need several lemmas.

Lemma 2.3: Let $C_1$ and $C_2$ be two q-ary linear codes satisfying $C_1 \subseteq C_2$. Let $G_1$, $(D_{G_1})$, $H_2$ and $(B_{H_2})$ be generator matrices of $C_1$, $C_2$, $C_2^S$ and $C_1^S$, respectively. Then $BD^T$ is invertible, where $T$ stands for transpose.

Proof: Note that both the sizes of $B$ and $D$ are $k \times n$, where $k$ is the difference between the dimensions of $C_2$ and $C_1$, and $n$ is the length of the codes. Thus, $BD^T$ is a square matrix of size $k$. The desired result is equivalent to the fact that the equation $BD^T x^T = 0$ has only the trivial solution. Suppose that this was false. Then there exists a nonzero vector $c \in F_q^k$ such that $BD^T c^T = 0$. Thus, $cD$ is a nonzero codeword of $C_2$, but not a codeword of $C_1$. This implies that $H_2(D^T c^T) = 0$ and $(B_{H_2}) (D^T c^T) \neq 0$. Hence, $BD^T c^T \neq 0$, a contradiction.

Lemma 2.4: Let $u, v$ be two vectors in $F_q^n$, then we have

$$q \cdot \text{wt}(u|v) = \text{wt}_H(u) + \text{wt}_H(v) + \sum_{\alpha \in F_q^*} \text{wt}_H(u + \alpha v).$$

Proof: Let $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$. It is sufficient to show that, for any $1 \leq i \leq n$, one has

$$q \cdot \text{wt}_s(u_i|v_i) = \text{wt}_H(u_i) + \text{wt}_H(v_i) + \sum_{\alpha \in F_q^*} \text{wt}_H(u_i + \alpha v_i).$$

(II.1)

We prove the above identity by considering the four cases.

(i) $u_i = v_i = 0$.

In this case, both sides of (II.1) are equal to 0.

(ii) $u_i = 0$ and $v_i \neq 0$.

The left hand side of (II.1) is clearly equal to $q$. The right hand side of (II.1) is $\text{wt}_H(v_i) + \sum_{\alpha \in F_q^*} \text{wt}_H(\alpha v_i)$ which is also equal to $q$.

(iii) $u_i \neq 0$ and $v_i = 0$.

The left hand side of (II.1) is clearly equal to $q$. The right hand side of (II.1) is $\text{wt}_H(u_i) + \sum_{\alpha \in F_q^*} \text{wt}_H(u_i) \alpha v_i$ which is also equal to $q$.

(iv) $u_i \neq 0$ and $v_i \neq 0$.

The left hand side of (II.1) is clearly equal to $q$. The right hand side of (II.1) is $2 + \sum_{\alpha \in F_q^*} \text{wt}_H(u_i + \alpha v_i)$. By the fact that $u_i + \alpha v_i = 0$ if and only if $c = -u_i/v_i$, i.e., $\text{wt}_H(u_i + \alpha v_i) = 1$ if and only if $c \in F^* \setminus \{u_i/v_i\}$, we get $\sum_{\alpha \in F_q^*} \text{wt}_H(u_i + \alpha v_i) = q - 2$. The identity (II.1) is also proved in this case.

This finishes the proof.

Lemma 2.5: For any monic polynomial $f(x)$ of degree $n$ over $F_q$, there exists a square matrix $A$ of size $n$ such that the characteristic polynomial of $A$ is equal to $f(x)$.

Proof: Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be any monic polynomial over $F_q$. Then the characteristic polynomial of the $n \times n$ square matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

is exactly $f(x)$.

Now we state the main result of this paper.

Theorem 2.6: Let $q$ be a prime power and let $C_1$ be a q-ary $[n, k_1, d_1]$-linear code which contains its Euclidean dual $C_1^S$. Suppose $C_1$ can be enlarged to an $[n, k_2, d_2]$-code $C_2$ with $k_2 > k_1 + 1$, i.e., $C_1 \subseteq C_2$. Then a pure q-ary quantum code of parameters $[n, k_1 + k_2 - n, \min\{d_1, ((1 + 1/q)d_2)\}]$ can be constructed.

Proof: Let $G_1$, $(D_{G_1})$, $H_2$ and $(B_{H_2})$ be generator matrices of $C_1$, $C_2$, $C_2^S$ and $C_1^S$, respectively. Let $C$ be the q-ary $[2n, k_1 + k_2]$-linear code with generator matrix

$$\begin{pmatrix} D & AD \\ G_1 & 0 \\ 0 & G_1 \end{pmatrix},$$

where $A$ is a $(k_2 - k_1) \times (k_2 - k_1)$ non-singular matrix with no eigenvalues in $F_q$ (Lemma 2.5 guarantees the existence of such a matrix). By Lemma 2.3, the matrix $BD^T$ is invertible. Thus, we can define a matrix $A := BD^T A^T (A^T)^{-1} (BD^T)^{-1}$.

Let $C^{+\times}$ be the symplectic dual of $C$. Then it is not difficult to verify that a generator matrix of $C^{+\times}$ is

$$\begin{pmatrix} \bar{A}B \\ H_2 & B \\ 0 & 0 \end{pmatrix}.$$

From the above generator matrix of $C^{+\times}$, we know that $C$ contains its symplectic dual $C^{+\times}$. Thus, by Proposition 2.1, there exists a q-ary $[[n, k_1 + k_2 - n, d]]$-quantum code with $d = \text{wt}_s(C(C^{+\times}))$.

It then remains to prove $d \geq \min\{d_1, [(1 + 1/q)d_2]\}$. It suffices to show that, for any nonzero $(u|v) \in C$, $\text{wt}_s(u|v) \geq \min\{d_1, [(1 + 1/q)d_2]\}$.

Assume that

$$(u|v) = (x, y, z) \begin{pmatrix} D & AD \\ G_1 & 0 \\ 0 & G_1 \end{pmatrix}$$

for some vectors $x, y$ and $z$. Then we have

$$u = xD + yG_1, \quad v = xAD + zG_1.$$

Case 1: $u = 0$. Then we have $x = 0$ and hence $v = zG_1$ is a nonzero codeword of $C_1$. Therefore, $\text{wt}_s(u|v) = \text{wt}_H(v) \geq d_1$.

Case 2: $v = 0$. The same argument gives that $\text{wt}_s(u|v) = \text{wt}_H(u) \geq d_1$.

Case 3: $\text{wt}_H(u) \geq d_1$. or $\text{wt}_H(v) \geq d_1$. In this case, it is clear that $\text{wt}_s(u|v) \geq d_1$.

Case 4: $0 < \text{wt}_H(u) < d_1$ and $0 < \text{wt}_H(v) < d_1$. In this case, both $u$ and $v$ are not codewords of $C_1$. This implies that $x \neq 0$. We claim that $u$ and $v$ are $F_q$-linearly independent. Suppose that this was false, then there exists a nonzero element $\beta \in F_q$ such that $u = \beta v$, i.e., $xD + yG_1 = \beta xAD + \beta zG_1$. This gives $(x(I - \beta A), y - \beta z) \in \mathbb{F}_q^2$. Therefore, we must have $x(I - \beta A) = 0$. This implies that $1/\beta$ is an eigenvalue of $A$, which contradicts the choice of $A$. 


Since both \( u \) and \( v \) are vectors of \( C_2 \), we have that \( \text{wt}_H(v) \geq d_2 \) and \( \text{wt}_H(u + \alpha v) \geq d_2 \) for all \( \alpha \in \mathbb{F}_q \). Now by Lemma 2.4, we have

\[
q \cdot \text{wt}_H(u)v = \text{wt}_H(u) + \text{wt}_H(v) + \sum_{\alpha \in \mathbb{F}_q} \text{wt}_H(u + \alpha v) \geq (q+1)d_2.
\]

The desired result follows.

### III. APPLICATION TO BCH CODES

From the previous section, we know that, to construct quantum codes from classical linear block codes, we need to find classical codes that contain their Euclidean duals. We can explore among some well-known codes from classical coding theory. In this section, we use classical BCH codes to construct quantum codes.

To apply the results of the previous section, we need to find classical BCH codes that contain their Euclidean duals. In [1], a sufficient condition for a classical BCH code to contain its Euclidean dual is given.

Let \( \text{BCH}(n, q; \delta) \) denote the \( q \)-ary narrow-sense BCH code of length \( n \) with designed distance \( \delta \).

Let \( x[m \text{ odd}] = \{ x \mid m \text{ is odd}, \}

Property 3.1: (see [1]) Let \( n \) be a positive integer co-prime to \( q \) and let \( m = \text{ord}_n(q) \) be the order of \( q \) modulo \( n \). Then

(i) if \( 2 \leq \delta \leq \delta_{\max} \), where

\[
\delta_{\max} := \left( \frac{n}{q^m - 1} \right) \left( q^{m/2} - 1 - (q - 2)[m \text{ odd}] \right),
\]

then \( \text{BCH}(n, q; \delta) \) contains its Euclidean dual \( \text{BCH}(n, q; \delta) = \);

(ii) if \( q^{m/2} < n \leq q^m - 1 \) and \( 2 \leq \delta \leq \min\{[nq^{m/2}]/(q^m - 1)\}, n \}, \) then the dimension of \( \text{BCH}(n, q; \delta) = n - m[\delta - 1](1 - q^{-1}) \).

By applying Proposition 3.1 and the construction in the paragraph after Proposition 2.1, we obtain a \( q \)-ary \( [n, k, \delta] \)-quantum code with \( k = n - 2m(\delta - 1)(1 - q^{-1}) \). This is one of the main results of [1] which is stated in [1, Theorem 19].

By applying our enlargement construction of Theorem 2.6, we can obtain a better quantum code.

**Theorem 3.2:** Let \( m = \text{ord}_n(q) \). Let \( n \) be in the range \( q^{m/2} < n \leq q^m - 1 \) and let \( \delta \) be in the range \( 2 \leq \delta \leq \delta_{\max} \), with

\[
\delta_{\max} = \frac{n}{q^m - 1} \left( q^{m/2} - 1 - (q - 2)[m \text{ odd}] \right),
\]

then there exists a quantum code with parameters

\([n, k, \geq \delta]_q\)

where

\[
k = n - m\left( \left( \delta - 1 \right) (1 - q^{-1}) \right) + \left( \left( \frac{q^\delta}{q + 1} \right) - 1 \right) (1 - q^{-1}) \).
\]

**Proof:** Proposition 3.1 implies that the \( q \)-ary narrow-sense BCH code \( C_1 := \text{BCH}(n, q; \delta) \) with parameters \([n, n - m(\delta - 1)(1 - q^{-1})], \geq \delta \) contains its Euclidean dual. By taking \( \delta' = \left( \frac{q^\delta}{q + 1} \right) \) and letting \( C_2 := \text{BCH}(n, q; \delta') \) be the narrow-sense \( q \)-ary BCH code with parameters \([n, n - m(\delta - 1)(1 - q^{-1})], \geq \delta' \), we obtain the desired result from Theorem 2.6.

### IV. APPLICATION TO ASYMPTOTIC BOUNDS

As in classical coding theory, asymptotical problems of quantum codes have been discussed in several papers (see, for example, [2], [3], [4], [6], [7]). We first recall some definitions and results from [7].

For a \( q \)-ary quantum code \( Q \), we denote by \( n(Q), K(Q), d(Q) \), and \( d(Q) \) the length, the dimension over \( C \), and the minimum distance of \( Q \), respectively. In this case, we say that \( Q \) is an \((n(Q), K(Q), d(Q))\)- or \([n(Q), q, d(Q)]\)-quantum code. Let \( U_q^Q \) be the set of ordered pairs \( (\delta, R) \in \mathbb{R}^2 \) for which there exists a family \( \{Q_i\}_{i=1}^\infty \) of \( q \)-ary quantum codes with \( n(Q_i) \to \infty \) and

\[
\delta = \lim_{i \to \infty} \frac{d(Q_i)}{n(Q_i)}, \quad R = \lim_{i \to \infty} \frac{\log_q K(Q_i)}{n(Q_i)},
\]

where \( \log_q \) denotes the logarithm to the base \( q \). The following description on the domain \( U_q^Q \) is given in [7].

**Proposition 4.1:** There exists a function \( \alpha_q^Q(\delta) \), \( \delta \in [0, 1] \), such that \( U_q^Q \) is the union of the domain

\[
\{(\delta, R) \in \mathbb{R}^2 : 0 \leq R < \alpha_q^Q(\delta), 0 \leq \delta \leq 1\}
\]

with some points on the boundary \( \alpha_q^Q(\delta) \). Moreover, \( \alpha_q^Q(0) = 1, \alpha_q^Q(\delta) = 0 \) for \( \delta \in [1/2, 1] \), and \( \alpha_q^Q(\delta) \) decreases on the interval \([0, 1]\).

Some upper bounds on the function \( \alpha_q^Q(\delta) \) were investigated in [3]. The first lower bound on \( \alpha_q^Q(\delta) \) was derived in [4] using algebraic geometry codes and later this bound was improved by Chen-Ling-Xing [6] and Matsumoto [8]. A very good existence lower bound for \( p \)-ary quantum codes was introduced by Ashikhmin and Knill [2]. It is called the quantum Gilbert-Varshamov bound, which is a benchmark for the function \( \alpha_q^Q(\delta) \). In [7], two lower bounds on \( q \)-ary quantum codes were derived from classical algebraic geometry codes and these two bounds improved the quantum Gilbert-Varshamov bound for square prime powers \( q \geq 19^2 \). In this section, we apply our enlargement construction to classical algebraic geometry codes again to obtain an improvement on these two algebraic geometry quantum bounds.

Before proceeding to the algebraic geometry bounds, we recall some background on classical algebraic geometry codes and a result on self-orthogonal algebraic geometry codes given in [11]. The reader may refer to [10], [12] for more details on algebraic geometry codes.

Let \( X/Q_q \) be an algebraic curve of genus \( g \). We denote by \( \mathbb{F}_q(X) \) the function field of \( X \). An element of \( \mathbb{F}_q(X) \) is called a function. We write \( \nu_p \) for the normalized discrete valuation corresponding to the point \( P \) of \( X/Q_q \).

For a divisor \( G \), we form the Riemann-Roch space

\[
\mathcal{L}(G) = \{ x \in \mathbb{F}_q(X) \setminus \{0\} : \text{div}(x) + G \geq 0 \} \cup \{0\}.
\]

Then \( \mathcal{L}(G) \) is a finite-dimensional vector space over \( \mathbb{F}_q \), and we denote its dimension by \( \ell(G) \). By the Riemann-Roch theorem we have
and equality holds if $\deg(G) = 2g - 1$.

Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a subset of $\mathcal{X}(\mathbb{F}_q)$.

Choose a divisor $G$ such that $\text{supp}(G) \cap \mathcal{P} = \emptyset$. Then $\nu_{P_i}(f) \geq 0$ for all $1 \leq i \leq n$ and any $f \in L(G)$.

Consider the map
\[
\phi : L(G) \to \mathbb{F}_q^n, \ f \mapsto (f(P_1), f(P_2), \ldots, f(P_n)).
\]
Then the image of $\phi$ forms a subspace of $\mathbb{F}_q^n$ that was defined as an algebraic geometry code by Goppa. The image of $\phi$ is denoted by $C_L(G; \mathcal{P})$. If $n$ is bigger than the degree of $G$, then $\phi$ is an embedding and the dimension $k$ of $C_L(G; \mathcal{P})$ is equal to $\ell(G)$. The Riemann-Roch theorem makes it possible to estimate the parameters of the code $C_L(G; \mathcal{P})$.

H. Stichtenoth showed in [11] that there exists a family of algebraic geometry codes achieving the TVZ bound that are equivalent to self-orthogonal codes. More precisely:

**Proposition 4.2**: Let $q$ be the square of a prime power. Then there exists a family $\{\mathcal{X}/\mathbb{F}_q\}$ of curves over $\mathbb{F}_q$ and a family of algebraic geometry codes $G(C; P)$ of length $n$ from the curves $\mathcal{X}/\mathbb{F}_q$ together with a family of vectors $v \in (\mathbb{F}_q^n)$ such that

(i) $vC(G; \mathcal{P})$ is self-orthogonal if its dimension is less than or equal to $n/2$; and $vC(G; \mathcal{P})$ contains its Euclidean dual if its dimension is bigger than or equal to $n/2$; 

(ii) the code $C(G; \mathcal{P})$ achieves the asymptotic TVZ bound, i.e.,
\[
\lim_{n \to \infty} \frac{\dim(C(G; \mathcal{P})) + d_H(C(G; \mathcal{P}))}{n} \geq 1 - \frac{1}{\sqrt{q} - 1}, 
\] 

where $d_H(\cdot)$ denotes the Hamming distance of a code.

We note that the curves $\mathcal{X}$ contain rational points other than those that are contained in $\mathcal{P}$. For instance, the rational points lying over the pole of $z$ of the rational function field $\mathbb{F}_q(z)$ do not belong to $\mathcal{P}$. See [11] for the details.

From Proposition 4.2 and the paragraph after Proposition 2.1, we can construct $q$-ary $[n, 2k - n, d]$-quantum codes with $k = \dim(C(G; \mathcal{P}))$ and $d = d_H(C(G; \mathcal{P}))$. If we let $d_{\lim_{n \to \infty}} d/n = \delta$, then, by the TVZ bound (IV.1), we obtain
\[
\alpha_q^Q(\delta) \geq 1 - 2\delta - \frac{2}{\sqrt{q} - 1}. \tag{IV.2}
\]

The bound (IV.2) was derived in [7] using algebraic geometry codes as well, but through a different approach. One notes that the bound (IV.2) beats the quantum Gilbert-Varshamov bound if $q \geq 19^2$ is an even power of a prime.

By using more careful analysis, the bound (IV.2) was further improved to the following in [7]
\[
\alpha_q^Q(\delta) \geq 1 - 2\delta - \frac{2}{\sqrt{q} - 1} + \log_q \left(1 + \frac{1}{q^3}\right). \tag{IV.3}
\]

Now we are ready to state and prove our main result of this section.

**Theorem 4.3**: Let $q$ be a prime power square, then one has
\[
\alpha_q^Q(\delta) \geq 1 - \left(2 - \frac{1}{q + 1}\right) \delta - \frac{2}{\sqrt{q} - 1}. \tag{IV.4}
\]

**Proof**: Let $C(G; \mathcal{P})$ be the algebraic geometry codes achieving the TVZ bound (IV.1) in Proposition 4.2 and let $v \in (\mathbb{F}_q^n)$ be a vector such that $vC(G; \mathcal{P})$ contains its Euclidean dual. Let $C_1 := vC(G; \mathcal{P})$, with parameters $[n, k_1, d_1]$. Choose a rational point $P$ outside of $\mathcal{P}$ (see paragraph after Proposition 4.2) and consider the code $C_2 := vC(G+rP; \mathcal{P})$, with parameters $[n, k_1 + r, d_1 - r]$ for some integer $r \geq 2$. Then it is clear that $C_1$ is a subspace of $C_2$. Moreover, $C_1$ contains its Euclidean dual if $k_1 \geq n/2$. Applying Theorem 2.6, we obtain a quantum code $[n, 2k_1 + r - n, \min\{d_1, (1 + 1/q)(d_1 - r)\}]$-code. By letting $r = \lfloor d_1/(q+1) \rfloor$ and letting $\lim_{n \to \infty} d_1/n = \delta$, we obtain the desired result from the bound (IV.1). $\blacksquare$

**References**


**Authors’ Biographies**

San Ling received the B.A. degree in mathematics from the University of Cambridge, Cambridge, U.K., in 1985 and the Ph.D. degree in mathematics from the University of California, Berkeley, in 1990.

Since April 2005, he has been a Professor with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Prior to that, he was with the Department of Mathematics, National University of Singapore. His research fields include arithmetic of modular curves and application of number theory to combinatorial designs, coding theory, cryptography and sequences.

Jinquan Luo was born in February 1980. He got his bachelor degree from Zhejiang University, China in July 2001 and Ph.D in January 2007 from Tsinghua University, China. He is now a lecturer in Yangzhou University, China.
February 2009 to February 2010, he was a research fellow at Nanyang Technological University, Singapore. His major research interests are coding theory, cryptology and number theory.

**Chaoping Xing** received his PhD degree in 1990 from University of Science and Technology of China. From 1990 to 1993 he was a lecturer and associate professor in the same university. He joined University of Essen, Germany as an Alexander von Humboldt fellow from 1993 to 1995. After this he spent most time in Institute of Information Processing, Austrian Academy of Sciences until 1998. From March of 1998 to November of 2007, he was working in National University of Singapore. Since December of 2007, he has been with Nanyang Technological University and currently is a full Professor. Dr. Xing has been working on the areas of algebraic curves over finite fields, coding theory, cryptography and quasi-Monte Carlo methods, etc.