Construction of Large Families of Pseudorandom Subsets of the Set $\{1, 2, \ldots, N\}$ Using Elliptic Curves

Zhixiong Chen[1], Li Xu[2], and Chenhuang Wu[1]
(Corresponding author: Zhixiong Chen)
Key Lab. of Applied Mathematics, Putian University, Putian, Fujian 351100, P.R.China[1]
Key Lab. of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian 350007, P.R.China[2]
(Email: {ptczx,wuchenhuang2008}@126.com, xuli@fjnu.edu.cn)
(Received Feb. 16, 2009; revised and accepted June 28 & Sep. 19, 2009)

Abstract

Pseudo-random subsets of the set $\{1, 2, \ldots, N\}$ have many applications in the fields of network security, cryptography and other security issues. Recently, Dartyge and Sárközy investigated the measures–the well distribution measure and the correlation measure of order k–of pseudorandomness of subsets of the set $\{1, 2, \ldots, N\}$, and they presented several constructive examples for subsets with strong pseudorandom properties when N is a prime number. In this article, we present a construction of pseudorandom subsets by using elliptic curves over finite fields and estimate their pseudorandom measures. Exponential sums play an important role in the proofs.

Keywords: Cryptography, pseudo-random subsets, elliptic curves

1 Introduction

Random subsets of the positive integers not exceeding a certain fixed integer N have many applications in the fields of network security, cryptography and other security issues. Many researchers find out that using random subsets can improve the efficiency and security performance in the key pre-distribution procedure, then propose key management and broadcasting authentication protocol in P2P, ad hoc network and wireless sensor network [1, 19]. Anonymous communication is one of important security methods to defense passive attacks in network. Random subsets can play an efficient role in constructing an anonymous path and avoid routing information being intercepted [21]. As we know random subsets can also be used to construct key exchange and private matching [20]. In particular, in stream ciphers random subsets of a finite field are applied to construct binary sequences with strong pseudorandom properties, see, e.g. [12, 17]. As indicated in [7], it suffices to study subsets of $\{1, 2, \ldots, N\}$, the study of subsets of other finite ordered sets can be reduced to this case, which leads to use the number theoretic tools intensively.

A challenging problem is how to efficiently construct random subsets of the positive integers not exceeding a certain fixed integer N. However, in most cases we replace the random subset by a pseudorandom subset, which "looks random", and which is constructed by a suitable algorithm. But when is a subset a "good" pseudorandom subset? Recently, Dartyge, Mosaki and Sárközy introduced and studied the pseudo-random measures of subsets of the set of the positive integers not exceeding N [7, 8, 9]. These measures are closely related to the measures of pseudorandomness of binary sequences introduced by Mauduit and Sárközy [17] and of the p-pseudorandom binary sequences defined by Hubert and Sárközy [13].

For a subset $\mathcal{R}$ of $\{1, 2, \ldots, N\}$, define the associated sequence E_N by

$$E_N = E_N(\mathcal{R}) = \{e_1, \ldots, e_N\} \in \left\{1 - \frac{|\,\mathcal{R}\,|}{N}, -\frac{|\,\mathcal{R}\,|}{N}\right\}^N$$

with

$$e_m = \begin{cases} 1 - \frac{|\mathcal{R}|}{N} & \text{for } m \in \mathcal{R} \\ -\frac{|\mathcal{R}|}{N} & \text{otherwise} \end{cases} \quad (m = 1, \ldots, N). \qquad (1)$$

Then the *well-distribution measure* of the subset $\mathcal{R}$ of $\{1, 2, \ldots, N\}$ is defined by

$$W(\mathcal{R}, E_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|$$

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \le a \le a + (t-1)b \le N$, while the *correlation measure of order* k of $\mathcal{R}$ is defined as

$$C_k(\mathcal{R}, E_N) = \max_{M,D} \left| \sum_{m=1}^{M} e_{m+d_1} e_{m+d_2} \cdots e_{m+d_k} \right|$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ with non-negative integers $0 \le d_1 < \cdots < d_k$ and M such that $M + d_k \le N$. One would expect that these measures are "small". Thus we may consider a subset $\mathcal{R}$ of $\{1, 2, \ldots, N\}$ as a "good" pseudo-random subset if $W(\mathcal{R}, E_N)$ and $C_k(\mathcal{R}, E_N)$ (at least for small k) are small; they must be $O(N)$ and ideally, they are $O(N^{1/2+\varepsilon})$ [10].

Dartyge, Mosaki and Sárközy presented some good constructions of pseudo-random subsets when N is a prime number in [7, 8, 9, 10]. In [5] we present a construction of pseudo-random subsets for $N = pq$ with $2 < p < q < 2p$ by using generalized cyclotomic classes modulo N. However in applications one usually needs large families of pseudo-random subsets. It is interesting to design "good" pseudo-random subsets for different N using different algebraic systems. It is a natural way to choose elliptic curves over finite fields, partially for the elliptic curve cryptography for extensive use. We will apply elliptic curves to constructing some families of pseudo-random subsets and analyze their pseudorandom measures in the present paper.

We first introduce some notions and basic facts of elliptic curves over finite fields. Let $p > 3$ be a (large) prime, $\mathbb{F}_p$ the finite field of p elements which we identify with the set $\{0, 1, \cdots, p-1\}$, $\mathbb{F}_p^*$ the set of non-zero elements of $\mathbb{F}_p$. Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$, given by an affine Weierstrass equation of the standard form

$$y^2 = x^3 + Ax + B$$

with coefficients $A, B \in \mathbb{F}_p$ and nonzero discriminant, see [11]. It is known that the set, denoted by $\mathcal{E}(\mathbb{F}_p)$, of $\mathbb{F}_p$-rational points of $\mathcal{E}$ forms an Abelian group under an appropriate composition rule denoted by $\oplus$ and with the point at infinity $\mathcal{O}$ as the neutral element. We recall that

$$|\#\mathcal{E}(\mathbb{F}_p) - p - 1| \le 2p^{1/2},$$

where $\#\mathcal{E}(\mathbb{F}_p)$ is the number of $\mathbb{F}_p$-rational points, including the point at infinity $\mathcal{O}$. The translation map by $W \in \mathcal{E}(\mathbb{F}_p)$ on $\mathcal{E}(\mathbb{F}_p)$ is defined as

$$\tau_W : P \mapsto P \oplus W.$$

It is obvious that $(f \circ \tau_W)(P) = f(\tau_W(P)) = f(P \oplus W)$.

In this article, for convenience, we always suppose that $\mathcal{E}(\mathbb{F}_p)$ is a cyclic group of order N and $G \in \mathcal{E}(\mathbb{F}_p)$ is a generator, i.e., $\mathcal{E}(\mathbb{F}_p) = \langle G \rangle$. In particular, $N \sim p$ in this case. A multiple of G is taken by $nG = \oplus_{i=1}^{n} G$. We write $nG = (x_n, y_n) \in \mathbb{F}_p \times \mathbb{F}_p$ on $\mathcal{E}$ for all $1 \le n \le N-1$ and set $X(nG) = x_n$ and $Y(nG) = y_n$.

Construction of subsets. We would like to study the pseudorandom properties of the subset $\mathcal{R}$ of $\{1, 2, \ldots, N\}$ defined by

$$\mathcal{R} := \{n \mid 1 \le n \le N,\ X(nG) \equiv h \pmod p \text{ for any } h \in H\} \quad (2)$$

where $r \in \mathbb{Z}, s \in \mathbb{N}, s < p/2$ and $H = \{r, r+1, \ldots, r+s-1\}$.

We remark that $\mathcal{R}$ can be defined in several different ways using elliptic curves, we refer to a preprint version of [12], which is available at http://iml.univ-mrs.fr/editions/preprint2002/preprint2002.html, and [2, 3, 4] for related issues.

We also note that one can use some rational functions $f(X, Y)$, a more general case, instead of X in Equation (2).

2 The Cardinality of $\mathcal{R}$

Exponential sums play an important role in the proofs to estimate the cardinality of $\mathcal{R}$ and its pseudo-random measures.

For any positive integer m, we identify $\mathbb{Z}_m$ with the residue ring modulo m. Put

$$e_m(z) = \exp(2\pi i z/m).$$

The exponential sums enter into our problem by means of the following well known basic identity.

Lemma 1 ([15]). *For any element $c \in \mathbb{Z}_m$, we have*

$$\sum_{z \in \mathbb{Z}_m} e_m(cz) = \begin{cases} m, & \text{if } c = 0 \\ 0, & \text{otherwise.} \end{cases}$$

We also need the following statement.

Lemma 2 ([15]). *The bound*

$$\sum_{c=0}^{m-1} \left| \sum_{z=u+1}^{u+v} e_m(cz) \right| \le m(1 + \log m)$$

holds for any integers u and $1 \le v \le m$.

Let $\psi(z) = \exp(2\pi i z/p)$ be a classical additive character of $\mathbb{F}_p$. We also need the following upper bound which is a special case of [14, Corollary 1].

Lemma 3. *Let f be a nonconstant rational function and $G \in \mathcal{E}(\mathbb{F}_p)$ be a rational point of order N. Then the bound*

$$\left| \sum_{\substack{z=0 \\ f(zG) \ne \infty}}^{N-1} \psi(\lambda f(zG)) e_N(\eta z) \right| \le 2\deg(f) p^{1/2}$$

holds for all $\lambda \in \mathbb{F}_p^*$ and $\eta \in \mathbb{Z}_N$. Hence the bound on incomplete sums

$$\left| \sum_{\substack{z=u \\ f(zG) \ne \infty}}^{v} \psi(\lambda f(zG)) \right| \le 2\deg(f) p^{1/2}(1 + \log N)$$

holds for all $\lambda \in \mathbb{F}_p^*$ and integers $0 \le u < v \le N-1$.

We now present a bound on the cardinality of $\mathcal{R}$.

Theorem 1. *Let $\mathcal{R}$ be defined as in Equation (2). Then the cardinality of $\mathcal{R}$ satisfies*

$$\left||\mathcal{R}| - \frac{sN}{p}\right| \le 4p^{1/2}(1+\log p).$$

Proof. From the definition of $\mathcal{R}$ in Equation (2) and Lemma 1, we have

$$\sum_{h=r}^{r+s-1}\sum_{\lambda\in\mathbb{F}_p}\psi(\lambda(X(nG)-h)) = \begin{cases} p, & \text{if } n\in\mathcal{R} \\ 0, & \text{otherwise.}\end{cases}$$

Hence by Lemmas 2 and 3 we obtain

$$\begin{aligned}
|\mathcal{R}| &= \sum_{n=1}^{N}\frac{1}{p}\sum_{h=r}^{r+s-1}\sum_{\lambda\in\mathbb{F}_p}\psi(\lambda(X(nG)-h)) \\
&= \frac{s(N-1)}{p} + \\
&\quad \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\sum_{h=r}^{r+s-1}\psi(-\lambda h)\sum_{n=1}^{N}\psi(\lambda X(nG)) \\
&\le \frac{s(N-1)}{p} + \\
&\quad \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\left|\sum_{h=r}^{r+s-1}\psi(-\lambda h)\right|\cdot\left|\sum_{n=1}^{N}\psi(\lambda X(nG))\right| \\
&\le \frac{sN}{p} + 4p^{1/2}(1+\log p).
\end{aligned}$$

We complete the proof of Theorem 1. □

3 Pseudo-random Measures of $\mathcal{R}$

Now we present upper bounds on the well-distribution measure and the correlation measure of order k of $\mathcal{R}$ defined in Equation (2). The associated sequence E_N defined by Equation (1) is

$$e_m = \begin{cases} 1-\alpha & \text{for } m\in\mathcal{R} \\ -\alpha & \text{otherwise,}\end{cases}$$

where

$$\alpha = \frac{|\,\mathcal{R}\,|}{N} = \frac{s}{p} + 8\theta p^{-1/2}(1+\log p)$$

with some θ satisfying $|\theta|<1$, since $N\sim p$. Let $\beta = \frac{s}{p}-\alpha$.

Throughout this paper, the implied constant in the symbol " $\ll$ " is absolute.

Theorem 2. *Let $\mathcal{R}$ be a subset of $\{1,\dots,N\}$ defined as in Equation (2), we have*

$$W(\mathcal{R},E_N) \ll p^{1/2}(1+\log p)(1+\log N).$$

Proof. For $1\le n\le N-1$, it is easy to see that

$$\begin{aligned}
e_n &= (1-\alpha)\frac{1}{p}\sum_{h=r}^{r+s-1}\sum_{\lambda\in\mathbb{F}_p}\psi(\lambda(X(nG)-h)) \\
&\quad -\alpha\left(1-\frac{1}{p}\sum_{h=r}^{r+s-1}\sum_{\lambda\in\mathbb{F}_p}\psi(\lambda(X(nG)-h))\right) \\
&= \frac{1}{p}\sum_{h=r}^{r+s-1}\sum_{\lambda\in\mathbb{F}_p}\psi(\lambda(X(nG)-h)) - \alpha \\
&= \frac{s}{p} - \alpha + \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\sum_{h=r}^{r+s-1}\psi(-\lambda h)\psi(\lambda X(nG)) \\
&= \beta + \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\sum_{h=r}^{r+s-1}\psi(-\lambda h)\psi(\lambda X(nG)). \qquad (3)
\end{aligned}$$

However $e_N = -\alpha$, since $NG=\mathcal{O}$.

Assume that $a,b,t\in\mathbb{N}$ and $1\le a\le a+b(t-1)\le N$. According to Equation (3), we obtain

$$\begin{aligned}
&\left|\sum_{i=0}^{t-1}e_{a+ib}\right| \\
&\le \left|\frac{1}{p}\sum_{i=0}^{t-1}\sum_{\lambda\in\mathbb{F}_p^*}\sum_{h=r}^{r+s-1}\psi(-\lambda h)\psi(\lambda X((a+ib)G))\right| \\
&\quad + \left|\sum_{i=0}^{t-1}\beta\right| + 1 \\
&\le \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\left|\sum_{h=r}^{r+s-1}\psi(-\lambda h)\right|\cdot\left|\sum_{i=0}^{t-1}\psi(\lambda X((a+ib)G))\right| \\
&\quad + |t\beta| + 1 \\
&\le 4p^{1/2}(1+\log p)(1+\log N) + |t\beta| + 1
\end{aligned}$$

by Lemma 2 and Lemma 3 or [3, Lemma 5], which is derived from Lemma 3. And

$$|t\beta| = 8t\theta p^{-1/2}(1+\log p) \le 16p^{1/2}(1+\log p)$$

since $t\le N\sim p$. So we have

$$\left|\sum_{i=0}^{t-1}e_{a+ib}\right| \ll p^{1/2}(1+\log p)(1+\log N).$$

We complete the proof of Theorem 2. □

Theorem 3. *Let $\mathcal{R}$ be a subset of $\{1,\dots,N\}$ defined as in Equation (2), for $k<p$, we have*

$$C_k(\mathcal{R},E_N) \ll kp^{1/2}(2+\log p)^k(1+\log N).$$

Proof. Assume that integers $d_1,\dots,d_k$ and $M\in\mathbb{N}$ with

$$0\le d_1<\cdots<d_k, M+d_k\le N.$$

Now using Equation (3), we obtain

$$\begin{aligned}
&\left|\sum_{m=1}^{M} e_{m+d_1}e_{m+d_2}\cdots e_{m+d_k}\right| \\
\le\ &\left|\sum_{m=1}^{M}\prod_{i=1}^{k}\left(\beta+\frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\right.\right. \\
&\left.\left.\sum_{h=r}^{r+s-1}\psi(-\lambda h)\psi(\lambda X((m+d_i)G))\right)\right|+1 \\
=\ &1+\frac{1}{p^k}\left|\sum_{m=1}^{M}\prod_{i=1}^{k}\left(p\beta+\sum_{\lambda\in\mathbb{F}_p^*}\right.\right. \\
&\left.\left.\sum_{h=r}^{r+s-1}\psi(-\lambda h)\psi(\lambda X((m+d_i)G))\right)\right| \\
=\ &1+\frac{1}{p^k}\left|\sum_{m=1}^{M}\sum_{u=0}^{k}\sum_{1\le j_1<\ldots<j_u\le k}(p\beta)^{k-u}\right. \\
&\left.\prod_{i=1}^{u}\left(\sum_{\lambda\in\mathbb{F}_p^*}\sum_{h=r}^{r+s-1}\psi(-\lambda h)\psi(\lambda X((m+d_{j_i})G))\right)\right| \\
=\ &1+\frac{1}{p^k}\left|\sum_{u=0}^{k}(p\beta)^{k-u}\sum_{1\le j_1<\ldots<j_u\le k}\right. \\
&\sum_{\lambda_1\in\mathbb{F}_p^*}\cdots\sum_{\lambda_u\in\mathbb{F}_p^*}\sum_{h=r}^{r+s-1}\psi(-h(\lambda_1+\ldots+\lambda_u)) \\
&\left.\sum_{m=1}^{M}\psi\left(\sum_{v=1}^{u}\lambda_v X((m+d_{j_v})G)\right)\right| \\
=\ &1+\frac{1}{p^k}\left|\sum_{u=0}^{k}(p\beta)^{k-u}\sum_{1\le j_1<\ldots<j_u\le k}\right. \\
&\sum_{\lambda_1\in\mathbb{F}_p^*}\sum_{h=r}^{r+s-1}\psi(-h\lambda_1)\cdots\sum_{\lambda_u\in\mathbb{F}_p^*}\sum_{h=r}^{r+s-1}\psi(-h\lambda_u) \\
&\left.\sum_{m=1}^{M}\psi((\lambda_1X\circ\tau_{d_{j_1}G}+\ldots+\lambda_uX\circ\tau_{d_{j_u}G})(mG))\right| \\
\le\ &1+\frac{1}{p^k}\sum_{u=0}^{k}\binom{k}{u}(p\beta)^{k-u}p^u(1+\log p)^u Z \\
=\ &1+\frac{1}{p^k}(p\beta+p(1+\log p))^k Z \\
=\ &1+(\beta+1+\log p)^k Z\le(2+\log p)^k Z
\end{aligned}$$

where

$$\left|\sum_{m=1}^{M}\psi((\lambda_1X\circ\tau_{d_{j_1}G}+\ldots+\lambda_uX\circ\tau_{d_{j_u}G})(mG))\right|\le Z.$$

It suffices to estimate the value of Z, i.e., the upper bound of

$$\sum_{m=1}^{M}\psi((\lambda_1X\circ\tau_{d_{j_1}G}+\ldots+\lambda_uX\circ\tau_{d_{j_u}G})(mG))$$

for any $\lambda_1,\ldots,\lambda_u\in\mathbb{F}_p^*$ and $1\le u\le k$. By [3, Lemma 1],

$$\lambda_1X\circ\tau_{d_{j_1}G}+\ldots+\lambda_uX\circ\tau_{d_{j_u}G}$$

is a nonconstant rational function of degree at most $2u$. So by Lemma 3 again, we obtain

$$\begin{aligned}
&\left|\sum_{m=1}^{M}\psi((\lambda_1X\circ\tau_{d_{j_1}G}+\ldots+\lambda_uX\circ\tau_{d_{j_u}G})(mG))\right| \\
\le\ &4up^{1/2}(1+\log N)\le 4kp^{1/2}(1+\log N).
\end{aligned}$$

We complete the proof of Theorem 3 by setting

$$Z=4kp^{1/2}(1+\log N).$$

□

4 Conclusion

Elliptic curves are widely used in cryptography for designing public key cryptosystems [11] and pseudorandom number generators [18]. It is a natural way to use elliptic curves to construct pseudorandom subsets, which is an important security primitive in network security and cryptography. In this article, we present an efficient method for constructing pseudorandom subsets of the set $\{1,2,\ldots,N\}$ using elliptic curves over finite fields and show that such pseudorandom subsets possess strong pseudorandom properties using the number theoretic tools of exponential sums.

Very recently, Liu and Gao studied a *quasi-random subset* of $\mathbb{F}_p$, which consists of the x-axis of all rational points on elliptic curves over $\mathbb{F}_p$ in [16]. The study of quasi-random subsets of $\mathbb{Z}_N$ is partially related to random graphs [6]. A relationship between quasi-randomness and pseudo-randomness is discussed in [10].

It is noted again that the pseudorandom subsets are constructed using modulo N residue rings in [7, 8, 9, 10] when N is a prime and in [5] when N is a product of two distinct primes. But in this article N can achieve other values depending on the elliptic curves. Our method can offer large families of pseudorandom subsets of the set $\{1,2,\ldots,N\}$ for different N by using different elliptic curves. Although we only restrict that $\mathcal{E}(\mathbb{F}_p)$ is a cyclic group of order N, it is easy to extend to any elliptic curves, which is defined over finite fields $\mathbb{F}_q$ for a prime power q, with a cyclic subgroup of order N of $\mathcal{E}(\mathbb{F}_q)$.

Acknowledgements

The research was partially supported by the Natural Science Foundation of Fujian Province of China under grant

2007F3086, 2008J0014, 2008F5049 and the Funds of the Education Department of Fujian Province under grant JA07164. The authors wish to thank the referees for their valuable comments.

References

[1] V. Bhandari and N. H. Vaidya, "Secure capacity of multi-hop wireless networks with random key predistribution," *The 27th Conference on Computer Communications (IEEE INFOCOM 2008)*, pp.1-6, Phoenix, USA, 2008.

[2] Z. Chen, S. Li and G. Xiao, "Construction of pseudorandom binary sequences from elliptic curves by using discrete logarithm," *The 4th International Conference on Sequences and Their Applications (SETA 2006)*, LNCS 4086, Springer Berlin/Heidelberg, pp.285-294, Bejing, China, 2006.

[3] Z. Chen and G. Xiao, "'Good' pseudo-random binary sequences from elliptic curves," *Cryptology ePrint Archive*, Report 2007/275, 2007. (http://eprint.iacr.org/)

[4] Z. Chen, "Elliptic curve analogue of Legendre sequences," *Monatshefte für Mathematik*, vol. 154, no. 1, pp. 1-10, 2008.

[5] Z. Chen, "Large families of pseudo-random subsets formed by generalized cyclotomic classes," *Monatshefte für Mathematik*, doi:10.1007/s00605-009-0117-z, 2009.

[6] F.R.K. Chung and R.L. Graham, "Quasi-random subsets of $\mathbb{Z}_N$," *J. Combin. Theory Ser.A*, vol. 61, pp. 64-86, 1992.

[7] C. Dartyge and A. Sárközy, "On pseudo-random subsets of the set of the integers not exceeding N," *Periodica Mathematica Hungarica*, vol. 54, no. 2, pp. 183-200, 2007.

[8] C. Dartyge and A. Sárközy, "Large families of pseudorandom subsets formed by power residues," *Uniform Distribution Theory*, vol. 2, no. 2, pp. 73-88, 2007.

[9] C. Dartyge, E. Mosaki, and A. Sárközy, "On large families of subsets of the set of the integers not exceeding N," *The Ramanujan Journal*, vol. 18, no. 2, pp. 209-229, 2009.

[10] C. Dartyge and A. Sárközy, "On pseudo-random subsets of $\mathbb{Z}_n$," *Monatshefte für Mathematik*, vol. 157, no. 1, pp. 13-35, 2009.

[11] A. Enge, *Elliptic Curves and Their Applications to Cryptography : An Introduction*. Dordrecht: Kluwer Academic Publishers, 1999.

[12] L. Goubin, C. Mauduit, and A. Sárközy, "Construction of large families of pseudorandom binary sequences," *Journal of Number Theory*, vol. 106, no. 1, pp. 56-69, 2004.

[13] P. Hubert and A. Sárközy, "On p-pseudorandom binary sequences," *Periodica Mathematica Hungarica*, vol. 49, pp. 73-91, 2004.

[14] D. Kohel and I. E. Shparlinski, "Exponential sums and group generators for elliptic curves over finite fields," *The 4th International Symposium on Algorithmic Number Theory (ANTS-IV 2000)*, LNCS 1838, pp. 395-404, Springer, The Netherlands, 2000.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, MA: Addison-Wesley, 1983.

[16] H. Liu and J. Gao, "Quasirandom subsets of $\mathbb{Z}_p$ from elliptic curves (in Chinese)," *Acta Mathematica Sinica, Chinese Series*, vol. 52, no. 2, pp. 209-216, 2009.

[17] C. Mauduit and A. Sárközy, "On finite pseudorandom binary sequences I: measures of pseudorandomness, the Legendre symbol," *Acta Arithmetica*, vol. 82, pp. 365-377, 1997.

[18] I. E. Shparlinski, "Pseudorandom number generators from elliptic curves," *Recent Trends in Cryptography, Contemporary Mathematics*, vol. 477, pp. 121-141, American Mathematical Society, 2009.

[19] Z. Su, C, Lin, and R. Yuan, "Hash chain based random keys pre-distribution scheme in wireless sensor networks (in Chinese)," *Chinese Journal of Computers*, vol. 32, no. 1, pp. 30-41, 2009.

[20] Z. Wu, Z. Chen, F. Guo, and L. Xu, "Identity based private matching," *The 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (IEEE SecPerU 2007)*, pp. 85-90, Istanbul, Turkey, 2007.

[21] L. Xu, S. Cheng, X. Huang, and Y. Mu, "Pseudonym and bloom filter based secure and anonymouse DSR protocol in wireless ad hoc network," *International Journal of Security and Network* (in press).

Zhixiong Chen was born in 1972 in Fujian province of China. He received the M.S degree in mathematics from Fujian Normal University in 1999 and Ph.D degree in cryptography from Xidian University, P.R.China, in 2006, respectively. Now he is an associate professor of Putian University. He is a member of CCF (China Computer Federation). His research interests include stream ciphers and elliptic curve cryptography.

Li Xu was born in 1970 in Fujian province of China. He graduated from the Department of Mathematics, Fujian Normal University, P.R China, in 1992. He received the M.S degree in mathematics from Fujian Normal University in 2001 and Ph.D degree in information engineer from Nanjing University of Post and Telecommunication, P.R.China, in 2004, respectively. Now he is a professor and Co-Director of Key Lab of Network Security and Cryptography of Fujian Normal University. Dr. Xu is the senior member of CCF and CIE in China. His research interests include network security, wireless communication and network.

Chenhuang Wu was born in 1981 in Fujian province of China. He received the M.S degree in mathematics from Zhangzhou Normal University in 2007. Now he is a

lecturer of Putian University. He is a member of CCF. His research interests include digital signatures and elliptic curve cryptography.