A Result on the Distribution of Quadratic Residues with Applications to Elliptic Curve Cryptography

Muralidhara V.N. and Sandeep Sen

Department of Computer Science and Engineering,
Indian Institute of Technology, Delhi
Hauz Khas, New Delhi 110 016, India
{murali,ssen}@cse.iitd.ernet.in

Abstract. In this paper, we prove that for any polynomial function f of fixed degree without multiple roots, the probability that all the $(f(x+1), f(x+2), ..., f(x+\kappa))$ are quadratic non-residue is $\approx \frac{1}{2^\kappa}$. In particular for $f(x) = x^3 + ax + b$ corresponding to the elliptic curve $y^2 = x^3 + ax + b$, it implies that the quadratic residues $(f(x+1), f(x+2), \ldots$ in a finite field are sufficiently randomly distributed. Using this result we describe an efficient implementation of El-Gamal Cryptosystem. that requires efficient computation of a mapping between plain-texts and the points on the elliptic curve.

1 Introduction

The distribution of quadratic residues is an interesting problem in Number theory and has many practical applications including Cryptography and Random number generation. In particular it is conjectured to be random and there are many constructions based on this conjecture [1,2]. Peralta [2] proves that for any randomly chosen $x \in F_q$, the probability of $(x+1, x+2, ..., x+\kappa)$ matching any particular quadratic sequence of length κ is in the range $\frac{1}{2^\kappa} \pm \kappa\frac{3+\sqrt{q}}{q}$. In this paper we prove a similar result for the sequence $(f(x+1), f(x+2), ..., f(x+\kappa))$, for any polynomial function f of fixed degree without multiple roots. In particular for $f(x) = x^3 + ax + b$ corresponding to the elliptic curve $y^2 = x^3 + ax + b$, it implies that the quadratic residues $(f(x+1), f(x+2), \ldots$ in a finite field are sufficiently randomly distributed.

The main motivation for this work is Elliptic Curve El-Gamal Cryptosystem and Koblitz's mapping from the message units to points on an elliptic curve. In the following sections we briefly describe these two methods.

1.1 El-Gamal Cryptosystem

We start with a fixed publicly known finite field K, an elliptic curve E/K defined over it and a base point $B \in E/K$ (we refer to [5] for basic definitions and

K. Srinathan, C. Pandu Rangan, M. Yung (Eds.): Indocrypt 2007, LNCS 4859, pp. 48–57, 2007.

notations). Each user chooses a random integer b, which is kept secret, and computes the point $x = bB$ which is the public key. To send a message P to Bob, Alice chooses a random integer k and sends the pair of points $(kB, P + k(bB))$ (where bB is Bob's public key) to Bob. To read the message, Bob multiplies the first point in the pair by his secret key b and subtracts the result from the second point: $P + k(bB) - b(kB)$ that yields P.

One of the commonly used ECC, El-Gamal Cryptosystem requires a mapping from the message units to points on an elliptic curve, i.e., we need an efficient algorithm which computes a mapping between the points on an elliptic curve and a plain-text which forms the basis of encryption and decryption routines.

To date no polynomial time deterministic algorithm is known for this problem. However we do have polynomial time randomized algorithms. We sketch such an algorithm due to Koblitz [5] that makes the following assumptions:

- F_q is a field with p^n elements ($p > 3$, prime).
- κ is a large enough integer so that we are satisfied with the failure probability $\frac{1}{2^\kappa}$ when we attempt to embed a plain text message m.
- Message units are integers between 0 and $M - 1$.
- The finite field is chosen in such a way that $q > \kappa \cdot M$.
- An integer $m = \sum_{i=0}^{n-1} a_i p^i$ is mapped to $(a_0, a_1, ..., a_{n-1}) \in F_q$.

Koblitz's algorithm

1. Given m, find an element $x \in F_q$ corresponding to $m\kappa + 1$ and compute $f(x) = x^3 + ax + b$ and check whether $f(x)$ is a quadratic residue.
   (This can be easily done because an element $\alpha \in F_q$ is a quadratic residue if and only if $\alpha^{(q-1)/2} = 1$).
2. If $f(x)$ is a quadratic residue then we can find a y such that $y^2 = x^3 + ax + b$ and we map m to $P_m = (x, y)$.
   (There are polynomial time probabilistic algorithms to find the square roots in finite fields of odd order [5]).
3. If $f(x)$ is not a quadratic residue then we try points corresponding to $m\kappa + j$, $1 < j \leq \kappa$ till we find an x such that $f(x)$ is a quadratic residue.

Suppose x_1 is the integer corresponding to the point $x \in F_q$. We can recover m from the point $P_m = (x, y)$ by dividing $x_1 - 1$ by κ ($x_1 - 1 = m\kappa + j$, $0 \leq j < \kappa$).

It has been conjectured that the probability that the above algorithm would fail to find an embedding of a given plain-text message is $\approx \frac{1}{2^\kappa}$, where κ is the number of repetitions of step 3. If quadratic residues in a finite field of odd order are randomly distributed then in fact the κ events (in the above algorithm) are independent and hence the probability that the algorithm would fail is exactly $\frac{1}{2^\kappa}$. In section 4 we show the existence of such finite fields; however we do not know of any efficient construction of finite fields in which quadratic residues are randomly distributed. A naive modification would be to map a message to a point on the curve by choosing a random field element; by Hasse's theorem [5,6], we will succeed with probability about 1/2. But the drawback

of such an approach would be that we have to send the random element with each message for decryption, thereby increasing the message expansion factor considerably.

1.2 Previous Results

There is an extensive literature on the distribution of quadratic residues and non residues over finite Fields [1,2]. In particular, Peralta [2] proves that for any randomly chosen $x \in F_q$, the probability of $(x+1, x+2, ..., x+\kappa)$ matching any particular binary sequence of length κ is in the range $\frac{1}{2^\kappa} \pm \kappa\frac{3+\sqrt{q}}{q}$. We note that we are interested in the sequence$(f(x+1), f(x+2), ..., f(x+\kappa))$ where $f(x) = x^3 + ax + b$ for an elliptic curve $y^2 = x^3 + ax + b$. In the rest of the paper $\chi(x)$ denote the characteristic function defined as

$$\chi(x) \;=\; \begin{cases} -1 & \text{if x is a quadratic non-residue} \\ 0 & \text{if x is zero} \\ 1 & \text{if x is quadratic residue} \end{cases}$$

To prove our main theorem we prove the following lemma,

Lemma 1. *Let $g(x)$ be any polynomial of degree d which don't have multiple roots and k be a positive integer such that $dk < p$. If $i_1, i_2, ..., i_m$ $(m \leq k)$, be any m distinct integers between 1 and k, then*

$$|\sum_{x \in F_q} \chi(g'(x))| \leq d'\sqrt{q} \tag{1}$$

where $g'(x) = \prod_{j=1}^{m} g(x + i_j))$ and $d' = dm - 1$, the degree of g'.

We note that C. Mauduit and A. Sárközy [1] prove results on the pseudorandom properties of distribution of quadratic residues of arithmetic progression (not exactly for the sequence that we are looking at). In the process, they prove that for any $g(x) \in F_q[X]$ polynomial of degree d that does not have multiple roots, then

$$|\sum_{x \in F_q} \chi(g(x))| \leq 9d\sqrt{q}\log q \tag{2}$$

So with an additional constraint $dk < p$, our bound is better by a factor $O(\log q)$.

1.3 Main Result

In this paper we address the following problem:

Let $S = \{(a_0, a_1, \ldots, a_{n-1}) : a_i \in \mathbb{Z}_p, 0 \leq i < n,\ p \text{ prime} > 3\}$. Order the elements of S^* in a reverse lexicographic order, that is,

$$\begin{aligned}
x_1 &= (1,0,0,\ldots,0).\\
x_2 &= (2,0,0,\ldots,0).\\
&\vdots\\
x_p &= (0,1,0,\ldots,0).\\
x_{p+1} &= (1,1,0,\ldots,0).\\
&\vdots\\
x_{2p+1} &= (1,2,0,\ldots,0).\\
&\vdots\\
x_{p^n-1} &= (p-1,p-1,p-1,\ldots,p-1).
\end{aligned}$$

Let $a, b \in S$ be two fixed elements. Given any $\kappa \in N$ can we bound the number of κ-sub-sequences

$$\langle x_{l+1}, x_{l+2}, \ldots, x_{l+\kappa}\rangle, \qquad 0 \le l < p^n - \kappa - 1$$

such that all of $x_{l+i}^3 + ax_{l+i} + b,\ 1 \le i \le \kappa$ are quadratic non-residues by $\approx \frac{p^n-1}{2^\kappa}$?

If the answer to this question is yes, then in Koblitz's algorithm, we can begin with a random element $x_l,\ 0 \le l \le p^n - \kappa$. The probability that all of $x_{l+i}^3 + ax_{l+i} + b,\ 1 \le i \le \kappa$ are quadratic non-residues is $\approx \frac{1}{2^\kappa}$ which will mean that the conjecture is correct.

In the following sections we prove a somewhat weaker version of this. We prove that if we choose a random element $x \in F_{p^n}$ then the probability that all of $(x+i)^3 + a(x+i) + b,\ 1 \le i \le \kappa$ are quadratic non-residues is $\approx \frac{1}{2^\kappa}$. Note that if $x = x_r$ and if $p|(r+1)$ then $x+1 = x_{r-p+1}$ else $x+1 = x_{r+1}$. Hence by randomly picking an element in the above sequence and adding 1 to it repeatedly we may be able to get at most p consecutive elements in the sequence.

By exploiting this result, we propose a provably efficient alternative to Koblitz scheme in section 3 that requires similar computations as Koblitz's original method and the (expected) message expansion factor is also identical.

We formally prove the following theorem in next section,

Theorem 1. *Let $g(x)$ be any polynomial of degree d which don't have multiple roots. If κ is any positive integer $< \frac{p}{d}$ then*

$$|\ \{x \in F_q \mid g(x+1), g(x+2), ..., g(x+\kappa) \textit{are quadratic non-residues}\}\ |$$

is between $\frac{q-\mu_\kappa(a,b)}{2^k} - (d\kappa-1)\sqrt{q}$ and $\frac{q-\mu_\kappa(a,b)}{2^k} + (d\kappa-1)\sqrt{q}$, where $q = p^n$ and $0 \le \mu_\kappa(a,b) \le 3$.

2 Proof of the Main Result

Let F_{p^n} be a field with $q = p^n$ (p is a prime > 3) elements. We define a relation $\sim$ on F_{p^n} as $x \sim y$ iff there is a non-negative integer k such that $x - y = 1+1+\ldots+1$, where 1 is added k times. This is an equivalence relation on F_{p^n}. Each equivalence class will have p (characteristic of F_{p^n}) elements.

Let α, β, γ be three distinct elements in the same equivalence class. We may assume that if μ_1 and μ_2 are least positive integers such that $\alpha = \beta + \mu_1, \alpha = \gamma + \mu_2$ then $\mu_1 < \mu_2$. Let $k_\alpha, k_\beta, k_\gamma$ be least positive integers such that $\alpha = \beta + k_\beta$, $\beta = \gamma + k_\gamma$, $\gamma = \alpha + k_\alpha$. Now $k_\alpha, k_\beta, k_\gamma$ are such that $\alpha = k_\beta + k_\gamma + k_\alpha + \alpha$ and $k_\alpha + k_\beta + k_\gamma = p$ (in general it can be any multiple of p, but the assumption $\mu_1 < \mu_2$ makes it p). Hence one of $k_\alpha, k_\beta, k_\gamma$ is $> p/3$.

So we may assume that $k_\alpha > p/3$. Let k be any positive integer $< p/3$. Now for any m integers, $i_1, i_2, \ldots, i_m$ such that $1 \leq i_1 < i_2 < \ldots < i_m \leq k$ the following should hold.

$$\alpha - i_1 \notin \{\beta - i_j \mid 1 \leq j \leq m\} \cup \{\gamma - i_j \mid 1 \leq j \leq m\}$$

Hence if α, β, γ are three distinct elements in the same equivalence class and $i_1, i_2, ..., i_m$ are any m integers such that $1 \leq i_1 < i_2 < ... < i_m \leq k < p/3$ then one of the following holds.

$$\begin{aligned}
\gamma - i_1 &\notin \{\alpha - i_j \mid 1 \leq j \leq m\} \cup \{\beta - i_j \mid 1 \leq j \leq m\} \\
\alpha - i_1 &\notin \{\beta - i_j \mid 1 \leq j \leq m\} \cup \{\gamma - i_j \mid 1 \leq j \leq m\} \\
\beta - i_1 &\notin \{\gamma - i_j \mid 1 \leq j \leq m\} \cup \{\alpha - i_j \mid 1 \leq j \leq m\}
\end{aligned}$$

This observation will be used to prove the following Lemma.

Lemma 2. *Let $g(x)$ be any polynomial of degree d which don't have multiple roots and k be a positive integer such that $dk < p$. If $i_1, i_2, ..., i_m$ $(m \leq k)$, be any m distinct integers between 1 and k, then $\prod_{j=1}^{m} g(x + i_j)$ cannot be written as $h(x)^2$ for some $h(x) \in F_{p^n}[X]$.*

Proof. Let $\alpha_1, \alpha_2, \ldots \alpha_d$ be the roots of g in the splitting field. From the definition these must be distinct. Also note that $\alpha_1 - i, \alpha_2 - i, \alpha_d - i$ are the roots of $g(x + i)$ $\forall i,\ 1 \leq i \leq k$.

If there exists a polynomial $h(x) \in F_{p^n}[X]$ such that

$$\prod_{j=1}^{m} g(x + i_j) = h(x)^2 \tag{3}$$

then m has to be even (as degree of $\prod_{j=1}^{m} g(x + i_j)$ is dm and degree of $h(x)^2$ is even). So the multiplicity of any root of $\prod_{j=1}^{m} g(x + i_j)$ is even. As i_j's are distinct $\alpha_i - i_a \neq \alpha_i - i_b$ for $\forall a, b \leq m$, it follows that multiplicity of any root of $\prod_{j=1}^{m} g(x + i_j)$ is $\leq d$, hence should be 2.

From the arguments given before this lemma, at least one of $\alpha_1 - i_1$, $\alpha_2 - i_1$, $\alpha_d - i_1$ can not be of multiplicity 2 (if α_i's are not in the same equivalence class then this is trivially true), which is a contradiction.

The proof of Lemma 1, follows from Lemma 2 and Weil's theorem on finite fields[6]. Now we are ready to prove Theorem 1.

Proof of Theorem 1. Let $A(x) = \prod_{i=1}^{\kappa}(1 - \chi(g(x + i))$.[1]
$S = \{x \in F_q \mid g(x + 1), g(x + 2), ..., g(x + \kappa)$ are quadratic non-residues$\}$

[1] Similar idea was used in [3] and was suggested to us by Radhakrishnan[9].

$S' = \{x \in F_q \text{ |at least one of } g(x+1)., g(x+\kappa) \text{ is a quadratic residues}\}$
$S'' = \{x \in F_q \mid g(x+1) = g(x+2) =, ..., = g(x+\kappa) = 0\}$.

Clearly, $F_q = S \cup S' \cup S''$ and

$$A(x) = \begin{cases} 2^\kappa & \text{if } x \in S, \\ 0 & \text{if } x \in S' \\ 1 & \text{if } x \in S'' \end{cases}$$

Let $\mid S \mid = N$ and denote $\mu_\kappa(a,b) = \mid S'' \mid$. Note that $\alpha \in S'' \Longrightarrow g(\alpha+1) = g(\alpha+2) =, ..., = g(\alpha+\kappa) = 0 \Longrightarrow \alpha - 1, \alpha - 2, ..., \alpha - \kappa$ are roots of $g(x)$ and hence $0 \le \mu_\kappa(a,b) \le d$ and $\mu_\kappa(a,b) = 0$ if $\kappa > d$.

Now

$$\sum_{x \in F_q} A(x) \;=\; 2^\kappa N + \mu_\kappa(a,b) \tag{4}$$

Notice that

$$A(x) \;=\; 1 + \sum_{m=1}^{\kappa} (-1)^m \sum_{1 \le i_1 < i_2 < ... < i_n \le \kappa} \chi(g(x+i_1)g(x+i_2)...g(x+i_n))$$

Hence

$$N2^\kappa + \mu_\kappa(a,b) - q = \sum_{x \in F_q} \sum_{m=1}^{\kappa} (-1)^m \sum_{1 \le i_1 < i_2 < ... < i_n \le \kappa} \chi(g(x+i_1)g(x+i_2)...g(x+i_n))$$

$$= \sum_{m=1}^{\kappa} (-1)^m \sum_{1 \le i_1 < i_2 < ... < i_n \le \kappa} \sum_{x \in F_q} \chi(g(x+i_1)g(x+i_2)...g(x+i_n))$$

By taking modulus,

$$\mid N2^\kappa + \mu_\kappa(a,b) - q \mid \le \mid \sum_{m=1}^{\kappa} (-1)^m \sum_{1 \le i_1 < i_2 < ... < i_n \le \kappa} \sum_{x \in F_q} \chi(g(x+i_1)g(x+i_2)...g(x+i_n)) \mid$$

By triangular inequality,

$$\mid N2^\kappa + \mu_\kappa(a,b) - q \mid \le \sum_{m=1}^{\kappa} \sum_{1 \le i_1 < i_2 < ... < i_n \le \kappa} \mid \sum_{x \in F_q} \chi(g(x+i_1)g(x+i_2)...g(x+i_n)) \mid$$

Applying Lemma 1

$$\le \sum_{m=1}^{\kappa} \kappa C_m (dm - 1)\sqrt{q}$$

$$< (d\kappa - 1)2^\kappa \sqrt{q}$$

Hence $\frac{q - \mu_\kappa(a,b)}{2^k} - (d\kappa - 1)\sqrt{q} < N < \frac{q - \mu_\kappa(a,b)}{2^k} + (d\kappa - 1)\sqrt{q}$

Corollary 1. *Let $y^2 = x^3 + ax + b$ be an elliptic curve over F_{p^n} (p is a prime > 3). Let $g(x) = x^3 + ax + b$. If κ is any positive integer $< \frac{p}{3}$ then for a randomly chosen $x \in F_q$ the probability that all of $g(x+1), g(x+2), ..., g(x+\kappa)$ are quadratic non-residues is $\approx \frac{1}{2^\kappa}$*

For $g(x) = x^3 + ax + b$, the result follows from Theorem 1.

3 A Modified ECC

Here we propose a modification for El-Gamal Cryptosystem with Koblitz's method for Embedding plain-texts on to the points of elliptic curve which exploits the result of the previous section. More specifically, given a plain-text message, we try to map it to a random point on the Elliptic Curve by choosing an initial random shift in Koblitz's algorithm.

3.1 Key Generation

We suppose that all parties have agreed upon an elliptic curve $E/K : y^2 = x^3 + ax + b$ over a finite field $K = F_{p^n}$ and $p > 3$, a point P of high order on it and a failure factor $\kappa (< p/3)$. Let $r_1, r_2, \ldots, r_t$ be t randomly chosen integers between 1 and p^n and they are made public.

Each party A does the following:

- Choose a random integer a.
- a is A's **Secret Key**.
- aP is A's **Public Key**.

3.2 Encryption

To send a message m to Alice, Bob does the following:

- Choose a random integer μ and s, $1 \leq s \leq t$.
- Obtain Alice's public key aP and Compute μaP a point on the elliptic curve.
- Find $x \in F_q$ corresponding to $m\kappa + r_s + 1$.
  If $x^3 + ax + b$ is a quadratic residue (or zero) then find a y such that $y^2 = x^3 + ax + b$ and take $P(m, r_s) = (x, y)$ else try with points corresponding to $m\kappa + r_s + j, 1 < j \leq \kappa$.
- Send $(\mu P, P(m, r_s) + \mu aP)$ and s.

The probability that Bob fails to find $P(m, r_s)$ with the shift corresponding to the random number r_s is $\frac{1}{2^\kappa}$ by Corollary 1. If he fails, then he tries with some other random number s for $1 \leq j \leq t$. If he fails with all the $r_1, r_2, \ldots, r_t$ then he would try with some random r's until he succeeds and he would send this r along with the message (This will happen with negligible probability $(1/2)^{t\kappa}$).

3.3 Decryption

To recover the message m, Alice does the following:

- Multiply the first point in the above pair by her secret key a and subtracts the results from the second point to get the point
$$P(m,r) \;=\; (P(m,r) + \mu aP) - a\mu P.$$
(Here r is one of the public r_i's or is sent with the message).
Let $P(m,r) = (x,y)$.
- Find x_1, the integer corresponding to x.
- m is obtained by dividing $x_1 - 1 - r$ by κ.
$$\text{i.e. } x_1 - 1 - r \;=\; m\kappa + j,\ 0 \le j < \kappa.$$

Our modified encryption and decryption schemes require similar computations as Koblitz's original method and the (expected) message expansion factor is also identical. Moreover, our method has following advantages over the original method:

1. The probability that Bob fails to encrypt a message with the shift corresponding to a random number μ is provably $\frac{1}{2^\kappa}$.
2. The *failure factor* κ can be small, because even if we fail with one *randomshift* we can try with another *random shift*. Small *failure factor* κ implies that the message units can be large, as $M\kappa < q$ where is message units m are such that $m < M$.
3. Random Embedding: The point $P(m,r)$ not only depends on m, it also depends on r, so even for a fixed message the point corresponding to the message will be different on different occasions. This prevents an eavesdropper from guessing the message. The usual procedure is to pad random bits, but strictly speaking it does not really make the message random.

4 Randomizing the Distribution of Quadratic Residues in a Finite Field

In this section we would like to address the question: *Can we Randomize the distribution of quadratic residues in a finite field?* The following theorem says that the answer is yes.

Theorem 2. *Let S be a set with p^n elements, p an odd prime, n any natural number. Given $x_1, x_2, \ldots, x_{\frac{p^n-1}{2}}$ in S, there exists two binary operations $\oplus$ and $\star$ such that $(S, \oplus, \star)$ is a field and the quadratic residues are precisely these x_i's.*

Proof. Let $(F_q, +, *)$ be a field with q elements where $q = p^n$ and β be a fixed non-residue in F_q. Let $a_i, i = 1, 2, \ldots, (p^n - 1)/2$ be the nonzero elements of F_q, written as n-tuples of elements of F_q, whose first nonzero coordinate lies in $\{1, 2, \ldots, (p-1)/2\}$, listed reverse lexicographically. Let $S = \{x_1, x_2, \ldots, x_{\frac{p^n-1}{2}}, y_1, y_2, \ldots, y_{\frac{p^n-1}{2}}, O\}$.

We define a bijection ϕ from S to F_q as[2],

$$\begin{aligned} O &\mapsto 0 \\ x_i &\mapsto a_i^2 \\ y_i &\mapsto \beta a_i^2 \ , \qquad 1 \leq i \leq \tfrac{p^n-1}{2}. \end{aligned}$$

With this we define two binary operations $\oplus$ and $\star$ on S as

$$\begin{aligned} a \ \oplus \ b &= \phi^{-1}\{\phi(a) + \phi(b)\} \\ a \star b &= \phi^{-1}\{\phi(a) * \phi(b)\}, \ \forall a, b \in S \end{aligned}$$

It can be easily verified that $(S, \oplus, \star)$ is a field and the quadratic residues in $S(+, \star)$ are x_i's.

Both ϕ and ϕ^{-1} can be found in polynomial time, however finding ϕ^{-1} involves finding square roots, which is very costly (compared to addition , multiplication, inversion) as it takes $O(\log p^n)$ operations. We note that each elliptic curve operation involves 6 additions, 3 multiplications and 1 inversion (field operations). Since implementation of El-Gamal Cryptosystem involves computing scalar multiplication, kP which would take $2 \log k$ elliptic curve operations, this method is not practical.

5 Weil's Theorem

Theorem 3. ***(Weil's Theorem)*** *Let $f(x) \in F_q[X]$ be any polynomial of positive degree that is not a square of any of polynomial.($f(x) \neq h^2(x)$ for all $h(x) \in F_q[X]$). Let d be the number of distinct roots of $f(x)$ in splitting field over F_q, then we have*

$$|\sum_{x \in F_q} \chi(f(x))| \leq (d-1)\sqrt{q} \tag{5}$$

where

$$\chi(x) \ = \ \begin{cases} -1 & \textit{if } x \textit{ is a quadratic non-residue} \\ 0 & \textit{if } x \textit{ is zero} \\ 1 & \textit{if } x \textit{ is quadratic residue} \end{cases}$$

For proof, the reader is referred to [6]

References

1. Mauduit, C., Sárközy, A.: On finite pseudorandom binary sequences 1: Measure of pseudorandomness, the Legendre symbol. Acta Arith. 82, 365–377 (1997)
2. Peralta, R.: On the distribution of quadratic residues and nonresidues modulo a prime number. Mathematics of Computation 58(197), 433–440 (1992)

[2] This construction was pointed out by an anonymous reviewer for an earlier version of the paper.

3. Babai, L., G'al, A., Koll'ar, J., R'onyai, L., Szab'o, T., Wigderson, A.: Extremal Bipartite Graphs and Superpolynomial Lowerbounds for Monotone Span Programs. In: Proc. ACM STOC 1996, pp. 603–611 (1996)
4. Gallant, R., Lambert, R., Vanstone, S.: Improving the parallelized Pollard lambda search on binary anomalous curves. Mathematics of Computation 69, 1699–1705 (2000)
5. Koblitz, N.: A Course in Number theory and Cryptography. Springer, New York (1994)
6. Lidl, R., Niederreiter, H., Cohn, P.M.: Encyclopedia of Mathematics and its Applications20-Finite Fields. Cambridge University Press, Cambridge (1997)
7. Menezes, A.: Elliptic Curve Public Key Cryptosystems. Kluwer Academic Publishers, Dordrecht (1996)
8. Pollard, J.: Monte Carlo methods for index computation mod p. Mathematics of computation 32, 918–924 (1978)
9. Radhakrishnan, J.: Private Communication
10. Van Oorschot, P., Wiener, M.: Parallel collision search with cryptanalytic applications. Journal of Cryptology 12, 1–28 (1999)
11. Wiener, M., Zuccherato, R.: Faster attacks on elliptic curve cryptosystems. In: Tavares, S., Meijer, H. (eds.) SAC 1998. LNCS, vol. 1556, pp. 190–200. Springer, Heidelberg (1999)