域 GF(2^n) 上安全椭圆曲线及基点的选取 [1]

刘胜利 郑 东 王育民

(西安电子科技大学 ISN 国家重点实验室 西安 710071)

摘 要 该文系统地介绍了如何利用 Weil 定理来寻找特征为 2 的域上的安全椭圆曲线. 提出了一种求曲线的基点的算法. 求基点的算法中涉及求域元素的迹的问题. 该文在最后还提出了一种求域 GF(2^l) 的扩域 GF(2^{lk}) 上元素的迹的快速实现方法.

关键词 椭圆曲线密码体制, 基点, 迹

中图号 TN918.1

1 引 言

类似于有限域的乘群上的离散对数, 椭圆曲线所构成的 Abel 群也可以形成离散对数问题, 应用于公钥体制、签名及认证。椭圆曲线上的离散对数问题可以描述如下: 已知曲线上的点 $P=(x_1,y_1)$ 和点 $Q=kP=(x_2,y_2)$, 求整数 k.

与基于有限域上离散对数问题的公钥体制相比, 椭圆曲线密码体制有如下优点:

(1) 安全性高: 攻击有限域上的离散对数问题有指数积分法, 其运算复杂度为 $O\{\exp[(\log p)\times(\log\log p)^2]^{1/3}\}$, 其中 p 是模值, 为素数. 而它对椭圆曲线上的离散对数问题并不有效. 目前攻击椭圆曲线上的离散对数问题只有适合攻击任何循环群上离散对数问题的大步小步法, 其运算复杂度为 $O(\exp(\log\sqrt{P_{\max}}))$, 其中 $P_{\max}$ 是椭圆曲线所形成的 Abel 群的阶的最大素因子。因此, 椭圆曲线密码体制比基于有限域上的离散对数问题的公钥体制更安全。

(2) 密钥量小: 由攻击两者的算法复杂度可知, 在实现相同的安全性能条件下, 椭圆曲线密码体制所需的密钥量远比基于有限域上的离散对数问题的公钥体制的密钥量小。

(3) 灵活性好: 有限域 GF(q) 一定的情况下, 其上的循环群就定了, 即 GF(q) − {0}. 而 GF(q) 上的椭圆曲线可以通过改变曲线参数, 得到不同的曲线, 形成不同的循环群。因此, 椭圆曲线具有丰富的群结构和多选择性。 正是由于椭圆曲线具有丰富的群结构和多选择性, 并可在保持和 RSA/DSA 体制同样安全性能的前提下大大缩短密钥长度 (目前 160bit 足以保证安全性), 因而在密码领域有着广阔的应用前景。表 1 给出了椭圆曲线密码体制 (ECC) 和 RSA/DSA 体制在保持同等安全的条件下各自所需的密钥的长度。

表 1 ECC 和 RSA/DSA 在保持同等安全的条件下所需的密钥的长度 (单位为 bit)

RSA/DSA	512	768	1024	2048	21000
ECC	106	132	160	211	600

一般来说, 在密码中普遍应用的是基于大素域 GF(p) 和特征为 2 的域 GF(2^n) 上的非超奇异椭圆曲线. 方程分别为

[1] 1998-12-28 收到, 1999-09-09 定稿
陕西省自然科学基金资助项目, 编号 98x04

$$E: y^2 = x^3 + ax + b \quad (a, b \in \mathrm{GF}(p),\ 4a^3 + 27b^2 \neq 0) \quad \text{和}$$
$$E: y^2 + xy = x^3 + ax^2 + b \quad (a, b \in \mathrm{GF}(2^n)).$$

由于计算机是以二进制为基础的，所以为了便于实现，我们将寻找特征为 2 的域上的安全椭圆曲线.

2 特征为 2 的域上安全椭圆曲线的选取

2.1 安全椭圆曲线的条件

下面介绍安全的椭圆曲线必须满足的三个条件：

(1) 必须是非超奇异的椭圆曲线，以避免 MOV 算法 [1] 攻击. 因为对于超奇异椭圆曲线，MOV 算法利用 Weil-pairing 方法，可以建立有限域 GF(q) 上椭圆曲线的加法群与有限扩张域 GF(q^r) 的乘法群之间的联系，特别是把计算椭圆曲线上的离散对数问题约化到计算有限域的乘法群上的离散对数，并用此方法证明了建立在超奇异椭圆曲线上的密码体制并不比原来的基于有限域上的离散对数问题的密码体制优越.

(2) 椭圆曲线上所选择的基点的级必须含有一个至少 40 位的素因子以防止大步小步法的攻击. 大步小步法适用于攻击任何基于循环群上的离散对数问题，且算法复杂度为 $O(l_p)$，其中 l_p 是循环群的阶的最大素因子的长度.

(3) 满足 MOV 条件 [1]：设椭圆曲线所基于的有限域为 GF(q)，基点为 P，其级为 n，则

$$q^i \neq 1 \bmod n, \quad i = 1, 2, \cdots, T, \quad T = \log_2 q/8.$$

2.2 域 GF(2^n) 上的安全椭圆曲线的选取

特征为 2 的非超奇异椭圆曲线可以表示为 $E: y^2 + xy = x^3 + ax^2 + b$，$ab \in \mathrm{GF}(2^n)$ 且 $b \neq 0$. 其中不变量 $j(E) = 1/b$.

定理 1[2]　设 E 是定义在 GF(q) 上的一条椭圆曲线，则曲线的阶 $\#E(\mathrm{GF}(q))$ 满足 $|\#E((\mathrm{GF}(q)) - q - 1| \leq 2\sqrt{q}$.

进一步，Weil 定理给出了 GF(q) 的 k 次扩域 GF(q^k) 上曲线的阶 $\#E(\mathrm{GF}(q^k))$ 的表达式：$\#E(\mathrm{GF}(q^k)) = q^k + 1 - \beta_k$. 其中 $\beta^k = a^k + b^k$，a, b 是方程 $1 - \beta T + qT^2 = 0$，$\beta = (q+1) - \#E(\mathrm{GF}(q^k))$ 的两个复根，即 $(1 - aT)(1 - bT) = 0$.

借助 Weil 定理 [3]，选择特征为 2 的域上安全椭圆曲线的方法如下：

步骤 1　首先计算 GF(2) 的小扩域 GF(q)=GF(2^l) 上的一个非超奇异椭圆曲线. 由于 q 很小，我们很容易就可以确定所有可能的椭圆曲线 $y^2 + xy = x^3 + ax^2 + b$，$a, b \in \mathrm{GF}(q) = \mathrm{GF}(2^l)$，$b \neq 0$，及其曲线上的点数 $\#E(\mathrm{GF}(q)) = q + 1 - \beta$，$|\beta| \leq 2\sqrt{q}$ 且 β 为奇数.

步骤 2　再计算 GF(q) 上的任一扩域上的椭圆曲线的点数 $\#E(\mathrm{GF}(q^k)) = q^k + 1 - \beta_k$，其中 $\beta_k = a^k + b^k$，a, b 是方程 $1 - \beta_0 T + qT^2 = 0$ 的两个复根.

步骤 3　由于 GF(q) 是 GF(q^k)=GF(2^{lk}) 的一个子群，则 $\#E(\mathrm{GF}(q^k))$ 一定包含小因子 $\#E(\mathrm{GF}(q))$. 计算 factor = $\#E(\mathrm{GF}(q^k))/\#E(\mathrm{GF}(q))$，其中 k 选择为素数，这是因为若 $t|k$，则 $E(\mathrm{GF}(q^t)) \subseteq E(\mathrm{GF}(q^k))$.

步骤 4 令 $n=lk$. 判断 factor 为素数否？若 factor 为素数，则 $p_{E(\mathrm{GF}(q^n))}=\mathrm{factor}$. 再判断 $\gcd(p_{E(\mathrm{GF}(q^n))},2^{ni}-1)=1$ 成立否？ $(i=1,2,\cdots,\log(q^k)/8=lk/8)$ 若是，则该曲线不满足 MOV 条件，易受 MOV 攻击. 若否，则该椭圆曲线即为所求。

由于这样构造出的椭圆曲线满足安全曲线的三个条件：非超奇异、含大素因子和满足 MOV 条件，所以所求出的曲线是安全的椭圆曲线。

2.3 特征为 2 的域上椭圆曲线基点的选取

要建立椭圆曲线密码体制，必须找到一个循环子群，使该子群的阶包含大素因子 $p_{E(\mathrm{GF}(q^n))}$ ，一个最好的方法就是使该循环子群的阶就是大素因子 $p_{E(\mathrm{GF}(q^n))}$. 亦即是要找到阶为 $p_{E(\mathrm{GF}(q^n))}$ 的循环子群的生成元，该生成元即为所求的基点。

2.3.1 *求特征为 2 的域上椭圆曲线上的点* 求特征为 2 的域上椭圆曲线上的点，就是要找到满足方程 $y^2+xy=x^3+ax^2+b$ $(a,b\in \mathrm{GF}(2^n),b\neq 0)$ 的坐标对 (x,y), $x,y\in \mathrm{GF}(2^n)$. 利用随机选取法是不足取的，因为随机选取的坐标对 (x,y) 是曲线上的点的概率仅为 $\#E(\mathrm{GF}(2^n))/2^{2n}\approx 2^{-n}$ ，这在实际中是不可行的. 幸而由下面的定理我们可以受到启发。

定义 若 $\alpha\in \mathrm{GF}(q^n)$ ，则 α 相对于 $\mathrm{GF}(q^n)$ 的子域 $\mathrm{GF}(q)$ 的迹定义为

$$\mathrm{Tr}_{\mathrm{GF}(q)}^{\mathrm{GF}(q^n)}(\alpha)=\alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}},\text{简记为 }\mathrm{Tr}(\alpha)。$$

定理 2 (文献 [4] 定理 8.4): 若 $\alpha\in \mathrm{GF}(q^n)$, 则 $\mathrm{Tr}_{\mathrm{GF}(q)}^{\mathrm{GF}(q^n)}(\alpha)=0$, 当且仅当存在一个域元素 $\beta\in \mathrm{GF}(q^n)$ 使得 $\alpha=\beta-\beta^q$.

定理 3 (文献 [4] 定理 8.5)：设 $\alpha,\theta\in \mathrm{GF}(q^n)$ ，若

$$\beta=\alpha\theta^q+(\alpha+\alpha^q)\theta^{q^2}+\cdots+(\alpha+\alpha^q+\cdots+\alpha^{q^{n-2}})\theta^{q^{n-1}},$$

$$\text{则 }\beta-\beta^q=\alpha(\mathrm{Tr}(\theta)-\theta)-\theta(\mathrm{Tr}(\alpha)-\alpha).$$

在特征为 2 的域上，定理 2 保证了在 $\mathrm{Tr}_{\mathrm{GF}(q)}^{\mathrm{GF}(q^n)}(\alpha)=0$ 时，方程 $x^2+x=\alpha$ 在 $\mathrm{GF}(q^n)$ 上有解. 定理 3 说明了在 $\mathrm{Tr}_{\mathrm{GF}(q)}^{\mathrm{GF}(q^n)}(\alpha)=0$ 时，方程 $x^2+x=\alpha$ 在 $x\in \mathrm{GF}(q^n)$ 上的两个解为 β 和 $\beta+1$ ，其中 θ 为 $x\in \mathrm{GF}(q^n)$ 中迹为 1 的任一元素。

由此，我们可以得到求特征为 2 的域上的椭圆曲线上点的方法。

步骤 1 任选一个域元素 $\theta\in \mathrm{GF}(2^n)$ ，计算该元素的迹 $\mathrm{Tr}(\theta)$ ，判断 $\mathrm{Tr}(\theta)=1$ 否？若否，则重新选择 θ 直至其迹为 1 . 若 $\mathrm{Tr}(\theta)=1$ 则转步骤 2 .

步骤 2 任取 $x\in \mathrm{GF}(2^n)$ ，令 $A=x$, $B=x^3+ax^2+b$ ，则原方程变为 $y^2+Ay=B$. 再令 $y=Ax'$ ，则方程变为 $x'^2+x'=B/A^2$. 令 $\xi=B/A^2$ ，方程变为 $x'^2+x'=\xi$.

步骤 3 计算 ξ 的迹 $\mathrm{Tr}(\xi)$ ，判断 $\mathrm{Tr}(\xi)=0$ 否？否，转步骤 2 ，重新选择 $x\in \mathrm{GF}(2^n)$ ；是，转步骤 4 .

步骤 4 计算 $\beta=\xi\theta^2+(\xi+\xi^2)\theta^{2^2}+\cdots+(\xi+\xi^2+\cdots+\xi^{2^{n-2}})\theta^{2^{n-1}}$ ，则 β 和 $\beta+1$ 是方程 $x'^2+x'=\xi$ 的两个解. 计算 $y_1=A\cdot\beta$ 和 $y_2=A\cdot(\beta+1)$ ，则 (x,y_1) 和 (x,y_2) 即为域 $\mathrm{GF}(2^n)$ 上的曲线 $y^2+xy=x^3+ax^2+b$ 上的两个点，所求的两个点是互逆点 (两点相加即为椭圆曲线上的无穷远点 O) .

2.3.2 基点的选取　任取曲线上的一个点 P，计算 $p_{E(\mathrm{GF}(2^n))} \cdot P = O$? 若否，则重新选点；若是，则 P 即为所求的基点。其中 $p_{E(\mathrm{GF}(2^n))}$ 是 $\#E(\mathrm{GF}(2^n))$ 最大的素因子。

3 特征为 2 的域上安全椭圆曲线的一个具体实现

3.1 仿射平面中特征为 2 的域上椭圆曲线上的加法运算

设 $P=(x_1,y_1), Q=(x_2,y_2)$ 为椭圆曲线 E 上的任意两点

(1) $O+P=P+O=O$;

(2) $-O=O$;

(3) 若 $P\neq O$，则 $-P=(x_1,x_1+y_1)$；

(4) 若 $P\neq O, Q\neq O$ 且 $P\neq -Q$，则 $P+Q=(x_3,y_3)$ 如下给出：

(a) 点加运算：若 $P\neq Q$，

$$x_3=L^3+L+x_1+x_2+a,$$
$$y_3=L\cdot(x_1+x_3)+x_3+y_1,$$
$$L=(y_1+y_2)/(x_1+x_2)\ .$$

(b) 倍点运算：若 $P=Q$，

$$x_3=L^2+L+a,$$
$$y_3=x_1^2+(L+1)\cdot x_3,$$
$$L=x_1+y_1/x_1\ .$$

3.2 域 GF(2^2) 上的所有非超奇异椭圆曲线

域 GF(2^2) 上的所有非超奇异椭圆曲线的形式如下：

$$y^2+xy=x^3+ax^2+b,\qquad a,b\in \mathrm{GF}(2^2),\quad b\neq 0.$$

如果利用本原多项式 x^2+x+1 来构造域 GF(2^2)，则 GF(2^2) 可以表示为 GF(2)$[x]/(x^2+x+1)$。通过穷举法，我们可以把域 GF(2^2) 上的所有的椭圆曲线的阶计算出来，得到表 2。

表 2　域 GF(2^2) 上的所有的椭圆曲线及其阶

椭圆曲线的阶 $\#E(\mathrm{GF}(2^2))$	椭圆曲线方程的系数：(a,b)
2	(2,1)(3,1)
4	(0,2),(0,3),(1,2),(1,3)
6	(2,2) (2,3) (3,2) (3,3)
8	(0,1) (1,1)

3.3 利用 Weil 定理计算扩域上椭圆曲线的阶

现在选择阶 $\#E(\mathrm{GF}(2^2))=4$ 的任意一条曲线 $y^2+xy=x^3+2$，则它一定是非超奇异的。选择一个素数 79，计算 GF(2^2) 上的扩域 GF($(2^2)^{79}$) 上的椭圆曲线的点数。

$E(\mathrm{GF}(2^{158}))=4000\ 0\ 0\ 0\ 0\ e58c\ 53f\ f269\ 3464\ b85c$ (十六进制)

$=365375409332725729550922292183917789809461213276$(十进制).

$\#E(\mathrm{GF}(2^{158}))$ 除因子 $\#E(\mathrm{GF}(2^2))=4$ 外，另一个因子为

$$\mathrm{factor}=\#E(\mathrm{GF}(2^{158}))/\#E(\mathrm{GF}(2^2))=1000\ 0\ 0\ 0\ 0\ 3963\ 14f\ fc9a\ 4d19\ 2e17\ (\text{十六进制})$$
$$=913438523331814323877305730459794474523653033 19(\text{十进制}).$$

上述的因子经测试是一个 47 位 (十进制位) 的概率素数. 而且, 该素因子满足 MOV 条件: $\log(2^{158})/4 \approx 40$. 经验证, 对于 $\forall i \in \{1,2,\cdots,40\}$, $\gcd(\text{factor}, 2^{158i}-1)=1$ 都成立. 因此, 可认为域 $\mathrm{GF}(2^{158})$ 上的曲线 $y^2+xy=x^3+2$ 是一条足够安全的椭圆曲线.

3.4 椭圆曲线上基点的选取

由第 2.3 节中求基点的方法最终得到的一个基点 P 为

十六进制表示: (6cfe $cd57$ $b683$ 2$f4$ $d6d5$ $a877$ 7$df2$ 3$d1c$ 6$d7c$,

3$da6$ $ad80$ 371c 9afd 4905 $a748$ 9141 4852 54ac $a0ef$),

十进制表示: (949483154899876595995544725633614898976703 6,

351965474778075522461122561994822274188269363439).

综上可知, 所得到的安全的椭圆曲线的各个参数为

(1) 所基于的域为 $\mathrm{GF}(2^{158})$;

(2) 椭圆曲线方程: $y^2+xy=x^3+2$;

(3) 基点 $P=$(949483154899876595995544725633614898976703 6,

351965474778075522461122561994822274188269363439);

(4) 基点的级: order(P)=913438523331814323877305730459794474523653033 19.

4 结 论

本文运用 Weil 定理, 提出了一种有效地寻找安全椭圆曲线及其基点的方法. 该方法与传统的寻找好的椭圆曲线的 SEA 算法相比简单易行, 但得到椭圆曲线的个数较少. 这是因为子域所能取的扩域是有限的, 且还需保证扩域上的椭圆曲线的阶包含大素因子. 此外, 本文的附录还给出了在寻找安全椭圆曲线基点时所涉及的求扩域上的元素的迹的快速算法.

附录

扩域 $\mathrm{GF}((2^l)^k)$ 上的元素相对于 $\mathrm{GF}(2)$ 的迹的快速算法

按迹的定义可知:

$$\mathrm{Tr}_{\mathrm{GF}(2)}^{\mathrm{GF}(2^{lk})}(\alpha)=\alpha+\alpha^2+\alpha^{2^2}+\cdots+\alpha^{2^{l-1}}+\alpha^{2^l}+\alpha^{2^{l+1}}+\cdots$$
$$+\alpha^{2^{2l-1}}+\alpha^{2^{2l}}+\alpha^{2^{2l+1}}+\cdots+\alpha^{2^{lk-1}}.$$

由于扩域 $\mathrm{GF}((2^l)^k)$ 的特殊构造, 其上任一元素 α 相对于 $\mathrm{GF}(2)$ 的迹, 可以按下述方法快速求得:

(1) 首先求出扩域 $\mathrm{GF}((2^l)^k)$ 的元素 α 相对于子域 $\mathrm{GF}(2^l)$ 的迹 $\beta=\mathrm{Tr}_{\mathrm{GF}(2^l)}^{\mathrm{GF}(2^{lk})}(\alpha)=\alpha+\alpha^{2^l}+\alpha^{2^{(l\,2)}}+\alpha^{2^{(l\,3)}}+\cdots+\alpha^{2^{(l(k-1))}}$.

(2) 再求出 $\mathrm{GF}(2^l)$ 的元素 β 相对于子域 $\mathrm{GF}(2)$ 的迹

$$\gamma=\mathrm{Tr}_{\mathrm{GF}(2)}^{\mathrm{GF}(2^l)}(\beta)=\beta+\beta^2+\beta^{2^2}+\cdots+\beta^{2^{l-1}},$$

则 γ 即为所求.

现证明两种求迹的方法是等价的.

证明

$$\begin{aligned}
\mathrm{Tr}_{GF(2)}^{GF(2^{lk})}(\alpha) &= \alpha+\alpha^2+\alpha^{2^2}+\cdots+\alpha^{2^{l-1}}+\alpha^{2^l}+\alpha^{2^{l+1}}+\cdots \\
&\quad +\alpha^{2^{2l-1}}+\alpha^{2^{2l}}+\alpha^{2^{2l+1}}+\cdots+\alpha^{2^{lk-1}}, \\
\gamma &= \mathrm{Tr}_{GF(2)}^{GF(2^l)}(\beta)=\beta+\beta^2+\beta^{2^2}+\cdots+\beta^{2^{l-1}} \\
&= (\alpha+\alpha^{2^l}+\alpha^{2^{(l\cdot 2)}}+\alpha^{2^{(l\cdot 3)}}+\cdots+\alpha^{2^{(l(k-1))}}) \\
&\quad +(\alpha+\alpha^{2^l}+\alpha^{2^{(l\ 2)}}+\alpha^{2^{(l\ 3)}}+\cdots+\alpha^{2^{(l(k-1))}})^2 \\
&\quad +(\alpha+\alpha^{2^l}+\alpha^{2^{(l\ 2)}}+\alpha^{2^{(l\ 3)}}+\cdots+\alpha^{2^{(l(k-1))}})^{2^2}+\cdots \\
&\quad +(\alpha+\alpha^{2^l}+\alpha^{2^{(l\ 2)}}+\alpha^{(2^{(l\cdot 3)}}+\cdots+\alpha^{(2^{(lk-1)})})^{2^{l-1}}.
\end{aligned}$$

由于域的特征为 2，因此 $\forall\alpha,\beta\in GF(2^m)$, $(\alpha+\beta)^{2^r}=\alpha^{2^r}+\beta^{2^r}$，其中 m, r 为任意的正整数. 故

$$\begin{aligned}
\gamma &= (\alpha+\alpha^{2^l}+\alpha^{2^{(l\cdot 2)}}+\alpha^{2^{(l\cdot 3)}}+\cdots+\alpha^{2^{(l(k-1))}}) \\
&\quad +(\alpha^2+\alpha^{2^{l+1}}+\alpha^{2^{(l\cdot 2+1)}}+\alpha^{2^{(l\ 3+1)}}+\cdots+\alpha^{2^{l(k-1)+1}}) \\
&\quad +(\alpha^{2^2}+\alpha^{2^{l+2}}+\alpha^{2^{(l\ 2+2)}}+\alpha^{(2^{(l\ 3+2)}}+\cdots+\alpha^{2^{l(k-1)+2}}) \\
&\quad +\cdots+(\alpha^{2^{l-1}}+\alpha^{2^{l\cdot 2-1}}+\alpha^{2^{(l\cdot 3-1)}}+\alpha^{(2^{(l\ 4-1)}}+\cdots+\alpha^{2^{lk-1}}) \\
&= (\alpha+\alpha^2+\alpha^{2^2}+\cdots+\alpha^{2^{l-1}})+(\alpha^{2^l}+\alpha^{2^{l+1}}+\alpha^{2^{l+2}}+\cdots+\alpha^{2^{2l-1}}) \\
&\quad +(\alpha^{2^{2l}}+\alpha^{(2^{2l+1})}+\alpha^{2^{2l+2}}+\cdots+\alpha^{2^{3l-1}})+\cdots \\
&\quad +(\alpha^{2^{l(k-1)}}+\alpha^{(2^{l(k-1)+1})}+\alpha^{2^{l(k-1)+2}}+\cdot+\alpha^{2^{lk-1}}) \\
&= \mathrm{Tr}_{GF(2)}^{GF(2^{lk})}(\alpha).
\end{aligned}$$

证毕

分析 $\forall\alpha\in GF((2^l)^k)$，利用定义求其迹需要 $lk-1$ 次平方运算和 lk 次加法运算，而利用本文所提出的求迹的算法，需要 $l(k-1)$ 次平方运算和 $l+k-2$ 次加法运算.

参 考 文 献

[1] Menezes A, Okamoto T, Vanstone S A. Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Trans. on IT, 1993, IT-39(5): 1639–1646.

[2] Koblitz N. A Course in Number Theory and Cryptography, Beijing: Springer-Verlag World Publishing Corp. 1990, 150–170.

[3] Beth T, Schaefer F. Non supersingular elliptic curves for public key cryptosystems. Advances in Cryptology-EUROCRYPT'91, Berlin: Springer-Verlag, 1992, 317–327.

[4] McEliece J. Finite Field for Computer Scientists and Engineers, Boston: Kluwer Academic, 1987, 97–105.

FINDING SECURE ELLIPTIC CURVES OVER GF(2^n) AND THEIR BASE POINTS

Liu Shengli Zheng Dong Wang Yumin

(*National Key Lab. on ISN, Xidian University, Xi'an* 710071, China)

Abstract This paper systematically introduces how to find secure elliptic curves with the help of Weil theorem, and proposes an algorithm to find base points in the curves. Finally, an efficient method of finding the trace of any element in GF(2^{lk}), which is involved in the algorithm of finding base points, is given.

Key words Elliptic curve cryptosystem, Base point, Trace

刘胜利： 女，1974 年生，博士生，密码学专业，研究方向为信息理论安全及椭圆曲线密码体制.

郑 东： 男，1964 年生，博士生，密码学专业，研究方向为安全协议的分析与设计.

王育民： 男，1936 年生，教授，博士生导师，长期从事信息论、信道编码、密码学以及通信网的安全等方面的研究.