F_2^m上基于ONB的椭圆曲线加密软件的设计与实现*)

张险峰　秦志光　陈兴容　刘锦德

(电子科技大学计算机学院IBM技术中心　成都610054)

Design and Implementation of Elliptic Curve Encryption Based on ONB over F_2^m

ZHANG Xian-Feng　QIN Zhi-Guang　CHEN Xing-Rong　LIU Jin-De

(IBM Technology Center, College of Computer Science and Engineering, UEST of China, Chendu 610054)

Abstract　This paper comprehensively introduces the mathematics theory for elliptic curve encryption based on ONB over F_2^m, like the ONB denotation of element over F_2^m, the elliptic curve over F_2^m, and some computing rules. Based on the theoretical introduction, an ECC-based encryption scheme is designed. The mechanism for key exchange is described in details for further applications. Underlying the given theoretical analysis and protocol description, an ECC software is implemented. The software is characterized by excellent security as well as high efficiency.

Keywords　Network security, Optimal normal base(ONB), Encryption software, Elliptic curve cryptography(ECC)

1　引言

目前，椭圆曲线密码体制(Elliptic Curve Cryptography, ECC)被认为能比其他公钥体制提供更好的加密强度、更快的执行速度和更小的密钥长度。ECC的安全性基于椭圆曲线离散对数问题的难解性[1~3]。

在实际应用的ECC中，椭圆曲线采用的是基于有限域F_p或F_2^m的椭圆曲线群。F_p中的域元素为整数集合{0,1,2,…,p-1}，其中p为素数。域F_2^m中的域元素为m位二进制比特串，如域元素$(a_0\,a_1\cdots a_{m-1})$，其中$a_0,a_1,\cdots,a_{m-1}$为F_2上元素，即0或1。

F_2^m中的域元素通常有两种表示法[1~3]：第一种是多项式表示法，第二种是正规基表示法。前者通过域多项式基来表示，设域多项式基为集合$\{1,t,t^2,\cdots,t^{m-1}\}$，则域元素$(a_0\,a_1\cdots a_{m-1})$表示成多项式$a_{m-1}t^{m-1}+\cdots+a_1t+a_0$；后者是指集合$\{t,t^2,t^{2\wedge2},\cdots,t^{2\wedge(m-1)}\}(t\in F_2^m)$，集合中的元素是线性无关的，根据正规基表示法，有限域F_2^m的域元素$\alpha(a_0\,a_1\cdots a_{m-1})$表示为：$\alpha=\sum_{i=0}^{m-1}a_it^{2\wedge i}$，其中：$a_i\in\{0,1\}$。

在有限域F_2^m上进行乘法运算时，多项式基相对正规基表示法简单；但在该域上进行乘方运算时，多项式基相对正规基表示法困难[1,2]。

优化正规基(Optimal Normal Base, ONB)是一种特殊的正规基。基于ONB表示法的域元素在执行平方运算时非常高效，仅需对表示元素的矢量进行循环移位；在幂运算方面ONB表示法也比多项式表示法有效得多。虽然在域F_2^m中ONB表示法在元素表达的意义上不及多项式表示法直观，但由于该元素表示法能使计算机在此域中高效地进行运算，故在研究设计与实现椭圆曲线加密软件时，我们采用F_2^m作为基域，并用ONB表示法来表示域中的元素。

下面，本文首先对域F_2^m中元素的ONB表示法进行说明；然后描述和分析了域运算法则、域F_2^m上椭圆曲线及点的运算法则；在第4节中，对本软件的开发进行了一些设计考虑；第5、6节中，设计实现一个基于ECC的加密方案，并给出了应用实例；最后，是本文的结论及下一步的工作。

2　有限域F_2^m的ONB表示法及域运算法则

2.1　ONB表示法

设F_q^n表示F_q的扩域，对于F_q^n中的某个α，若它有如下形式的基：$\{\alpha,\alpha^q,\alpha^{q\wedge2},\cdots,\alpha^{q\wedge n-1}\}$，则$F_q^n$在$F_q$上的基被称作正规的。设$(a_0,a_1,\cdots,a_{n-1})$和$(b_0,b_1,\cdots,b_{n-1})$是域中元素A和B相应于$F_q$上的正规基的坐标向量。若C=AB，则C有坐标向量$(C_0,C_1,\cdots,C_{n-1})$，其中$C_K$是$a_i$和$b_j$的双线性型$(0\leqslant i,j\leqslant n-1)$。容易证明型$C_K$可由型$C_0$通过它所包含的变量的k次循环移位得到。令C(N)表示C_0中非零项的个数(其中N表示使用的正规基)，因而也是C_i的非零项的个数，其中$0\leqslant i\leqslant n-1$，从而C(N)满足不等式$C(N)\geqslant 2n-1$。若N使得等号成立，则称N为一个优化正规基，即ONB[4]。ONB使得乘法和乘方运算都比较容易。

对于每个有限域F_2^m，都存在正规基，但不一定存在ONB。当$m>1$且m不能被8整除时，可令T=1或T=2并按以下算法检验有限域F_2^m是否存在ONB[3]：

(1)$p=Tm+1$；

(2)若p不是素数，则不存在ONB；

(3)求k使$2^k\equiv1(\mathrm{mod}\ p)$；

(4)$h=Tm/k$；

(5)计算$d=GCD(h,m)$，GCD(h,m)表示h与m的最大公约数；

(6)若d=1，则存在ONB；否则不存在ONB。

对F_2上的m阶不可约多项式p(t)，如果在模p(t)的条件下，由向量$(1,t,t^2,\cdots,t^{m-1})$到向量$(t,t^2,t^{2\wedge2},\cdots,t^{2\wedge(m-1)})$的转移矩阵是可逆的，则称p(t)为正规多项式。有限域F_2^m的正规基表示法与一个m阶正规多项式相关，则该多项式称为这个基的域多项式。

*)本课题得到国防预研基金的资助。张险峰　博士生，主要研究方向：信息和网络安全。秦志光　教授，主要研究方向：网络安全、电子商务。陈兴容　硕士生，主要研究方向：密码学。刘锦德　教授，博导，主要研究方向：开放系统及其安全、中间件技术。

域 F_2^m 只存在两类 ONB[2]。当域 F_2^m 有 I 型 ONB 时，其域多项式可表示为 $p(t)=t^m+t^{m-1}+\cdots+t^2+t+1$；当域 F_2^m 有 II 型 ONB 时，则按以下的迭代公式计算 $p(t)=p_m(t)$：

$p_0(t)=1$，
$p_1(t)=t+1$，
…，
$p_{i+1}(t)=tp_i(t)+p_{i-1}(t)$，$i=1,\cdots,m$。

在以上每步计算中，多项式 $p_i(t)$ 的系数都进行模2的运算，因此，多项式 $p(t)$ 是最高次数为 m、系数属于 F_2 的整数多项式。

2.2 基于 ONB 的有限域 F_2^m 域运算法则

设有限域 F_2^m 的 ONB 为 $\{t,t^{2\wedge 2},\cdots,t^{2\wedge(m-1)}\}(t\in F_2^m)$，域元素 $a=(a_0\,a_1\cdots a_{m-1})$，$b=(b_0\,b_1\cdots b_{m-1})$。a 的 ONB 表示法为：$a=\sum_{i=0}^{m-1}a_i\beta^{2\wedge i}$，b 的 ONB 表示法为：$b=\sum_{i=0}^{m-1}b_i\beta^{2\wedge i}$。

2.4.1 *域元素加法* 域 F_2^m 中域元素 a 与 b 的和定义为：$a+b=(c_0\,c_1\cdots c_{m-1})$，这里 $c_i=(a_i+b_i)\bmod 2$。

2.4.2 *F_2^m 上的域元素平方及平方根运算* 对于域 F_2^m 中域元素 $a=\sum_{i=0}^{m-1}a_i\beta^{2\wedge i}$：

$$(a)^2=(\sum_{i=0}^{m-1}a_i\beta^{2\wedge i})^2=\sum_{i=0}^{m-1}a_i\beta^{2\wedge(i+1)}=\sum_{i=0}^{m-1}a_{((i-1)\bmod m)}\beta^{2\wedge i}=(a_{m-1}\,a_0\,a_1\cdots a_{m-2})$$

即域元素 a 的平方是域元素 a 对应的比特串循环右移一位的结果。

$$(a)^{\frac{1}{2}}=(\sum_{i=0}^{m-1}a_i\beta^{2\wedge i})^{\frac{1}{2}}=\sum_{i=0}^{m-1}a_i\,\beta^{2\wedge(i-1)}=\sum_{i=0}^{m-1}a_{((i+1)\bmod m)}\beta^{2\wedge i}=(a_1\,a_2\cdots a_{m-1}\,a_0)$$

即域元素 a 的平方根是域元素 a 对应的比特串循环左移一位的结果。

可见，在域元素用 ONB 表示时，可以非常高效地进行平方及平方根运算。

2.4.3 *F_2^m 的域元素乘法* 当 F_2^m 域元素用 ONB 表示时，其乘法法则由一个 m * m 的矩阵 M（称之为乘法矩阵）来表征，该矩阵的每个元素属于 F_2。设 ONB 对应的域多项式为：$p(t)=t^m+c_{m-1}t^{m-1}+\cdots+c_1t+c_0$，求该乘法矩阵的运算步骤如下[3]：

(1)设在模 p(t) 条件下，由向量 $(1,t,t^2,\cdots,t^{m-1})$ 到向量 $(t,t^2,t^{2\wedge 2},\cdots,t^{2\wedge(m-1)})$ 的转移矩阵为 A，其逆矩阵为 B，即 $B=A^{-1}$。

(2)设矩阵 C 为：

$$\begin{pmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\&&\cdots&&\\0&0&0&\cdots&1\\c_0&c_1&c_2&\cdots&c_{m-1}\end{pmatrix}$$

在 F_2 上计算矩阵 $D=ACB$，设 $D=[d_{ij}]_{m\times m}$，其中 $0\leqslant i,j\leqslant m-1$ 且为整数。

(3)设 $s_{ij}=d_{j-i,-i}$，下标在模 m 条件下计算。则乘法矩阵 M 为：

$$\begin{pmatrix}s_{0,0}&s_{0,1}&s_{0,2}&\cdots&s_{0,m-1}\\s_{1,0}&s_{1,1}&s_{1,2}&\cdots&s_{1,m-1}\\s_{2,0}&s_{2,1}&s_{2,2}&\cdots&s_{2,m-1}\\&&\cdots&&\\s_{m-1,0}&s_{m-1,1}&s_{m-1,2}&\cdots&s_{m-1,m-1}\end{pmatrix}$$

按上述步骤生成了乘法矩阵 M 后，设有限域 F_2^m 中进行乘法的两个域元素为：$x=(a_0a_1\cdots a_{m-1})$，$y=(b_0b_1\cdots b_{m-1})$，其乘法运算的结果为 $c=(c_0c_1\cdots c_{m-1})$，用 x_k,y_k 分别表示 $(a_0a_1\cdots a_{m-1})$，$(b_0b_1\cdots b_{m-1})$ 循环左移 k 位的比特串，则：

$c_k=x_kMy_k^{tr}$（其中 y_k^{tr} 表示 y_k 的转置）。

例如：$c_0=xMy^{tr}$（其中 y^{tr} 表示 y 的转置），根据上式可求出 c。

2.4.4 *F_2^m 上域元素逆元的求法* F_2^m 上的域元素可以表示为 F_2 上的多项式，故求域元素的逆可以用扩展欧几里得算法[3]。

同时，由于：$a=a^{2^m}$（这相当于将 a 的比特串 $(a_0\,a_1\cdots a_{m-1})$ 循环移位 m 次），因此 a 的逆元 $a^{-1}=a^{2^m-2}$。而 $2^m-2=2^{m-1}+2^{m-2}+\cdots+2$，故 $a^{-1}=a^{2^{m-1}}\times a^{2^{m-2}}\times\cdots\times a^2$，因此也可通过 (m-1) 次乘方和乘法运算求出 a^{2^m-2}，也就求出了 a^{-1}。

3 有限域 F_2^m 上的椭圆曲线及点的运算法则

3.1 有限域 F_2^m 上的椭圆曲线

有限域 F_2^m 的椭圆曲线方程通常约定为：$E:y^2+xy=x^3+ax^2+b$，其中 $a,b\in F_2^m$。当 $b\neq 0$ 时，椭圆曲线 E 包含所有满足方程的点 $(x,y)(x,y\in F_2^m)$ 加上一个称为无限远点 0 构成一阿贝尔群，称为椭圆曲线群。只要指定域 F_2^m 上一个不可约的 m 次的非零多项式 f(x)，即可确定椭圆曲线上的点。

根据 IEEE P1363标准，椭圆曲线常用一个七元组表示：$T=(m,f(x),a,b,G,n,h)$。其中：m 决定了有限域 F_2^m，可根据安全级的需要指定 m 的大小。实际应用的基于 ONB 的 ECC 对 m 有所约束，$m\in\{113,131,163,193,233,239,283,409,571\}$；a、b 确定了椭圆曲线方程 E；G 是 E 的基点，满足 $nG=0$，其中 n 为 G 的阶，整数 h 为公因子，$h=\#E(F_2^m)/n$，其中 $\#E(F_2^m)$ 为 $E(F_2^m)$ 上点的总数[3]。

当取 $a=1,b=1$ 时，椭圆曲线方程为：$y^2+xy=x^3+x^2+1$。此类椭圆曲线为 Koblitz 椭圆曲线，它能特别有效地执行，而且尚无数学发现证明随机产生的椭圆曲线的 ECDLP 比 Koblitz 椭圆曲线的 ECDLP 更难[1,2]。

3.2 椭圆曲线点的运算法则

(1)*点的加减法* 若点 $P=(x_P,y_P)\in E$，则其逆元 $-P=(x_P,x_P+y_P)$。对所有 $P\in E$，$P+(-P)=0$，$P+0=0+P=P$。若点 $Q=(x_Q,y_Q)\in E$ 且 $Q\neq -P$，设 $P+Q=R=(x_R,y_R)$，则：

若 $P=Q$，有 $x_R=x_P^2+\frac{b}{x_P^2}$，$y_R=x_P^2+(x_P+\frac{y_P}{x_P})x_R+x_R$；

若 $P\neq Q$，有 $x_R=(\frac{y_P+y_Q}{x_P+x_Q})^2+(\frac{y_P+y_Q}{x_P+x_Q})+x_P+x_q+a$，$y_R=(\frac{y_P+y_Q}{x_P+x_Q})(x_P+x_R)+x_R+y_P$；

对定义在有限域 F_2^m 中 E 上两点之差 $P-Q=P+(-Q)$，即点 P 与 Q 之差为 P 加上 Q 的逆元 (-Q)，其运算法则与两点之和一样。

(2)*点的标乘* 设椭圆曲线 E 上一点 P，其阶为 n，即 $nP=0$，k 为整数且 $1\leqslant k\leqslant n$，计算 E 上另一点 Q，$Q=kP$ 的运算称为点 P 的标乘。

通过上面定义的点加运算，在椭圆曲线群上可以由点 P 计算得到 2P、3P 直到 kP，但由于 $k\in F_2^m$，因此 k 可表示为：$k=\sum_{i=0}^{h-1}k_i2^i$，其中 h，i 为整数，且 $1\leqslant h\leqslant m$，$k_i\in\{0,1\}$，因此：

$$kP=\sum_{i=0}^{h-1}k_i2^iP=2(\cdots2(2k_{h-1}P+k_{h-2}P)+\cdots)+k_0P$$

因此此方法要求 h 次自加和 w_k-1次加法，其中 w_k 表示 k 的二进制表示法中1的个数[5]。

(3)*点的求取* 对应于 E 的基点和公钥都是 E 上的点，

它们的横、纵坐标都为 F_2^m 上的域元素。为了生成这些点，常用的方法是首先生成一域元素，并将其假定为某点的横坐标(x)，然后由椭圆曲线方程求出相应的纵坐标(y)。设 E 的方程为：$y^2+xy=x^3+a_2x^2+a_6$，求与已知横坐标 x 对应的的椭圆曲线点的步骤为：

(a)由 x 计算出 $x^3+a_2x^2+a_6$ 的值，设值为 b；

(b)解方程 $y^2+xy=b$，即解形如 $y^2+xy+b=0$ 的方程。

在有限域 F_2^m 上解形如 $y^2+xy+b=0$ 方程的方法和实数域上的解法不同，其解法如下：

(a)令 $y=xz$，则原方程变形为 $z^2+z+b/x^2=0$；

(b)因为在有限域 F_2^m 中，元素加法的运算是对应比特的异或运算，因此方程 $z^2+z+b/x^2=0$ 等价于 $z^2=z+b/x^2$，也即 $z^2=(z^{\frac{1}{2}})^2+((b/x^2)^{\frac{1}{2}})^2$。又因为在有限域 F_2^m 中域元素 u 和 v，有 $(u+v)^2=u^2+v^2$，因此原方程等价于：$z=z^{1/2}+(b/x^2)^{1/2}$。也即：$z^{1/2}=z+(b/x^2)^{1/2}$；

(c)设 $z=(z_0\,z_1\cdots z_{m-1})$，$k=(b/x^2)^{1/2}=(k_0\,k_1\cdots k_{m-1})$，方程又等价于 $(z_{m-1}z_0\,z_1\cdots z_{m-2})=(z_0\,z_1\cdots z_{m-1})+(k_0\,k_1\cdots k_{m-1})$。

因此，只要先确定 z 的一个 bit，则可按上述等式求出 z 的其余 bit 位，相应地求出 y。

当然，对一个随机的域元素，它不一定是给定椭圆曲线上一点的横坐标。此时可对域元素1，再判断是否为椭圆曲线上一点的横坐标，若不是，继续递增，直到求出相应的点[3]。

4 设计考虑

在设计中，我们采用基于 ECC 的公钥方案实现共享密钥的生成，然后在此密钥作用下应用对称密钥算法来对数据进行加密。在基于 ECC 的公钥方案设计中，需要确定使用的椭圆曲线、椭圆曲线所基于的有限域 F_2^m 和密钥交换协议。为了保证数据的完整性，我们还将采取消息认证码(MAC)方案。

4.1 椭圆曲线的选择

目前，m 取160左右的数时基于有限域 F_2^m 的 ECC 可有效抵抗攻击者的穷举攻击，根据 IEEE P1363标准，我们取 m=163，从而也确定了椭圆曲线所基于的有限域 F_2^{163}。在选择椭圆曲线方程：$y^2+xy=x^3+a.x^2+b$，$a,b\in F_2^m$ 时，为了提供更大的灵活性，我们考虑随机生成参数 a 和 b，但随机产生的椭圆曲线有可能是超奇异曲线或不规则椭圆曲线，会导致安全上的漏洞，因此，需要对生成的曲线进行验证[1,3]。

4.2 基于 ECC 的密钥交换协议

为有效实现通信双方共享密钥的生成，在设计中，我们采用基于 ECC 的 Diffie-Hellman 密钥交换协议[3]。设基于有限域 F_2^m 的椭圆曲线方程为：$y^2+xy=x^3+a.x^2+b$，基点为 G。G 的阶为 n。n 为素数。设欲秘密通信的用户为 U 和 V，U 的公私钥对为(Q_U、d_U)，V 的公私钥对为(Q_V、d_V)。基于 ECC 的 Diffie-Hellman 协议规程如图1所示。

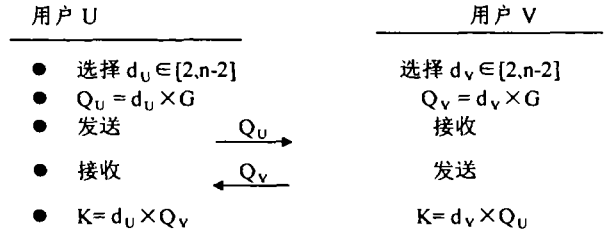

图1 基于 ECC 的 Diffie-Hellman 协议

上图中，K 为椭圆曲线 E 上的点。所以通信双方通过计算对方的公钥及本方的私钥得到了曲线上一相同的点。此点的一部分(x 坐标或 y 坐标)可进一步生成用于加密原消息的会话密钥。对于非法截取信息者，仅仅知道 Q_U、Q_V 和基点 G，他无法得到点 K，因为这相当于从 Q_U、Q_V 和基点 G 中得到 d_U 或 d_V，这相当解 ECDLP 的困难问题。

5 加密方案的设计

基于以上的说明和分析，我们确定了以下设计方案(为说明方便，我们假设需秘密通信的双方为服务器和客户)：

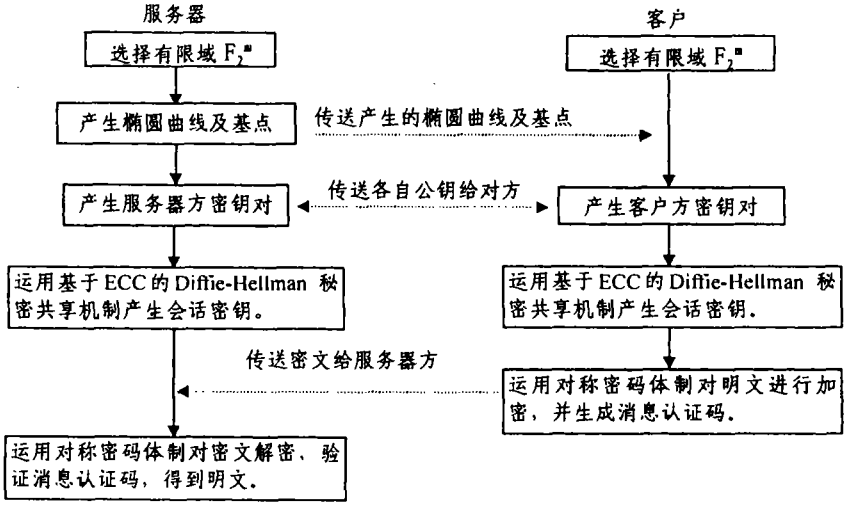

图2 加密方案逻辑流程图

(1)通信双方确定使用的有限域 F_2^m；

(2)服务器产生双方共用的椭圆曲线和基点，并将产生的椭圆曲线和基点传送给客户；

(3)双方交换公钥，然后运用基于 ECC 的 Diffie-Hellman 协议实现共享密钥的产生；

(4)在该共享秘密的作用下，运用对称密钥加密算法(异或加密算法、DES、IDEA、3DES 加密算法或)来完成秘密信息的传输。为了保证加密信息的完整性，本方案还考虑采用消息认证码机制对明文消息进行认证。

本方案执行的逻辑流程见图2。

6 实现及应用

在加密软件的实现中，我们选择的对称加密算法是异或

(下转第101页)

信网的投资，也保护了现有因特网上传统路由器的投资，又实现了两者的融合并向宽带分组化网络平滑演进和升级，使网络运营商能在业务量快速增长和QoS要求的外部因素、网络资源优化的内部因素间找到了合适的平衡点。因此，MPLS已经发展成为一种被普遍认同的理想的骨干网技术。在MPLS网络上构建的VPN，由于标记堆栈的运用，使得VPN具有了很好的可扩展性，另外，MPLS在流量工程方面的优势，将会为VPN QoS问题的解决提供良好的解决方案。

IPSec是IETF为了解决Internet没有任何安全保障的现实，经过几年的努力，开发出来的一种基于IP协议层的网络安全体系结构。IPSec提供了一种标准的、健壮的和内容广泛的安全机制，通过对网络层IP协议的扩展，增加了安全协商、数据包和通信流的加密、数据完整性和数据来源认证以及面向主机的访问控制等安全措施，为IP及上层协议(如TCP和UDP)提供安全保证。由于IPSec提供了高级别的安全保障，加上它是IETF制定的标准，所以，IPSec是解决VPN数据安全和网络安全的首要选择。

GRE的突出特点就是它的通用性，适合任何的网络协议。它本身并不具有传送能力，但它是传送协议和被传送协议之间的桥梁，它使得在任何网络环境下，都能够实现隧道技术，实现数据包的透明传输。例如，它能实现在IP上封装一个IP载荷数据包。

IP-in-IP的特点就是简单，而且它直接利用IP协议的ICMP消息，实现隧道的建立和维护，不需要额外的开销。它的局限性就是许多功能都要依赖于IP协议，制约了它的使用。

L2TP最显著的作用就是将NAS服务器与第2层链路设备分离，不再要求NAS服务器必须是第2层链路终端。由于L2TP可以建立在ATM、FR或IP网络上，因此NAS服务器可以是ATM网络、FR网络或IP网络上的任何一台主机。对VPN而言，L2TP是实现VPDN(虚拟专用拨号网)[10]的重要技术，已经在电信网中广泛使用。

经过以上的分析可知，各种隧道技术的功能差异显著，优势明显，如MPLS VPN有良好的可扩展性，IPSec能提供高级别的安全保证等，所以，结合它们各自的优势是势在必行，可以看出，VPN的发展有这样的趋势：(1)在MPLS网络上构建VPN；(2)利用MPLS的流量工程优势实现VPN的QoS保证；(3)通过IPSec实现VPN的数据安全和网络安全；(4)远程访问企业网采用L2TP隧道技术。

结束语 通过对比分析，不同的隧道技术各有特点，功能差异比较大，所以，希望在VPN中只采用一种隧道技术是不可能的，VPN领域中势必是各种隧道技术共存，特别是MPLS、IPSec和L2TP之间的相互融合有可能会成为VPN发展中的一个重要研究方向。本文只对相关的隧道技术进行了宏观上的分析比较，具体的融合方案有待进一步研究。

参考文献

1 Callon R, Suzuki M, Gleeson B, et al. A Framework for Provider Provisioned Virtual Private Networks. Internet-draft (draft-ietf-ppvpn-framework-01.txt), July 2001

2 Rosen E, Viswanathan A, Callon R. Multiprotocol Label Switching Architecture. RFC3031, Jan. 2001

3 Hanks S, Li T, Farinacci D, et al. Generic Routing Encapsulation (GRE). RFC1701, Oct. 1994

4 Kent S, Atkinson R. Security Architecture for the Internet Protocol. RFC2401, Nov. 1998

5 Simpson W. IP in IP Tunneling. RFC1853, Oct. 1995

6 Townsley W, Valencia A, Rubens A, et al. Layer Two Tunneling Protocol "L2TP". RFC2661, Aug. 1999

7 Andersson L, Doolan P, Feldman N, et al. LDP Specification. RFC3036, Jan. 2001

8 Braden R, Zhang L, Berson S, et al. Resource ReSerVation Protocol (RSVP) --Version 1 Functional Specification. RFC2205, Sep. 1997

9 Rekhter Y, Rosen E C. Carrying Label Information in BGP-4. Internet-draft (draft-ietf-mpls-bgp4-mpls-05.txt), Jan. 2001

10 Gleeson B, Lin A, Heinanen J, et al. A Framework of IP Based Virtual Private Networks. RFC2764, Feb. 2000

(上接第130页)

加密算法，加密数据分组长度为1024比特。选定的消息认证码(MAC)方案是HMAC_SHA-1_160。

F_{2^m}上基于ONB的椭圆曲线加密软件的实现，归根结底是通过基于ONB的F_{2^m}上的域元素运算、椭圆曲线点的运算、点及域元素间的转换等基本算法来实现上面提出的加密方案。这些基本算法在第2、3节已进行了说明和分析。

实现中，我们采用Turbo C 2.0作为开发工具，并将开发的软件以动态链接库(ECC.dll)的形式提供给用户使用。目前，该软件包已应用在成电领先软件有限公司研发的"用户身份识别"项目中，其基本思想是在客户端通过指纹传感器采集用户的活体指纹，然后通过该加密软件包将指纹信息加密传输到服务器端，最后在服务器端解密指纹信息并进行匹配，达到身份认证的目的。通过实际测试，该软件的安全性、运行效率完全合乎要求。

结束语 由于椭圆曲线密码体制与其他公开密码体制相比，在安全性和执行效率上具有独特的优势，因此基于ECC的安全应用正成为密码学界研究的热点。

本文设计的加密软件既保持了ECC的安全性，同时具有对称密钥加密体制的速度。我们下一阶段的工作：一是对开发的软件包进行严格的测试；二是从事基于ECC的门限密码体制的研究。由于门限密码体制一般采用同态密码算法(如RSA)来实现，因此基于ECC的门限密码体制研究中尚有许多难点需要解决。

参考文献

1 张险峰，秦志光，刘锦德. 椭圆曲线加密体制的性能分析. 电子科技大学学报，2001

2 Ceiticom Corporation Whitepaper. Canada: Ceiticom Corporation, 1997

3 IEEE P1363. Standard Specifications for Public Key Cryptography Draft Version 13, 1999

4 Agnew G B, Mullin R C, Vanstone S A. An implementation of elliptic curve cryptosystems over $F_{2^{155}}$. IEEE journal on selected areas in communications, 1993, 11(5): 804～813

5 Lopez J, Dahab R. An O verview of Elliptic Curve Cryptography. http://citeseer.nj.nec.com/333066.html

6 Menezes A J. Elliptic Curve Public Key Cryptosystems. USA: Kluwer Academic Publishers, 1993

7 Desmedt Y. Some Recent Research Aspects of Threshold Cryptography. http://www.cs.fsu.edu/~desmedt/ISW97.ps