基于环 Z_n 上圆锥曲线上的 A-EKE 协议及其应用

郝思佳[1] 方颖珏[2] 王 标[1] 邬静阳[3]
(国际关系学院信息科技系 北京 100091)[1] (深圳大学数学与计算科学学院 深圳 518060)[2]
(总装备部 63956 部队)[3]

摘 要 提出了一个基于环 Z_n 上圆锥曲线用 ElGamal 签名算法实现的 A-EKE 协议并给出了方案的数值模拟。方案具备 A-EKE 协议、ElGamal 签名算法和环 Z_n 上圆锥曲线的组合优势，A-EKE 协议同时使用对称和公钥密码算法为计算机网络基于口令的身份认证系统提供了安全性和鉴别性，在通信主机上存储口令的单向哈希值而非口令明文，并在扩充部分要求用户发送一条含有口令明文的加密消息来验证身份，使得攻击者即使获得了口令哈希值也无法向主机冒充用户；用 ElGamal 签名算法实现 A-EKE，协议加强了方案的健壮性；方案能够能够抵抗主动攻击，重放攻击，中间人攻击，保护口令不受离线字典攻击和破坏口令文件的攻击。方案运算在环 Z_n 上的圆锥曲线上，综合利用了大数分解的困难性和环上圆锥曲线群上离散对数问题的困难性，从而增强了该方案的安全性，且具有明文嵌入方便、运算速度快、更易于实现等优点，尤其是标准二进制的引入能够节约 1/4 计算量，对于工程实现具有现实意义。

关键词 剩余类环 Z_n，圆锥曲线，EKE，A-EKE，标准二进制
中图法分类号 TP309.7 **文献标识码** A

Applications of A-EKE Protocol with ElGamal Signature Scheme Based on the Conic Curve over Z_n

HAO Si-jia[1] FANG Ying-jue[2] WANG Biao[1] WU Jing-yang[3]
(Department of Information Technology, University of International Relations, Beijing 100091, China)[1]
(College of Mathematics and Computational Science, Shenzhen University, Shenzhen 518060, China)[2]
(63956Troops, General Armament Department, China)[3]

Abstract This paper proposed a scheme in which A-EKE is formed on the basis of conic curve over residue class ring Z_n using ElGamal signature algorithm, and presented the numerical simulation of the scheme. This scheme has combining advantages: A-EKE Protocol using a combination of asymmetric(public-key) and symmetric(secret-key) cryptography provides security and identification for communication on computer network. A-EKE allows hosts not to store cleartext passwords, and thus can prevent the attacker from mimicking the user to the host. Implementing the scheme using ElGamal signature algorithm also strengthens the scheme. The scheme can secure against active attack, overlay attack, man-in-the-middle attack, off-line dictionary attack and password profile compromise. Comprehensively using the difficulties in factorizing large integer and computing discrete logarithm with Conic Curve over Z_n, the security of this scheme is increased. For the facility of plaintext embedding and the computing of rank and point on conic $C_n(a,b)$, the scheme has the advantages of speedy operation and easy realization, especially by using the NAF. These advantageous properties of the schemes have pragmatic significance for the design and realization of secure and efficient identity authentication and key negotiation system.

Keywords Residue class ring Z_n, Conic curve, EKE, A-EKE, NAF

1 引言

基于口令的身份认证系统是当前网络系统安全中的重要技术之一。用户自己选择的口令通常易于记忆，但也因此容易遭到口令猜测攻击。1992 年，Bellovin 和 Merritt 提出了加密密钥交换协议，即 EKE 协议，能够保护口令不受离线字典攻击。1993 年，针对 EKE 协议需要双方主机知道口令明文的缺陷，Bellovin 和 Merritt 于又提出了扩充的 EKE 协议，即 A-EKE 协议，它为基于口令的身份认证系统选择特殊的单项哈希函数来存储口令值，能够有效抵抗字典攻击和破坏口令文件的攻击。

口令认证系统不仅需要安全性，还需要高效性。基于环 Z_n 上圆锥曲线的公钥密码体制，除了保留椭圆曲线上的原有优点外，还具有明文嵌入方便、运算速度快、更易于实现等优点，在群元素的整数倍计算过程中，引入标准二进制，比著名的“平方-和-乘法”算法节约近 1/4 的计算量，并被证明无法

郝思佳(1986－)，女，硕士生，主要研究方向为信息安全，E-mail：haosijia929@163.com；方颖珏(1978－)，女，博士，讲师，主要研究方向代数学、信息安全，E-mail：joyfang@szu.edu.cn(通信作者)；王 标(1979－)，男，博士，副教授，主要研究方向为信息安全、风险评估；邬静阳(1986－)，助理工程师，主要研究方向为信息安全。

再改进[1]。

本文重点研究了基于环 Z_n 上圆锥曲线用 ElGamal 签名算法实现的加强的 A-EKE 协议，通过数值模拟验证了该方案的可行性，可将其应用在基于口令认证的计算机系统中，以保护用户的隐私安全。

2 预备知识

2.1 环 Z_n 上的圆锥曲线 $C_n(a,b)$

环上圆锥曲线的定义和性质详见文献[2,3]。设 Z_n 是模 n 的剩余类环，Z_n 上的圆锥曲线 $C_n(a,b)$ 是同余方程：

$$y^2\equiv ax^2-bx(\bmod n) \tag{1}$$

在 Z_n 上解 (x,y) 的集，这里 $n=pq$，其中 p、q 为两个不同的奇素数，$(a,n)=(b,n)=1$。

显然 $O=(0,0)\in C_n(a,b)$。记 $C_n(a,b)$（即同余式(1)的解集）为：

$$C_n(a,b)=\{(x,y)\in Z_n\times Z_n \mid y^2\equiv ax^2-bx\equiv 0(\bmod n)\}$$

文献[2]定义了加法⊕，证明定理：环 Z_n 上的圆锥曲线 $(C_n(a,b),\oplus)$ 构成一个有限交换群。

同时，式(1)的解 $C_n(a,b)=C_1\cup C_2\cup C_3\cup O$。其中：

$C_1=\{P_1(t)=(b(a-t^2)^{-1},bt(a-t^2)^{-1},(a-t^2,n)=1,\forall t\in Z_n\}$

$C_2=\{P_2(t)=(pp^{-1}b(a-t^2)^{-1},pp^{-1}bt(a-t^2)^{-1},(a-t^2,q)=1,\forall t\in Z_n,pp^{-1}\equiv 1(\bmod q),(a-t^2)(a-t^2)^{-1}\equiv 1(\bmod q)\}$

$C_3=\{P_3(t)=(qq^{-1}b(a-t^2)^{-1},qq^{-1}bt(a-t^2)^{-1},(a-t^2,p)=1,\forall t\in Z_n,qq^{-1}\equiv 1(\bmod p),(a-t^2)(a-t^2)-1\equiv 1(\bmod p)\}$

显然，$\#C_n(a,b)=|C_1|+|C_2|+|C_3|+1$，$|C|$ 表示 C 的阶。

由于同于式(1)的解集等价于同余方程组：

$$\begin{cases}y^2\equiv ax^2-bx(\bmod p)\\ y^2\equiv ax^2-bx(\bmod q)\end{cases}$$

的解集，对于 $C_n(a,b)$ 上每一个点 $M=(x,y)\in C_n(a,b)$ 利用中国剩余定理能被唯一表示成一对 $[M_p,M_q]=[(x_p,y_p),(x_q,y_q)]$，其中 $M_p\in C_p(a,b)$，$M_q\in C_q(a,b)$。

$x\equiv x_p(\bmod p)$，$x\equiv x_q(\bmod q)$

$y\equiv y_p(\bmod p)$，$y\equiv y_q(\bmod q)$

通过这个对应关系，$C_n(a,b)$ 与 $C_p(a,b)\times C_q(a,b)$ 之间存在一一对应关系。因此我们可以十分方便地利用 $C_p(a,b)$ 和 $C_q(a,b)$ 的阶来得到 $C_n(a,b)$ 的阶。显然有：

命题 1[2]

1) 当 $\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)=-1$ 时，$\#C_n(a,b)=(p+1)(q+1)$；

2) 当 $\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)=1$ 时，$\#C_n(a,b)=(p-1)(q-1)$；

3) 当 $\left(\frac{a}{p}\right)=1,\left(\frac{a}{q}\right)=-1$ 时，$\#C_n(a,b)=(p-1)(q+1)$；

4) 当 $\left(\frac{a}{p}\right)=-1,\left(\frac{a}{q}\right)=1$ 时，$\#C_n(a,b)=(p+1)(q-1)$；

这里 $\left(\frac{a}{p}\right),\left(\frac{a}{q}\right)$ 表示勒让德符号。

命题 2[3] $C_n(a,b)$ 上通过映射和坐标定义的两种加法是一致的。

命题 3[3] $n=pq$，p、q 是两个不同的大素数，$\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)=-1$，$p+1=2r$，$q+1=2s$，其中 r，s 是素数，有：

1) 当 $a-b\equiv 1(\bmod n)$ 时，则：

$$G=\begin{cases}P_1(1)，\text{如果}(1,1)\text{是}C_p(a,b)\text{的生成元或}\\ \quad(1,1)\text{是}C_q(a,b)\text{的生成元}\\ P_1(a)，\text{如果}(1,1)\text{是}C_p(a,b)\text{的}r\text{阶元或}\\ \quad(1,1)\text{是}C_q(a,b)\text{的}s\text{阶元}\end{cases}$$

2) 当 $a-b\equiv 4(\bmod n)$ 时，则：

$$G=\begin{cases}P_1(2)，\text{如果}(1,2)\text{是}C_p(a,b)\text{的生成元或}\\ \quad(1,2)\text{是}C_q(a,b)\text{的生成元}\\ P_1\left(\frac{a}{2}\right)，\text{如果}(1,2)\text{是}C_p(a,b)\text{的}r\text{阶元或}\\ \quad(1,2)\text{是}C_q(a,b)\text{的}s\text{阶元}\end{cases}$$

上述命题 2 和命题 3 为环上圆锥曲线上密码体制的实现奠定了应用基础。

在密码算法的实现过程中，通常 p、q 均取大素数，此时可假定运算过程均在 C_1 中进行（若运算过程出现在 C_2 或 C_3 中，可得 n 的分解，故这种可能性极小），与 $C_P(a,b)$ 中的运算类似，在 C_1 中的计算过程，可用点的参数表示来进行：设 $P_1(t_1)\in C_1$，$P_1(t_2)\in C_1$，则 $P_1(t_1)\oplus P_1(t_2)=P_1(t_3)$，其中：

$$t_3=\begin{cases}\frac{t_1t_2+a}{t_1+t_2}, & (t_1+t_2,n)=1\\ \infty, & t_1+t_2=0\end{cases}$$

2.2 EKE 协议研究

2.2.1 基本 EKE 协议

Steven Bellovin 和 Michael Merritt 设计了加密密钥交换(EKE)协议[4]。它同时使用对称和公开密钥密码实现密钥的协商、传递以及用户身份认证，在这个方案中，用户双方共享一个口令值作为对称密钥，并用该口令值加密随机产生的公开密钥，然后通过互相交换加密的认证信息来确定对方的身份。

Alice 和 Bob（可以是两个用户，一个用户和主机，等）共享一个口令 P，利用这个协议，他们能相互鉴别并产生一个公共会话密钥 K。

1) A 产生一个随机公开密钥 E_A，并将口令 P 作为对称密钥系统的密钥来加密公钥 E_A，结果为 $P(E_A)$。A 向 B 发送：$A,P(E_A)$。A 是以明文形式传送的 Alice 的名字。

2) B 知道共享的口令 P，他解密这个消息得到 $P^{-1}(P(E_A))=E_A$，然后产生一个随机秘密密钥 K，并用公钥 E_A 和 P 对它加密，得到 $P(E_A(K))$。B 发送给 A：$P(E_A(K))$。

3) A 用 P 和 D_A 解密此消息得到 K，然后产生一个特殊的质询消息 $challenge_A$，并用 K 对其加密然后发送给 B：$K(challenge_A)$。

4) B 解密消息得到 $challenge_A$，并也产生一个特殊的质询消息 $challenge_B$，然后将这两条消息用密钥 K 进行加密并发送给 A：$K(challenge_A,challenge_B)$。

5) A 解密消息得到 $challenge_A$ 和 $challenge_B$，然后将 $challenge_A$ 与她之前发送给 B 的 $challenge_A$ 进行比较，如果一样，A 就用 K 加密 $challenge_B$ 然后发送给 B：$K(challenge_B)$。

6)B解密消息得到 challenge$_B$，并将 challenge$_B$ 与他之前发给 A 的 challenge$_B$ 进行比较，如果相同，这个协议就完成了。也就是说，如果从第 3 步到第 6 步的质询响应协议是成功的，在第 3 步到第 5 步 *Alice* 证实了 *Bob* 知道 K，第 4 步到第 6 步 *Bob* 证实了 *Alice* 知道 K，于是双方成功地进入了会话阶段，可以用对称密钥系统和会话密钥 K 对会话内容进行保护[4]。

通过发送随机质询消息的形式，协议能够抵抗重放攻击。此外，由于 E_A 和 K 都是从很大的密钥空间中随机选取的，攻击者无法证实对口令 P 的猜测，因此它们能够抵抗对口令的字典攻击。

2.2.2 A-EKE(扩充的 EKE)协议

在基本 EKE 协议中，共享口令由一个可信的密钥分配中心通过网络传递给通信双方，并以明文形式存储在主机中，当通信双方用口令在网络上交换信息协商会话密钥时，EKE 协议可以保护口令不受字典攻击。但文献[5,6]指出，让大部分主机以明文形式或可以恢复的密文形式存储口令值是不合适的，最好是存储口令 P 的单项哈希函数值 $H(P)$。

在 A-EKE 协议中，只有用户知道口令 P，主机是不知道的，主机仅存有 P 的单向哈希函数值 $H(P)$，而且无法通过 $H(P)$ 推出 P。主机通过计算用户键入的 P' 的单向散列值 $H(P')$ 并将其与存储的哈希值进行比较来验证 P' 的真实性。协议双方用 $H(P)$ 值来代替 EKE 协议中的 P 值进行密钥交换。

在某些特殊情况下 $H(P)$ 可能遭到攻击，在用户与单独的主机进行通话的情形中，攻击者如果得到了 $H(P)$，就能够对主机冒充用户。针对这种情况，A-EKE 协议要求用户必须另外发送一条加密消息 $K[F(P,K)]$ 来扩充 EKE 协议，使得攻击者即使获得了 $H(P)$ 也无法向主机冒充用户。$F(P,K)$ 是一个有关口令和协商好的会话秘钥的单向函数。这个值连同 $H(P)$ 和会话密钥一起通过计算 $T(H(P),F(P,K),K)$ 的真伪来验证用户的身份。$T()$ 只有当真正的口令 P 被用来计算 $H(P)$ 和 $F(P,K)$ 时才是正确的。

A-EKE 协议的前 5 步只是将 EKE 中的 P 换成了 $H(P)$。在扩充部分，用户 A 发送 $K[F(P,K)]$ 给主机 B，B 收到 $K[F(P,K)]$ 后解密得到 $F(P,K)$，如果计算出 $T(H(P),F(P,K),K)$ 的值为真，那么协议就圆满完成了。

值得注意的是，攻击者从主机得到 H(P)后仍能够向用户冒充主机。

3 基于环 Z_n 上圆锥曲线用 ElGamal 签名算法实现的 A-EKE 协议

EKE 协议最适合使用指数密钥交换[4]，会话密钥 K 由协议双方共同产生，因而能够抵抗主动攻击。可以使用数字签名算法来实现 A-EKE 协议的扩充部分。用形如 $S_X(Y)$ 的数字签名来实现 $F(P,K)$，对 Y 进行数字签名的私钥是从 X 导出的。于是 $K[F(P,K)]$ 就变为 $K[S_P(K)]$，可知对 K 进行数字签名的私钥 S_P 是从 P 值导出的。主机收到 $K[S_P(K)]$ 后解密得到 $S_P(K)$，当且仅当 $V_P(K^{-1}[K[S_P(K)]],K)$ 的值为真，那么协议就圆满完成了。值得注意的是，用 RSA 来实现数字签名是不合适的[7]。

在 ElGamal 数字签名系统中，计算公钥 V_P 比计算私钥的开销要大得多，因为任何数字(例如口令 P 或者其它具有相同功能的数字)都能够被用作私钥，而公钥必须由计算得出，所以用户不应该在登录时进行这项计算。因此，让主机同时储存单项哈希函数值 $H(P)$ 和从 P 求得的公钥 V_P 会更高效[7]。理论上来说，扩充 EKE 协议最直接的方法就是用 $H(P)$ 作为数字签名方案的公钥 V_P，即可以取 $V_P=H(P)$。

本文用 Diffie-Hellman 算法实现基本 EKE 协议部分，用 ElGamal 签名算法实现协议的扩充部分，直接用 $H(P)$ 作为 ElGamal 签名算法的公钥 V_P。

用户 Alice 注册时，主机 Bob 计算并存储口令哈希值 $H(P)$ 和公钥 V_P，此处 $V_P=H(P)$；Alice 登录后，用 $H(P)$ 进行加密密钥交换部分，同时根据 P 产生私钥 S_P(其值可以为 P 或者其它具有相同功能的数字)，然后用 S_P 执行 *A-EKE* 协议的扩展部分，而 V_P 则能够用来验证签名。

3.1 协议描述

首先选定一条圆锥曲线：$y^2\equiv ax^2-bx(\bmod n)$。其中 a，$b\in Z_n$，$(a,n)=(b,n)=1$。$n=pq$，p、q 为两个大素数，满足 $\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)=-1$ 时，$\#C_n(a,b)=(p+1)(q+1)$，且 $p+1=2r$，$q+1=2s$，其中 r，s 也为素数，将此圆锥曲线记为 $C_n(a,b)$。G 为基点，其阶为 $N_n=rs$ 或 $2rs$。

下面建立环 Z_n 上圆锥曲线上的 ElGamal 签名系统，Alice 随机选取 $d\in Z_{Nn}^*$ 作为 ElGamal 签名系统的私钥 S_P，$Q=dG$ 为签名验证公钥 V_P。d 即相当于 Alice 的秘密口令 P，设 $P(u)=Q$，则 $u=y_Qx_Q^{-1}$ 即相当于 Alice 和 Bob 共享口令的哈希函数值 $H(P)$。Alice 选取随机整数 $k\in Z_{Nn}^*$，并计算 $l=k-1(\bmod N_n)$。

公开(a,b,n,N_n,G,Q)，私钥为 d。

1) Alice 选择随机数 R_A 并发送给 Bob：

$A,R_AG(\bmod n)$

2) Bob 选择随机数 R_B，并计算 $K=R_AR_BG(\bmod n)$，他产生一个随机数 S_B，然后发送给 Alice：

$E_u((R_BG(\bmod n)),E_K(S_B)$

3) Alice 解密该消息前一半获得 $R_BG(\bmod n)$，计算 $K=R_AR_BG(\bmod n)$，并解密 $E_K(S_B)$ 得到 S_B，然后她也产生一个随机数 S_A，用 K 来加密这两个随机数，把结果发送给 Bob：

$E_K(S_A,S_B)$

4) Bob 解密消息得到 S_A、S_B，假定他从 Alice 处得到的 S_B 与他在第 2 步中发送给 Alice 的 S_B 一样，他便用 K 加密 S_A，同时把结果发送给 Alice：

$E_K(S_A)$

5) Alice 解密该消息，假定她从 Bob 处得到的 S_A 与她在第 3 步中发送给 Bob 的 S_A 一样，那么 Alice 计算 $kG=(x_1,y_1)$，令 $\gamma=x_1$，$m=y_Kx_K^{-1}$，$\delta=(m-d\gamma)l(\bmod N_n)$，于是$(\gamma,\delta)$即为 Alice 对 K 的签名，然后 Alice 发送给 Bob：

$E_k[(\gamma,\delta)]$

6) Bob 解密消息得到(γ,δ)，取 $u_1=\gamma$，$u_2=\delta k(\bmod n)$。然后计算 $U=u_1Q\oplus u_2G(\bmod n)$。如果 $U=(0,0)$ 则拒绝这个签名，否则计算 $V=mG(\bmod n)$。当且仅当 $U=V$ 时接受这个签名。签名验证证明：

$U=u_1Q\oplus u_2G(\bmod n)=\gamma Q\oplus\delta kG=\gamma dG\oplus(m-d\gamma)lkG$

$=mG(\bmod n)$

$V=mG(\bmod n)$

当且仅当 $U=V$ 时，接受这个签名，于是协议圆满完成。

3.2 数值模拟

选取圆锥曲线 $C_{65}: y^2\equiv 2x^2-x(\bmod 5809)$，即 $a=2,b=1,n=5809$，此时有 $p=37,q=157$，满足 $\left(\frac{a}{p}\right)=\left(\frac{2}{37}\right)=-1$，$\left(\frac{a}{q}\right)=\left(\frac{2}{157}\right)=-1$。$r=(p+1)/2=19,s=(q+1)/2=79$，所以 $N_n=2rs=3002$。

由于 $a-b\equiv 1(\bmod n)$，且 $(1,1)$ 在 $C_{65}(2,1)$ 中的阶为 $r=19$，由命题 3 可取基点 $G=P_1(2)$。

下面建立环 Z_n 上圆锥曲线上的 ElGamal 签名系统，Alice 随机选取 $d=11$ 满足 $d\in Z_{N_n}^*$ 作为 ElGamal 签名系统的私钥，$Q=dG$ 为签名验证公钥。11 的标准二进制表示为(1 0 −1 0 −1)，于是：

$$\begin{aligned}Q=dG&=11P_1(2)=(1\ 0\ -1\ 0\ -1)P_1(2)\\&=-P_1(2)\oplus 2^2(P_1(-2)\oplus 2^2P_1(2))\\&=-P_1(2)\oplus 2^2(P_1(-2)\oplus P_1(3390))\\&=-P_1(2)\oplus 2^2P_1(24921)\\&=-P_1(2)\oplus P_1(970)\\&=P_1(10)\end{aligned}$$

d 即为 Alice 的秘密口令，设 $P(u)=Q$，则 $u=y_Qx_Q^{-1}=10$ 即相当于 Alice 和 Bob 共享口令的哈希值。

Alice 选取随机整数 $k=1887$ 满足 $k\in Z_{N_n}^*$，并计算 $l=k^{-1}(\bmod N_n)=35(\bmod 3002)$。

公钥为 $a=2,b=1,n=5809,N_n=3002,G=P_1(2),Q=P_1(10)$；

私钥为 $d=11$。

1) Alice 选择随机数 $R_A=5$，并计算：

$$\begin{aligned}R_AG(\bmod n)&=5P_1(2)=2^2P_1(2)\oplus P_1(2)=2P_1(2906)\\&\quad\oplus P_1(2)\\&=P_1(3390)\oplus P_1(2)=P_1(5102)(\bmod 5809)\end{aligned}$$

然后她发送给 Bob：Alice，$P_1(5102)$；

2) Bob 选择随机数 $R_B=8$，并计算：

$$\begin{aligned}R_BG(\bmod n)&=8P_1(2)=2^3P_1(2)=2^2P_1(2906)\\&=2P_1(3390)=P_1(1354)\end{aligned}$$

$$\begin{aligned}K&=R_AR_BG(\bmod n)=2^3P_1(5102)=2^2P_1(4594)\\&=2P_1(3105)=P_1(5311)\end{aligned}$$

他产生一个随机数 $S_B=1679$，然后发送给 Alice：

$$\begin{aligned}&[E_P(R_BG(\bmod n)),E_K(S_B)]\\&=(1354^{-1}\bmod 5809,1679^{-1}\bmod 5809)\\&=(4395,1377)\text{；}\end{aligned}$$

3) Alice 解密消息前一半得 $4395^{-1}(\bmod 5809)=1354$，可知 $R_BG(\bmod n)=P_1(1354)$，计算：

$$\begin{aligned}K&=R_AR_BG(\bmod n)=5P_1(1354)\\&=2^2P_1(1354)\oplus P_1(1354)\\&=2P_1(4594)\oplus P_1(1354)\\&=P_1(3105)\oplus P_1(1354)\\&=P_1(5311)\end{aligned}$$

并解密 $E_K(S_B)$ 得到 $S_B=1377^{-1}(\bmod 5809)=1679$，然后她也产生一个随机数 $S_A=2354$，用 K 来加密这两个随机数，把结果发送给 Bob：

$$\begin{aligned}E_K(S_A,S_B)&=(2354^{-1}\bmod 5809,1679^{-1}\bmod 5809)\\&=(4395,1377)\end{aligned}$$

4) Bob 解密消息得：

$S_A=4395^{-1}\bmod 5809=2354$，$S_B=1377^{-1}\bmod 5809=1679$

式中，求得的 S_B 与他发送给 Alice 的 S_B 一样，他便用 K 加密 S_A，然后把结果发送给 Alice：

$$E_K(S_A)=2354^{-1}\bmod 5809=4395$$

5) Alice 解密该消息得 $S_A=4395^{-1}\bmod 5809=2354$，与她在第 3 步中发送给 Bob 的 S_A 一样，于是 Alice 计算

$$\begin{aligned}kG&=1887P_1(2)\\&=(1\ 0\ 0\ 0\ -1\ 0\ -1\ 0\ 0\ 0\ 0\ -1)\ P_1(2)\\&=-P_1(2)\oplus 2^5(P_1(-2)\oplus 2^2(P_1(-2)\oplus\\&\quad 2^4P_1(2)))\\&=-P_1(2)\oplus 2^5(P_1(-2)\oplus 2^2(P_1(-2)\oplus\\&\quad P_1(4594)))\\&=-P_1(2)\oplus 2^5(P_1(-2)\oplus 2^2P_1(5344))\\&=-P_1(2)\oplus 2^5(P_1(-2)\oplus P_1(2695))\\&=-P_1(2)\oplus 2^5P_1(2209)\\&=-P_1(2)\oplus P_1(1472)\\&=-P_1(4416)\\&=(3254,5007)\end{aligned}$$

取 $\gamma=x_1(\bmod N_n)=3254\bmod 3002=252$，$m=y_Kx_K^{-1}=5311$，计算 $\delta=(m-d\gamma)l(\bmod N_n)=(5311-11*252)(\bmod 3002)=2539$，于是 $(\gamma,\delta)=(252,2539)$ 即为 Alice 对 K 的签名，然后 Alice 发送给 Bob：

$$\begin{aligned}E_k[(\gamma,\delta)]&=(252^{-1}\bmod 5809,2539^{-1}\bmod 5809)\\&=(3573,4617)\end{aligned}$$

6) Bob 解密消息得到：

$$\begin{aligned}(\gamma,\delta)&=(3573^{-1}\bmod 5809,4617^{-1}\bmod 5809)\\&=(252,2539)\end{aligned}$$

取 $u_1=\gamma=252$，$u_2=\delta k(\bmod n)=2539*1887(\bmod 3002)=2903$。然后计算：

$$\begin{aligned}U&=u_1Q\oplus u_2G(\bmod n)\\&=(252P_1(10)\oplus 2903P_1(2))(\bmod 5809)\\u_1Q&=252P_1(10)=(1\ 0\ 0\ 0\ 0\ 0\ -1\ 0\ 0)\ P_1(10)\\&=P_1(4272)(\bmod 5809)\\u_2G&=2903P_1(2)=(1\ 0\ -1\ 0\ 0\ -1\ 0\ -1\ 0\ -1\ 0\ 0\\&\quad -1)\ P_1(2)\\&=P_1(1174)(\bmod 5809)\end{aligned}$$

则 $U=P_1(4272)\oplus P_1(1174)=P_1(5686)(\bmod 5809)$

$U\neq(0,0)$，于是计算：

$$\begin{aligned}V&=mG(\bmod n)=5311\ P_1(2)=(1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ -1\ 0\\&\quad 0\ -1)\ P_1(2)\\&=P_1(5686)(\bmod 5809)\end{aligned}$$

所以有 $U=V$，于是 Bob 接受这个签名，接下来，Alice 和 Bob 就用会话密钥 $K=P_1(5311)$ 进行通信。

结束语 EKE 协议的提出主要是为了实现主机对用户身份的认证，用 Diffie-Hellman 算法实现基本的 EKE 协议，以破解指数密钥交换的困难性，抵御口令猜测攻击。扩充的

EKE协议要求用户发送额外的消息来证实其知道口令 P 的明文，使得攻击者在获取了用于加密密钥交换的口令，哈希值在 $H(P)$ 的情况下也无法向主机冒充用户。用户选择的口令通常是一些便于记忆的弱口令，本文构建的基于环 Z_n 上圆锥曲线用 ElGamal 签名算法实现的 A-EKE 协议，不需要协议双方保存口令明文，能抵抗主动攻击、字典攻击和破坏口令文件的攻击，使得即使在用户选用弱口令的情况下也能保证身份认证的有效性和密钥协商的安全性，从而保证信息传输的安全性，并且能够有效减少计算机处理开销，在加密处理速度、通信带宽和对硬件的要求方面都有更大的优势，对于在网络通信中实现高效的身份认证和安全信息传递有一定的现实意义。

参 考 文 献

[1] 孙琦，张起帆，彭国华. 计算群元的整数倍的一种算法及其在公钥密码体制中的应用[A]//密码学进展——ChinaCrypt'2002：第七届中国密码学学术会议论文集[C]. 北京：电子工业出版社，2002

[2] 孙琦，朱文余，王标. 环 Z_n 上圆锥曲线和公钥密码协议[J]. 四川大学学报：自然科学版，2005，42(3)

[3] 王标，朱文余，孙琦. 基于剩余类环 Z_n 圆锥曲线的公钥密码体制[J]. 四川大学学报：工程科学版，2005，37(5)

[4] Bellovin S M，Merritt M. Encrypted Key Exchange：Password-Base Protocols Secure Against Dictionary Attacks[C]// Proceedings of the 1992 IEEE Computer Society Conference on Research in Security and Privacy. 1992

[5] Morris R H，Thompson K. Unix password security[J]. Communications of the ACM，1979，22

[6] A proposed Federal Information Processing Standard for digital signature standard (DSS)[S]. Docket No. 910807- 1207，RIN 0693-AA86

[7] Bellovin S M，Merritt M. Agumented Encrypted Key Exchange：a Password-Based Protocol Secure Against Dictionary Attacks and Password File Comprise[C]// Proceedings of the 1st ACM Conference on Computer and Communications Security. 1993

[8] 张明志. 用圆锥曲线分解整数[J]. 四川大学：自然科学版，1996，33(4)

(上接第 113 页)

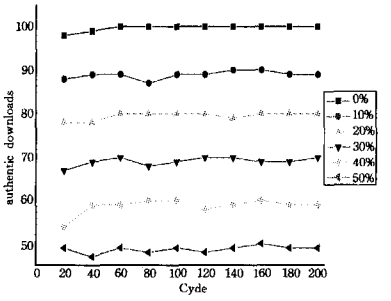

图 11 成功下载次数对比

(3)不成功下载次数对比结果

描述了 0%、10%、20%、30%、40%、50%恶意节点随即下载过程中对于不成功下载次数对比的仿真结果。对每 20 个查询周期选一个进行比较，如图 12 所示。

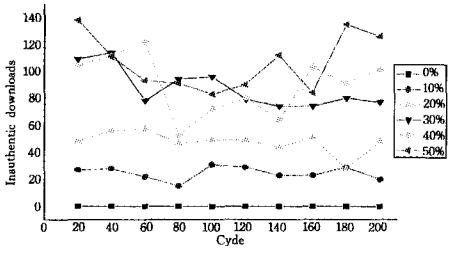

图 12 不成功下载次数对比

4.2 结果分析

由上述仿真结果可知，基于终端可信的分层可信平台通过对点对点文件共享网络中的节点可信度直接作用，对下载成功率、成功下载次数均有明显提高，对不成功下载次数显著下降。点对点文件共享网络计算环境下，下载成功率、成功下载次数、不成功下载次数都可以代表其可信度。仿真系统数据结果说明，提高可信节点的比例对于提高可信计算环境整体的可信度有显著效果。

结束语 现有的 TCG 规范的可信计算模型是一种基于终端可信的通用模型，由于可信根以硬件的方式进行实现，因此要求对现有的计算机硬件体系结构以及硬件驱动软件做出较大改动，模型实现存在较大困难。所以，研究与现行的计算机网络相适应的可信计算模型，具有很强的理论和实践意义。

本文给出的基于可信终端的分层可信计算平台，对 TCG 所定义的可信计算模型进行了结构上的改动，通过把原有的 TPM 模块逻辑化为一个信任度量的状态矩阵，较大地降低了系统实施的复杂性。由于该模型中信任的度量可以灵活地实施在任意相对独立的可信计算平台的任意逻辑层，因此可以从信任根的完整度量节点出发构建完整的可信链，保证可信计算平台的安全性。同时，广义的可信计算平台包括了所有的人机接口，进而实现真正的用户对用户可信。

参 考 文 献

[1] Shangyuan G，et al. Trust management and service selection in pervasive computing environments[C]// International Conference on Computational Intelligence and Security Workshops. Dec. 2008：15-19

[2] Feng D，Qin Y. Research on attestation method for trust computing environment[J]. Jisuanji Xuebao/Chinese Journal of Computers，2008，31(9)：1640-1652

[3] TCG. TCG Specification Architecture Overview. Ver1. 4 [EB/OL]. (2007-8-2) [2008-11-24]

[4] Brizek J，Khan M，Seifert J P，et al. A Platform-level Trust-Architecture for Hand-held Devices [C]// 2005 Workshop on Cryptographic Advances in Secure Hardware (CRASH). Belgium，2005

[5] Eisenbarth T，Güneysu T，Paar C，et al. Reconfigurable Trusted Computing in Hardware [C]// Proceedings of the 2007 ACM workshop on Scalable trusted computing. VA，USA，2007：15-20

[6] 林闯，田立勤，王元卓. 可信网络中用户行为可信的研究[J]. 计算机研究与发展，2008(12)

[7] 邓晓衡. iVCE 中基于可信评价的资源调度研究[J]. 计算机学报，2007(10)

[8] 章勤. 基于网格环境的可信计算平台共享模型[J]. 华中科技大学学报：自然科学版，2007(12)

[9] 林闯. 可信网络研究[J]. 计算机学报，2005，28(5)：751-758

[10] TCG. TCG TNC(Trusted Network Connect) Architecture for Interoperability. Ver1. 2 [EB/OL]. (2007-5-2) [2008-11-24]