文章编号:1001 - 9081(2010)07 - 1805 - 04

有效的强安全组群密钥交换协议

邓少锋,邓 帆,李益发
(信息工程大学 信息工程学院,郑州 450002)
(dsfcyandyfiest@163.com)

摘 要:组合公钥密码(CPK)体制无需证书来保证公钥的真实性,克服了用户私钥完全由密钥管理中心生成的问题。基于 CPK 设计了一个常数轮的组群密钥交换协议,该协议在 CDH 假设下可证安全并具有完美的前向安全性,只需两轮通信即可协商一个组群会话密钥,在通信和计算方面都很高效;并且高效地支持组群成员动态加入/离开,尤其对于多成员加入/离开的情况,只需额外的少量通信和计算即可更新组群密钥,确保了前向保密性和后向保密性。此外,本协议提供了强安全性保证,它能保持密钥的秘密性,除非某一方的临时私钥和长期私钥同时被泄露。最后,该协议提供了一个设计常数轮强安全组群密钥交换协议的方法,大部分的秘密共享体制均可直接应用于该协议。

关键词:组群密钥交换;组合公钥密码;强安全性;秘密共享;动态组群
中图分类号: TP309 **文献标志码**:A

Efficient group key exchange protocol with strong security

DENG Shao-feng, DENG Fan, LI Yi-fa
(*Institute of Information Engineering, Information Engineering University, Zhengzhou Henan* 450002, *China*)

Abstract: Combined Public Key (CPK) cryptography does not need certificates to guarantee the authenticity of public keys, and avoids the problem that user's private key completely depends on the Key Management Center (KMC). Based on CPK, a constant-round group key exchange protocol was presented, which was provably secure under the intractability of computation Diffie-Hellman problem and achieved perfect forward secrecy. The protocol has only two communication rounds and it is more efficient than other protocols both in communication and computation. It supports group member join/leave operations efficiently and only needs minimum amount of computation and communication to renew the group key especially for multiple joins/leaves. At the same time, it also assures backward secrecy and forward secrecy. Moreover, the protocol achieves strong security. It can keep the session key secret from the adversary except that one party's ephemeral private key and static private key are all revealed to the adversary. Lastly, the protocol provides a method to design efficient constant-round group key exchange protocols with strong security and most secret sharing schemes can be adopted to construct the protocol.

Key words: group key exchange; Combined Public Key Cryptography (CPK); strong security; secret sharing; dynamic group

0 引言

目前的认证系统普遍采用非对称密码技术,比如公钥基础设施(Public Key Infrastructure, PKI)和基于身份的公钥密码(Identity-based Public Key Cryptography, ID-PKC)。典型的 PKI 系统需要复杂的证书管理。ID-PKC 体制不可避免地引入了密钥托管问题。Al-Riyami 等人[1]引入了无证书公钥密码(Certificateless Public Key Cryptography, CL-PKC)的概念,克服了 ID-PKC 的密钥托管问题,并且不需要证书来保证公钥的真实性,综合了 ID-PKC 和 PKI 两者的优势。正如 Joseph 等人[2]所指出的那样,在 CL-PKC 体制中用户无法判断公钥的真正归属者,从而带来了拒绝解密(Denial-of-Decryption, DoD)攻击和密钥分发问题。唐文等人[3]提出了一种新的基于身份的高效公钥管理方案——组合公钥密码体制(Combined Public Key Cryptography, CPK),该方案具有 CL-PKC 体制的所有优势,并且不存在密钥分发和 DoD 攻击问题。

近年来,组群通信的应用越来越广泛,但其安全问题需要进一步解决。组群密钥交换协议是实现安全组群通信的重要方式之一,它允许组群成员间建立一个共同的组群密钥。下面简单介绍一些相关的工作。Barua 等人[4]基于三元树结构设计了一个多方密钥交换体制,但该体制不是常数轮的,随着通信方数 n 的增大,体制的执行将面临瓶颈。宋震等人[5]利用二叉树结构提出一个基于身份的组密钥协商方案,该方案支持成员动态加入或者离开,但存在密钥托管问题。曹春杰等人[6]利用 CL-PKC 和秘密共享体制设计了一个常数轮的组群密钥交换协议,但该协议不支持成员动态变化。文献[7]基于 CPK 提出一个两轮的高效组群密钥协商协议,但该协议也不支持成员动态变化。在某些场景下,攻击者可能会获得所攻击会话的一些秘密信息(比如:用户的随机数生成器发生泄露)。文献[8-9]的安全模型中,攻击者被赋予额外的能力来获得会话的临时私钥。但是,攻击者不允许同时获得某个用户的会话临时私钥和长期私钥,否则协议的安全性会被轻易攻破。从而,如何设计高效强安全的组群密钥交换协议是一个值得深入研究的课题。目前,这方面的成果较少,前

收稿日期:2010 - 01 - 04;**修回日期**:2010 - 03 - 01。 **基金项目**:通信技术重点实验室基金资助项目(9140C1103040902)。

作者简介:邓少锋(1984 -),男,江西高安人,硕士研究生,主要研究方向:安全协议设计与分析; 邓帆(1980 -),男,云南曲靖人,硕士研究生,主要研究方向:安全协议设计与分析; 李益发(1964 -),男,安徽芜湖人,副教授,博士,主要研究方向:密码学、信息安全。

面的组群密钥交换协议[4-7]均没有考虑会话临时私钥泄漏问题。Bressen等人[10]提出一个三轮强安全的组群密钥交换协议,但该协议比较复杂,效率不太高。

针对会话秘密信息泄漏问题,基于高效CPK体制,提出一个两轮的强安全组群密钥交换协议,它能提供完美的前向安全性和完全的健壮性,高效地支持组群成员动态加入或者离开;能保持会话密钥的秘密性,除非攻击者同时获得某一方此次会话的临时私钥和长期私钥;此外该协议提供了一种设计常数轮组群密钥交换协议的方法,并且大部分密钥共享体制可直接应用于该协议而得到一个全新的常数轮强安全组群密钥交换协议。

1 椭圆曲线组合公钥体制原理

在CPK体制中,组合密钥由标识密钥、系统密钥、更新密钥组成。标识密钥由用户的身份标识通过组合矩阵生成。组合矩阵由密钥管理中心(Key Management Center,KMC)产生,分为私钥矩阵(***SKM***)和公钥矩阵(***PKM***)。标识密钥对记为(isk, IPK)。系统密钥是KMC为各用户生成的随机序列。系统密钥对记为(ssk, SPK)。更新密钥由用户自己选择,因此CPK体制不存在密钥托管问题。更新密钥对记为(usk, UPK)。用户A的公钥$PK_A = IPK_A + SPK_A + UPK_A$,对应的私钥$sk_A = isk_A + ssk_A + usk_A$。

椭圆曲线组合公钥(Elliptic Curve Combined Public Key,ECCPK)[11]是基于椭圆曲线的CPK方案,其系统参数为$\kappa = (p,q,E,G,\boldsymbol{PKM},\theta(\cdot))$。其中$E$是有限域$F_p$上的椭圆曲线,$G$是$E$上阶为$q$的一个点,使得$\langle G\rangle$上的离散对数问题难解,$\theta(\cdot)$为查询函数。KMC根据用户身份、***SKM***和$\theta(\cdot)$可以确定用户的标识私钥isk。***SKM***由KMC秘密保管,而***PKM***是公开的。每个用户可以类似地由对方身份、***PKM***和$\theta(\cdot)$获得对方的标识公钥IPK。记用户系统公钥和更新公钥之和为用户的伴随公钥BPK,相应地用户系统私钥和更新私钥之和为用户的伴随私钥bsk。ECCPK的更详尽介绍请查阅文献[11]。

2 基于CPK的强安全组群密钥交换协议

系统公开参数为$\kappa = (p,q,E,G,\boldsymbol{PKM},\theta(\cdot),m)$,$m$为允许参与组群通信用户数的上限。SHA-1,$H_1$,$H_2$为Hash函数,其中SHA-1用于ECDSA签名,H_1为单向密钥导出函数,H_2:$\langle G\rangle \rightarrow F_q$。用户$U_i(1 \leqslant i \leqslant n)$的长期私钥记为$sk_i$,对应的长期公钥为$PK_i$。假设$n$个用户参与组群通信,基于CPK设计的强安全的组群密钥交换协议P详细描述如下:

第1轮 用户$U_i(1 \leqslant i \leqslant n)$随机选择自己的临时私钥$r_i \in Z_q^*$,计算自己的临时公钥$O_i = r_iG$,广播消息($ID_i$,$O_i$,$BPK_i$),其中$BPK_i$为$U_i$的伴随公钥。

第2轮 收到所有其他用户的消息后,U_i随机选择$k_i \in Z_q$,计算n次多项式:$f_i(x) = k_i + a_{i_1}x + a_{i_2}x^2 + \cdots + a_{i_n}x^n$,使得$f_i(x)$经过点$(j,H_2((r_i + sk_i)(O_j + PK_j)))$,$1 \leqslant j \leqslant n$和点$(0,k_i)$,其中$PK_j = BPK_j + IPK_j$,$IPK_j$可根据$ID_j$和***PKM***查询得到。记$O_i = (u_i,v_i)$,计算$R_i = u_i \bmod q$,$h_i = \text{SHA-1}(O_i \| k_i \| T_s \| G_{ID})$,$P_{ij} = f_i(m + j)$,$s_i = r_i^{-1}(h_i + sk_iR_i) \bmod q$。其中,$T_s$为时间戳,$G_{ID}$为组群ID。广播消息($ID_i$,$P_{ij}$,$T_s$,$s_i$)。

组群密钥的计算 收到所有其他用户的(ID_j,P_{ji},T_s,s_j)后,U_i首先验证T_s的新鲜性,若验证不通过,则终止协议。其次,利用Lagrange插值公式重构$f_j'(x)$,$j \neq i$,使得$f_j'(x)$经过点$(m + l,P_{jl})$,$1 \leqslant l \leqslant n$和点$(i,H_2((r_i + sk_i)(O_j + PK_j)))$,其中$PK_j = BPK_i + IPK_j$,$IPK_j$可根据$ID_j$和***PKM***查询得到,然后计算$k_{ij} = f_j'(0)$。最后,$U_i$验证$U_j$的ECDSA签名是否有效。记$O_j = (u_j,v_j)$,计算$R_j = u_j \bmod q$,$w_j = s_j^{-1} \bmod q$,$(u,v) = w_j(R_jPK_j + h_jG)$,其中$h_j = \text{SHA-1}(O_j \| k_{ij} \| T_s \| G_{ID})$,若$u \bmod q = R_j$则签名有效。$U_i$验证所有其他用户的签名有效后,计算组群会话密钥:$k = H_1(k_{i1} + \cdots + k_{in}) = H_1(k_1 + \cdots + k_n)$。

3 协议的安全性分析

3.1 可证安全性

本节主要使用Bressen等人提出的安全模型[12]来证明协议P是安全的,该模型的详细介绍请参考文献[12]。首先说明协议满足安全性定义中的一致性条件。根据$(r_i + sk_i)(O_j + PK_j) = (r_j + sk_j)(O_i + PK_i)$,用户$U_i$由Lagrange插值公式重构的$f_j'(x)$,$j \neq i$等于$f_j(x)$,从而$k_{ij} = f_j'(0) = f_j(0) = k_j$。通过验证其他用户的ECDSA签名确保对方身份和$k_j$的有效性。从而,即使有攻击者的参与,所有非腐化用户在正确执行协议后均能获得相同的组群会话密钥。接下来证明攻击者攻击协议的优势是可忽略的。

主动攻击者A在时间t内做q_{ex}次Execute查询,q_{se}次Send查询,q_h次Hash查询,攻击协议P获得的最大优势记为$Adv_A^P(t,q_{ex},q_{se},q_h)$。

定理1 假设Hash函数H_1,H_2均为随机Oracle,则协议P在计算Diffie-Hellman(Computational Diffie-Hellman,CDH)假设下提供完美的前向安全性。具体为:

$$Adv_A^{GK-PFS}(t,q_{ex},q_{se},q_h) \leqslant 2n \cdot Succ_{\text{ECDSA}}(t) + 2(q_{ex} + q_{se}) \cdot q_h \cdot Succ_{\text{CDH}}(t)$$

其中$Succ_{\text{ECDSA}}(t)$,$Succ_{\text{CDH}}(t)$分别为时间复杂度为t的攻击者伪造ECDSA签名,解决CDH困难实例的最大优势。

证明 可以将A攻破协议P规约为如下两个事件之一发生:1)A成功伪造了某个用户U_i的ECDSA签名;2)A成功地解决了一个CDH问题实例,从而能正确区分随机数和组群会话密钥。利用A可以分别构造ECDSA签名的伪造者Γ和CDH问题攻击者ψ。定理1的详细证明过程与文献[7]中的定理证明过程比较相似,为避免重复,这里省略。

3.2 安全性质

通常情况下,一些安全性质被用来衡量协议的安全性,包括已知密钥安全(Known Session Key Security,KSK)、抗未知密钥共享攻击(Unknown Key-share Resilience,UKS)、完美前向安全性(Perfect Forward Security,PFS)、抗密钥泄露伪装攻击(Key Compromise Impersonation Resilience,KCI)和抗临时私钥泄露攻击(Leakage of Ephemeral Private Keys,LEP),等等。根据本协议的执行流程,易知其具有如下一些好的安全性质。

已知密钥安全 每次会话中每个用户都独立选取不同的部分密钥k_i,从而泄露的会话密钥不会危及其他会话产生的会话密钥。

未知密钥共享安全 通过验证其他用户的ECDSA签名和消息的新鲜性,每个用户可以确认其每个通信对象身份的有效性。从而,当其成功地与一些用户建立一个组群会话密钥时,它不会错误地认为该会话密钥是与另外一些用户共享的。

抗密钥泄露伪装攻击 当攻击者获得某一方(比如

Alice)的长期私钥时,它显然能向其他参与者冒充为 Alice;但是,攻击者不能反过来向 Alice 冒充为其他参与者(比如 Bob),因为根据 CDH 假设它不能计算正确的新鲜 ECDSA 签名。

完美前向安全性　假设协议参与者的长期私钥被攻击者获得。根据 CDH 问题假设,只知道两方的临时公钥 O_i, O_j,攻击者仍不能计算得到 $r_i r_j G$。从而,根据 Lagrange 定理攻击者也无法获得用户的部分密钥 k_i,进而不能计算长期私钥泄露前已建立的会话密钥。

无密钥控制　每个参与者通过独立选取自己的部分密钥 k_i,在组群会话密钥的建立过程中发挥同样的作用,从而任何人都不能独自预确定将要生成的组群会话密钥。

抗临时密钥泄露攻击　假设协议参与者的临时私钥被攻击者获得。根据 CDH 假设,只知道两方的长期公钥 PK_i, PK_j,攻击者仍不能计算得到 $sk_i sk_j G$。从而,根据 Lagrange 定理攻击者也无法获得用户的部分密钥 k_i,进而不能计算临时私钥泄露前已建立的会话密钥。除非某一方的临时私钥和长期私钥同时泄露给攻击者时,攻击者才能计算获得已建立的组群会话密钥。

4　成员加入/离开操作

很多情况下通信组群的成员结构是动态变化的,参与组群通信的成员可能随时离开或者不断地有新成员加入当前组群。为了达到组群通信安全的目的,需要确保成员加入或者离开时,组群密钥交换协议能提供后向保密性和前向保密性。所谓前向保密性即指主动退出或者强制退出的成员无法继续参与组群通信,也即无法利用它们掌握的密钥解密后续组群数据或者生成有效的加密数据。后向保密性指新加入成员无法破解其加入前的组群加密数据。解决方案之一为每当有成员加入或者离开时,新组群成员重新执行组群密钥交换协议协商一个新组群会话密钥,显然此方案所花代价过高,尤其当短时间内很多成员频繁加入或者离开时,此方案的执行将面临瓶颈。为高效支持多成员加入或者离开操作,在第 2 章组群密钥交换协议基础上提出一个更新组群会话密钥的新方案。具体描述如下:

1)加入操作:假设成员 U_{n+1} 希望加入 n 个成员的组群 U 中。

a)原成员 $U_i, 1 \leqslant i \leqslant n$ 计算当前会话密钥 k 的 Hash 值 $H_1(k)$,原成员之一 U_i 发送 $ID_i, H_1(k), T_s, O_1, O_2, \cdots, O_n, BPK_1, \cdots, BPK_n$ 以及对发送消息的 ECDSA 签名给 U_{n+1}。

b) U_{n+1} 收到 U_i 的消息后,验证消息的新鲜性和 ECDSA 签名的有效性,若验证都通过则完整地执行第 2 章中的第 1 轮和第 2 轮。其中 $f_{n+1}(x)$ 次数变为 $n+1$,经过点 $(j, H_2((r_{n+1} + sk_{n+1})(O_j + PK_j)))$, $1 \leqslant j \leqslant n+1$ 和点 $(0, k_{n+1})$, $P_{n+1,s} = f_{n+1}(m+s)$, $1 \leqslant s \leqslant n+1$。

组群密钥的计算　原成员收到 U_{n+1} 的消息后,首先验证消息的新鲜性,若验证不通过,则终止协议。其次, U_i 利用 Lagrange 插值公式重构 $f'_{n+1}(x)$,计算 $k'_{n+1} = f'_{n+1}(0)$,验证 U_{n+1} 的 ECDSA 签名,若验证通过则计算新密钥 $k_{new} = H_1(K) + k'_{n+1}$。$U_{n+1}$ 直接计算 $k_{new} = H_1(K) + k_{n+1}$。

上述过程中只有新加入成员需要完整执行第 2 章中的第 1 轮和第 2 轮,原成员只需重新计算组群密钥,从而效率得到大大的提高。对于成员加入操作比较频繁的组群,原成员可以轮流充当 U_i 的角色,尽量使每成员承担的工作量相等。多成员加入情况与单成员加入情况相似。设新加入成员数目为 w,则步骤 b)中新成员 $U_{n+l}, 1 \leqslant l \leqslant w$ 选取的多项式 $f_{n+l}(x)$ 次数变为 $n+w$。$f_{n+l}(x)$ 经过点 $(j, H_2((r_{n+l} + sk_{n+l})(O_j + PK_j)))$, $1 \leqslant j \leqslant n+w$ 和点 $(0, k_{n+l})$, $P_{n+l,s} = f_{n+l}(m+s)$, $1 \leqslant s \leqslant n+w$。原成员通过 Lagrange 插值公式计算获得所有新加入成员的 k_{n+l}',新加入成员类似地获得所有其他新加入成员的 k_{n+l}'。在所有 ECDSA 签名有效性和消息新鲜性验证都通过后,所有成员计算新组群密钥 $k_{new} = H_1(K) + k_{n+1}' + \cdots + k_{n+w}'$。当 n 很大时, $f_{n+l}(x)$ 的次数 $n+w$ 也变得很大,导致每个成员的计算量很大。针对这一问题,提出的解决方案如下:

a)原成员 $U_i, 1 \leqslant i \leqslant n$ 计算当前会话密钥 k 的 Hash 值 $H_1(k)$,原成员之一 U_i 广播 $ID_i, H_1(k)$, $T_s, O = kG, BPK_1, \cdots, BPK_n$ 以及对发送消息的 ECDSA 签名(等价于将所有原成员虚拟为一个成员)。

b)所有新加入成员 $U_{n+l}, 1 \leqslant l \leqslant w$ 接收到 U_i 的消息后,完整地执行第 2 章中的第 1 轮和第 2 轮。其中 $f_{n+l}(x)$ 次数为 $w+1$,,经过点 $(n+j, H_2((r_{n+l} + sk_{n+l})(O_{n+j} + PK_{n+j})))$, $1 \leqslant j \leqslant w$ 和点 $(0, k_{n+l})$, $(n, H_2((r_{n+l} + sk_{n+l}) \cdot O))$, $P_{n+l,s} = f_{n+l}(m+s)$, $1 \leqslant s \leqslant w+1$。

组群密钥的计算　原成员 $U_i, 1 \leqslant i \leqslant n$ 利用 Lagrange 插值公式重构 $f_{n+l}'(x)$,计算 $k_{n+l}' = f_{n+l}'(0)$。在所有的 ECDSA 签名有效性和消息新鲜性验证都通过后,计算新密钥 $k_{new} = H_1(K) + k_{n+1}' + \cdots + k_{n+w}'$。新加入成员 U_{n+l} 类似地计算得到 $k_{n+j}', 1 \leqslant j \leqslant w, j \neq l$,验证 U_{n+j} 和 U_i 的 ECDSA 签名和发送消息的新鲜性,若所有的验证都通过,则计算新密钥 $k_{new} = H_1(K) + k_{n+1}' + \cdots + k_{n+l} + \cdots + k_{n+w}'$。

由上述过程可知, $f_{n+l}(x)$ 的次数固定为 $w+1$,与 n 无关,从而在多成员加入操作中效率更高。根据 H_1 的单向性以及离散对数难题,新加入成员无法由 $H_1(k)$ 或者 kG 恢复出旧会话密钥 K,从而加入操作能提供后向保密性。

2)离开操作:假设成员 U_i 将要离开或者退出原组群,更新组群密钥的过程如下:

a)剩下成员之一比如 U_j 重做第 2 章中的第 2 轮步骤,即 U_j 重新选择自己的组群密钥贡献部分 k_j。U_j 重新选取的多项式 $f_j(x)$ 次数变为 $n-1$,经过点 $(s, H_2((r_j + sk_j)(O_s + PK_s)))$, $1 \leqslant s \leqslant n, s \neq i$ 和点 $(0, k_j)$,计算 $P_{js} = f_j(m+s)$。注意 $f_j(x)$ 不经过点 $(i, H_2((r_j + sk_j)(O_i + PK_i)))$,也不计算 $P_{ji} = f_j(m+i)$。

b)组群密钥的计算:剩下成员重构 $f_j'(x)$,计算 $k_j' = f_j'(0)$。验证 U_j 的 ECDSA 签名和消息的新鲜性,如果验证都通过,则计算新密钥 $k_{new} = k + k_j$。

当有频繁的离开操作时, U_j 的角色可以由剩下成员轮流分担,使每成员分担的工作量相等。多成员离开的情况和单成员离开情况相似。设离开成员的数目为 w,此时 $f_j(x)$ 的次数变为 $n-w$。不妨设离开成员为 $U_1, \cdots, U_w$,从而 $f_j(x)$ 不经过点 $(i, H_2((r_j + sk_j)(O_i + PK_i)))$, $1 \leqslant i \leqslant w$,且无需计算 $P_{ji} = f_j(m+i), 1 \leqslant i \leqslant w$。新组群密钥的计算与上面一样。由上述过程可知,根据 Lagrange 原理离开成员无法重构 $f_j(x)$,从而无法获得更新的 k_j,进而无法获得新组群密钥,所以离开操作能提供前向保密性。

5　对比

协议的效率通过通信和计算代价来衡量。通信花销包括一次协议执行过程中所需的通信轮数以及传输的消息总数。

计算花销主要是指所需的指数运算数、对运算数等。本协议与协议 ID-TT[4]、ID-BD[13]、ID-CMM[6]，CPK-DDL[7] 的比较结果如表1所示。

表1 几个组群密钥交换协议效率的对比

协议	轮数	消息数	指数运算数	对运算数
ID-TT	$\lceil \log_3 n \rceil$	$5(n-1)$	$9(n-1)$	$5n\lceil \log_3 n \rceil + 3$
ID-BD	2	$2n$	$n(n+8)$	$4n$
ID-CMM	2	$2n$	$2n(n+1)$	$2n$
CPK-DDL	2	$2n$	$O(n^2)$	0
本协议	2	$2n$	$O(n^2)$	0

从表1中易知：协议 ID-TT 通信轮数与通信方数 n 有关，而剩下四个协议是常数轮的，但协议 ID-BD 不能抵抗共谋攻击[14]。本协议能高效支持成员加入/离开操作，但协议 ID-CMM、CPK-DDL 不支持此操作并且协议 ID-CMM 需要双线性对运算。此外协议 ID-CMM 和 CPK-DDL 均不能抵抗临时密钥泄露攻击，但本协议提供了强安全性保证。综合各方面的考虑，本协议在安全性和效率方面都具有优势。此外，本协议还提供组群密钥交换协议的完全健壮性。协议执行过程中丢失的用户只会使其他用户接收不到该用户选择的部分密钥 k_i，但剩余用户仍可以正确计算剩余用户之间共享的组群会话密钥 $k = H_1(k_{i_1} + \cdots + k_{i_t})$，其中 $U_{i_1}, \cdots, U_{i_t}$ 为剩余用户。丢失用户可以通过加入组群操作继续参与组群安全通信。

6 结语

基于高效 CPK 体制，本文提出了一个两轮的强安全组群密钥交换协议。本协议提供显式密钥认证和完全的健壮性，高效支持多成员动态加入或者离开，并且成员加入或者离开操作能确保前向保密性和后向保密性。它能一直保持会话密钥的秘密性，除非某一方的会话临时私钥和长期私钥同时泄露。它也能抵抗密钥泄露伪装攻击和临时密钥泄露攻击，提供完美的前向安全性。此外，本协议相当于提供了一个设计常数轮强安全组群密钥交换协议的方法，且大部分的秘密共享体制均可直接应用于本协议。

参考文献：

[1] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography[C]// Proceedings of Asiacrypt'03. Berlin: Springer-Verleg, 2003:205-217.

[2] JOSEPH K L, MAN H A, WILLY S. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model[C]// Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2007:273-283.

[3] 唐文,南湘浩,陈钟. 基于椭圆曲线密码系统的组合公钥技术[J]. 计算机工程与应用, 2003, 39(21):1-3.

[4] BARUA R, DUTTA R, SARKAR P. Extending Joux's protocol to multi-party key exchange[C]// Proceedings of Indocrypt'03. Berlin: Springer-Verlag, 2003:205-217.

[5] 宋震,周贤伟,窦文华. 一种基于身份标识的 MANET 组密钥协商协议[J]. 电子学报,2008,36(10):11-18.

[6] CAO C J, MA J F, MOON S J. Provable efficient certificateless group key exchange protocol[J]. Wuhan University Journal of Natural Sciences, 2007, 12(1): 041-045.

[7] 邓少锋,邓帆,李益发. 基于 CPK 的可证安全组群密钥交换协议[J]. 信息安全与通信保密, 2009(8):316-319.

[8] KRAWCZYK H. HMQV: A high-performance secure Diffie-Hellman protocol[C]// Proceedings of CRYPTO 2005. Berlin: Springer-Verlag, 2005:546-566.

[9] LAMACCHIA K, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange[C]// Proceedings of ProvSec 2007. Berlin: Springer-Verlag, 2007:1-16.

[10] BRESSEN E, MANULIS M. Securing group key exchange against strong corruptions[C]// Proceedings of ASIACCS'08. New York: ACM, 2008:249-260.

[11] 南湘浩,陈华平. 组合公钥(CPK)体制标准 V2.1[J]. 计算机安全, 2008(9):1-2.

[12] BRESSON E, CHEVASSUT O, POINTCHEVAL D, *et al*. Provably authenticated group Diffie-Hellman key exchange[C]// Proceedings of ACM CCS'01. New York: ACM, 2001:255-264.

[13] CHOI K, HWANG J, LEE D. Efficient ID-based group key exchange with bilinear maps[C]// Proceedings of PKC'04. Berlin: Springer-Verleg, 2004: 130-144.

[14] ZHANG F, CHEN X. Attack on an ID-based authenticated group key exchange scheme from PKC 2004[J]. Information Processing Letters, 2004, 91(4):191-193.

(上接第1804页)

研究而言，定点格式下与浮点格式下所得的研究结果不能轻易相互引用。本文给出的混沌序列周期随浮点计算精度变化的分布关系，对于混沌加密理论而言具有重要意义，为寻找混沌系统的抗退化机制提供了一个检测的参考标准。

参考文献：

[1] LI SHUJUN, CHEN GUANRONG, MOU XUANQIN. On the dynamical degradation of digital piecewise linear chaotic maps[J]. International Journal of Bifurcation and Chaos, 2005, 15(10): 3119-3151.

[2] GREBOGI C, OTT E, YORKE J A. Roudoff-induced periodicity and the correlation dimension of chaotic attractors[J]. Physical Review A, 1988, 38(7): 3688-3692.

[3] CURIAC D I, IERCAN D, DRANGA O, *et al*. Chaos-based cryptography: end of the road?[C] // Proceedings of the International Conference on Emerging Security Information, Systems, and Technologies. Washington, DC: IEEE Computer Society, 2007:71-76.

[4] LI S J, MOU X Q, CAI Y L, *et al*. On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computing precision[J]. Computer Physics Communications, 2003, 153(1): 52-58.

[5] 盛利元,闻姜,曹莉凌,等. TD-ERCS 混沌系统的差分分析[J]. 物理学报, 2007, 56(1): 78-83.

[6] CERNAK J. Digital generators of chaos[J]. Physica Letters A, 1996, 214(3/4): 151-160.

[7] BECK C, ROEPSTORFF G. Effects of phase space discretization on the long-time behavior of dynamical systems[J]. Physica D, 1987, 25(1/3): 173-180.

[8] MAO YAOBIN, CAO LIU, LIU WENBO. Design and FPGA implementation of a pseudo-random bit sequence generator using spatio-temporal chaos[EB/OL]. [2009-10-05]. http://citeseerx.ist.psu.edu/viewdoc/download%3Fdoi%3D10.1.1.113.9525.

[9] DAVID G. What every computer scientist should know about floating-point arithmetic[J]. ACM Computer Surveys, 1991, 23(1): 5-48.

[10] IEEE Std 754-2008. IEEE standard for floating-point arithmetic[S], 2008.