基于身份密钥交换的安全模型

刘文菊[1]，张俊伟[2]，马建峰[2]，杨超[2]，李兴华[2]

（1. 天津工业大学 计算机科学与软件学院，天津 300160；

2. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071）

摘 要：研究了基于身份的密钥交换协议的可证明安全问题。在通用可组合安全框架下，提出了基于身份密钥交换协议的模型。在攻击模型中，添加了攻陷密钥生成中心的能力。根据基于身份密钥交换的特点，设计了基于身份密钥交换的理想函数。在新的攻击模型和理想函数下，提出的模型既保证了基于身份密钥交换的通用可组合安全性，又保证了一个重要的安全属性——密钥生成中心前向保密性。此外，带有密钥确认属性的 Chen-Kudla 协议可以安全实现基于身份密钥交换的理想函数。

关键词：基于身份密钥交换；UC 安全；密钥生成中心前向保密性

中图分类号：TP309 **文献标识码**：B **文章编号**：1000-436X(2010)03-0089-06

Security model for ID-based key exchange

LIU Wen-ju[1], ZHANG Jun-wei[2], MA Jian-feng[2], YANG Chao[2], LI Xing-hua[2]

(1. School of Computer Science and Software, Tianjin Polytechnic University, Tianjin 300160, China;

2. Key Laboratory of Computer Networks and Information Security (Ministry of Education), Xidian University, Xi'an 710071, China)

Abstract: The provable security of ID-based key exchange protocols was investigated. In the universally composable framework, the provable secure model of ID-based key exchange was proposed. The ability of the adversary to corrupt key generation center was added to the adversary model. According to the characteristics of ID-based key exchange, the ideal functionality of ID-based key exchange was presented. Based on the adversary model and the ideal functionality, the proposed model captures not only the universally composable security of ID-based key exchange, but also implies one of the important properties of ID-based key exchange——key generation center forward secrecy. In addition, the protocol (with key confirmation) proposed by Chen and Kudla can securely realize the functionality of ID-based KE with KGC-FS.

Key words: ID-based key exchange; UC secure; key generation center forward secrecy

1 引言

1984 年，Shamir 首次提出了基于身份（ID-based）的非对称密码系统的概念[1]。与传统的非对称密码系统不同，ID-based 密码系统简化了密钥管理的过程：用户的公钥可以由用户的身份信息产生，而私钥由一个可信的密钥生成中心产生。随着 ID-based 密码学的发展，一些基于身份的密钥交换(ID-based KE)协议被提出[2,3]。在 AKE 安全模型[4]下，Chen 和 Kudla 研究了可证安全的 ID-based KE[4]。在

收稿日期：2009-09-02；**修回日期**：2010-02-11

基金项目：天津科技攻关计划基金资助项目（06YFGZGX17500）；国家自然科学基金资助项目（60573036，60702059）

Foundation Items: The Science and Technology Problem of Tianjin (06YFGZGX17500); The National Natural Science Foundation of China(60573036, 60702059)

Canetti-Krawczyk 模型(CK 模型)下，ID-based KE 的可证安全模型也被提出[5,6]。但 AKE 安全模型和 CK 模型[7]仅仅保证 ID-based KE 协议在独立运行情况下的安全性，而不能保证协议组合情况下的安全性。

通用可组合安全框架(UC, universally composable framework)[8]可以保证协议的组合安全性，即在 UC 框架下证明安全的协议，在该协议与其他协议并发运行的情况下，或者该协议作为一个系统的组件时，仍能保证协议的安全性。理想函数是 UC 安全框架中十分重要的部分，它扮演着一个不可攻陷的可信角色，能够完成协议所执行的特定功能。目前已经定义了多个理想函数，如认证消息传输、安全消息传输、密钥交换、公钥加密、签名、承诺、不经意传输[9]等。

在 UC 框架下设计协议的困难和核心内容就在于形式化和抽象一个完美的并且可以安全实现的理想函数。Nishimaki 等在 UC 框架中提出了 ID-based Encryption 和 ID-based Signature 的理想函数[10,11]。但在 UC 框架中针对 ID-based KE 还没有形式化的定义。

本文在 UC 框架下提出了基于身份密钥交换的安全模型。针对 ID-based KE 的安全需求，在攻击模型添加了攻陷密钥生成中心的能力，并设计了 ID-based KE 的理想函数。在新的攻击模型和理想函数下，提出的模型既保证了 ID-based KE 的通用可组合安全性，又保证了一个重要安全属性——密钥生成中心前向保密性(KGC-FS, key generation center forward secrecy)。针对理想函数的实现问题，证明了带有密钥确认属性(key confirmation)的 Chen-Kudla 协议能安全实现 ID-based KE 的理想函数。

本文剩余部分组织如下：第 2 节介绍了 UC 框架；第 3 节在 UC 框架下给出了满足 ID-based KE 安全需求的理想函数；第 4 节证明了带有密钥确认属性的 Chen-Kudla 协议能安全实现 ID-based KE 的理想函数；第 5 节是结束语。

2 UC 框架

UC 框架如图 1 所示。首先，UC 框架定义了现实环境。现实环境描述协议的真实运行情况，其中所有参与方在真实敌手攻击 $\mathcal{A}$ 存在的环境下运行真实协议。其次，UC 框架定义了理想环境用来描述密码协议的理想运行。在理想环境下，存在虚拟参与方，理想敌手 $\mathcal{S}$ 和一个理想函数 $\mathcal{F}$。参与方之间以及敌手 $\mathcal{S}$ 与参与方不直接通信；所有参与方和敌手 $\mathcal{S}$ 均与理想函数交互。理想函数本质上是一个不可攻陷的可信角色，用来完成协议所需的理想运行和功能。在 UC 的安全框架中，环境 $\mathcal{Z}$ 来模拟协议运行的整个外部环境（包括其他并行的协议、攻击者等），$\mathcal{Z}$ 可以与所有的参与者以及攻击者 $\mathcal{A}$ 和 $\mathcal{S}$ 直接通信，$\mathcal{Z}$ 不允许直接访问理想函数 $\mathcal{F}$。

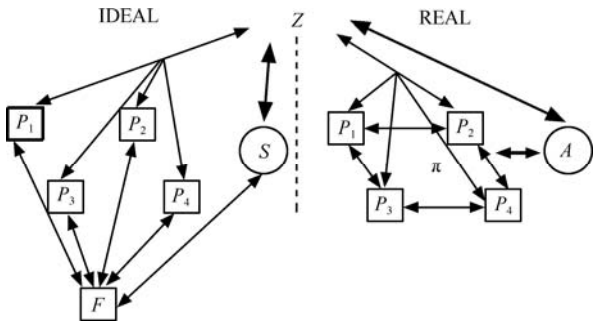


图 1 UC 框架

1) UC 仿真

协议 π 仿真理想函数 $\mathcal{F}$ 当且仅当对于任意现实敌手 $\mathcal{A}$，存在理想敌手 $\mathcal{S}$，使得任意环境 $\mathcal{Z}$，至多以可忽略的概率来区分：存在真实敌手 $\mathcal{A}$ 及协议 π 的现实环境和存在理想敌手 $\mathcal{S}$ 及理想函数 $\mathcal{F}$ 的理想环境。如果协议 π 能 UC 仿真理想函数 $\mathcal{F}$，就称协议 π 在 UC 框架下安全实现了理想函数 $\mathcal{F}$，也称 π 是 UC 安全的。

2) UC 仿真的传递性

如果协议 π_1 能 UC 仿真协议 π_2 并且协议 π_2 能 UC 仿真协议 π_3，那么 π_1 可以 UC 仿真 π_3。

3) 组合定理[8]

如果协议 ρ 实现理想函数 $\mathcal{F}$，且 π 是 $\mathcal{F}$-混合模型[8]下的协议，那么协议 $\pi^{\rho/\mathcal{F}}$（用协议 ρ 替换协 π 中的理想函数 $\mathcal{F}$ 所得到的组合协议）UC 仿真 $\mathcal{F}$-混合模型下的协议 π。特别地，如果协议 π 在 $\mathcal{F}$-混合模型下实现理想函数 $\mathcal{G}$，那么协议 $\pi^{\rho/\mathcal{F}}$ 也实现了理想函数 $\mathcal{G}$。

3 ID-based KE 的理想函数

3.1 攻陷 KGC

在 UC 框架中，给攻击者增加了攻陷 KGC 的能力(记为 CorruptKGC)。当攻击者发起 CorruptKGC 攻击后，攻击者可以获得 KGC 的内部状态，即系统主密钥，这就意味着所有参与方的长期私钥泄

漏。同时，KGC 被标记为 corrupted；所有参与者被记为 compromised（compromised 表明该参与方的长期密钥已经泄漏）。需要特别指出的是：由于 KGC 的特殊性，这里假定 KGC 不能被已有的 Corrupt 攻陷，只能被 CorruptKGC 攻陷。

3.2 理想函数 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$

理想函数 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 如下。

Setup

当从 KGC 收到 (Setup, *sid*, *KGC*)：

- 将(Setup, *sid*, *KGC*)发送给 $\mathcal{S}$；
- 当从 $\mathcal{S}$ 收到(Set, *sid*, PK_s), 给 KGC 输出(Set, *sid*, PK_s)；
- 记录(*KGC*, PK_s)并标记为 fresh。

Extract

当从 P_i 收到(Extract, *sid*, ID_i, PK_s')：

- 如果记录(*KGC*, PK_s')存在, ID_i 是 P_i 的身份标识, 那么在 ID-Reg 中记录(ID_i, P_i), 标示为 fresh. 否则, 不记录；
- 将(Extract, *sid*, ID_i, PK_s')发送给 $\mathcal{S}$, 随后从 $\mathcal{S}$ 收到(Received, *sid*)；
- 将(Extracted, *sid*, ID_i, PK_s')发送给 P_i 和 KGC(如果 PK_s'没有被记录,或者 ID_i 不是 P_i 的身份标识, 不发送这个消息)。

Key Exchange

当从 P_i 收到 (NewSession, *sid*, P_i, P_j, *role*, ID_i, PK_s')：

- 将(NewSession, *sid*, P_i, P_j, role, ID_i, PK_s')发送给 $\mathcal{S}$；
- 如果这是第一个 NewSession 质询并且存在记录(*KGC*, PK_s')和(ID_i, P_i), 或者这是第二个 NewSession 质询且(P_j, P_i, ID_j)已被记录, 存在记录(*KGC*, PK_s')和(ID_i, P_i), 那么记录(P_i, P_j, ID_i)。

当从 $\mathcal{S}$ 收到 (NewKey, *sid*, P_i, ID_i, *sk*), 其中 |*sk*|=*k*, 如果存在记录(P_i, P_j, ID_i)且这是对 P_i 的第一次 NewKey 质询, 那么：

- 如果 P_i 或 P_j 被攻陷,输出(*sid*, *sk*)给 P_i；
- 否则, 如果存在记录(P_j, P_i, ID_j), 且已经给 P_j 发送过密钥 *sk*',输出(*sid*, *sk*')给 P_i；
- 否则, 选取一个新的随机数 *sk*'（长度为 *k*）作为密钥, 发送(*sid*, *sk*')给 P_i。

当从 $\mathcal{S}$ 收到 (Corrupt, *sid*, P_i)：

如果 P_i 不是 KGC 且 P_i 还没被攻陷, 那么：

- 将 P_i 标记为 corrupted；
- 如果记录(ID_i, P_i)未泄露, 标示 P_i 为 compromised。

当收到来自敌手 $\mathcal{S}$ 的消息(CorruptKGC, *sid*, *KGC*):

如果 KGC 未被攻陷, 那么：

- 将 KGC 标示为 corrupted；
- 如果存在记录(*KGC*, PK_s'), 那么 ID-Reg 中的所有未泄露记录标示为 compromised。

其中 Setup：当 KGC 发送系统建立的请求时，理想函数将这个请求发送给敌手 $\mathcal{S}$。$\mathcal{S}$ 决定系统的公共参数并且将这些参数发送给 KGC。

Extract：当参与方发出注册请求时，理想函数在 ID-Reg 中记录这个 ID 并将这个请求发送给敌手 $\mathcal{S}$。当收到 $\mathcal{S}$ 的响应时，将结果发送给参与方和 KGC。

Key Exchange：在会话密钥产生前，如果任意一方被攻陷，敌人 $\mathcal{S}$ 可以决定会话密钥的值。否则，$\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 生成一个随机数作为会话密钥。

3.3 KGC-FS

KGC-FS：即使 KGC 被攻陷（这意味着系统主密钥泄露，进而导致系统中所有参与方的长期私钥泄露），任何已经建立的密钥仍是安全的。KGC-FS 属性也保证了另一个重要属性——无密钥托管（without key escrow）。

KGC-FS 对于 ID-based KE 是一个非常重要的属性。一方面，如果 ID-based KE 协议不能保证 KGC-FS，那么 KGC 就可以获得系统中任意两方协商的会话密钥，进而得到双方交换的消息内容。如果通信双方希望保证他们通信的机密性，甚至也不希望 KGC 获得他们之间的通信内容，那么 ID-based KE 协议就必须满足 KGC-FS，即无密钥托管。另一方面，如果不能保证 KGC-FS，那么，当 KGC 被攻陷时，敌人可以获得所有系统中已经建立的会话密钥，进而得到系统中所有的已经通信的消息内容。

理想函数 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 满足 KGC-FS。原因如下：$\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 会对 CorruptKGC 做出相应的响应。但是，在仅仅发生 CorruptKGC 的情况下，产生的会话密钥仍然是随机的，即敌手不能决定会话密钥的值，不能威胁会话密钥的安全。

4 实现 ID-based KE 的理想函数

本节证明带有密钥确认属性的 Chen-Kudla 协

议（记为 π_{idKE}）能安全实现理想函数 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$。

需要说明的是，在 Setup 和 Extract 阶段，协议运行在一个安全的信道下。这样可以确保系统主密钥和参与方长期私钥在密钥交换前的安全性。下面给出了协议 π_{idKE} 的详细描述。

Setup

当 KGC 输入(Setup, *sid*, P_s)：

- KGC 产生 2 个群(G_1, +) (G_2,×), $G_1 \times G_1 \mapsto G_2$；
- H 是散列函数，f 和 g 是伪随机函数；
- 随机选择系统密钥 $s \in Z_q^*$，系统公钥为 $P_{\text{pub}}=sP$；
- KGC 将 s 作为系统密钥，并公开系统参数 PK_s= (G_1, G_2, e, n, P, P_{pub}, H, f, g)，输出(Set, *sid*, PK_s)。

Extract

当 P_i 输入(Extract, *sid*, ID_i, PK_s')，如果 PK_s'存在且 ID_i 是 P_i 身份标识：

- 令 $Q_i=H(ID_i)$, P_i 的私钥为 $S_i=sQ_i$, 秘密地发送 S_i 给 P_i；
- 输出 (Extracted, *sid*, ID_i, PK_s')。

参与方 P_j 的注册过程与 P_i 的过程类似。

Key Exchange

发起者 P_i 输入(P_i, P_j, *sid*, *ID*, *initiator*)，类似地，响应者输入(P_j, P_i, *sid*, *ID'*, *responder*)。

- P_i 随机选择 $a \in Z_q^*$，发送(P_i, *sid*, μ, α)给 P_j，其中, $\mu=aQ_i$, $\alpha=aP$；
- 收到(P_i, *sid*, μ, α)后, P_j 随机选择 $b \in Z_q^*$，令 $v=bQ_j$, $\beta=bP$，P_j 计算 $\gamma_1=e(\mu+bQ_i, S_j)$, $\gamma_2=b\alpha$, 并删除 b，计算 $\kappa_d=f((\gamma_1, \gamma_2), 0)$,$\kappa_a=f((\gamma_1, \gamma_2), 1)$，则 $\sigma_j=g(\kappa_a, (ID, ID', \mu, v, \alpha, \beta, l)$, 其中 l 为消息计数器，发送(P_j, *sid*, v, β, l, σ_j)给 P_i；
- 收到(P_j, *sid*, v, β, l, σ_j)后, P_i 计算 $\kappa_d'= f((\gamma_1', \gamma_2'), 0)$和 $\kappa_a' =f((\gamma_1', \gamma_2'), 1)$, 并删除 a, 其中 $\gamma_1'=e(S_i, v + aQ_j)$, $\gamma_2'=a\beta$，然后, P_i 用 κ_a'验证 σ_j 的正确性，如果正确, P_i 计算 $\sigma_i=g(\kappa_a', (ID, ID', \mu, v, \alpha, \beta, l'))$, l'为消息计数器，发送(P_i, *sid*, l', σ_i)给 P_j, 输出(*sid*, P_i, P_j, κ_d')；
- 收到(P_i, *sid*, l', σ_i)后, P_j 用 κ_a 验证 σ_i 的正确性，如果正确, 输出(*sid*, P_j, P_i, κ_d)。

定理 1 如果 BDH 假设和 CDH 假设成立，f 和 g 是伪随机函数，则 π_{idKE} 安全实现理想函数 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$。

证明 令现实敌手为 $\mathcal{A}$。构造理想敌手 $\mathcal{S}$，对于任何环境 $\mathcal{Z}$ 仅能以一个可忽略的概率区分是：$\mathcal{A}$ 与 π_{idKE} 交互的真实环境(标记为 *REAL*)和 $\mathcal{S}$ 与 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 交互的理想环境(标记为 *IDEAL*)。

1) 构造 $\mathcal{S}$

首先构造内部状态仿真器 I (如果 g 是伪随机函数，π_{idKE} 具有应答属性)。输入(κ_d, s, P_i, P_j)，I 输出 $\tau_i=\tau_j=(\kappa_d, r, s, P_i, P_j)$，其中 r 是随机数且$|r|=|\kappa_d|$。有关应答属性和内部状态仿真器的详细内容请参阅文献[12]。

敌手 $\mathcal{S}$ 运行如下。

Setup

当 $\mathcal{S}$ 从 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 收到(Setup, *sid*, *KGC*)且 KGC 未被攻陷，$\mathcal{S}$ 为 $\mathcal{A}$ 仿真 π_{idKE} 并以(Setup, *sid*, *KGC*)为输入。

π_{idKE} 输出(Set, *sid*, PK_s)后，当从 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 收到(Setup, *sid*, *KGC*)时，$\mathcal{S}$ 将(Set, *sid*, PK_s)发给 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$。

Extract

当 $\mathcal{S}$ 从 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 收到(Extract, *sid*, ID_i, PK_s')且 P_i 未被攻陷，$\mathcal{S}$ 将(Extract, *sid*, ID_i, PK_s')作为输入运行 π_{idKE}。

π_{idKE} 输出(Extracted, *sid*, ID_i, PK_s')后，当 $\mathcal{S}$ 从 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 收到(Extract, *sid*, ID_i, PK_s')时，发送(Received, *sid*)给 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$。

Key Exchange

当 $\mathcal{S}$ 从 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 收到(NewSession, *sid*, P_i, P_j, *role*, ID_i, PK_s')，即 P_i 请求与 P_j 运行密钥交换协议(会话标识为 *sid*)，$\mathcal{S}$ 以(*sid*, P_i, P_j, *role*)为输入运行 π_{idKE}。

当 $\mathcal{A}$ 发送 (P_i, *sid*, μ, α)给 P_j，$\mathcal{S}$ 仿真从 P_i 到 P_j 的消息(P_i, *sid*, μ, α)。同样，当 $\mathcal{A}$ 发送 (P_j, *sid*, v, β, l, σ_j)给 P_i，σ_j 为 MAC 值，$\mathcal{S}$ 仿真从 P_j 到 P_i 的消息(P_j, *sid*, v, β, l, σ_j)。当 $\mathcal{A}$ 发送 (P_i, *sid*, l', σ_i)给 P_j，σ_j 为 MAC 值，$\mathcal{S}$ 仿真从 P_i 到 P_j 的消息(P_i, *sid*, l', σ_i)。

当 π_{idKE} 输出(*sid*, P_i, P_j, κ)时，$\mathcal{S}$ 发送(NewKey, *sid*, P_i, κ)给 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$。

CorruptKGC

当 $\mathcal{A}$ 攻陷 KGC 时，$\mathcal{S}$ 发送(CorruptKGC, *sid*, *KGC*)给 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$。

Corrupt

当 $\mathcal{A}$ 攻陷 P_i 时，$\mathcal{S}$ 发送(Corrupt, *sid*, P_i)给 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$。在这种情况下，如果 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$ 已经发送密钥给 P_i，那么 $\mathcal{S}$ 获得密钥 κ。另外，如果在发生攻陷时，P_i 和 P_j

都没有输出密钥，那么，$\mathcal{S}$ 将 π_{idKE} 中 P_i 的内部状态发送给 $\mathcal{A}$。如果在发生攻陷的时刻，P_i 或 P_j 已经输出密钥，$\mathcal{S}$ 应用内部状态仿真器 I 得到仿真的内部状态 τ_i 和 τ_j，并且将 τ_i 发送给 $\mathcal{A}$ 作为 P_i 的内部状态(如果 P_j 被攻陷，那么 $\mathcal{A}$ 将得到 τ_j)。

2) IDEAL 和 REAL 的不可区分性

根据仿真器 $\mathcal{S}$，证明不可区分性分为以下 3 种情况：CORRUPT 事件表示 P_i 或 P_j 至少有一个被攻陷（事件 1）；NONE 事件表示 CORRUPT 和 CKGC 均未发生（事件 2）；CKGC 表示 KGC 被攻陷，P_i 和 P_j 未被攻陷（事件 3）。然后，证明在这 3 种事件下，IDEAL 和 REAL 是不可区分的。

事件 1　CORRUPT

当 CORRUPT 事件发生时，$\mathcal{S}$ 完美仿真了敌手 $\mathcal{A}$，因此，IDEAL 和 REAL 是不可区分的。

事件 2　NONE

首先定义协议 π_0、π_1 和 π_2。π_0：π_0 随机选取 γ_1(或 γ_1')和 γ_2(或 γ_2')，然后 π_0 随机产生 κ_d 和 κ_a，以及 MAC 值。π_1：与 π_0 相比，修改了计算 γ_1(或 γ_1')和 γ_2(或 γ_2')的方法。π_1 计算 $\gamma_1=e(\mu+bQ_i, S_j)$和 $\gamma_1'=e(S_i, \nu+aQ_j)$。类似地，$\gamma_2=b\alpha$ 和 $\gamma_2'=a\beta$。π_2：与 π_1 相比，修改了计算 κ_d(or κ_d')和 κ_a(or κ_a')的方法。π_2 使用伪随机函数 f 计算 κ_d 和 κ_d'。类似地，π_2 使用 f 计算 κ_a 和 κ_a'。

π_0 随机选取 γ_1(或 γ_1')和 γ_2 (或 γ_2')的值，随机产生会话密钥和 MAC 值，那么 π_0 的输出为随机数。因此，从环境 $\mathcal{Z}$ 的角度，IDEAL 和 π_0 是不可区分的，即 $IDEAL\approx\pi_0$。

引理 1　如果 BDH 假设和 CDH 假设成立，π_1 和 π_0 是不可区分的，即 $\pi_0\approx\pi_1$。

假设存在环境 $\mathcal{Z}$ 以不可忽略的概率区分 π_1 和 π_0。在 $\mathcal{Z}$ 的基础上，能构造 2 个算法 $\mathcal{D}_1$ 和 $\mathcal{D}_2$。$\mathcal{D}_1$ 能在概率多项式时间内（PPT）以不可忽略的概率解决 BDH 问题，这与 BDH 假设相矛盾。类似地，$\mathcal{D}_2$ 可以成功解决 CDH 问题，这与 CDH 假设矛盾。

由于篇幅限制，这里简要地给出 $\mathcal{D}_1$ 算法的核心内容来说明 $\mathcal{D}_1$ 如何利用 $\mathcal{Z}$ 来解决 BDH 问题。

$\mathcal{D}_1$ 选择 x 作为系统主密钥，xP 作为系统公钥。

$\mathcal{D}_1$ 令 P_i 的公钥为 $Q_i=yP$，P_j 的公钥为 $Q_j=(a+b)^{-1}zP$。

$\mathcal{D}_1$ 激活 $\mathcal{Z}$，运行协议 π_0 和 $\mathcal{A}$，其中 $\mu=aP$，$\nu=bP$。

当 $\mathcal{Z}$ 输出 1 时，$\mathcal{D}_1$ 计算 $\gamma_1=e(yP,(a+b)^{-1}zP)^{x(a+b)}=e(P,P)^{xyz}$。

因此，如果 $\mathcal{Z}$ 能以不可忽略的概率区分 π_0 和 π_1，$\mathcal{D}_1$ 也能以不可忽略的概率解决 BDH 问题。这与 BDH 假设相矛盾。$\mathcal{D}_2$ 与 $\mathcal{D}_1$ 类似，这里不做赘述。

引理 2　如果函数 f 是伪随机函数，π_2 和 π_1 是不可区分的，即 $\pi_1\approx\pi_2$。

如果 $\mathcal{Z}$ 能以不可忽略的概率区分 π_2 和 π_1，则能构造一个区分器区分伪随机函数 f 生成的数和随机数。这与函数 f 是伪随机函数相矛盾。

引理 3　如果函数 g 是伪随机函数，REAL 和 π_2 是不可区分的，即 $\pi_2\approx REAL$。

证明过程与引理 2 类似。

根据 UC-仿真的传递性，如果 BDH 假设和 CDH 假设成立，f 和 g 是伪随机函数，那么 $IDEAL\approx\pi_0\approx\pi_1\approx\pi_2\approx REAL$。即事件 NONE 发生时，$\mathcal{Z}$ 仅能以可忽略的概率区分 REAL 和 IDEAL。

事件 3　CKGC

事件 CKGC 发生时，$\mathcal{Z}$ 只能以可忽略的概率区分 REAL 和 IDEAL。这与发生 NONE 事件的证明类似。唯一的区别在于 $\pi_1\approx\pi_0$ 的证明。在这里，π_1 和 π_0 的不可区分性仅仅依靠 CDH 假设，而不是 BDH 假设，因为 $\mathcal{Z}$ 可以计算 $\gamma_1=e(S_i, \nu)\times e(\mu, S_j)$。

根据以上 3 种情况的分析，定理 2 得证。　□

5　结束语

本文在 UC 框架下提出了基于身份密钥交换的可组合安全模型。在攻击模型中添加了 CorruptKGC，设计了 ID-based KE 理想函数 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$。提出的模型满足了 ID-based KE 的通用可组合安全性和 KGC-FS。同时，证明了带有密钥确认性质的 Chen-Kudla 协议可以安全实现理想函数 $\mathcal{F}_{\text{idKE}}^{\text{KGC}}$。

参考文献：

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Advances in Cryptology-CRYPTO'84[C]. Springer-Verlag, 1984. 47-53.

[2] CHEN L, KUDLA C. Identity based authenticated key agreement protocols from pairings[A]. CSFW'03[C]. 2003.219-236.

[3] 汪小芬, 陈原, 肖国镇. 基于身份的认证密钥协商协议的安全分析与改进[J]. 通信学报, 2008, 29(12):16-21.
WANG X F, CHEN Y, XIAO G Z. Analysis and improvement of an ID-based key agreement protocol[J]. Journal on Communications, 2008, 29(12): 16-21.

[4] BELLARE M, ROGAWAY P. Entity authentication and key distribution[A]. Advances in Cryptology-Crypto'93[C]. 1993. 232-249.

[5] LI X H, MA J F, MOON S J. Security extension for the

canetti-krawczyk model in identity-based system[J]. Science in China (F series), 2005, 48(1): 117-124.

[6] ZHU R W, TIAN X J, WONG D S. A suite of enhanced security models for key compromise impersonation resilience and ID-based key exchange[EB/OL]. http://eprint.iacr. org/2005/ 455, 2005.

[7] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[A]. Proc EUROCRYPT 2001[C]. Springer-Verlag, 2001. 453-474.

[8] CANETTI R. Universally composable security: a new paradigm for cryptographic protocols[EB/OL]. http://eccc.uni-trier.de/eccc-reports/ 2001/ TR01-016/, 2001.

[9] 李凤华,冯涛,马建峰. 基于 VSPH 的 UC 不经意传输协议[J]. 通信学报, 2007, 28(7):28-34.
LI F H, FENG T, MA J F. Universally composable oblivious transfer protocol based on VSPH[J]. Journal on Communications, 2007, 28(7):28-34.

[10] NISHIMAKI R, MANABE Y, OKAMOTO T. Universally composable identity-based encryption[A]. The 2006 Symposium on Cryptography and Information Security Hiroshima[C]. Japan, 2006.17-20.

[11] NISHIMAKI R, MANABE Y, OKAMOTO T. Universally composable identity-based encryption[J]. IEICE Trans Fundamentals, 2008, (E91-A) (1): 262-271.

[12] CANETTI R, KRAWCZYK H. Universally composable key exchange and secure channels[A]. Eurocrypt 02[C]. 2002. 337-351.

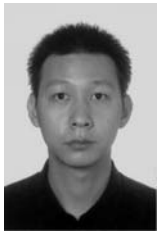
作者简介：

刘文菊（1963-），女，天津人，天津工业大学副教授，主要研究方向为网络安全和计算机智能监控。

张俊伟（1982-），男，陕西西安人，西安电子科技大学博士生，主要研究方向为密码学、网络安全。

马建峰（1963-），男，陕西西安人，西安电子科技大学教授、博士生导师，主要研究方向为计算机安全、密码学。

杨超（1979-），男，陕西西安人，西安电子科技大学副教授，主要研究方向为无线网络安全、协议测试与仿真。



李兴华（1978-），男，河南南阳人，西安电子科技大学副教授，主要研究方向为无线网络安全、协议形式化分析与设计。