改进的基于标准模型的一轮密钥交换协议

胡学先[①] 刘文芬[①] 兰巨龙[②]
[①](信息工程大学信息工程学院 郑州 450002)
[②](国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：该文提出了一个一轮密钥交换协议。协议是基于标准模型的，没有用到可能会影响协议安全性的真随机谕示模型(ROM)。基于 DDH 假设和伪随机函数簇两个基本的计算复杂度假设，可以证明协议是 SK 安全的，并且协议具有较低的通信复杂度和计算复杂度。

关键词：密钥交换协议；可证明安全；标准模型
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2009)11-2720-05

Improved One-Round Key Exchange Protocol in the Standard Model

Hu Xue-xian[①] Liu Wen-fen[①] Lan Ju-long[②]
[①](*Department of Information Research*, *Information Engineering University*, *Zhengzhou* 450002, *China*)
[②](*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: In this paper, a new authenticated key exchange protocol is proposed and its security is proved in the stronger version of the well-known CK model revised by Krawczyk. The analysis of the protocol is under standard model instead of Random Oracle Model (ROM). The proposal is based on the two basic computational complexity assumptions of DDH assumption and the existence of Pseudo Random Function (PRF) family. Compared with Boyd et al.'s protocol, the protocol possesses simpler communication and computation complexity.

Key words: Key exchange protocol; Provable security; Standard model

1 引言

密钥交换协议在对称密钥系统中起着重要的作用，它使得两个或多个用户能够利用不安全的信道建立一个共享的会话密钥，用于数据的安全传输。虽然密钥交换协议对密码系统至关重要，但众多密码学家的研究表明，设计安全、高效、实用的密钥交换协议是密码学中的困难问题之一[1,2]。

为了保证所设计的协议能够抵抗各种攻击方法，需要在严格的形式化分析模型下证明协议的安全性可以归约为一些公认的计算困难性问题。文献[3]提出了密钥交换的第 1 个形式化分析模型，但是存在敌手能力过弱，模型可移植性不强等缺点。随后，人们提出了一系列的安全性模型[1−4]。CK2001 模型[1]是其中较为典型的一种，该模型考虑了部分用户的内部状态泄露对其它用户间的密钥协商的影响，但是没考虑 KCI 攻击。2005 年 Krawczyk[5]对 CK 模型作了进一步修改使之能够抵抗 KCI 攻击。模型安全性的逐渐增强导致在早期模型下设计并证明安全的密钥交换协议在现有模型中可能存在安全性问题。

关于密钥交换协议分析和设计的另外一个问题是，早期的协议多基于随机谕示模型(ROM)[6][6]。而 Dent[7]指出，在 ROM 下证明安全的协议在实际中可能会存在安全性缺陷。因此，现在协议设计的趋势之一是采用标准模型，即不采用随机谕示假设。

Boyd 等在文献[8]中提出了一个标准模型下安全的密钥交换协议，协议分析基于 Krawczyk 等修改的 CK 模型，能保证协议抗 KCI 攻击。但是，该协议依靠额外的 DH 交换提供前向安全性。本文提出了一个新的基于标准模型的密钥交换协议，利用加密的 DH 指数同时保证会话密钥的私密性和前向安全性，该协议在和 Boyd 等的协议具有相同的安全性的前提下，具有更低的通信复杂度和计算复杂度。

2 预备知识

本节给出协议中将用到的一些假设和定义。

DDH 假设 设$\mathbb{G}=<g>$是阶为素数p的乘法循环群，满足$|p|=k$。定义集合$\mathbb{D}=\{(g^a,g^b,g^{ab})\,|\,a,b\in\mathbb{G}\}$，$\mathbb{R}=\{(g^a,g^b,g^c)\,|\,a,b,c\in\mathbb{G}\}$。如果对任意的概率多项式时间攻击者$\mathcal{D}$，其区分上述两个集合上的均匀分布的优势

2008-11-24 收到，2009-06-08 改回
国家 863 计划项目(2007AA01Z2a1)资助课题

$$\mathrm{Adv}_{G,\mathcal{D}}^{\mathrm{DDH}}(k)=|\Pr\{\mathcal{D}(1^k,\rho)=1\mid\rho\overset{U}{\leftarrow}\mathbb{D}\}-\Pr\{\mathcal{D}(1^k,\rho)=1\mid\rho\overset{U}{\leftarrow}\mathbb{R}\}| \quad (1)$$

均是可忽略的，则称 G 满足 DDH 假设。

伪随机函数簇(PRF)　设 k 是安全参数。一个函数总体 $F=\{F_k\}_{k\in\mathbb{N}}$ 是一个随机变量序列 $F=\{F_k\}_{k\in\mathbb{N}}$，其中 F_k 的取值空间是所有 $\{0,1\}^{l_1(k)}$ 到 $\{0,1\}^{l_2(k)}$ 的函数的集合。相应的均匀函数总体是 $H=\{H_k\}_{k\in\mathbb{N}}$，其中 H_k 是所有 $\{0,1\}^{l_1(k)}$ 到 $\{0,1\}^{l_2(k)}$ 函数的集合上的均匀分布。如果对任意能够访问谕示 $\mathcal{O}$ 的概率多项式时间攻击者 $\mathcal{D}^{\mathcal{O}}$，其优势

$$\mathrm{Adv}_{F,\mathcal{D}}^{\mathrm{PRF}}(k)=|\Pr[\mathcal{D}^{F_k}(1^k)=1]-\Pr[\mathcal{D}^{H_k}(1^k)=1]| \quad (2)$$

均是可忽略的，则称函数总体 $F=\{F_k\}_{k\in\mathbb{N}}$ 是伪随机的。本文用到的 F_k 是集合 $\{f_s:\{0,1\}^{4k}\to\{0,1\}^k\}_{s\in G_k}$ 上的均匀分布。

基于身份的加密体制(IBE)　一个基于身份的加密体制 $\varepsilon=(\mathrm{KeyGen},\mathrm{KeyDer},\mathrm{Enc},\mathrm{Dec})$ 由以下 4 个多项式时间算法组成：

(1) $(pk,\alpha)\leftarrow\mathrm{KeyGen}(1^k)$，给定安全参数 $k\in\mathbb{N}$，主密钥生成函数 KeyGen 生成可信中心(PKG)的公开密钥 pk 和私钥 α；

(2) $d_{id}\leftarrow\mathrm{KeyDer}(pk,\alpha,id)$，给定用户身份 id，生成对应该身份的私钥；

(3) $C\leftarrow\mathrm{Enc}(pk,id,m)$，给定用户身份 id 和消息 m，生成密文 C；

(4) $m\leftarrow\mathrm{Dec}(pk,d_{id},C)$，给定密文 C，解密得到相应的消息 m。

基于身份的加密体制的安全性通过下述游戏来定义：

$\mathrm{Experiment}\ \mathrm{Exp}_{\varepsilon,\mathcal{A}}^{\mathrm{IBE}}(k)$

$(pk,\alpha)\leftarrow\mathrm{KeyGen}(1^k)$

$(id^*,m_0,m_1,\mathrm{state})\leftarrow\mathcal{A}^{\mathcal{O}_{\mathrm{KeyDer}}(\cdot),\mathcal{O}_{\mathrm{Dec}}(\cdot,\cdot)}(\mathrm{find},pk)$

$b\overset{U}{\leftarrow}\{0,1\},C^*=\mathrm{Enc}(pk,id,m_b)$

$b'\leftarrow\mathcal{A}^{\mathcal{O}_{\mathrm{KeyDer}}(\cdot),\mathcal{O}_{\mathrm{Dec}}(\cdot,\cdot)}(\mathrm{guess},C^*,\mathrm{state})$

其中当 $id\neq id^*,C\neq C^*$ 时，攻击者 $\mathcal{A}$ 具有访问谕示 $\mathcal{O}_{\mathrm{KeyDer}}(id)=\mathrm{KeyDer}(pk,\alpha,id)$，$\mathcal{O}_{\mathrm{Dec}}(id,C)=\mathrm{Dec}(pk,\mathrm{KeyDer}(pk,\alpha,id),C)$ 的能力。如果对任意多项式时间的攻击者 $\mathcal{A}$，其优势 $\mathrm{Adv}_{\varepsilon,\mathcal{A}}^{\mathrm{IBE}}(k)=|2\Pr[b'=b]-1|$ 均是可忽略的，则称相应的加密体制 ε 是 CCA2 安全的。

3　安全性模型

本节首先简要介绍 Krawczyk[5]改进的包含了 KCI 攻击的 CK 模型。

模型中假设共有 n 个用户参与通信，它们被模型化为概率多项式时间图灵机。每个用户中可能同时运行协议的多项式个副本，称为会话(Session)。协议中还有一个被模型化为概率多项式时间图灵机的攻击者 $\mathcal{A}$。攻击者 $\mathcal{A}$ 控制着网络的所有通信，能够随意修改、丢弃和伪造消息，能够编排消息的发送顺序或者修改消息的接受方。攻击者还能通过发送 establish-session(P_i,P_j,s) 请求或输入消息 (P_i,P_j,s,m) 随意激活会话，其中 P_i 是会话的拥有方，s 是会话标识，P_j 是会话的意定通信方。

会话在被激活后，按照协议规范运行并产生相应的输出消息或者是会话密钥，生成了相应的会话密钥的会话称为完成的。称两个会话 (P_i,P_j,s) 和 (P_i',P_j',s') 是匹配会话，如果 $P_i=P_j',P_j=P_i',s=s'$。为了模型化协议运行过程中一些特殊信息的泄露对会话密钥安全的影响，还允许攻击者 $\mathcal{A}$ 发出下列询问或请求：

(1) corrupt(P_i)，返回给攻击者 $\mathcal{A}$ 用户 P_i 的长期密钥；

(2) session-state(P_i,P_j,s)，返回 P_i 中会话 s 的所有会话状态。需要说明的是，用户长期私钥和会话密钥不在会话状态中。除协议特别说明外，其它中间计算值均在会话状态中；

(3) session-expitation(P_i,P_j,s)，这种请求只能针对已经完成的会话，相应的会话从内存中擦除会话密钥；

(4) session-key(P_i,P_j,s)，这种询问只能针对一个完成的、未过期的会话，返回的是相应的会话密钥；

(5) test-session(P_i,P_j,s)，这种询问攻击者只能发出一次，且只能针对一个完成的、未打开的会话。均匀的随机抛币 $b\in\{0,1\}$，如果 $b=1$ 返回给攻击者相应的会话密钥，否则返回给攻击者一个和密钥同分布的随机值。其中，如果攻击者曾经对一个会话或其匹配会话发出 session-state 或 session-key 询问，或者是在该会话的匹配会话过期之前对其拥有方发出 corrupt 询问，称该会话是打开的。

协议的安全性通过攻击者 $\mathcal{A}$ 和运行协议的用户之间的游戏来定义。攻击者除可以随意控制消息和用户的激活顺序之外，可以任意发出上述询问中的前 4 种，并且根据这些知识选择测试会话。攻击者只允许发出 1 次 test-session 询问，并且在此之后仍旧不能打开测试会话。最后，攻击者计算并做出对 b 的有根据的猜测 $b'\in\{0,1\}$，其优势定义为

$$\mathrm{Adv}_{\pi,\mathcal{A}}^{\mathrm{SK}}(k)=|2\Pr[b'=b]-1| \quad (3)$$

定义 1(SK 安全性)[5][5]　称一个密钥交换协议 π 是带 PFS 的 SK 安全的，如果对任意的多项式时间攻击者 $\mathcal{A}$：

(1)如果两个未被腐化的用户完成了匹配会话，则它们生成的会话密钥相同；

(2) $\mathcal{A}$ 的优势是一个可忽略量。

满足上述定义的协议能够抵抗已知会话密钥攻击，KCI 攻击，并能保证完善前向安全(PFS)。由于一轮的密钥交换协议不可能保证 PFS[9]，所以本文考虑弱前向安全(WFS)，特别地额外要求攻击者不能对测试会话以及其匹配会话采取主动攻击。

4 协议描述

给定安全参数 k，首先选取一个满足 DDH 假设的，阶为素数 p，$|p|=k$ 的乘法循环群 $\mathbb{G}=<g>$。假设 $\varepsilon=(\mathrm{KeyGen},\mathrm{KeyDer},\mathrm{Enc},\mathrm{Dec})$ 是明文空间包含 $\mathbb{G}$ 的基于身份的加密体制，$F=\{\{f_s:\{0,1\}^{4k}\rightarrow\{0,1\}^k\}_{s\in\mathcal{G}_k}\}_{k\in\mathcal{N}}$ 是伪随机函数簇，本文给出的一轮密钥交换协议如图 1 所示。

A		B
$y_A\overset{R}{\leftarrow}\mathbb{Z}_p^*, Y_A=g^{y_A}$		$y_B\overset{R}{\leftarrow}\mathbb{Z}_p^*, Y_B=g^{y_B}$
$C_A=\mathrm{Enc}(pk,id_B,Y_A)$		$C_B=\mathrm{Enc}(pk,id_A,Y_B)$
	$\xrightarrow{A,C_A}$	
	$\xleftarrow{B,C_B}$	
$s=A\|\|B\|\|C_A\|\|C_B$		$s=A\|\|B\|\|C_A\|\|C_B$
$Y_B=\mathrm{Dec}(pk,d_A,C_B)$		$Y_A=\mathrm{Dec}(pk,d_B,C_A)$
$K_A=\mathrm{PRF}_{Y_B^{y_A}}(s)$		$K_B=\mathrm{PRF}_{Y_A^{y_B}}(s)$
擦掉除(K_A,s)外的所有状态信息		擦掉除(K_B,s)外的所有状态信息

图 1 一轮密钥交换协议

用户 A 从 $\mathbb{Z}_p^*$ 中随机地选择元素 y_A，计算 $Y_A=g^{y_A}$，并且用 B 的公钥对消息进行加密后，将得到的密文 C_A 以及 A 的身份发送给 B。用户 B 的操作与 A 类似。用户 B 收到消息 A,C_A 后，首先计算得到会话标识 $s=A\|\|B\|\|C_A\|\|C_B$，利用私钥 B 对 C_A 进行解密得到 Y_A，计算会话密钥为 $K_B=\mathrm{PRF}_{Y_A^{y_B}}(s)$。协议中特别限制解密得到的信息(例如，对 B 中的会话包括 $Y_A,Y_A^{y_B}$)不在会话状态中。做出这样限制的合理性在于，解密后信息可以立即被用作计算。

本文的协议是文献[8]中的协议 2 的改进。不同于原协议中用户传送的消息需要包含一个随机值的密文以及一个 DH 指数，本文的协议只需要传输一个 DH 指数对应的密文，减少了通信代价。另外，本协议没有采用随机性扩展函数，并且需要更少的伪随机函数的调用次数，降低了生成会话密钥时的计算复杂度。具体的性能比较见表 1。消息长度表示每次交互过程中用户所需要传递的消息长度，本文协议需要传递的消息长度为文献[8]中的 $2/3$。计算指数次数列表示每次密钥协商每个用户所要计算指数的次数，本文协议和文献[8]中协议指数计算次数相同。随机性扩展函数列和伪随机性函数列表示每次密钥协商每个用户调用该函数的次数，本文协议没有用到随机性扩展函数，并且相比于文献[8]中的协议 3 次调用伪随机性函数，本文协议只调用 1 次伪随机性函数。

表 1 协议性能比较

	消息长度	计算指数次数	随机性扩展函数	伪随机性函数
Boyd's 协议[8]	$3k$	2	3	3
本文协议	$2k$	2	0	1

5 安全性分析

本文协议安全性分析基于 Krawczyk [5]改进 CK 模型。除了涵盖 CK 模型中考虑到的攻击者能力之外，该模型还允许攻击者在协议开始之前腐化测试会话的拥有方，即考虑攻击者能实施 KCI 攻击的情形下协议的安全性。本节证明了协议满足定义 1 中的安全性定义，即该协议和文献[8]中的协议具有相同的安全性。

定理 1 假设 k 是安全参数，$\mathbb{G}$ 满足 DDH 假设，$\varepsilon=(\mathrm{KeyGen},\mathrm{KeyDer},\mathrm{Enc},\mathrm{Dec})$ 是 CCA2 安全的基于身份的加密体制，$F=\{F_k\overset{R}{\leftarrow}\{f_s:\{0,1\}^{4k}\rightarrow\{0,1\}^k\}_{s\in\mathcal{G}_k}\}_{k\in\mathcal{N}}$ 是伪随机函数，则上述一轮密钥交换协议是带 WFS 的 SK 安全的。

证明 在下述证明中，记攻击者 $\mathcal{A}$ 激活的第 i 个会话为 Π_X^i，其中 X 是会话的拥有方。根据协议运行过程中是否有用户被腐化，可以分以下 3 种情形对协议进行分析：

情形 1 测试会话的意定通信方没有被腐化，但是测试会话的拥有方可能在会话开始之前或者是会话过期之后被腐化；

情形 2 测试会话的拥有方没有被腐化，但是测试会话的意定通信方可能在测试会话的匹配会话过期之后被腐化；

情形 3 两个用户同时被腐化。

情形 1 的分析：在这种情形下，测试会话的意定通信方没有被腐化，但是测试会话的拥有方可能在会话开始之前或者是在会话过期之后被腐化。需要注意的是，此时测试会话的意定通信方中可能并没有相应的会话被激活，而是攻击者冒充该用户与测试会话进行了通信。这部份的证明将用到下述 5 个游戏 $\mathrm{G0},\cdots,\mathrm{G4}$。记 win_i 为事件“攻击者在第 i 个游戏中猜测正确”，Adv_i 为相应的优势，即 $\mathrm{Adv}_i=|2\Pr[\mathrm{win}_i]-1|$。

游戏G0　这个游戏是攻击者和协议的真实交互，即协议的参与方严格按照协议规范运行，攻击者按照模型规定的能力发出询问并得到相应的回答。特别地，当攻击者 $\mathcal{A}$ 向一个完成的、未过期的会话发出 test-session 询问时，随机地选择 $b\in\{0,1\}$，当 $b=0$ 时返回给攻击者 $\mathcal{A}$ 真实的会话密钥，当 $b=1$ 时返回给攻击者 $\mathcal{A}$ 一个随机值。

游戏G1　这个游戏和游戏G0基本相同，下述情况除外：当两个不同的会话输出相同的消息并且拥有相同的意定通信方时候，停止协议运行，攻击者独立地、等概地随机选取 $b'\in\{0,1\}$ 作为猜测结果。

假设 p 为协议运行过程中两个会话选择的 DH 指数经过加密后密文相等的概率，n_{orac} 是攻击者调用的最大会话数，则根据生日攻击原理可知，

$$\text{Adv}_{\mathcal{A}}^{\text{SK}}(k)=\text{Adv}_0\le n_{\text{orac}}^2p+\text{Adv}_1 \tag{4}$$

游戏G2　这个游戏和游戏G1基本相同，下述情况除外：在攻击者开始运行之前，随机地选取 $m\in\{1,2,\cdots,n_{\text{orac}}\}$。如果攻击者没有选择这个会话作为测试会话，协议停止运行，攻击者随机选取 $b'\in\{0,1\}$ 作为猜测结果。如果攻击者恰好选择第 m 个会话作为测试会话，则按照协议规范正常运行。此时，记测试会话接收到的消息为 C，输出的消息为 $C*$，会话的拥有方为 T，会话的意定通信方为 $T*$。

由于攻击者恰好选择第 m 个会话作为测试会话的概率为 $1/n_{\text{orac}}$，从而易知该游戏中攻击者的优势 $\text{Adv}_2=\text{Adv}_1/n_{\text{orac}}$。

游戏G3　这个游戏和游戏G2基本相同，下述情况除外：随机地选择 $x_T\in_R\mathbb{Z}_{p'}^*$，并用 x_T 和 $X_T=g^{x_T}$ 替代测试会话 Π_T^m 在计算密钥 K_T 中用到的 y_T 和 Y_T，记得到的密钥为 $K_T^{'}$。当攻击者发出 test-session 询问时，随机地选择 $b\in\{0,1\}$，当 $b=0$ 时返回给攻击者 $\mathcal{A}$ 密钥 $K_T^{'}$，当 $b=1$ 时返回给攻击者 $\mathcal{A}$ 一个随机值。并且，如果 $T*$ 的某个会话接收到消息 $C*$，用 X_T 替代会话中的 $\text{Dec}(pk,d_{T^*},C^*)$，记得到的密钥为 $K_{T^*}^{'}$。

为了分析游戏G2和游戏G3中攻击者的优势差，按照如下方式构造针对基于身份的加密体制的攻击者 $\mathcal{B}$，使得当 $\mathcal{B}$ 的输入是 m_0 所对应的密文时，$\mathcal{B}$ 所能得到的信息和游戏G2中攻击者所能得到的信息相同，当 $\mathcal{B}$ 的输入是 m_1 所对应的密文时，$\mathcal{B}$ 所能得到的信息和游戏G3中攻击者所能得到的信息相同。

攻击者 $\mathcal{B}$ 建立协议的模拟运行环境，并且调用 $\mathcal{A}$，按照游戏G2运行。协议运行过程中的 $\mathcal{B}$ 可能会访问谕示 $\mathcal{O}_{\text{KeyDer}}(\cdot),\mathcal{O}_{\text{Dec}}(\cdot,\cdot)$。当第 m 个会话被激活后，攻击者 $\mathcal{B}$ 根据交互历史信息选择两个明文 $M_0=g^{m_0},M_1=g^{m_1}$，得到的是密文 $C^*=\text{Enc}(pk,id,M_b)$，其中 id 是第 m 个会话的拥有方，$b\in\{0,1\}$ 是均匀随机抛币。$\mathcal{B}$ 用 $C*$ 替代第 m 个会话的输出。当协议攻击者 $\mathcal{A}$ 停止并输出对测试会话中抛币的猜测，当 $\mathcal{A}$ 的猜测正确时，$\mathcal{B}$ 输出对加密体制中抛币的猜测 $b'=0$，否则输出 $b'=1$。

当 $C^*=\text{Enc}(pk,id,M_0)$ 时，$\mathcal{B}$ 正确的概率是 $\Pr[\text{win}_2]$；当 $C^*=\text{Enc}(pk,id,M_1)$ 时，$\mathcal{B}$ 正确的概率是 $1-\Pr[\text{win}_3]$。根据 $\mathcal{B}$ 的优势的定义，

$$\begin{aligned}\text{Adv}_{\varepsilon,\mathcal{B}}^{\text{IBE}}(k)&=\left|2(\Pr[\text{win}_2]+1-\Pr[\text{win}_3])-1\right|\\&=\left|\Pr[\text{win}_2]-\Pr[\text{win}_3]\right|\end{aligned}$$

从而

$$\text{Adv}_2\le 2\text{Adv}_{\varepsilon,\mathcal{B}}^{\text{IBE}}(k)+\text{Adv}_3 \tag{5}$$

游戏G4　这个游戏和游戏G3基本相同，下述情况除外：对任意 s'，当要计算 $\text{PRF}_{X_T^{'},y_T*}(s')$ 时，用一个从 $\mathbb{U}_2$ 中随机选取的值代替(相同的 s' 选择相同的值，不同的 s' 独立选择不同的值)。

构造针对伪随机函数簇的 $F=\{F_k\}_{k\in\mathcal{N}}$ 的区分攻击者 $\mathcal{D}$，使得当 $\mathcal{D}$ 能够访问的谕示是伪随机函数时，协议攻击者 $\mathcal{A}$ 的输出和游戏G3中攻击者 $\mathcal{A}$ 的输出同分布，当 $\mathcal{D}$ 能够访问的谕示是真随机函数时，协议攻击者 $\mathcal{A}$ 和游戏G4中攻击者 $\mathcal{A}$ 的输出同分布。

攻击者 $\mathcal{D}$ 得到输入 $F=\{F_k\}_{k\in\mathcal{N}}$ 后，按照游戏G3运行，并且当需要计算 $\text{Expd}_{X_T^{'}}(s')$ 时，用 $\mathcal{O}(s')$ 替代上述值。当 $\mathcal{A}$ 停止并输出对抛币 b 的猜测 b' 时，$\mathcal{D}$ 检验是否有 $b=b'$。若答案是肯定的，$\mathcal{D}$ 输出“$\mathcal{O}(\cdot)$ 属于上述伪随机函数簇”，否则输出“$\mathcal{O}(\cdot)$ 属于真随机函数簇”。从而 $\mathcal{D}$ 猜测正确的概率是 $\Pr[\mathcal{D}\text{ correct}]=(1/2)(\Pr[\text{win}_3]+1-\Pr[\text{win}_4])$。根据随机性扩展函数安全性的定义，有

$$\begin{aligned}\text{Adv}_{\mathcal{F},D}^{\text{PRF}}(k)&=|\,2\Pr[\mathcal{D}\text{ correct}]-1\,|\\&=|\,\Pr[\text{win}_3]-\Pr[\text{win}_4]\,|\end{aligned}$$

进一步

$$\text{Adv}_3\le 2\text{Adv}_{\mathcal{F},D}^{\text{PRF}}(k)+\text{Adv}_4 \tag{6}$$

由于在游戏G4中，无论测试会话中的抛币如何，攻击者始终得到的是均匀随机选取的随机变量，从而攻击者的优势 $\text{Adv}_4=0$。　结合式(4)-式(6)可得

$$\text{Adv}_{\mathcal{A}}^{\text{SK}}(k)\le n_{\text{orac}}^2p+2n_{\text{orac}}\cdot(\text{Adv}_{\varepsilon,\mathcal{B}}^{\text{IBE}}(k)+\text{Adv}_{\mathcal{F},D}^{\text{PRF}}(k)) \tag{7}$$

情形 2 的分析：在这种情形下，测试会话的拥有方没有被腐化，但是测试会话的意定通信方可能在会话过期之后被腐化。这部份的证明同样将用到

5 个游戏，除游戏G3外其它的游戏定义与情形 1 中的定义相同。

游戏G3这个游戏和游戏G2基本相同，下述情况除外：随机地选择 $x_{T^*} \in_R \mathbb{Z}_p^*$，并用 x_{T^*} 和 $X_{T^*} = g^{x_{T^*}}$ 替代测试会话的匹配会话在计算密钥 K_{T^*} 中用到的 y_{T^*} 和 Y_{T^*}。并且，如果 T 的某个会话接收到消息 C，用 X_{T^*} 替代会话中的 $\mathrm{Dec}(pk, d_T, C)$。记测试会话按照修改后的方法得到的密钥为 $K_T^{'}$。当攻击者发出 test-session 询问时，随机地选择 $b \in \{0,1\}$，当 $b=0$ 时返回给攻击者 $\mathcal{A}$ 密钥 $K_T^{'}$，当 $b=1$ 时返回给攻击者 $\mathcal{A}$ 一个随机值。

类似于情形 1 中对攻击者优势的分析，可以得到

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SK}}(k) \le n_{\mathrm{orac}}^2 p + 2n_{\mathrm{orac}} \cdot (\mathrm{Adv}_{\varepsilon,\mathcal{B}}^{\mathrm{IBE}}(k) + \mathrm{Adv}_{\mathcal{F},D}^{\mathrm{PRF}}(k)) \tag{8}$$

情形 3 的分析：在这种情形下，测试会话的拥有方可能在会话开始之前或者是在会话过期之后被腐化，测试会话的意定通信方可能在会话过期之后被腐化。为估计这种情形下攻击者的优势，定义下述 5 个游戏，除游戏G2,G3外其它的游戏定义与情形 1 中的定义相似。

游戏G2这个游戏和游戏G1基本相同，下述情况除外：在攻击者开始运行之前，随机地选取 $m_1, m_2 \in \{1,2,\cdots,n_{\mathrm{orac}}\}$。如果攻击者恰好选择第 m_1 个会话作为测试会话，并选择第 m_2 个会话作为其匹配会话，则按照协议规范正常运行。此时，记测试会话接收到的消息为 C，输出的消息为 C^*，会话的拥有方为 T，会话的意定通信方为 T^*。否则，协议终止，攻击者随机选取 $b' \in \{0,1\}$ 作为猜测结果。

由于攻击者恰好选择第 m_1 个会话作为测试会话的概率为 $1/n_{\mathrm{orac}}$，选择第 m_2 个会话作为测试会话的概率为 $1/n_{\mathrm{orac}}$，从而易知该游戏中攻击者的优势 $\mathrm{Adv}_2 = \mathrm{Adv}_1 / n_{\mathrm{orac}}^2$。

游戏G3这个游戏和游戏G2基本相同，下述情况除外：给定 (g^x, g^y, h)，分别用 g^x, g^y, h 替代会话 $\Pi_T^{m_1}$ 和 $\Pi_{T^*}^{m_2}$ 中的 Y_T, Y_{T^*} 以及 DH 值，其它的按照协议规范运行。

为了分析游戏G2和游戏G3中攻击者的优势差，按照如下方式构造DDH区分攻击者 $\mathcal{D}'$。攻击者 $\mathcal{D}'$ 得到输入 (g^a, g^b, h) 后，按照游戏G2运行。当协议攻击者停止并输出对抛币的猜测时，$\mathcal{D}'$ 检验是否 $b = b'$。若答案是肯定的，$\mathcal{D}'$ 输出“$(g^a, g^b, h) \in \mathbb{R}_k$”，否则输出“$(g^a, g^b, h) \in \mathbb{D}_k$”。从而 $\mathcal{D}'$ 猜测正确的概率是

$$\Pr[\mathcal{D}' \text{ correct}] = \frac{1}{2}(\Pr[\mathrm{win}_3] + 1 - \Pr[\mathrm{win}_4]) \tag{9}$$

根据 DDH 问题安全性的定义，可知 $\mathrm{Adv}_2 \le 2\mathrm{Adv}_{G,\mathcal{D}}^{\mathrm{DDH}}(k) + \mathrm{Adv}_3$。因此，

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SK}}(k) \le n_{\mathrm{orac}}^2 p + 2n_{\mathrm{orac}}^2 \left(\mathrm{Adv}_{G,\mathcal{D}}^{\mathrm{DDH}}(k) + \mathrm{Adv}_{\mathcal{F},D}^{\mathrm{PRF}}(k)\right) \tag{10}$$

6 结束语

本文提出了一个基于 DDH 假设、伪随机函数簇和标准模型的可证明安全的一轮密钥交换协议，协议具有弱前向安全性(WFS)，并且能够抵抗 KCI 攻击。虽然本文的协议使用的是基于 ID 的加密体制，对于基于 PKI 的加密体制同样适用。相比于 Boyd 等的协议，本文的协议在提供相同的安全性的前提下，具有较低的通信复杂度和计算复杂度。

参 考 文 献

[1] Canetti R and Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels[C]. EUROCRYPT 2001, LNCS 2045: 453–474.

[2] Smart N. Update to provable security: design and open questions. Technical Report D.AZTEC.5, 2007. Available at: http://www.ecrypt.org/documents. 2008, 9.

[3] Bellare M and Rogaway P. Entity authentication and key distribution[C]. CRYPTO 1993, LNCS 773: 232–249.

[4] Bellare M, Canetti R, and Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols[C]. In Proc. 30th ACM Symp. on Theory of Computing, Las Vegas, May 1998: 419–428.

[5] Krawczyk H. HMQV: A high-performance secure Diffie-Hellman protocol[C]. CRYPTO 2005, LNCS 3621: 546–566.

[6] Canetti R, Goldreich O, and Halevi S. The random oracles methodology, revisited[C]. In Proc. 30th ACM Symp. on Theory of Computing, Las Vegas, May 1998: 209–218.

[7] Dent A W. Adapting the weaknesses of the random oracle model to the generic group model[C]. ASIACRYPT 2002, LNCS 2781: 100–109.

[8] Boyd C, Cliff Y, Nieto J G, and Paterson K G. Efficient one-round key exchange in the standard model[C]. ACISP 2008, LNCS 5107: 69–83.

[9] Bellare M, Pointcheval D, and Rogaway P. Authenticated key exchange secure against dictionary attack[C]. EUROCRYPT 2000, LNCS 1807: 139–155.

胡学先： 男，1982 年生，博士生，研究方向为概率统计及其在密码中的应用.

刘文芬： 女，1965 年生，教授，博士生导师，研究方向为概率统计及其在密码和通信中的应用.

兰巨龙： 男，1962 年生，教授，博士生导师，主要研究方向为网络路由理论与技术.