通用可组合的组密钥交换协议

贾洪勇[①③] 卿斯汉[②] 谷利泽[①] 杨义先[①]
[①](北京邮电大学网络与交换技术国家重点实验室信息安全中心 北京 100876)
[②](中国科学院软件研究所 北京 100190)
[③](解放军信息工程大学电子技术学院 郑州 450004)

摘 要：该文提出了一个通用可组合框架下的组密钥交换理想函数，并在防篡改硬件令牌的基础上，利用部分隔离状态下证据不可区分知识证明，设计了一个组密钥交换协议，安全地实现了这个理想函数。和采用 CRS 模型的协议相比，降低了把整个信任集中于一处带来的风险。提出的组密钥交换协议经过证明具有 AKE 安全，并且能够抵抗适应性敌手攻击和恶意参与者攻击。

关键词：保密通信；通用可组合；证据不可区分；知识证明；公共参考串模型
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2009)07-1571-05

Universally Composable Group Key Exchange Protocol

Jia Hong-yong[①③] Qing Si-han[②] Gu Li-ze[①] Yang Yi-xian[①]
[①](*Information Security Center*, *State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
[②](*Institute of Software*, *Chinese Academy of Science*, *Beijing* 100190, *China*)
[③](*Institute of Electronic Technology of PLA Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: In this article, a universally composable group key exchange ideal function is proposed and realized using witness indistinguishable proof of knowledge with partially isolated party based on the tamper-proof hardware token. Compared with protocols under the CRS model, the group key exchange protocol can greatly reduce the risk of putting all trusts in one place. The protocol is proved to be AKE secure and resistant to the attacks of adaptive adversaries and malicious insiders.

Key words: Secure communication; Universally composable; Witness indistinguishable; Proof of knowledge; Common Reference String (CRS) model

1 引言

绝大部分的组密钥交换协议是在孤立模型中进行分析的[1,2]。但是实际协议运行环境的最大特点是并发性。比如，组密钥交换协议协商出来的会话密钥会提供给上层组通信协议使用，多个组密钥交换协议可能会并发运行。在孤立模型中被证明安全的协议，在并发环境中不一定安全。为了解决协议的并发组合安全性问题，Canetti 在 2001 年提出了一个计算复杂性理论模型：通用可组合安全(Universally Composable Security)，简称 UC 安全[3]。在这种模型中设计证明的安全协议，可以和其它任何协议并发组合运行，也可以作为一个子协议嵌入到复杂协议中，仍然能够保持相应的安全性。

2008-01-11 收到，2009-01-20 改回
国家 973 计划项目(2007CB310704)，国家自然科学基金(60673098)和国家自然科学基金委员会与香港研究资助局联合科研基金(60731160626)资助课题

UC安全对安全性要求非常高，文献[4,5]证明了几乎所有的具有实际意义的安全多方计算函数，要想获得UC安全性，必须具备一定的前提假设，比如CRS(Common Reference String，公共参考串)模型，密钥注册(Key Registration，KR)模型等，需要多方计算最终把信任集中到某个假设条件上，这样做往往具有很大的安全隐患。Katz在文献[6]中提出一种新的前提假设，也就是利用防篡改硬件来解决信任问题。Damgard等人基于Katz的工作在文献[7]中又提出了部分隔离的参与方安全计算模型。这种模型中，防篡改硬件被提升为一个通信受限的、处于一定隔离状态的参与方。本文采用这种方案作为UC安全组密钥交换的前提假设条件，把它同基于树的Diffie-Hellman假设结合在一起，同时利用已经证明过具有UC安全性的签名方案[8]构造了一个在混合模型下具有UC安全的组密钥交换协议，对协议的安全性进行了完整的证明，该协议具有标准的AKE安全性，在静态组成员条件，能够抗击适应性敌手和恶

意参与者攻击。

2 相关工作

很少有文献使用UC框架对组密钥交换协议进行分析，在文献[9]中，Katz首次在组密钥交换协议的设计和分析中应用了UC框架，但是并没有完整地把UC框架应用到组密钥交换协议中，只是对恶意内部攻击者进行了建模和分析，提出了一个协议编译器，可以把孤立模型中具有AKE(Authenticated Key Exchange)安全的组密钥交换协议转换成UC安全的协议，没有充分发挥出UC框架强大的安全协议分析功能。本文完全使用UC框架对组密钥交换进行了分析证明。

3 理论基础

基于树的判定Diffie-Hellman假设(Tree Decisional Diffie-Hellman，TDDH)，由Kim等在文献[10]中提出。τ_n代表所有具有n个叶子结点的二叉树的集合。对于任意$T_n \in \tau_n$，每个结点用标签$<l,v>$表示(其中l代表结点所在的层数，v表示结点在这一层的位置)，这个结点的两个子结点用$<l+1,2v>,<l+1,2v+1>$表示，$<0,0>$代表根结点。T_n^*代表去除了根结点的所有结点的集合。

叶子结点集合：$\mathrm{LN}_{\tau_n} := \{<l,v>|<l,v>\in T_n, <l+1,2v>\notin T_n, <l+1,2v+1>\notin T_n\}$；

内部结点集合：$\mathrm{IN}_{\tau_n} := \{<l,v>|<l,v>\in T_n, <l+1,2v>\in T_n^*, <l+1,2v+1>\in T_n^*\}$。

X代表随机选取的变量$x_{(l,v)}$的集合，$(l,v)\in \mathrm{LN}_{T_n}$,对于所有$(l,v)\in \mathrm{IN}_{T_n}$可以递归地定义$x_{(l,v)}$，$x_{(l,v)}=g^{x_{(l+1,2v)}x_{(l+1,2v+1)}}$，$\mathrm{TDH}_{T_n}(X)=\{(l,v),g^{x_{(l,v)}}\}_{(l,v)\in T_n^*}$。另外，对于随机数$r$，定义元组：$\mathrm{TDDH}^*_{T_n}(X)$和$\mathrm{TDDH}^{\$}_{T_n}(X)$。

$$\mathrm{TDDH}^*_{T_n}(X)=\mathrm{TDH}_{T_n}(X)\bigcup(<0,0>,g^{x_{(1,0)}x_{(1,1)}})$$

$$\mathrm{TDDH}^{\$}_{T_n}(X,r)=\mathrm{TDH}_{T_n}(X)\bigcup(<0,0>,g^{r})$$

定义1 TDDH假设：对于所有$n>1$，任意的$T_n\in\tau_n$，任意PPT (Probabilistic Polynomial Time，概率多项式时间)算法A，以下的区分优势是可以忽略的：

$$\mathrm{Adv}^{\mathrm{TDDH}}_{T_n,G}(A):=\left|\Pr_X[A(\mathrm{TDDH}^*_{T_n}(X))=1]-\Pr_{X,r}[A(\mathrm{TDDH}^{\$}_{T_n}(X,r))=1]\right|$$

定理1 TDDH问题和DDH问题是多项式渐近相等的。

$$\mathrm{Adv}^{\mathrm{DDH}}_{G}(K)\le\mathrm{Adv}^{\mathrm{TDDH}}_{T_n,G}(K)\le(2n-3)\mathrm{Adv}^{\mathrm{DDH}}_{G}(K)$$

定理1证明参考文献[11]。

定理2 在知识证明协议(Proofs of Knowledge, PK)中，如果知识证明方与外界环境之间的信息交流不超过L比特，那么可以构造出满足下列性质的知识证明协议：证明具有完整性、证明具有知识可靠性、证据不可区分性WI(Witness Indistinguishable)。定理2证明参考文献[12]。

4 组密钥交换理想函数

组密钥交换理想函数$\mathcal{F}_{\mathrm{gke}}$：以$k$为安全参数，$(P_1,P_2,\cdots,P_n)$为$n$个协议参与方，用$P$代表整个参与方集合。

(1)协议初始化阶段：当从参与方P_i收到$(\mathrm{NewSession},\mathrm{sid},P,P_i)$消息后，如果是第1次，把这个消息记录下来，同时把它转发给模拟器S，如果此时理想函数已经收到了$|P|-1$条这样的消息，就存储消息$(\mathrm{Ready},\mathrm{sid},P)$，并把这条消息转发给模拟器$S$。

(2)组密钥生成阶段：当理想函数从模拟器S收到消息$(\mathrm{OK},\mathrm{sid},P)$，此时检查是否存在消息$(\mathrm{Ready},\mathrm{sid},P)$，如果有，则进行如下操作：

(a)如果所有协议的参与方都没有被敌手攻陷，那么就由理想函数$\mathcal{F}_{\mathrm{gke}}$生成组会话密钥：$K\leftarrow\{0,1\}^k$，保存消息$(\mathrm{SessionKey},\mathrm{sid},P,K)$。

(b)如果有某一个协议参与方被敌手攻陷，那么理想函数就等待模拟器S发送消息$(\mathrm{Key},\mathrm{sid},K)$，收到后保存为$(\mathrm{SessionKey},\mathrm{sid},P,K)$。

(3)密钥的发送：当收到模拟器S发送的消息$(\mathrm{Delivery},\mathrm{sid},P_i)$时，理想函数检查是否存在消息$(\mathrm{SessionKey},\mathrm{sid},P,K)$和$P_i$是否属于$P$，如果都符合，向$P_i$发送消息$(\mathrm{SessionKey},\mathrm{sid},P,K)$，如果有一个不符合，则忽略掉这条消息。

在孤立模型中对协议安全性进行证明时，通常是把敌手的攻击能力建模成各种预言机(oracle)，然后利用游戏证明，在这些攻击下，协议能够保持相应的安全性如AKE安全性，详细见文献[9]。协议不可能抵抗没有列出的敌手攻击。在UC安全框架中，不是一一列出，而是通过理想函数准确地表达安全协议要达到的目标。UC安全性是比孤立模型中的AKE安全性更加严格和全面的安全模型，满足UC安全性的组密钥交换协议必然满足孤立的AKE安全性，反之则不一定，证明见文献[9]。

5 实现理想函数的安全协议

本文在混合模型$(\mathcal{F}_{\mathrm{agent}},\mathcal{F}_{\mathrm{sig}})$基础上提出了安全地实现了组密钥交换理想函数的协议：LTDH。

5.1 混合模型

$\mathcal{F}_{\mathrm{agent}}$理想函数：它是对部分隔离硬件令牌功能的抽象，由隔离参数L决定。在本文的协议中，P_i通

过这个理想函数向CA提供知识证明，证明 P_i 公私钥对的合法性(根据需要构建的多个CA被看作是协议的特殊参与方)。$\mathcal{F}_{\text{agent}}$ 的接口定义如下：

(1)当从 P_i 收到消息 $(\text{Create},\text{sid},P_i,P_j,M)$ 后，初始化硬件令牌M的各种内部状态。

(2)当从 P_i 收到消息 $(\text{Run},\text{sid},P_i,P_j,\text{msg})$ 后，查询对应令牌的信息，如果 msg 是发送给 P_j 的，则直接发送，如果有其它消息是发送给 P_i 的，则检查 M 与 P_i 的总通信量是否超过上限值 L，超过则不发送。

$\mathcal{F}_{\text{sig}}$ 理想函数：由Canetti在文献[13]中提出的具有UC安全特性的签名方案，可以直接用在本文的协议中，这充分体现了UC模型在安全协议模块化设计方面的强大优势。

5.2 组密钥交换协议形式化描述

5.2.1 协议相关计算函数　根据协议的参与方构造协议对应的线性二叉树，每个叶子结点对应一个协议参与方，每个结点具有两个值：结点值 $x_{(l,v)}$，结点幂值 $y_{(l,v)}$。在下面协议中 $\text{sid}_i,\text{pid}_i$ 分别代表协议会话标识，参与方身份物理标识。

(1)结点值：选择安全参数k，调用函数Gen()生成结点值：$x_{(l,v)} \leftarrow \text{GenValue}(1^k)$。

(2)结点幂值：$y_{(l,v)} = \text{NodeExp}(x_{(l,v)}) = g^{x_{(l,v)}}$。

(3)根据结点值的集合，求对应的各个结点幂值集合的函数：NodeSetExp()。

输入　l，$X \coloneqq \{x_{(l,0)},x_{(l-1,0)},\cdots,x_{(1,0)}\}$，$l$ 代表集合中深度值最大的结点。

输出　$Y \coloneqq \{y_{(l,0)},y_{(l-1,0)},\cdots,y_{(1,0)}\}$，求出的结点集合的幂值。

(4)求线性二叉树中叶子结点到根结点路径上所有结点值的函数：LeafToRootVal()。

输入　$l,v,x_{(l,v)},y_{(l,1-v)},Y$，其中 $Y=\{y_{(j,1)}\,|\,(y=j-1,j-2,\cdots,1)\}$。

输出　$X\coloneqq\{x_{(l,v)},x_{(l-1,0)}\}\cup\{x_{(j,0)}\coloneqq(y_{(j+1,1)}^{\,x_{(j+1,0)}}\,|\,y_{(j+1,1)}\in Y,\forall j=l-2,\cdots,0\}$。

5.2.2 协议描述　密钥注册阶段：由外部环境 Z 决定参与方何时向 CA 进行公钥注册，当参与方 P_i 收到外部环境发送的消息 $(\text{Register},P_i,\text{CA}_j)$ 后，它调用密钥生成算法生成自己的公私钥对：$(\text{PK}_i,\text{SK}_i)\leftarrow\text{GenKeyPair}(1^k)$，利用私钥 SK_i 来构造一个防篡改硬件 PPT ITM M (概率多项式时间的交互式图灵机)，实现向 CA 证明自己公私钥对合法性的功能。然后向理想函数 $\mathcal{F}_{\text{agent}}$ 发送消息：$(\text{Create},\text{sid},P_i,\text{CA}_j,M)$，再向 CA_j（P_j 信任 CA_j）发送消息 $(\text{Register},P_i,\text{CA}_j,\text{PK}_i)$。在本文的协议中，CA 被看作是一个特殊的参与方，CA 有多个，每个参与方可以选择自己信任的 CA，多个参与方可以信任相同的 CA，CA 之间不需要存在相互的信任关系，在对协议进行的安全性证明中也不依赖于 CA 之间的信任。P_i 希望和 P_j 通信时，必须要向 P_j 信任的 CA_j 进行公钥注册，同时进行私钥证明。如果 CA_j 接受了注册，则向信任它的各个参与方广播这个消息，否则不采取行动。P_j 只有收到这样的消息后，才和 P_i 进行下一步协议交互，否则忽略掉所有来自 P_i 的消息。

协议第1轮运行：根据协议参与方的个数，构造线性二叉树 T_n，这种树除了最低层有两个叶子结点外，每层都只有1个叶子结点，这些叶子结点，从最左边排序，依次对应协议参与方：$P_1,P_2,\cdots,P_n$。有3个参与方的协议树结构如图1所示：

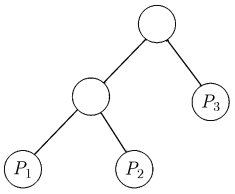

图1 具有3个参与方的线性二叉树

在本协议中，会话ID为 sid，根据UC框架规定，由组密钥交换协议的上层协议提供。每个参与方 P_i 调用伪随机函数 $\text{GenValue}(1^k)$，生成一个秘密的结点值 $x_{(l_i,v_i)}$，计算结点幂值 $y_{(l_i,v_i)}=g^{x_{(l_i,v_i)}}$，向理想函数 $\mathcal{F}_{\text{sig}}$ 发送消息 $(\text{Sign},\text{sid},0\,|\,y_{(l_i,v_i)}\,|\,\text{pid}_i)$，从 $\mathcal{F}_{\text{sig}}$ 获得返回的签名值，$\sigma_i=\text{Sign}_{SK_i}(0\,|\,y_{(l_i,v_i)}\,|\,\text{pid}_i)$，向各个参与方广播：$U_i\,|\,0\,|\,y_{(l_i,v_i)}\,|\,\sigma_i$，$U_i$ 代表发送消息者的简单编号，P_i 对应编号为 i。

第2轮：　位于协议树 l_i 级结点的 P_i，收到第1轮中广播的消息后进行如下操作：对于每个 $j\neq i$，向理想函数 $\mathcal{F}_{\text{sig}}$ 发送验证签名的消息 $(\text{Verify},\text{sid},P_j,\sigma_j)$。如果验证通过，则进行如下操作。$P_1$ 单独作如下运算：计算 $X_1=\{x_{(l-2,0)},x_{(l-3,0)},\cdots,x_{(1,0)}\}$，$l=d(T_n)$。其中 $x_{(l,0)}=y_{(l+1,1)}^{\,x_{(l+1,0)}}$，然后计算 $Y_1^{'}$，$Y_1^{'}=\text{NodeSetExp}(n-1,X_1)$，向理想函数 $\mathcal{F}_{\text{sig}}$ 发送消息 $(\text{Sign},\text{sid},1\,|\,Y_1^{'}\,|\,\text{pid}_1)$，从理想函数中获得签名值 $\sigma_1^{'}=\text{Sig}_{\text{Sk}_1}(1\,|\,Y_1^{'}\,|\,\text{pid}_1)$。广播消息 $U_1\,|\,1\,|\,Y_1^{'}\,|\,\text{pid}_1\,|\,\sigma_1^{'}$。

第3轮：　P_i 首先根据在第1轮中收到的 $y_{(l_j,v_j)}$，构造集合 $X_i=\{x_{(l_i,0)},x_{(l_{i-1},0)}\cdots,x_{(0,0)}\}$，$i\geq 2$ 这个集合代表了从叶子结点到根结点路径上的内部结点的值，最终的目的是求得根结点的值 sk_i，每个参与方就可以把这个共同的值作为生成组会话密钥的种子。X_i 中每个元素的计算方法是，对于 $0\leq l<d(T_n)-1$，$X\coloneqq\{x_{(l,v)},x_{(l-1,0)}\}\cup\{x_{(j,0)}\coloneqq(y_{(j+1,1)}^{\,x_{(j+1,0)}}\,|\,y_{(j+1,1)}\in Y,\forall j=l-2,\cdots,0\}$。

第4轮： P_i 计算 $\mathrm{ack}_i = F_{\mathrm{sk}_i}(0)$， $\mathrm{sk}_i' = F_{\mathrm{sk}_i}(1)$，然后 P_i 擦除除了 ack_i， sk_i'， sid， pid_i 之外的所有内部临时数据。向理想函数 $\mathcal{F}_{\mathrm{sig}}$ 发送消息 (Sign,sid, $\mathrm{pid}_i, \mathrm{ack}_i$)，获得签名 $\bar{\sigma}_i$，广播消息 $U_i \,|\, 2 \,|\, \mathrm{pid}_i \,|\, \bar{\sigma}_i$。当收到本轮中从其它参与方发送的消息后，向理想函数 $\mathcal{F}_{\mathrm{sig}}$ 发送消息 (Verify,sid, $P_j, \bar{\sigma}_j$)，如果所有的验证都通过，则擦除所有内部状态，输出 (sid,$\mathrm{pid}_i, \mathrm{sk}_i'$)，$\mathrm{sk}_i'$ 为最终的会话密钥，如有验证未通过，则停止运行。

6 LTDH 协议安全性证明

定理3 如果通信受限的硬件令牌能够以证据不可区分方式证明私钥合法性，TDDH 假设多项式等价于 DDH，函数 GenValue(1^k)，GenKeyPair(1^k) 是安全的伪随机函数，函数 F 是抵抗碰撞的伪随机函数，那么协议 LTDH 能够在 $(\mathcal{F}_{\mathrm{agent}}, \mathcal{F}_{\mathrm{sig}})$ 混合模型下，安全地实现了组密钥交换理想函数 $\mathcal{F}_{\mathrm{gke}}$。

6.1 模拟器构造及运行

6.1.1 模拟器构造 模拟器 S 的构造：S 调用外部环境 Z，真实协议中的敌手 A 以及所有协议参与方的拷贝，在内部运行。如果在真实协议中 A 攻陷了参与方 P_i，那么 S 就攻陷理想协议中对应的虚构参与方 $\tilde{P}_i$，当一个被攻陷的虚构参与方 $\tilde{P}_i$ 从环境 Z 收到一个消息 m，那么 S 通知外部环境的拷贝 Z' 把 m 发送给 P_i，如果一个被攻陷的 P_i 向 Z' 发送了一个消息 m，S 通知被攻陷的 $\tilde{P}_i$ 向环境 Z 输出消息 m，详细说明请参考文献[3]。

6.1.2 模拟器的运行 (1)模拟参与方制作防篡改硬件，并向 CA 进行密钥注册的过程：

有4种情景需要模拟，其中如果 P_i,CA_j 全部被攻陷了，或者全部都是诚实的，那么模拟就很简单了，下面只考虑剩下的两种情况：

诚实的 P_i，攻陷的 CA_j：在理想协议中，模拟器S看到了消息 (Register,P_i,CA_j,PK_i) 以 P_i 的名义，发送给了理想函数 $\mathcal{F}_{\mathrm{gke}}$，模拟器$S$简单地按照真实协议中 P_i 的行为进行模拟，为每个参与方生成一个公私钥对 (PK_i,SK_i)，并把这个记录下来。由于 CA_j 已经被攻陷，那么真实协议中的敌手A将能够以 CA_j 的名义，自由地通过理想函数 $\mathcal{F}_{\mathrm{agent}}$ 和具有防篡改功能的硬件证明者M进行交互，但是这并没有给 CA_j 更多的能力，因为它只能以协议交互的方式访问M，此处的模拟和真实协议的执行是一样的。

攻陷的 P_i，诚实的 CA_j：当A试图以 P_i 的名义进行密钥注册时，它发送消息 (Register,P_i,CA_j, PK_i) 到 CA_j，向 $\mathcal{F}_{\mathrm{agent}}$ 发送消息：(Create,sid,P_i, CA_j,M)，模拟器收到这些消息后，获得了证明者M和公钥 PK_i，它和M一起运行验证协议。如果协议的结果是拒绝，则模拟器忽略这些注册请求，如果协议同意，则利用 L - IPoK 提取器从中提取公钥合法性的证据，如果证据提取成功，则模拟器向理想函数 $\mathcal{F}_{\mathrm{gke}}$ 发送消息 (Register,P_i,CA_j)，如果证据提取失败，则模拟失败。

(2)模拟组密钥交换协议的运行： 在理想协议中，当模拟器S收到一个消息 (NewSession,sid,P),简单地把这个消息转发给敌手A。当模拟器S收到理想函数 $\mathcal{F}_{\mathrm{gke}}$ 发送的消息 (Ready,sid,P) 后，向理想函数 $\mathcal{F}_{\mathrm{gke}}$ 发送消息 (OK, sid,P)，然后按照以下方法进行模拟：对于被攻破的参与方，借助于假设前提防篡改硬件，获得公私钥信息，提取出该参与方的输入，用这个输入进行模拟，对于没有被攻破的协议参与方，则以随机生成的值作为输入进行模拟。

6.2 不可区分性证明

采用做3次混合试验的方法来对理想协议(模拟器模拟出来的协议)与真实协议的不可区分性进行证明。构造3个过渡协议 $H1, H2, H3$，并证明：$\mathrm{LTDH} \approx H1 \approx H2 \approx H3 \approx \mathcal{F}_{\mathrm{gke}}$，LTDH 代表真实协议，证明的过程实际上就是以不可区分的方式逐渐地改变真实协议中的各种密码学原语，使得最后构造的协议与模拟协议明显地不可区分。3种混合试验的定义如下：

$H1$：它和外部环境 Z 同敌手 A 和真实协议 LTDH 在 $(\mathcal{F}_{\mathrm{agent}}, \mathcal{F}_{\mathrm{sig}})$ 混合模型下进行交互后的输出类似，唯一的差别在于：在 LTDH 协议中，上级结点的值是按照公式 $x_{(l,v)} = g^{x_{(l+1,2v)}x_{(l+1,2v+1)}}$ 计算的，而在$H1$协议中，各个结点的x值则是取一个随机值 r，然后计算 g^r 作为该结点的 x 值，由于三元组 $(g^{x_1}, g^{x_2}, g^{x_1x_2})$ 与 (g^{x_1}, g^{x_2}, g^r) 对于 PPT 敌手 A，在计算上是不可区分的，所以协议 $\mathrm{LTDH} \approx H1$ 。

$H2$：它与 $H1$ 类似，唯一的差别在于，在$H1$协议中调用伪随机函数 GenKeyPair(1^k) 生成公私钥对时，$H2$ 中调用真正的随机函数生成一对公私钥，由于安全的伪随机函数与真正的随机函数，对于 PPT 敌手 A 来说是计算上不可区分的。所以协议 $H2 \approx H1$。

$H3$：它实际上就是理想函数 $\mathcal{F}_{\mathrm{gke}}$，它与 $H2$ 类似，唯一的差别在于，在 $H2$ 协议中调用伪随机函数 GenValue(1^k) 生成每个结点的秘密值时，$H3$ 中调用真正的随机函数生成一个随机数，由于安全的伪随机函数与真正的随机函数，对于 PPT 敌手 A 来说是计算上不可区分的。所以协议 $H3 \approx H2$。最后可得 $\mathrm{LTDH} \approx \mathcal{F}_{\mathrm{gke}}$，定理3得证。

7 总结

本文利用UC安全框架对组密钥交换协议进行

了分析，提出了组密钥交换理想函数，在通信受限的防篡改硬件模型基础上，利用部分隔离的知识证明技术，设计了一个实现了这个理想函数的安全协议，并对协议的安全性进行了证明。以后的工作可以在基本的组密钥交换函数的基础上增加其它额外功能，如可否认性、匿名性等。另外一个方向就是继续改进通信受限硬件假设，使之更加实用化。

参 考 文 献

[1] Manulis M. Survey on security requirements and models for group key exchange. Technical Report 2006/02, Horst-Gortz Institute, Network and Data Security Group, November 2006.

[2] Manulis M. Security-focused survey on group key exchange protocols. HGI Network and Data Security Group Technical Report 2006/03.

[3] Canetti R. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report, 2000/067 (2005). Available at http://eprint.iacr.org/2000/067.

[4] Canetti R and Fischlin M. Universally composable commitments. Advances in Cryptology-Crypto 2001, Lecture Notes in Computer Science, 2001, Vol. 2139: 19–40.

[5] Canetti R, Kushilevitz E, and Lindell Y. On the limitations of universally composable two-party computation without set-up assumptions. *J. Cryptology*, 2006, 19(2): 135–167.

[6] Katz J. Universally composable multi-party computation using tamper-proof hardware. Proceedings of EuroCrypt 2007, LNCS 4515: 115–128.

[7] Damgard I, Nielsen J B, and Wichs D. Universally composable multiparty computation with partially isolated parties. eprint.iacr.org/2007/.

[8] Canetti R. Universally composable signature, certification, and authentication. 17th IEEE Computer Security Foundations Workshop (CSFW), Pacific Grove, CA, USA, 2004: 219–245.

[9] Katz J and Shin J. Modeling insider attacks on group key exchange protocols. http://eprint.iacr.org/2005/.

[10] Kim Y, Perrig A, and Tsudik G. Tree-based group key agreement. *ACM Transactions on Information and System Security*, 2004, 7(1): 60–96.

[11] Manulis M. Group key exchange secure against strong corruptions. http://eprint.iacr.org/2007/.

[12] Damgard I, Nielsen J B, and Wichs D. Isolated proofs of knowledge and isolated zero knowledge. http://eprint.iacr.org / 2007/.

[13] Canetti R. On universally composable notions of security for signature, certification and authentication. Cryptology ePrint Archive, November 2003.

贾洪勇： 男，1975年生，讲师，研究领域为安全协议分析、安全多方计算.

卿斯汉： 男，1939年生，研究员，主要研究领域为信息系统安全理论和技术.

谷利泽： 男，1965年生，副教授，主要研究领域为密码学.

杨义先： 男，1963年生，教授，主要研究领域为编码理论、密码学.