UC 安全的高效不经意传输协议

冯 涛,马建峰,李凤华
(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: 非承诺加密机制是语义安全的,不能抵抗选择密文攻击. 在 non-erase 模型的安全假设下,基于非承诺加密机制的不经意传输协议不能实现自适应攻击者 UC(Universally Composable)安全的定义. 利用可否认加密体制和可验证平滑投影哈希函数,提出了一个新的不经意传输协议,可否认加密体制通过陷门承诺的双陷门解密技术实现,新协议方案是可证明 UC 安全的,基于公共参考串模型,安全性可以归约为确定性复合剩余假设. 新协议参与方能够处理指数空间的消息,计算效率得到改善,通过两次协议交互可以实现 string-OT 协议,与 bit-OT 协议相比单轮通信效率提高 $O(n)$ 倍.

关键词: 信息安全; 不经意传输; UC 安全; 可否认加密
中图分类号: TP301 **文献标识码**: A **文章编号**: 0372-2112 (2008) 01-0017-07

Efficient and Universally Composable Security Oblivious Transfer

FENG Tao, MA Jian-feng, LI Feng-hua
(Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract: Non-committing encryption achieved only semantic security, in contrast, applications often require security against chosen ciphertext attacks. A main ingredient in the previous adaptive universally composable (UC) oblivious transfer protocols are non-committing encryptions. the previous proposals are not UC secure against adaptive adversaries in the so-called non-erase model. A new UC secure oblivious transfer protocols were proposed and schemes utilize two primitives of the verifiably smooth projective hashing and deniable encryption as constructed by. the double trapdoor decryption mechanism based on trapdoor commitment. Our construction is based on the decisional composite residuosity in common reference string (CRS) model. We constructed a two-message (1-round) string oblivious transfer protocol, which improves computational efficient that supports message spaces of size exponential and save $O(n)-1$ rounds communications efficient than bit-OT protocols.

Key words: information security; oblivious transfer; universally composable; security; deniable encryption

1 引言

不经意传输协议(Oblivious Transfer Protocols, OTP)是密码学中的一个基本协议,可用于实现比特承诺,两方 Circuit Evaluation、安全的多方计算、电子支付,网上交易等协议[1~5]. 在不经意传输协议初始阶段,发送者 T 拥有两个信息 m_0 和 m_1,接收者 R 拥有一个选择比特 b; 协议执行结束后,接收者 R 获得选择信息 m_b,但是不知道 m_{1-b} 信息,发送者 T 不知道接收者 R 的选择比特 b.

我们的目标是设计一个不经意传输协议,该协议将作为在许多应用中使用的子协议,或者和其他应用复合在一起使用的协议. 同时,我们试图开发一种只需分析一次就可广泛应用的协议. 为了实现这个目标,我们在协议安全的形式化方法中引入了一种特殊的方法,即通用可复合(Universally Composable, UC)安全模型[6].

协议安全定义通常按照真实协议"仿真"与理想协议"仿真"之间的计算不可区分性定义,该方法首先由 Beaver 提出[7],针对协议并行运行的安全需求,Canetti 提出了更为实际的异步并行环境 UC 形式化安全模型,具有 UC 安全的协议在并行条件和协议复合条件下仍然保持安全性,它很容易嵌入到更加复杂的协议中,并且不需要在每次新的应用中重新分析其安全性.

在 UC 框架模型中,典型的 UC 安全的 OTP[8~10]都利用了非承诺加密[11](Non-Committing Encryption, NCE). 在多方计算安全协议中,NCE 广泛的用于防御自适应的攻击者. NCE 是语义安全的,不能抵抗选择密文攻击.

收稿日期:2006-11-06;修回日期:2007-07-16
基金项目:国家自然科学基金(No. 60573036, 60633020);陕西省自然科学基金(No. 2005F28, 2007F37);西安市科技攻关项目(No. GG06017);西安电子科技大学研究生创新基金(No. 创 05006)

NCE 除了具有基本的加密性质之外,可以构造一个"假想的仿真器"提供"可仿真密文","可仿真密文"可以通过两种方式解密.但是 NCE 的"可仿真密文"不是由密文的发送者产生,而是由"假想的仿真器"产生.在 NCE 的使用中,假设自适应的主动攻击者在协议执行过程中截获了密文消息,在协议结束之后,攻击者攻陷了密文消息的发送者和接收者,这时,攻击者获得接收者的私钥(non-erase 模型)并要求消息发送者提供加密时使用的随机数,更进一步,攻击者可获得加密的明文消息,密文消息的发送者不具有防御自适应的主动攻击者的能力.

当使用基于仿真的可证明安全方法时,协议开始攻击者 A 没有攻陷发送者 T,仿真器 S 不知道发送者 T 输入的消息 (m_1, m_0),那么参与方局部仿真的输入消息 (m_1', m_0') 将与真实的输入消息 (m_1, m_0) 不同,如果攻击者 A 在协议执行结束后攻陷了密文消息的发送者和接收者,那么被攻陷的参与方使用的加密体制是否能够为仿真器 S 提供明文消息的可仿真来防御自适应的主动攻击者是协议安全证明的关键.

可否认加密机制可以实现明文消息的可仿真性,在多方计算安全协议中,可否认加密体制可用于防御在 non-erase 模型的安全假设下的自适应能力攻击者[12].例如,可否认加密为密文消息的发送者提供一个"伪造的随机数"使得密文消息"看起来像"不同明文的加密密文,该机制提供了明文的保密性,同时,可仿真的密文是发送者提供的而不是由"假想的仿真器"提供的,当使用基于仿真的可证明安全方法时,为仿真器 S 提供了"同一密文的可仿真明文".文献[13]提出了具有可否认加密性质的基于陷门承诺的双陷门解密体制(Double Trapdoor Decryption,DTD).

本文提出了一个新的 UC 安全的 OTP 方案,新的方案利用了两个密码学安全原语:"可验证平滑投影哈希函数(Verifiably Smooth Projective Hashing,VSPH)[4]"和具有可否认加密性质的 DTD 体制.新的协议具有如下功能和特点:(1)实现了"明文消息的可仿真性",对于在 non-erase 模型的安全假设下的自适应能力攻击者,新的 OT 协议是 UC 安全的.(2)通过 VSPH 防止协议发送者和接收者的恶意行为.(3)协议的基本安全原语结构简单,具有良好的计算效率,例如,VSPH 和具有可否认加密性质 DTD 体制可以归约为确定性复合剩余(Decisional Compounding Residuosity,DCR)假设[14].(4)基于公共参考串(Common References String,CRS)模型[15],协议在一轮交互中实现 UC 安全的 string-OT 协议,与 bit-OT 协议相比单轮通信效率提高 $O(n)$ 倍.

本文的安排如下:第一部分是 UC 安全框架模型简介及 UC-OT 协议安全模型的定义.第二部分说明本文使用的两个安全原语,第三部分提出了一个新的 UC-OT 协议方案.第四部分通过基于仿真的可证明安全技术,证明该协议是 UC 安全的.第五部分比较了相关工作.第六部分是本文的结论.

2 预备知识

2.1 UC 模型

UC 框架模型对"安全协议"进行了形式化的定义.首先,协议 π 的安全服务需求被定义为"理想函数 F",针对理想函数,存在虚拟攻击者 S(通常称为仿真器 S),该模型称为理想模型.其次,在真实的运行环境中,参与方可以实现协议的功能,同时存在真实的攻击者实体 A,该模型称为现实模型.基于"计算不可区分"概念,UC 框架模型定义了一个特殊的攻击者实体"环境机 Z",它代表着外部环境,协议 π 安全被定义为参与方在任何现实环境中的协议交互信息与参与方在具有可信任"理想函数"的理想模型中的协议交互信息对于"环境机 Z"是"计算不可区分的".UC 安全即协议 π 安全实现理想函数 F.

现实模型:攻击者 A 与运行协议 π 的参与方 $P_1, \cdots, P_n$ 共存.令 $REAL_{\pi,A,Z}(k, z, r)$ 表示当 Z 与攻击者 A、参与方在运行协议 π 时的交互信息视图,其中,随机信息 $r = r_Z, r_A, r_1, r_2, \cdots, r_n$,$k$ 是安全参数,z 是 Z 的输入信息,当交互信息分布空间 $X = \{REAL_{\pi,A,Z}(k, z, r)\}_{k\in N, z\in\{0,1\}^*}$,简记为 $REAL_{\pi,A,Z}$.

理想模型:理想模型包括理想函数 F、理想过程攻击者 S、虚构的参与方 $p_1', \cdots, p_n'$.令 $IDEAL_{F,S,Z}(k, z, r)$ 表示当 Z 与攻击者 S、理想函数 F 运行时的交互信息视图,其中,随机信息 $r = r_Z, r_S, r_1, r_2, \cdots, r_n$.当交互信息分布空间 $X = \{IDEAL_{F,S,Z}((k, z, r)\}_{k\in N, z\in\{0,1\}^*}$,简记为 $IDEAL_{F,S,Z}$.

区分器 在理想模型和现实模型之间存在一个区分器"环境机 Z".Z 通过提供参与方的输入 z,阅读参与方的输出与参与方交互,Z 也可以单独与攻击者 A 或 S 通信.

定义 1 令 $n\in N$,F 是理想函数,π 是 n 方协议,称 π 通用可复合安全实现 F,若任何攻击者 A 都存在一个理想过程攻击者 S,这使得外部环境 Z 有

$$REAL_{\pi,A,Z} \overset{c}{\approx} IDEAL_{F,S,Z} \tag{1}$$

2.2 安全假设

如果攻击者攻陷参与方,仅仅获得参与方输入的初始秘密信息,那么称为 erase 攻陷模型;如果攻击者可以获得参与方在协议执行过程中的所有的随机比特信息、秘密信息,那么称为 non-erase 攻陷模型.攻击者在协议执行开始之前就攻陷了参与方,该类攻击者称静

态攻击者;攻击者在协议交互的任意点攻陷协议,该类攻击者称自适应攻击者(目前最强的攻击者模型). 基于 CRS 模型,许多基本的协议可以满足并行 UC 安全定义,例如承诺协议、零知识证明协议等. CRS 模型假设仿真器 S 已知某些可信任的参与方建立的公开参考串. 基于 CRS 模型,本文在 non-erase 攻陷模型和自适应攻击者能力模型假设下研究 UC 安全的 OT 协议.

2.3　UC-OTP 的理想函数 F_{OT}

根据可证明安全协议理论,协议的安全属性和协议功能通过协议的安全模型描述. 在 UC 框架模型中,协议安全模型称为"理想函数".

UC-OTP 的理想函数 F_{OT}[8]:协议参与方包括发送者 T,接收者 R,协议的攻击者 S. 安全参数为 k.

(1) 根据从 T 处接收到的消息 $(Send, Sid, T, R, m_1, m_0)$,其中 $m_b \in \{0,1\}^{|m|}$, $b \in \{0,1\}$, F_{OT} 函数记录元组 (m_1, m_0). Sid 是协议本次的唯一会话标识,$|m|$ 表示消息的长度.

(2) 根据从 R 处接收到的消息 $(Receive, Sid, R, T, b)$, F_{OT} 函数向 R 发送 (Sid, m_b),向 S 发送 (Sid),然后终止.

定义 2　令 $n \in N$, F_{OT} 是不经意传输理想函数,UC-OTP 是异步并行的两方不经意传输协议,称 UC-OTP 通用可复合安全实现 F_{OT},若任何攻击者 A 都存在一个理想过程攻击者 S,这使得外部环境 Z 有

$$REAL_{UC\text{-}OTP,A,Z} \overset{c}{\approx} IDEAL_{F_{OT},S,Z} \qquad (2)$$

3　协议的安全原语

3.1　可验证平滑投影哈希函数

Cramer-Shoup 首次定义了投影哈希函数[16]. 投影哈希函数有 2 个密钥,一个是秘密的哈希密钥 k,一个是公开的投影密钥 α. 投影哈希函数的多元组表示为:$H = (H, K, X, L, \Pi, \beta, \alpha)$. 令 $\{H_k: X \to \Pi\}_{k \in K}$ 是以 $K(\xi)$ 为密钥的哈希函数集合,X 是消息集合,Π 是哈希函数值的集合,K 是哈希函数密钥集合. 定义投射密钥函数 $\beta: K \to \alpha$,即 $\alpha = \beta(k)$,α 是投影密钥集合. 困难子集成员问题针对每一个实例 ξ 说明了 2 个有限非空集合 X, $W \subseteq \{0,1\}^{ploy|k|}$ 和一个 NP 关系 $R_{NP} \subset X \times W$,即 $\xi = (X, W, R)$ 使得对应的语言 $L = \{x: \exists w. s. t(x, w) \in R\}$ 是非空的. VSPH 整合了投影哈希函数和可验证困难子集成员问题,强调了困难子集成员问题中的成员采样和非成员采样的可验证性[4]. 文献[4]基于 DCR 假设构造的安全的 VSPH.

定义 3　可验证困难子集成员问题　称困难子集成员问题 M 是可验证样本,若下列条件成立

(1) 问题可采样:存在一个概率多项式算法 $P(n)$, $n = 1^k$,采样得到一个实例 $\xi = (X, W, R) \leftarrow I_k$.

(2) 成员可采样:存在一个输入是实例 $\xi = (X, W, R) \in M$ 的概率多项式算法,输出是 $x \in L$ 和 $w \in W$,使得 x 的分布是 L 统计可忽略的均匀分布.

(3) 非成员可采样:存在一个输入是实例 $\xi = (X, W, R) \in M$ 和元素 $x_0 \in X$ 的概率多项式算法 $NO\text{-}M$,输出 $x_1 = NO\text{-}M(\xi, x_0)$ 使得:如果 $x_0 \in_R L$,那么 x_1 的分布是 $Y \subseteq X - L$ 统计可忽略的均匀分布;如果 $x_0 \in_R X$,那么 x_1 的分布是 X 统计可忽略的均匀分布.

(4) 非成员可验证:存在一个输入是任意的三元组 (ξ, x_0, x_1) 的概率多项式算法 YV,可验证存在比特 $b \in (0,1)$ 使得 $x_{1-b} \in Y \subseteq X - L$. 即

①如果 $x_0 \notin Y$ 且 $x_1 \notin Y$ 成立,那么 $YV(\xi, x_0, x_1) = 0$

②存在比特 b,如果 $x_b \in L$, $x_{1-b} \in NO\text{-}M(\xi, x_0)$,那么 $YV(\xi, x_0, x_1) = 1$

定义 4　投影哈希函数　称 $(H, K, \Pi, \alpha, \beta)$ 是困难子集成员问题 M 的投影哈希函数,若对每个实例 $\xi \in M$ 存在一个函数 f 使得每一个 $x \in L(\xi)$ 和每一个 $k \in K(\xi)$, $\alpha = \beta(k)$,有 $f(x; \beta(k), w) = H_k(x)$.

定义 5　非成员平滑投影哈希函数　称 $(H, K, \Pi, \alpha, \beta)$ 是困难子集成员问题 M 的非成员平滑投影哈希函数,若对每个实例 $\xi = (X, W, R)$ 和 $x_{1-b} \in Y$,其中 $Y \subseteq X - L$ 时,$(\beta(k_{1-b}), H_k(x_{1-b}))$ 和 $(\beta(k_{1-b}), \Pi \leftarrow \{0,1\}^k)$ 是不可区分的.

3.2　可否认加密性质 DTD 体制

为了实现"同一密文的可仿真明文",可否认加密体制可以通过基于陷门承诺的双陷门解密体制实现. 陷门承诺是指存在一个抗碰撞函数,对于抗碰撞函数,假定不知道陷门信息,对于不同的输入值,通过函数发现碰撞是不可能的;如果已知陷门信息,通过函数发现碰撞是容易的. 陷门承诺的功能由三个概率多项式时间算法组成:密钥生成算法 G,承诺算法 C,碰撞发现算法 F,简记为:$(G; C; F)$.

在基于陷门承诺的 DTD 体制中,解密方具有全局主私钥 sk_A 和全局主公钥 pk_A,加密方具有局部私钥 sk_L 和局部公钥 pk_L,其中加密方的局部私钥 sk_L 可由解密方的全局主私钥 sk_A 求出. 加密方使用局部公钥 pk_L 和全局主公钥 pk_A 加密信息,密文信息由两部分组成,例如 $c = (c_A \| c_L)$. 解密方如果使用主私钥 sk_A,那么解密算法需要全部密文信息 $c = (c_A \| c_L)$,对于加密方而言,加密方的局部私钥 sk_L 和局部公钥 pk_L 提供陷门承诺功能,密文信息 c_L 与明文信息相关. 基于陷门承诺的 DTD 体制由五个概率多项式时间算法组成,简记为:$(G; E; D, C, F)$. 本文选用基于 DCR 假设构造陷门承诺和 DTD 体制[13].

密钥生成算法 $G:(pk_A, sk_A) \leftarrow G_A(1^k)$, $(sk_L) \leftarrow G_{AL}(sk_A)$, $(pk_L, sk_L) \leftarrow G_L(1^k)$, k 是安全参数.

加密算法 $E: c = (c_A \| c_L) \leftarrow E(pk_A, pk_L, m_b, r_b)$, m_b 是消息明文, $c = (c_A \| c_L)$ 是密文, r_b 是随机数.

解密算法 $D: m_b \leftarrow D_A(sk_A, (c_A \| c_L))$.

承诺算法 $C: c_L \leftarrow C(pk_L, m_b, r_b)$, m_b 是消息明文, pk_L 是局部公钥, r_b 是随机数, c_L 是承诺值.

碰撞发现算法 F:如果 $r_F \leftarrow F(sk_L, c_L, m_b, r_b, m_F)$, m_b 是消息明文, r_b 是随机数, m_F 是任意消息明文,那么 $c_L = C(pk_L, m_F, r_F)$.

除了加密体制的需求以外,上述算法需要(1) $(G; E, D; C; F)$ 是多项式时间可计算. (2)没有有效算法以不可忽略的概率使得 $m_F \neq m_b$, $r_F \neq r_b$,而 $C(pk_L, m_F, r_F) = C(pk_L, m_b, r_b)$. (3)对于任何 m,$\{c_L = C(pk_L, m, r)\}_{r \in R}$是均匀分布不可区分的.

4 UC 安全的 OT 协议

本文提出的 UC-OTP 以 Kalai 提出的不经意传输协议[4]为基础,Kalai 定义了"可验证平滑哈希函数",可验证平滑哈希函数防止了恶意的消息接收者同时获得不经意传输的两个消息.但是,在 UC 框架模型中,如果假定攻击者在协议执行的任意点攻陷参与方(自适应的攻击者),文献[17]分析并说明了 Kalai 协议方案不能满足自适应攻击者模型的 UC 安全定义.基于 CRS 模型,文献[10]利用 NCE 实现了 UC 安全的 Kalai 协议方案,CRS 信息包括 NCE 虚拟密钥的辅助信息和虚拟密文,"假想的仿真器"提供的虚拟密文不包括参与方局部仿真的输入消息 m_b',当密文消息的发送者被攻陷后,"假想的仿真器"提交虚拟密钥信息实现密文的可仿真性,可仿真的密文并不是发送者提供.文献[10]通过 CRS 信息建立的安全假设较强,本文方案减弱了通过 CRS 信息建立的安全假设,在 non-erase 攻陷模型假设条件下利用可否认加密性质的 DTD 体制,参与方局部仿真的输入消息为 (m_1', m_0'),如果攻击者 A 在协议执行结束后攻陷了密文消息的发送者和接收者,那么仿真器 S 能够保证被仿真的现实模型中攻击者 A 具有与被攻陷的参与方一致的输入消息 (m_1, m_0).

协议的符号与本文 2 相同.协议具体的描述如下:

(1) $R \rightarrow T$:接收者 R 产生三元组 (x_0, x_1, w_b),其中 $x_0 \in_R L$, $(x_0, w_b) \in_R R_{NP}$, $x_1 \in_R X - L$, $b \in \{0,1\}$,保留证人 w_b.根据可否认加密性质的 DTD 体制密钥生成算法 $G:(pk_A, sk_A) \leftarrow G_A(1^k)$,获得密钥对 (pk_A, sk_A),向 T 发送 (Sid, x_0, x_1, pk_A). Sid 是 OT 协议并行运行时一个协议实例的会话标识.

(2) $T \rightarrow R$:根据接收到的消息 (Sid, x_0, x_1),如果 $YV(\cdot) = 0$,协议终止,如果 $YV(\cdot) = 1$,那么选择两个不同的随机哈希函数密钥 (k_0, k_1),计算哈希函数值 $(H_{k0}(x_0), H_{k1}(x_1))$,执行投影算法 $\beta(\cdot)$,获得投影密钥 $(\alpha_0 = \beta(k_0), \alpha_1 = \beta(k_1))$,根据陷门承诺密钥生成算法 $G:(pk_L, sk_L) \leftarrow G_L(1^k)$,获得密钥对 (pk_L, sk_L),根据加密算法 $E: c \leftarrow E(pk_A, pk_L, m, r)$,计算 $c_0 = E(pk_A, pk_L, m_0, r_0)$, $c_1 = E(pk_A, pk_L, m_1, r_1)$,最后计算 $y_1 = c_1 \oplus H_{k1}(x_1)$, $y_0 = c_0 \oplus H_{k0}(x_0)$.向 R 发送 $(Sid, \alpha_0, \alpha_1, y_0, y_1)$.

R:已知证人 w_b 和投影密钥 α_b,通过函数 $c_b = y_b \oplus f(x_b, \beta(k_b), w_b)$ 恢复 c_b,根据获得的 c_b,执行解密算法 $D: m_b \leftarrow D_A(sk_A, c_b)$ 恢复 m_b.

5 UC-OT 协议的安全性分析

定理 1 基于公共参考串模型,利用 VSPH 和可否认加密性质的 DTD 体制,对于在 non-erase 模型的安全假设下的自适应能力攻击者,两方 UC-OTP 安全实现理想函数 F_{OT}.

证明:证明思路如下:首先使用可证明安全的仿真器技术,建立各种仿真情景,其次证明本文的定义 2 成立.基于 CRS 模型,对于本文而言,仿真器 S 已知发送方的随机哈希函数密钥 (k_0, k_1) 和局部私钥 sk_L,接收方的全局主私钥 sk_A.

令 A 是自适应攻击者.构造一个理想过程中针对 F_{OT} 的攻击者 S(称为仿真器),在理想过程中,S 可以与理想函数 F_{OT} 和环境机 Z 交互. S 因 A 的副本 $\tilde{A}$ 调用而工作,副本 $\tilde{A}$ 与现实模型中的 A 交互.对于仿真器 S,在理想过程中的交互称为仿真器 S 的外部交互,与 A 的副本 $\tilde{A}$ 之间的交互称为仿真器 S 的内部交互.

仿真器 S 的工作情况如下:

仿真发送者 T.

(1)发送方 T 未被攻陷,接收方 R 未被攻陷的情况.在理想过程中,仿真器 S 获得 (Sid),然后终止.对于现实模型中的发送者 T 和接收者 R 的仿真通过协议规程完成.仿真器 S 模拟虚拟的接收者 R 提供 (x_0, x_1, w_b);模拟虚拟的发送方 T 验证数据的非成员采样,基于 CRS 模型,仿真器 S 随机选择 (k_0, k_1),计算 $H_{kb}(x_b)$ 并利用投影密钥算法 $\beta(\cdot)$ 生成投影密钥 (α_0, α_1);随机选择任意消息明文 $m_F \leftarrow \{0,1\}^{|m|}$,利用加密算法 $E: c' \leftarrow E(pk_A, pk_L, m_F, r_F)$ 生成仿真密文 $c_b' = c_{Ab} \| c_{Lb}$,其中 $c_{Lb} = C(pk_L, m_F, r_F)$,计算 $y_b \leftarrow c_b' \oplus H_{kb}(x_b)$,另外随机选择 $y_{1-b} \leftarrow \{0,1\}^{|m|}$,并发送 $(y_0, y_1, \alpha_1, \alpha_0)$.由于两个参与方都没有被攻陷,仿真器 S 仿真的消息 $(y_0, y_1, \alpha_1, \alpha_0)$, (c_b, m_F, r_F) 都是随机分布的.

(2) T 未被攻陷,攻击者 A 攻陷接收方 R 的情况.仿真器 S 在内部交互的仿真过程中,通过 $\tilde{A}$ 获得真实

接收者 R(A 攻陷接收方 R)提供的消息(x_1, x_0). 仿真器 S 在外部交互中模仿接收者 R($\tilde{A}$ 将 w_b 提供给仿真器 S)向理想函数 F_{OT}提供(b)并获得从 F_{OT}发向虚拟接收者 R 的消息(m_b),[见 F_{OT}理想函数定义第二条]. 这时,仿真器 S 在内部交互的仿真过程中,随机选择(k_0, k_1),计算 $H_{kb}(x_b)$ 并利用投影密钥算法 $\beta(\cdot)$ 生成投影密钥(α_0, α_1),根据获得的真实的 m_b,利用加密算法 E: $c_b \leftarrow E(pk_A, pk_L, m_b, r_b)$,生成 c_b,计算 $y_b \leftarrow c_b \oplus H_{kb}(x_b)$,另外随机选择 $y_{1-b} \leftarrow_R \{0,1\}^{|m|}$,并发送($y_0$, y_1, α_1, α_0). 仿真器 S 仿真的消息(y_{1-b}, α_1, α_0),(r_b)都是随机分布的.

(3)发送方 T 给理想函数发送消息(m_0, m_1)之前,攻击者 A 攻陷发送方 T 的情况. $\tilde{A}$ 将(m_0, m_1)提供给仿真器 S. 由于仿真器 S 获得了被攻陷发送方 T 提供的(m_0, m_1)[见 F_{OT}理想函数定义第一条]. 那么,仿真器 S 在内部交互和外部交互的仿真过程中都使用加密算法 $E: c \leftarrow E(pk_A, pk_L, m, r)$ 和真实的(m_0, m_1)产生消息(c_1, c_0)及(y_1, y_0).

(4)发送方 T 给理想函数发送秘密消息(m_0, m_1)之后,攻击者 A 攻陷发送方 T 的情况.

①如果接收者 R 已被攻陷,仿真器 S 接收到 F_{OT}发向虚拟接收者 R 的消息(m_b),仿真情况与本节仿真发送者 T 情况(2)是一样的.

②如果此时接收者 R 仍然未被攻陷,仿真情况与本节仿真发送者 T 情况(1)是一样的.

仿真接收者 R.

(1)接收者 R 未被攻陷,发送者 T 未被攻陷的情况. 这种情况如同仿真发送者 T 情况的(1).

(2)接收者 R 在协议开始被攻陷,T 未被攻陷的情况. 这种情况如同仿真发送者 T 情况的(2).

(3)接收者 R 发送(x_0, x_1)后被攻陷,发送方 T 给理想函数发送秘密消息(m_0, m_1)之前未被攻陷的情况. 这种情况如同仿真发送者 T 情况的(2).

(4)发送方 T 发送消息(y_1, y_0)之后,接收方 R 最后被攻陷的情况.

①如果 T 仍然未被攻陷. 这种情况如同仿真发送者 T 情况的(2).

②如果 T 最后也被攻陷. 攻击者 A 此时获得真实的(m_0, m_1)信息并通过已知证人 w_b 和投影密钥 α_b,函数 $c_b = y_b \oplus f(x_b; \alpha_b, w_b)$ 恢复 $c_b = c_{Ab} \| c_{Lb}$. 同时,仿真器 S 在交互外部获得了被攻陷发送方 T 提供的(m_0, m_1)和被攻陷接收方 R 提供的 w_b,仿真器 S 已知 $c_{Ab} \| c_{Lb}$和 m_b,利用碰撞发现算法 F 获得 $r_b \leftarrow F(sk_L, c_L, m_b, r_F, m_F)$. 此时,在内部交互的仿真过程中假定攻击者 A 要求验证仿真器 S 仿真的消息 c_{Lb}是否一致,由于 $c_{Lb} = C(pk_L, m_b, r_b) = C(pk_L, m_F, r_F)$,仿真器 S 将 r_b 提供给攻击者 A,A 使用 r_b, m_b 验证 $c_{Lb} = C(pk_L, m_b, r_b)$.

通过上面的描述,仿真器 S 仿真了协议运行的全部状态.

定义 2 的证明. 由于 Z 和 A 及 UC-OTP 参与方交互获得的观察序列与理想过程中 Z 和 S 及在内部交互中副本 $\tilde{A}$ 的观察序列等价,Z 的观察序列的不可区分性证明转化为仿真器 S 的内部交互仿真与外部交互仿真的不可区分. 仿真器 S 内部交互仿真与外部交互仿真的不可区分性最终归约为两个密码学原语的安全性. 完美仿真通过五种情况证明.

参与方都未被攻陷的仿真是不可区分的. 对于仿真器 S 而言,S 按照协议规则,仿真的消息都是均匀随机分布的,因此是完美仿真的.

参与方开始被攻陷(静态攻击者)的仿真是不可区分的. 对于仿真器 S 而言,由于参与方被攻陷,S 仿真的消息将与现实模型中协议的消息保持一致,因此是完美仿真的.

T 被攻陷的仿真是不可区分的. 假定发送者 T 被攻陷,攻击者 A 控制发送者 T,完美仿真意味着攻击者 A 获得接收者 R 的选择消息 b 是可忽略的.

反证法. 假设存在一个不可忽略的概率多项式攻击算法 B 预知 w_b'. 攻击者 B 可以通过预知 w_b 进而区分 $x \in_R L$ 和 $x \in_R X$,这将破坏困难子集成员问题 M 的定义 3.

假定一个实例 $\xi_k(X, W, R) \leftarrow I_k$ 和一个元素 $x \in X$. (1)随机选择 b,令 $x_b = x$. (2)利用算法 $NO\text{-}M(\cdot)$ 产生 x_{1-b}. (3)将(x_0, x_1)发给攻击者 B,并获得攻击者 B 预知的 w_b'. (4)如果 $w_b' = w_b$ 那么表明攻击者 B 预知 $x \in_R L$. 如果 $w_b' \neq w_b$,那么表明攻击者 B 预知 $x \in_R X$. 一方面,如果预知 $x_b \in_R L$,那么存在一个不可忽略的概率多项式攻击者 B 预知 w_b,与本文定义 3 矛盾. 另一方面,如果 $x_b \in_R X$,那么 $x_{1-b} \in_R X$,这种情况 w_b 是不可预知的(信息论已有理论). 既然不存在不可忽略的概率多项式攻击者 B,那么也不可能存在同样能力的攻击者 A 和 Z.

R 被攻陷的仿真是不可区分的. 假定接收者 R 被攻陷,攻击者 A 控制接收者 R,完美仿真意味着发送者 T 送出的(m_0, m_1)和(m_b, $r \leftarrow_R \{0,1\}^{|m|}$)是不可区分的. VSPH 的性质保证接收方只能获得(m_0, m_1)中的一个.

关于(y_0, y_1)的随机均匀分布. 发送者 T 产生的 $y_b \leftarrow c_b \oplus H_{kb}(x_b)$, $y_{1-b} \leftarrow_R \{0,1\}^{|m|}$)是不可区分的. 根据非成员采样,必存在 $x_0 \in X - L$ 或 $x_1 \in X - L$,否则,协议终止. 对于 $b \in_R \{0,1\}$ 不失一般性,假定 $x_{1-b} \in X - L$,那么根据非成员平滑投影哈希函数的性质(见本文定义

5),(α_{1-b}, $H_{k1-b}(x_{1-b})$)和(α_{1-b}, $r \leftarrow \{0,1\}^{|m|}$)是不可区分的,从而($\alpha_b$, $c_b \oplus H_{kb}(x_b)$)与(α_{1-b}, $r \leftarrow \{0,1\}^{|m|}$)是均匀分布的.

关于(c_b, c_b')的随机均匀分布. $T(1)$中,仿真器 S 提供的 $c_b' \leftarrow E(pk_A, pk_L, m_F, r_F)$. $T(2)$中,仿真器 S 提供的 $c_b = E(pk_A, pk_L, m_b, r_b)$. 根据陷门承诺的性质:可以为"仿真器"提供"同一密文的可仿真明文",即 $c_{Lb} = C(pk_L, m_b, r_b) = C(pk_L, m_F, r_F)$,因此 c_b 和 c_b' 是不可区分的.

基于 non-erase 模型的仿真是不可区分. 仿真器 S 在仿真过程中需要仿真参与方的随机信息并写入随机纸带,随机信息是参与方的内部数据,例如,加密算法 E 的随机信息(r_b),碰撞发现算法 F 获得(r_F),可否认加密为密文消息的发送者提供一个"伪造的随机数"使得密文消息"看起来像"不同明文的加密密文,该机制为密文消息的发送者提供了明文的保密性,为"仿真器"提供了"同一密文的可仿真明文". 因此是完美仿真的.

(证毕)

6 相关工作的比较

基于大多数诚实参与方模型,文献[8]提出了一个由第三方辅助完成的 UC-OT 协议. 该方案在四步交互中利用特殊的辅助信息实现了自适应攻击者安全的 bit-OT 功能,首先接收者 R 和辅助者第三方分别利用发送者 T 的 NCE 的公钥加密各自的随机密钥;其次要求发送者 R 提供辅助比特信息;最后发送者 R 通过辅助比特信息实现 erase 模型的 UC-OTP. 但是该方案存在以下问题:基于 DDH 假设,该方案的协议计算效率仅能处理多项式空间消息,为了实现自适应攻击者安全的 UC-OT 协议,降低了协议参与方被攻陷的安全假设,例如基于 erase 攻陷模型. 无法防止接收方与辅助第三方共谋获得发送者提供的全部消息(m_0, m_1);辅助第三方的假设,增加了协议的交互次数,降低了协议的通信效率,限定了协议的应用场景.

基于公共参考串模型,文献[9]提出了不经意密钥生成技术的 NCE 的 UC-OTP. 该方案在三步交互中实现了自适应攻击者安全的 bit-OT 功能. 但是该方案存在以下问题:协议的结构复杂,在使用 NCE 机制之前,协议必须实现不经意密钥生成算法和密钥可逆算法,通过零知识证明预防接收者的恶意行为,计算效率、通信效率都不理想,协议整体效率不高.

文献[10]改善了文献[9]方案的计算效率和通信效率,提出了基于 VSPH 的 NCE 的 UC-OTP. 该方案实现了 string-OT,与 bit-OT 协议相比通信效率提高了 $O(n)$ 倍,协议的安全性基于确定性复合剩余假设,提高了协议的计算效率.

本文修正了基于 non-erase 模型的 UC-OTP 协议的安全分析,根据 NCE 固有的工作机制,我们知道现有 UC-OTP 协议[8~10]假设密文消息的发送者对于明文消息是可以 erase 的,在 non-erase 模型的安全假设下不能实现自适应攻击者 UC 安全的定义. 现有 UC-OTP 协议通过 CRS 信息建立的安全假设较强. 本文弱化了 CRS 模型,增强了协议安全模型,使用了新的可否认加密体制原语. 同时,本文保留了我们已提出方案的优点[10],新的 UC-OPT 协议仍然直接实现了串的 OT 传输,与 bit-OT 协议相比单轮通信效率提高 $O(n)$ 倍,利用 VSPH 实现了证人不可区分,简化了零知识证明. 表 1 为本文方案与其它 UC 安全的 OTP 方案的比较.

表 1 UC 安全的 OTP 方案比较

UC-OTP Scheme	a multi-party setting	Data erasure assumption	Against malicious receiver.	The encryption method.	Protocol Interactive	1-round
Fischlin 's scheme[8]	the setting of honest majorities.	sender erase	homomorphic commitment	non-committing encryption	4	Bit-OT
Canetti 's scheme[9]	The strong CRS model	sender erase	an expensive compiler	non-committing encryption	3	Bit-OT
LFM 's scheme[10]	The strong CRS model	sender erase	the VSPH method	non-committing encryption	2	String-OT
Our 's scheme	The weak CRS model	non-erase	the VSPH method	deniable encryption	2	String-OT

7 结论

不经意传输协议是密码学协议中的一个基本安全原语,本文提出了一个利用可否认加密体制和 VSPH 实现的不经意传输协议,该协议将作为在许多应用中使用的子协议,或者和其他应用复合在一起使用的协议. 同时,在 UC 框架中,该协议只需分析一次就可广泛应用的协议. 本文方案弱化了通过 CRS 信息建立的安全假设,使得不经意传输协议安全模型具有更强的安全属性,在多方计算安全协议中,该协议实现了"明文消息的可仿真性",在 non-erase 模型的安全假设下新的 OT 协议是 UC 安全的,可以更好的防御自适应的主动攻击者.

参考文献:

[1] Rabin M O. How to exchange secretes by oblivious transfer [R]. Tech. Rep. TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[2] Shimon Even, Oded Goldreich, Abraham Lempel. A randomized

protocol for signing contracts [J]. Communications of the ACM, 1985, 28(6): 637 - 647.

[3] Moni Naor, Benny Pinkas. Efficient oblivious transfer protocols [A]. In Proceedings of SODA 2001[C]. SIAM Symposium on Discrete Algorithms, 2001. 448 - 457.

[4] Yael Tauman Kalai. Smooth projective hashing and two-message oblivious transfer [A]. In Advances in Cryptology-Eurocrypt[C]. 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 78 - 95.

[5] 李顺东,戴一奇,游启友. 姚氏百万富翁问题的高效解决方案[J]. 电子学报, 2005, 33(5): 769 - 773.
LI Shun-dong, DAI Yi-qi, YOU Qi-you. An efficient solution to Yao's millionaires' Problem [J]. Acta Electronica Sinica, 2005, 33(5): 769 - 773. (in Chinese)

[6] R Canetti. Universally composable security: A new paradigm for cryptographic protocols [A]. In Proceedings of the 42nd IEEE Symposium on the FOCS[C]. New York: IEEE Computer Society Press, 2001. 136 - 145.

[7] Beaver, D. Foundations of secure interactive computing[A]. In Proc Advances in Cryptology (CRYPTO 1991) [C]. LNCS 576, Berlin: Springer, 1991. 377 - 391.

[8] Marc Fischlin. Universally composable oblivious transfer in the multi-party setting [OL]. www. mi. informatik. uni-frankfurt. de/ people/ marc/ publications/ fischlin. uc-ot. 2006. pdf.

[9] R Canetti, Y Lindell, R Ostrovsky, A Sahai. Universally composable two-party and multi-party secure computation [A]. In 34th ACM Symposium on the Theory of Computing[C]. Quebec, ACM. 2002. 494 - 503.

[10] 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 Feng-hua, FENG Tao, MA Jian-feng. Universally composable oblivious transfer protocols based on VSPH[J]. Journal on Communications. 2007, 28(7): 28 - 34. (in Chinese)

[11] I Damgard, J B Nielsen. Improved non-committing encryption schemes based on general complexity assumptions [A]. In CRYPTO '00[C]. LNCS 1880. Berlin: Springer-Verlag, 2000. 432 - 450.

[12] R Canetti, C Dwork, M Naor, R Ostrovsky. Deniable Encryption[OL]. http://theory.lcs.mit.edu/tcryptol, 1996.

[13] E Bresson, D Catalano, D Pointcheval. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications [A]. Advances in Cryptology-Proceedings of Asiacrypt '03 [C]. C. S. Laih Ed. LNCS 2894. Berlin: Springer-Verlag, 2003. 37 - 54.

[14] P Paillier. Public-key cryptosystems based on composite-degree residuosity classes[A]. In Advances in Cryptology, Eurocrypt '99[C]. LNCS 1592, Berlin: Springer-Verlag, 1999. 223 - 238.

[15] Goldreich O, Micali S, Wigderson A. How to play any mental game-a completeness theorem for protocols with honest majority[A]. In Proceedings of the 19th Annual ACM Symposium on Theory of Computing[C]. 1987. 218 - 229.

[16] R Cramer, V Shoup. Universal hash proofs and a paradigm for adaptive chosen cipher text secure public-key encryption[A]. Advances in Cryptology, Eurocrypt 2002 [C]. LNCS vol. 2332, Berlin: Springer-Verlag, 2002. 45 - 64.

[17] 冯涛,马建峰. Y-SPH-OT 协议的安全性分析[A]. 2006TCS 论文集[C]. 长春,计算机科学, 2006, 33(8 supplement): 125 - 129
FENG Tao, MA Jian-feng. The security analysis for Y-smooth projective hashing oblivious transfer protocols [A]. In Proc 2006TCS[C]. changchun, computer science, 2006, 33(8 supplement): 125 - 129. (in Chinese)

作者简介:

冯　涛　男,1970 年生于甘肃临洮,西安电子科技大学博士生,兰州理工大学研究员. 主要研究兴趣为安全协议复合理论、无线传感器网络安全. E-mail: fengt@lut.cn

马建峰　男,1963 年生于陕西西安,西安电子科技大学计算机学院院长,教授,博导. 主要研究领域为计算机安全、密码学、移动与无线网络安全.

李凤华　男,1966 年生于湖北浠水,西安电子科技大学博士生,北京电子科技学院教授. 主要研究方向为网络安全与可信计算.