

普适复合水银承诺方案

徐海霞 李红达 李 宝

(中国科学院研究生院信息安全国家重点实验室 北京 100049)

摘 要 水银承诺方案是一般承诺方案的一种有趣变形. 水银承诺方案中增加了模糊公开阶段, 模糊公开阶段不要求绑定性但是不能与真实的公开阶段冲突. 普适复合安全性基本框架最早由 Canetti 等人提出. 普适复合能够保证更高等级的安全性, 比如满足普适复合性质即能实现并发安全、自适应安全以及非延展安全等等. 文中提出一种普适复合水银承诺方案的构造并且在公共参数模型中证明其安全性. 文中的结论一方面深化了水银承诺方案的研究, 另一方面回答了 Gennaro 和 Micali 提出的一个公开问题.

关键词 普适复合; 水银承诺

中图法分类号 TP309

Universally Composable Mercurial Commitment Scheme

XU Hai-Xia LI Hong-Da LI Bao

(State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049)

Abstract A mercurial commitment scheme is an interesting variation of a regular commitment scheme, which extends to allow for a soft decommit stage. The soft decommitments are not binding but can not conflict with the true decommitments. The original application of mercurial commitment is to construct zero knowledge sets. The universally composable framework initiated by Canetti is very useful due to its ensuring stronger securities such as concurrent security, adaptive security, non-malleability, etc. This paper proposes a universally composable mercurial commitment scheme and proves its security in the common reference string (CRS) model. On one hand, the research on mercurial commitment scheme is deepened, on the other hand the result answers an open problem presented by Gennaro and Micali.

Keywords universally composable; mercurial commitment

1 引 言

承诺方案是理论密码学中重要的基本模块之一. 承诺方案由两个 PPT 算法组成, 分别称为承诺方和接收方. 承诺方案有两个阶段: 承诺阶段和公开阶段. 在承诺阶段, 承诺方发送其秘密输入 m 的承诺值给接收方; 在公开阶段, 承诺方可以公开其秘密

输入 m . 承诺方案要满足隐藏性和绑定性两个性质. 所谓隐藏性是指接收方根据承诺值不能计算关于承诺方秘密输入 m 的信息. 绑定性是指承诺方不能将承诺值公开为两个不同的 m 和 m' .

水银承诺最早由 Chase 等在文献[1]中提出, 是经典承诺方案的一种有趣变形. 较之于经典的承诺方案, 水银承诺方案关于绑定性质有显著的放松. 水银承诺方案将通常承诺方案的公开阶段分成两个阶

段, 分别称为模糊公开 (soft-open) 和确定公开 (hard-open) 阶段. 在模糊公开阶段, 不要求满足绑定性质但是不能与真正的公开信息矛盾. 确定公开阶段即如通常承诺方案的公开阶段. 在水银承诺方案中, 每一个承诺值要满足以下条件之一: (1) 同时模糊公开和确定公开为同样的 m ; (2) 可以模糊公开为任何 m' , 但是不能再确定公开. 相应地, 在承诺阶段, 承诺方有两种承诺算法可以选择. 可以采用模糊承诺算法 (不对任何具体值做承诺), 也可以采用确定承诺算法 (与通常承诺方案的承诺算法相同, 只对唯一的值做承诺). 接收方不能区分其收到的承诺值是经由哪一种承诺算法得到的. 在 Catalano 等人向 2006 年的理论密码学会议 (TCC'06) 提交的论文^[2]中, 解决了这种新的密码学原语的最小假设问题并且提出几类高效的构造方案.

水银承诺的概念最早来源于零知识集协议^[3]. 零知识集协议是指: 证明者对一个秘密集合 S 做承诺, 将承诺值发送给验证者, 验证者提出询问 x , 证明者证明 x 是否属于集合 S , 不能泄露关于集合 S 的其它任何信息, 甚至不能泄露集合 S 的势. 在开放的网络中, 对于协议的安全性有较高需求. 需要满足某些附加的安全性. 非延展性质就是一种重要的考量指标. 在文献[4]中, Gennaro 和 Micali 研究了零知识集的非延展性质以及独立性质, 后者是比非延展性更强的安全性要求.

根据对几类经典非延展承诺方案构造的深入考察, Gennaro 和 Micali 首先分离出独立承诺的概念. 独立承诺是指不论诚实的承诺方如何公开其承诺值, 敌手都只能以唯一的方式公开它自己产生的承诺值. 在该文献中, 进一步提出独立零知识集的概念. 为了深入分析独立零知识集和非延展性零知识集, 作者提出了几个公开问题, 普适复合水银承诺方案的存在性即是其中之一.

普适复合安全性框架, 由 Canetti 在文献[5]中提出. 普适复合安全性沿袭了安全多方计算^[6]的基本思想和方法, 并能保证更强的安全性. 协议 Π 的参与方记为 P_1, P_2, \dots, P_n . 攻击协议 Π 的敌手记为 \mathcal{A} . 敌手 \mathcal{A} 控制各个参与方之间的通信, 是自适应的 (敌手根据目前收集到的信息决定将要入侵哪一个参与方), 能够实行主动 (active) 攻击, 运行于异步网络. 实际上, 对于这种模型中的敌手几乎没有限制, 是最一般的情形. 为了定义普适复合结构的安全性, 引入了环境机 \mathcal{Z} 的概念. 这里, n 个参与方 P_1, P_2, \dots, P_n , 敌手 \mathcal{A} 以及环境机 \mathcal{Z} 都是概率多项式时

间的交互图灵机. 实际协议的执行过程如下: 首先环境机 \mathcal{Z} 被激活, 被激活之后, 环境机 \mathcal{Z} 或者给某个参与方 P_i 提供输入, 或者发送消息给敌手 \mathcal{A} . 如果某个参与方 P_i 收到输入, 则此时 P_i 被激活, P_i 可以发送消息 (通过被敌手控制的信道) 给其它参与方或者向环境机发布输出. 如果敌手 \mathcal{A} 被激活, 那么它可以采取下列动作之一: 入侵某个诚实的参与方; 以被入侵参与方的身份发布消息; 传递消息 (敌手控制通信信道); 与环境交互. 在理想模型中, 理想函数是一个交互图灵机, 表示协议要完成的功能. 每个参与方将各自的输入提交给理想函数 \mathcal{F} , 等待计算结果, 参与方互相之间没有交互. 理想模型敌手的攻击行为是入侵理想模型中的参与方进而可以改变他们的输入, 阻滞或监测 \mathcal{F} 发给各个参与方的输出结果. 显然, 理想模型是平凡安全的协议. 协议 Π 的普适复合安全性定义为对于任意有效的攻击实际协议的敌手 \mathcal{A} , 存在有效的理想模型敌手 \mathcal{S} , 使得任意环境机 \mathcal{Z} 不能区分是与 \mathcal{A} 和参与方在实际协议中交互还是与 \mathcal{S} 和 \mathcal{F} 在理想模型中交互.

为了解决文献[4]中提出的公开问题, 也由于普适复合方案其自身的优势, 我们提出一个普适复合的水银承诺方案, 并且证明在公共参数 (common reference string) 模型中, 在无爪陷门置换对和不可区分的抵抗自适应选择密文攻击加密方案存在的基础上, 该方案满足普适复合安全性.

2 背景知识

可忽略函数. 一个函数 $\mu(n)$ 称为可忽略函数, 如果对任意正多项式 $p(\cdot)$, 存在正整数 N , 使得对任意 $n > N, \mu(n) \leq \frac{1}{p(n)}$.

有效算法. 本文中的有效算法是指概率多项式时间图灵机.

计算不可区分. 两个随机变量族 $X = \{X_\omega\}_{\omega \in S}$ 和 $Y = \{Y_\omega\}_{\omega \in S}$ 称为计算不可区分的, 如果下列条件成立: 对于任意多项式尺寸电路族 $\{C_n\}_{n \in \mathbb{N}}$, 任意正多项式 $p(\cdot)$, 充分大的 n , 任意 $\omega \in S \cap \{0, 1\}^n$, 有下式成立

$$| \Pr[C_n(X_\omega) = 1] - \Pr[C_n(Y_\omega) = 1] | < \frac{1}{p(n)}.$$

3 水银承诺方案

与经典的承诺方案相比, 水银承诺方案需要以

下两个附加要求:(1) 在承诺阶段, 承诺方可以选择确定承诺算法或者模糊承诺算法;(2) 在公开阶段, 承诺方可以选择确定公开算法或者模糊公开算法. 水银承诺方案要满足下列条件:(1) 给定一个承诺值(无论是确定承诺值还是模糊承诺值)不能泄露关于被承诺值的信息;(2) 没有 PPT 算法能够区分一个承诺值是确定承诺值还是模糊承诺值;(3) 确定承诺值能够确定公开也能够模糊公开, 但是必须公开为同一个值;(4) 模糊承诺值不能确定公开, 能够模糊公开并且可模糊公开为任意值. 此处我们直接引用文献[2]中的定义.

定义 1. 水银承诺方案由以下 7 个算法组成:

$$\mathcal{C} = (\text{MCom-Gen}, \text{HCom}, \text{HOpen}, \text{HVer}, \text{SCom}, \text{SOpen}, \text{SVer}),$$

其中前面 4 个算法与经典承诺方案中相应的算法完全相同.

$\text{MCom-Gen}(1^k)$, 承诺密钥生成算法. 输入安全参数 1^k , 算法输出承诺方案需要的公钥 pk .

$\text{HCom}_{pk}(m; r)$, 确定承诺算法. 给定输入 pk , 消息 m 以及随机数 r , 算法输出关于消息 m 的确定承诺值 c .

$\text{HOpen}_{pk}(m; r)$, 确定公开算法. 给定输入 pk , m 和承诺算法中应用的随机串 r , 算法产生确定公开值 d .

$\text{HVer}_{pk}(m, c, d)$, 确定验证算法. 给定输入 pk , m, c, d , 如果 (c, d) 是 m 的承诺/公开值, 则算法输出 1; 否则输出 0.

$\text{SCom}_{pk}(\cdot; r)$, 模糊承诺算法. 给定输入 pk 和随机串 r , 算法产生承诺值 c (注意此时 c 与任何消息 m 无关).

$\text{SOpen}_{pk}(m, FLAG; r)$, 模糊公开算法, 其中 $m \in \mathcal{M}$ 且 $FLAG \in \{H, S\}$. 算法产生关于 m 的模糊公开值 τ . 如果 $FLAG = H$, 那么 τ 经由确定承诺 $c = \text{HCom}_{pk}(m; r)$ 产生; 如果 $FLAG = S$, 那么 τ 经由模糊承诺 $c = \text{SCom}_{pk}(\cdot; r)$ 产生.

$\text{SVer}_{pk}(m, c, \tau)$, 模糊验证算法. 如果 τ 能够证明 c 是对 m 的模糊承诺, 则输出 1; 否则输出 0.

上述 7 个算法要满足如下要求.

正确性. 对任意 $m \in \mathcal{M}$, 下列等式成立:

$$\begin{aligned} \text{HVer}_{pk}(m, \text{HCom}_{pk}(m; r), \text{HOpen}_{pk}(m; r)) &= 1, \\ \text{SVer}_{pk}(m, \text{HCom}_{pk}(m; r), \text{SOpen}_{pk}(m, H; r)) &= 1, \\ \text{SVer}_{pk}(m, \text{SCom}_{pk}(\cdot; r), \text{SOpen}_{pk}(m, S; r)) &= 1. \end{aligned}$$

水银绑定. 没有 PPT 敌手 \mathcal{A} 能够提出 (c, m, π, m', π') ($\text{resp. } (c, m, \tau, m', \pi')$) 使得 $\pi(\text{resp. } \tau)$ 是公开为 m 的确定(模糊)公开值, 而 π' 是 c 公开为 m' 的

确定公开值, 并且 $m \neq m'$.

水银隐藏. 没有 PPT 敌手可以区分 $(m, \text{HCom}_{pk}(m; r), \text{SOpen}_{pk}(m, H; r))$ 和 $(m, \text{SCom}_{pk}(\cdot; r), \text{SOpen}_{pk}(m, S; r))$.

关于水银承诺的最小假设问题以及方案具体构造请参见文献[1-2].

4 普适复合安全框架

在文献[5, 7-8]中, Canetti 等提出普适复合安全性的基本框架. 为了判断一个给定协议是否能够普适复合地安全实现某个密码学任务, 他们首先定义了理想函数, 理想函数体现并抽象出协议要完成的功能, 之后证明给定协议是否能够安全实现这一理想功能. 实际协议 Π 的执行在 n 个参与方 P_1, P_2, \dots, P_n , 敌手 \mathcal{A} 以及环境机 \mathcal{Z} 之间进行. 环境机 \mathcal{Z} 首先被激活, 生成 n 个参与方 P_1, P_2, \dots, P_n 的输入. 敌手 \mathcal{A} 控制通信信道, 在参与方 P_1, P_2, \dots, P_n 以及环境机之间进行消息传递. 用随机变量 $\text{REAL}_{\Pi, \mathcal{A}, \mathcal{Z}}$ 表示环境机 \mathcal{Z} 与敌手 \mathcal{A} 和执行 Π 的参与方交互之后的输出. 理想过程由 n 个虚构参与方 P_1, P_2, \dots, P_n , 理想函数 \mathcal{F} , 攻击理想模型的敌手 \mathcal{S} 以及环境机 \mathcal{Z} 组成. 当某个虚构参与方 P_i 被激活, 则 P_i 向理想函数 \mathcal{F} 提交输入, 并等待 \mathcal{F} 发回的输出. 用随机变量 $\text{IDEAL}_{\mathcal{F}, \mathcal{S}, \mathcal{Z}}$ 表示环境机 \mathcal{Z} 与理想模型敌手 \mathcal{S} 和理想函数 \mathcal{F} 在理想模型中交互的结果. 称协议 Π 普适复合安全实现某个理想函数 \mathcal{F} , 如果对任意敌手 \mathcal{A} , 都存在一个理想模型敌手 \mathcal{S} , 使得对于任意环境机 \mathcal{Z} , 随机变量 $\text{REAL}_{\Pi, \mathcal{A}, \mathcal{Z}}$ 和 $\text{IDEAL}_{\mathcal{F}, \mathcal{S}, \mathcal{Z}}$ 是计算不可区分的. 普适复合安全结构中的复合定理在文献[5]中给出证明. 考察在混合模型中运行的协议 Π , 所谓混合模型是指参与方如实际协议中通信, 但是某些子协议的调用被替换成对于理想函数的调用. 如果调用的理想函数是 \mathcal{F} , 则这种混合模型记为“ \mathcal{F} -混合模型”. 复合定理是: 令 ρ 是在“ \mathcal{G} -混合模型”中安全实现 \mathcal{F} 的协议, 那么在“ \mathcal{G} -混合模型”中运行的复合协议 Π^ρ 与在“ \mathcal{F} -混合模型”中运行的协议 Π 效果相同. 本文当中, 关于普适复合水银承诺方案的设计与分析是基于公共参数(common reference string)模型, 因此方案是在“ \mathcal{F}_{CRS} -混合模型”中运行. “ \mathcal{F}_{CRS} -混合模型”的理想函数是 \mathcal{F}_{CRS} , 表示“根据某种给定分布选择一个比特串, 并将这个串发送给所有参与方”. 下述图 1 给出理想函数 \mathcal{F}_{CRS} 的详细描述, 其中 sid 是区分不同 \mathcal{F}_{CRS} 的标志(Session ID).

理想函数 \mathcal{F}_{CRS}

给定分布 D , \mathcal{F}_{CRS} 如下执行:

首次被某个参与方提供的输入 ($value, sid$) 激活, 选择 $d \leftarrow D$;
发送 d 给提供输入的参与方;
之后每次被激活, 将 d 返回给发送消息的参与方.

图 1 CRS 函数

关于普适复合安全性的具体细节, 请参见文献[5, 8].

5 普适复合水银承诺方案

本节我们提出普适复合水银承诺方案, 分为 3 个小节. 在第 5.1 节, 首先提出理想模型中的水银承诺理想函数; 第 5.2 节, 给出普适复合水银承诺方案; 第 5.3 节给出安全性证明, 即证明在第 5.2 节给出的方案安全实现理想模型中的水银承诺理想函数.

5.1 水银承诺理想函数

在本小节, 我们首先提出水银承诺理想函数. 由于每一个水银承诺方案自身即包含两种不同的承诺算法(模糊承诺算法和确定承诺算法), 相应地在理想模型中提出的水银承诺理想函数要求能同时处理多个承诺值(反映在实际协议中表示来自于不同的承诺方案), 用 cid 作为区分不同承诺方案的标志. 函数 \mathcal{F}_{MC} 见图 2. 关于图 2 的说明如下:

确定承诺阶段. \mathcal{F}_{MC} 收到来自于某个参与方 P_i (承诺方) 的消息 ($\text{Hard-Commit}, sid, cid, P_i, P_j, b$). 此处 sid 是用来区分不同理想函数 \mathcal{F}_{MC} 的 Session ID, cid 是在同样一个理想函数 \mathcal{F}_{MC} 中区分不同承诺的标志. P_j 是接收方的身份, $b \in \{0, 1\}$ 是被承诺值. 作为回答, \mathcal{F}_{MC} 通知接收方 P_j 和敌手 S , P_i 对某个比特做了承诺. 注意此时接收方 P_j 和敌手 S 不但不能知道是对哪个比特的承诺, 也不能知道承诺方 P_i 选择的是确定承诺还是模糊承诺. 实际上, \mathcal{F}_{MC} 只是向 P_j 和 S 发送了一个收条, 表示它收到了来自于承诺方 P_i 的一个承诺值, 即发送 ($\text{Receipt}, sid, cid, P_i, P_j$) 给接收方 P_j 和敌手 S .

模糊承诺阶段. \mathcal{F}_{MC} 收到来自于某个参与方 P_i (承诺方) 的消息 ($\text{Soft-Commit}, sid, cid, P_i, P_j$). 注意此处 P_i 发来的消息中没有包含被承诺的比特, 即模糊承诺是不对具体比特做承诺的. 尽管在确定承诺和模糊承诺阶段, \mathcal{F}_{MC} 收到了不同的值, 但是 \mathcal{F}_{MC} 对于接收方 P_j 和敌手 S 的回答是相同的, 即 \mathcal{F}_{MC} 通知接收方 P_j 和敌手 S , P_i 对某个比特做了承诺. 这是实际协议中, 确定承诺和模糊承诺计算不可区分在理想模型中的反映. 因为在实际协议中, 接收方和敌

手根据接收的承诺值, 不能判断是来自于哪一种承诺算法, 因此在理想模型中, 对于确定承诺和模糊承诺, 理想函数给接收方和敌手同样的消息.

模糊公开阶段. 分成两个部分. 如果 \mathcal{F}_{MC} 收到 P_i 发来对某个确定承诺的模糊公开要求, 即发送 ($\text{Soft-Open}, H, sid, cid, P_i, P_j$), 那么 \mathcal{F}_{MC} 检查是否曾经收到过 ($\text{Hard-Commit}, sid, cid, P_i, P_j, b$). 如果曾经收到过, \mathcal{F}_{MC} 发送 ($\text{Soft-Open}, sid, cid, P_i, P_j, b$) 给接收方 P_j 和敌手 S , 否则中止. 这说明对于比特 b 的确定承诺不能模糊公开为不同的比特. 如果 \mathcal{F}_{MC} 收到 P_i 发来对某个模糊承诺的模糊公开要求, 即发送 ($\text{Soft-Open}, S, sid, cid, P_i, P_j, x$) 那么 \mathcal{F}_{MC} 检查是否曾经收到过 ($\text{Soft-Commit}, sid, P_i, P_j$). 如果曾经收到过, \mathcal{F}_{MC} 发送 ($\text{Soft-Open}, sid, cid, P_i, P_j, x$) 给接收方 P_j 和敌手 S , 否则中止. 这说明承诺方 P_i 可以根据自己的意愿随意决定如何模糊公开它的模糊承诺值.

确定公开阶段. 承诺方发送 ($\text{Hard-Open}, sid, cid, P_i, P_j$) 给理想函数 \mathcal{F}_{MC} , \mathcal{F}_{MC} 检查是否曾经收到过 ($\text{Hard-Commit}, sid, cid, P_i, P_j, b$). 如果曾经收到过, \mathcal{F}_{MC} 发送 ($\text{Hard-Open}, sid, cid, P_i, P_j, b$) 给接收方 P_j 和敌手 S , 否则中止.

定义 2. 称一个方案是普适复合水银承诺方案, 如果这个方案能够安全实现理想函数 \mathcal{F}_{MC} .

理想函数 \mathcal{F}_{MC}

\mathcal{F}_{MC} 如下执行, 与 P_1, P_2, \dots, P_n 和理想模型敌手 S 交互.

1. 收到 P_i 发来的消息 ($\text{Hard-Commit}, sid, cid, P_i, P_j, b$), 记录此消息 ($\text{Hard-Commit}, sid, cid, P_i, P_j, b$), 并发送 ($\text{Receipt}, sid, cid, P_i, P_j$) 给 P_j 和敌手 S . 忽略之后的形如 ($\text{Hard-Commit}, sid, cid, P_i, P_j, *$) 的消息.
2. 收到 P_i 发来的消息 ($\text{Soft-Commit}, sid, cid, P_i, P_j$), 记录此消息 ($\text{Soft-Commit}, sid, cid, P_i, P_j$), 并发送 ($\text{Receipt}, sid, cid, P_i, P_j$) 给 P_j 和敌手 S . 忽略之后的形如 ($\text{Soft-Commit}, sid, cid, P_i, P_j$) 的消息.
3. 收到 P_i 发来的消息 ($\text{Soft-Open}, H, sid, cid, P_i, P_j$), 如果消息 ($\text{Hard-Commit}, sid, cid, P_i, P_j, b$) 被记录过, 发送 ($\text{Soft-Open}, sid, cid, P_i, P_j, b$) 给 P_j 和敌手 S . 不然中止; 收到 P_i 发来的消息 ($\text{Soft-Open}, S, sid, cid, P_i, P_j, x$), 如果消息 ($\text{Soft-Commit}, sid, cid, P_i, P_j$) 被记录过, 发送 ($\text{Soft-Open}, sid, cid, P_i, P_j, x$) 给 P_j 和敌手 S . 不然中止.
4. 收到 P_i 发来的消息 ($\text{Hard-Open}, sid, cid, P_i, P_j$), 如果消息 ($\text{Hard-Commit}, sid, cid, P_i, P_j, b$) 被记录过, 发送 ($\text{Hard-Open}, sid, cid, P_i, P_j, b$) 给 P_j 和敌手 S . 不然中止.

图 2 水银承诺理想函数

5.2 普适复合水银承诺方案

本节给出公共参数模型的普适复合水银承诺方案. 注意此处的公共参数要求是可以重复使用的, 即

固定选定的公共参数能够做多次承诺。我们方案的安全性基于参与方擦除特定数据,即在擦除模型中能够抵抗自适应敌手的攻击。

方案用到如下两个基本工具:一个是无爪的陷门置换对,这个概念最早出现在文献[9]中,简言之,对于陷门置换对 (f_0, f_1) ,没有有效算法能够找到一个爪 (r_0, r_1) ,使得 $f_0(r_0) = f_1(r_1)$;另一个是不可区分的抵抗自适应选择密文攻击(IND-CCA2)的加密方案。

我们的普适复合水银承诺方案必须同时满足普适复合性质和水银性质。普适复合性质,本质上意味着二义性和抽取性质。二义性由以下事实保证:首先,并非所有密文都被解密;其次,理想模型中的敌手掌握无爪陷门置换对的陷门。在理想模型中持有加密方案的私钥使得抽取性质成为可能。而由于模糊公开只要求公开被承诺值的部分信息导致水银性质出现。

我们的普适复合水银承诺方案 UCMC 构造如下。

公共参数。 pk_{claw} ——无爪陷门置换对的公钥;
 pk_{ϵ} ——加密方案 Enc 的公钥

确定承诺。 P_i 对 P_j 做关于比特 $b \in \{0, 1\}$ 的确定承诺如下,身份和承诺方案标志分别为 sid 和 cid :
均匀选取 $x_0, x_1, r_0, r_1 \in \{0, 1\}^n$, 计算

$$\text{HCom}(b; x_0, x_1) = (y_0, y_1) = (f_b(x_b), f_{1-b}(x_{1-b})), \\ c_b = \text{Enc}(x_b, r_b), c_{1-b} = \text{Enc}(0^n, r_{1-b}), \text{擦除 } r_1.$$

发送 $(\text{Com}, sid, cid, ((y_0, y_1), c_0, c_1))$ 给 P_j 并记录 $(\text{HCom}, sid, cid, b, x_0, x_1, r_0)$ 。

一旦 P_j 收到来自于 P_i 的消息 $(\text{Com}, sid, cid, ((y_0, y_1), c_0, c_1))$, P_j 输出 $(\text{Receipt}, sid, cid, P_i, P_j)$ 。

模糊承诺。 P_i 对 P_j 做模糊承诺,身份和承诺方案标志分别为 sid 和 cid :

计算 $\text{SCom}(\cdot; x_0, x_1) = (y_0, y_1) = (f_0(x_0), f_0(x_1))$,

$$(c_0, c_1) = (\text{Enc}(x_0, r_0), \text{Enc}(x_1, r_1)).$$

发送 $(\text{Com}, sid, cid, ((y_0, y_1), c_0, c_1))$ 给 P_j 并记录 $(\text{SCom}, sid, cid, x_0, x_1, r_0, r_1)$ 。一旦 P_j 收到来自于 P_i 的消息 $(\text{Com}, sid, cid, ((y_0, y_1), c_0, c_1))$, P_j 输出 $(\text{Receipt}, sid, cid, P_i, P_j)$ 。

模糊公开。 对于 $(\text{HCom}, sid, cid, b, x_0, x_1, r_0)$, 发送 $(\text{Sopen}, sid, cid, b, x_0, r_0)$ 给 P_j 。收到 $(\text{Sopen}, sid, cid, b, x_0, r_0)$, P_j 验证等式 $y_b = f_0(x_0)$ 和 $c_b = \text{Enc}(x_b, r_b)$ 是否成立; 如果等式成立, P_j 输出

$(\text{Sopen}, sid, cid, P_i, P_j, b)$ 。不然中止。

模糊公开。 对于 $(\text{SCom}, sid, cid, x_0, x_1, r_0, r_1)$, 发送 $(\text{Sopen}, sid, cid, b, x_b, r_b)$ 给 P_j 。收到 $(\text{Sopen}, sid, cid, b, x_b, r_b)$, P_j 验证等式 $y_b = f_0(x_b)$ 和 $c_b = \text{Enc}(x_b, r_b)$ 是否成立; 如果等式成立, P_j 输出 $(\text{Sopen}, sid, cid, P_i, P_j, b)$ 。不然中止。

确定公开。 对于 $(\text{HCom}, sid, cid, b, x_0, x_1, r_0)$ 发送 $(\text{Hopen}, sid, cid, b, x_0, x_1, r_0)$ 给 P_j 。收到 $(\text{Hopen}, sid, cid, b, x_0, x_1, r_0)$, P_j 验证等式 $y_b = f_0(x_0)$, $y_{1-b} = f_1(x_1)$ 和 $c_b = \text{Enc}(x_b, r_b)$ 是否成立; 如果等式成立, P_j 输出 $(\text{Hopen}, sid, cid, P_i, P_j, b)$ 。不然中止。

5.3 安全性证明

定理 1. 如果无爪的陷门置换对和不可区分的抵抗自适应选择密文攻击的加密方案存在, 则 5.2 节构造的方案在“ \mathcal{F}_{CRS} -混合模型”中构成普适复合水银承诺方案。

证明。 对于任意攻击实际协议的敌手 \mathcal{A} , 要构造攻击理想模型的敌手 \mathcal{S} , 使得 \mathcal{S} 能够模拟 \mathcal{A} 与参与方之间以及与环境机 \mathcal{Z} 的交互。算法 \mathcal{S} 构造如下:

1. 首先模拟器 \mathcal{S} 根据密钥生成算法生成密钥 $(pk_{\text{claw}}, td_{\text{claw}}) \leftarrow \text{KGen}_{\text{claw}}(1^n)$ 和 $(pk_{\epsilon}, sk_{\epsilon}) \leftarrow \text{KGen}_{\epsilon}(1^n)$, 确定 $(pk_{\text{claw}}, pk_{\epsilon})$ 作为公钥, 保存私钥 $(td_{\text{claw}}, sk_{\epsilon})$ 。注意此时在理想模型中, 公钥 $(pk_{\text{claw}}, pk_{\epsilon})$ 是由 \mathcal{S} 自己产生的, 而不是通过“ \mathcal{F}_{CRS} ”产生, 由于 \mathcal{S} 也是调用与 \mathcal{F}_{CRS} 中一样的密钥生成算法产生的公钥, 因此对于敌手 \mathcal{A} 和环境 \mathcal{Z} , 这两种密钥是计算不可区分的。但是因为理想模型中 \mathcal{S} 掌握私钥, 而使得模拟成为可能。 \mathcal{S} 按照以下步骤模拟敌手 \mathcal{A} 与环境机 \mathcal{Z} 的交互。

2. 如果环境机 \mathcal{Z} 指令某个诚实参与方 P_i 发送承诺值, 则 P_i 发送消息 $(\text{Hard-Commit}, sid, cid, P_i, P_j, b)$ 或者 $(\text{Soft-Commit}, sid, cid, P_i, P_j)$ 给理想函数, 这时模拟算法 \mathcal{S} 收到来自于理想函数的收条 $(\text{Receipt}, sid, cid, P_i, P_j)$ 。即 \mathcal{S} 获知 P_i 给 P_j 发送了一个承诺, 但是不能知道是哪一种承诺算法, 也不能知道被承诺的比特(如果 P_i 采用的是确定承诺算法)。 \mathcal{S} 均匀选取随机串 $x_0, x_1, r_0, r_1 \in \{0, 1\}^n$ 并且计算 $(y_0, y_1) = (f_0(x_0), f_0(x_1))$ 和 $z_0 = f_1^{-1}(y_0)$, $z_1 = f_1^{-1}(y_1)$, 即 $(y_0, y_1) = (f_0(x_0), f_0(x_1)) = (f_1(z_0), f_1(z_1))$; $(c_0, c_1) = (\text{Enc}(x_0, r_0), \text{Enc}(x_1, r_1))$ 。 \mathcal{S} 告知敌手 \mathcal{A} 在实际协议中参与方 P_i 发送消息 $(\text{Com}, sid, cid, ((y_0, y_1), c_0, c_1))$ 给参与方 P_j 。

3. 如果环境机 \mathcal{Z} 指令 P_i 将之前的承诺值模糊公开为比特 b , 则 \mathcal{S} 由理想函数 \mathcal{F}_{MC} 处得到比特 b 。 \mathcal{S} 通过提供 (b, x_b, r_b) 给 \mathcal{A} , 假称之前发送的消息 $(\text{Com}, sid, cid, ((y_0, y_1), c_0, c_1))$ 即为对比特 b 的模糊承诺, 并声称已经擦除另外一个随机串。

4. 如果环境机 \mathcal{Z} 指令 P_i 将之前的承诺值确定公开为比特 b , 则 \mathcal{S} 由理想函数 \mathcal{F}_{MC} 处得到比特 b 。 \mathcal{S} 通过提供 (b, x_b, z_{1-b}, r_b) 给 \mathcal{A} , 假称之前发送的消息 $(\text{Com}, sid, cid, ((y_0, y_1), c_0, c_1))$ 即为对比特 b 的确定承诺, 并声称已经擦除另外一个

随机串。

5. 如果被模拟的敌手 \mathcal{A} 指令某个被入侵方 P_i 发送消息 $(\text{Com}, \text{sid}, \text{cid}, ((y_0^*, y_1^*), c_0^*, c_1^*))$ 给诚实方 P_j , 则 \mathcal{S} 应用自己保存的私钥 sk_e 解密 c_0^* 和 c_1^* . 记为 $\text{Dec}(c_0^*) = m_0^*$, $\text{Dec}(c_1^*) = m_1^*$. \mathcal{S} 比较 (y_0^*, y_1^*) 与 $(f_0(m_0^*), f_0(m_1^*))$: 如果 $y_0^* = f_0(m_0^*)$ 并且 $y_1^* = f_0(m_1^*)$, 那么 \mathcal{S} 判断此时 P_i 发出的承诺是模糊承诺, 并以 P_i 的身份发送 $(\text{Soft-Commit}, \text{sid}, \text{cid}, P_i, P_j)$ 给理想函数 \mathcal{F}_{MC} ; 如果 $y_0^* = f_0(m_0^*)$ 并且 $y_1^* \neq f_0(m_1^*)$, 那么 \mathcal{S} 判断此时 P_i 发出的承诺是对比特 0 的确定承诺, 并以 P_i 的身份发送 $(\text{Hard-Commit}, \text{sid}, \text{cid}, P_i, P_j, 0)$ 给理想函数 \mathcal{F}_{MC} ; 如果 $y_0^* \neq f_0(m_0^*)$ 并且 $y_1^* = f_0(m_1^*)$, 那么 \mathcal{S} 判断此时 P_i 发出的承诺是对比特 1 的确定承诺, 并以 P_i 的身份发送 $(\text{Hard-Commit}, \text{sid}, \text{cid}, P_i, P_j, 1)$ 给理想函数 \mathcal{F}_{MC} . 如以上情形都不成立, \mathcal{S} 忽略此消息。

6. 如果敌手 \mathcal{A} 指令被入侵方 P_i 将承诺值 $(\text{Com}, \text{sid}, \text{cid}^*, ((y_0^*, y_1^*), c_0^*, c_1^*))$ 确定公开为比特 b^* , 则 \mathcal{S} 验证该承诺值是否为确定承诺以及 b^* 是否等于 \mathcal{S} 在第 5 步抽取出的比特 b ; 只要有一个验证等式不成立, \mathcal{S} 忽略此消息. 否则 (即两个验证都成立), \mathcal{S} 以 P_i 的身份发送 $(\text{Hard-open}, \text{sid}, \text{cid}, P_i, P_j, b)$ 给 \mathcal{F}_{MC} .

7. 如果敌手 \mathcal{A} 指令被入侵方 P_i 将承诺值 $(\text{Com}, \text{sid}, \text{cid}^*, ((y_0^*, y_1^*), c_0^*, c_1^*))$ 模糊公开为比特 b^* , 则 \mathcal{S} 首先考察此承诺值是确定承诺还是模糊承诺. 如果是确定承诺, \mathcal{S} 比较比特 b^* 与之前抽取出的比特是否一致, 不一致则忽略此消息; 否则 \mathcal{S} 以 P_i 的身份发送 $(\text{Soft-open}, \text{H}, P_i, P_j, b^*)$ 给 \mathcal{F}_{MC} . 如果是模糊承诺, \mathcal{S} 以 P_i 的身份发送 $(\text{Soft-open}, \text{S}, P_i, P_j, b^*)$ 给 \mathcal{F}_{MC} . 不然 \mathcal{S} 忽略此消息。

8. 只要被模拟的敌手 \mathcal{A} 入侵某个参与方, 则 \mathcal{S} 在理想模型中入侵同样的参与方并获知全部的内部信息. \mathcal{S} 根据获知的内部信息如第 4 步调整其公开信息, 并将调整过的信息交给敌手 \mathcal{A} . 这样敌手 \mathcal{A} 通过 \mathcal{S} 实现了入侵, 并且不能察觉。

为了证明环境机在实际模型中与理想模型中的输出不可区分, 我们考虑如下 3 个随机变量:

$\text{Real}_{\text{Genuine}}$. 环境机 \mathcal{Z} 与执行实际协议的参与方和敌手 \mathcal{A} 交互之后的输出。

$\text{Real}_{\text{Fake}}$. 基本类似于 $\text{Real}_{\text{Genuine}}$, 区别只在于诚实方对比特 b 的确定承诺或者模糊承诺形如 $(y_0, y_1) = (f_0(x_0), f_0(x_1))$ 和 $(c_0, c_1) = (\text{Enc}(x_0, r_0), \text{Enc}(x_1, r_1))$. 对应此承诺值的模糊公开为 (b, x_b, r_b) , 确定公开为 $(b, x_b, f_1^{-1}(y_{1-b}), r_b)$.

$\text{Ideal}_{\text{Fake}}$. 环境机 \mathcal{Z} 与理想模型敌手 \mathcal{S} 和函数 \mathcal{F}_{MC} 在理想模型交互之后的输出。

随机变量 $\text{Real}_{\text{Genuine}}$ 和 $\text{Real}_{\text{Fake}}$ 计算不可区分. 这两个随机变量之间唯一的区别在于诚实方的确定和模糊承诺. 在 $\text{Real}_{\text{Genuine}}$ 中, 诚实方的确定承诺是 $(y_0, y_1) = (f_b(x_b), f_{1-b}(x_{1-b}))$ 和 $c_b = \text{Enc}(x_0)$, $c_{1-b} = \text{Enc}(0^n)$; 在 $\text{Real}_{\text{Fake}}$ 中, 诚实方的确定承诺是 $(y_0, y_1) = (f_0(x_0), f_0(x_1))$, $c_0 = \text{Enc}(x_0)$ 和 $c_1 =$

$\text{Enc}(x_1)$. 由于加密方案是不可区分的抵抗自适应选择密文攻击 (IND-CCA2) 安全的, 这种差别根据密文是不能区分的, 因此这两个随机变量是计算不可区分的。

随机变量 $\text{Real}_{\text{Fake}}$ 和 $\text{Ideal}_{\text{Fake}}$ 计算不可区分. 这两个随机变量之间的区别在于模拟过程中的以下 3 个事实: 分别记为事件 $\mathcal{E}_1, \mathcal{E}_2$ 和 \mathcal{E}_3 .

事件 \mathcal{E}_1 : (1) 在 $\text{Ideal}_{\text{Fake}}$ 中, 被模拟的敌手 \mathcal{A} (以某个被入侵参与方的身份) 生成承诺值 $((y_0^*, y_1^*), c_0^*, c_1^*)$; (2) \mathcal{S} 判断此承诺值是一个模糊承诺; (3) 敌手 \mathcal{A} 将 $((y_0^*, y_1^*), c_0^*, c_1^*)$ 成功地确定公开为 0.

事件 \mathcal{E}_2 : (1) 在 $\text{Ideal}_{\text{Fake}}$ 中, 被模拟的敌手 \mathcal{A} (以某个被入侵参与方的身份) 生成承诺值 $((y_0^*, y_1^*), c_0^*, c_1^*)$; (2) \mathcal{S} 判断此承诺值是一个模糊承诺; (3) 敌手 \mathcal{A} 将 $((y_0^*, y_1^*), c_0^*, c_1^*)$ 成功地确定公开为 1.

事件 \mathcal{E}_3 : (1) 在 $\text{Ideal}_{\text{Fake}}$ 中, 被模拟的敌手 \mathcal{A} (以某个被入侵参与方的身份) 生成承诺值 $((y_0^*, y_1^*), c_0^*, c_1^*)$; (2) \mathcal{S} 判断此承诺值是对 b 的确定承诺; (3) 敌手 \mathcal{A} 将 $((y_0^*, y_1^*), c_0^*, c_1^*)$ 成功地确定公开为 $1-b$.

只要以上 3 个事件 $\mathcal{E}_1, \mathcal{E}_2$ 和 \mathcal{E}_3 不发生, 那么 \mathcal{Z} 在 $\text{Real}_{\text{Fake}}$ 中的输出与在 $\text{Ideal}_{\text{Fake}}$ 中的输出一致。

我们的目标是将这 3 个事件 $\mathcal{E}_1, \mathcal{E}_2$ 和 \mathcal{E}_3 归约到无爪对 (f_0, f_1) 的安全性. 但是直接的归约有困难. 此处我们引入一个新的实验, 记为 $\text{Ideal}'_{\text{Fake}}$. $\text{Ideal}'_{\text{Fake}}$ 与 $\text{Ideal}_{\text{Fake}}$ 的区别只是在于: 在 $\text{Ideal}'_{\text{Fake}}$ 中, (被模拟的) 诚实承诺方不存在, 即在 $\text{Ideal}'_{\text{Fake}}$ 中所有的承诺值都是由敌手生成的. 在实验 $\text{Ideal}'_{\text{Fake}}$ 中, 将被模拟的敌手记为 \mathcal{A}' , 模拟器算法记为 \mathcal{S}' , 并且定义相应的事件 $\mathcal{E}'_1, \mathcal{E}'_2$ 和 \mathcal{E}'_3 如下:

事件 \mathcal{E}'_1 : (1) 在 $\text{Ideal}'_{\text{Fake}}$ 中, 被模拟的敌手 \mathcal{A}' (以某个被入侵参与方的身份) 生成承诺值 $((y_0^*, y_1^*), c_0^*, c_1^*)$; (2) \mathcal{S}' 判断此承诺值是一个模糊承诺; (3) 敌手 \mathcal{A}' 将 $((y_0^*, y_1^*), c_0^*, c_1^*)$ 成功地确定公开为 0.

事件 \mathcal{E}'_2 : (1) 在 $\text{Ideal}'_{\text{Fake}}$ 中, 被模拟的敌手 \mathcal{A}' (以某个被入侵参与方的身份) 生成承诺值 $((y_0^*, y_1^*), c_0^*, c_1^*)$; (2) \mathcal{S}' 判断此承诺值是一个模糊承诺; (3) 敌手 \mathcal{A}' 将 $((y_0^*, y_1^*), c_0^*, c_1^*)$ 成功地确定公开为 1.

事件 \mathcal{E}'_3 : (1) 在 $\text{Ideal}'_{\text{Fake}}$ 中, 被模拟的敌手 \mathcal{A}' (以某个被入侵参与方的身份) 生成承诺值 $((y_0^*, y_1^*), c_0^*, c_1^*)$; (2) \mathcal{S}' 判断此承诺值是对 b 的确定承诺; (3) 敌手 \mathcal{A}' 将 $((y_0^*, y_1^*), c_0^*, c_1^*)$ 成功地确定公开为 $1-b$.

对于以上 3 个事件 $\mathcal{E}_1, \mathcal{E}_2$ 和 \mathcal{E}_3 的归约方法是相同的, 为了简化描述, 我们只就事件 \mathcal{E}_1 给出证明, 即证明事件 \mathcal{E}_1 在 $Ideal_{\text{Fake}}$ 中发生的概率是可忽略的. 证明分成两个引理, 引理 1 中证明, 事件 \mathcal{E}_1 在 $Ideal_{\text{Fake}}$ 中发生的概率与事件 \mathcal{E}'_1 在 $Ideal'_{\text{Fake}}$ 中发生的概率的差别是可忽略的; 引理 2 中证明事件 \mathcal{E}'_1 在 $Ideal'_{\text{Fake}}$ 中发生的概率是可忽略的.

根据这两个引理的结论, 我们可以直接得到期望的结果, 即环境机 \mathcal{Z} 与 $Real_{\text{Fake}}$ 交互之后的输出和 \mathcal{Z} 与 $Ideal_{\text{Fake}}$ 交互之后的输出是计算不可区分的.

在下述引理 1 的证明中, 主要利用加密方案的抵抗选择密文攻击性质. 根据文献[10]中的结论, 语义安全的抵抗自适应选择密文攻击的安全性与不可区分的抵抗自适应选择密文攻击的安全性是等价的, 这里我们应用语义安全性证明引理 1. 语义安全的抵抗自适应选择密文攻击的加密方案如下定义: 敌手给定公钥 pk_e 并产生三元电路组 (M, h, f) . 明文 $x \leftarrow M$ 的密文以及关于明文的部分信息 $h(x)$ 作为挑战密文, 其中 M 是明文的分布, 函数 h 表示明文的先验信息, 函数 f 表示敌手期望获得的关于明文的信息. 敌手的目标是猜测 $f(x)$, 语义安全性意味着敌手的成功概率与只给定 $h(x)$ 和 $1^{|x|}$ 的某个算法(没有给定密文)的成功概率相当.

引理 1. 事件 \mathcal{E}_1 在 $Ideal_{\text{Fake}}$ 中发生的概率与事件 \mathcal{E}'_1 在 $Ideal'_{\text{Fake}}$ 中发生的概率的区别是可忽略的.

证明. 事件 \mathcal{E}_1 发生意味着敌手 \mathcal{A} 生成一个承诺值 $((y_0^*, y_1^*), (c_0^*, c_1^*))$, 使得 $\text{Dec}(c_0^*) = m_0^*$, $\text{Dec}(c_1^*) = m_1^*$, 满足 $y_0^* = f_0(m_0^*)$ 并且 $y_1^* = f_0(m_1^*)$. 这样导致 \mathcal{S} 判断这个承诺值是模糊承诺; 同时 \mathcal{A} 生成的承诺值也满足 $y_0^* = f_0(m_0^*)$ 和 $y_1^* = f_1(m_2^*)$ 使得 \mathcal{A} 确定公开此承诺值为 0. 即 \mathcal{A} 在 $Ideal_{\text{Fake}}$ 中找到爪 (m_1^*, m_2^*) .

利用上述敌手算法 \mathcal{A} , 我们构造算法 \mathcal{D} 如下攻击加密方案的语义安全性:

1. \mathcal{D} 给定安全参数 1^n 和模拟算法 \mathcal{S} 产生的公钥 pk_e ;
2. 算法 \mathcal{D} 输出三元组电路 (M, h, f) , 其中 M 是 $\{0, 1\}^n$, $h = n$ 是明文的长度, $f(x) = \mathcal{A}(1^n, pk_e, \text{Enc}(x))$;
3. 当 \mathcal{S} 模拟某个诚实方 P_i 发送承诺值 $(\text{Com}, \text{sid}, \text{cid}, ((y_0, y_1), c_0, c_1))$, 将密文 c_1 作为挑战密文提交给 \mathcal{D} .
4. 如果被模拟的敌手 \mathcal{A} 以某个被入侵参与方 P_i 的身份发送承诺值 $(\text{Com}, \text{sid}, \text{cid}^*, ((y_0^*, y_1^*), (c_0^*, c_1^*)))$, 则 \mathcal{D} 如下执行:
 - 4.1. 如果挑战密文 c_1 不等于 c_0^* 和 c_1^* 中的某一个, 则 \mathcal{D} 询问解密 oracle, 解密 c_0^* 和 c_1^* . 如果 $y_0^* = f_0(m_0^*)$ 并且 $y_1^* = f_0(m_1^*)$, 则 \mathcal{D} 执行步 5; 否则中止.

4.2. 如果挑战密文 c_1 等于 c_0^* 或 c_1^* 之一, 则 c_0^* 或 c_1^* 一定作为某个诚实方的承诺出现过. 对于那个承诺, 回忆 \mathcal{S} 的行为, 如果 \mathcal{S} 将其(模糊或者确定)公开为 0, 则 \mathcal{D} 中止; 否则即 \mathcal{S} 将其(模糊或者确定)公开为 1, 即满足 $y_1 = f_0(m_1^*) (= y_0^*)$, 则 \mathcal{D} 执行步 5.

5. 如果 \mathcal{A} 将承诺值 $(\text{Com}, \text{sid}, \text{cid}^*, ((y_0^*, y_1^*), (c_0^*, c_1^*)))$ 确定公开为 0, 提供的公开信息中包含 m_0^* 和 m_2^* , 满足 $y_0^* = f_0(m_0^*)$ 和 $y_1^* = f_1(m_2^*)$, 那么 \mathcal{D} 输出 (m_1^*, m_2^*) .

显然, \mathcal{D} 输出 $(m_1^*, m_2^*) = \mathcal{A}(1^n, pk_e, c_{1-b}) = f(x_{1-b})$ 的概率等于事件 \mathcal{E}_1 在 $Ideal_{\text{Fake}}$ 中发生的概率. 由于我们选择的加密方案的语义安全性, 对于算法 \mathcal{D} , 存在算法 \mathcal{D}' 使得对任意正多项式 $p(\cdot)$ 以及充分大的 n , 有 $\Pr[(m_1^*, m_2^*) \leftarrow \mathcal{D}(1^n, pk_e, c_1)] - \Pr[(m_1^*, m_2^*) \leftarrow \mathcal{D}'(1^n)] < \frac{1}{p(n)}$. 根据 \mathcal{D}' 令 $A' = \mathcal{D}'$, 使得 $(m_1^*, m_2^*) \leftarrow A'(1^n)$, 即算法 A' 在没有诚实方提供密文的情形, 能够输出 (m_1^*, m_2^*) , 形成爪, 导致事件 \mathcal{E}'_1 在 $Ideal'_{\text{Fake}}$ 中发生.

$$\begin{aligned} & \Pr[\mathcal{E}_1 \text{ occurs in } Ideal_{\text{Fake}}] \\ &= \Pr[(m_1^*, m_2^*) \leftarrow \mathcal{D}(pk_e, c_1)] \\ &< \Pr[(m_1^*, m_2^*) \leftarrow \mathcal{D}'(1^n)] + \frac{1}{p(n)} \\ &< \Pr[\mathcal{E}'_1 \text{ occurs in } Ideal'_{\text{Fake}}] + \frac{1}{p(n)}. \end{aligned}$$

证毕.

引理 2. 事件 \mathcal{E}'_1 在实验 $Ideal'_{\text{Fake}}$ 中发生的概率是可忽略的.

证明. 事件 \mathcal{E}'_1 在 $Ideal'_{\text{Fake}}$ 中发生意味着, 对于给定的环境机 \mathcal{Z} 和敌手 \mathcal{A}' , \mathcal{A}' 能够提供承诺 $((y_0^*, y_1^*), (c_0^*, c_1^*))$, 并能将其确定公开为 0, 即 \mathcal{A}' 能够在实验 $Ideal'_{\text{Fake}}$ 中找到爪. 构造算法 \mathcal{F} 在无爪对 (f_0, f_1) 中找到爪:

(1) \mathcal{F} 生成 $(pk_e, sk_e) \leftarrow \text{KGen}(1^n)$.

(2) 如果 \mathcal{A}' 提供承诺值 $((y_0^*, y_1^*), (c_0^*, c_1^*))$, 则 \mathcal{F} 应用它自己产生的私钥 sk_e 将 (c_0^*, c_1^*) 解密为 (m_0^*, m_1^*) , 若 $y_0^* = f_0(m_0^*)$ 和 $y_1^* = f_0(m_1^*)$ 那么 \mathcal{F} 存储 m_1^* , 不然中止.

(3) 如果 \mathcal{A}' 成功提交 m_2^* 使得承诺值 $((y_0^*, y_1^*), (c_0^*, c_1^*))$ 确定公开为 0, 那么一定有等式 $y_1^* = f_1(m_2^*)$ 成立. \mathcal{F} 输出 (m_1^*, m_2^*) .

$$\begin{aligned} & \Pr[\mathcal{E}'_1 \text{ occurs in } Ideal'_{\text{Fake}}] \\ &= \Pr[\mathcal{F} \text{ finds claw } (m_1^*, m_2^*) \text{ in claw-free pair } (f_0, f_1)] \\ &< \frac{1}{p(n)}. \end{aligned}$$

证毕.

6 结 论

在 Internet 这样开放的网络环境中, 普适复合安全性框架是设计和分析协议的强有力工具. 这是因为它处理的是最一般的情形, 比如是异步通信, 容忍自适应攻击, 可以并发等等. 对于新的密码学原语, 提出其普适复合的实现方式是重要的研究方向之一. 本文提出了普适复合水银承诺方案的一种构造方案, 接下来的工作重点在于构造基于一般假设的普适复合方案, 以及探索在密码学其它领域中的应用.

参 考 文 献

- [1] Chase M et al. Mercurial commitment with applications to zero-knowledge sets//Proceedings of the EUROCRYPT'05. Aarhus, Denmark, 2005; 422-439
- [2] Catalano D, Dodis Y, Visconti I. Mercurial commitments: Minimal assumptions and efficient constructions//Proceedings of the TCC 2006. New York, USA, 2006; 120-144



XU Hai-Xia, born in 1973, Ph. D., associate professor. Her research interests include cryptology, information security.

Background

This work is supported by the National Natural Science Foundation of China under grant No. 60673073, National High Technology Research and Development Program (863 Program) of China under Grant No. 2006AA01Z427, National Basic Research Program of China (973 Program) of China under grant Nos. 2007CB311201, 2007CB311202 and Foundation of Graduate University of Chinese Academy of Sciences (065001G).

The notion of commitment scheme is one of the most important primitives in cryptography. A commitment scheme must be hiding and binding. Mercurial commitments, proposed by Chase et al., are an interesting variation of regular commitments. Compared to the conventional commitment schemes, the mercurial commitment schemes admit a relaxation of the binding property. Mercurial commitments change the regular open phase into a two-stage opening protocol.

- [3] Micali S, Rabin M, Kilian J. Zero-knowledge sets//Proceedings of the 44th FOCS. Cambridge, MA, USA, 2003; 80-91
- [4] Gennaro R, Micali S. Independent zero-knowledge Sets//Proceedings of the ICALP 2006. Venice, Italy, 2006; 34-45
- [5] Canetti R. Universally composable security: A new paradigm for cryptographic protocols//Proceedings of the 42nd FOCS. Las Vegas, Nevada, 2001; 136-145
- [6] Goldreich O, Micali S, Wigderson A. How to play any mental game or a completeness theorem for protocols with honest majority//Proceedings of the 19th Symposium on the Theory of Computing. New York, USA, 1987; 218-229
- [7] Canetti R, Fischlin M. Universally composable commitments//Proceedings of the CRYPTO'01. California, USA, 2001; 19-40
- [8] Canetti R, Lindell Y, Oatrovsky R, Sahai A. Universally composable two-party and multi-party secure computation//Proceedings of the STOC 2002. Québec, Canada, 2002; 494-503
- [9] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 1988, 17(2): 281-308
- [10] Goldreich O. Foundations of Cryptography (Volume 2, Basic Applications). Cambridge, UK: Cambridge University Press, 2004

LI Hong-Da, born in 1966, Ph. D., associate professor. Her research interests include cryptology, information security.

LI Bao, born in 1962, Ph. D., professor, Ph. D. supervisor. His research interests include cryptology, information.

One is the soft-open stage which is not binding but cannot conflict with the true decommitment. The other is the hard-open stage which is the same as the open stage in an usual commitment scheme.

The universal composability framework, presented by Canetti, inherits the ideal-process vs. real-world method initiated by Goldreich et al, but ensures stronger security properties such as concurrent composition, adaptive security, non-malleability, etc. In this paper, the authors present a universally composable mercurial commitment scheme based on the assumption of existence of claw-free trapdoor permutations and an semantic security encryption scheme under adaptive chosen ciphertext attacks. The authors show that their scheme securely realizes an ideal mercurial commitment functionality in the common reference string (CRS) model.