软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(2):884−898 [doi: 10.13328/j.cnki.jos.006423]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

适应性安全的离线证据加密*

刘牧华[1,2], 王 琳[1], 朱军龙[1], 邢 玲[1], 张明川[1], 吴庆涛[1]

[1](河南科技大学 信息工程学院, 河南 洛阳 471023)

[2](河南科技大学 数学与统计学院, 河南 洛阳 471023)

通信作者: 吴庆涛, E-mail: wqt8921@haust.edu.cn

摘 要: 离线证据加密通过将复杂的计算移到初始化算法提升加密算法的效率, 相比证据加密具有更广泛的应用. 然而, 已有的离线证据加密方案大多满足选择安全性, 即敌手在得到公共参数之前必须输出一对挑战明文(m_0,m_1)和一个命题实例x. Chvojka 等人通过引入可穿孔加密构造了半适应安全的离线证据加密方案, 该安全性允许敌手适应性选择挑战密文, 但是敌手得到公共参数(pp_e,pp_d)之前需要输出挑战密文对应的命题实例x, 将构造完全适应安全的离线证据加密方案作为"Open Problem"提了出来. 首次构造了满足完全适应安全的离线证据加密方案. 初始化算法输出一对公共参数(pp_e,pp_d), 其中加密密钥pp_e包含两个公钥, 一个公共参考串和一个承诺, 解密密钥pp_d是一个混淆电路. 该算法只需运行一次, 公共参数可以使用任意多次. 加密算法利用密钥封装机制和证据不可区分证明系统构造一个 Naor-Yung 形式的密文. 通过提前选定封装的密钥解决在选择安全性中敌手需要提前输出挑战明文的问题. 另外, 所提构造可以直接转化为适应性安全的离线函数证据加密, 密钥生成阶段将函数f嵌入到解密私钥中, 可以实现针对函数f解密私钥的可重复使用.

关键词: 适应性安全; 密钥封装机制; 公钥加密; 不可区分的混淆; 承诺方案

中图法分类号: TP309

中文引用格式: 刘牧华, 王琳, 朱军龙, 邢玲, 张明川, 吴庆涛. 适应性安全的离线证据加密. 软件学报, 2023, 34(2): 884–898. http://www.jos.org.cn/1000-9825/6423.htm

英文引用格式: Liu MH, Wang L, Zhu JL, Xing L, Zhang MC, Wu QT. Offline Witness Encryption with Fully Adaptive Security. Ruan Jian Xue Bao/Journal of Software, 2023, 34(2): 884–898 (in Chinese). http://www.jos.org.cn/1000-9825/6423.htm

Offline Witness Encryption with Fully Adaptive Security

LIU Mu-Hua[1,2], WANG Lin[1], ZHU Jun-Long[1], XING Ling[1], ZHANG Ming-Chuan[1], WU Qing-Tao[1]

[1](School of Information Engineering, Henan University of Science and Technology, Luoyang 471023, China)

[2](School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang 471023, China)

Abstract: Compared with witness encryption, offline witness encryption is more extensive in the practical applications because of its high-efficiency by transferring the hard computation work to setup phase. However, most of the current offline witness encryption schemes only satisfy the selective security, that is, the adversary must commit a pair of challenge messages (m_0, m_1) and an instance x before obtaining the public parameters. Chvojka *et al*. proposed an offline witness encryption construction that achieves semi-adaptive security by introducing the puncturable encryption. The semi-adaptive security permits the adversary to choose challenge messages adaptively. However, the instance of the considered NP language that is used to create the challenge ciphertext must be fixed before the adversary gets the public parameters (pp_e, pp_d). Therefore, they leave it as an open problem to construct offline witness encryption schemes with fully adaptive security. This study firstly proposes an offline witness encryption scheme that achieves the fully adaptive security. The setup

* 基金项目: 国家自然科学基金 (61871430, 61971458); 中原科技创新领军人才 (214200510012); 河南省高校科技创新团队 (20IRTSTHN018, 21IRTSTHN015) ; 河南省高校基础研究专项 (19zx010)
收稿时间: 2021-04-27; 修改时间: 2021-06-27, 2021-07-05; 采用时间: 2021-08-02; jos 在线出版时间: 2022-03-24
CNKI 网络首发时间: 2022-11-15

algorithm outputs public parameters (pp_e, pp_d), where pp_e, the encryption key, contains two public keys, a common reference, and a commitment, and the decryption key pp_d is an obfuscated circuit. This algorithm needs to be run only once, and the parameters can be used for arbitrary many encryptions. The encryption algorithm outputs a Naor-Yung's ciphertext by using key encapsulation mechanism and non-interactive witness indistinguishable proofs system. The problem of outputting the challenge plaintext in advance during the proving process of selective security have solved by selecting the encapsulation key in advance. In addition, the proposed scheme can also be turned into a functional offline witness encryption scheme directly to realize the reuse of the decryption key for the function f by embedding f into the decryption key in the key generation phase.

Key words: fully adaptive security; key encapsulated mechanism; public key encryption; indistinguishability obfuscation; commitment

传统加密方案仅能提供"all-or-nothing"的隐私数据访问模式, 即加密数据可以被私钥的拥有者解密获得明文, 而其他人从密文中不能获得明文的任何信息. 之后, 出现了许多支持细粒度访问控制的加密方案, 例如基于特征加密[1,2], 基于属性加密[3,4], 谓词加密[5,6], 函数加密[7−9]等. Garg 等人[10]利用具有证据关系 $\mathcal{R}:\mathcal{L}=\{\exists w:\mathcal{R}(x,w)=1\}$ 的 NP 语言 $\mathcal{L}$ 提出了证据加密概念. 和传统加密方案不同, 证据加密的加密算法除了输入公钥 pp 和明文消息 m 之外, 还需要输入一个命题实例 x, 然后输出一个密文 CT. 任何人拥有 $x\in\mathcal{L}$ 的证据 w, 可以解密密文 CT 得到明文 m. 在证据加密中, 只有当命题实例 $x\in\mathcal{L}$, 密文 CT 才可以被解密. 如果加密消息 m 用到的命题实例 $x\notin\mathcal{L}$, 任何人不能解密密文 CT. 证据加密可以用来构造特征加密, 属性加密和基于口令的加密[11]. 除此之外, 证据加密还存在一些实际的应用, 例如, 加密者可以使用谜题加密明文 m, 使得只有能解出谜题的人得到明文, 该谜题可以是数学难题, 纵横字谜, 数独或者一些数学假设的证明等.

Garg 等人[10]利用多线性映射构造了证据加密方案, 然而该方案的加密算法效率较低, 使得一些计算能力受限的设备很难完成加密运算. Abusalah 等人[12]针对该问题提出了离线证据加密模型. 该模型通过将整个复杂运算过程移到初始化算法减少加密算法的计算量, 它包含 3 个算法: 初始化算法, 加密算法和解密算法. 初始化算法输入安全参数 λ, 输出一对公共参数 $(pp_e,pp_d)\leftarrow Setup\left(1^{\lambda}\right)$; 加密算法输入明文消息 m 和命题实例 x, 输出密文 $CT\leftarrow Enc(1^{\lambda},x,m,pp_e)$; 解密算法输入密文 CT 和对应的证据 w, 如果 $\mathcal{R}(x,w)=1$, 输出解密结果 $m\leftarrow Dec(CT,w,pp_d)$. 初始化算法可以由可信第三方运行, 一旦生成公共参数, 可以使用任意多次. 离线证据加密适用于任何证据加密的场景, 同时, 文献 [12] 给出了一个具体的应用, 利用密文的威慑手段解决一些实际问题. 例如, 数据拥有者允许订阅者通过设置口令访问相关信息. 数据拥有者通常存储口令的哈希值, 为了阻止订阅者分发他们的口令给其他用户, 数据拥有者可以用口令的哈希值加密订阅者的敏感信息并公布密文. 任何人得到口令可以解密密文从而得到订阅者的敏感信息, 因此, 订阅者为了自己的利益必须保管好口令.

Abusalah 等人[12]通过不可区分混淆和非交互零知识证明系统构造了离线证据加密方案. 然而, 该方案只满足选择不可区分安全性, 即敌手在得到公共信息 (pp_e,pp_d) 前需要输出挑战密文 (m_0,m_1) 和命题实例 x. Pal 等人[13]利用可抽取的证据伪随机函数和随机编码构造了离线证据加密方案, 他们的方案也仅满足选择安全性. Chvojka 等人[14]通过引入可穿孔加密 (puncturable encryption) 构造了半适应安全的离线证据加密方案, 该安全性允许敌手适应性选择挑战密文, 但是敌手得到公共参数 (pp_e,pp_d) 之前需要输出挑战密文对应的命题实例 x, 他们将构造完全适应安全 (fully-adaptive security) 的离线证据加密方案作为"Open Problem"提了出来.

在本文中, 我们的目标是构造完全适应安全的离线证据加密方案. 我们采用 Naor-Yung 双重加密机制, 结合非交互证据不可区分证明系统和不可区分的混淆构造离线证据加密. 在初始化算法中, 首先利用公钥加密方案生成两对公私钥 (pk_1,sk_1) 和 (pk_2,sk_2), 然后分别加密 (x,m) 得到密文 (CT_1,CT_2). 为了保证 CT_1 和 CT_2 是同一个消息的密文, 利用非交互证据不可区分证明系统生成一个证明 π, 证明系统的实例 y 包含两部分: 第 1 部分为 CT_1 和 CT_2 是同一个消息的密文, 对应真实的证据 w_{real}; 第 2 个部分是 C 为密文 $CT_1|CT_2$ 的承诺, 对应一个陷门证据 w_{trap}. 设置加密密钥 $pp_e=(pk_1,pk_2,crs,C)$, 其中 crs 为非交互证据不可区分证明的公共参考串, C 为两个密文长度的 0 串承诺, 利用私钥 sk_1 和不可区分的混淆构造解密密钥 pp_d. 然而, 这种构造只满足选择安全性, 主要原因是在证明阶段需要提前生成挑战密文的承诺, 然后利用陷门证据产生的证明 π 通过证明系统的验证算法, 因此, 敌手需提前输出挑战明文.

为解决这个问题, 我们利用密钥封装机制修改上述构造. 在加密阶段, 首先选取一个对称加密密钥 k, 利用

Naor-Yung 双重加密机制生成密钥 k 的两个密文 (CT_1, CT_2), 并使用密钥 k 加密明文信息 (x,m) 得到新的密文 CT_3. 明文消息 (x,m) 的密文包含 5 部分 $(CT_1, CT_2, CT_3, \pi, x)$, 其中 π 用来证明 CT_1 和 CT_2 是同一个消息的密文. 因为对称加密密钥 k 是从密钥空间中随机选取的, 因此在适应安全性证明过程中, 可以提前选定对称加密的私钥 k^*, 并生成公钥中的承诺 C. 一旦敌手输出挑战明文, 直接使用私钥加密 k^* 并生成挑战密文 CT_3^*. 在证明过程中, 可以使用陷门证据产生的证明 π 通过证明系统的验证算法, 从而实现适应性不可区分的安全性.

另外, 我们利用相同的方法构造了适应性安全的离线函数证据加密方案. Boyle 等人[15]首次提出了函数证据加密方案, 加密算法中除了输入命题 x 和消息 m, 还需输入电路 f. 任何人拥有 $x \in \mathcal{L}$ 的证据 w 都可以解密密文得到函数值 $f(m,w)$, 但不能得到消息 m 的其他任何信息. 不可区分的安全性要求: 如果 $f_0(m_0,w) = f_1(m_1,w)$, 即便 $x \in \mathcal{L}$, 对所有的证据 w, 使得 $\mathcal{R}(x,w) = 1$ 成立, (x,m_0) 和 (x,m_1) 的密文是计算不可区分的. 已有的函数证据加密方案[12,13,15]仅满足选择安全性. 本文, 我们利用不可区分的混淆构造函数 f 的解密密钥, 输入密文 $CT = (CT_1, CT_2, CT_3, \pi, x)$, 如果通过非交互证据不可区分验证算法, 则输出函数值 $f(m,w)$. 在本文方案中, 针对函数 f 的解密密钥可以重复使用, 适应性不可区分安全性的证明方法和离线证据加密类似.

1 相关研究

Boneh 等人[10]首先提出了模拟安全的函数加密定义, 并给出了如何将已有的相关概念映射到该形式化功能加密, 并给出了几个公开问题. Garg 等人[16]首次提出了支持多项式规模电路的函数加密方案. Goldwasser 等人[17]针对任何多项式时间可计算的函数给出了简洁的函数加密构造, 在该方案中, 密文的大小不会随着电路规模的增长而变大, 然而他们的方案仅满足选择安全性. Ananth 等人[18]证明了不增加任何假设前提下, 可以将任何选择安全的函数加密转换为适应性安全. Abdalla 等人[19]基于标准假设提出了第一个内积函数加密方案, 他们的方案仅被证明满足选择安全性. Agrawal 等人[20]利用哈希证明系统给出了满足适应安全性的内积函数加密方案.

Goldwasser 等人[21]引入了多输入函数加密模型, 该模型将通用函数加密的场景扩展到了具有多个输入的函数族, 即在多输入函数加密的解密算法输入解密私钥 sk_f 和密文 $(CT_1, CT_2, \ldots, CT_n)$, 输出函数值 $f(m_1, m_2, \ldots, m_n)$. Ananth 等人[22]利用通用公钥函数加密构造了满足选择安全性的多输入函数加密. Brakerski 等人[23]在不增加任何假设的前提下, 利用通用单输入对称函数加密构造了多输入对称函数加密方案, 并在标准模型下证明了适应安全性. Abdalla 等人[24]基于素数阶双线性群上的 k-Lin 假设构造了多输入的内积函数加密. Datta 等人[25]首次提出了实际高效的多输入对称内积函数加密方案, 他们的方案在标准 k-Lin 假设下可以达到完全隐藏安全性.

Garg 等人[26]证明了通用差异输入的混淆 (general-purpose differing-inputs obfuscation) 表明了具有辅助输入的可抽取证据加密. Zhandry[27]利用证据伪随机函数及子集求和编码方案构造了可重复使用的证据加密, 它本质上和离线证据加密的定义是相同的. 在初始化算法中同样生成一对密钥用于加密和解密算法, 但是他们的方案不能直接扩展为函数证据加密. 相比于我们的构造, 文献 [27] 中密文的长度更短. 然而, 子集求和编码是通过多线性映射实例化得到的, 加密阶段它需要计算一个层数与描述 NP 关系 $\mathcal{R}$ 的电路门个数呈线性关系的多线性映射, 加密算法与输入的长度相关, 因此效率较低. 在我们的构造中加密算法需要计算两次公钥加密, 一次对称加密和一个非交互证据不可区分的证明, 算法的时间复杂度不依赖于明文和命题实例的 x 长度, 具有更高的效率, 同时我们的方案可以直接扩展为完全适应性安全的离线函数证据加密.

2 预备知识

定义 $\lambda \in \mathbb{N}$ 为安全参数, 若对所有的多项式 $poly(\lambda)$ 和任意大的 λ, $|negl(\lambda)| < 1/poly(\lambda)$ 成立, 则称 $negl(\lambda)$ 是可忽略函数. 定义 $x|y$ 为字符串 x 和 y 的连接. 假设读者熟悉公钥加密和对称加密方案, 定义 CPA 为选择明文攻击安全性, 这里我们省略公钥加密和对称加密方案相关定义的具体描述. 下面给出不可区分的混淆, 非交互证据不可区分证明, 完美绑定承诺方案的具体定义.

2.1 不可区分的混淆

Garg 等人[16]针对电路类 $P/poly$ 给出了第一个不可区分混淆 $i\mathcal{O}$ 的构造, 以下给出正式定义的描述:

定义 1. 不可区分的混淆. 如果电路族$\{\mathcal{C}_\lambda\}$满足下述条件, 则称$i\mathcal{O}$为不可区分的混淆:

● 正确性. 对所有安全参数$\lambda\in\mathbb{N}$, 电路$C\in\mathcal{C}_\lambda$, 和所有的输入$x\in\{0,1\}^\lambda$, 有下式成立:

$$\Pr[C'(x)=C(x):C'\leftarrow i\mathcal{O}(\lambda,C)]=1.$$

● 不可区分性. 对任意的概率多项式时间的区分器$\mathcal{D}$, 存在可忽略函数$negl(\lambda)$, 满足要求: 对任意安全参数$\lambda\in\mathbb{N}$, 任意电路$C_0,C_1\in\mathcal{C}_\lambda$使得$\forall x\in\{0,1\}^\lambda, C_0(x)=C_1(x)$, 下式成立:

$$|\Pr[\mathcal{D}(i\mathcal{O}(\lambda,C_0))=1]-\Pr[\mathcal{D}(i\mathcal{O}(\lambda,C_1))=1]|\leqslant negl(\lambda).$$

Jain 等人[28]基于 learning with errors (LWE) 假设, learning party with noise 假设, boolean pseudo-random generator 的存在性和 symmetric external Diffie-Hellman (SXDH) 假设证明了存在针对所有多项式电路的不可区分的混淆.

2.2 非交互证据不可区分证明

在本节, 我们描述非交互证据不可区分证明 (non-interactive witness indistinguishable proofs, *NIWI*) 的定义[29]. 证明系统的可靠性需抵抗具有无限计算能力的恶意证明者的攻击.

定义 2. 非交互证据不可区分证明. 针对具有关系$\mathcal{R}$的 NP 语言$\mathcal{L}$, 非交互证据不可区分证明系统包含 3 个概率多项式时间算法$NIWI=(NIWI.Setup,NIWI.P,NIWI.V)$, 满足下面的性质:

● 完美完备性. 对任意的$(x,w)\in\mathcal{R}$,下式成立:

$$\Pr[NIWI.V(crs,x,NIWI.P(crs,x,w))=1]=1,$$

其中, $crs\leftarrow NIWI.Setup(1^\lambda)$, 概率取自$NIWI.Setup,NIWI.P,NIWI.V$这 3 个算法的随机性.

● 统计可靠性. 对任意的敌手$\mathcal{A}$, 存在可忽略函数$negl(\lambda)$, 使得下式成立:

$$\Pr[NIWI.V(crs,x,\pi)=1\wedge x\notin\mathcal{L}|crs\leftarrow NIWI.Setup(1^\lambda);(x,\pi)\leftarrow\mathcal{A}(crs)]=negl(\lambda).$$

● 证据不可区分性. 对任意的概率多项式时间敌手$\mathcal{A}$, 若三元组(x,w_0,w_1)满足$(x,w_0)\in\mathcal{R}$, $(x,w_1)\in\mathcal{R}$, 则分布$\{crs,NIWI.P(crs,x,w_0)\}$和$\{crs,NIWI.P(crs,x,w_1)\}$是计算不可区分的, 其中$crs\leftarrow NIWI.Setup(1^\lambda)$.

2.3 标准承诺方案

定义 3. 标准承诺方案. 标准承诺方案Com(standard commitment schemes) 是一个概率多项式时间的算法, 输入x和一个随机串r, 输出承诺值$C\leftarrow Com(x;r)$. 完美绑定的承诺方案应满足以下两条性质:

● 完美绑定性. 该性质要求任意两个不同的输入不会有相同的承诺值. 具体的, $\forall x_1\neq x_2$和r_1,r_2, $Com(x_1;r_1)\neq Com(x_2;r_2)$.

● 计算隐藏性. 对任意概率多项式时间敌手$\mathcal{A}$, 和所有的x_0,x_1, 满足$|x_0|=|x_1|$, 存在可忽略函数$negl(\lambda)$, 使得下式成立:

$$|\Pr[.\mathcal{A}(Com(x_0))=1]-\Pr[.\mathcal{A}(Com(x_1))=1]|\leqslant negl(\lambda).$$

3 离线证据加密

3.1 离线证据加密定义

离线证据加密方案包含 3 个算法$OWE=(Setup,Enc,Dec)$: 输入安全参数1^λ, 初始化算法$Setup$输出一对密钥(pp_e,pp_d); 加密算法Enc输入安全参数1^λ, NP 实例x和明文消息1^λ, 输出密文CT; 解密算法Dec输入密文CT, 对应 NP 实例$x\in\mathcal{X}$的证据w和解密密钥pp_d, 输出解密结果. 我们沿用 Bellare 等人[11]提出的证据加密定义, 具体描述如下:

定义 4. 离线证据加密. 针对具有证据关系$\mathcal{R}:\mathcal{X}\times\mathcal{W}\to\{0,1\}$的 NP 语言$\mathcal{L}\in NP$, 离线证据加密方案包含 3 个概率多项式时间的算法$(Setup,Enc,Dec)$:

● 初始化算法. $Setup\left(1^\lambda\right)\to(pp_e,pp_d)$: 输入安全参数$1^\lambda$, 初始化算法输出一对密钥$(pp_e,pp_d)$, pp_e用于加密, pp_d用于解密;

● 加密算法. $Enc\left(1^{\lambda},x,m,pp_e\right)\to CT$: 输入安全参数 1^{λ}, 命题 $x\in\mathcal{X}$, 明文消息 $m\in\mathcal{M}$, 加密密钥 pp_e, 加密算法输出密文 CT;

● 解密算法. $Dec(CT,w,pp_d)\to m\ or\ \perp$: 输入密文 CT, 证据 $w\in\mathcal{W}$ 和解密密钥 pp_d, 解密算法输出 $m\in\mathcal{M}\cup\{\perp\}$.

离线证据加密应满足正确性和安全性, 定义如下.

定义 5. 正确性. 对所有的 $\lambda\in\mathbb{N}$, $(x,w)\in\mathcal{X}\times\mathcal{W}$, 使得 $\mathcal{R}(x,w)=1$, $m\in\mathcal{M}$, 下式成立:

$$\Pr\left[(pp_e,pp_d)\leftarrow Setup\left(1^{\lambda}\right),CT\leftarrow Enc\left(1^{\lambda},x,m,pp_e\right):Dec(CT,w,pp_d)\to m\right]=1.$$

定义 6. 适应性不可区分安全性. 针对具有证据关系 $\mathcal{R}$ 的语言 $\mathcal{L}\in NP$, 任意敌手 $\mathcal{A}$ 对于离线证据加密方案 $OWE=(Setup,Enc,Dec)$ 进行适应性安全攻击的实验定义如下. 对于任意 $b\in\{0,1\}$, 实验 $Expt^{adp-b}_{\mathcal{L},\mathcal{A},OWE}(\cdot)$ 输入 1^{λ}.

(1) 挑战者利用初始化算法生成一对密钥 $(pp_e,pp_d)\leftarrow Setup\left(1^{\lambda}\right)$, 并发送给敌手 $\mathcal{A}$.

(2) 敌手得到密钥 (pp_e,pp_d) 后, 输出一个命题 x 和一对等长消息 (m_0,m_1), 使得 $|m_0|=|m_1|$.

(3) 挑战者加密消息 (x,m_b) 得到密文 $CT^*\leftarrow Enc\left(1^{\lambda},x,m_b,pp_e\right)$.

(4) 敌手 $\mathcal{A}$ 得到密文 CT^*, 输出一个比特 $b'\in\{0,1\}$. 如果 $x\in\mathcal{L}$, 则实验输出 0, 否则实验输出 b'.

对于语言 $\mathcal{L}\in NP$ 的离线证据加密方案 $OWE=(Setup,Enc,Dec)$, 如果任何概率多项式时间敌手 $\mathcal{A}$ 在上述实验 $Expt^{adp-b}_{\mathcal{L},\mathcal{A},OWE}(\cdot)$ 中成功的优势 $Adv^{adp-b}_{\mathcal{L},\mathcal{A},OWE}\left(1^{\lambda}\right)$ 是可忽略的, 即存在可忽略函数 $negl(\lambda)$, 使得下式成立:

$$Adv^{adp-b}_{\mathcal{L},\mathcal{A},OWE}\left(1^{\lambda}\right)=\left|\Pr\left[Expt^{adp-0}_{\mathcal{L},\mathcal{A},OWE}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt^{adp-1}_{\mathcal{L},\mathcal{A},OWE}\left(1^{\lambda}\right)=1\right]\right|\leqslant negl(\lambda),$$

则称 OWE 具有适应性不可区分安全性.

3.2 离线证据加密构造

定义 $PKE=(PKE.Gen,PKE.Enc,PKE.Dec)$ 为一个公钥加密方案, Com 为承诺方案, $NIWI=(NIWI.Setup,NIWI.P,NIWI.V)$ 为非交互证据不可区分证明系统, $i\mathcal{O}$ 为不可区分的混淆, $SE=(SE.Enc,SE.Dec)$ 为对称加密方案, 令 $len_c=len_c\left(1^{\lambda}\right)$ 为公钥加密密文的长度, 定义参数 $len=2\cdot len_c$. 对称加密需满足如下性质:

$$\Pr\left[(k_0,k_1)\leftarrow\{0,1\}^{\ell_{SE}},k_0\neq k_1,CT\leftarrow SE.Enc(k_0,m):SE.Dec(k_1,CT)=m\right]\leqslant negl(\lambda),$$

其中, $\{0,1\}^{\ell_{SE}}$ 为对称加密的密钥空间, $negl(\lambda)$ 为可忽略函数.

构造离线证据加密方案如下.

● 初始化算法. $Setup\left(1^{\lambda}\right)\to(pp_e,pp_d)$: 输入安全参数 1^{λ}.

(1) 运行公钥加密密钥生成算法得到两对密钥: $(pk_1,sk_1)\leftarrow PKE.Gen\left(1^{\lambda}\right)$ 和 $(pk_2,sk_2)\leftarrow PKE.Gen\left(1^{\lambda}\right)$;

(2) 利用证据不可区分证明系统初始化算法生成公共参考串 $crs\leftarrow NIWI.Setup\left(1^{\lambda}\right)$;

(3) 计算承诺 $C\leftarrow Com\left(0^{len}\right)$;

(4) 计算 $\tilde{\mathcal{G}}=i\mathcal{O}(\mathcal{G})$, 其中 $\mathcal{G}$ 定义如图 1 所示.

(5) 设置 $pp_e=(pk_1,pk_2,C,crs)$, $pp_d=\tilde{\mathcal{G}}$.

● 加密算法. $Enc\left(1^{\lambda},x,m,pp_e\right)\to CT$: 输入安全参数 1^{λ}, 命题 $x\in\mathcal{X}$, 明文消息 $m\in\mathcal{M}$, 加密密钥 pp_e.

(1) 随机生成一个对称加密密钥 $k\leftarrow\{0,1\}^{\ell_{SE}}$, 利用公钥加密分别计算密文 $CT_1\leftarrow PKE.Enc(pk_1,k;r_1)$, $CT_2\leftarrow PKE.Enc(pk_2,k;r_2)$, 并计算对称加密密文 $CT_3\leftarrow SE.Enc(k,(x,m))$;

(2) 针对 NP 命题 y 计算非交互式证据不可区分证明 $\pi\leftarrow NIWI.P(crs,y,w)$, 其中 $y=(CT_1,CT_2,C,pk_1,pk_2)$ 满足:

① CT_1 和 CT_2 为同一个消息的密文, 即 $CT_1\leftarrow PKE.Enc(pk_1,k';r_1)$, $CT_2\leftarrow PKE.Enc(pk_2,k';r_2)$;

② 或者 C 为 $CT_1|CT_2$ 的承诺, 即 $C=Com(CT_1|CT_2)$.

命题第 1 部分对应真实证据 $w_{\text{real}}=(k,r_1,r_2)$, 其中 k 为对称加密密钥, r_1,r_2 分别为生成密文 CT_1,CT_2 对应的随机串; 命题第 2 部分对应陷门证据 $w_{\text{trap}}=s$, 其中 s 为生成承诺 C 对应的随机串.

(3) 输出密文 $CT=(CT_1,CT_2,CT_3,\pi,x)$.

输入: (CT, w)

嵌入: sk_1, pk_1, pk_2

1. $CT=(CT_1, CT_2, CT_3, \pi, x)$;

2. 如果 $NIWI.V(crs, y, \pi)\neq 1$, 则输出 $\perp$; 否则执行下一步;

3. 计算 $PKE.Dec(sk_1, CT_1)=k$, $SE.Dec(k, CT_3)=(\tilde{x}, \tilde{m})$ 如果 $(\tilde{x}=x)\wedge\mathcal{R}(x, w)=1$, 则输出 $\tilde{m}$; 否则输出 $\perp$.

图 1 电路 $\mathcal{G}$ 描述

● 解密算法. $Dec(CT, w, pp_d)\rightarrow m$ or $\perp$: 输入密文 CT, 证据 $w\in\mathcal{W}$ 和解密密钥 pp_d, 计算 $m=\tilde{\mathcal{G}}(CT, w)$.

(1) 正确性. 构造的离线证据加密方案正确性可以从不可区分的混淆, 非交互证据不可区分证明系统和公钥加密方案的正确性得到. 加密阶段, 采用 Naor-Yung 双重加密和密钥封装机制相结合的方法, 并利用非交互证据不可区分证明保证双重加密的两个密文对应同一个明文. 解密阶段, 输入合法生成的密文 $CT=(CT_1, CT_2, CT_3, \pi, x)$ 和证据 w, 电路 $\mathcal{G}$ 首先验证 CT_1, CT_2 为同一个消息的密文, 然后解密 CT_3 得到 $(\tilde{x}, m)$, 如果满足 $\mathcal{R}(\tilde{x}, w)=1$ 和 $\tilde{x}=x$, 电路 $\mathcal{G}$ 输出 m.

(2) 算法的时间复杂度. 在初始化算法中, 首先生成了两对公钥加密的公私钥, 一个长度为 len 的 0 串的承诺, 一个非交互证据不可区分证明的公共参考串, 然后构造并混淆了一个电路 $\mathcal{G}$, 该算法的时间复杂度为 $O(|\mathcal{G}|)$. 加密阶段, 计算了两次公钥加密, 一次对称加密和一个非交互证据不可区分的证明. 相比于公钥加密, 对称加密算法的效率较高, 因此, 我们仅考虑计算公钥加密和非交互证据不可区分证明的时间复杂度. 在实际加密过程中, 可以采用 ElGamal 公钥加密和 Groth-Sahai 证明系统[29]. 利用 ElGamal 加密算法加密对称加密密钥 k 需进行 6 次模幂运算和 2 次群运算. 利用基于 SXDH 假设的非交互证据不可区分证明的构造[29], 证明 π 共包含 4 个群元素, 需进行 6 次多标量乘运算和 8 次双线性对乘积运算. 由于 $NIWI$ 证明的是 CT_1 和 CT_2 为对称加密密钥 k 的密文, 与消息 m 和命题 x 无关, 因此, 加密算法仅需进行常数次双线性群运算, 时间复杂度和输入明文及 NP 实例 x 的长度无关. 在解密算法中, 解密者需要计算混淆电路 $\tilde{\mathcal{G}}$ 关于密文 CT 的输出, 算法的时间复杂度为 $O(|\mathcal{G}|)$. 高效的加密算法是离线证据加密提出的主要动机. 在我们的构造中, 初始化算法仅需运行一次, 生成的公共参数 (pp_e, pp_d) 可以被使用任意多次, 采用 Gennaro 等人[30]分摊模型的思想, 公共参数的生成可以在多次加密计算上进行摊销.

接下来, 我们给出上述构造的离线证据加密适应性安全证明过程.

定理 1. 如果 PKE 是 CPA 安全的公钥加密方案, SE 为一个 CPA 安全的对称加密方案, Com 为完美绑定的承诺方案, $i\mathcal{O}$ 为不可区分的混淆, $NIWI$ 为证据不可区分的证明系统, 则上述构造的 OWE 方案满足适应性不可区分安全性 (见定义 6).

证明: 根据定义 6 对于离线证据加密左右世界的实验和定义, 假设概率多项式时间敌手 $\mathcal{A}$ 对于 OWE 进行适应性安全攻击. 我们首先定义一系列的实验, 然后利用序列实验的方法证明定理的结论, 即证明存在可忽略函数 $negl(\lambda)$, 使得下式成立

$$Adv^{adp-b}_{\mathcal{L},\mathcal{A},OWE}\left(1^{\lambda}\right)=\left|\Pr\left[Expt^{adp-0}_{\mathcal{L},\mathcal{A},OWE}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt^{adp-1}_{\mathcal{L},\mathcal{A},OWE}\left(1^{\lambda}\right)=1\right]\right|\leqslant negl(\lambda).$$

$Expt^0_1$ 是 $\mathcal{A}$ 对于 OWE 的适应性安全攻击实验 $Expt^{adp-0}_{\mathcal{L},\mathcal{A},OWE}(\cdot)$, 其中挑战密文为 (x, m_0) 的加密. 我们提前选定加密挑战明文用到的对称加密密钥 k_0, 并生成挑战密文的前两部分 CT^*_1 和 CT^*_2. 因为对称加密密钥和挑战明文无关, 因此提前选定 k_0 不会影响方案的安全性, 具体描述如下.

(1) 挑战者利用公钥加密方案的密钥生成算法计算两对密钥 $(pk_1, sk_1)\leftarrow PKE.Gen\left(1^{\lambda}\right)$ 和 $(pk_2, sk_2)\leftarrow PKE.Gen\left(1^{\lambda}\right)$, 利用非交互证据不可区分证明生成 $crs\leftarrow NIWI.Setup\left(1^{\lambda}\right)$, 计算承诺 $C\leftarrow Com\left(0^{len}\right)$, 构造电路 $\mathcal{G}$ (如图 1 所示), 并计算 $\tilde{\mathcal{G}}=i\mathcal{O}(\mathcal{G})$. 随机选择对称加密密钥 k_0, 并计算 $CT^*_1\leftarrow PKE.Enc(pk_1, k_0; r_1)$ 和 $CT^*_2\leftarrow PKE.Enc(pk_2, k_0; r_2)$. 设置 $pp_e=(pk_1, pk_2, C, crs)$, $pp_d=\tilde{\mathcal{G}}$, 并将 (pp_e, pp_d) 发送给敌手 $\mathcal{A}$;

(2) 敌手 $\mathcal{A}$ 输出一对等长明文消息 (m_0, m_1) 和一个命题 x;

(3) 挑战者加密消息 m_0 如下: 利用 k_0 加密 (x, m_0) 得到 $CT^*_3\leftarrow SE.Enc(k_0, (x, m_0))$; 针对 $y^*=\left(CT^*_1, CT^*_2, C, pk_1, pk_2\right)$

计算非交互证据不可区分证明 $\pi^* \leftarrow NIWI.P(crs, y^*, w)$, 最后输出挑战密文 $CT^* = \left(CT_1^*, CT_2^*, CT_3^*, \pi^*, x\right)$.

(4) 敌手 $\mathcal{A}$ 得到密文 CT^*, 输出一个比特 b'. 如果 $x \in \mathcal{L}$, 则实验输出 0, 否则实验输出 b'.

由上述实验可以得到, 实验 $Expt_1^0$ 输出 1, 当且仅当 $Expt_{\mathcal{L},\mathcal{A},OWE}^{adp-0}\left(1^\lambda\right)$ 输出 1, 即:

$$\Pr\left[Expt_{\mathcal{L},\mathcal{A},OWE}^{adp-0}\left(1^\lambda\right)=1\right]=\Pr\left[Expt_1^0\left(1^\lambda\right)=1\right].$$

$Expt_2^0$ 与实验 $Expt_1^0$ 的不同在于: 初始化算法中承诺 C 的生成方式, 令 $CT^* = \left(CT_1^*, CT_2^*, CT_3^*, \pi^*, x\right)$ 为挑战密文, 则 $C = Com\left(CT_1^* | CT_2^*\right)$. 注意到 CT_1^*, CT_2^* 为密钥 k_0 的密文, 不涉及到挑战明文信息, 因此可以提前选取.

引理 1. 假设 Com 为完美绑定的承诺方案, 则存在可忽略函数 $negl_1(\lambda)$, 使得下式成立:

$$\Pr\left[Expt_1^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_2^0\left(1^\lambda\right)=1\right]\leqslant negl_1(\lambda).$$

证明: 实验 $Expt_2^0$ 和实验 $Expt_1^0$ 唯一不同的是加密密钥 pp_e 中承诺 C 的生成方式. 在实验 $Expt_1^0$ 中, C 是 0^{len} 的承诺, 而在实验 $Expt_2^0$ 中, C 是部分挑战密文 $CT_1^* | CT_2^*$ 的承诺. 我们证明如果存在一个概率多项式时间敌手 $\mathcal{A}$ 以不可忽略的概率区分实验 $Expt_1^0$ 和实验 $Expt_2^0$ 的输出, 则存在一个概率多项式时间敌手 $\mathcal{B}$ 可以以相同的概率成功攻击承诺方案 Com 的计算隐藏性. 敌手 $\mathcal{B}$ 的定义如下.

(1) $\mathcal{B}$ 生成两对密钥 $(pk_1, sk_1) \leftarrow PKE.Gen\left(1^\lambda\right)$, $(pk_2, sk_2) \leftarrow PKE.Gen\left(1^\lambda\right)$ 和公共参考串 $crs \leftarrow NIWI.Setup\left(1^\lambda\right)$, 随机选择对称加密密钥 $k_0 \leftarrow \{0,1\}^{\ell_{SE}}$, 计算密文 $CT_1^* \leftarrow PKE.Enc(pk_1, k_0)$, $CT_2^* \leftarrow PKE.Enc(pk_2, k_0)$. 然后, $\mathcal{B}$ 发送 0^{len} 和 $CT_1^* | CT_2^*$ 给承诺方案的挑战者, 得到承诺 C^*, 其中 $|0^{len}| = |CT_1^* | CT_2^*|$. 最后, 敌手 $\mathcal{B}$ 构造电路 $\mathcal{G}$ (如图 1 所示), 计算 $\tilde{\mathcal{G}} = i\mathcal{O}(\mathcal{G})$, 发送 $pp_e = (pk_1, pk_2, C^*, crs)$ 和 $pp_d = \tilde{\mathcal{G}}$ 给敌手 $\mathcal{A}$.

(2) $\mathcal{A}$ 输出一个命题 x 和一对等长明文 (m_0, m_1).

(3) $\mathcal{B}$ 利用密钥 k_0 计算挑战密文 $CT_3^* \leftarrow SE.Enc(k_0, (x, m_0))$, 并按照实验 $Expt_1^0$ 的方法生成非交互证据不可区分证明 π^*, 返回挑战密文 $CT^* = \left(CT_1^*, CT_2^*, CT_3^*, \pi^*, x\right)$ 给敌手 $\mathcal{A}$.

(4) 最终, $\mathcal{B}$ 输出 $\mathcal{A}$ 的输出结果.

可以观察到, 如果 C^* 是 0^{len} 的承诺, 即 $C^* = Com\left(0^{len}\right)$, 则 $\mathcal{B}$ 完美模拟了实验 $Expt_1^0$, 可得:

$$\Pr\left[Expt_1^0\left(1^\lambda\right)=1\right]=\Pr\left[\mathcal{B}\left(Com\left(0^{len}\right)\right)=1\right].$$

如果 C^* 是 $CT_1^* | CT_2^*$ 的承诺, 即 $C^* = Com\left(CT_1^* | CT_2^*\right)$, 则 $\mathcal{B}$ 完美模拟了实验 $Expt_2^0$, 可得:

$$\Pr\left[Expt_2^0\left(1^\lambda\right)=1\right]=\Pr\left[\mathcal{B}\left(Com\left(CT_1^* | CT_2^*\right)\right)=1\right].$$

注意到计算承诺 C^* 所用到的随机串并没有出现在方案其他地方, 因此根据承诺方案 Com 的计算隐藏性质可以得到, 对任意概率多项式时间敌手 $\mathcal{B}$, 存在可忽略函数 $negl_1(\lambda)$, 使得

$$\left|\Pr\left[Expt_1^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_2^0\left(1^\lambda\right)=1\right]\right|=\left|\Pr\left[\mathcal{B}\left(Com\left(0^{len}\right)\right)=1\right]-\Pr\left[\mathcal{B}\left(Com\left(CT_1^* | CT_2^*\right)\right)=1\right]\right|\leqslant negl_1(\lambda).$$

$Expt_3^0$ 与 $Expt_2^0$ 的不同在于: 挑战密文 $CT^* = \left(CT_1^*, CT_2^*, CT_3^*, \pi^*, x\right)$ 中 π^* 的生成方式, $\pi^* \leftarrow NIWI.P\left(crs, y^*, w_{\text{trap}}\right)$, 其中 $w_{\text{trap}} = s$ 为陷门证据, s 为生成承诺 C 用到的随机串.

引理 2. 假设 $NIWI$ 为证据不可区分的证明系统, 则存在可忽略函数 $negl_2(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_2^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_3^0\left(1^\lambda\right)=1\right]\right|\leqslant negl_2(\lambda).$$

证明: 实验 $Expt_3^0$ 和实验 $Expt_2^0$ 唯一的不同在于挑战密文 $CT^* = \left(CT_1^*, CT_2^*, CT_3^*, \pi^*, x\right)$ 中证明 π^* 的生成方式. 在实验 $Expt_2^0$ 中, 通过真实证据 $w_{\text{real}} = (k_0, r_1, r_2)$ 计算得到证明 π^*; 在实验 $Expt_3^0$ 中, 通过陷门证据 $w_{\text{trap}} = s$ 生成证明 π^*. 我们证明如果存在一个概率多项式时间敌手 $\mathcal{A}$ 以不可忽略的概率区分实验 $Expt_3^0$ 和实验 $Expt_2^0$ 的输出, 则存在一个概率多项式时间敌手 $\mathcal{B}$ 可以以相同的概率成功攻击 $NIWI$ 的证据不可区分性. 敌手 $\mathcal{B}$ 的定义如下.

(1) $\mathcal{B}$ 从 $NIWI$ 的挑战者得到公共参考串 crs, 运行公钥加密算法生成两对密钥 $(pk_1, sk_1) \leftarrow PKE.Gen\left(1^\lambda\right)$ 和 $(pk_2, sk_2) \leftarrow PKE.Gen\left(1^\lambda\right)$, 随机选择对称加密密钥 $k_0 \leftarrow \{0,1\}^{\ell_{SE}}$, 并计算密文 $CT_1^* \leftarrow PKE.Enc(pk_1, k_0; r_1)$, $CT_2^* \leftarrow PKE.Enc(pk_2, k_0; r_2)$ 和承诺 $C = Com\left(CT_1^* | CT_2^*; s\right)$. 敌手 $\mathcal{B}$ 构造电路 $\mathcal{G}$ (如图 1 所示), 计算 $\tilde{\mathcal{G}} = i\mathcal{O}(\mathcal{G})$, 然后发送

$pp_e=(pk_1,pk_2,C,crs)$, $pp_d=\tilde{\mathcal{G}}$ 给敌手 $\mathcal{A}$.

(2) $\mathcal{A}$ 输出一个命题 x 和一对等长明文 (m_0,m_1).

(3) $\mathcal{B}$ 利用密钥 k_0 计算挑战密文 $CT_3^*\leftarrow SE.Enc(k_0,(x,m_0))$, 并构造 NP 命题 $y^*=\left(CT_1^*,CT_2^*,C,pk_1,pk_2\right)$, 满足:

- CT_1 和 CT_2 为同一个消息的密文, 即 $CT_1\leftarrow PKE.Enc(pk_1,k';r_1)$, $CT_2\leftarrow PKE.Enc(pk_2,k';r_2)$;
- 或者 C 为 $CT_1^*|CT_2^*$ 的承诺, 即 $C=Com\left(CT_1^*|CT_2^*;s\right)$.

命题第 1 部分对应真实证据 $w_{\text{real}}=(k_0,r_1,r_2)$, 命题第 2 部分对应陷门证据 $w_{\text{trap}}=s$, 其中 r_1,r_2 分别为生成密文 CT_1^*,CT_2^* 对应的随机串, s 为生成承诺 C 对应的随机串. 因为 C 为挑战密文 $CT_1^*|CT_2^*$ 的承诺, 并且 CT_1^* 和 CT_2^* 为 (x,m_0) 的密文, 因此命题 y^* 成立存在两个证据 w_{real} 和 w_{trap}. $\mathcal{B}$ 将 $\left(y^*,w_{\text{real}},w_{\text{trap}}\right)$ 发送给 $NIWI$ 的挑战者, 得到证明 π^*, 然后将挑战密文 $CT^*=\left(CT_1^*,CT_2^*,CT_3^*,\pi^*,x\right)$ 返回 $\mathcal{A}$.

(4) 最终, $\mathcal{B}$ 输出 $\mathcal{A}$ 的输出结果.

可以观察到, 如果证明 π^* 是由真实证据 $w_{\text{real}}=(k_0,r_1,r_2)$ 生成的, 则 $\mathcal{B}$ 完美模拟了实验 $Expt_2^0$, 可得:

$$\Pr\left[Expt_2^0\left(1^\lambda\right)=1\right]=\Pr[\mathcal{B}(crs,NIWI.P(crs,y^*,w_{\text{real}}))=1].$$

如果证明 π^* 是由陷门证据 $w_{\text{trap}}=s$ 生成的, 则 $\mathcal{B}$ 完美模拟了实验 $Expt_3^0$, 可得:

$$\Pr\left[Expt_3^0\left(1^\lambda\right)=1\right]=\Pr\left[\mathcal{B}\left(crs,NIWI.P\left(crs,y^*,w_{\text{trap}}\right)\right)=1\right].$$

由 $NIWI$ 的证据不可区分性可得, 对任意概率多项式时间敌手 $\mathcal{B}$, 存在可忽略函数 $negl_2(\lambda)$, 使得:

$$\left|\Pr\left[Expt_2^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_3^0\left(1^\lambda\right)=1\right]\right|=$$
$$\left|\Pr[\mathcal{B}(crs,NIWI.P(crs,y^*,w_{\text{real}}))=1]-\Pr\left[\mathcal{B}\left(crs,NIWI.P\left(crs,y^*,w_{\text{trap}}\right)\right)=1\right]\right|\leqslant negl_2(\lambda).$$

$Expt_4^0$ 与 $Expt_3^0$ 的不同在于: 挑战密文 $CT^*=\left(CT_1^*,CT_2^*,CT_3^*,\pi^*,x\right)$ 中的 CT_2^* 是 k_1 的密文, 即 $CT_2^*\leftarrow PKE.Enc(pk_2,k_1)$, 其中 k_1 是对称加密的密钥.

引理 3. 假设 PKE 是 CPA 安全的公钥加密方案, 则存在可忽略函数 $negl_3(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_3^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_4^0\left(1^\lambda\right)=1\right]\right|\leqslant negl_3(\lambda).$$

证明: 实验 $Expt_4^0$ 和实验 $Expt_3^0$ 唯一不同在于挑战密文中 CT_2^* 的生成方式: 在实验 $Expt_3^0$ 中, CT_2^* 是密钥 k_0 的密文, 而在实验 $Expt_4^0$ 中, CT_2^* 是密钥 k_1 的密文. 我们证明如果存在一个概率多项式时间敌手 $\mathcal{A}$ 以不可忽略的概率区分实验 $Expt_4^0$ 和实验 $Expt_3^0$ 的输出, 则存在一个概率多项式时间敌手 $\mathcal{B}$ 可以以相同的概率成功攻击公钥加密方案 PKE. 敌手 $\mathcal{B}$ 的定义如下.

(1) $\mathcal{B}$ 从公钥加密方案 PKE 的挑战者得到 pk, 输出一对密钥 $(k_0,k_1)\leftarrow\{0,1\}^{\ell_{SE}}$, 发送给挑战者, 得到 CT_2^*.

(2) $\mathcal{B}$ 生成一对密钥 $(pk_1,sk_1)\leftarrow PKE.Gen\left(1^\lambda\right)$ 和公共参考串 $crs\leftarrow NIWI.Setup\left(1^\lambda\right)$, 然后计算密文 $CT_1^*\leftarrow PKE.Enc(pk_1,k_0)$, 承诺 C 和 $\tilde{\mathcal{G}}=i\mathcal{O}(\mathcal{G})$, 其中电路 $\mathcal{G}$ 如图 1 所示, 设置 $pp_e=(pk_1,pk,C,crs)$, $pp_d=\tilde{\mathcal{G}}$, 并发送 (pp_e,pp_d) 给敌手 $\mathcal{A}$.

(3) $\mathcal{A}$ 输出一个命题 x 和一对等长明文 (m_0,m_1).

(4) $\mathcal{B}$ 利用密钥 k_0 计算挑战密文 $CT_3^*\leftarrow SE.Enc(k_0,(x,m_0))$, 并按照实验 $Expt_1^0$ 的方法生成非交互证据不可区分证明 π^*, 返回挑战密文 $CT^*=\left(CT_1^*,CT_2^*,CT_3^*,\pi^*,x\right)$ 给敌手 $\mathcal{A}$.

(5) 最终, $\mathcal{B}$ 输出 $\mathcal{A}$ 的输出结果.

可以观察到, 如果 CT_2^* 是密钥 k_0 的密文, 则 $\mathcal{B}$ 完美模拟了实验 $Expt_3^0$, 可得:

$$\Pr\left[Expt_3^0\left(1^\lambda\right)=1\right]=\Pr[\mathcal{B}(pk,PKE.Enc(pk,k_0))=1].$$

如果 CT_2^* 是密钥 k_1 的密文, 则 $\mathcal{B}$ 完美模拟了实验 $Expt_4^0$, 可得:

$$\Pr\left[Expt_4^0\left(1^\lambda\right)=1\right]=\Pr[\mathcal{B}(pk,PKE.Enc(pk,k_1))=1].$$

由公钥加密 PKE 的 CPA 安全性得, 对任意概率多项式时间敌手 $\mathcal{B}$, 存在可忽略函数 $negl_3(\lambda)$, 使得:

$$\left|\Pr\left[Expt_3^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_4^0\left(1^\lambda\right)=1\right]\right|=\left|\Pr[\mathcal{B}(pk,PKE.Enc(pk,k_0))=1]-\Pr[\mathcal{B}(pk,PKE.Enc(pk,k_1))=1]\right|\leqslant negl_3(\lambda).$$

$Expt_5^0$ 与实验 $Expt_4^0$ 的不同在于: 解密密钥 pp_d 的生成方式, 在实验 $Expt_5^0$ 中, $pp_d=i\mathcal{O}(\mathcal{G}^*)$, 其中电路 $\mathcal{G}^*$ 和 $\mathcal{G}$ 运行方式不同在于:

(1) 电路 $\mathcal{G}^*$ 嵌入私钥 sk_2 代替电路 $\mathcal{G}$ 中的私钥 sk_1.

(2) 电路 $\mathcal{G}^*$ 中使用 sk_2 解密 CT 的第 2 个密文 CT_2. 具体的, 在电路 $\mathcal{G}$ 的第 3 步中, 通过解密 CT_2 得到对称加密的密钥 k, 即 $PKE.Dec(sk_2,CT_2)=k$.

引理 4. 假设 $i\mathcal{O}$ 是不可区分的混淆, Com 为完美绑定的承诺方案, $NIWI$ 为证据不可区分的证明系统, 则存在可忽略函数 $negl_4(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_4^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_5^0\left(1^\lambda\right)=1\right]\right|\leqslant negl_4(\lambda).$$

证明: 实验 $Expt_5^0$ 和实验 $Expt_4^0$ 唯一的不同在于实验 $Expt_4^0$ 中解密密钥 $pp_d=i\mathcal{O}(\mathcal{G})$, 而实验 $Expt_5^0$ 中解密密钥 $pp_d=i\mathcal{O}(\mathcal{G}^*)$. 我们证明如果存在一个概率多项式时间敌手 $\mathcal{A}$ 以不可忽略的概率区分实验 $Expt_5^0$ 和实验 $Expt_4^0$ 的输出, 则存在一个概率多项式时间的区分器 $\mathcal{D}$ 可以以相同的概率攻击 $i\mathcal{O}$ 的不可区分性. 区分器 $\mathcal{D}$ 的定义如下.

(1) $\mathcal{D}$ 生成一对密钥 $(pk_1,sk_1)\leftarrow PKE.Gen\left(1^\lambda\right)$, $(pk_2,sk_2)\leftarrow PKE.Gen\left(1^\lambda\right)$ 和公共参考串 $crs\leftarrow NIWI.Setup\left(1^\lambda\right)$, 计算密文 $CT_1^*\leftarrow PKE.Enc(pk_1,k_0)$, $CT_2^*\leftarrow PKE.Enc(pk_2,k_1)$ 和承诺 $C=Com\left(CT_1^*|CT_2^*\right)$, 并分别构造电路 $\mathcal{G}$ 和 $\mathcal{G}^*$ 发送给 $i\mathcal{O}$ 挑战者, 得到混淆电路 $pp_d=\tilde{\mathcal{G}}$. 设置 $pp_e=(pk_1,pk_2,C,crs)$, 发送 (pp_e,pp_d) 给敌手 $\mathcal{A}$.

(2) $\mathcal{A}$ 输出一个命题 x 和一对等长消息 (m_0,m_1).

(3) $\mathcal{D}$ 利用密钥 k_0 计算挑战密文 $CT_3^*\leftarrow SE.Enc(k_0,(x,m_0))$, 并按照实验 $Expt_1^0$ 的方法生成非交互证据不可区分证明 π^*, 返回挑战密文 $CT^*=\left(CT_1^*,CT_2^*,CT_3^*,\pi^*,x\right)$ 给敌手 $\mathcal{A}$.

(4) 最终, $\mathcal{D}$ 输出 $\mathcal{A}$ 的输出结果.

可以观察到, 如果 $\tilde{\mathcal{G}}=i\mathcal{O}(\mathcal{G})$, 则 $\mathcal{D}$ 完美模拟了实验 $Expt_4^0$, 可得:

$$\Pr\left[Expt_4^0\left(1^\lambda\right)=1\right]=\Pr[\mathcal{D}(i\mathcal{O}(\lambda,\mathcal{G}))=1].$$

如果 $\tilde{\mathcal{G}}=i\mathcal{O}(\mathcal{G}^*)$, 则 $\mathcal{D}$ 完美模拟了实验 $Expt_5^0$, 可得:

$$\Pr\left[Expt_5^0\left(1^\lambda\right)=1\right]=\Pr[\mathcal{D}(i\mathcal{O}(\lambda,\mathcal{G}^*))=1].$$

为了证明实验 $Expt_5^0$ 和实验 $Expt_4^0$ 的输出是计算不可区分的, 我们需要首先证明电路 $\mathcal{G}$ 和 $\mathcal{G}^*$ 有相同的输入-输出行为. 然后, 通过不可区分混淆的安全性可以得到, 对任意的概率多项式时间的区分器 $\mathcal{D}$, 存在可忽略函数 $negl_4(\lambda)$, 使得:

$$\left|\Pr[\mathcal{D}(i\mathcal{O}(\lambda,\mathcal{G}))=1]-\Pr[\mathcal{D}(i\mathcal{O}(\lambda,\mathcal{G}^*))=1]\right|\leqslant negl_4(\lambda),$$

从而得证该定理. 下面分两种情形来讨论实验 $Expt_5^0$ 和实验 $Expt_4^0$ 的输入输出行为.

情形 1: 对任意的输入 $CT=(CT_1,CT_2,CT_3,\pi,x)$, 电路 $\mathcal{G}$ 输出 $\perp$ 当且仅当电路 $\mathcal{G}^*$ 输出 $\perp$.

观察到电路输出 $\perp$ 存在 2 种情况.

1) 密文中的证明 π 不能通过非交互证据不可区分证明系统的验证算法, 即 $NIWI.V(crs,y,\pi)\neq 1$;

2) 密文中的 CT_3 解密得到的 $(\tilde{x},\tilde{m})$, $\tilde{x}\neq x$ 或者 $\mathcal{R}(x,w)\neq 1$.

如果情况 1) 成立, 则电路 $\mathcal{G}$ 和 $\mathcal{G}^*$ 同时输出 $\perp$. 如果情况 2) 成立, 若输入 CT 不是挑战密文, 因为 $\tilde{x}\neq x$ 或者 $\mathcal{R}(x,w)\neq 1$, 则电路 $\mathcal{G}$ 和 $\mathcal{G}^*$ 同时输出 $\perp$; 若输入 CT 为挑战密文, 则 $x\notin\mathcal{L}$, 即 $\mathcal{R}(x,w)\neq 1$ 成立, 因此电路 $\mathcal{G}$ 和 $\mathcal{G}^*$ 同时输出 $\perp$. 如果输入 $CT=(CT_1,CT_2,CT_3,\pi,x)$, 电路 $\mathcal{G}$ 不输出 $\perp$, 则称 CT 是有效的. 下面, 我们证明对任意的有效输入, 电路 $\mathcal{G}$ 和 $\mathcal{G}^*$ 具有相同的功能.

情形 2: 对任意有效输入 $CT=(CT_1,CT_2,CT_3,\pi,x)$, $\mathcal{G}(CT)=\mathcal{G}^*(CT)$.

对于有效输入 $CT=(CT_1,CT_2,CT_3,\pi,x)$, 可以得到 $NIWI.P(crs,y,\pi)=1$, 则分两种情况.

1) 若命题 y 的第 1 部分成立, 即 CT_1 和 CT_2 为同一个消息的密文, 则得到对称加密密钥 $PKE.Dec(sk_1,CT_1)=$

$PKE.Dec(sk_2,CT_2)=k$. 利用 k 解密密文 CT_3 得到 $(\tilde{x},\tilde{m})$, CT 为有效输入, $\mathcal{G}$ 和 $\mathcal{G}^*$ 同时输出 $\tilde{m}$.

2) 若命题 y 的第 2 部分成立, 即 $C=Com\left(CT_1^*|CT_2^*\right)$, 由承诺方案 Com 完美绑定的性质可得 $CT_1|CT_2=CT_1^*|CT_2^*$. 若 $CT_3=CT_3^*$, 根据情形 1 的描述, 电路 $\mathcal{G}$ 和 $\mathcal{G}^*$ 同时输出 $\perp$; 若 $CT_3\neq CT_3^*$, CT_1^*,CT_2^* 分别为对称密钥 k_0,k_1 的密文. 因为 $k_0,k_1\leftarrow\{0,1\}^{\ell_{SE}}$, 加密密文 CT_3 使用的密钥为 k_0,k_1 的概率为 $1/2^{(\ell_{SE}-1)}$, 根据对称加密的性质, 解密 CT_3 得到的 $\tilde{x}$ 和密文 CT 中 x 相等的概率小于可忽略函数 $1/2^{(\ell_{SE}-1)}$, 所以 $\mathcal{G}$ 和 $\mathcal{G}^*$ 同时输出 $\perp$.

从上述分析可以得到, 电路 $\mathcal{G}$ 和 $\mathcal{G}^*$ 有相同的输入-输出行为, 即 $\forall x,\mathcal{G}(x)=\mathcal{G}^*(x)$, 因此, 根据 $i\mathcal{O}$ 的不可区分性, 存在可忽略函数 $negl_4(\lambda)$, 使得:

$$\left|\Pr\left[Expt_4^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_5^0\left(1^\lambda\right)=1\right]\right|=\left|\Pr[\mathcal{D}(i\mathcal{O}(\lambda,\mathcal{G}))=1]-\Pr[\mathcal{D}(i\mathcal{O}(\lambda,\mathcal{G}^*))=1]\right|\leqslant negl_4(\lambda).$$

$Expt_6^0$ 与实验 $Expt_5^0$ 的不同在于: $CT^*=\left(CT_1^*,CT_2^*,CT_3^*,\pi^*,x\right)$ 中的 CT_1^* 是密钥 k_1 的密文, 即 $CT_1^*\leftarrow PKE.Enc(pk_1,k_1)$, 其中 k_1 是对称加密的密钥.

引理 5. 假设 PKE 是 CPA 安全的公钥加密方案, 则存在可忽略函数 $negl_5(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_5^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_6^0\left(1^\lambda\right)=1\right]\right|\leqslant negl_5(\lambda).$$

证明: 证明方法和引理 3 类似.

$Expt_7^0$ 与实验 $Expt_6^0$ 的不同在于: 挑战密文 $CT^*=\left(CT_1^*,CT_2^*,CT_3^*,\pi^*,x\right)$ 中 CT_3^* 的生成方式, 在实验 $Expt_7^0$ 中, 随机生成一个新的对称加密密钥 k_2, 利用 k_2 代替 k_0 生成密文 CT_3^*, 即 $CT_3^*\leftarrow SE.Enc(k_2,(x,m_0))$.

引理 6. 实验 $Expt_7^0$ 和实验 $Expt_6^0$ 的输出是统计不可区分的, 即存在可忽略函数 $negl_6(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_6^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_7^0\left(1^\lambda\right)=1\right]\right|\leqslant negl_6(\lambda).$$

证明: 实验 $Expt_7^0$ 和实验 $Expt_6^0$ 不同在于加密生成 CT_3^* 使用的密钥: 在实验 $Expt_6^0$ 中, 使用 k_0 加密 (x,m_0) 生成 CT_3^*; 而在实验 $Expt_7^0$ 中, 使用 k_2 加密 (x,m_0) 生成 CT_3^*. 观察到 k_0 和 k_2 全部随机选自对称加密的密钥空间 $\{0,1\}^{\ell_{SE}}$, 并且独立于密文 CT_1^* 和 CT_2^*, 因此存在可忽略函数 $negl_6(\lambda)=1/2^{\ell_{SE}}$, 使得:

$$\left|\Pr\left[Expt_6^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_7^0\left(1^\lambda\right)=1\right]\right|\leqslant negl_6(\lambda).$$

$Expt_8^1$ 与实验 $Expt_7^0$ 的不同在于: $CT^*=\left(CT_1^*,CT_2^*,CT_3^*,\pi^*,x\right)$ 中 CT_3^* 是 (x,m_1) 的密文, 即 $CT_3^*\leftarrow SE.Enc(k_2,(x,m_1))$.

引理 7. 假设 $(SE.Enc,SE.Dec)$ 是一个 CPA 安全的对称加密方案, 则存在可忽略函数 $negl_7(\lambda)$, 使下式成立:

$$\left|\Pr\left[Expt_7^0\left(1^\lambda\right)=1\right]-\Pr\left[Expt_8^1\left(1^\lambda\right)=1\right]\right|\leqslant negl_7(\lambda).$$

证明: 证明方法类似于引理 3, 由对称加密的 CPA 安全性可以直接得到上述结论.

$Expt_9^1$ 与实验 $Expt_8^1$ 的不同之处在于: 挑战密文 $CT^*=\left(CT_1^*,CT_2^*,CT_3^*,\pi^*,x\right)$ 中的 CT_1^* 是密钥 k_2 的密文, 即 $CT_1^*\leftarrow PKE.Enc(pk_1,k_2)$.

引理 8. 假设 PKE 是 CPA 安全的公钥加密方案, 则存在可忽略函数 $negl_8(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_8^1\left(1^\lambda\right)=1\right]-\Pr\left[Expt_9^1\left(1^\lambda\right)=1\right]\right|\leqslant negl_8(\lambda).$$

证明: 证明方法和引理 3 类似.

$Expt_{10}^1$ 与实验 $Expt_9^1$ 的不同在于: pp_d 的生成方式, 在实验 $Expt_{10}^1$ 中, $pp_d=i\mathcal{O}(\mathcal{G})$, 其中 $\mathcal{G}$ 的描述如图 1 所示.

引理 9. 假设 $i\mathcal{O}$ 是不可区分的混淆, Com 为完美绑定的承诺方案, $NIWI$ 为证据不可区分的证明系统, 则存在可忽略函数 $negl_9(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_9^1\left(1^\lambda\right)=1\right]-\Pr\left[Expt_{10}^1\left(1^\lambda\right)=1\right]\right|\leqslant negl_9(\lambda).$$

证明: 证明方法和引理 4 类似.

$Expt_{11}^1$ 与实验 $Expt_{10}^1$ 的不同在于: 挑战密文 $CT^*=\left(CT_1^*,CT_2^*,CT_3^*,\pi^*,x\right)$ 中的 CT_2^* 是密钥 k_2 的密文, 即 $CT_2^*\leftarrow PKE.Enc(pk_2,k_2)$.

引理 10. 假设 PKE 是 CPA 安全的公钥加密方案, 则存在可忽略函数 $negl_{10}(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_{10}^{1}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{11}^{1}\left(1^{\lambda}\right)=1\right]\right|\leqslant negl_{10}(\lambda).$$

证明: 证明方法和引理 3 类似.

$Expt_{12}^{1}$ 与实验 $Expt_{11}^{1}$ 的不同在于: 挑战密文 $CT^{*}=\left(CT_{1}^{*},CT_{2}^{*},CT_{3}^{*},\pi^{*},x\right)$ 中证明 π^{*} 的生成方式, 在实验 $Expt_{12}^{1}$ 中, $\pi^{*}\leftarrow NIWI.P(crs,y^{*},w_{\text{real}})$, 其中 $w_{\text{real}}=(k_{2},r_{1},r_{2})$ 为真实证据, k_{2} 为对称加密密钥, r_{1},r_{2} 分别为生成密文 CT_{1}^{*},CT_{2}^{*} 对应的随机串.

引理 11. 假设 $NIWI$ 为证据不可区分的证明系统, 则存在可忽略函数 $negl_{11}(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_{11}^{1}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{12}^{1}\left(1^{\lambda}\right)=1\right]\right|\leqslant negl_{11}(\lambda).$$

证明: 证明方法和引理 2 类似.

$Expt_{13}^{1}$ 与实验 $Expt_{12}^{1}$ 的不同在于: 初始化算法中承诺 C 的生成方式, 在实验 $Expt_{13}^{1}$ 中, $C\leftarrow Com\left(0^{len}\right)$.

引理 12. 假设 Com 为完美绑定的承诺方案, 则存在可忽略函数 $negl_{12}(\lambda)$, 使得下式成立:

$$\left|\Pr\left[Expt_{12}^{1}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{11}^{1}\left(1^{\lambda}\right)=1\right]\right|\leqslant negl_{12}(\lambda).$$

证明: 证明方法和引理 1 类似.

可以发现, 在实验 $Expt_{13}^{1}$ 中, $Pr\left[Expt_{\mathcal{L},\mathcal{A},OWE}^{adp-1}\left(1^{\lambda}\right)=1\right]=\Pr\left[Expt_{13}^{1}\left(1^{\lambda}\right)=1\right]$, 综合引理 1 至引理 12 的结果, 利用绝对值三角不等式有:

$$\begin{aligned}
Adv_{\mathcal{L},\mathcal{A},OWE}^{adp-b}\left(1^{\lambda}\right)&=\left|\Pr\left[Expt_{\mathcal{L},\mathcal{A},OWE}^{adp-0}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{\mathcal{L},\mathcal{A},OWE}^{adp-1}\left(1^{\lambda}\right)=1\right]\right|=\left|\Pr\left[Expt_{1}^{0}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{13}^{1}\left(1^{\lambda}\right)=1\right]\right|\\
&=\Bigg|\Pr\left[Expt_{1}^{0}\left(1^{\lambda}\right)=1\right]-\sum_{i=2}^{7}\left(\Pr\left[Expt_{i}^{0}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{i}^{0}\left(1^{\lambda}\right)=1\right]\right)\\
&\quad-\sum_{i=8}^{12}\left(\Pr\left[Expt_{i}^{1}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{i}^{1}\left(1^{\lambda}\right)=1\right]\right)-\Pr\left[Expt_{13}^{1}\left(1^{\lambda}\right)=1\right]\Bigg|\\
&\leqslant\sum_{i=1}^{6}\left(\left|\Pr\left[Expt_{i}^{0}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{i+1}^{0}\left(1^{\lambda}\right)=1\right]\right|\right)+\left|\Pr\left[Expt_{7}^{0}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{8}^{1}\left(1^{\lambda}\right)=1\right]\right|\\
&\quad+\sum_{i=8}^{12}\left(\left|\Pr\left[Expt_{i}^{1}\left(1^{\lambda}\right)=1\right]-\Pr\left[Expt_{i+1}^{1}\left(1^{\lambda}\right)=1\right]\right|\right)\leqslant\sum_{i=1}^{12}negl_{i}(\lambda),
\end{aligned}$$

由于每个 $negl_{i}(\lambda),i=1,2,\ldots,12$ 均为可忽略函数, 根据可忽略函数的性质可得 $\sum_{i=1}^{12}negl_{i}(\lambda)$ 仍是一个可忽略函数. 定理 1 得证.

4 离线函数证据加密

4.1 离线函数证据加密定义

离线函数证据加密包含 4 个算法 $FOWE=(F.Setup,F.KeyGen,F.Enc,F.Dec)$: 输入安全参数 1^{λ}, 初始化算法 $F.Setup$ 输出一对密钥 (pp,msk); 密钥生成算法 $F.KeyGen$ 输入主私钥 msk 和函数 $f\in\mathcal{F}_{\lambda}$, 输出解密密钥 sk_{f}; 加密算法 $F.Enc$ 输入安全参数 1^{λ}, NP 实例 x, 明文消息 m, 输出密文 CT; 解密算法 $F.Dec$ 输入密文 CT 和对应 NP 实例 $x\in\mathcal{L}$ 的证据 w, 输出明文消息 $f(m,w)$. 我们沿用 Boyle 等人[15]提出的函数证据加密定义, 并作适当修改, 具体描述如下.

定义 7. 离线函数证据加密. 针对具有证据关系 $\mathcal{R}:\mathcal{X}\times\mathcal{W}\rightarrow\{0,1\}$ 的 NP 语言 $\mathcal{L}\in NP$, 及函数族 $\mathcal{F}_{\lambda}$, 离线函数证据加密方案包含 4 个概率多项式时间的算法 $(F.Setup,F.KeyGen,F.Enc,F.Dec)$:

(1) 初始化算法: $F.Setup(1^{\lambda})\rightarrow(pp,msk)$: 输入安全参数 1^{λ}, 初始化算法输出一对密钥 (pp,msk), pp 用于加密, msk 用于生成解密密钥;

(2) 密钥生成算法: $F.KeyGen(msk,f)\rightarrow sk_{f}$: 输入主私钥 msk 和函数 $f\in\mathcal{F}_{\lambda}$, 密钥生成算法输出解密密钥 sk_{f};

(3) 加密算法: $F.Enc(1^{\lambda},x,m,pp)\rightarrow CT$: 输入安全参数 1^{λ}, 命题 $x\in\mathcal{X}$, 明文消息 $m\in\mathcal{M}$, 加密密钥 pp, 加密算法输出密文 CT;

(3) 解密算法: $F.Dec(CT,w,sk_{f})\rightarrow f(m,w)\ or\perp$: 输入密文 CT, 证据 $w\in\mathcal{W}$ 和解密密钥 sk_{f}, 解密算法输出 $f(m,w)$ 或 $\perp$.

需要说明的是 Boyle 等人[15]的函数证据加密的初始化算法和离线证据加密的初始化算法定义类似, 中间并不涉及到函数 f, 加密算法将函数 f 作为明文消息的一部分, 解密输出 $f(m,w)$. 不同于 Boyle 等人[15]给出的定义, 我们重新定义了一个针对函数 f 的密钥生成算法, 生成的解密密钥 sk_f 可以多次使用, 即生成密钥 sk_f 后, 可以计算任意多次关于 f 的函数值.

离线函数证据加密需满足正确性和安全性, 定义如下.

定义 8. 正确性. 对所有的 $\lambda\in\mathbb{N}$, $(x,w)\in\mathcal{X}\times\mathcal{W}$, 使得 $\mathcal{R}(x,w)=1$, $m\in\mathcal{M}$, $f\in\mathcal{F}_\lambda$ 满足:

$$Pr[(pp,msk)\leftarrow F.Setup(1^\lambda);sk_f\leftarrow F.KeyGen(msk,f);CT\leftarrow F.Enc(1^\lambda,x,m,pp):F.Dec(CT,w,sk_f)\rightarrow f(m,w)]=1.$$

定义 9. 适应性不可区分安全性. 针对具有证据关系 $\mathcal{R}$ 的语言 $\mathcal{L}\in NP$, 任意敌手 $\mathcal{A}$ 对于离线函数证据加密方案 $FOWE=(F.Setup,F.KeyGen,F.Enc,F.Dec)$ 进行适应性安全攻击的实验定义如下, 对于任意 $b\in\{0,1\}$, 实验 $Expt^{adp-b}_{\mathcal{L},\mathcal{A},FOWE}(\cdot)$ 输入 1^λ:

(1) 挑战者利用初始化算法生成一对密钥 (pp,msk), 并将公钥 pp 发送给敌手 $\mathcal{A}$.

(2) 敌手 $\mathcal{A}$ 得到密钥 pp 后, 可以进行密钥生成询问. 敌手 $\mathcal{A}$ 适应性选择 $f_i\in\mathcal{F}_\lambda$ 并发送给挑战者, 挑战者运行密钥生成算法 $F.KeyGen(msk,f_i)\rightarrow sk_{f_i}$, 将 sk_{f_i} 返回给敌手 $\mathcal{A}$. 敌手 $\mathcal{A}$ 可以重复询问密钥生成算法, 然后输出一个命题 x 和一对等长明文 (m_0,m_1), 使得对所有询问过密钥生成算法的 f_i 满足 $f_i(m_0,w)=f_i(m_1,w)$.

(3) 挑战者加密消息 (x,m_b), 得到密文 $CT^*\leftarrow Enc(1^\lambda,x,m_b,pp)$.

(4) 敌手 $\mathcal{A}$ 得到密文 CT^*, 仍可以针对函数 f_j 询问密钥生成算法, 其中 f_j 需满足 $f_j(m_0,w)=f_j(m_1,w)$, 最后输出一个比特 $b'\in\{0,1\}$. 最终, 实验输出比特 b'.

对于语言 $\mathcal{L}\in NP$ 的离线函数加密方案 $FOWE=(F.Setup,F.KeyGen,F.Enc,F.Dec)$, 如果任何概率多项式敌手 $\mathcal{A}$ 在上述实验 $Expt^{adp-b}_{\mathcal{L},\mathcal{A},FOWE}(\cdot)$ 中成功的优势 $Adv^{adp-b}_{\mathcal{L},\mathcal{A},FOWE}(1^\lambda)$ 是可忽略的, 则存在可忽略函数 $negl(\lambda)$, 使得下式成立:

$$Adv^{adp-b}_{L,\mathcal{A},FOWE}(1^\lambda)=|\Pr[Expt^{adp-0}_{L,\mathcal{A},FOWE}(1^\lambda)=1]-\Pr[Expt^{adp-1}_{L,\mathcal{A},FOWE}(1^\lambda)=1]|\leqslant negl(\lambda),$$

则称 $FOWE$ 具有适应性不可区分安全性.

4.2 离线函数证据加密构造

定义 $PKE=(PKE.Gen,PKE.Enc,PKE.Dec)$ 为一个公钥加密方案, Com 为承诺方案, $NIWI=(NIWI.Setup,NIWI.P,NIWI.V)$ 为非交互证据不可区分证明系统, $i\mathcal{O}$ 为不可区分的混淆, $SE=(SE.Enc,SE.Dec)$ 为对称加密方案, 令 $len_c=len_c(1^\lambda)$ 为公钥加密密文的长度, 定义参数 $len=2\cdot len_c$. 对称加密需满足如下性质:

$$\Pr\left[(k_0,k_1)\leftarrow\{0,1\}^{l_{SE}},k_0\neq k_1,CT\leftarrow SE.Enc(k_0,m):SE.Dec(k_1,CT)=m\right]\leqslant negl(\lambda),$$

其中, $\{0,1\}^{\ell_{SE}}$ 为对称加密的密钥空间, $negl(\lambda)$ 为可忽略函数.

构造离线证据加密方案如下.

- 初始化算法. $F.Setup(1^\lambda)\rightarrow(pp,msk)$: 输入安全参数 1^λ,

(1) 运行公钥加密密钥生成算法得到两对密钥: $(pk_1,sk_1)\leftarrow PKE.Gen(1^\lambda)$ 和 $(pk_2,sk_2)\leftarrow PKE.Gen(1^\lambda)$;

(2) 利用证据不可区分证明系统初始化算法生成公共参考串 $crs\leftarrow NIWI.Setup(1^\lambda)$;

(3) 计算承诺 $C\leftarrow Com(0^{len})$;

(4) 设置 $pp=(pk_1,pk_2,C,crs),msk=sk_1$.

- 密钥生成算法. $F.KeyGen(msk,f)\rightarrow sk_f$:

(1) 计算 $\tilde{\mathcal{G}}_1=i\mathcal{O}(\mathcal{G}_1)$, 其中 $\mathcal{G}_1$ 定义如图 2 所示:

(2) 设置 $sk_f=\tilde{\mathcal{G}}_1$.

- 加密算法. $F.Enc(1^\lambda,x,m,pp)\rightarrow CT$: 输入安全参数 1^λ, 命题实例 $x\in\mathcal{X}$, 明文消息 $m\in\mathcal{M}$, 加密密钥 pp, 加密方法和离线证据加密算法相同, 首先生成对称加密密钥 k 的两个密文 CT_1 和 CT_2, 并用密钥 k 加密明文消息 m 和命题实例 x 得到密文 CT_3, 然后计算非交互证据不可区分的证明 π, 最后输出 $CT=(CT_1,CT_2,CT_3,\pi,x)$.

- 解密算法. $F.Dec(CT,w,sk_f)\rightarrow m$ or $\perp$: 输入密文 CT, 证据 $w\in\mathcal{W}$ 和解密密钥 sk_f, 计算 $f(\tilde{m},w)=\tilde{\mathcal{G}}_1(CT,w)$.

(1) 正确性. 正确性和离线证据加密方案类似, 电路 $\widetilde{\mathcal{G}_1}$ 输入正确生成的密文 $CT=(CT_1,CT_2,CT_3,\pi,x)$, 如果满足 $NIWI.V(crs,y,\pi)=1$ 且 $(\tilde{x}=x)\wedge\mathcal{R}(x,w)=1$ 成立, 则解密算法输出 $f(\tilde{m},w)$.

(2) 算法的时间复杂度. 上述构造的离线函数证据加密方案的初始化算法和密钥生成算法的时间复杂度类似于离线证据加密的初始化算法, 不同的是在密钥生成阶段我们将函数 f 嵌入到了电路 $\mathcal{G}_1$ 中, 密钥生成算法的时间复杂度为 $O(|\mathcal{G}_1|)$. 初始化算法需要计算两公钥加密的密钥生成算法, 证据不可区分证明的公共参考串以及一个长度为 *len* 的 0 串的承诺, 我们仍然采用 ElGamal 加密算法和 Groth-Sahai 证明系统[29], 算法的时间复杂度为 $O(\lambda)$. 加密算法和解密算法的时间复杂度与离线证据相同.

输入: (CT, w)

嵌入: sk_1, f, pk_1, pk_2

1. $CT=(CT_1, CT_2, CT_3, \pi, x)$;
2. 如果 $NIWI.V(crs, y, \pi)\neq 1$, 则输出 $\perp$; 否则执行下一步;
3. 计算 $PKE.Dec(sk_1, CT_1)=k$, $SE.Dec(k, CT_3)=(\tilde{x}, \tilde{m})$. 如果 $(\tilde{x}=x)\wedge R(x, w)=1$, 则输出 $f(\tilde{m}, w)$; 否则输出 $\perp$.

图 2 电路 $\mathcal{G}_1$ 描述

定理 2. 如果 PKE 是 CPA 安全的公钥加密方案, SE 为一个 CPA 安全的对称加密方案, Com 为完美绑定的承诺方案, $i\mathcal{O}$ 为不可区分的混淆, $NIWI$ 为证据不可区分的证明系统, 则构造的 $FOWE$ 方案满足适应性不可区分安全性 (具体见定义 9).

证明方法类似定理 1.

5 结 论

本文提出了一种完全适应安全的离线证据加密方案的构造方法. 通过 Naor-Yung 的双重加密机制结合密钥封装机制和证据不可区分的证明系统解决了选择安全性证明过程中需要敌手提前输出挑战密文和命题实例的问题, 从而解决了 Chvojka 等人[14]提出的“Open Problem”. 此外, 我们利用相同的方法构造了离线函数证据加密方案, 允许敌手多次询问解密密钥生成算法, 在挑战密文满足 $f_j(m_0,w)=f_j(m_1,w)$ 的情况下, 可以类似的证明该方案满足完全适应安全性.

References:

[1] Sahai A, Waters B. Fuzzy identity-based encryption. In: Proc. of the 24th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Aarhus: Springer, 2005. 457–473. [doi: 10.1007/11426639_27]

[2] Boyen X, Waters B. Anonymous hierarchical identity-based encryption (without random oracles). In: Proc. of the 26th Annual Int'l Conf. on Cryptology. Santa Barbara: Springer, 2006. 290–307. [doi: 10.1007/11818175_17]

[3] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. In: Proc. of the 13th ACM Conf. on Computer and Communications Security. Alexandria: ACM, 2006. 89–98. [doi: 10.1145/1180405.1180418]

[4] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. In: Proc. of the 14th ACM Conf. on Computer and Communications Security. Alexandria: ACM, 2007. 195–203. [doi: 10.1145/1315245.1315270]

[5] Shen E, Shi E, Waters B. Predicate privacy in encryption systems. In: Proc. of the 6th Int'l Conf. on Theory of Cryptography Conf. San Francisco: Springer, 2009. 457–473. [doi: 10.1007/978-3-642-00457-5_27]

[6] Katz J, Yerukhimovich A. On black-box constructions of predicate encryption from trapdoor permutations. In: Proc. of the 15th Int'l Conf. on Theory and Application of Cryptology and Information Security. Tokyo: Springer, 2009. 197–213. [doi: 10.1007/978-3-642-10366-7_12]

[7] Boneh D, Sahai A, Waters B. Functional encryption: Definitions and challenges. In: Proc. of the 8th Int'l Conf. on Theory of Cryptography Confere. Providence: Springer, 2011. 253–273. [doi: 10.1007/978-3-642-19571-6_16]

[8] Agrawal S, Wu DJ. Functional encryption: Deterministic to randomized functions from simple assumptions. In: Proc. of the 36th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Paris: Springer, 2017. 30–61. [doi: 10.1007/978-3-319-56614-

6_2]

[9] Liu MH, Zhang P. An adaptively secure functional encryption for randomized functions. The Computer Journal, 2020, 63(8): 1247–1258. [doi: 10.1093/comjnl/bxz154]

[10] Garg S, Gentry C, Sahai A, Waters B. Witness encryption and its applications. In: Proc. of the 45th Annual ACM Symp. on Theory of Computing. Palo Alto: ACM, 2013. 467–476. [doi: 10.1145/2488608.2488667]

[11] Bellare M, Hoang VT. Adaptive witness encryption and asymmetric password-based cryptography. In: Proc. of the 18th IACR Int'l Conf. on Practice and Theory in Public-Key Cryptography. Gaithersburg: Springer, 2015. 308–331. [doi: 10.1007/978-3-662-46447-2_14]

[12] Abusalah H, Fuchsbauer G, Pietrzak K. Offline witness encryption. In: Proc. of the 14th Int'l Conf. on Applied Cryptography and Network Security. Guildford: Springer, 2016. 285–303. [doi: 10.1007/978-3-319-39555-5_16]

[13] Pal T, Dutta R. Offline witness encryption from witness PRF and randomized encoding in CRS model. In: Proc. of the 24th Australasian Conf. on Information Security and Privacy. Christchurch: Springer, 2019. 78–96. [doi: 10.1007/978-3-030-21548-4_5]

[14] Chvojka P, Jager T, Kakvi SA. Offline witness encryption with semi-adaptive security. In: Proc. of the 18th Int'l Conf. on Applied Cryptography and Network Security. Rome: Springer, 2020. 231–250. [doi: 10.1007/978-3-030-57808-4_12]

[15] Boyle E, Chung KM, Pass R. On extractability obfuscation. In: Proc. of the 11th Theory of Cryptography Conf. San Diego: Springer, 2014. 52–73. [doi: 10.1007/978-3-642-54242-8_3]

[16] Garg S, Gentry C, Halevi S, Raykova M, Sahai A, Waters B. Candidate indistinguishability obfuscation and functional encryption for all circuits. In: Proc. of the 54th Annual IEEE Symp. on Foundations of Computer Science. Piscataway: IEEE Computer Society, 2013. 40–49. [doi: 10.1109/FOCS.2013.13]

[17] Goldwasser S, Kalai Y, Popa RA, Vaikuntanathan V, Zeldovich N. Reusable garbled circuits and succinct functional encryption. In: Proc. of the 45th ACM Symp. on Theory of Computing. Palo Alto: ACM, 2013. 555–564. [doi: 10.1145/2488608.2488678]

[18] Ananth P, Brakerski Z, Segev G, Vaikuntanathan V. From selective to adaptive security in functional encryption. In: Proc. of the 35th Annual Cryptology Conf. Santa Barbara: Springer, 2015. 657–677. [doi: 10.1007/978-3-662-48000-7_32]

[19] Abdalla M, Bourse F, de Caro A, Pointcheval D. Simple functional encryption schemes for inner products. In: Proc. of the 18th IACR Int'l Conf. on Practice and Theory in Public-Key Cryptography. Gaithersburg: Springer, 2015. 733–751. [doi: 10.1007/978-3-662-46447-2_33]

[20] Agrawal S, Libert B, Stehlé D. Fully secure functional encryption for inner products, from standard assumptions. In: Proc. of the 36th Annual Int'l Conf. on Cryptology. Santa Barbara: Springer, 2016. 333–362. [doi: 10.1007/978-3-662-53015-3_12]

[21] Goldwasser S, Gordon SD, Goyal V, Jain A, Katz J, Liu FH, Sahai A, Shi E, Zhou HS. Multi-input functional encryption. In: Proc. of the 33rd Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Copenhagen: Springer, 2014. 578–602. [doi: 10.1007/978-3-642-55220-5_32]

[22] Ananth P, Jain A. Indistinguishability obfuscation from compact functional encryption. In: Proc. of the 35th Annual Cryptology Conf. Santa Barbara: Springer, 2015. 308–326. [doi: 10.1007/978-3-662-47989-6_15]

[23] Brakerski Z, Komargodski I, Segev G. Multi-input functional encryption in the private-key setting: Stronger security from weaker assumptions. Journal of Cryptography, 2018, 31(2): 434–520. [doi: 10.1007/s00145-017-9261-0]

[24] Abdalla M, Gay R, Raykova M, Wee H. Multi-input inner-product functional encryption from pairings. In: Proc. of the 36th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Paris: Springer, 2017. 601–626. [doi: 10.1007/978-3-319-56620-7_21]

[25] Datta P, Okamoto T, Tomida J. Full-hiding (unbounded) multi-input inner product functional encryption from the *k*-linear assumption. In: Proc. of the 21st Int'l Conf. on Practice and Theory of Public-key Cryptography. Rio de Janeiro: Springer, 2018. 245–277. [doi: 10.1007/978-3-319-76581-5_9]

[26] Garg S, Gentry C, Halevi S, Wichs D. On the implausibility of differing-inputs obfuscation and extractable witness encryption with auxiliary input. Algorithmica, 2017, 79(4): 1353–1373. [doi: 10.1007/s00453-017-0276-6]

[27] Zhandry M. How to avoid obfuscation using witness PRFs. In: Proc. of the 13th Int'l Conf. on Theory of Cryptography. Tel Aviv: Springer, 2016. 421–448. [doi: 10.1007/978-3-662-49099-0_16]

[28] Jain A, Lin HJ, Sahai A. Indistinguishability obfuscation from well-founded assumptions. In: Proc. of the 53rd Annual ACM SIGACT Symp. on Theory of Computing. Istanbul: ACM, 2021. 60–73. [doi: 10.1145/3406325.3451093]

[29] Groth J, Sahai A. Efficient non-interactive proof systems for bilinear groups. In: Proc. of the 27th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Istanbul: Springer, 2008. 415–432. [doi: 10.1007/978-3-540-78967-3_24]

[30] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In: Proc. of the 30th Annual Cryptology Conf. Santa Barbara: Springer, 2010. 465–482. [doi: 10.1007/978-3-642-14623-7_25]

刘牧华(1987－), 男, 博士, 讲师, 主要研究领域为信息安全, 密码学, 安全协议.

王琳(1986－), 女, 博士, 讲师, 主要研究领域为人工智能, 图像识别, 机器学习, 网络安全.

朱军龙(1982－), 男, 博士, 副教授, CCF 专业会员, 主要研究领域为优化理论, 机器学习.

邢玲(1978－), 女, 博士, 教授, 主要研究领域为信息安全, 网络隐私保护.

张明川(1977－), 男, 博士, 教授, CCF 专业会员, 主要研究领域为未来互联网, 工业互联网, 网络安全, 机器学习.

吴庆涛(1975－), 男, 博士, 教授, CCF 高级会员, 主要研究领域为网络与信息安全, 云计算与物联网, 智能信息处理.