软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2024,35(7):3482−3496 [doi: 10.13328/j.cnki.jos.006930]

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

完备的 IBE 密码学逆向防火墙构造方法*

赵 一[1], 刘 行[1], 明 洋[1], 杨 波[2]

[1](长安大学 信息工程学院, 陕西 西安 710064)

[2](陕西师范大学 计算机科学学院, 陕西 西安 710119)

通信作者: 明洋, E-mail: yangming@chd.edu.cn

摘　要: 斯诺登事件后, 以算法替换攻击为代表的后门攻击带来的威胁受到广泛关注. 该类攻击通过不可检测的篡改密码协议参与方的算法流程, 在算法中嵌入后门来获得秘密信息. 为协议参与方配置密码学逆向防火墙(cryptographic reverse firewall, CRF)是抵抗算法替换攻击的主要手段. 基于身份加密(identity-based encryption, IBE)作为一种广泛应用的公钥加密体制, 亟需构建合适的 CRF 方案. 然而, 已有工作仅实现了 CRF 再随机化的功能, 忽视了将用户私钥直接发送给作为第三方的 CRF 的安全风险. 针对上述问题, 首先给出适用于 IBE 的 CRF 安全性质的形式化定义和安全模型. 其次提出可再随机化且密钥可延展的无安全信道 IBE (rerandomizable and key-malleable secure channel free IBE, RKM-SFC-IBE)的形式化定义并给出传统 IBE 转化为 RKM-SFC-IBE 以及增加匿名性的方法. 最后基于 RKM-SFC-IBE 给出对应 CRF 的一般性构造方法, 并给出标准模型下 IBE 方案的 CRF 构造实例与性能优化方法. 与已有工作相比, 提出完备的适用于 IBE 的 CRF 安全模型, 给出一般构造方法, 明确为表达力更强的加密方案构造 CRF 时的基本原则.

关键词: 算法替换攻击; 密码学逆向防火墙; 无安全信道的基于身份加密; 安全保持性

中图法分类号: TP309

中文引用格式: 赵一, 刘行, 明洋, 杨波. 完备的IBE密码学逆向防火墙构造方法. 软件学报, 2024, 35(7): 3482–3496. http://www.jos.org.cn/1000-9825/6930.htm

英文引用格式: Zhao Y, Liu H, Ming Y, Yang B. Construction Method of Complete Cryptographic Reverse Firewall for IBE. Ruan Jian Xue Bao/Journal of Software, 2024, 35(7): 3482–3496 (in Chinese). http://www.jos.org.cn/1000-9825/6930.htm

Construction Method of Complete Cryptographic Reverse Firewall for IBE

ZHAO Yi[1], LIU Hang[1], MING Yang[1], YANG Bo[2]

[1](School of Information Engineering, Chang'an University, Xi'an 710054, China)

[2](School of Computer Science, Shaanxi Normal University, Xi'an 710119, China)

Abstract: Since the Snowden revelations, threats from backdoor attacks represented by algorithm substitution attack (ASA) have been widely concerned. This kind of attack subverts the process of the algorithm that tampers with the cryptographic protocol participants in an undetectable manner, which embeds backdoors to obtain secrets. Building a cryptographic reverse firewall (CRF) for protocol participants is a well-known and feasible approach against ASA. Identity-based encryption (IBE), as a quite applicable public key infrastructure, has vital importance to be protected by appropriate CRF schemes. However, the existing work only realizes the CRF re-randomization, ignoring the security risk of sending users' private keys directly to the third-party CRF. Given the above problem, the formal definition and security model of security properties of CRF applicable to IBE are proposed. Then, the formal definition of rerandomizable and key-malleable secure channel free IBE (RKM-SCF-IBE) and the method of transforming traditional IBE to RKM-SFC-IBE are presented. In addition, an approach to increasing anonymity is also given. Finally, a generic provably secure framework of CRF construction for IBE is proposed based on RKM-SFC-IBE, with several instantiations from classic IBE schemes in the standard model and simulation results with

* 基金项目: 国家自然科学基金 (62072054, U2001205, 61772326, 61802241, 61802242); 陕西省重点研发计划 (2021GY-047, 2022GY-032)
收稿时间: 2022-11-15; 修改时间: 2023-01-01, 2023-02-09; 采用时间: 2023-03-06; jos 在线出版时间: 2023-08-23
CNKI 网络首发时间: 2023-08-28

optimization methods. Compared with existing work, the proposed scheme is proven secure under a more complete security model with a generic approach to building CRF for IBE schemes and clarifies the basic principles when constructing CRF for more expressive encryption schemes.

Key words: algorithm substitution attack; cryptographic reverse firewall (CRF); secure channel free identity-based encryption; security preserving

2013 年棱镜门事件的爆发, 将美国国家安全局利用后门攻击实施大范围监控的事实展示在大众面前. 该类攻击通过在参数或者随机数中嵌入后门, 在用户难以察觉的情况下窃取秘密信息, 超出了传统密码学研究的范围. 自此后门攻击及相关抵抗方法成为热门研究领域[1,2].

算法替换攻击 (algorithm substitution attack, ASA) 是通过木马等手段, 篡改算法执行方算法流程来获取秘密信息的后门攻击方式. 已有研究给出了针对对称加密[3]、公钥加密[4]和数字签名[5,6]的算法替换攻击方法. 由于 ASA 具备不可检测性, 因此攻击手段主要是在随机化算法的随机数选择阶段, 以特定分布选择随机数或者嵌入伪随机的后门. 针对这一特点, Bellare 等人[7]提出使用确定性的密码原语来抵抗 ASA. 然而, 确定性算法在功能性和传统安全性上有其内在的劣势, 比如确定性公钥加密在传统安全性意义上不具备抵抗选择明文攻击 (chosen plaintext attack, CPA) 的安全性.

为密码协议参与方配置密码学逆向防火墙 (cryptographic reverse firewall, CRF)[8]是目前广泛使用的随机化算法抵抗算法替换攻击的方法之一. 所谓“逆向”, 是指相比抵御外界有害信息的传统防火墙, CRF 是防止受到 ASA 攻击的参与方发出带有秘密的信息. 具体来说, 将参与方发出的消息再随机化后才发出, 导致植入的后门或者非均匀的随机数就会被均匀化处理而不会泄露信息. 该技术路线的主要问题是高效再随机化原语的设计缺少一般化的方法, 因此需要针对每种随机化密码算法的特点单独设计 CRF. 目前公钥加密消息和密钥交换[9−11]、不经意传输[11]、数字签名[5]、交互式证明系统[12]等原语, 已经有了对应的 CRF 构造.

基于身份加密 (identity based encryption, IBE)[13]解决了传统公钥加密证书管理问题, 该机制中, 电话、邮箱等信息可以直接作为用户的公钥而不需要用户自己生成公钥. 然而, 算法替换攻击作为新的攻击方式, 其对于 IBE 机制的威胁与针对性防御仍然没有受到足够重视. 由于 IBE 在公司级别机构的网络架构中有着广泛应用, 对 ASA 攻击缺少抵抗手段将带来广泛的商业风险. 目前仅有少量工作对适用于 IBE 的逆向防火墙进行了初步研究. 为了系统地解决针对 IBE 的 ASA 问题, 需要对 ASA 在 IBE 不同于传统公钥加密的环节, 也就是身份私钥提取过程, 进行进一步研究, 给出较为完善的解决方案. 本文的具体贡献如下.

(1) 指出已有工作存在安全性不能保持的问题, 给出 IBE 机制中完备 CRF 构造的形式化安全模型, 重点刻画了身份私钥提取过程中用户私钥对 CRF 的保密性要求.

(2) 提出可再随机化且密钥可延展的无安全信道基于身份加密 (rerandomizable and key-malleable secure channel free IBE, RKM-SCF-IBE) 的定义与安全模型, 并给出从传统 IBE 方案到 RKM-SCF-IBE 的一般性转换方法.

(3) 提出 RKM-SCF-IBE 方案中的 CRF 构造并给出形式化证明. 该构造是目前最完备的用于 IBE 的 CRF, 可以抵抗恶意的 CRF, 且可扩展到匿名 IBE 中.

本文第 1 节介绍适用于 IBE 的逆向防火墙的研究现状并分析已有工作存在的问题. 第 2 节介绍需要用到的基础知识和安全模型. 第 3 节强调 IBE 的逆向防火墙应该满足的安全性质和模型. 第 4 节提出 RKM-SCF-IBE 定义与安全模型, 并给出从传统 IBE 方案到 RKM-SCF-IBE 的一般性转换方法. 第 5 节给出适用于 IBE 的逆向防火墙的具体构造并对其安全性进行证明. 第 6 节对本文方案进行实验仿真分析, 展示方案的实用性. 最后总结全文, 并对逆向防火墙技术未来的发展进行探讨.

1 相关研究

1.1 相关研究现状

IBE 作为广泛应用的密码学原语近年间发展迅速. Boneh 等人利用双线性对的性质, 在随机谕言机模型

(random oracle model, ROM) 下提出了第一个结构简单且实用的 IBE 机制[14]. 在标准模型下, Boneh 等人给出了选择安全的 IBE 构造[15], Waters 提出了全安全的 IBE 构造[16]. 之后有一系列 IBE 的研究工作集中在实现全安全性的紧规约上[17−19], 然而方案的基础框架依然来自文献 [15,16]. 近年, 有工作开始研究基于计算性假设的 IBE[20], 然而到目前为止仅有理论上的意义. 由上述可见, 适用于文献 [15,16] 中方案的逆向防火墙如果存在, 能够比较容易地扩展到适用于大多数 IBE 方案.

已有工作对逆向防火墙的构造, 一般直接使用可再随机化原语来实现再随机化功能. 文献 [9] 使用可再随机化的公钥加密来构造适用于消息传输协议的 CRF, 文献 [10] 同样利用可再随机化的公钥加密给出适用于无证书加密的 CRF. 文献 [5] 使用可再随机化的签名来构造适用于签名的 CRF. 文献 [11] 利用可延展的哈希证明系统作为基础原语, 给出了消息传输协议和不经意传输协议的逆向防火墙构造. 文献 [12] 通过可延展的 sigma 协议构造了适用于 IPsec 协议的逆向防火墙.

针对 IBE 的逆向防火墙构造, 文献 [21] 沿着公钥加密的框架尝试给出了适用于文献 [14] 中 IBE 方案的逆向防火墙. 同样的, 文献 [22] 提出了具有 CRF 的 CP-ABE 方案. 上述两个方案都能够实现 CRF 需要的密钥可延展和密文可再随机化的功能.

1.2 存在的问题

IBE、ABE 等机制相比传统公钥加密机制, 不同之处在于存在密钥生成中心 (private key generator, *PKG*) 这个角色. 在传统的 IBE 方案中, *PKG* 和用户之间通过安全信道来传输用户私钥. 而从 CRF 在协议中所扮演的角色来讲, 它并不是整体协议的可信参与方, 而是一个第三方协助角色[8]. 为 IBE 的参与方配置 CRF, 控制所有发出的消息, 实际上会导致 IBE 方案中不会再有安全信道的存在. 具体来说, IBE 只要考虑配置 CRF, 就难以避免在身份私钥提取过程中将本该只有 *PKG* 和用户双方知道的用户私钥发送给 CRF. 然而, CRF 对身份私钥的再随机化操作, 只能防止受到算法替换攻击的 *PKG* 发出非法信息, 但是身份私钥的有效性不随再随机化而改变. 通过身份私钥提取过程, CRF 获得了原本在安全信道中发送的用户身份私钥等秘密信息. 因此, 应当为身份私钥设计在公开信道中安全发送的方法, 从而使得 CRF 不能直接得到身份私钥本身. 上述方案中, 文献 [21] 没有考虑 *PKG* 受到后门攻击时需要配置防火墙的问题; 文献 [22] 在身份私钥提取阶段, *PKG* 将用户私钥直接交给 CRF, 实际上让 CRF 掌握了有效的用户私钥, 使得方案的安全性需要可信的 CRF 来保障. 这与 CRF 的安全性要求中, 系统安全性不依赖 CRF 的要求不符. 因此上述工作并没有给出完善的与 IBE/ABE 原语匹配的 CRF 解决方案. 目前也没有其他 CRF 相关工作解决 CRF 直接处理用户密钥的问题.

1.3 动机与思路

针对上述问题, 本文以构建完备的适用于 IBE 的 CRF 为目标, 基于 IBE 体制的自身特点, 设计适用于标准模型下安全方案的 CRF; 本文还将提炼一般性的构造方法, 模块化的解决 IBE 的 CRF 构造问题, 为将来构造 ABE, 函数加密等原语的 CRF 构造研究提供基本框架.

为避免传统 IBE 安全信道与 CRF 的安全性要求冲突的问题, 需要引入无安全信道 (secure channel free, SCF) 的 IBE 这一原语. 该原语中身份私钥提取过程是一个交互式协议, 允许身份私钥提取在公开信道进行的同时不泄露身份私钥, 即身份私钥以加密的方式公开发送. 由于 IBE 和公钥可搜索加密 (public key encryption with keyword search, PEKS) 之间可以互相转化的关系, SCF-IBE 实质上已经以 SCF-PEKS 的形式进行了研究[23−25], 主要用于防止外部敌手的离线关键字猜测攻击. 而考虑 ASA 环境下配置 CRF 时, 已有的 SCF-PEKS 方案中构造公开信道的方法并不能直接使用, 因为 CRF 要求可再随机化性质. 而且在 PEKS 环境中, 允许接收方设置长期公钥来加密, 而在 IBE 环境下, 用户设置长期公钥将会使得系统不再符合基于身份的概念.

基于上述需求, 本文提出 RKM-SCF-IBE 的定义, 其中身份私钥及其加密形式、密文都可以进行再随机化, 主密钥可以延展. 然后利用一次性的密文可再随机化和密钥可延展公钥加密, 对身份私钥进行加密给出从传统 IBE 方案到 RKM-SCF-IBE 的一般性转换方法. 这样 CRF 得到的是身份私钥的密文, 而不能得到身份私钥. 那么只要

该密文是密钥可延展和可再随机化的, 就可以构造出符合要求的 CRF. 其中, 密钥可延展性确保公钥在发送阶段被随机化后, 无法发出带后门信息的同时确保密钥的有效性. 密文可再随机化性确保密文发送过程中被随机化后, 无法在随机数中嵌入后门的同时确保密文对应明文不变. 另外, 在实例化的过程中, 本文给出了以再随机化替代部分加密的效率优化方案, 即用户本地解密得到身份私钥, 进行再随机化后使用, 从而可以不用对身份私钥中的随机数承诺项进行加密. 这一技巧也使得密文被随机化的同时, 密文对应的明文即身份私钥也被随机化, 使得 CRF 的构造更为简洁.

2 基础知识

2.1 逆向防火墙

设 $P=(trans,out)$ 是密码协议的参与方, m_r^P 表示 P 收到的消息, m_s^P 表示 P 发出的消息, m_o^P 表示协议结束后 P 的最终输出, $state_P$ 表示 P 的状态, 则有 $m_s^P=trans(m_r^P;state_P)$, $m_o^P=out(m_r^P,m_s^P;state_P)$.

定义 1. 逆向防火墙. 对于协议参与方 P, 如果一个算法 W 处理 P 发送和接收的消息, 且处理过的消息参与协议运行, 则 W 称作 P 的逆向防火墙, 称 $W\circ P$ 为复合参与方, 则 $m_r^P=W(m_r^{W\circ P};state_W)$, $m_s^{W\circ P}=W(m_s^P;state_W)$.

定义 2. 功能保持性. 如果 W 满足 $m_o^{W\circ P}=m_o^P$ 且 $m_o^{W\circ\ldots\circ W\circ P}=m_o^P$, 称 W 具有功能保持性.

定义 3. 安全保持性. 如果协议 $\mathcal{P}$ 满足安全性质 $\mathcal{S}$, 其中参与方 P 由 $W\circ P$ 代替, 当 P 受到任意敌手 ASA 攻击依然满足安全性质 $\mathcal{S}$, 称 W 是强安全保持的. 当 P 受到功能保持敌手 ASA 攻击, 仍满足安全性质 $\mathcal{S}$, 称 W 是弱安全保持的.

定义 4. 抗渗透性. 令 λ 是安全参数, P_1 和 P_2 是协议 $\mathcal{P}$ 的两个参与方, $\overline{P_i}$ 表示受到敌手 $\mathcal{A}$ 的 ASA 攻击后的参与方, T 为 P_1 和 P_2 在 $\mathcal{P}$ 中交互生成的文本, 定义游戏 $\mathrm{LEAK}(\mathcal{P},P_1,P_2,W,\lambda)$, 如图 1 所示.

$\left(\overline{P_1},\overline{P_2},input\right)\leftarrow\mathcal{A}\left(1^\lambda\right)$
$b\leftarrow_R\{0,1\}$
If $b=1$, $P^*\leftarrow W\circ\overline{P_1}$
Else, $P^*\leftarrow W\circ P_1$
$T^*\leftarrow\mathcal{P}_{P_1\to P^*,P_2\to\overline{P_2}}(input)$
$b^*\leftarrow\mathcal{A}\left(T^*,state_{\overline{P_2}}\right)$
Output $\left(b=b^*\right)$

图 1 抗渗透性的游戏

敌手 $\mathcal{A}$ 在上述游戏中的优势定义为: $Adv_{\mathcal{A},W}^{\mathrm{LEAK}}(\lambda)=\left|\Pr[\mathrm{LEAK}(\mathcal{P},P_1,P_2,W,\lambda)=1]-1/2\right|$.

如果不存在多项式时间敌手 $\mathcal{A}$ 在上述游戏中以不可忽略的优势获胜, 称逆向防火墙 W 是抗 P_1 向 P_2 渗透的.

如果不存在功能保持的多项式敌手 $\mathcal{A}$ 在上述游戏中以不可忽略的优势获胜, 称逆向防火墙 W 是弱抗 P_1 向 P_2 渗透的.

一般来说, 进行 ASA 攻击的敌手都是功能保持的, 否则容易被检测到, 因此多数场景可以使用弱安全保持和弱抗渗透的定义.

2.2 双线性映射

令 q 是素数, G 和 G_T 是 q 阶乘法循环群, g 是 G 的生成元. 则满足下列性质的映射 $e:G\times G\to G_T$ 称作双线性映射.

双线性: 对任意 $a,b\in\mathbb{Z}_q^*$, 有 $e(g^a,g^b)=e(g,g)^{ab}$.

非退化性: $e(g,g)\neq 1_{G_T}$.

可计算性: 对任意的 $P,Q\in G$, $e(P,Q)$ 可以在多项时间内计算.

本文剩余章节中记双线性映射的生成算法为 $\mathcal{G}$.

2.3 基于身份加密

2.3.1 形式化定义

定义 5. 一个 IBE 方案 Π 由算法四元组 (Gen, Ext, Enc, Dec) 构成, 具体算法描述如下.

$Gen(1^{\lambda}) \to (mpk, msk)$: 系统参数生成算法 Gen, 由 PKG 运行, 产生系统公共参数主公钥 mpk 和主私钥 msk.

$Ext(id, msk) \to sk_{id}$: 身份私钥提取算法 Ext, 由 PKG 运行, 生成用户的私钥 sk_{id}, 通过安全信道发送给身份为 id 的用户.

$Enc(m, id) \to C$: 加密算法 Enc, 由加密者运行, 生成密文 C.

$Dec(C, sk_{id}) \to m$: 解密算法 Dec, 由解密者运行, 输出明文 m.

本文使用的 IBE 构造需要具有密文密钥的可再随机化性和密钥可延展性, 其中:

密文可再随机化性即存在密文再随机化算法 $Rand_{\Pi}(C; r) = C'$ 满足 $Dec(C) = Dec(C')$. 该性质可使得随机化加密算法生成的密文, 在不解密的情况下转化为使用新的随机数生成的密文.

密钥可再随机化性即存在密钥再随机化算法 $Rand_{ikey}(sk_{id}; r) = sk'_{id}$. 该性质可使得随机化身份私钥提取算法生成的身份私钥, 不利用主私钥重新计算的情况下转化为使用新的随机数生成的身份私钥.

密钥可延展性包含两个算法, 一个是主公钥延展算法 $Maul_{mpk}(y) \to y'$, 该算法将公钥再随机化为另一个公钥; 另一个是身份私钥延展算法 $Maul_{sk_{id}}(sk_{id,y}) \to sk_{id,y'}$, 该算法将延展前主公钥对应的身份私钥转化为延展后主公钥对应的身份私钥. 注意到当延展后的主公钥 y' 公布之后, 身份私钥的延展算法是一个确定性算法. 因此该算法不能替代身份私钥本身的再随机化算法.

定义 6. 如果一个 IBE 方案中, 以上密文密钥再随机化算法和密钥延展算法都成立, 则算法元组 $\Pi = (Gen, Ext, Enc, Dec, Rand_{\Pi}, Rand_{ikey}, Maul_{mpk}, Maul_{sk_{id}})$ 被称为 RKM-IBE 方案.

2.3.2 经典 IBE 构造

标准模型下 IBE 方案中, 只需要改变身份的编码方式, 可以得到不同的 IBE 方案. 设身份 id 的编码为 $F(id)$. 当 $Gen(1^{\lambda})$ 选择两个随机群元素 u, h 并定义 $F(id) = u^{id}h$ 时, 以下构造为文献 [15] 中的方案. 当 $Gen(1^{\lambda})$ 中选择多个公开参数 $(u_1, \ldots, u_{|id|})$, 并定义 $F(id) = h\prod_{i=1}^{|id|} u_i^{id(i)}$ 时, 以下构造是文献 [16] 中的方案.

$Gen(1^{\lambda})$: $\mathcal{G}(1^{\lambda}) = (q, g, G, G_T, e(\cdot,\cdot))$, 其中 G 和 G_T 是 q 阶乘法循环群, g 是 G 的生成元. 随机选择 $\alpha \in \mathbb{Z}_q$, 则 $mpk = (q, g, F, y = e(g,g)^{\alpha})$, $msk = \alpha$.

$Ext(id, msk)$: 随机选择 $r \in \mathbb{Z}_q$, 计算 $sk_{id} = (k_1, k_2) = (g^r, g^{\alpha}F^r(id))$.

$Enc(m, id)$: 随机选择 $s \in \mathbb{Z}_q$, 计算 $C = (c_1, c_2, c_3) = (g^s, F^s(id), y^s m)$.

$Dec(C, sk_{id})$: $y^s = e(k_2, c_1)/e(k_1, c_2)$, $m = c_3/y^s$.

上述构造满足 RKM-IBE 方案的性质, 下面给出上述构造的密文密钥再随机化算法、主公钥与用户私钥的密钥延展算法.

$Rand_{\Pi}(C; s')$: 随机选择 $s' \in \mathbb{Z}_q$, $C' = (c_1 g^{s'}, c_2 F^{s'}(id), c_3 y^{s'} m)$.

$Rand_{ikey}(sk_{id}; r')$: 随机选择 $r' \in \mathbb{Z}_q$, $sk'_{id} = (k_1 g^{r'}, k_2 F^{r'}(id))$.

$Maul_{mpk}(y; \gamma)$: $y' = y^{\gamma}$.

$Maul_{sk_{id}}(sk_{id,y}; \gamma)$: $sk_{id,y'} = (k_1^{\gamma}, k_2^{\gamma})$.

2.4 密文可再随机化与密钥可延展的公钥加密

定义 7. 如果对一个公钥加密方案 $PE = (G(1^{\lambda}) = (pk, sk), E(pk, m) = C, D(sk, C) = m)$, 存在再随机化算法 $Rand_{PE}$、$Maul_{key}$、$Maul_C$ 满足:

$Rand_{PE}(C) = C'$ 且 $D(sk, C) = D(sk, C')$,

$Maul_{key}(pk, sk) = (pk', sk')$,

$Maul_C(C_{pk}) = C'_{pk'}$ 且 $D(sk, C_{pk}) = D(sk', C'_{pk'})$,

则 PE 被称为 RKM-PKE 方案.

3 IBE 中 CRF 的性质与系统模型

3.1 安全独立性

IBE 中逆向防火墙除了满足定义 1–定义 4 外, 还应满足安全独立性, 即逆向防火墙作为不可信第三方不能直接获得协议的秘密信息. 一般性的定义 4 中, 仅强调参与方之间的抗渗透, 对 CRF 自身对协议的安全性影响的要求并没有体现, 而这对于 IBE 的 CRF 来说尤为关键. 没有安全独立性, 安全保持性事实上也无法获得, 即本身具备特定安全性的方案配置逆向防火墙后, 仅对逆向防火墙之外的敌手保持安全性.

定义 8. 安全独立性. IBE 方案 Π 中, 接收者身份为 id, 发送者 S, 定义形式化游戏 $\mathrm{IND}(\Pi,\mathrm{PKG},S,id,\lambda)$ 如图 2, 其中 U_m 是消息空间上的均匀分布.

$(W_{PKG},W_S,W_{id})\leftarrow\mathcal{A}(1^\lambda)$
$PKG\leftarrow W_{PKG}\circ PKG$
$S\leftarrow W_S\circ S$ $User_{id}\leftarrow W_{id}\circ User_{id}$
$m^*\leftarrow\mathcal{A}$ $b\leftarrow_R\{0,1\}$
If $b=0$, $C^*=Enc(m^*)$
Else, $C^*=Enc(U_m)$
$b^*\leftarrow\mathcal{A}(C^*,state_{W_{PKG},W_S,W_{id}})$
Output $b=b^*$

图 2 安全独立性的游戏

敌手 $\mathcal{A}$ 在上述游戏中的优势定义为: $Adv_{\mathcal{A}}^{\mathrm{IND}}(\lambda)=|\Pr[\mathrm{IND}(\Pi,PKG,S,id,\lambda)=1]-1/2|$.

如果任意多项式时间敌手 $\mathcal{A}$ 在上述游戏中的优势都是可忽略的, 则称方案 Π 具备独立于逆向防火墙的安全性.

容易验证文献 [21,22] 中的 CRF 方案并不满足该性质, CRF 拥有用户私钥使得方案的安全性必须依赖于 CRF 的可信性. 在 CRF 不可信的情况下, 安全保持性必须以安全独立性为前提.

3.2 系统模型

IBE 方案的安全独立性主要体现在身份私钥提取阶段, 本文将分为两阶段阐述 CRF 在 IBE 中的配置及其作用.

(1) 身份私钥提取阶段

本阶段为用户与 PKG 的交互过程. 用户向 PKG 提交身份与辅助信息, PKG 给用户发送私钥, 该过程中 PKG 和用户均需要配置 CRF 处理发出的消息. esk 是身份私钥的封装, CRF 不能从中得到 sk_{id} 的信息; aux 是辅助信息, 用以帮助用户从 esk 中恢复 sk_{id}. 具体模型见图 3.

(2) 消息发送阶段

本阶段为发送者加密消息, 接收者使用身份私钥解密的过程. 在 IBE 中, 公钥是确定性的身份, 接收者不向发送者发送任何消息, 因此该阶段接收者不需要 CRF 处理任何信息, 只有发送者端需要通过 CRF 处理发出的密文. 具体模型见图 4.

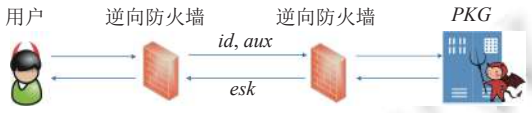

图 3 身份私钥提取模型

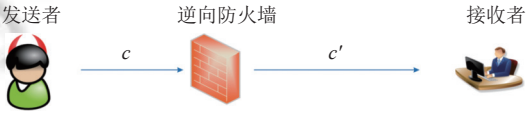

图 4 消息发送

4 RKM-SCF-IBE

一般 IBE 方案直接配置 CRF 后不具备安全独立性, 因此需要具备额外性质的 IBE 方案作为基础模块来构建完备的适用于 IBE 的 CRF. 本节首先给出 RKM-SCF-IBE 的定义, 然后给出基于常见经典 RKM-IBE 方案构造

RKM-SCF-IBE 方案的通用方法, 并证明方案满足所需性质.

4.1 定 义

定义 9. RKM-SCF-IBE 方案 Π_{RSCF} 由算法元组 (GEN, $EnExt$, $DeExt$, ENC, DEC, $RAND_{esk}$, $RAND_C$, $MAUL_{mpk}$, $MAUL_{esk}$, $MAUL_{aux}$, $MAUL_{esk,aux}$) 构成, 算法具体描述如下.

$GEN(1^\lambda) \to (mpk, msk)$: 与定义 5 相同.

$EnExt(id, msk; aux) \to esk_{id}$: 封装私钥算法 $EnExt$, 由 PKG 运行, 生成用户的身份私钥 sk_{id} 的密文 esk_{id}, 通过公开信道发送给用户 id. 这里 aux 是用户向 PKG 申请身份私钥时发送的辅助信息.

$DeExt(esk_{id}; aux) \to sk_{id}$: 身份私钥提取算法 $DeExt$, 由用户运行, 得到的身份私钥 sk_{id}.

$ENC(m, ID) \to C$: 与定义 5 相同.

$DEC(C, sk_{id}) \to m$: 与定义 5 相同.

$RAND_{esk}(esk_{id}) \to esk'_{id}$: 私钥封装的再随机化算法, 由 CRF 运行, 满足 $DeExt(esk'_{id}; aux) = sk'_{id}$.

$RAND_C(C) \to C'$: 密文再随机化算法, 满足 $DEC(C, sk_{id}) = DEC(C', sk'_{id})$.

$MAUL_{mpk}(mpk; r) \to mpk'$: 主公钥延展算法.

$MAUL_{esk}(esk_{id,mpk}; r) \to esk_{id,mpk'}$: 封装主公钥延展算法.

$MAUL_{aux}(aux) \to aux'$: 辅助信息延展算法

$MAUL_{esk,aux}(esk_{id,aux}; r) \to esk_{id,aux'}$: 封装辅助信息延展算法.

需要注意的是, 上述算法中, 由于身份私钥是可随机化的, $RAND_{esk}$ 不要求对应身份私钥不变, 只需满足是有效私钥即可. $RAND_C$ 要求密文再随机化后对应明文不变.

定义 10. 如果方案 Π_{RSCF} 中, 各密文再随机化算法和密钥延展算法都成立, 且 esk_{id} 是 sk_{id} 的安全封装, 则 Π_{RSCF} 是一个 RKM-SCF-IBE 方案.

4.2 通用构造

本节将给出基于 RKM-IBE 方案构造 RKM-SCF-IBE 的一般性方法.

给定 RKM-IBE 方案 $\Pi = (Gen, Ext, Enc, Dec, Rand_\Pi, Rand_{ikey}, Maul_{mpk}, Maul_{sk_{id}})$ 和 RKM-PKE 方案 $PE = (G, E, D, Rand_{PE}, Maul_{key}, Maul_C)$, RKM-SCF-IBE 方案 Π_{RSCF} 构造如下.

$GEN(1^\lambda)$: 与 Gen 相同, 输出 (mpk, msk).

$EnExt(id, msk; aux): G(1^\lambda) = (tpk, tsk), aux = tpk, esk_{id} = E_{tpk}(Ext(id, msk))$.

$DeExt(esk_{id}; tsk): sk_{id} = D_{tsk}(esk_{id})$.

$ENC(mpk, m, ID): C = Enc(mpk, m, id)$.

$DEC(C, sk_{id}): m = Dec(sk_{id}, C)$.

$RAND_{esk}(esk_{id}): esk'_{id} = Rand_{PE}(esk_{id}) = Rand_{PE}(E_{tpk}(Rand_{ikey}(Ext(id, msk))))$.

$RAND_C(C): C' = Rand_\Pi(C)$.

$MAUL_{mpk}(mpk; r): mpk' = Maul_{mpk}(mpk; r)$.

$MAUL_{esk}(esk_{id,mpk}; r): esk_{id,mpk'} = Rand_{PE}(E_{tpk}(Maul_{sk_{id}}(sk_{id,mpk}; r)); r)$.

$MAUL_{aux}(aux): aux' = Maul_{key}(aux)$.

$MAUL_{esk,aux}(esk_{id,aux}; r): esk_{id,aux'} = Maul_C(esk_{id,aux}; r)$.

定理 1. 如果 RKM-PKE 方案 PE 是 CPA 安全的, 则上述构造 Π_{RSCF} 是 RKM-SCF-IBE 方案.

证明过程可简述如下, 密文可再随机化性质和密钥可延展性质直接从基础方案 Π 继承而来. esk_{id} 是 PE 的密文, 由其 CPA 安全性可以直接得到结论.

4.3 实例化与性能优化

基于第 4.2 节给出的一般性构造方法, 本节使用第 2.3.2 节中经典 IBE 构造作为 RKM-IBE 的实例, 使用 ElGamal

加密方案作为 RKM-PKE 方案的实例给出一个具体的实现, 并基于此实例进行后续的仿真, 具体方案如下.

$GEN(1^\lambda): Gen(1^\lambda)=(q,g,G,G_T,e(\cdot,\cdot)), mpk=y=e(g,g)^\alpha, msk=\alpha$.

$EnExt(id,msk;aux): G(1^\lambda)=(tpk=h=g^x, tsk=x), aux=tpk, sk'_{id}=Ext(id,msk)=(k'_1,k'_2)=(g^s,g^\alpha F^s(id))$,

$esk_{id}=(c_1,c_2,k'_1)=(g^r,h^r k'_2,k'_1)$.

$DeExt(esk_{id};tsk): sk_{id}=(k_1,k_2)$, 其中 $k_1=g^{s+s'}$, $k_2=c_1^{-x}c_2F^{s'}(id)=g^\alpha F^{s+s'}(id)$.

$ENC(mpk,m,ID): C=(c_1,c_2,c_3)=(g^t,F^t(id),y^t m)$.

$DEC(C,sk_{id}): m=c_3 e(k_1,c_2)/e(k_2,c_1)$.

$RAND_{esk}(esk_{id}): esk'_{id}=(c_1 g^r, c_2 h^r F^{s'}(id), k'_1 g^{s'})$.

$RAND_C(C): C'=(c_1 g^{t'}, c_2 F^{t'}(id), c_3 y^{t'})$.

$MAUL_{mpk}(mpk;r): mpk'=y^r$.

$MAUL_{esk}(esk_{id,mpk};r): esk_{id,mpk'}=(c_1^r,c_2^r,(k'_1)^r)$.

$MAUL_{aux}(aux): aux'=tpk^r=g^{rx}$.

$MAUL_{esk,aux}(esk_{id,aux};r): esk_{id,aux'}=(c_1^r,c_2,k'_1)$.

需要注意的是, $EnExt(id,msk;aux)$ 算法中, esk_{id} 只加密了 sk'_{id} 的第 2 项. 而按照第 4.2 节的构造, 应该给出两套公钥系统将 sk'_{id} 全部加密. 这里是给出了一个实现中的效率优化, 由于 k'_1 是一个随机生成的承诺项, 本身是均匀分布的, 因此用户得到身份私钥 sk'_{id} 之后只需要做再随机化, 敌手就不能从 k'_1 得到 sk_{id} 的任何信息. 即这里用一次再随机化计算替代了一次加密的运算与一个群元素的空间. 该优化带来的另一个优势是使得密文再随机化的同时随机化了明文, 简洁地在不解密的情况下实现了对密文对应明文再随机化的功能.

为了更清楚地阐述方案的构造, 以下分阶段说明各个算法的作用.

阶段 1. 身份私钥提取阶段 (图 5).

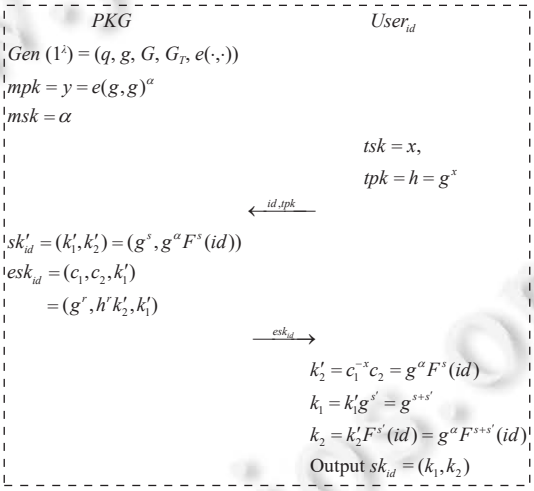

图 5 身份私钥提取

阶段 2. 消息发送阶段 (图 6).

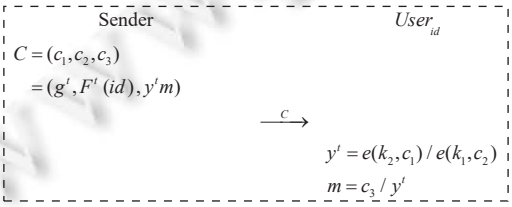

图 6 消息发送

该阶段与传统 IBE 的步骤相同.

4.4 匿名的身份私钥提取

扩展第 4.3 节身份私钥提取阶段的协议流程, 就可以得到具有匿名性的协议. 具体见图 7.

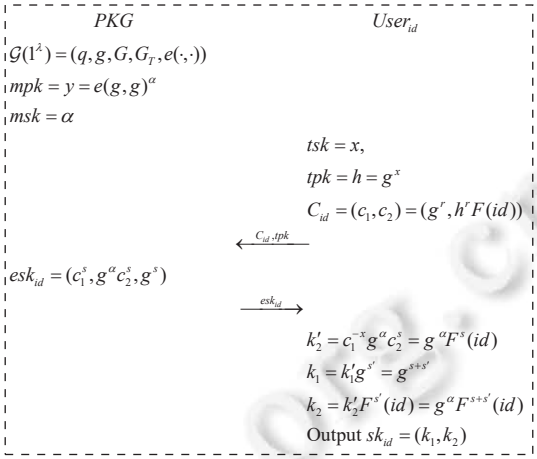

图 7 匿名身份私钥提取

5 IBE 的 CRF 构造

基于 RKM-SCF-IBE, 本节给出带 CRF 的 IBE 的具体构造 $\Pi_{\text{CRF-IBE}}$.

5.1 *PKG* 的 CRF

实际环境中, 在 ASA 攻击下被篡改的 *PKG* 有两种方式泄露秘密信息. 一是选择带后门的主公钥公开发送, 使得敌手能够通过后门得到主私钥的信息. 二是生成带后门的身份私钥, 向申请私钥的用户 (可能被敌手收买) 泄露信息. 因此, 抗 *PKG* 渗透且具有安全独立性的 CRF, 需要对主公钥进行随机化延展, 并且将用户私钥的密文进行随机化以及密钥延展后再发送给用户. 这样, 即使 *PKG* 选择的初始主公钥和给用户发送的私钥都是不安全的, CRF 都能够保障该 IBE 方案是 CPA 安全的. 另外, 对于 CRF 而言, 只要 CRF 是功能保持的, 即使 CRF 是好奇的敌手, IBE 方案对 CRF 也是 CPA 安全的, 即 CRF 不能获得任何主密钥或者用户私钥信息.

给定第 4.3 节的方案 $\Pi_{\text{RKM-SCF}}$, *PKG* 的 CRF W_{PKG} 具体构造见图 8.

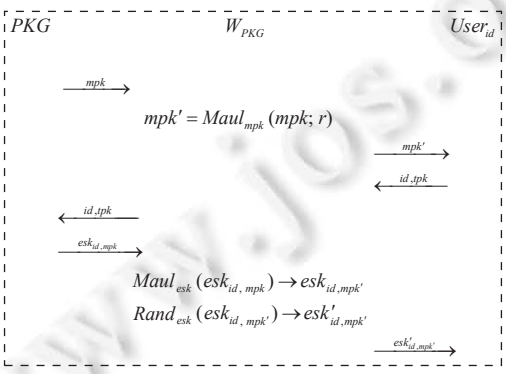

图 8 *PKG* 的 CRF 构造

定理 2. 如果 $\Pi_{\text{RKM-SCF}}$ 是一个 RKM-SCF-IBE 方案, 上述 CRF 构造对 *PKG* 功能保持、安全独立、安全性保持, 且弱抵抗 *PKG* 向外界和用户的渗透.

证明:

(1) 功能保持性

PKG 的功能是发送身份私钥, 因此只需验证最终用户得到的身份私钥是对应延展后公钥的合法身份私钥即可.

$mpk' = MAUL_{mpk}(mpk;r) = y^r = e(g,g)^{\alpha r}$.

$sk_{id,mpk} = (k_1,k_2) = (g^s, g^\alpha F^s(id))$.

$esk_{id} = (c_1, h^{r_1}k_2, k_1)$.

$MAUL_{esk}(esk_{id,mpk};r) = esk_{id,mpk'} = (c_1^r, c_2^r, k_1^r)$.

$RAND_{esk}(esk_{id,mpk'};r_2,s') = esk'_{id,mpk'} = (c_1^r g^{r_2}, c_2^r h^{r_2} F^{s'}(id), k_1^r g^{s'})$.

$DeExt(esk'_{id,mpk'};tsk) = (g^{sr+s'}, g^{\alpha r} F^{sr+s'}(id)) = sk_{id,mpk'}$.

由上可知, 用户得到的是合法的身份私钥.

(2) 抗渗透性

设 $\mathcal{A}$ 是定义 4 中游戏 $\mathrm{LEAK}(\mathcal{P}, PKG, User_{id}, W_{PKG}, \lambda)$ 的敌手, 则构造算法 B 以 $\mathcal{A}$ 为子进程判断 esk_{id} 是否是由受到攻击的参与方生成.

在 $\mathrm{LEAK}(\mathcal{P}, PKG, User_{id}, W_{PKG}, \lambda)$ 中, $\mathcal{A}$ 给出两个受到篡改的参与方 $\overline{PKG}$ 和 $\overline{User_{id}}$. B 首先运行诚实的复合参与方 $W_{PKG} \circ PKG$ 与 $\overline{User_{id}}$ 的私钥提取协议, 得到协议文本中身份私钥的密文 $esk_{id,0}$, 运行被篡改的复合参与方 $W_{PKG} \circ \overline{PKG}$ 与 $\overline{User_{id}}$ 的私钥提取协议, 得到协议文本中身份私钥的密文 $esk_{id,1}$. B 随机选择 $b \in \{0,1\}$, 将 $esk_{id,b}$ 发送给 $\mathcal{A}$, $\mathcal{A}$ 输出猜测 b^*.

由于 W_{PKG} 的再随机化操作, $esk_{id,0}$ 和 $esk_{id,1}$ 的分布相同, $\mathcal{A}$ 猜测的优势为 0. 因此 W_{PKG} 是抗渗透的.

(3) 安全独立性

当 W_{PKG} 是敌手时, 由于方案是 SCF 的, 即 W_{PKG} 看到的是身份私钥的密文, 因此无法获得身份私钥的信息. 由此可得方案安全性与 W_{PKG} 是独立的.

(4) 安全保持性

由上述性质可知, 可知 W_{PKG} 是弱安全保持的, 即系统在功能保持敌手 $\overline{PKG}$ 存在时依然保持原 IBE 系统的 CPA 安全性.

证毕.

5.2 用户端的 CRF

在 IBE 系统中, 用户仅在身份私钥提取阶段向 *PKG* 发起私钥提取申请, 因此用户端的 CRF 仅在该阶段处理用户发出的信息. 一个 ASA 敌手只能通过选择带有后门的临时公钥来泄露信息. 为了防止渗透, CRF 需要对公钥进行再随机化, 再对 *PKG* 发送的密文进行密钥延展, 将密文恢复为初始公钥所加密的密文, 否则用户不能解密, 即不满足功能保持的要求. 和 *PKG* 的 CRF 不同, 由于用户不掌握 PKG 的秘密信息, 因此任意篡改用户的算法都不会让敌手获得传递密文中的明文, 即用户的 CRF 可以强抵抗用户对外界的渗透.

给定第 4.3 节的方案 $\Pi_{\mathrm{RKM\text{-}SCF}}$, 用户端的 CRF W_{id} 具体构造见图 9.

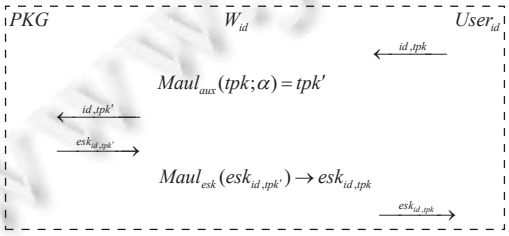

图 9 用户端的 CRF 构造

定理 3. 如果 $\Pi_{\text{RKM-SCF}}$ 是一个 RKM-SCF-IBE 方案, 则上述 CRF 构造对用户 $User_{id}$ 是功能保持、安全性独立、安全性保持, 且强抵抗用户向外界和用户的渗透.

证明:

(1) 功能保持性

用户在私钥提取阶段的功能是接收身份私钥, 因此只需验证最终用户能得到正确的身份私钥即可.

$aux' = Maul_{key}(tpk;r) = h' = h^r$.

$sk_{id,mpk} = (k_1,k_2) = (g^s, g^{\alpha}F^s(id))$.

$esk'_{id} = (c_1,c_2,k_1) = (g^{rr_1},(h')^{r_1}k_2,k_1)$.

$MAUL_{esk,aux}(esk_{id,aux'};r^{-1}) = esk_{id,aux} = (c_1^{r^{-1}},c_2,k_1)$.

$DeExt(esk_{id,aux};tsk) = sk_{id,aux}$.

由上可知, 用户得到的的确是合法的身份私钥.

(2) 抗渗透性

设 $\mathcal{A}$ 是定义 4 中游戏 LEAK($\mathcal{P},User_{id},PKG,W_{id},\lambda$) 的敌手, 我们构造算法 B 以 $\mathcal{A}$ 为子进程判断 aux_{id} 是否是由受到攻击的参与方生成.

在 LEAK($\mathcal{P},User_{id},PKG,W_{id},\lambda$) 中, $\mathcal{A}$ 给出两个受到篡改的参与方 $\overline{User_{id}}$ 和 $\overline{PKG}$. B 首先运行诚实的复合参与方 $W_{id}\circ User_{id}$ 与 $\overline{PKG}$ 的私钥提取协议, 得到协议文本中的临时公钥记为 $aux_{id,0}$, 然后运行被篡改的复合参与方 $W_{id}\circ\overline{User_{id}}$ 与 $\overline{PKG}$ 的私钥提取协议, 得到协议文本中的临时公钥记为 $aux_{id,1}$. B 随机选择 $b\in\{0,1\}$, 将 $aux_{id,b}$ 发送给 $\mathcal{A}$, $\mathcal{A}$ 输出猜测 b^*.

由于 W_{id} 的再随机化操作, $aux_{id,0}$ 和 $aux_{id,1}$ 的分布相同, $\mathcal{A}$ 猜测的优势为 0. 因此 W_{id} 是抗渗透的.

(3) 安全独立性

当 W_{id} 是敌手时, 由于方案是 SCF 的, 即 W_{id} 仅得到的是身份私钥的密文, 因此无法获得身份私钥的信息. 由此可得方案安全性与 W_{id} 是独立的.

(4) 安全保持性

由上述性质可知, 由于 $User_{id}$ 不掌握任何秘密信息, 仅能通过 aux 泄露与 IBE 无关的非法信息, 因此 W_{id} 是强安全保持的, 即系统对任意敌手 $\overline{User_{id}}$ 都可以保持原 IBE 系统的 CPA 安全性.

证毕.

5.3 发送端的 CRF

密文发送者作为明文的持有者, 没有 CRF 能够抵抗任意的算法篡改泄露信息, 必须要求篡改后的算法是功能保持的, 因此只能做到弱抗渗透. 密文发送者只有通过在密文的随机数中设置后门来泄露信息, CRF 只需要再随机化发出的密文即可, 具体构造见图 10.

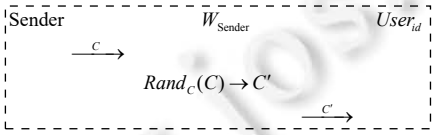

图 10 发送端的 CRF 构造

定理 4. 如果 $\Pi_{\text{RKM-SCF}}$ 是一个 RKM-SCF-IBE 方案, 则上述 CRF 构造对发送者功能保持、安全独立且安全性保持, 且弱抵抗发送者向外界和用户的渗透.

证明:

(1) 功能保持性

发送者的功能是将明文发送给接收者, 因此只需验证 W_{Sender} 存在时用户依然能接收到密文即可.

$C = (c_1,c_2,c_3) = (g^s, F^s(id), y^s m)$.

$C' = Rand_C(C) = (g^{s+s'}, F^{s+s'}(id), y^{s+s'}m)$.

$Dec(sk_{id}, C') = m$.

(2) 抗渗透性

该部分证明与同样构造了发送者 CRF 的文献 [21] 相关证明类似. 此处不再赘述.

(3) 安全独立性

与定理 2,定理 3 相同, W_{Sender} 处理的是密文, 密文的 CPA 安全性对 W_{Sender} 依然成立, 因此方案的安全性和 W_{Sender} 是独立的.

(4) 安全保持性

由上述结论可知 W_{Sender} 是弱安全保持的, 即系统在功能保持敌手 $\overline{\text{Sender}}$ 存在时依然保持原 IBE 系统的 CPA 安全性.

证毕.

5.4 CRF 的安全独立性

定理 2–定理 4 说明给出的 CRF 能够在抵抗外部 ASA 敌手的基础上, 还分别具备各自的安全独立性, 即所提方案的安全性不依赖于可信的 CRF, 即使 CRF 是半诚实的, 所提方案对于 CRF 敌手依然是 CPA 安全的. 综合定理 2–定理 4 可得如下定理 5.

定理 5. 如果 $\Pi_{\text{RKM-SCF}}$ 是一个 RKM-SCF-IBE 方案, 则 $\Pi_{\text{CRF-IBE}}$ 方案的安全性是独立于 CRF 的.

6 性能分析与仿真实验

本节主要对提出方案进行性能分析, 并通过仿真实验, 测试方案性能. 将所提的方案与现有的相关研究工作[21]对比, 分析说明本文方案在实际场景中的可用性.

6.1 性能分析

本部分将从方案特点对所提的方案和文献 [21] 的方案进行考察, 结果如表 1 所示, 本文方案中可以抵抗 *PKG* 的后门攻击, 协议的安全性不依赖于 CRF, 在身份私钥提取阶段不需要安全通道, 而且安全性规约到了标准模型下.

表 1 方案特点对比

方案	抗*PKG*后门攻击	无安全通道	标准模型
文献[21]	×	×	×
本文方案	√	√	√

6.2 仿真实验

为了进行详细的评估, 使用 Charm-Crypto 框架[26]在 80 bits 的安全级别下实现了文献 [21] 和本文方案. 测试环境为 4 GB 内存, Intel(R) Core(TM) i7-7700HQ @ 2.80 GHz (8 CPUs), 50 GB 磁盘存储的 64 位 Ubuntu 18.04.5 LTS. 由于交互过程中不可预测因素太多, 如网络带宽、传输方式、数据流方向以及数据传输模式等等, 故先不考虑交互过程. 通过使用 1 000 次的平均时间来评估每个阶段的计算开销.

图 11 和图 12 分别给出了身份私钥提取阶段和消息发送阶段的计算开销.

如图 11 所示, 在身份私钥提取阶段中, 测试了多个用户同时发送私钥提取请求时用户和 *PKG* 共同的计算开销. 文献 [21] 的方案和本文方案中身份私钥提取阶段的计算代价和用户数量存在线性关系. 由于本文方案不使用安全信道以及实现了 *PKG* 侧的抗后门攻击, 故本文方案的身份私钥提取阶段的计算开销比文献 [21] 的方案要大. 一般来讲, 一个用户在整个方案周期中不会频繁进行私钥提取操作, 这意味着本文方案使用不大的计算代价换取到了整个方案的安全性提升. 当 100 个用户同时进行私钥提取请求时, 本文方案需要 2.24 s, 这个值相比于多用户场景下的网络通信时延是可以接受的.

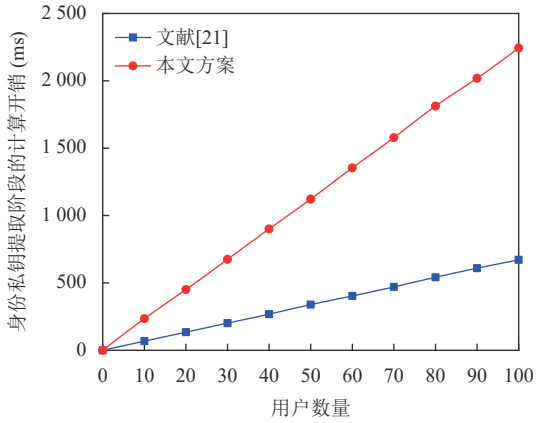

图 11 身份私钥提取阶段的计算开销

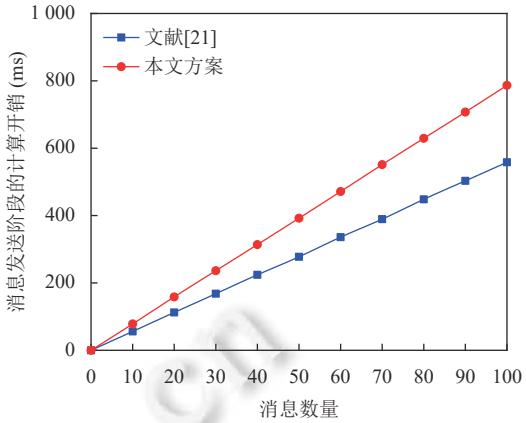

图 12 消息发送阶段的计算开销

如图 12 所示, 在消息发送阶段中, 测试了密文发送者和接收者对多个消息进行加密和解密的计算开销. 文献 [21] 的方案和本文方案中消息发送阶段的计算代价和消息数量呈正相关. 可以看出本文方案的私钥提取阶段的计算开销比文献 [21] 的方案要大, 但是在文献 [21] 的方案中, 接收者需要设置长期公钥, 这不符合基于身份加密体系的思想. 当密文发送者向接收者发送 100 个消息时, 本文方案需要 0.786 7 s, 在实际的应用中, 这个值是可接受的.

图 13 比较了本文方案中每个实体在不同安全级别下的计算开销所占的比例. 可以看出 *PKG* 花费了最多的时间, 这主要是因为 *PKG* 负责整个系统的建立, 而在实际应用中, 系统的建立只需要运行 1 次. 同时, CRF 的计算开销所占的比例低于其他实体的计算开销的比例, 这意味着本文方案中部署 CRF 所增加的时间成本是可接受的.

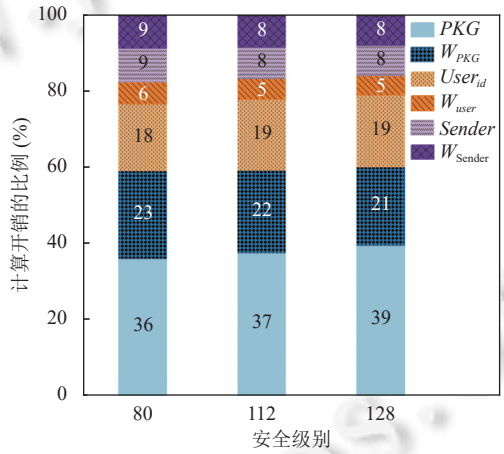

图 13 不同安全级别下每个实体的计算开销所占的比例

7 结论与未来展望

针对 IBE 机制的 CRF 构造问题, 本文系统性提出 CRF 在基于身份场景下应该满足的功能、安全性定义与安全模型, 指出 CRF 作为第三方应当具备安全独立性. 为使得 CRF 在私钥提取过程中不直接获得用户私钥, 本文首先提出能够满足该要求的 RKM-SCF-IBE 的概念, 其次给出基于 IBE 方案的一般性构造方法与具体实例. 最后给出用于 RKM-SCF-IBE 的 CRF 构造, 形式化证明表明其满足安全独立性、抗渗透性等性质. 为后续给 IBE、ABE 等表达力更强的原语配置 CRF 的工作明确了应该避免的问题.

然而, 整体来说, 基于 CRF 抵抗后门攻击的方法, 依赖大量的再随机化计算和对需要保护信息的再随机化加

密. 为简单的公钥加密或者 IBE 配置 CRF, 代价还可以接受. 若为 ABE 或者函数加密等复杂原语构造 CRF, 带来的计算开销和通信代价偏高. 且每个用户都需要配置 CRF, 经济成本较高. 探索高效经济的新方法, 是抗后门的密码方案从理论走向应用的关键.

References:

[1] Li G, Liu JW, Zhang ZY. An overview on cryptography against mass surveillance. Journal of Cryptologic Research, 2019, 6(3): 269–282 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000301]

[2] Kang BR, Zhang L, Zhang R, Meng XY, Chen T. Cryptographic algorithms against backdoored pseudorandom number generator. Ruan Jian Xue Bao/Journal of Software, 2021, 32(9): 2887−2900 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5976.htm [doi: 10.13328/j.cnki.jos.005976]

[3] Bellare M, Paterson KG, Rogaway P. Security of symmetric encryption against mass surveillance. In: Proc. of the 34th Annual Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2014. 1–19. [doi: 10.1007/978-3-662-44371-2_1]

[4] Russell A, Tang Q, Yung M, Zhou HS. Generic semantic security against a kleptographic adversary. In: Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security. Dallas: ACM, 2017. 907–922. [doi: 10.1145/3133956.3133993]

[5] Ateniese G, Magri B, Venturi D. Subversion-resilient signature schemes. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security. Denver: ACM, 2015. 364–375. [doi: 10.1145/2810103.2813635]

[6] Liu C, Chen RM, Wang Y, Wang YJ. Asymmetric subversion attacks on signature schemes. In: Proc. of the 23rd Australasian Conf. on Information Security and Privacy. Wollongong: Springer, 2018. 376–395. [doi: 10.1007/978-3-319-93638-3_22]

[7] Bellare M, Brakerski Z, Naor M, Ristenpart T, Segev G, Shacham H, Yilek S. Hedged public-key encryption: How to protect against bad randomness. In: Proc. of the 15th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Tokyo: Springer, 2009. 232–249. [doi: 10.1007/978-3-642-10366-7_14]

[8] Mironov I, Stephens-Davidowitz N. Cryptographic reverse firewalls. In: Proc. of the 34th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Sofia: Springer, 2015. 657–686. [doi: 10.1007/978-3-662-46803-6_22]

[9] Dodis Y, Mironov I, Stephens-Davidowitz N. Message transmission with reverse firewalls-secure communication on corrupted machines. In: Proc. of the 36th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2016. 341–372. [doi: 10.1007/978-3-662-53018-4_13]

[10] Zhou YY, Guo J, Li FG. Certificateless public key encryption with cryptographic reverse firewalls. Journal of Systems Architecture, 2020, 109: 101754. [doi: 10.1016/j.sysarc.2020.101754]

[11] Chen RM, Mu Y, Yang GM, Susilo W, Guo FC, Zhang MW. Cryptographic reverse firewall via malleable smooth projective hash functions. In: Proc. of the 22nd Int'l Conf. on the Theory and Application of Cryptology and Information Security. Hanoi: Springer, 2016. 844–876. [doi: 10.1007/978-3-662-53887-6_31]

[12] Ganesh C, Magri B, Venturi D. Cryptographic reverse firewalls for interactive proof systems. Theoretical Computer Science, 2021, 855: 104–132. [doi: 10.1016/j.tcs.2020.11.043]

[13] Shamir A. Identity-based cryptosystems and signature schemes. In: Proc. of the Advances in Cryptology. Berlin: Springer, 1984. 47–53. [doi: 10.1007/3-540-39568-7_5]

[14] Boneh D, Franklin MK. Identity-based encryption from the weil pairing. In: Proc. of the 21st Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2001. 213–229. [doi: 10.1007/3-540-44647-8_13]

[15] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In: Proc. of the 2004 Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Interlaken: Springer, 2004. 223–238. [doi: 10.1007/978-3-540-24676-3_14]

[16] Waters B. Efficient identity-based encryption without random oracles. In: Proc. of the 24th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Aarhus: Springer, 2005. 114–127. [doi: 10.1007/11426639_7]

[17] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Proc. of the 7th Theory of Cryptography Conf. on Theory of Cryptography. Zurich: Springer, 2010. 455–479. [doi: 10.1007/978-3-642-11799-2_27]

[18] Chen J, Wee H. Fully, (almost) tightly secure IBE and dual system groups. In: Proc. of the 33rd Annual Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2013. 435–460. [doi: 10.1007/978-3-642-40084-1_25]

[19] Wee H. Déjà Q: Encore! Un Petit IBE. In: Proc. of the 13th Int'l Conf. on Theory of Cryptography. Tel Aviv: Springer, 2016. 237–258. [doi: 10.1007/978-3-662-49099-0_9]

[20] Döttling N, Garg S. Identity-based encryption from the Diffie-Hellman assumption. Journal of the ACM, 2021, 68(3): 14. [doi: 10.1145/3422370]

[21] Zhou YY, Guan YF, Zhang ZW, Li FG. Cryptographic reverse firewalls for identity-based encryption. In: Proc. of the 2nd Int'l Conf. on Frontiers in Cyber Security. Xi'an: Springer, 2019. 36–52. [doi: 10.1007/978-981-15-0818-9_3]

[22] Ma H, Zhang R, Yang GM, Song ZS, Sun SZ, Xiao YT. Concessive online/offline attribute based encryption with cryptographic reverse firewalls-secure and efficient fine-grained access control on corrupted machines. In: Proc. of the 23rd European Symp. on Research in Computer Security. Barcelona: Springer, 2018. 507–526. [doi: 10.1007/978-3-319-98989-1_25]

[23] Baek J, Safavi-Naini R, Susilo W. Public key encryption with keyword search revisited. In: Proc. of the Int'l Conf. on Computational Science and its Applications. Perugia: Springer, 2008. 1249–1259. [doi: 10.1007/978-3-540-69839-5_96]

[24] Fang LM, Susilo W, Ge CP, Wang JD. A secure channel free public key encryption with keyword search scheme without random oracle. In: Proc. of the 8th Int'l Conf. on Cryptology and Network Security. Kanazawa: Springer, 2009. 248–258. [doi: 10.1007/978-3-642-10433-6_16]

[25] Emura K, Miyaji A, Rahman MS, Omote K. Generic constructions of secure-channel free searchable encryption with adaptive security. Security & Communication Networks, 2015, 8(8): 1547–1560. [doi: 10.1002/sec.1103]

[26] Akinyele JA, Garman C, Miers I, Pagano MW, Rushanan M, Green M, Rubin AD. Charm: A framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 2013, 3(2): 111–128. [doi: 10.1007/s13389-013-0057-3]

附中文参考文献:

[1] 李耕, 刘建伟, 张宗洋. 抗大规模监视密码学研究综述. 密码学报, 2019, 6(3): 269–282. [doi: 10.13868/j.cnki.jcr.000301]

[2] 康步荣, 张磊, 张蕊, 孟欣宇, 陈桐. 抗随机数后门攻击的密码算法. 软件学报, 2021, 32(9): 2887−2900. http://www.jos.org.cn/1000-9825/5976.htm [doi: 10.13328/j.cnki.jos.005976]

赵一(1985－), 男, 博士, 讲师, 主要研究领域为公钥密码学, 抗后门攻击, 隐私保护.

明洋(1979－), 男, 博士, 教授, 博士生导师, CCF 专业会员, 主要研究领为域密码学, 网络安全.

刘行(1999－), 男, 硕士生, 主要研究领域为公钥密码学, 区块链技术.

杨波(1963－), 男, 博士, 教授, 博士生导师, 主要研究领域为密码学, 信息安全.