软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(10):3236−3253 [doi: 10.13328/j.cnki.jos.006013]

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

安全随机数部分重用及在多接收方签密的应用*

刘 镇, 韩益亮, 杨晓元, 柳曙光

(武警工程大学 密码工程学院,陕西 西安 710086)

通讯作者: 韩益亮, E-mail:hanyil@163.com

摘 要: 为了在构造多接收方签密方案时,既不牺牲安全性又可以节约通信和计算开销,首先将随机数重用的安全理论丰富到另一种常见情况,提出了随机数部分重用的概念,并以签密体制为研究对象,定义了随机数部分重用的多接收方签密方案、随机数部分重用可再生的签密方案及安全模型;然后给出并证明了可再生性定理——随机数部分重用的安全条件为方案是可再生的;最后证明了 LWWD16 的格基签密方案是一个随机数部分重用可再生的签密方案,并基于 LWWD16 首次构造了一个基于格的随机数部分重用的多消息多接收方签密方案,证明了方案满足抗自适应选择密文攻击不可区分(IND-CCA2)和抗自适应选择消息攻击不可伪造(euf-CMA)安全性.效率分析表明,基于随机数部分重用构造的多消息多接收方签密方案可以有效地节约系统计算和通信开销.为多消息多接收方签密的构造提供了一种通用方法.

关键词: 签密;多接收方;随机数部分重用;可证明安全性;抗量子攻击

中图法分类号: TP309

中文引用格式: 刘镇,韩益亮,杨晓元,柳曙光.安全随机数部分重用及在多接收方签密的应用.软件学报,2021,32(10):3236−3253. http://www.jos.org.cn/1000-9825/6013.htm

英文引用格式: Liu Z, Han YL, Yang XY, Liu SG. Secure re-use of partial randomness and its application in multi-receiver signcryption scheme. Ruan Jian Xue Bao/Journal of Software, 2021,32(10):3236−3253 (in Chinese). http://www.jos.org.cn/1000-9825/6013.htm

Secure Re-use of Partial Randomness and its Application in Multi-receiver Signcryption Scheme

LIU Zhen, HAN Yi-Liang, YANG Xiao-Yuan, LIU Shu-Guang

(College of Cryptography Engineering, Engineering University of PAP, Xi'an 710086, China)

Abstract: To save bandwidth and computation without sacrificing security while constructing a multi-receiver signcryption scheme, this study extended the paradigm namely the re-use of all randomness to another common scenario, proposed the re-use of partial randomness, and redefined the multi-receiver signcryption scheme, reproducible signcryption scheme, and security model to the re-use of partial randomness. It then given and proved the reproducibility theorem that the security condition of the re-use of partial randomness is that the scheme is reproducible. Finally, it proved that the LWWD16 signcryption scheme based on lattice is a reproducible signcryption scheme with the re-use of partial randomness, and firstly constructed a multi-message to multi-receiver signcryption scheme with the re-use of partial random numbers based on lattice, which satisfied the security of adaptively indistinguishable against chosen ciphertext attacks (IND- CCA2) and existentially unforgeable against chosen message attacks (euf-CMA). Efficiency analysis shows that the multi-message

* 基金项目: 国家自然科学基金(61572521, U1636114, 61772550); 国家重点研发计划(2017YFB0802000); 陕西省自然科学基金(2018JM6078); 武警工程大学科研创新团队基金(KYTD201805)

Foundation item: National Natural Science Foundation of China (61572521, U1636114, 61772550); National Key Research and Development Project of China (2017YFB0802000); Natural Science Foundation of Shanxi Province of China (2018JM6078); Research and Innovation Team Fund of Armed Police Force Engineering University (KYTD201805)

收稿时间: 2019-09-29; 修改时间: 2019-12-11; 采用时间: 2020-01-19

and multi-receiver signcryption scheme with the re-use of partial randomness can effectively save bandwidth and computation, and it provides a general construction method for multi-message to multi-receiver signcryption.

Key words: signcryption; multi-receiver; re-use of partial randomness; provable security; quantum attack resistance

1 引 言

1.1 研究背景

在通信领域中会经常遇到一个用户向多个用户发送消息的场景,这里面又可分为两种情况:一种情况发送的消息是相同的,我们称为单消息多接收方(single message to multi receivers,简称 SM-MR)通信;另一种情况发送的消息是不同的,我们称为多消息多接收方(multi messages to multi receivers,简称 MM-MR)通信.MM-MR 可以看作是多用户通信的一般场景,而 SM-MR 则可以看作是一种特殊的 MM-MR 通信.在 MM-MR 通信中,消息的传输通常是以广播的方式进行的,因此在构造 MM-MR 通信方案时,在不影响通信内容的前提下有效降低通信量,对系统性能的提升具有重要意义.

信息安全问题是通信系统需要考虑的一个重要内容,为了保护信息的机密性和完整性,最常用的方法是使用密码技术.要实现多用户环境下的密码通信,最直接的方法是将一对一的标准密码方案独立使用多次,这种方法虽然简单,但是多消息多用户通信可能存在内部敌手,此时一些方案可能不安全.例如,Håstad[1]发现,独立使用 RSA 方案用于多接收方就有可能泄露信息.Baudron 等人[2]和 Bellare 等人[3]分别对多接收方加密的安全条件进行了证明,他们指出:如果基础方案是不可区分性安全的,那么独立使用多次的方案也是不可区分性安全的.该结果可以用来检验多接收方密码方案的安全性,但没有考虑到系统通信性能的优化.这种直接方式构造的多接收方密码方案,会带来系统通信量 N(设接收方个数为 N)倍的增长.

公钥密码方案为了满足特定的安全性,都会引入一些随机数,于是需要增加一些冗余信息来辅助解密,而这些冗余信息造成了密文的膨胀.如果在构造多接收方密码方案多次执行标准密码方案过程中适当地重用一些随机数,就可以有效降低系统的开销,节约通信和计算量.然而,随机数对方案的安全性至关重要,重用随机数可能导致方案产生严重的安全问题,因此,研究满足何种条件时在构造多接收方密码方案多次执行标准密码方案重用随机数才安全,是一项具有实用意义的工作.

1.2 相关工作

为了提高多接收方加密方案的计算和通信效率,Kurosawa[4]提出了随机数重用的概念,并基于 ElGamal[5]和 Cramer-Shoup[6]方案+构造了随机数重用的多接收方加密方案.例如,发送方 S 想要用 EIGamal 加密发送消息 m_i 给接收方 R_i,其中,R_i 的公钥为 $PK_i=g^{x_i}(i=1,2,...,N)$.最直接的方式是独立随机选择 N 个随机数$(r_1,r_2,\ldots,r_N)$,对 i=1,2,…,N,分别计算接收方 R_i 的密文 $c_i=(g^{r_i},m_ig^{x_ir_i})$,最后将密文 C=$(c_1,c_2,\ldots,c_N)$广播给接收方.而 Kurosawa 的随机数重用方式是只选择一个随机数 r,计算密文 $C=(g^r,m_1g^{x_1r},m_2g^{x_2r},...,m_Ng^{x_Nr})$ 并广播给接收方,两者密文量对比如图 1 所示.与直接构造的多接收方加密方案相比,系统的通信和计算开销节省了将近一半.

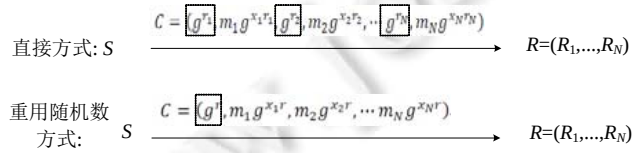


Fig.1 Comperision of ciphertex size for multi-receivers encryption between naive construction and randomness re-use construction

图 1 直接方式与随机数重用方式构造的多接收方加密方案密文量对比

通常,随机数对系统的安全性至关重要,随机数重用可能会导致严重的安全问题.但是,Kurosawa 指出:在某些情况下,随机数重用并不会影响系统的安全性.Bellare 等人[7,8]系统地研究了随机数重用相关理论及其在构造

多接收方加密方案中的应用,给出了可再生性(reproducibility)定理来验证随机数重用加密方案的安全性,从而为构造安全的随机数重用加密方案提供了思路.如今,随机数重用在构造多接收方加密及具有其他性质的加密方案中得到了广泛应用[9−12].

签密由 Zheng[13]首次提出,它将加密和签名结合成一步,可同时保护系统的保密性与认证性,是一个重要的密码学原语.韩益亮等人[14]将随机数重用理论推广到了签密,对随机数重用签密方案的构造及安全性进行了研究,给出了签密方案的可再生性定理,证明了基于随机数重用可再生的方案构造的多接收方签密与原方案具有相同的安全强度,并基于离散对数困难问题构造了一个随机数重用的多接收方签密方案.随后,一批随机数重用的多接收方签密成果陆续被提出[15−17].

上述现有关于随机数重用的方案都是针对基础方案中所有的随机数.通常,许多安全的点对点密码通信方案,尤其是基于格的签密方案中包含多个随机数,一方面,可再生签密方案的定义对标准方案需要满足的安全条件非常严苛,重用所有随机数对方案的安全性带来了很大的挑战,目前还没有结果证明现有的某个基于格的签密方案是随机数全重用可再生的;另一方面,重用一个或者几个关键的随机数也能有效地节约系统的通信和计算开销.因此,研究如何安全地重用部分随机数来构造多接收方签密,是一件非常有意义的工作.

另外,直接构造和随机数全重用构造方式可以看作是随机数重用构造方式的两种情况.当重用的随机数个数为空时,随机数重用构造方式退化到直接构造的方式(即非随机数重用);当重用的随机数个数为标准方案所有随机数时,随机数重用构造方式演化成随机数全重用构造方式.从现实情况来看,还有另一种更常见的情况是重用的随机数个数为标准方案中部分随机数,此时的构造方式称为随机数部分重用构造方式.

1.3 本文的工作

本文借鉴 Kurosawa、Bellare 和韩益亮等人的思路,结合格基签密方案多随机数的实际情况,以多接收方签密为研究对象,将随机数重用构造多接收方密码的安全理论丰富到随机数部分重用的场景,提出了随机数部分重用的概念,定义了随机数部分重用的多接收方签密方案和随机数部分重用可再生的签密方案,研究了可安全随机数部分重用的条件(标准签密方案是随机数部分重用可再生的方案),给出并证明了随机数部分重用可再生性定理:如果标准密码方案是随机数部分重用可再生的方案,那么采用随机数部分重用构造的多接收方密码方案与标准方案具有相同的安全强度;最后,基于随机数部分重用可再生的签密方案定义,证明了路秀华等人格基签密方案是部分随机数重用可再生的签密方案.然后,基于路秀华的标准签密方案,构造了一个部分随机数重用的格基多接收方签密方案,并基于可再生性定理证明了所构造方案的安全性.效率分析表明:与直接构造相比,随机数部分重用的构造可有效地节约计算和通信开销.

1.4 组织结构

本文的章节组织如下:

- 第 1 节介绍本文的研究背景、相关工作、本文的工作以及本文的组织结构;
- 第 2.1 节介绍通信模型;第 2.2 节介绍标准签密方案(定义 1)及安全性定义(定义 2 和定义 3);第 2.3 节介绍多接收方签密方案(定义 4)及安全性定义(定义 6 和定义 8),同时还介绍随机数重用的多接收方签密方案(即如何基于定义 1 的标准签密方案,采用随机数重用的方式来构造一个多接收方签密方案的通用方法,见定义 5)及安全性定义(定义 7 和定义 9);
- 第 3 节研究部分随机数重用的多接收方签密安全理论,其中,第 3.1 节给出标准签密方案可部分随机数重用的安全条件(即标准签密方案是可再生的签密方案,见定义 10);第 3.2 节指出:如果一个标准签密方案是定义 10 描述的部分随机数重用可再生的签密方案,那么基于该标准签密方案构造的多接收方签密方案的安全性可规约到标准签密方案,进一步地在定理 1 和定理 2 中给出形式化描述和详细的证明;
- 第 4 节介绍部分随机数重用安全理论的应用,其中,第 4.1 节介绍格相关理论;第 4.2 节介绍一个基于格的标准签密方案 LWWD16;第 4.3 节基于标准签密方案,首先在定理 5 证明该标准签密方案是部分随机数重用可再生的签密方案(即满足部分随机数重用安全条件);然后,采用定义 5 的方法构造一个相应的

部分随机数重用多接收方签密方案;接着,定理 6 和定理 7 分别给出并证明该方案的保密和不可伪造性安全性(定理 6 的证明可由定理 1 和定理 5 得到,定理 7 的证明可由定理 2 和定理 5 得到),然后介绍方案相关参数的选取;最后,将构造的随机数部分重用的多接收方签密方案与原标准签密方案独立运行 N 次以及其他基于格的多接收方签密方案的效率进行对比分析.

2 模型及定义

2.1 通信模型

我们的通信模型主要考虑 MM-MR 的场景,如图 2 所示.设发送方 S 想要以广播的方式分别将 N 个不同的消息$(m_1,m_2,\ldots,m_N)$发送给 N 个不同的接收方$(R_1,R_2,\ldots,R_N)$,发送方将消息签密后得到签密文 $C=(c_1,c_2,\ldots,c_N)$并加以广播,对 $i=1,2,\ldots,N$,接收方 R_i 从广播的消息中获得自己的密文 c_i 并解密.

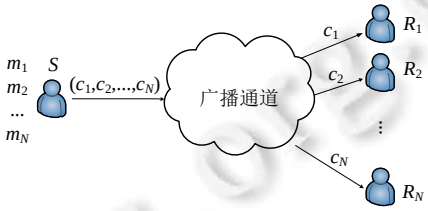


Fig.2 Communication model of MM-MR signcryption

图 2 MM-MR 签密通信模型

值得注意的是:MM-MR 签密可以看作是签密的一般情况,标准的一对一签密和 SM-MR 签密都可以看作是其特殊情况.当 $m_1=m_2=\ldots=m_N$ 时,MM-MR 签密退化成 SM-MR 签密;当 $N=1$ 时,MM-MR 签密退化成标准的一对一签密.

2.2 标准的签密方案

在签密方案的构造中,我们需要用到一些随机数,它们的选取方法与具体算法相关,通常在签密方案的定义中并不描述.由于我们研究的是多接收方签密方案构造中的随机数部分重用的安全性问题,需区分方案中重用和非重用的随机数两种情况.为了方案的定义更规范、清晰,本文用 $Coin_{SC}$ 来描述签密算法 SC 按照具体要求选取方案所需的所有随机数,用 $CoinsRu_{SC}$ 来描述签密算法 SC 按照具体要求选取方案所需可重用的随机数,用 $CoinsNRu_{SC}$ 来描述签密算法 SC 按照具体要求选取方案所需非重用的随机数,用 $Coins_{MSC}$ 来描述签密算法 MSC 按照具体要求选取方案所需的全部随机数.

定义 1(标准签密方案). 一个语义安全的签密方案$\Sigma=(Gen,Kgen,SC,DSC)$是一个四元组,Gen 是随机化的参数生成算法,输入安全参数 $k\in N$,输出随机化系统参数 $parm$,可表示为 $parm\leftarrow_{Rnd}Gen(k)$;$Kgen$ 是随机化的密钥生成算法,输入系统参数 $parm$,输出随机化系统通信双方密钥对(pk_S,sk_S)和(pk_R,sk_R),用$(pk_S,sk_S)(pk_R,sk_R)\leftarrow_{Rnd}Kgen(parm)$来表示;$SC$ 是随机化签密算法,输入发送方私钥 sk_S,接收方公钥 pk_R,明文 m,随机数集合 $r\leftarrow_{Rnd}Coins_{SC}(parm,sk_S,pk_R)$,输出签密文 $c=SC(sk_S,pk_R,m,r)$,用 $c\leftarrow_{Rnd}SC(sk_S,pk_R,m)$来表示;$DSC$ 是确定性的解签密算法,输入密文 c,发送方的公钥 pk_S,接收方私钥 sk_R,输出明文 m 或者终止符$\perp$,用$(m,\perp)\leftarrow DSC(c,pk_S,sk_R)$来表示.

设系统参数 $parm$,$Mspc(parm)$表示明文 m 的消息空间,要求对于所有 $m\in Mspc(parm)$,满足:

$$DSC(SC(sk_S,pk_R,m,r),pk_S,sk_R)=m.$$

保密性和不可伪造性是签密方案两个基本的安全概念,我们给出定义如下.

定义 2(保密安全性)[14]. 给定一个签密方案$\Sigma=(Gen,Kgen,SC,DSC)$,$attk=\{CPA,CCA2\}$,对于任意多项式时间敌手 A,考虑以下 $attkExp$ 实验.

- $attkExp^{attk\text{-}b}_{\Sigma,A}(k)$.

(1) $parm \leftarrow_{Rnd} Gen(k)$,$(State) \leftarrow A(select,parm)$;

(2) $(pk_S,sk_S)(pk_R,sk_R) \leftarrow_{Rnd} Kgen(parm)$;

(3) 若 $attk=CCA2$,$(m_0,m_1,State) \leftarrow A^{SC(\cdot),RO(\cdot),DSC(\cdot)}(Find,State)$,$(|m_0|=|m_1|)$;若 $attk=CPA$,$(m_0,m_1,State) \leftarrow A^{SC(\cdot),RO(\cdot)}(Find,State)$,$(|m_0|=|m_1|)$;

(4) $b \leftarrow_{Rnd} \{0,1\}$,$c^* \leftarrow_{Rnd} SC(sk_S,pk_R,m_b)$;

(5) 如果 $attk=CCA2$,$b' \leftarrow A^{SC(\cdot),RO(\cdot),DSC(\cdot)}(Guess,c^*,State)$,要求不能再询问 c^*的知识,返回 b';如果 $attk=CPA$,返回 b'.

上述实验过程中,设 k 为安全参数,A 是一个自适应的三阶敌手,在选择(select)阶段,A 被给定系统参数,输出状态信息 $State$;在发现阶段,A 可以向签密预言机 $SC(\cdot)$、随机预言机 $RO(\cdot)$询问(本文安全性定义都是在随机预言机模型下的,如果在标准模型下,则无 $RO(\cdot)$),如果 $attk=CCA2$,A 还可以向解签密预言机 $DSC(\cdot)$询问,随后输出两个等长的消息(m_0,m_1)以及状态信息 $State$;在猜测阶段,随机选择一个比特 b,计算并输出消息 m_b 的挑战签密 c^*.当 $attk=CCA2$ 时,A 可以继续进行 $SC(\cdot)$、$RO(\cdot)$和 $DSC(\cdot)$询问,但是不能询问 c^*的知识,最后输出一个猜测的比特 b'.当 $attk=CPA$ 时,限制 A 不可以进行 $DSC(\cdot)$询问,直接输出一个猜测的比特 b'.

我们定义敌手 A 的优势为 $Adv_{\Sigma,A}^{attk}(k)=|\Pr[attkExp_{\Sigma,A}^{attk\text{-}0}(k)=0]-\Pr[attkExp_{\Sigma,A}^{attk\text{-}1}(k)=0]|$.如果敌手 A 的优势 $Adv_{\Sigma,A}^{CCA2}(k)$ 是可以忽略的,则称Σ是一个抗自适应选择密文攻击不可区分(IND-CCA2)安全的签密方案;如果敌手 A 的优势 $Adv_{\Sigma,A}^{CPA}(k)$ 是可以忽略的,则称Σ是一个抗选择明文攻击不可区分(IND-CPA)安全的签密方案.

定义 3(不可伪造安全性)[14]. 给定一个签密方案$\Sigma=(Gen,Kgen,SC,DSC)$,对于任意多项式时间伪造者 F,考虑以下选择消息攻击(CMA)伪造实验 $ForgeExp$.

- $ForgeExp_{\Sigma,F}^{CMA}(k)$

(1) $parm \leftarrow_{Rnd} Gen(k)$,$(State) \leftarrow F(select,parm)$;

(2) $(pk_S,sk_S)(pk_R,sk_R) \leftarrow_{Rnd} Kgen(parm)$;

(3) $(m,c) \leftarrow F^{SC(\cdot),RO(\cdot)}(pk_S,pk_R,sk_R)$.如果满足 $DSC^{RO(\cdot)}(c,pk_S,sk_R)=m$ 且没有向签密预言机 $SC(\cdot)$询问过 m 的签密,则返回 1;否则,返回 0.

上述实验过程中,设 k 为安全参数,F 是一个自适应的伪造者,在选择(select)阶段(1)和阶段(2),F 被给定系统参数,输出状态信息 $State$;在伪造阶段(3),A 可以适应性地向签密预言机 $SC(\cdot)$与随机预言机 $RO(\cdot)$询问,并获得应答.随后输出一个消息 m 以及相应的伪造签密文 c,如果该签密文是消息 m 的合法签密文,且没有以 m 询问过签密预言机的消息,则 F 赢得伪造实验.

我们定义伪造者 F 的优势为 $Adv_{\Sigma,F}^{CMA}(k)=\max\{\Pr[ForgeExp_{\Sigma,F}^{CMA}(k)=1]\}$.如果任意敌手 F 的优势 $Adv_{\Sigma,F}^{CMA}(k)$ 是可以忽略的,则称Σ是一个抗选择消息攻击不可伪造性(euf-CMA)安全的签密方案.

2.3 多接收方签密方案

定义 4(多接收方签密方案). 一个语义安全的多接收方签密方案 $M\Sigma=(Gen,Kgen,MSC,DSC)$是一个四元组:参数生成算法 Gen、密钥生成算法 $Kgen$ 和解签密算法 DSC 与上述定义 1 的标准签密方案相同;MSC 是随机化的多接收方签密算法,输入发送方私钥 sk_S,接收方公钥向量 $PK_R=(pk_{R_1},pk_{R_2},...,pk_{R_N})$,明文向量 $M=(m_1,m_2,\ldots,m_N)$,随机数集合 $r \leftarrow_{Rnd} Coins_{MSC}(parm,sk_S,PK_R)$,输出签密文向量 $C=(c_1,c_2,\ldots,c_N)=MSC(M,sk_S,PK_R,r)$,$Coins_{MSC}(parm,sk_S,PK_R)$表示多接收方签密算法 MSC 按照具体要求选取算法所需的随机数.设系统参数 $parm$,$Mspc(parm)$表示明文向量 M 所有分量 $m_i(1\leqslant i\leqslant N)$的消息空间,要求对于所有满足 $m_i \in Mspc(parm)$的明文向量 M,下面的过程以概率 1 返回结果 1.

(1) 计算$(pk_S,sk_S) \leftarrow_{Rnd} Kgen(parm)$;

(2) 对于 $i=1,2,\ldots,N$,计算 $(pk_{R_i},sk_{R_i}) \leftarrow_{Rnd} Kgen(parm)$;

(3) 计算 $C=(c_1,c_2,\ldots,c_N)=MSC(M,sk_S,PK_R,r)$;

(4) 随机选择 $j\in(1,2,\ldots,N)$,如果 $DSC_{sk_j}(c_j)=m_j$, 返回 1;否则,返回 0.

本文主要的研究对象为随机数重用的多接收方签密,我们定义如下.

定义 5(随机数重用的多接收方签密). 对于给定一个定义 1 的标准语义安全签密方案Σ=(*Gen*,*Kgen*,*SC*,*DSC*),设签密算法 *SC* 中包含 *w* 个随机数,$M\Sigma$=(*Gen*,*Kgen*,*MSC*,*DSC*)是定义 4 描述的Σ所对应的多接收方签密方案,定义随机数重用的多接收方签密算法 *MSC* 如下.

(1) $\bar{r}=(r_1,r_2,\ldots,r_d)\leftarrow_{Rnd} CoinsRu_{SC}(parm,sk_S)$;

(2) 对 i=1,2,…,N,选择 $\tilde{r}_{R_i}=(r_{(d+1)_i},r_{(d+2)_i},\ldots,r_{w_i})\leftarrow_{Rnd} CoinsNRu_{SC}(parm,sk_S,pk_{R_i})$, 令 $r_{R_i}=(r_1,r_2,\ldots,r_d,r_{(d+1)i},\ldots,r_{w_i})$, 计算 $c_i=SC(sk_S,pk_{R_i},m_i,r_{R_i})$;

(3) 返回 $C=(c_1,c_2,\ldots,c_N)$.

如果 $d=w$,则称 $M\Sigma$为随机数全重用的多消息多接收方签密方案(all randomness reuse for multi messages to multi receivers,简称 ARRU-MM-MR);如果 $d=0$,则称 $M\Sigma$为非随机数重用的多消息多接收方签密方案(non randomness reuse for multi messages to multi receivers,简称 NRRU-MM-MR);否则,称 $M\Sigma$为随机数部分重用的多消息多接收方签密方案(partial randomness reuse for multi messages to multi receivers,简称 PRRU-MM-MR).

对于 SM-MR 签密,所有接收方收到的消息都是相同的,信息的泄露主要针对外部敌手,通常不考虑内部攻击.而对于 MM-MR 签密,由于每个接收方收到的消息都不相同,信息的泄露可能会是内部敌手,任何想得到其他接收方消息的接收方都可能是潜在敌手.因此,在定义保密性安全时,我们借鉴了文献[8,14]的攻击模型,考虑了内部敌手,他可以腐败部分其他接收方,除了自己的密钥外,还拥有其他部分接收方的密钥.

定义 6(保密安全性)[14]. 给定一个 PRRU-MM-MR 签密方案 $M\Sigma$=(*Gen*,*Kgen*,*MSC*,*DSC*),设 k 为安全参数,接收方个数为自然数 $N=n(k)$,$l(1\leqslant l\leqslant N)$为正整数,*attk*={*CPA*,*CCA*2},对于任意多项式时间敌手 A,考虑以下 *attkExp* 实验.

- $attkExp^{N\text{-}MR\text{-}attk\text{-}b}_{M\Sigma,A}(k)$.

(1) $parm\leftarrow_{Rnd}Gen(k)$,$(1^l,State)\leftarrow A(select,N,parm)$;

(2) $(pk_S,sk_S)\leftarrow_{Rnd}Kgen(parm)$;

(3) 对 i=1,2,…,N,计算 $(pk_{R_i},sk_{R_i})\leftarrow_{Rnd} Kgen(parm)$;

(4) 当 *attk*=*CCA*2 时,计算 $(\boldsymbol{M}_0,\boldsymbol{M}_1,\boldsymbol{M},\boldsymbol{CoinsKgen},State)\leftarrow A^{MSC(\cdot),RO(\cdot),DSC^1(\cdot),\ldots,DSC^l(\cdot)}(Find,pk_{R_1},\ldots,pk_{R_l},State)$;
当 *attk*=*CPA* 时,计算 $(\boldsymbol{M}_0,\boldsymbol{M}_1,\boldsymbol{M},\boldsymbol{CoinsKgen},State)\leftarrow A^{MSC(\cdot),RO(\cdot)}(Find,pk_{R_1},\ldots,pk_{R_l},State)$, 其中,
$((\boldsymbol{M}_0,\boldsymbol{M}_1)\in Mspc^l(parm),\boldsymbol{M}=(m_{l+1},\ldots,m_N)\in Mspc^{N-l}(parm),\boldsymbol{CoinsKgen}=(CoinsKgen_{l+1},CoinsKgen_{l+2},\ldots,CoinsKgen_N))$;

(5) 对 $i=l+1,\ldots,N$,计算 $(pk'_{R_i},sk'_{R_i})\leftarrow Kgen(parm,CoinsKgen_i)$;

(6) 令 $\boldsymbol{PK}_R=(pk_{R_1},\ldots,pk_{R_l},pk'_{R_{l+1}},\ldots,pk'_{R_N})$, $\boldsymbol{M}^*=(m_1^*,\ldots,m_N^*)=(m_{b_1},\ldots,m_{b_l},m_{l+1},\ldots,m_N)$;

(7) $\bar{r}=(r_1,r_2,\ldots,r_d)\leftarrow_{Rnd} CoinsRu_{SC}(parm,sk_S)$;

(8) 对 i=1,2,…,N,选择 $\tilde{r}_{R_i}=(r_{(d+1)_i},r_{(d+2)_i},\ldots,r_{w_i})\leftarrow_{Rnd} CoinsNRu_{SC}(parm,sk_S,pk_{R_i})$, 令 $r_{R_i}=(r_1,r_2,\ldots,r_d,r_{(d+1)i},\ldots,r_{w_i})$, 计算 $c_i^*=SC(sk_S,pk_{R_i},m_i^*,r_{R_i})$;

(9) 令 $\boldsymbol{C}^*=(c_1^*,\ldots,c_N^*)$, 当 *attk*=*CCA*2 时, $b'\leftarrow A^{MSC(\cdot),RO(\cdot),DSC^1(\cdot),\ldots,DSC^l(\cdot)}(Guess,\boldsymbol{C}^*,State)$ (要求不能询问 $\boldsymbol{C}^*$的有关知识);当 *attk*=*CPA* 时,$b'\leftarrow A(Guess,\boldsymbol{C}^*,State)$;

(10) 返回 b'.

上述实验过程中,设 A 是一个自适应的三阶敌手,已腐败 $N-l$ 个接收方.不失一般性,设 l 个未腐的接收方为 $R_1,\ldots,R_l$.在选择(select)阶段,A 被给定系统参数 *parm*、用户数 N、输出腐败用户数 $l(1\leqslant l\leqslant N)$以及状态信息 *State*;在发现阶段,$A$ 被给定系统参数 *parm*、状态信息 *State*、l 个未腐败用户的公钥 $pk_{R_1},\ldots,pk_{R_l}$, 可以向签密预言机 *MSC*(·)、随机预言机 *RO*(·)询问,如果 *attk*=*CCA*2,还可以向解签密预言机 *DSC*(·)询问,随后输出两个等长的 N 维向量消息$(\boldsymbol{M}_0,\boldsymbol{M}_1)$、一个 $N-l$ 维向量消息 $\boldsymbol{M}$、$N-l$ 维的密钥生成算法所需的随机数向量 ***CoinsKgen*** 以及状态信

息 *State*,然后生成 *N*–*l* 腐败用户的公私钥对,并输出接收方公钥 $\boldsymbol{PK}_R$;在猜测阶段,挑战者基于随机比特 *b*,生成挑战消息 $\boldsymbol{M}^*$,并计算挑战签密 $\boldsymbol{C}^* = (c_1^*,...,c_N^*)$. 当 *attk*=*CCA*2 时,*A* 可以继续进行 *MSC*(·)、*RO*(·)和 *DSC*(·)询问,但不能询问 $\boldsymbol{C}^*$的知识,最后输出一个猜测的比特 *b*′;当 *attk*=*CPA* 时,*A* 直接输出一个猜测的比特 *b*′.

我们定义敌手 *A* 的优势为 $Adv_{M\Sigma,A}^{N\text{-}MR\text{-}attk}(k) = |\Pr[attkExp_{M\Sigma,A}^{N\text{-}MR\text{-}attk\text{-}0}(k)=0] - \Pr[attkExp_{M\Sigma,A}^{N\text{-}MR\text{-}attk\text{-}1}(k)=0]$. 如果敌手 *A* 的优势 $Adv_{M\Sigma,A}^{N\text{-}MR\text{-}CCA2}(k)$ 是可以忽略的,则称该 PRRU-MM-MR 签密方案 *MΣ*是抗自适应选择密文攻击不可区分(IND-CCA2)安全的;如果敌手 *A* 的优势 $Adv_{M\Sigma,A}^{N\text{-}MR\text{-}CPA}(k)$ 是可以忽略的,则称该 PRRU-MM-MR 签密方案 *MΣ*是抗选择明文攻击不可区分(IND-CPA)安全的.

定义 7(PRRU-IND-CPA 和 PRRU-IND-CCA2 安全的签密)[14]. 给定一个语义安全的签密方案*Σ*=(*Gen*,*Kgen*,*SC*,*DSC*),设 *MΣ*=(*Gen*,*Kgen*,*MSC*,*DSC*)是对应的 PRRU-MM-MR 签密方案,如果 *MΣ*是 IND-CPA 或 IND-CCA2 安全的,那么我们称*Σ*是 PRRU-IND-CPA 或 PRRU-IND-CCA2 安全的签密方案.

定义 8(不可伪造安全性)[14]. 对于多接收方签密来说,不可伪造性是指任意敌手无法伪造一个合法的签密文.与外部敌手相比,通常内部敌手具有更多的优势来伪造一个签密文,如果他能够伪造一个发送方的签名,那么他就能伪造一个发送方的合法签密.如果一个签密方案是抗内部攻击者不可伪造性安全的,那么该方案也是抗外部攻击者不可伪造性安全的.鉴于此,我们考虑的安全模型包括内部敌手.

对于给定的 PRRU-MM-MR 签密方案 *MΣ*=(*Gen*,*Kgen*,*MSC*,*DSC*),设 *k* 为安全参数,接收方个数为自然数 *N*=*n*(*k*),对于任意多项式时间伪造者 *F*,考虑以下 *ForgeExp* 实验.

- $ForgeExp_{M\Sigma,F}^{N\text{-}MR\text{-}CMA}(k)$.

(1) $parm \leftarrow_{Rnd} Gen(k)$,$(State) \leftarrow F(select,N,parm)$;

(2) $(pk_S,sk_S) \leftarrow_{Rnd} Kgen(parm)$;

(3) 对于 i=1,2,…,N,计算 $(pk_{R_i},sk_{R_i}) \leftarrow_{Rnd} Kgen(parm)$, 令 $\boldsymbol{PK}_R = (pk_{R_1},...,pk_{R_N})$, $\boldsymbol{SK}_R = (sk_{R_1},...,sk_{R_N})$;

(4) 输出一对伪造签密文$(m_i,c_i) \leftarrow F^{SC(\cdot),RO(\cdot)}(pk_S,\boldsymbol{PK}_R,\boldsymbol{SK}_R)$,其中,$i \in (1,2,\ldots,N)$.若满足 $DSC^{RO(\cdot)}(c_i,pk_S,sk_{R_i}) = m_i$ 且没有向签密预言机 *MSC*(·)询问过 m_i 的签密,则返回 1;否则,返回 0.

上述实验过程中,*F* 是一个自适应的伪造者,在选择(select)阶段,*F* 被给定系统参数 *parm* 和输出状态信息 *State*;在伪造阶段,*F* 可以向签密预言机 *MSC*(·)、随机预言机 *RO*(·)询问,随后输出某个接收方的消息 m_i 以及相应的伪造签密文 c_i,如果该签密文是消息 m_i 的合法签密文,且没有以 m_i 向签密预言机询问过知识,则 *F* 赢得伪造实验.

我们定义伪造者 *F* 的优势为 $Adv_{M\Sigma,F}^{N\text{-}MR\text{-}CMA}(k) = \max\{\Pr[ForgeExp_{M\Sigma,F}^{N\text{-}MR\text{-}CMA}(k)=1]\}$.

如果任意敌手 *A* 的优势 $Adv_{M\Sigma,F}^{N\text{-}MR\text{-}CMA}(k)$ 是可以忽略的,则称该 PRRU-MM-MR 签密方案 *MΣ*是一个抗自适应内部选择消息攻击不可伪造(euf-CMA)性安全的签密方案.

定义 9(PRRU-euf-CMA 安全的签密)[15]. 给定一个语义安全的签密方案*Σ*=(*Gen*,*Kgen*,*SC*,*DSC*),设 *MΣ*=(*Gen*,*Kgen*,*MSC*,*DSC*)是对应的 PRRU-MM-MR 签密方案,如果 *MΣ*是 euf-CMA 安全的,那么我们称*Σ*是 PRRU-euf-CMA 安全的签密方案.

3 安全随机数部分重用条件

在给多个接收方发送不同的消息时,我们需要多次运行标准密码方案,如果在多次运行标准密码方案的过程中使用相同的随机数(重用随机数),就可以有效地节约系统开销(例如图 1 描述的情况).然而,如果标准的密码方案中的随机数在解密算法中被接收方解密,那么一个接收方就可以知道其他接收方密码方案中的随机数.众所周知,随机数对方案的安全性至关重要,在考虑内部敌手的情况下,此时其他接收方的消息就不再安全.那么,满足什么条件的标准密码方案中的随机数可以重用呢?

2007 年,Bellare[8]提出了可再生的加密方案概念,指出,一个标准的加密方案可安全地随机数重用的充分条件为方案是可再生的.给出并证明了随机数重用可再生性定理.随后,韩益亮等人将它推广到签密的场景.然而,

他们的研究对象都是随机数全重用的情况.值得注意的是:随机数全重用和非随机数重用只是随机数重用的两种情况,而另一种更常见的情况是随机数部分重用,当重用的随机数为空时,随机数重用退化称为非随机数重用;当重用的随机数为方案中所有随机数时,随机数重用演化成随机数全重用;当重用的随机数为方案中的部分随机数时,随机数重用称为随机数部分重用.

下面我们将随机数重用的安全理论丰富到另一种常见的情况,从随机数部分重用的角度,定义随机数部分重用可再生的签密方案(即随机数部分重用的安全条件),给出并证明随机数部分重用可再生性定理(即基于可再生签密方案构造的随机数部分重用的多接收方签密方案是安全的).

3.1 可再生的签密方案定义

从信息论上说,一个标准的签密方案可随机数部分重用的安全条件可描述为:已知发送方的公私钥对、一个接收方公钥以及一个随机消息经该公钥加密生成的签密文,对于任意给定的另一个接收方公私钥对,可以构造出任意其他消息的有效签密文,要求所构造的签密文与给定的签密密文重用部分相同的随机数.

定义 10(可再生的签密方案). 给定一个定义 1 的标准签密方案$\Sigma=(Gen,Kgen,SC,DSC)$和一个多项式 $n(\cdot)$,设 k 为安全参数,接收方个数为自然数 $N=n(k)$.如果存在一个多项式时间再生算法 RP,输入一个发送方的私钥 sk_S、一个接收方的公钥 pk_R、一个签密文 c(某个随机消息 m 经该公钥 pk_R 生成的签密)、另一个随机消息 m'、另一个接收方的公私钥对$(pk_{R'},sk_{R'})$以及部分随机数集合 $\tilde{r}_{R'}$, 输出一个合法的签密文 c',则称签密方案Σ是可再生的.

我们可以用以下实验来描述.

- $Exp^{rep}_{\Sigma',RP}(k)$.

(1) $parm\leftarrow_{Rnd}Gen(k),(pk_S,sk_S)(pk_R,sk_R)\leftarrow_{Rnd}Kgen(parm),m\leftarrow_{Rnd}Mspc(parm)$;

(2) $\bar{r}=(r_1,r_2,...,r_d)\leftarrow_{Rnd}CoinsRu_{SC}(parm,sk_S)$;

(3) 对 i=1,2,…,N,选择 $\tilde{r}_R=(r_{(d+1)_i},r_{(d+2)_i},...,r_{w_i})\leftarrow_{Rnd}CoinsNRu_{SC}(parm,sk_S,pk_R)$ 令 $r_R=(\bar{r},\tilde{r}_R)=(r_1,r_2,...,r_d,r_{(d+1)_i},...,r_{w_i})$, 计算 $c=SC(sk_S,pk_R,m,\bar{r},\tilde{r}_R)$;

(4) $(pk_{R'},sk_{R'})\leftarrow_{Rnd}Kgen(parm),m'\leftarrow_{Rnd}Mspc(parm)$;

(5) $\tilde{r}_{R'}\leftarrow_{Rnd}CoinsNRu_{SC}(parm,sk_S,pk_{R'})$;

(6) 如果 $SC(sk_S,pk_{R'},m',\bar{r},\tilde{r}_{R'})=RP(sk_S,pk_R,c,pk_{R'},sk_{R'},m',\tilde{r}_{R'})$, 返回 1;否则,返回 0.

如果存在一个概率多项式时间再生算法 RP 使上述实验以 1 的概率返回 1,则称签密方案是可再生的.特别地,当 $\tilde{r}_{R'}=\varnothing$ 时,称Σ是随机数全重用可再生的签密方案;当 $\tilde{r}_{R'}\neq r_{R'}$ 且 $\tilde{r}_{R'}\neq\varnothing$ 时,称Σ是随机数部分重用可再生的签密方案.

3.2 可再生性定理

如果一个标准签密方案是随机数部分重用可再生的,且是 IND-CPA(IND-CCA2)和 euf-CMA 安全的,那么它也是 PRRU-IND-CPA(PRRU-IND-CCA2)和 PRRU-euf-CMA 安全的.下面我们用随机数部分重用可再生性定理来描述.

定理 1(可再生保密安全性). 给定一个定义 1 的标准签密方案$\Sigma=(Gen,Kgen,SC,DSC)$和一个多项式 $n(\cdot)$,设 k 为安全参数,接收方个数为自然数 $N=n(k)$,设 $M\Sigma=(Gen,Kgen,MSC,DSC)$是相应的 PRRU-MM-MR 签密方案(见定义 5).如果Σ是可再生的签密方案(见定义 10),那么对于任意多项式时间敌手 MA,存在着一个多项式时间敌手 A,对于任意安全参数 k 满足:

$$Adv^{N\text{-}MR\text{-}attk}_{M\Sigma',MA}(k)\leqslant n(k)\cdot Adv^{attk}_{\Sigma',A}(k).$$

证明:从保密性角度看,由于 IND-CCA2 是目前签密方案中最强的安全概念,一个 IND-CCA2 安全的签密方案意味着也同时满足 IND-CPA 安全性.因此,定理证明时我们只考虑 IND-CCA2 安全性情况,IND-CPA 安全情况也可同理得证.

设 MA 是一个多项式时间三阶敌手,可以攻击 PRRU-MM-MR 签密方案 $M\Sigma$的 IND-CCA2 安全性,我们构造一个三阶敌手 A,他将 MA 作为一个子过程调用(利用 MA 的知识)来攻击相应的标准签密方案Σ的 IND-CCA2

安全性.

首先,我们借鉴文献[8]的混合实验思路,结合 PRRU-MM-MR 多接收方签密的概念,构造一个混合实验 $HBExpH_j(k)$如下.

- $HBExpH_j(k)(1\leqslant j\leqslant N)$.

(1) $parm\leftarrow_{Rnd}Gen(k),(1^l,State)\leftarrow MA(select,N,parm)$;

(2) $(pk_S,sk_S)\leftarrow_{Rnd}Kgen(parm)$;

(3) 对 i=1,2,…,l,计算 $(pk_{R_i},sk_{R_i})\leftarrow_{Rnd} Kgen(parm)$;

(4) 计算 $(\boldsymbol{M}_0,\boldsymbol{M}_1,\boldsymbol{M},\boldsymbol{CoinsKgen},State)\leftarrow A^{MSC(\cdot),RO(\cdot),DSC^1(\cdot),\ldots,DSC^l(\cdot)}(Find,pk_{R_1},\ldots,pk_{R_l},State)$,其中,$((\boldsymbol{M}_0,\boldsymbol{M}_1)\in Mspc^l(parm),\boldsymbol{M}=(m_{l+1},\ldots,m_N)\in Mspc^{N-l}(parm),\boldsymbol{CoinsKgen}=(CoinsKgen_{l+1},CoinsKgen_{l+2},\ldots,CoinsKgen_N))$;

(5) 对 i=l+1,2,…,N,计算 $(pk'_{R_i},sk'_{R_i})\leftarrow Kgen(parm,CoinsKgen_i)$;

(6) 令 $\boldsymbol{PK}_R=(pk_{R_1},\ldots,pk_{R_l},pk'_{R_{l+1}},\ldots,pk'_{R_N})$;

(7) 如果 $j\leqslant l$,令 $\boldsymbol{M}^*=(m_1^*,\ldots,m_N^*)=(m_{01},\ldots,m_{0j},m_{1(j+1)},\ldots,m_{1l},m_{l+1},\ldots,m_N)$; 否则,令:

$$\boldsymbol{M}^*=(m_1^*,\ldots,m_N^*)=(m_{01},\ldots,m_{0l},m_{l+1},\ldots,m_N);$$

(8) $\bar{r}=(r_1,r_2,\ldots,r_d)\leftarrow_{Rnd} CoinsRu_{SC}(parm,sk_S)$;

(9) 对 i=1,2,…,N,选择 $\tilde{r}_{R_i}=(r_{(d+1)_i},r_{(d+2)_i},\ldots,r_{w_i})\leftarrow_{Rnd} CoinsNRu_{SC}(parm,sk_S,pk_{R_i})$, 令 $r_R=(r_1,r_2,\ldots,r_d,r_{(d+1)_i},\ldots,r_{w_i})$, 计算 $c_i^*=SC(sk_S,pk_{R_i},m_i^*,r_{R_i})$;

(10) 令 $\boldsymbol{C}^*=(c_1^*,\ldots,c_N^*),b'\leftarrow A^{MSC(\cdot),RO(\cdot),DSC^1(\cdot),\ldots,DSC^l(\cdot)}(Guess,\boldsymbol{C}^*,State)$(要求不能询问 $\boldsymbol{C}^*$的有关知识);

(11) 返回 b'.

设 p_j=Pr[$HBExpH_j(k)$=0].上述 $HBExpH_j(k)$实验中,当 $j=N$ 时,从敌手 MA 的角度看,此时的挑战密文 $\boldsymbol{M}^*$恰好与 $attkExp_{M\Sigma,MA}^{N\text{-}MR\text{-}CCA2\text{-}0}(k)$ 实验中的挑战密文相一致,于是可以得出:

$$p_N=\Pr[HBExpH_N(k)=0]=\Pr[attkExp_{M\Sigma,MA}^{N\text{-}MR\text{-}CCA2\text{-}0}(k)=0].$$

当 j=0 时,从敌手 MA 的角度看,此时的挑战密文 $\boldsymbol{M}^*$恰好与 $attkExp_{M\Sigma,MA}^{N\text{-}MR\text{-}CCA2\text{-}1}(k)$ 实验中的挑战密文是一致的,可以得出 $p_0=\Pr[attkExp_{M\Sigma,MA}^{N\text{-}MR\text{-}CCA2\text{-}1}(k)=0]$.因此,我们可以计算敌手 MA 的优势为 $Adv_{M\Sigma,MA}^{N\text{-}MR\text{-}CCA2}(k)=|p_n-p_0|$.

然后,我们构造一个三阶敌手 A,描述如下.

- $A(select,parm)$.

(1) $parm\leftarrow_{Rnd}Gen(k),(1^l,State')\leftarrow MA(select,N,parm),j\leftarrow_{Rnd}(1,\ldots,l)$;

(2) $j\leftarrow_{Rnd}(1,\ldots,l)$;

(3) 返回 $State$

- $A(Find,State,pk_R)$.

(1) $(pk_S,sk_S)\leftarrow_{Rnd}Kgen(parm)$;

(2) 若 $j\leqslant l$,对 i=1,…,j–1,j+1,…,l,计算 $(pk_{R_i},sk_{R_i})\leftarrow_{Rnd} Kgen(parm)$, 然后令 $pk_{R_j}=pk_R$; 否则,对 i=1,2,…,l,计算 $(pk_{R_i},sk_{R_i})\leftarrow_{Rnd} Kgen(parm)$;

(3) 计算 $(\boldsymbol{M}_0,\boldsymbol{M}_1,\boldsymbol{M},\boldsymbol{CoinsKgen},State')\leftarrow MA^{MSC(\cdot),RO(\cdot),DSC^1(\cdot),\ldots,DSC^l(\cdot)}(Find,pk_{R_1},\ldots,pk_{R_l},State')$, 其中,$((\boldsymbol{M}_0,\boldsymbol{M}_1)\in Mspc^l(parm),\boldsymbol{M}=(m_{l+1},\ldots,m_N)\in Mspc^{N-l}(parm),\boldsymbol{CoinsKgen}=(CoinsKgen_{l+1},CoinsKgen_{l+2},\ldots,CoinsKgen_N))$;

(4) 对 $i=l$+1,…,N,计算 $(pk'_{R_i},sk'_{R_i})\leftarrow Kgen(parm,CoinsKgen_i)$;

(5) 令 $\boldsymbol{PK}_R=(pk_{R_1},\ldots,pk_{R_l},pk'_{R_{l+1}},\ldots,pk'_{R_N})$;

(6) 如果 $j>l$,令 $m_{0j}\leftarrow m_j,m_{1j}\leftarrow m_j$;

(7) $State\leftarrow(State',l,j,\boldsymbol{M}_0,\boldsymbol{M}_1,\boldsymbol{M},pk_R)$;

(8) 返回$(m_{0j},m_{1j},State)$

- $A(Guess,c,State)$.

(1) 对 i=1,…,j–1,j+1,…,N,判断:如果 $i>l$,令 $m'\leftarrow m_i$;如果 $i\leqslant l$ 且 $i\leqslant j$,令 $m'\leftarrow m_{0i}$;如果 $i\leqslant l$ 且 $i>j$,令 $m'\leftarrow m_{1i}$.选择 $\tilde{r}_{R_i}\leftarrow_{Rnd} CoinsNRu_{SC}(parm,sk_S,pk_{R_i})$,然后计算 $c_i=RP(sk_S,pk_R,c,pk_{R_i},sk_{R_i},m',\tilde{r}_{R_i})$;

(2) 令 $\boldsymbol{C}'=(c_1,\ldots,c_{j-1},c,c_{j+1},\ldots,c_N)$;

(3) $b'\leftarrow MA^{MSC(\cdot),RO(\cdot),DSC^1(\cdot),\ldots,DSC^l(\cdot)}(Guess,\boldsymbol{C}',State')$ (要求不能询问 $\boldsymbol{C}'$的有关知识);

(4) 返回 b'.

上述构造中,对敌手 A 来说,j=1,2,…,N 是等概率,在 MA 的挑战密文中,接收方 R_j 的密文恰好是敌手 A 的挑战密文,而方案 $M\Sigma$的可再生性保证了挑战密文中所有 N 个密文使用了相同的部分随机数 $\bar{r}$.显然,实验 $attkExp_{\Sigma,A}^{CCA2\text{-}0}(k)$ 与实验 $HBExpH_j(k)$是一致的,可以得出 $\Pr[attkExp_{\Sigma,A}^{CCA2\text{-}0}(k)=0]=\frac{1}{N}\sum_{i=1}^{N}p_i$.

同理,实验 $attkExp_{\Sigma,A}^{CCA2\text{-}1}(k)$ 与实验 $HBExpH_{j-1}(k)$是一致的,可以得出 $\Pr[attkExp_{\Sigma,A}^{CCA2\text{-}1}(k)=0]=\frac{1}{N}\sum_{i=1}^{N}p_{i-1}$.于是,我们可以计算 A 的优势 $Adv_{\Sigma,A}^{CCA2}(k)=\frac{|p_n-p_0|}{N}$,从而可得 $Adv_{M\Sigma,MA}^{N\text{-}MR\text{-}CCA2}(k)=n(k)\cdot Adv_{\Sigma,A}^{CCA2}(k)$.由于敌手 A 将敌手 MA 作为一个子过程调用,A 可以利用 MA 的所有知识,因此综合可得:

$$Adv_{M\Sigma,MA}^{N\text{-}MR\text{-}attk}(k)\leqslant n(k)\cdot Adv_{\Sigma,A}^{attk}(k). \qquad \square$$

由上述定理 1 可知:如果标准签密方案Σ是随机数部分重用可再生的,且是 IND-CPA(IND-CCA2)安全的,即攻击者 A 的优势 $Adv_{\Sigma,A}^{attk}(k)$ 可以忽略,那么Σ对应的多接收方签密方案 $M\Sigma$中,攻击者 MA 的优势 $Adv_{M\Sigma,MA}^{N\text{-}MR\text{-}attk}(k)\leqslant n(k)\cdot Adv_{\Sigma,A}^{attk}(k)$ 也可以忽略.因此,采用定义 5 的方法基于标准方案Σ构造的多接收方方案 $M\Sigma$也是 IND-CPA(IND-CCA2)安全的.

定理 2(可再生不可伪造安全性). 给定一个标准签密方案Σ=(Gen,$Kgen$,SC,DSC)和一个多项式 $n(\cdot)$,设 k 为安全参数,接收方个数为自然数 $N=n(k)$,$M\Sigma$=(Gen,$Kgen$,MSC,DSC)是相应的 PRRU-MM-MR 签密方案.如果Σ是可再生的,那么对于任意多项式时间敌手 FA,存在着一个多项式时间敌手 FB,对任意安全参数 k,满足:

$$Adv_{M\Sigma,FA}^{N\text{-}MR\text{-}CMA}(k)\leqslant n(k)\cdot Adv_{\Sigma,FR}^{CMA}(k).$$

证明:如果一个多项式时间伪造者 FA 可以伪造 $M\Sigma$的签密文,我们构造一个伪造者 FR,他将实验的接收方 R 设置为 FA 伪造实验的接收方 R_j,并把 FA 作为一个子过程调用,攻击Σ的不可伪造安全性.

- ($State$)←FR($select$,$parm$).

(1) $parm\leftarrow_{Rnd}Gen(k)$,($State'$)←$FA$($select$,$N$,$parm$),$j\leftarrow_{Rnd}(1,\ldots,N)$;

(2) 选取:

$\boldsymbol{CoinsKgen}=(CoinsKgen_1,\ldots,CoinsKgen_{j-1},CoinsKgen_{j+1},\ldots,CoinsKgen_N)$,$State\leftarrow(State',j,\boldsymbol{CoinsKgen})$;

(3) 返回 $State$

- $(m,c)\leftarrow FB^{SC(\cdot),RO(\cdot)}(State',pk_S,pk_R,sk_R)$.

(1) 对于 i=1,…,j–1,j+1,…,l,计算 $(pk_{R_i},sk_{R_i})\leftarrow_{Rnd}Kgen(parm,CoinsKgen_i)$,$(pk_{R_j},sk_{R_j})\leftarrow(pk_R,sk_R)$,令:

$$\boldsymbol{PK}_R=(pk_{R_1},\ldots,pk_{R_N}),\boldsymbol{SK}_R=(sk_{R_1},\ldots,sk_{R_N});$$

(2) 计算$(m_i,c_i)\leftarrow F^{MSC(\cdot),RO(\cdot)}(pk_S,\boldsymbol{PK}_R,\boldsymbol{SK}_R)$,其中,$i\in(1,2,\ldots,N)$.如果满足 $DSC^{RO(\cdot)}(c_i,pk_S,sk_{R_i})=m_i$ 且没有向签密预言机 $MSC(\cdot)$询问过 m_i 的签密,选取 $\tilde{r}_{R_j}\leftarrow_{Rnd}CoinsNRu_{SC}(parm,sk_S,pk_{R_j})$,然后计算:

$$c_j=RP(sk_S,pk_{R_i},c_i,pk_{R_j},sk_{R_j},m_j,\tilde{r}_{R_j});$$

(3) 返回(m_j,c_j).

上述过程中,FA 如果赢得了游戏,输出一对合法的签密文(m_i,c_i).对于任意接收方 R_j,伪造者利用再生算法 RP 可以构造出一对合法的签密文(m_j,c_j),因此有 $\Pr[ForgeExp_{\Sigma,FR_1}^{CMA}(k)=1]=\ldots=\Pr[ForgeExp_{\Sigma,FR_N}^{CMA}(k)=1]$.

对 FR 的伪造实验 $ForgeExp_{\Sigma,FR_j}^{CMA}(k)$ 来说,伪造的签密文需要通过特定的一个接收方 R_j 的验证才能赢得游戏;而对 FA 的伪造实验 $ForgeExp_{M\Sigma,FA}^{N\text{-}MR\text{-}CMA}(k)$ 来说,伪造的签密文只要任意一个接收方通过验证即可赢得游戏,因

此, $\Pr[ForgeExp_{M\,\Sigma,FA}^{N\text{-}MR\text{-}CMA}(k)=1]=\sum_{j=1}^{N}\Pr[ForgeExp_{\Sigma,FR_j}^{CMA}(k)=1]=N\Pr[ForgeExp_{\Sigma,FR}^{CMA}(k)=1]$. 又由于 FR 把 FA 作为子过程调用,则可以利用 FA 的所有知识,综合可得:

$$Adv_{M\,\Sigma,FA}^{N\text{-}MR\text{-}CMA}(k)\leqslant n(k)\cdot Adv_{\Sigma,FR}^{CMA}(k).$$ □

由上述定理 2 可知:如果标准签密方案Σ是随机数部分重用可再生的,且是 euf-CMA 安全的,即伪造者 FR 的优势 $Adv_{\Sigma,FR}^{CMA}(k)$ 是可以忽略的,那么对应的多接收方签密方案 $M\Sigma$中,伪造者 FA 的优势 $Adv_{M\,\Sigma,FA}^{N\text{-}MR\text{-}CMA}(k)\leqslant n(k)\cdot Adv_{\Sigma,FR}^{CMA}(k)$ 也是可以忽略的.因此,采用定义 5 的方法基于标准方案Σ构造的多接收方签密方案 $M\Sigma$也是 euf-CMA 安全的.

4 基于格的随机数部分重用 MM-MR 签密方案

本节主要采用随机数部分重用理论,证明路秀华等人(LWWD16)[18]的无陷门格基签密方案Σ=(*Gen*,*Kgen*,*SC*,*DSC*)是随机数部分重用可再生的签密方案;然后,基于该方案构造一个 PRRU-MM-MR 签密方案,并证明方案的安全性,分析方案在系统开销方面的节约.

4.1 格相关知识

4.1.1 格

设 $n\geqslant k>0$,k 维格$\boldsymbol{\Lambda}$是$\mathbb{R}^n$的一个子群,它包含 k 个线性独立的向量组$\{\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_k\}=\boldsymbol{B}$ 的所有线性组合,例如,$\boldsymbol{\Lambda}=\boldsymbol{\Lambda}(\boldsymbol{B})=\{\boldsymbol{Bx}|\boldsymbol{x}\in\mathbb{Z}^k\}$.定义格的秩为 $\det(\boldsymbol{\Lambda}(\boldsymbol{B}))=\sqrt{\det(\boldsymbol{B}^T\boldsymbol{B})}$.如果 $q\mathbb{Z}\subset\boldsymbol{\Lambda}$,那么$\boldsymbol{\Lambda}\in\mathbb{Z}^n$被称作 q-ary 格.

4.1.2 高斯分布

定义 11[19]. 对于任意参数 $s>0$,我们定义$\mathbb{R}^n$上中心为 $\boldsymbol{c}$ 的高斯函数:

$$\forall x\in\mathbb{R}^n,\rho_{s,c}(\boldsymbol{x})=\exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/s^2).$$

当 s 和 $\boldsymbol{c}$ 省略时,表示它们分布取 0 和 1.

定义 12[19]. 对于任意 $\boldsymbol{c}\in\mathbb{R}^n$、实数 $s>0$、n 维格$\boldsymbol{\Lambda}$,定义$\boldsymbol{\Lambda}$上的离散高斯分布:

$$\forall x\in\boldsymbol{\Lambda},D_{\Lambda,s,c}(\boldsymbol{x})=\rho_{s,c}(\boldsymbol{x})/\rho_{s,c}(\boldsymbol{\Lambda}).$$

4.1.3 困难问题

定义 13(LWE 分布)[20]. 设 q 为素数或素数的幂积,n 为正整数,χ为某一错误分布,向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$. 定义 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的 LWE 分布 $A_{s,\chi}=(\boldsymbol{a},b=\langle\boldsymbol{a},\boldsymbol{s}\rangle+e \bmod q)$,其中,$e\leftarrow\chi$, $\boldsymbol{a}\in\mathbb{Z}_q^n$ 是均匀随机选取的.

定义 14(判定性 $\boldsymbol{LWE_{q,n,m,\chi}}$问题)[20]. 对于 m 次独立抽样 $(\boldsymbol{a}_i,b_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$, 区分它们是从两个分布中的哪一个抽样的:(1) LWE 分布 $A_{s,\chi}$,其中,每次抽样 $\boldsymbol{s}\in\mathbb{Z}_q^n$ 都相同;(2) $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的均匀分布.

定义 15(小整数解 $\boldsymbol{SIS_{n,q,\beta,m}}$ 问题)[20]. 设 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 是由 m 次独立抽样 $\boldsymbol{a}_i\in\mathbb{Z}_q^n$ 组成的矩阵,找到一个非零的整数向量 $\boldsymbol{z}\in\mathbb{Z}^m$,其中,$\|\boldsymbol{z}\|<\beta$,满足:

$$\boldsymbol{Az}=\sum_i\boldsymbol{a}_i\cdot z_i=0\in\mathbb{Z}_q.$$

4.2 LWWD16签密方案介绍

LWWD16 无陷门格基签密方案Σ=(*Gen*,*Kgen*,*SC*,*DSC*)是一个四元组.

- *Gen*(系统初始化).

(1) 设 k 为安全参数,$n=2k$,参数ω使得不等式 $2^{\omega}\binom{k}{\omega}\geqslant 128$ 成立,选取小自然数 M(典型地可取 8)和 d(典型地可取 24),参数 $0<\alpha<1$,模数 $q\geqslant 2^d$,令 $\sigma=\alpha q$, $u=7\sigma\sqrt{\omega k}$, $U=14\sigma\sqrt{\omega}(k-1)$;

(2) D_σ和 D_u 是均值为 0、标准差分别为σ和 u 的高斯分布;

(3) 选取矩阵 $\boldsymbol{A}\leftarrow_{Rnd}\mathbb{Z}_q^{n\times k}$, 选取一个安全的对称加密算法$(Enc_{key}(\cdot),Dec_{key}(\cdot))$,其中,$key$ 为对称密钥,密钥

空间用 $keysp(k)$表示;

(4) 选取 3 个抗碰撞的哈希函数(H_1,H_2,H_3),其中,$H_1:\{0,1\}^*\to\{\boldsymbol{v}:\boldsymbol{v}\in\{-1,0,1\}^k,\|\boldsymbol{v}\|_1\leqslant\omega\}$,$H_2:\{0,1\}^k\to keysp(k)$,$H_3:\{0,1\}^*\times\{0,1\}^*\to IT(keysp(k)$表示密钥空间,$IT$表示多次抛硬币得到的随机空间.设 $keysp(k)$和IT空间大小分别为 f_1 与 f_2).

- *Kgen*(密钥生成算法).

(1) 选取矩阵 $\boldsymbol{X}\leftarrow_{Rnd}\mathbb{Z}_q^{k\times k}$,$\boldsymbol{E}\leftarrow_{Rnd}\mathbb{Z}_q^{n\times k}$, 要求 $\boldsymbol{X}$ 和 $\boldsymbol{E}$ 的所有分量大小都不超过 7σ,若不满足,则重新选择;

(2) 计算 $\boldsymbol{B}=\boldsymbol{AX}+\boldsymbol{E}(\bmod q)$;

(3) 返回发送方 S 的公私钥对$(pk_S=\boldsymbol{B}_S,sk_S=\boldsymbol{X}_S)$,接收方 R 的公私钥对 $pk_R=\boldsymbol{B}_R,sk_R=\boldsymbol{X}_R$.

- $SC(sk_S,pk_R,m)$(签密算法).

(1) 选取 $y\leftarrow_{Rnd}D_u^k$;

(2) 计算 $\boldsymbol{b}=H_1(\lfloor\boldsymbol{Ay}(\bmod q)\rceil_d,m)$和 $\boldsymbol{z}=\boldsymbol{X}_S\boldsymbol{b}+\boldsymbol{y}$,其中,$\lfloor x\rceil_d=(x-[x]_{2^d})/2^d$,$[x]_{2^d}$ 表示唯一的一个在区间$(-2^{d-1},2^{d-1}]$中满足 $x\equiv[x]_{2^d}(\bmod 2^d)$ 的整数;

(3) 计算 $\boldsymbol{w}=\boldsymbol{Az}-\boldsymbol{B}_S\boldsymbol{b}(\bmod q)$,如果 $\boldsymbol{w}$ 的某个分量 w_i 不满足$|[w_i]_{2^d}|\leqslant 2^{d-1}-7\sigma\omega$, 返回步骤(1)重新开始;

(4) 根据概率 $\min\left(\dfrac{D_u^k(\boldsymbol{z})}{MD_{u,X_S\boldsymbol{b}}^k(\boldsymbol{z})},1\right)$保留$(\boldsymbol{z},\boldsymbol{b})$;

(5) 选取随机数$\boldsymbol{\tau}\in\{0,1\}^k$,计算 $\mu=Enc_{H_2(\boldsymbol{\tau})}(m,\boldsymbol{z},\boldsymbol{b})$;

(6) 选取错误向量 $\boldsymbol{e}_1\leftarrow_{Rnd}D_\sigma^n,\boldsymbol{e}_2\leftarrow_{Rnd}D_\sigma^k$, 令$\theta=H_3(\boldsymbol{\tau},\mu)$,由$\theta$的随机性选取错误向量 $\boldsymbol{e}_3\leftarrow D_\sigma^k$, 计算:

$$\boldsymbol{v}_1^T=-\boldsymbol{e}_1^TA+\boldsymbol{e}_2^T(\bmod q),\boldsymbol{v}_2^T=\boldsymbol{e}_1^T\boldsymbol{B}_R+\boldsymbol{e}_3^T+\boldsymbol{\tau}\lfloor q/2\rfloor(\bmod q);$$

(7) 返回密文 $c=(\boldsymbol{v}_1,\boldsymbol{v}_2,\mu)$.

- $DSC(pk_S,sk_R,c)$(解签密算法).

(1) 计算 $\boldsymbol{\tau}'=(\tau_1',...,\tau_k')\leftarrow\boldsymbol{v}_1^T\boldsymbol{X}_R+\boldsymbol{v}_2^T(\bmod q)$;

(2) 对 i=1,…,k,如果 $\tau_i'\in[-q/4,q/4]$, 令 $\tau_i'=0$; 否则,令 $\tau_i'=1$;

(3) 令$\boldsymbol{\tau}\leftarrow\boldsymbol{\tau}'$;

(4) 计算 $(m,\boldsymbol{z},\boldsymbol{b})=Dec_{H_2(\tau)}(\mu)$;

(5) 验证 $\boldsymbol{b}=H_1(\lfloor\boldsymbol{Az}-\boldsymbol{B}_S\boldsymbol{b}(\bmod q)\rceil_d,m)$以及$\|\boldsymbol{z}\|_2\leqslant U$是否成立:如果成立,则输出明文 m;否则,输出终止符号$\perp$.

方案的正确性详见文献[18],下面我们给出安全性描述.

引理 3(保密安全性). 在随机预言机模型下,如果存在敌手 A,进行不多于 q_{SC} 次签密询问、q_{DSC} 次解签密询问、 q_{H_1} 次预言机 H_1 询问、 q_{H_2} 次预言机 H_2 询问、 q_{H_3} 次预言机 H_3 询问,以不可忽略的优势ε_A攻击上述标准签密方案Σ的 IND-CCA2 安全性,那么存在敌手 B,以不可忽略的优势 $\varepsilon_B\geqslant\varepsilon_A\left[1-q_{DSC}\left(\dfrac{q_{H_1}}{2^k}+\dfrac{q_{H_2}}{2^{f_1}}+\dfrac{q_{H_3}}{2^{f_2}}\right)\right]$攻破判定性带差错的学习(LWE)问题[18].

路秀华等人已给出了方案保密性的可证明安全性,这里不再介绍,详见 LWWD16 定理 2.需要说明的是:在签密算法 SC 的步骤(6)中,我们将错误向量 $\boldsymbol{e}_1$、$\boldsymbol{e}_2$ 的选取方式由原方案根据θ的随机性选取描述为随机选取,这并不影响解密.由于θ是伪随机的,描述为随机选取不会降低方案的任何安全性.可以看出,它也不影响 LWWD16 定理 2 的证明过程.由于假定了 H_3 是一个随机预言机,在随机预言机模型下,$\theta=H_3(\boldsymbol{\tau},\mu)$的随机性与真随机是不可区分的,因此,上述方式选取的错误向量 $\boldsymbol{e}_1$、$\boldsymbol{e}_2$ 与原方案的错误向量 $\boldsymbol{e}_1$、$\boldsymbol{e}_2$ 在随机预言机模型下是不可区分的,即方案的安全性是等价的.由于 LWWD16 定理 2 并没有给出量化的优势,下面我们分析敌手 B 的优势量化.

从 LWWD16 定理 2 的证明过程可以看出:导致模拟不完美的唯一事件是合法密文在解签密询问时被拒绝,它是由哈希函数(H_1,H_2,H_3)的模拟引起的,其中,对 H_1 询问的模拟,该概率不会超过 $q_{H_1}/2^k$; 对 H_2 询问的模拟,该概率不会超过 $q_{H_2}/2^{f_1}$; 对 H_3 询问的模拟,该概率不会超过 $q_{H_3}/2^{f_2}$.对于 q_{DSC} 次解签密询问来说,总概率不超过

$q_{DSC}\left(\frac{q_{H_1}}{2^k}+\frac{q_{H_2}}{2^{f_1}}+\frac{q_{H_3}}{2^{f_2}}\right)$.综合可得,敌手 B 的优势 $\varepsilon_B \geqslant \varepsilon_A\left[1-q_{DSC}\left(\frac{q_{H_1}}{2^k}+\frac{q_{H_2}}{2^{f_1}}+\frac{q_{H_3}}{2^{f_2}}\right)\right]$.

引理 4(不可伪造安全性). 在随机预言机模型下,如果存在伪造者 FA,运行时间为 t_{FA},进行不多于 q_{SC} 次签密询问、q_{H_1} 次预言机 H_1 询问、q_{H_2} 次预言机 H_2 询问、q_{H_3} 次预言机 H_3 询问,在 $ForgeExp^{CMA}_{\Sigma,FA}(k)$ 实验中,以不可忽略的优势 ε_{FA} 伪造一个上述标准签密方案 Σ 的合法签密文,那么存在敌手 FB,以不可忽略的优势 $\varepsilon_{FB} \geqslant \varepsilon_{FA}\left(1-\frac{q_{SC}q_{H_1}}{2^k}-\frac{1}{2^{k^2}}\right)$ 攻破小整数解(SIS)问题[18].

路秀华等人已给出了方案不可伪造性的可证明安全性,这里不再介绍,详见 LWWD16 定理 3.由于 LWWD16 定理 2 并没有给出量化的优势,下面我们分析敌手 FB 的量化优势.

在签密询问阶段,敌手 FB 应答失败的概率为 $q_{SC}q_{H_1}/2^k$;在解签密阶段,由于 FB 扮演真实解密者,他不能拒绝一个合法的签密文.另外,伪造者 FA 在不经过询问的情况下,伪造一个合法密文的概率相当于猜测私钥的概率,大小为 $1/2^{k^2}$. 综合可得,敌手 FB 的优势 $\varepsilon_{FB} \geqslant \varepsilon_{FA}\left(1-\frac{q_{SC}q_{H_1}}{2^k}-\frac{1}{2^{k^2}}\right)$.

4.3 PRRU-MM-MR签密方案

4.3.1 LWWD16 方案的可再生性

LWWD16 方案中,签密算法共包含 5 个随机数.不难看出,该方案并不满足随机数全重用的安全条件(典型地,随机数 τ 在解签密过程中被接收方解密,如果重用该随机数,在考虑内部攻击的模型下,方案的安全性必然受到影响).但是需要指出的是,该方案满足重用两个随机数的安全条件.下面我们基于随机数部分重用可再生的签密方案的定义,证明该方案是随机数部分重用可再生的;并基于此标准签密方案 Σ 构造一个 PRRU-MM-MR 签密方案 $M\Sigma$,通过重用部分随机数,该方案在不牺牲安全性的条件下节约了计算和通信开销.

定理 5. 对上述标准签密方案 Σ=(*Gen*,*Kgen*,*SC*,*DSC*),令 $\bar{r}=(\boldsymbol{e}_1,\boldsymbol{e}_2)$,$\tilde{r}_R=(\boldsymbol{y},\boldsymbol{\tau},\boldsymbol{e}_3)$, 那么 Σ 是重用随机数 $\bar{r}$ 可再生的.

证明:设一个发送方的私钥 sk_S,一个接收方的公钥 pk_R,一个签密文 c=($\boldsymbol{v}_1$,$\boldsymbol{v}_2$,μ)(某个随机消息 m 经该公钥生成的签密文),另一个随机消息 m',另一个接收方的公私钥对($pk_{R'}$,$sk_{R'}$)以及非重用部分随机数 $\tilde{r}_{R'}=(\boldsymbol{y}',\boldsymbol{\tau}',\boldsymbol{e}_3')$, 下面我们构造一个多项式时间再生算法 RP,输出一个合法签密文 $c'=(\boldsymbol{v}_1,\boldsymbol{v}_2',\mu')$.

- $RP(sk_S, pk_R, c, pk_{R'}, sk_{R'}, m', \tilde{r}_{R'})$.

(1) 选取 $y' \leftarrow_{Rnd} D_u^k$;

(2) 计算 $\boldsymbol{b}'=H_1(\lfloor \boldsymbol{A}\boldsymbol{y}' (\mathrm{mod}\ q) \rceil_d, m')$,$\boldsymbol{z}'=\boldsymbol{X}_S\boldsymbol{b}'+\boldsymbol{y}'$;

(3) 计算 $\boldsymbol{w}'=\boldsymbol{A}\boldsymbol{z}'-\boldsymbol{B}_S\boldsymbol{b}' (\mathrm{mod}\ q)$,如果 $\boldsymbol{w}'$ 的某个分量 w_i' 不满足 $|[w_i']_{2^d}| \leqslant 2^{d-1}-7\sigma\omega$, 返回步骤(1)重新开始;

(4) 根据概率 $\min\left(\frac{D_u^k(\boldsymbol{z}')}{MD_{u,\boldsymbol{X}_S\boldsymbol{b}'}^k(\boldsymbol{z}')},1\right)$ 保留($\boldsymbol{z}'$,$\boldsymbol{b}'$);

(5) 选取随机数 $\boldsymbol{\tau}' \in \{0,1\}^k$,计算 $\mu'=Enc_{H_2(\boldsymbol{\tau}')}(m',\boldsymbol{z}',\boldsymbol{b}')$;

(6) 令 $\boldsymbol{\tau}'=(\tau_1',...,\tau_k')$,对 i=1,…,k,如果 $\tau_i'=0, \tau_i'' \leftarrow_{Rnd} [-\lfloor q/4 \rfloor, \lfloor q/4 \rfloor]$; 否则, $\tau_i'' \leftarrow_{Rnd} [q/2-\lfloor q/4 \rfloor, q/2+\lfloor q/4 \rfloor]$,令: $\boldsymbol{\tau}''=(\tau_1'',...,\tau_k'')$;

(7) 计算 $\boldsymbol{v}_2'^T=\boldsymbol{\tau}''-\boldsymbol{v}_1^T\boldsymbol{X}_{R'} (\mathrm{mod}\ q)$;

(8) 返回密文 $c'=(\boldsymbol{v}_1,\boldsymbol{v}_2',\mu')$.

根据上述 RP 的构造,显然有 $DSC(pk_S,sk_{R'},c')=m'$,因此它是消息 m' 一个合法签密文,又签密文 c 与 c' 使用了部分相同的随机数 $\bar{r}$, 综合可得 $SC(sk_S, pk_{R'}, m', \bar{r}, \tilde{r}_{R'}) = RP(sk_S, pk_R, c, pk_{R'}, sk_{R'}, m', \tilde{r}_{R'})$. 根据可再生的签密方案定义 10 可得,$\Sigma$ 是重用随机数 $\bar{r}$ 可再生的. □

4.3.2 PRRU-MM-MR 签密方案的构造

对于上述标准签密方案Σ=(*Gen*,*Kgen*,*SC*,*DSC*)和安全参数 k,设 $n(\cdot)$为某个多项式,接收方个数为自然数 $N=n(k)$,定义$M\Sigma$=(*Gen*,*Kgen*,*MSC*,*DSC*)是相应的PRRU-MM-MR签密方案,发送方公私钥对(pk_S,sk_S),接收方公钥向量 $PK_R=(pk_{R_1},pk_{R_2},...,pk_{R_N})$,明文向量 $M=(m_1,m_2,\ldots,m_N)$,其中,$m_i\in Mspc(parm)(1\leqslant i\leqslant N)$为发送方 S 发送给接收方 R_i 的消息,参数生成算法 *Gen*,密钥生成算法 *Kgen* 以及解签密算法 *DSC* 与方案Σ相同,签密算法 *MSC* 的构造如下.

(1) 计算$(pk_S,sk_S)\leftarrow_{Rnd}Kgen(parm)$;

(2) 对于 $i=1,2,\ldots,N$,计算 $(pk_{R_i},sk_{R_i})\leftarrow_{Rnd}Kgen(parm)$;

(3) 设 $\bar{r}=(r_1,r_2)=(\boldsymbol{e}_1,\boldsymbol{e}_2)$, 其中,$(\boldsymbol{e}_1,\boldsymbol{e}_2)$的选取同 SC 算法;

(4) 对 $i=1,2,\ldots,N$,选择 $\tilde{r}_{R_i}=(\boldsymbol{y}_i,\boldsymbol{\tau}_i,\boldsymbol{e}_{3i})$, 其中,$(\boldsymbol{y}_i,\boldsymbol{\tau}_i,\boldsymbol{e}_{3i})$的选取同 SC 算法.令 $r_{R_i}=(\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{y}_i,\boldsymbol{\tau}_i,\boldsymbol{e}_{3i})$, 计算:

$$c_i=(\boldsymbol{v}_1,\boldsymbol{v}_{2i},\mu_i)=SC(sk_S,pk_{R_i},m_i,r_{R_i});$$

(5) 返回 $C=(\boldsymbol{v}_1,\boldsymbol{v}_{21},\mu_1,\boldsymbol{v}_{22},\mu_2,\ldots,\boldsymbol{v}_{2N},\mu_N)$.

发送方 S 将密文广播给接收方,对 $i=1,2,\ldots,N$,每个接收方 R_i 获得自己的密文$(c_i=(\boldsymbol{v}_1,\boldsymbol{v}_{2i},\mu_i))$.

上述构造的多接收方签密方案是基于定义 5 描述的基于标准签密方案重用部分随机数来构造多接收方签密方案的通用方法构造的,由标准签密方案Σ可得 $DSC(pk_S,sk_{R'},c')=m'$,即上述 PRRU-MM-MR 签密方案满足正确性,下面我们分析方案的安全性.

4.3.3 安全性

定理 6(保密安全性). 在随机预言机模型下,如果存在敌手 *MA*,进行不多于 q_{MSC} 次签密询问、q_{DSC} 次解签密询问、q_{H_1} 次预言机 H_1 询问、q_{H_2} 次预言机 H_2 询问、q_{H_3} 次预言机 H_3 询问,以不可忽略的优势ε_{MA}攻击上述 PRRU-MM-MR 签密方案 $M\Sigma$的 IND-CCA2 安全性,那么存在敌手 B,以不可忽略的优势$\varepsilon_B\geqslant\frac{\varepsilon_{MA}}{N}\left[1-q_{DSC}\left(\frac{q_{H_1}}{2^k}+\frac{q_{H_2}}{2^{f_1}}+\frac{q_{H_3}}{2^{f_2}}\right)\right]$攻破判定性 LWE 问题.

证明:由定理 5 可得,上述多接收签密方案 $M\Sigma$所基于的标准签密方案Σ是可再生的.由保密再生性定理 1,如果标准签密方案Σ是可再生的签密方案,那么对于相应的多接收方签密方案 $M\Sigma$的任意多项式时间敌手 *MA*,存在着一个多项式时间敌手 A,对于任意安全参数 k,满足 $\varepsilon_{MA}=Adv_{M\Sigma,MA}^{N\text{-}MR\text{-}CCA2}(k)\leqslant N\cdot Adv_{\Sigma,A}^{CCA2}(k)$. 然后,由引理 3 可得,方案$\Sigma$是 IND-CCA2 安全的.如果存在敌手 A,以不可忽略的优势 $\varepsilon_A=Adv_{\Sigma,A}^{CCA2}(k)$ 攻击上述标准签密方案Σ的IND-CCA2安全性,那么存在敌手B,以不可忽略的优势 $\varepsilon_B\geqslant\varepsilon_A\left[1-q_{DSC}\left(\frac{q_{H_1}}{2^k}+\frac{q_{H_2}}{2^{f_1}}+\frac{q_{H_3}}{2^{f_2}}\right)\right]$攻破判定性带差错的学习(LWE)问题.综合可得 $\varepsilon_B\geqslant\varepsilon_A\left[1-q_{DSC}\left(\frac{q_{H_1}}{2^k}+\frac{q_{H_2}}{2^{f_1}}+\frac{q_{H_3}}{2^{f_2}}\right)\right]\geqslant\frac{\varepsilon_{MA}}{N}\left[1-q_{DSC}\left(\frac{q_{H_1}}{2^k}+\frac{q_{H_2}}{2^{f_1}}+\frac{q_{H_3}}{2^{f_2}}\right)\right]$, 上述 PRRU-MM-MR 签密方案 $M\Sigma$的 IND-CCA2 的安全性得证. □

定理 7(不可伪造安全性). 在随机预言机模型下,如果存在伪造者 *MFA*,进行不多于 q_{MSC} 次签密询问、q_{DSC} 次解签密询问、q_{H_1} 次预言机 H_1 询问、q_{H_2} 次预言机 H_2 询问、q_{H_3} 次预言机 H_3 询问,以不可忽略的优势ε_{MFA}攻击上述 PRRU-MM-MR 签密方案 $M\Sigma$的 euf-CMA 安全性,那么存在敌手 *FB*,以不可忽略的优势$\varepsilon_{FB}\geqslant\frac{\varepsilon_{MFA}}{N}\left(1-\frac{q_{SC}q_{H_1}}{2^k}-\frac{1}{2^{k^2}}\right)$攻破 SIS 问题.

证明:由定理 5 可得,上述多接收签密方案 $M\Sigma$所基于的标准签密方案Σ是可再生的.再由不可伪造再生性定理 2 可得:如果Σ是可再生的,那么对于相应的多接收方签密方案 $M\Sigma$的任意多项式时间伪造者 *FA*,存在着一个多项式时间伪造者 *FR*,对于任意安全参数 k,满足 $\varepsilon_{MFA}=Adv_{M\Sigma,FA}^{N\text{-}MR\text{-}CMA}(k)\leqslant N\cdot Adv_{\Sigma,FR}^{CMA}(k)$. 然后,由引理 4 可得,方案$\Sigma$

是 euf-CMA 安全的.如果存在伪造者 FR 以不可忽略的优势 $\varepsilon_{FR}=Adv_{\Sigma,FR}^{CMA}(k)$ 伪造一个上述标准签密方案Σ的合法签密文,那么存在敌手 FB,以不可忽略的优势 $\varepsilon_{FB}\geqslant\varepsilon_{FA}\left(1-\frac{q_{SC}q_{H_1}}{2^k}-\frac{1}{2^{k^2}}\right)$ 攻破小整数解(SIS)问题.

综合可得 $\varepsilon_{FB}\geqslant\varepsilon_{FA}\left(1-\frac{q_{SC}q_{H_1}}{2^k}-\frac{1}{2^{k^2}}\right)\geqslant\frac{\varepsilon_{MFA}}{N}\left(1-\frac{q_{SC}q_{H_1}}{2^k}-\frac{1}{2^{k^2}}\right)$,上述 PRRU-MM-MR 签密方案 $M\Sigma$的 euf-CMA 安全性得证. □

4.3.4 相关参数的选取

本文的多接收方签密方案是基于标准签密方案 LWWD16 构造的,相关参数值的选取与 LWWD16 方案相同.由于 LWWD16 的方案中只对某些参数选取给出了简要说明,并未给出详细的参数选取,结合 LWWD16 的前人工作 BG14[21],我们在表 1 中给出具体的参数选取及建议值.

Table 1 Parameter selection and recommended values

表 1 参数选取及建议值

参数	选取要求	建议值
n k	n=2k	1 280 640
ω	$2^{\omega}\binom{k}{\omega}\geqslant 128$	18
log$q$ d	$q\geqslant 2^d$	34 24
B	$B=14\sigma\sqrt{\omega}(k-1)$	2.201×10^6
α ω	$\sigma=\alpha q$	3.376×10^{-9} 58
u	$u=7\sigma\sqrt{\omega k}$	4.358×10^4
N	正整数	1 000

4.3.5 效率分析

随机数重用的多接收方签密在保持高安全性的同时,可节约系统开销.这里,我们首先将本文多接收方签密方案与所基于的标准签密方案 LWWD16 进行比较,然后再将其与现有的基于格的多接收方签密进行比较.

考虑发送方 S 有 N 个消息分别发送给 N 个不同用户的情况.采用上述标准签密方案Σ签密,共需运行签密算法 N 次;而采用上述 PRRU-MM-MR 签密方案,由于重用了随机数 $\boldsymbol{e}_1$ 和 $\boldsymbol{e}_2$,各接收方的密文中 $\boldsymbol{v}_1$ 是相同的,于是,$\boldsymbol{v}_1$ 只需计算 1 次并广播即可,因此显著地节约了系统计算和通信开销.表 2 给出了该通信场景下标准签密方案 LWWD16 与 PRRU-MM-MR 签密方案 $M\Sigma$的效率对比,其中,公私钥尺寸只表示一个用户的量,l_{me} 表示消息长度,l_{ID} 表示身份的比特长度,模数 q 为安全参数 k 的多项式,S_D 表示高斯采样运算,S_T 表示原像抽样,S_B 表示陷门基抽样,*Invert* 表示带陷门的求逆运算,l_r 表示安全随机数 r 的比特长度,M_V 表示矩阵向量乘法运算.

Table 2 Efficiency comparison between LWWD16 and $M\Sigma$ (N messages-N receivers)

表 2 LWWD16 与 $M\Sigma$的效率对比(N 消息-N 接收方)

	LWWD16	方案 $M\Sigma$	节约开销
密文量	$N(l_{me}+4k\log q)$	$N(l_{me}+3k\log q)+k\log q$	$k(N-1)\log q$
签密运算量	$N(4S_D+6M_V)$	$N(4S_D+5M_V)+M_V$	$(N-1)M_V$
解签密运算量	$3M_V$	$3M_V$	0

从上表可以看出:方案 $M\Sigma$与 LWWD16 相比,在密文量上节省了 $\frac{k(N-1)\log q}{N(l_{me}+4k\log q)}$(当 N 较大时,由于基于格的签密消息大小远小于密文增量,密文量上节省约 25%);在签密运算量上节省了 $\frac{(N-1)M_V}{N(4S_D+6M_V)}$(当 N 较大时,签密运算的计算量得到显著节约).

为了密文量对比更直观,我们根据 LWWD16 和 BG14 的工作,对相关参数取建议值 k=640,l_{me}=64,log$q$=34,N=1000,可得签密方案Σ与 $M\Sigma$的密文量对比(N 消息-N 接收方)见表 3.

Table 3 Ciphertex size comparison between LWWD16 and $M\Sigma$ (N messages-N receivers)

表 3 LWWD16 与 $M\Sigma$的密文量对比(N 消息-N 接收方)

	LWWD16	方案 $M\Sigma$	节约开销	节约开销百分比
密文量(bit)	8.7104×10^7	6.5366×10^7	2.1738×10^7	24.95%

接下来,将本文的 PRRU-MM-MR 签密方案 $M\Sigma$与现有的两个基于格的单消息多接收方(SM-MR)签密方案 LWJ13[22]和 ZXX18[23]进行比较(目前,基于格的签密成果并不丰富,还未见基于格的多消息多接收方(MM-MR)签密相关方案).

值得注意的是:SM-MR 签密方案只能发送 1 个消息到 N 个接收方,当需要发送 N 个不同消息到 N 个接收方时,SM-MR 签密方案需要运行 N 次;而 MM-MR 签密方案只需运行 1 次.我们在表 4 中给出了发送 1 个消息到 N 个接收方情况下的效率对比,在表 5 中给出了发送 N 个消息到 N 个接收方情况下的效率对比.

Table 4 Efficiency comparison of related lattice-based signcryption schemes (1 message-N receivers)

表 4 相关基于格的多接收方签密方案效率对比(1 消息-N 接收方)

	LWJ13	ZXX18	方案 $M\Sigma$
公钥尺寸(bit)	$nk\log q$	$nk\log q$	$nk\log q$
私钥尺寸(bit)	$k^2\log q$	$k^2\log q$	$k^2\log q$
密文量(bit)	$l_{me}+l_r+Nk\log q$	$N(l_{me}+l_{ID}+k\log q)+l_r$	$N(l_{me}+3k\log q)+k\log q$
签密运算量	NS_T+M_V	$N(S_T+2M_V)$	$N(4S_D+5M_V)+M_V$
解签密运算量	S_B+2M_V	$M_V+Invert$	$3M_V$

Table 5 Efficiency comparison of related lattice-based signcryption schemes (N messages-N receivers)

表 5 相关基于格的多接收方签密方案效率对比(N 消息-N 接收方)

	LWJ13	ZXX18	方案 $M\Sigma$
公钥尺寸(bit)	$nk\log q$	$nk\log q$	$nk\log q$
私钥尺寸(bit)	$k^2\log q$	$k^2\log q$	$k^2\log q$
密文量(bit)	$N(l_{me}+l_r+Nk\log q)$	$N(N(l_{me}+l_{ID}+k\log q)+l_r)$	$N(l_{me}+3k\log q)+k\log q$
签密运算量	$N(NS_T+M_V)$	$N(N(S_T+2M_V))$	$N(4S_D+5M_V)+M_V$
解签密运算量	S_B+2M_V	$M_V+Invert$	$3M_V$

为了上述对比更直观,我们对相关参数取建议值 k=640,n=1280,l_{me}=l_{ID}=64,l_r=256,log$q$=34,N=1000,可得相关基于格的多接收方签密方案 1 消息-N 接收方和 N 消息-N 接收方的效率对比分布见表 6 和表 7.

Table 6 Efficiency comparison value of related lattice-based signcryption schemes (1 message-N receivers)

表 6 相关基于格的多接收方签密方案效率对比值(1 消息-N 接收方)

	LWJ13	ZXX18	方案 $M\Sigma$
公钥尺寸(bit)	2.7853×10^7	2.7853×10^7	2.7853×10^7
私钥尺寸(bit)	1.3926×10^7	1.3926×10^7	1.3926×10^7
密文量(bit)	2.1760×10^7	2.1888×10^7	6.5366×10^7

Table 7 Efficiency comparison value of related lattice-based signcryption schemes (N messages-N receivers)

表 7 相关基于格的多接收方签密方案效率对比值(N 消息-N 接收方)

	LWJ13	ZXX18	方案 $M\Sigma$
公钥尺寸(bit)	2.7853×10^7	2.7853×10^7	2.7853×10^7
私钥尺寸(bit)	1.3926×10^7	1.3926×10^7	1.3926×10^7
密文量(bit)	2.1760×10^7	2.1888×10^7	6.5366×10^7

从表 4 和表 6 可以看出:在发送 1 个消息到 N 个接收方的情况下,本文方案 $M\Sigma$与 LWJ13 和 ZXX18 相比,公私钥尺寸相当,密文量接近 3 倍(N 较大时,l_{me} 与 l_{ID} 远小于 $k\log q$).然而,由于陷门产生、原像抽样和带陷门的

求逆运算的复杂性远大于高斯采用和矩阵向量乘法运算(陷门生成、原像抽样和带陷门的求逆算法的复杂度是影响格密码实用性的重要原因),因此,方案 $M\Sigma$的计算效率较高.

从表 5 和表 7 可以看出:当发送 N 个消息到 N 个接收方的情况下,由于 LWJ13 和 ZXX18 的密文量和计算量呈 N 倍增加,而本文方案 $M\Sigma$密文量与计算量不变,因此,方案 $M\Sigma$的密文量只近似为 LWJ13 和 ZXX18 方案的 $3/N$,计算效率更胜于 LWJ13 和 ZXX18 方案.

5 结 论

随机数重用在构造多接收方密码方案时可以有效地节约系统开销,但容易导致方案的安全问题.研究如何进行安全的随机数重用,是一个非常有意义的研究课题.随机数全重用和随机数无重用可以看成是随机数部分重用的两种情况:当重用的随机数个数为 0 时,随机数重用退化成随机数无重用;当重用的随机数个数为方案中所有随机数时,随机数重用演化成随机数全重用.本文将随机数重用的概念丰富到另一种更常见的情况——随机数部分重用,研究了安全重用部分随机数的相关理论,将该理论应用到基于格的多接收方签密中,首次构造了一个基于格的可证明安全的 PRRU-MM-MR 签密方案.与直接构造方式相比,该方案的计算开销得到一定的节约,密文量节约了近 25%.本文的工作为构造多接收方签密方案提供了一种通用方法,即:先构造或选定一个可再生的标准签密方案;然后再借鉴定义 5 的方法,基于标准签密方案构造相应的部分随机数重用的多接收方签密方案.另外,本文的方法不仅限于签密,也可适用于签名或者加密的情况.

References:

[1] Hastad J. Solving simultaneous modular equations of low degree. SIAM Journal on Computing, 1988,17(2):336−341.

[2] Baudron O, Pointcheval D, Stern J. Extended notions of security for multicast public key cryptosystems. In: Proc. of the Int'l Colloquium on Automata, Languages, and Programming. Berlin, Heidelberg: Springer-Verlag, 2000. 499−511.

[3] Bellare M, Boldyreva A, Micali S. Public-key encryption in a multi-user setting: Security proofs and improvements. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2000. 259−274.

[4] Kurosawa K. Multi-recipient public-key encryption with shortened ciphertext. In: Proc. of the Int'l Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2002. 48−63.

[5] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985,31(4):469−472.

[6] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Proc. of the Annual Int'l Cryptology Conf. Berlin, Heidelberg: Springer-Verlag, 1998. 13−25.

[7] Bellare M, Boldyreva A, Staddon J. Randomness re-use in multi-recipient encryption schemeas. In: Proc. of the Int'l Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2003. 85−99.

[8] Bellare M, Boldyreva A, Kurosawa K, *et al*. Multirecipient encryption schemes: How to save on bandwidth and computation without sacrificing security. IEEE Trans. on Information Theory, 2007,53(11):3927−3943.

[9] Wei P, Zheng Y, Wang W. Multi-recipient encryption in heterogeneous setting. In: Proc. of the Int'l Conf. on Information Security Practice and Experience. Cham: Springer-Verlag, 2014. 462−480.

[10] Hajiabadi M, Kapron BM. Reproducible circularly secure bit encryption: Applications and realizations. Journal of Cryptology, 2017,30(4):1187−1237.

[11] Zhang J, Ou P. Privacy-preserving multi-receiver certificateless broadcast encryption scheme with de-duplication. Sensors, 2019, 19(15):3370.

[12] Cheng H, Li X, Qian H, *et al*. CCA secure multi-recipient KEM from LPN. In: Proc. of the Int'l Conf. on Information and Communications Security. Cham: Springer-Verlag, 2018. 513−529.

[13] Zheng Y. Digital signcryption or how to achieve cost (signature &encryption) ≪ cost (signature)+ cost (encryption). In: Proc. of the Annual Int'l Cryptology Conference. Berlin, Heidelberg: Springer-Verlag, 1997. 165−179.

[14] Han Y, Gui X. Adaptive secure multicast in wireless networks. Int'l Journal of Communication Systems, 2009,22(9):1213−1239.

[15] Ullah I, Ul Amin N, Zareei M, *et al*. A lightweight and provable secured certificateless signcryption approach for crowdsourced IIoT applications. Symmetry, 2019,11(11):1386.

[16] Pang L, Kou M, Wei M, *et al*. Efficient anonymous certificateless multi-receiver signcryption scheme without bilinear pairings. IEEE Access, 2018,6:78123−78135.

[17] Pang L, Wei M, Li H. Efficient and anonymous certificateless multi-message and multi-receiver signcryption scheme based on ECC. IEEE Access, 2019,7:24511−24526.

[18] Lu XH, Wen QY, Wang LC, *et al*. A lattice-based signcryption scheme without trapdoors. Journl of Electronic Information Technology, 2016,38:2287−2293 (in Chinese with English abstract).

[19] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM Journal on Computing, 2007, 37(1):267−302.

[20] Peikert C. A decade of lattice cryptography. Foundations and Trends® in Theoretical Computer Science, 2016,10(4):283−424.

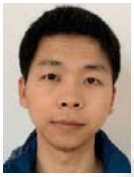
[21] Bai S, Galbraith SD. An improved compression technique for signatures based on learning with errors. In: Proc. of the Cryptographers' Track at the RSA Conf. Cham: Springer-Verlag, 2014. 28−47.

[22] Lu X, Wen Q, Jin Z, *et al*. A lattice-based multi-receiver signcryption scheme for point to multi-point communication. In: Proc. of the 2013 Int'l Conf. on Information and Network Security (ICINS 2013). IET, 2013. 1−7.

[23] Zhang X, Xu C, Xue J. Efficient multi-receiver identity-based signcryption from lattice assumption. Int'l Journal of Electronic Security and Digital Forensics, 2018,10(1):20−38.

附中文参考文献:

[18] 路秀华,温巧燕,王励成,等.无陷门格基签密方案.电子与信息学报,2016,38(9):2287−2293



刘镇(1985－),男,博士生,讲师,主要研究领域为公钥密码算法,可证明安全.

杨晓元(1959－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.

韩益亮(1977－),男,博士,教授,博士生导师,主要研究领域为密码学,隐私保护,社交网络分析.

柳曙光(1976－),男,副教授,主要研究领域为计算机应用,信息安全.