密钥隔离密码系统研究现状

秦志光[1)] 刘京京[2)] 赵 洋[1)] 吴松洋[3)] 熊 虎[1)] 聂旭云[1)] 朱国斌[1)]

[1)](电子科技大学信息与软件工程学院 成都 610054)

[2)](电子科技大学计算机科学与工程学院 成都 611731)

[3)](公安部第三研究所 上海 201204)

摘 要 当密码系统被部署到不安全环境或者遇到木马攻击时,密钥泄漏问题将不可避免.为减少密钥泄漏带来的损失,基于密钥进化思想的前向安全、密钥隔离以及入侵容忍等密码体制被陆续提出.其中,由 Dodis 于 2002 年提出的能够同时达到前向安全和后向安全的密钥隔离密码系统(Key-Insulated Cryptosystem)已成为信息安全界及密码学界的研究热点.鉴于该系统在抵御密钥泄漏中的重要性,文中对密钥隔离密码系统的研究进展进行了综述.不仅对密钥隔离系统的基本概念、形式化定义、安全模型以及安全要求进行了阐述,同时对密钥隔离方案的设计原理进行了深入分析.最后对目前已有的密钥隔离加密、签名以及密钥协商方案进行了分析,并对当前的方案从性能、安全模型及安全性等方面进行了比较.

关键词 密码系统;密钥泄漏;密钥隔离;加密;签名;密钥协商;密码学

中图法分类号 TP309 **DOI 号** 10.3724/SP.J.1016.2015.00759

A Survey of Key-Insulated Cryptography

QIN Zhi-Guang[1)] LIU Jing-Jing[2)] ZHAO Yang[1)] WU Song-Yang[3)]

XIONG Hu[1)] NIE Xu-Yun[1)] ZHU Guo-Bin[1)]

[1)](*School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu* 610054)

[2)](*School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu* 611731)

[3)](*The Third Research Institute of Ministry of Public Security, Shanghai* 201204)

Abstract When the cryptosystem is deployed into the hostile environment, the secret key leakage seems to be inevitable. In order to ease the destructive result incurred by key compromise, forward security, intrusion tolerance and key-insulated cryptosystem has been proposed based on the idea of key evolution respectively. The key-insulated cryptosystem, which was initially introduced in 2002 by Dodis, has attracted extensive concern from the information security and cryptology community since this mechanism can simultaneously achieve forward security and backward security. Due to the significance of key-insulated cryptosystem, this paper offers a solid survey of key-insulated cryptosystem. This paper not only describes the basic concepts, formal definition, security models and security requirements of key-insulated system, but also analyzes design philosophy. Finally, this paper reviews the existing key-insulated cryptosystems in view of the public-key certificate authentication approach, efficiency and formal security proof.

Keywords cryptosystem; key-insulated; key compromise; encryption; signature; key agreement; cryptography

---

收稿日期:2014-06-19;最终修改稿收到日期:2014-11-12.本课题得到国家自然科学基金(61003230, 61370026)、广东省产学研重点项目(2012B091000054)、四川省应用基础研究计划项目(2014JY0041)资助.**秦志光**,男,1956 年生,博士,教授,主要研究领域为计算机开放系统与网络安全性、信息系统安全.E-mail:qinzg@uestc.edu.cn.**刘京京**,男,1988 年生,硕士研究生,主要研究方向为信息安全、网络安全.**赵 洋**,男,1973 年生,博士,副教授,主要研究方向为信息安全.**吴松洋**(通信作者),男,1982 年生,博士,副研究员,主要研究方向为信息安全与云计算.E-mail:wusongyang@stars.org.cn.**熊 虎**,男,1982 年生,博士,副教授,主要研究方向为网络安全与密码学.**聂旭云**,男,1975 年生,博士,副教授,主要研究方向为信息安全、密码学.**朱国斌**,男,1981 年生,博士研究生,主要研究方向为信息安全、密码学.

1 引 言

当今计算机以及通讯设备在军事、金融以及日常生活等领域大量使用.在计算机以及通讯设备在通信中的重要信息一旦被人截获就会导致信息泄漏.为了应对信息泄漏,现代密码系统开始被广泛应用到计算机以及通信领域.不过现代密码系统提供的安全性依赖于用户的密钥,如果发生了密钥泄露,那么所有安全性就会被完全破坏.

关于解决密钥泄漏问题的研究有很多,一般是3种方式:

(1)基于在线PKG(私钥生成中心,Private Key Generator).用户需要定时与在线PKG通信以完成密钥更新,不过这样会给PKG带来很大的负荷,当负荷过大时PKG将面临瘫痪的风险,并且在用户与PKG通信时有昂贵的通信代价.

(2)分布式存储密钥.将密钥分为多个部分,每个部分存储在不同地方,当使用时再组合到一起.其中主要的方法有

①秘密共享(Secret Sharing)[1].将密钥分成很多片段,只有拥有足够多的片段,或者不同的部分的片段,或者所有的片段才能还原密钥.

②门限密码系统(Threshold Cryptosystem)[2].在一个(t,n)门限密码系统中,密钥被分为n个部分,当且仅当有超过t个部分存在时密钥才能被还原.

③前摄密码系统(Proactive Cryptosystem)[3].这种系统需要将密钥生命周期分为一个时间序列.前摄密码系统在每一个时间序列片段内都是一个独立的(t,n)门限密码系统即每个时间序列片段的门限表达式相互独立.当系统从一个时间序列片段转到另一个时间序列片段时,系统会利用前摄秘密共享方法变换门限密码系统秘密的表达式,并将上一个时间序列片段的表达式删除.

不过分布式存储密钥会导致较大的系统计算消耗并且有足够份额的密钥块发生了泄漏也会导致密钥泄漏.

(3)基于密钥进化的方案.这是当前主要用于解决密钥泄漏问题的方案,其基本思想:将系统时间分为N个不同的时间片.在保持公钥始终保持不变的情况下,不同的时间片的私钥不同.在密钥进化思想下主要有3种抵御密钥泄漏的方案:

①前向安全密码系统(Forward-Secure Cryptosystem)[4].该系统通过在用户密钥生成过程中引入二叉树(或者其他的数据结构)的概念,使得用户能够根据前一个时间片的密钥推导出与当前时间片对应的密钥,同时,该系统保证当前的密钥不能根据当前时间片的密钥推导得出该时段之前任意时间片对应的密钥即前向安全性(Forward-security).

②密钥隔离密码系统(Key-Insulated Cryptography)[5].密钥隔离密码系统方案是Dodis于2002年时提出的,其主要思想为:将密钥分成两个部分,一部分由用户自己控制,另一部分用一个物理安全的协助者保存.在需要使用密钥时将两部分的密钥进行"拼接"从而得到一个完整的密钥.系统中协助者的密钥在整个生命周期中不会改变,只有用户的临时私钥会随着时间进行更新.对于一个(t,N)密钥隔离方案来说,方案将系统的生命周期分为N个时间片,其中若只有少于t个时间片的密钥发生泄漏,那么泄漏只能威胁到丢失密钥时间片时的系统安全,对泄漏时间片之前或者之后的系统安全并无影响;只有当发生密钥泄漏的时间片超过t个时,系统其他$N-t$个时间片的安全性才会受到威胁.密钥隔离方案能够保证通过已经发生泄漏的密钥不能推导出该泄漏时段之前以及之后的密钥即保证前向安全性和后向安全性(Backward-security).

③入侵容忍密码系统(Intrusion-Resilience Cryptosystem)[6].入侵容忍方案与密钥隔离方案具有很多相似之处:将系统的生命周期分为N个时间片、需要协助者硬件、具有前向安全以及后向安全等.不过入侵容忍也有与密钥隔离不同的地方:入侵容忍方案中协助者密钥也要进行更新,并且方案只有在协助者以及用户的某个时间片的密钥同时丢失时对应时间片的系统才可能不安全.

前向安全、密钥隔离以及入侵容忍是最常用、最有效的应对密钥泄漏的方案,虽然这3种方案都使用了密钥进化思想、都将系统时间进行分片、对每个分片时间的私钥进行处理使得每个时间片中使用的密钥不一样、公钥在整个系统时间内保持不变、都具有前向安全性.不过它们也有不同点.这3种方案的属性比较如表1所示.

表1 基于密钥进化思想的密钥泄漏抵御方案比较

	协助者硬件	协助者密钥更新	后向安全性	随机密钥更新
前向安全	×	×	×	×
密钥隔离	√	×	√	√
入侵容忍	√	√	√	×

前向安全、入侵容忍以及密钥隔离这 3 种方案中，安全性最高的是入侵容忍，密钥隔离方案的安全性次于入侵容忍，因为前向安全方案只具有前向安全这个安全性质，所以前向安全的安全性次于密钥隔离. 但是在效率方面，由于入侵容忍不仅有用户加密密钥或者签名密钥更新阶段还有协助者密钥更新阶段，这使得入侵容忍方案的结构更加复杂，所以入侵容忍的效率比密钥隔离的效率低且构造难度要远远高于构造密钥隔离方案. 再而密钥隔离方案是入侵容忍方案的构造原型或者构造因子之一，对密钥隔离方案的研究对未来入侵容忍方案研究有积极影响，所以综合效率，构造难度以及安全性等情况，密钥隔离方案成为了信息安全及密码学界的研究热点.

对于一个密钥隔离系统而言，其使用的加密密钥或者签名密码是随时间进行更新的，而这个密钥是通过用户和系统交互获得的. 如用户初次使用密钥隔离系统时需要提供一个密钥，系统根据用户密钥生成一个对应的加密密钥或者签名密钥以及一个协助者密钥. 当用户需要进行加密或者签名时，用户直接使用这个密钥进行相应的操作. 当用户发现其加密密钥或者签名密钥发生了泄露或者需要进行密钥更新时，用户直接跟协助者进行交互以获得新的加密密钥或者签名密钥. 由于密钥隔离系统具有前向安全性以及后向安全性，获得了前一个时段的用户加密密钥或者签名密钥的攻击者在新的时段内就不能使用旧加密密钥或者旧签名密钥了，且这个泄露的加密密钥或者签名密钥也不能为攻击者提供新加密密钥或者新签名密钥的任何信息即无法通过旧加密密钥或者旧签名密钥推测出新加密密钥或者新签名密钥. 例如用户在时间段 i 中使用的密钥为 SK_i，如果攻击者获得了这个密钥，其能够在时间段 i 中使用这个密钥进行伪造攻击等，但是用户进行了密钥更新，新的密钥为 SK_j，此时 SK_i 将无法在新的时间段使用且不能由 SK_i 推断出 SK_j.

鉴于密钥隔离系统在抵御密钥泄漏中的重要性，本文对密钥隔离密码系统的研究进展进行了综述. 本文不仅对密钥隔离系统的基本概念、形式化定义、安全模型以及安全要求进行了阐述，同时对密钥隔离方案的设计原理进行了深入分析. 最后对目前已有的密钥隔离加密、签名以及密钥协商方案进行了分析，并对当前的方案从性能、安全模型及安全性等方面进行了比较. 本文既能让初步研究密钥隔离的研究者了解密钥隔离的方法以及过程，也能让其他的研究者找到可能的兴趣点从而继续研究. 本文对密钥隔离密码系统进行的综述也能为无论是学术界还是工业界的密钥隔离研究提供参考.

2　形式化定义与安全模型

作为密码系统的 3 个原型的加密、签名以及密钥协商为通信等服务提供了隐秘性、完整性等，其中加密提供了隐秘性，签名提供了完整性验证以及身份认证，密钥协商提供了在不可信的信道上进行保密通信的可能. 不过在面对密钥泄漏时这 3 个原型也会失去原有的作用. 随着对密钥隔离方案的研究，当前衍生出多种不同形式的密钥隔离加密、签名以及密钥协商方案以解决密钥泄漏. 为了更好地说明密钥隔离，以下将说明密钥隔离方案中最原始的加密、签名和密钥协商的形式以及相关的安全定义和模型.

2.1　密钥隔离加密

2.1.1　形式化定义

一个具有密钥隔离功能的公钥加密算法一般由 5 个多项式时间算法组成：

(1) 密钥生成算法 $KeyGen$，主要由秘密参数 1^k 以及这个方案的周期总数 N 生成公钥 PK、主密钥 SK^* 以及初始化密钥 SK_0.

(2) 协助者密钥更新算法 $Update^*$，主要是由协助者通过当前时间片 $i\in[1,N]$ 以及主密 SK^* 生成与时间等参数相关的部分密钥 SK_i'.

(3) 用户密钥更新算法 $Update$，主要是由前一个时间片的密钥 SK_{i-1}、协助者产生的部分密钥 SK_i' 以及当前时间片 i 生成时间片 i 的用户临时密钥 SK_i.

(4) 加密算法 E，由公钥 PK、时间片 i 以及待加密信息 M 生成密文 (i,c).

(5) 解密算法 D，由时间片 i 的密钥 SK_i 以及密文 (i,c) 得到信息 M 或者特殊符号 $\perp$.

2.1.2　密钥隔离加密中的安全模型

(1) 密钥隔离安全(选择密文攻击安全)的模型：

$KeyGen$：挑战者 $\mathcal{C}$ 将方案的周期总数 N 等公共参数发给攻击者 $\mathcal{A}$.

第 1 阶段. $\mathcal{A}$ 向 $\mathcal{C}$ 发出请求，$\mathcal{C}$ 对请求进行回答.

① 私钥请求阶段. $\mathcal{A}$ 向 $\mathcal{C}$ 请求私钥 SK_0；

② 临时私钥请求阶段. $\mathcal{C}$ 运用 $Update$ 算法通过

SK'_i产生时间片 i 的密钥 SK_i，并将其发送给$\mathcal{A}$；

③解密请求阶段. $\mathcal{C}$运行算法 D 对密文(i,c)进行解密并将结果发给$\mathcal{A}$.

挑战阶段. 当$\mathcal{A}$认为第 1 阶段可以结束了，则$\mathcal{A}$向$\mathcal{C}$发送时间片 x 以及两个等长的信息 m_0,m_1. $\mathcal{C}$接收信息并对其中之一进行加密产生密文 $c'=E(m_y)$，$y\in\{0,1\}$并发送给$\mathcal{A}$.

第 2 阶段. $\mathcal{A}$进行类似第 1 阶段的询问，$\mathcal{C}$进行类似的回答. 不过$\mathcal{A}$不能产生有关时间片 x 的询问如时间片 x 时的部分密钥 SK'_x、时间片 x 时的密钥 SK_x以及对于密文(x,c')的解密.

猜测阶段. $\mathcal{A}$猜测 $y=y'$，如果 $y=y'$确实成立，则$\mathcal{A}$赢得游戏.

(2)强密钥隔离安全模型. 在这种模式下，攻击者$\mathcal{A}$能获得协助者密钥或者主密钥 SK^*，但是不能对临时密钥进行询问.

KeyGen. 挑战者$\mathcal{C}$将方案的周期总数 N 等公共参数发给攻击者$\mathcal{A}$.

第 1 阶段. $\mathcal{A}$向$\mathcal{C}$发出请求，$\mathcal{C}$对请求进行回答.

①私钥查询阶段. $\mathcal{A}$向$\mathcal{C}$请求私钥 SK_0；

②协助者密钥查询阶段. $\mathcal{A}$向$\mathcal{C}$询问协助者密钥 SK^*；

③解密查询阶段. $\mathcal{C}$运行算法 D 对密文(i,c)进行解密并将结果发给$\mathcal{A}$.

挑战阶段. 当$\mathcal{A}$认为第 1 阶段可以结束了，则$\mathcal{A}$向$\mathcal{C}$发送时间片 x 以及两个等长的信息 m_0,m_1. $\mathcal{C}$接收信息并对其中之一进行加密产生密文 $c'=E(m_y)$，$y\in\{0,1\}$并发送给$\mathcal{A}$.

第 2 阶段. $\mathcal{A}$进行类似第 1 阶段的询问，$\mathcal{C}$进行类似的回答. 不过$\mathcal{A}$不能产生有关时间片 x 的询问如时间片 x 时的部分密钥 SK'_x，时间片 x 时的密钥 SK_x以及对于密文(x,c')的解密.

猜测阶段. $\mathcal{A}$猜测 $y=y'$，如果 $y=y'$确实成立，则$\mathcal{A}$赢得游戏.

2.2 密钥隔离签名

2.2.1 形式化定义

一般来说一个具有密钥隔离的公钥签名算法由 5 个多项式时间算法组成：

(1)密钥生成算法 *KeyGen*，主要由秘密参数 1^k 以及这个方案的周期总数 N 生成公钥 PK、主密钥 SK^* 以及初始化密钥 SK_0.

(2)协助者密钥更新算法 Upd^*，主要是由协助者通过当前时间片 $i,j(1\leq i,j\leq N)$ 以及主密钥 SK^* 生成与时间片 i,j 等参数相关的部分密钥$SK'_{i,j}$.

(3)用户密钥更新算法 *Upd*，主要是由前一个时间片的密钥 SK_i、协助者产生的部分密钥 $SK'_{i,j}$以及时间片生成当前时间片 j 的密钥 SK_j.

(4)签名算法 *Sign*，由密钥 SK_i、时间片 i 以及待签名信息 M 生成签名信息(i,s).

(5)解密算法 *Vrfy*，由公钥 PK 以及签名信息(i,s)得到一个信息 b，如果 $b=1$，则接受签名.

2.2.2 密钥隔离签名中的安全模型

(1)密钥隔离安全在选择密文攻击下不可伪造的模型：

KeyGen. 挑战者$\mathcal{C}$将方案的周期总数 N 等公共参数发给攻击者$\mathcal{A}$.

第 1 阶段. $\mathcal{A}$向$\mathcal{C}$发出请求，$\mathcal{C}$对请求进行回答.

①私钥请求阶段. $\mathcal{A}$向$\mathcal{C}$请求私钥 SK_0；

②临时私钥请求阶段. $\mathcal{C}$运用 *Upd* 算法通过 $SK'_{j,i}$产生时间片 i 的密钥 SK_i，并将其发送给$\mathcal{A}$；

③验证请求阶段. $\mathcal{C}$运行算法 *Sign* 由时间片 i，待签名信息 m 以及私钥 SK_i产生签名信息(i,s)发给$\mathcal{A}$.

挑战阶段. 当$\mathcal{A}$认为第 1 阶段可以结束了，则$\mathcal{A}$向$\mathcal{C}$发送在第 1 阶段没有询问过的时间片 x 和信息 m'以及对应的签名(x,s'). $\mathcal{C}$对签名进行验证并发送结果给$\mathcal{A}$. 若通过验证即 $Vrfy(x,s',m')=1$，则$\mathcal{A}$赢得游戏；否则$\mathcal{A}$的伪造失败.

(2)强密钥隔离安全在选择密文攻击下不可伪造的模型：在这种模式下，攻击者$\mathcal{A}$能获得协助者密钥或者主密钥 SK^*.

KeyGen. 挑战者$\mathcal{C}$将方案的周期总数 N 等公共参数发给攻击者$\mathcal{A}$.

第 1 阶段. $\mathcal{A}$向$\mathcal{C}$发出请求，$\mathcal{C}$对请求进行回答.

①私钥请求阶段. $\mathcal{A}$向$\mathcal{C}$请求私钥 SK_0；

②协助者密钥查询阶段. $\mathcal{A}$向$\mathcal{C}$询问协助者密钥 SK^*；

③验证请求阶段. $\mathcal{C}$运行算法 *Sign* 由时间片 i，待签名信息 m 以及私钥 SK_i产生签名信息(i,s)发给$\mathcal{A}$.

挑战阶段. 当$\mathcal{A}$认为第 1 阶段可以结束了，则$\mathcal{A}$向$\mathcal{C}$发送在第 1 阶段没有询问过的时间片 x 和信息 m'以及对应的签名(x,s'). $\mathcal{C}$对签名进行验证并发送结果给$\mathcal{A}$. 若通过验证即 $Vrfy(x,s',m')=1$，则$\mathcal{A}$赢得游戏；否则$\mathcal{A}$的伪造失败.

2.3　密钥隔离密钥协商

一个密钥隔离的密钥协商主要由 4 个多项式算法组成：

(1) 密钥生成算法 $KeyGen$，主要由秘密参数 1^k 以及这个方案的周期总数 N 生成主密钥 SK^* 以及初始化密钥 SK_0.

(2) 协助者密钥更新算法 Upd^*，主要是由协助者通过当前时间片 $i(1\leq i\leq N)$ 以及主密钥 SK^* 生成与时间片 i 等参数相关的密钥更新种子 SK'_i.

(3) 用户密钥更新算法 Upd，主要是由前一个时间片的密钥 SK_i、协助者产生的部分密钥 $SK'_{i,j}$ 以及时间片 i,j 生成当前时间片 j 的密钥 SK_j.

(4) 密钥协商 $KeyDer$，用户 a,b 之间要进行密钥协商，则用户 a 进行 $CK_{(a,b)(i)}=SK_{a(i)}\times U_b$，其中 $CK_{(a,b)(i)}$ 为用户 a,b 之间的协商后的会话密钥，$SK_{a(i)}$ 为用户 a 在时间片 i 时的密钥，U_b 为用户 b 的信息. 同样用户 b 运行 $CK_{(a,b)(i)}=SK_{b(i)}\times U_a$.

2.4　安全要求

(k,N) 密钥隔离. 在一个将生命周期分为 N 份的密钥隔离方案中，若只有 k 个时间片的密钥发生泄漏，发生泄漏的这 k 个时间片不会影响到其他 $N-k$ 时间片的系统安全.

完美密钥隔离. 是 (k,N) 密钥隔离方案中，当 $k=N-1$ 的情况即当有 $N-1$ 个时间片的密钥发生了泄漏，未泄漏的时间片的密钥系统仍然能保证安全.

安全密钥更新. 即使密钥更新时协助者产生的部分密钥和用户临时密钥同时发生了泄漏，也不会影响到其他时间片的系统安全.

无限制时间片数目. 与一般的密钥隔离方案不同，系统将不会在初始化时期定好时间片数目，具有无限多个时间片.

随机密钥更新. 一般来说密钥更新的时间片是顺序的，不过如果具有随机密钥更新则密钥能从任意时间片更新到其他任意时间片.

2.5　经典方案与设计原理

2.5.1　经典密钥隔离方案

第 1 个密钥隔离加密方案以及第 1 个密钥隔离签名方案分别由 Dodis 于 2002 年、2003 年提出. 虽然当前很多密钥隔离方案无论是在效率还是安全性上都超过这两个原始方案. 不过这两个方案第 1 次具体的提出了在加密以及签名方案中如何使用密钥隔离思想，为后续的密钥隔离加密以及签名提供了思路.

(1) Dodis 密钥隔离加密方案[5]

Dodis 密钥隔离加密方案由 5 个多项式时间算法组成：密钥生成算法、协助者密钥更新算法、用户临时密钥更新算法、加密算法以及解密算法.

假设 p,q 都为素数，并且 $|q|=k$，$p=2q+1$. $\mathcal{G}$ 是 $\mathbb{Z}_p^*$ 的一个子群，随机选取 $g,h\in\mathcal{G}$.

① 密钥生成算法

算法输入一个安全参数 1^k.

随机选择 $x_0^*,y_0^*,\cdots,x_t^*,y_t^*\leftarrow\mathbb{Z}_q$.

计算：$z_0^*=g^{x_0^*}h^{y_0^*},\cdots,z_t^*=g^{x_t^*}h^{y_t^*}$；

公钥 $PK=(g,h,z_0^*,\cdots,z_t^*)$.

系统密钥 $SK^*=(x_1^*,y_1^*,\cdots,x_t^*,y_t^*)$，这个方案中系统密钥就是协助者密钥.

用户初始临时密钥 $SK_0=(x_0^*,y_0^*)$.

算法输出公钥 PK，系统密钥 SK^*，用户初始临时密钥 SK_0.

② 协助者密钥更新算法

算法输入时间片 i 以及系统密钥 $SK^*=(x_1^*,y_1^*,\cdots,x_t^*,y_t^*)$.

计算：$x'_i=\sum_{j=1}^{t}x_j^*(i^j-(i-1)^j)$，

$$y'_i=\sum_{j=1}^{t}y_j^*(i^j-(i-1)^j).$$

算法输出部分密钥 $SK'_i=(x'_i,y'_i)$.

③ 用户临时密钥更新算法

算法输入时间片 i、用户当前临时密钥 $SK_{i-1}=(x_{i-1},y_{i-1})$ 以及部分密钥 $SK'_i=(x'_i,y'_i)$.

计算：$x_i=x_{i-1}+x'_i$，

$y_i=y_{i-1}+y'_i$.

如

$SK_1=(x_1,y_1)$，

$x_1=x_0^*+\sum_{j=1}^{t}x_j^*$，

$y_1=y_0^*+\sum_{j=1}^{t}y_j^*$，

$SK_2=(x_2,y_2)$，

$x_2=x_1^*+\sum_{j=1}^{t}x_j^*(2^j-1)=x_0^*+\sum_{j=1}^{t}x_j^*2^j$，

$y_2=y_1^*+\sum_{j=1}^{t}y_j^*(2^j-1)=y_0^*+\sum_{j=1}^{t}y_j^*2^j$，

$SK_t=(x_t,y_t)$，

$x_t=x_0^*+\sum_{j=1}^{t}x_j^*t^j$，

$y_t=y_0^*+\sum_{j=1}^{t}y_j^*t^j$.

每次更新的部分实际上都是表达式后半部分即 $\sum_{j=1}^{t} y_j^* i^j$，其中 i 就是时间标签. 这个表达式就是带时间的表达式，每次进行密钥更新主要是对这个部分进行更新以达到密钥与时间片相关.

算法输出时间片 i 时的用户临时密钥 $SK_i=(x_i,y_i)$.

④加密算法

输入公钥 PK、时间片 i 以及待加密信息 M.

计算：

$$z_i:=\prod_{j=0}^{t}(z_j^*)^{i^j}$$

$$=\prod_{j=0}^{t}(g^{x_j^*}h^{y_t^*})^{i^j}=g^{x_0^*+\sum_{j=1}^{t}x_j^* i^j}h^{y_0^*+\sum_{j=1}^{t}y_j^* i^j}.$$

这个表达式可看出密钥与这个加密种子的关系. 这个 z_i 可以直接通过公钥计算，且可以通过密钥更新后的用户密钥进行计算.

选择随机数 $r\leftarrow\mathbb{Z}_q$.

密文 $C=(g^r,h^r,z_i^r M)$，

$$C=(g^r,h^r,(g^{x_0^*+\sum_{j=1}^{t}x_j^* i^j}h^{y_0^*+\sum_{j=1}^{t}y_j^* i^j})^r M).$$

算法输出加密信息$\langle i,C\rangle$.

⑤解密算法

输入用户临时密钥 $SK_i=(x_i,y_i)$ 以及加密信息$\langle i,C=(u,v,w)\rangle$.

计算并得到明文信息

$$M=w/u^{x_i}v^{y_i}$$

$$=(g^{x_0^*+\sum_{j=1}^{t}x_j^* i^j}h^{y_0^*+\sum_{j=1}^{t}y_j^* i^j})^r M/g^{rx_i}h^{ry_i}=M.$$

算法输出明文 M.

在只是考虑密钥隔离的情况下可知由于每次解密的密钥跟时间相关且如果不知道密钥更新种子时，无法从某个时刻 i 得到下一个时刻的密钥，由此无法对下一个时刻的密文进行解密.

(2) Dodis 密钥隔离签名方案[7]

Dodis 密钥隔离签名方案由 5 个多项式时间算法组成：密钥生成算法、协助者密钥更新算法、用户临时密钥更新算法、签名算法以及验证算法.

假设 p,q 都为素数，并且 $p=2q+1$. $\mathcal{G}$ 是 $\mathbb{Z}_p^*$ 的一个子群，随机选取 $g,h\in\mathcal{G}$.

①密钥生成算法

输入一个安全参数 1^k 以及周期数 N.

随机抽取：$x_0^*,y_0^*,\cdots,x_t^*,y_t^*\leftarrow\mathbb{Z}_q$.

计算：$v_i^*=g^{x_i^*}h^{y_i^*}$，$i\in[0,t]$.

公钥 $PK=(g,h,v_0^*,\cdots,v_t^*)$.

系统密钥 $SK^*=(x_1^*,y_1^*,\cdots,x_t^*,y_t^*)$，这个方案中系统密钥就是协助者密钥.

用户初始临时密钥 $SK_0=(x_0^*,y_0^*)$.

算法输出公钥 PK，系统密钥 SK^* 以及用户初始临时密钥 SK_0.

②协助者密钥更新算法

算法输入时间片 i,j 以及系统密钥 $SK^*=(x_1^*,y_1^*,\cdots,x_t^*,y_t^*)$.

计算：$x'_{i,j}=\sum_{k=1}^{t}x_k^*(j^k-i^k)$，

$$y'_{i,j}=\sum_{k=1}^{t}y_k^*(j^k-i^k).$$

算法输出部分密钥 $SK'_{i,j}=(x'_{i,j},y'_{i,j})$.

③用户临时密钥更新算法

算法输入时间片 i,j、用户当前临时密钥 $SK_i=(x_i,y_i)$ 以及部分密钥 $SK'_{i,j}=(x'_{i,j},y'_{i,j})$.

计算：$x_j=x_i+x'_{i,j}$，

$$y_j=y_i+y'_{i,j}.$$

算法输出时间片 i 时的用户临时密钥 $SK_j=(x_j,y_j)$.

④签名算法

算法输入时间片 i 时的用户临时密钥 $SK_i=(x_i,y_i)$、时间片 i 以及待签名信息 M.

选择随机数 $r_1,r_2\leftarrow\mathbb{Z}_q$.

计算：$w=g^{r_1}h^{r_2}$，

$$\tau=H(i,M,w),$$

$$a=r_1-\tau x_i,$$

$$b=r_2-\tau y_i.$$

算法返回签名信息$\langle i,(w,a,b)\rangle$.

⑤验证算法

算法输入公钥 PK、信息 M 以及签名信息$\langle i,(w,a,b)\rangle$.

计算：$v_i=\prod_{k=0}^{t}(v_i^*)^{i^k}$，

$$\tau=H(i,M,w).$$

算法输出：如果等式 $w=g^a h^b v_i^\tau$ 成立，则输出 1；如果等式不成立，则输出 0.

这个方案与第 1 个加密方案使用的密钥隔离方式相似，大体上也是因为签名密钥中具有当前时间片的信息，而这个信息更新时需要协助者发出的密钥更新种子，如果不知道密钥更新种子就无法由前一个时间片的密钥更新到下一个时间片的密钥.

2.5.2　设计原理

对于密钥隔离方案来说最重要的部分就是密钥更新的方式.密钥更新方式控制了方案中临时密钥的结构即控制了时间片嵌入到用户临时密钥的方式,而时间片嵌入临时密钥就是密钥进化在密钥隔离中的核心体现.无论是具有密钥隔离性质的加密、签名还是密钥协商,在实现密钥隔离时,各个方案在密钥更新的方式上都有所不同.本文根据算法的复杂性将密钥更新方式大体分为替代、群操作法以及组合法.

假设时间片为 i,ID 为用户的身份标识,H 为 Hash 函数,F_{key} 为以 key 为密钥的伪随机函数,主密钥 SK^*,用户私钥为 usk,协助者密钥为 hsk,$sk_i=SK^*\times H(i)$ 为用户临时私钥的组成部分之一,私钥协助者生成的部分密钥 $SK'_{i,j}$,用户在时间片 i 时的临时密钥 SK_i,用户在时间片 j 时的密钥 SK_j.

(1)替代方式.在这种情况下,用户的临时密钥是由用户私钥与时间片的组成部分直接连接得到的,并没有运用其他计算.所以密钥更新方式为:将私钥里的部分数据与协助者发出的部分密钥进行替换.如图 1 所示.而具体的例子如下:

用户的临时密钥为 $SK_i=(usk,sk_i)$.

协助者发送的部分密钥:

$$SK'_{i,j}=sk_j=hsk\times H(j).$$

用户在时间片 j 时的临时密钥为

$$SK_j=(usk,sk_j).$$

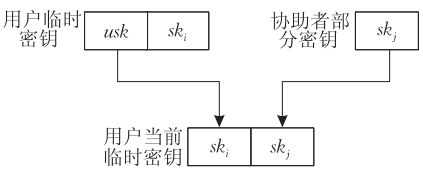

图 1　密钥更新-替换

(2)群操作.群操作是使用了群论的一些方法,通过群计算进行密钥更新,如使用群加减法进行密钥更新.在这种情况下,用户的临时密钥是由用户私钥与时间片的组成部分进行群加法得到.所以密钥更新方式是用上一个时间片的密钥加上协助者发出的部分密钥得到当前时间片的用户临时密钥.如图 2 所示.而具体例子如下:

用户临时密钥为

$$SK_i=SK^*\times H(ID)+hsk\times H(ID,i).$$

协助者发出的部分密钥为

$$SK'_{i,j}=hsk\times[H(ID,i)-H(ID,j)].$$

用户在时间片 j 时的临时密钥为

$$SK_j=SK_i+SK'_{i,j}.$$

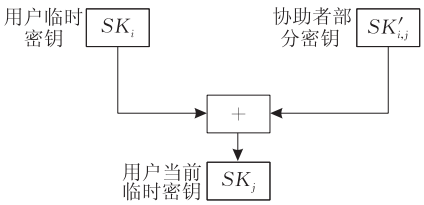

图 2　密钥更新-群操作

(3)基于基本方法组合的方式:为了提高安全性,有时会将方式(1)和(2)两种方式进行结合达到更高的安全性,例如将替代与群操作法结合并加入由随机数产生的临时生成密钥的密钥.例如:其中 $r\in Z$ 为一个随机数.

用户临时密钥为

$$SK_i=(usk\times H(ID)^r\times H(ID,i)^{F_{hsk}(i\|ID)},g^{F_{hsk}(i\|ID)},g^r).$$

为方便将此密钥表示为 (sk'_i,sk''_i,s'''_k).

协助者发出的部分密钥为

$$SK'_{i,j}=(H(ID,j)^{F_{hsk}(j\|ID)}/H(ID,i)^{F_{hsk}(i\|ID)},g^{F_{hsk}(j\|ID)}).$$

将此部分密钥表示为 (skh'_j,skh''_j).

用户在时间片 j 时的临时密钥为

$$SK_j=(sk'_i\times skh'_j,skh''_j,sk''').$$

3　研究现状

2002 年 Dodis 提出了密钥隔离思想以及第 1 个密钥隔离加密算法,因为其较高的安全性以及效率,密钥隔离开始受到广泛关注.从 2002 年开始直至现在已有大量关于密钥隔离方案的研究.研究不但包含了普通的加密以及签名,还包含了对密钥隔离方案的改进、特殊应用的改进以及针对原密钥隔离方案的扩展方案如平行密钥隔离方案、基于身份的密钥隔离方案等等.

3.1　密钥隔离加密方案

2002 年,Bellare 等人[8]在 Boneh-Franklin 的基于身份加密模型下,使用 Dodis 的密钥隔离模型构造了一种简单、现实并且可扩展的模型——SKIE-OT(Strongly Key-Insulated Encryption with Optimal Threshold),这种模型能够进行随机密钥更新并且满足强密钥隔离.同年,Hanaoka 等人[9]构造了一种无条件安全的密钥隔离加密方案 DMKIE(Dynamic and Mutual Key Insulated Encryption),并证明了 DMKIS 可以由 KPS(Key Predistribution Schemes)

或 BES(Broadcast Encryption Schemes)构造,不过方案有内存大小的限制,其对密文、用户密钥、主密钥、协助者密钥以及发送者密钥所需内存的大小具有一定要求.

2004 年,文献[10]证明了时间缓冲的加密算法可以类似于具有最优门限的密钥隔离算法.在介绍了时间缓冲加密算法的概念后给出了一种满足强密钥隔离的认证加密算法方案.

2006 年,Cheon 等人[11]沿着文献[10]继续研究,证明了一定存在一种具有最优门限以及随机密钥更新的密钥隔离加密方案与一种选择密文安全的时间缓冲公钥加密方案相似,并构造了一种可证明安全的具有时间缓冲的认证公钥加密方案.

2008 年,Li 等人将密钥隔离思想应用到了基于身份的模糊加密(Fuzzy Identity-Based Encryption,FIBE)中提出了基于身份的模糊密钥隔离加密系统(FIBKIE)①,从而解决了在 FIBE 中的密钥泄漏问题.方案能够进行安全密钥更新、支持随机密钥更新并满足完美密钥隔离.并且方案是基于 DBDH 问题的,所以方案具有可证明安全性.

2009 年,文献[12]将密钥隔离思想应用到无线传感器网络中,提出了基于密钥预分配的密钥隔离加密方案.方案中每个节点都有一个与自身 ID 相关的私钥,不过所有节点共有一个公钥.这个方案不但具有语义安全还具有$(N-1,N)$密钥隔离的性质.并且经证明此方案中增加的存储以及通信增加的消耗在可接受范围内.

3.2 密钥隔离签名方案

2003 年,Dodis 等人[7]证明了任意已存在的标准签名方案都能构造完美密钥隔离签名方案并证明了在离散对数假设下(t,n)密钥隔离方案具有可证明安全性.然后利用 Okamoto-Schnorr 的签名方案构造了一种完美密钥隔离方案并利用陷门签名构造了一种具有强密钥隔离以及完美密钥隔离的签名方案,方案中验证了:即使敌手获得了不安全设备(保存密钥)以及某个时期的密钥也不能伪造其他任意时期的签名;即使敌手获得了物理安全的设备(保存主密钥的设备)也不能伪造任意时刻的签名.由于构造方案时使用了随机预言模型,所以整个方案的效率比在标准模型下更快.同年,文献[13]提出了一种满足强密钥隔离的签名方案 KUS-SKI(Key Updating Signature with Strong Key Insulation),方案能够进行随机密钥更新并且满足完美密钥隔离,文中还提出了一种不保证其他时刻安全的入侵容忍签名方案 KUS-IR,其能够进行随机密钥更新并满足完美密钥隔离.

2004 年,文献[14]中利用密钥隔离思想设计了一套签名方案 D-OCSP,这个方案主要用于在线证书检索.方案中使用了 Micali 的撤销系统,使用户验证应答者私钥正确性的效率比 CRL 更高.同年,González-Deleito 等人[15]设计了一种同时满足强密钥隔离以及完美密钥隔离的签名方案.方案中密钥长度固定并且具有独立的隔离周期,而且方案能够在某个给定时间段内所有密钥都发生泄漏的情况下保持前向安全.由于 González-Deleito 等人设计的方案参考了 Guillou-Quisquater[16]的文献中的签名方案,所以效率比 Dodis 提出的密钥隔离签名方案高.

2007 年,文献[17]中将密钥隔离运用到群签名中,减少了密钥泄漏给群签名带来的损失.文中提出的基于随机预言模型的密钥隔离群签名方案能够进行安全密钥更新,并且还满足匿名性、可溯性、不可伪造性以及强密钥隔离性.方案还支持选择性撤销即只有撤销某些被暴露时期用户的签名密钥.整个方案使用了基于碰撞容忍的 ACJT 模型,而对方案的安全性分析利用了 BSZ 模型,并由于整个方案建立于强 RSA 问题,所以方案可证明安全.而且方案的签名以及公钥的长度都与时间片以及撤销成员的数量独立,由此整个方案的安全性更高.文献[18]就文献[17]的研究提出了另一种方案,与文献[17]的方案不同处为:新方案加入了 VLR(Verifier-Local Revocation)以及反向不可连接的特性,安全性有所加强.

2008 年,文献[19]中提出了一种前向安全的环签名和一种门限密钥隔离的环签名,在这两种方案中每个用户都有一个协助者硬件并都使用了(t,n)门限思想:即使有 t 个用户的密钥被攻陷也不会影响到方案的安全性,两种方案都是无条件完全匿名的并且在随机预言模型下都是可证明安全的,其中密钥隔离环签名能满足强密钥隔离.文献[20]中 Lee 等人说明了密钥隔离方案并不能对密钥泄露进行完全保护,并说明在电子商务等情况下密钥的一次泄露也会导致非常大的损失,从而提出了一种保护方案.方案使用了基于 NOVOMODO 和计数器

① Li Jin, Kim Kwangjo. Fuzzy identity-based key-insulated cryptosystem. http://caislab.kaist.ac.kr/publication/paper_files/2008/JWIS08_JinLi.pdf

的一次 Hash，所以即使发生了一次密钥泄漏，泄漏也能够被发现，由此密钥泄漏会被及时发现使得方案得到完全保护. 文献[21]中提出了一种基于 Abe-Okamoto 签名模型的强密钥隔离签名方案，这种签名方案的效率比此篇文章之前的强密钥隔离签名方案效率更高，其中方案的签名密钥长度只有以前方案的长度的 2/5，并且方案能够满足一个服务端对多个用户模型的现实应用. 文中还证明了方案满足完美密钥隔离，并且由于方案的安全性建立于离散对数，所以在随机预言模型下可证明安全.

2009 年，Bellare 等人[22]指出由于密钥隔离方案需要通过用户与协助者硬件之间的通信来进行密钥更新，所以密钥隔离系统需要一个安全信道. 由此 Bellare 等人给出了相应的模型讨论在秘密信道以及公共信道上密钥隔离的问题，并说明了在秘密信道上密钥隔离在主动攻击以及被动攻击下是不会被攻破的，不过必须确信信道是安全的，而在公共信道上密钥隔离在主动攻击下是脆弱的，但是在被动攻击下安全性可以得到保证. 由此提示密钥隔离以及入侵弹回的研究者选择信道的重要性.

2010 年，Kang 等人[23]指出文献[21]中的签名方案存在的缺陷：(1) 由于原方案中的验证算法计算太复杂，所以是不可实行的；(2) 协助者必须参与每一次密钥更新因此方案效率不高；(3) 不具备随机密钥更新的能力. 根据这些缺陷，Kang 等人对文献[21]中的方案进行了相应的改进：增加了随机密钥更新的能力，改进方案中每过一定时间才进行密钥更新. 使得方案变得更加安全、高效. 文章最后指出由于改进方案使用了 Go Ohtake 的模型，所以改进方案可证明安全. 同年，文献[24]根据计算安全的密钥隔离签名方案以及信息理论安全的多接收者认证提出了具有信息理论安全的多接收者密钥隔离认证方案. 文中给出了两种构造方案的方法：直接构造以及一般构造. 并且文中说明了直接构造是最优的并证明了在他们的安全定义下，方案是可证明安全的.

2012 年，文献[25]在随机预言模型下设计了一种基于证书的密钥隔离签名(CBKIS)方案. 方案满足强密钥隔离以及随机密钥更新等安全属性. 文章最后证明，由于方案的安全性建立于 CDH 问题，所以在面对选择明文攻击时，签名也是不可伪造的，是可证明安全的.

2013 年，Lin 等人[26]在随机预言模型下提出了一种新的基于身份的密钥隔离多重签名方案. 为了使得方案高效，其使用了 Wu 等人[27]方案中的密钥更新过程. 这个方案还保证了无限时间片以及随机密钥更新. Lin 等人最后还证明了在这个方案能够抵抗自适应选择密文攻击. Wan 等人[28]基于 Waters 的基于身份的加密方案以及 Weng 等人的基于身份的 PKIS 方案构造了标准模型下的第 1 种平行密钥隔离签名方案.

2014 年，Chen 等人[29]基于 CDH 问题设计了一种新的基于属性的密钥隔离签名方案，同时文中介绍了两种构造这个方案的方法. Li 等人[30]在随机预言模型下构造了一种基于证书的密钥隔离签名方案，在文中 Lin 等人给出了形式化定义以及安全模型并证明了方案的安全性.

3.3　密钥隔离密钥协商方案

2011 年，文献[31]中提出了具有信息理论安全的密钥隔离密钥协商方案(KI-KA)，解决了在密钥协商时密钥泄漏导致的问题，文中不但给出了模型定义还给出了具体构造并证明了方案是可证明安全的也证明了方案是最优的. 文章最后还给出了一些具体应用.

4　扩展方案

4.1　分层密钥隔离(Hierarchical Key-Insulated Scheme)

2004 年，由于不同用户群会有一些与其他用户群不同的信任的 CA，如果需要验证的用户群之间信任不同的 CA，这就会带来跨域的问题. Le 等人[32]说明了如果使用分层的 CA 结构，那么由于多个 CA 能够缩短验证路径并能减少 CA 私钥泄漏带来的危害，不过每个 CA 的密钥隔离仍然是弱点，所以结合分层结构、多个 CA 以及密钥隔离思想设计出分层密钥隔离签名方案. 方案应用了两个理论：(1) 素数有无限个；(2) 每个正整数能够分解为唯一的素数乘积序列. 当已有多个 CA 的情况下，方案允许加入新的 CA 并为新的 CA 产生相应私钥.

2005 年，Hanaoka 等人[33]证明了前向安全的分层基于身份的加密方案在文中建立的安全模型下是不安全的. 而后给出了用任意基于身份的加密构造安全的基于身份的分层加密方案的方法. 由此设计了一种基于身份的分层强密钥隔离加密方案，方案能够在不进行交互，不利用任何认证中心的情况

下进行解密密钥更新.并且在随机预言下,方案可证明安全.

4.2 平行密钥隔离(Parallel Key-Insulated Scheme)

2006 年,Hanaoka 等人[34]解决了频繁密钥更新导致的协助者密钥泄漏概率变大的问题.其提出了使用两个协助者的密钥隔离方案.两个协助者在不同时间进行密钥更新从而减小了协助者密钥暴露的概率.并且对于原基于身份加密(BF-IBE)的方案来说,方案在解密密钥长度、密文长度以及解密的计算消耗上没有改变.Weng 等人[35]将平行密钥隔离应用到了基于身份的加密系统中设计了一种基于身份的平行密钥隔离加密方案.方案拥有安全密钥更新以及平行密钥隔离方案的安全属性,能够在不增加协助者密钥暴露的情况下进行多次密钥更新.在标准模型下,由于方案基于 DBDH 问题,所以方案能够抵抗选择明文攻击;又由于方案使用的是 Waters 的 IBE 系统且 IBE 系统具有选择密文攻击安全,所以方案能够抵抗选择密文攻击.由此整个方案是可证明安全的.

2007 年,Libert 等人[36]使用双线性对构造出基于标准模型的平行密钥隔离加密方案,方案不仅满足强密钥隔离还保证了相当的效率,Libert 等人也说明了 PKIE 与 Boneh 等人提出的聚合签名之间的关系.

2008 年,文献[37]中提出标准模型下的基于身份的平行密钥隔离签名方案.方案在标准模型下是可证明安全的,并在 CDH 问题下满足强密钥隔离以及完美密钥隔离等安全属性.

2011 年,文献[38]提出了一种标准模型下基于身份的平行密钥隔离签名方案.提出的方案比文献[37]中的方案在验证上效率更高.在标准模型下,方案是可证明安全的,并且在 CDH 问题下还满足安全密钥更新、完美密钥隔离以及强密钥隔离等安全属性.文献[39]中说明一般的平行密钥隔离加密方案是通过使用两个不相关的长期密钥更新来改变短期密钥的,而这种情况下,一旦有一个长期密钥发生泄漏,就会导致一半的短期密钥或者一半密文发生泄漏.由此文献提出了多个长期密钥的平行密钥隔离加密方案.方案中长期密钥的个数决定了单个长期密钥泄漏时导致的短期密钥或者密文泄漏的比例,如当长期密钥有 n 个,则短期密钥以及密文暴露数量则为 $1/n$.

2012 年,文献[40]提出了在标准模型下基于密文策略属性基的平行密钥隔离加密(CPABPKIE)方案,方案满足强密钥隔离安全等安全属性,并且在 DBDH 问题上,当所用的伪随机函数是理想的伪随机函数时,方案在选择明文攻击下是不可区分的即选择明文安全.方案也能通过文献[41]中的方法证明出其具有选择密文安全.

4.3 基于身份的密钥隔离

2006 年 Zhou 等人[42]提出了基于身份的密钥隔离签名.方案是基于 SOK-IBS(Sakai-Ogishi-Kasahara identity based signature)签名的.虽然方案将密钥隔离运用到 IBS(Identity Based Signature,基于身份的签名)中,减少了密钥泄漏带来的危害,但是由于其充分训练后的密钥是完全保存在协助者这个硬件中的,所以它不满足强密钥隔离安全;并且随机预言模型在现实世界可能并不安全,所以文中的方案并不安全.Weng 等人[43]先指出文献[42]中的方案并不是强密钥隔离,然后在文中重新形式化定义了 IBKIS(ID-Based Key-Insulated Signature)模型的以及其安全性,其中的安全性定义比文献[42]中的安全性定义更加严厉.在基于新的 IBKIS 模型以及安全性,Weng 等人提出了一种满足强密钥隔离以及完美密钥隔离的签名方案,方案没有固定的生命周期限制并且能够进行随机密钥更新.文章最后对提出的方案的效率以及安全性进行了分析,文章证明了在随机预言模型下由于 CDH 问题,方案满足强密钥隔离以及完美密钥隔离等安全属性.

2007 年,文献[44]中在标准模型下构造了一种具有可证明安全的基于身份的密钥隔离签名方案 IBKIS.在 CDH 问题下,方案在面对选择密文攻击下是不可伪造并满足密钥隔离等安全属性.

2008 年,文献[45]改进了文献[42]中的 IBKIS 方案,提出了标准模型下基于身份的密钥隔离签名方案.文中证明了在 CDH 问题上,当方案使用的 Hash 函数能够忍耐碰撞并且使用的伪随机函数是真正的伪随机的情况下,方案满足安全密钥更新、完美密钥隔离以及强密钥隔离等安全属性.

2009 年,因为对于电子现金系统来说密钥泄漏是致命的威胁,所以文献[46]中将密钥隔离应用到电子现金系统中,其改进了文献[47]中的方案使其能够应对密钥泄漏问题.方案的安全性是建立于 CDH 和 DDH 问题的,所以具有安全依据.最后文章证明了方案还满足匿名性、公平性以及密钥隔离的性质.

2010 年,Hanaoka 等人[48]提出了构造平行密

钥隔离的方案即其可以通过使用一次性前向安全公钥加密系统(OTFS-PKE)构造，其中 OTFS-PKE 又可通过任意 IBE 或者分层 IBE 构造，因此得到完整的构造过程，并且文章给出了相应的例子. 文章还说明了可以不用双线性对而只是使用二次剩余假设等困难问题来构造平行密钥隔离方案. 同时证明了由此构造的平行密钥隔离方案的密文较短并且加解密的计算消耗也较小，文中最终给出了 3 种不同的构造实例并给出了效率对比.

2011 年，Wang 等人[49]将密钥隔离应用到环签名中. 提出了标准模型下基于身份的密钥隔离环签名方案. 方案使用了 Brent Waters 的基于身份加密模型. 方案在标准模型下可证明安全，并具有完全匿名以及可在不增加协助者密钥泄漏的风险下频繁更新密钥的特点. 最后 Wang 等人证明了方案在 CDH 问题上满足强密钥隔离以及完美密钥隔离等安全属性. Lin[50]提出了随机预言模型下的基于身份的可变换认证的密钥隔离加密方案(IB-KICAE)，方案不仅满足任意变换、无限时间片以及随机密钥更新等安全属性，还具有不可区分性以及不可伪造性以对抗自适应选择密文攻击以及选择明文攻击. 最后 Lin 还说明了从效率上看方案在现实应用中是可行的.

2012 年，Wu 等人[27]提出了能够分批验证的并具有密钥隔离的基于身份的签名方案. 其中的分批验证有两种情况：(1) 同一时间验证多个文件；(2) 不同时间验证多个文件. 因为方案的安全性主要依赖于 CDH 问题以及 DDH 问题，所以安全性是可证明的. 方案还满足强密钥隔离以及不可伪造等安全属性. 文献[51]中设计了一种具有密钥隔离的基于身份的签密方案. 文中证明了在标准模型下，方案可证明安全. 文中也证明了方案在 DBDH 问题以及 CDH 问题上满足密钥隔离以及强密钥隔离的. 文中还说明了方案较其他类似方案来说效率更高.

4.4　其　他

4.4.1　门限密钥隔离

2008 年，文献[52]提出了标准模型下的基于身份的门限密钥隔离加密方案(IBTKIE)，方案中有多个协助者，对于一种 (k,n) 门限密钥隔离方案，在总共 n 个协助者中会有 k 个协助者对密钥更新提供帮助. 如果方案中没有协助者被攻陷，那么方案与原密钥隔离方案相似；当有协助者被攻陷时，被攻陷协助者即使有 $k-1$ 个，方案仍然能保持安全性；如果所有协助者都被攻陷，那么只要临时密钥不泄漏，系统的安全性仍然能得到保证. 这种门限密钥隔离方案比起传统的密钥隔离方案更加安全，而且比起平行密钥隔离来说其更加灵活. 由于整个方案是基于 Waters 的 IBE 系统的，所以在标准模型下是可证明安全的. 虽然比起平行密钥隔离方案其更新密钥的时间花销有所增加，但是就整个方案过程来说，其比平行密钥隔离方案更加高效. 方案还满足随机密钥更新、密钥隔离以及强密钥隔离安全等安全属性，并且能够抵御选择密文攻击，更重要是其能够抵御协助者被攻陷导致的欺骗攻击.

4.4.2　代理签名

2009 年，文献[53]将密钥隔离引入到代理签名中，由于方案是基于 CDH 问题的，所以文中提出的方案满足强密钥隔离、完美密钥隔离性质. 同时这个方案没有周期限制并且能够进行随机密钥更新. 方案中有委托信息，委任者会发给被委任者一个信息，信息包括委任信息以及相应的保护委任信息完整性并能认证委任者的信息. 被委任者的签名密钥具有密钥更新的能力.

4.4.3　无证书密钥隔离

2009 年，文献[54]中设计了标准模型下的无证书密钥隔离签名方案，其主要解决了无证书签名中的私钥泄漏问题以及基于身份的密钥隔离签名的密钥托管问题. 文中最后证明在 NGBDH 问题以及 Many-DH 问题下，方案的签名信息是无法伪造的. 并且方案也能够进行安全密钥更新.

2011 年，文献[55]基于 Weng 的 IBKIS 模型以及 Xiong 的无证书签名模型在随机模型下设计出一种强密钥隔离无证书签名方案. 由于方案是无证书密钥隔离签名方案，所以没有密钥托管的问题. 最后文章证明了在 NGBDH 问题以及 Many-DH 问题下签名信息是无法伪造的，并证明该方案在随机预言模型下是可证明安全的，并且方案还满足完美密钥隔离、强密钥隔离以及安全密钥更新等安全属性.

表 2 和表 3 为部分密钥隔离加密方案的小结，表 4 和表 5 为部分密钥隔离签名方案小结. 表 2、表 3、表 4 和表 5 中某个文章分 3 行表示文中提出的 3 种方法，如表中[34]-1 表示文献[34]提出的第 1 种方案，[34]-2 表示文献[34]提出的第 2 种方案，[34]-3 表示文献[34]提出的第 3 种方案. 其他有多个方案的文献类似. 如果文献只有一种方案则直接表示而不用加“-1”等.

表 2 密钥隔离加密方案安全性

方案	公钥密码体制	模型	数学难题	强密钥隔离	完美密钥隔离	安全密钥更新	随机密钥更新	无限制时间片数目
[34]-1	PKI	ROM	CBDH	*	*	*	×	×
[34]-2	PKI	ROM	CBDH	*	*	*	×	×
[34]-3	PKI	ROM	CBDH	*	*	*	×	×
[35]	ID-PKC	SM	DBDH	√	×	√	×	×
[36]	PKI	SM	BDH、DBDH	√	*	*	×	×
[39]	ID-PKC	SM	ABDHE	*	*	*	×	√
[40]	PKI	SM	DBDH	√	*	*	×	√
[48]-1	PKI	SM	DBDH	*	*	*	×	√
[48]-2	PKI	SM	DBDH	*	*	*	×	√
[48]-3	PKI	SM	DBDH	*	*	*	×	√
[52]	ID-PKC	SM	CDH	√	*	*	√	√

表 3 密钥隔离加密方案效率

方案	密文长度	密钥长度	加密开销	解密开销
[34]-1	$\|t\|+\|G_1\|+\|Z\|$	$\|G_1\|$	t_e+2t_p+T	t_p
[34]-2	$\|t\|+\|G_1\|+\|Z\|$	$\|G_1\|+\|Z\|$	t_e+2t_p+T	t_p
[34]-3	$\|t\|+\|G_1\|+\|Z\|$	$\|G_1\|$	t_e+2t_p+T	t_e+t_p
[35]	$\|t\|+3\|Z\|+\|G_1\|+\|G_2\|$	$4\|G_1\|$	$4t_e+t_p+T$	$4t_p$
[36]	$3\|G_1\|+\|G_2\|$	$3\|G_1\|$	$3t_e+t_p+T$	$3t_p$
[39]	$\|t\|+(n+1)\|G_1\|+2\|G_2\|$	$(1+n)\|G_1\|+\|Z\|$	$(1+n)t_e+2t_p+2T$	$(1+n)t_p+2T$
[48]-1	$2\|G_1\|+\|G_2\|$	$5\|G_1\|$	$3t_e+T$	$2t_p$
[48]-2	$3\|G_1\|+\|G_2\|$	$6\|G_1\|$	$6t_e+T$	$3t_p$
[48]-3	$2\|G_1\|+\|G_2\|$	$(2n+1)\|G_1\|$	$3t_e+T$	$2t_p$
[52]	$3\|G_1\|+\|G_2\|$	$4\|G_1\|$	$3t_e+T$	$3t_p$

表 4 密钥隔离签名方案效率

方案	签名开销	验证开销	签名长度
[7]	$2t_e$	$(k+2)t_e+(k+4)T$	$\|t\|+3\|Z\|$
[13]	$2t_e$	t_e	$\|t\|+\|G_1\|+\|Z\|$
[21]	t_e	$4t_e$	$\|t\|+\|G_1\|+2\|Z\|$
[23]	t_e	$3t_e$	$\|t\|+\|G_1\|+2\|Z\|$
[25]	$2t_e$	$5t_p$	$\|t\|+3\|G_1\|$
[26]	t_e+nt_p+nT	$2t_p+T$	$\|t\|+2\|G_1\|+\|G_2\|$
[27]-1	$3t_e$	$3t_p+2t_e$	$\|t\|+3\|G_1\|$
[27]-2	$3t_e$	$3t_p+2t_e$	$\|t\|+3\|G_1\|$
[27]-3	$3t_e$	$3t_p+(n+1)\ t_e$	$\|t\|+3\|G_1\|$
[28]	$6t_e$	$5t_p$	$\|t\|+4\|G_1\|$
[29]	$7t_e$	$4t_p+T$	$\|t\|+4\|G_1\|$
[30]	$2t_e$	$5t_p$	$\|t\|+3\|G_1\|$
[37]	$6t_e$	$6t_p$	$\|t\|+5\|G_1\|$
[38]	$3t_e+3T$	$2t_p+3T$	$\|t\|+2\|G_1\|+3\|G_2\|$
[42]	$2t_e$	$4t_p$	$\|t\|+3\|G_1\|$
[43]	$2t_e$	$4t_p$	$\|t\|+3\|G_1\|$
[44]	$2t_e$	$5t_p$	$\|t\|+4\|G_1\|$
[45]	$4t_e$	$5t_p$	$\|t\|+4\|G_1\|$
[54]	$2t_e$	$7t_p$	$\|t\|+4\|G_1\|$
[55]	$2t_e$	$5t_p$	$\|t\|+3\|G_1\|$

表 2 和表 5 中"*"代表文中没有提及，ROM 表示随机预言模型，SM 表示标准模型，PKI 表示公钥基础设施，ID-PKC 表示基于身份，CL-PKC 代表无证书，AB 表示基于属性，CB_PKC 表示基于证书. DLA 代表离散对数假设，CDH 代表 Computational Diffie-Hellman problem，BDH 代表 Bilinear Diffie-Hellman problem，DDH 代表Decision Diffie-Hellman problem，NGBDH 代表 Non-pairing-based Generalized Bilinear Diffie-Hellman problem，Many-DH 代表 Many Diffie-Hellman，CBDH 代表 Computational Bilinear Diffie-Hellman problem，DBDH 代表 Decision Bilinear Diffie-Hellman problem，ABDHE 代表 Augmented Bilinear Diffie-Hellman Exponent problem.

表 3 和表 4 中$|t|$表示一个时间片段的长度，$|Z|$表示一个 Z 元素的长度，$|G_1|$表示一个 G_1 中的元素的长度，$|G_2|$表示一个 G_2 中的元素的长度，t_e表示一个乘法运算的运算时间，t_p表示一次双线性对运算时间，k 代表阈值，i 代表时间片，T 代表指数运算.

总体来说密钥隔离的发展分为如下 3 个阶段：

(1) 2002 年～2003 年，密钥隔离启蒙阶段. 2002 年 Dodis 提出密钥隔离思想并实现了第 1 种密钥隔离加密方案；2003 年，Dodis 实现了第 1 种密钥隔离签名方案. 这个阶段大部分研究主要集中在非扩展的密钥隔离研究上.

(2) 2004 年～2005 年，密钥隔离方案扩展阶段. 从 2004 年开始出现了关于密钥隔离扩展即将密钥隔离方案放到不同场景中，增强不同应用场景对于密钥泄露的容忍能力. 如 2004 年为了解决多个 CA 的跨域以及密钥泄露问题提出的分层的密钥隔离系统；2005 年，为了解决基于身份加密方案中的

表 5　密钥隔离签名方案安全性

方案	公钥密码体制	模型	数学难题	强密钥隔离	完美密钥隔离	安全密钥更新	随机密钥更新	无限制时间片数目
[7]	PKI	ROM	DLA	√	*	√	√	×
[13]	PKI	SM	CDH	√	√	√	√	×
[19]	PKI	ROM	Strong RSA Problem	√	×	*	×	×
[21]	PKI	ROM	DLA	√	√	*	√	×
[23]	PKI	ROM	DLA	√	√	*	√	×
[25]	PKI	ROM	CDH	√	×	×	√	×
[26]	ID-PKC	ROM	CDH	√	×	*	√	√
[27]-1	ID-PKC	ROM	CDH,DDH	√	×	×	×	×
[27]-2	ID-PKC	ROM	CDH,DDH	√	×	×	×	×
[27]-3	ID-PKC	ROM	CDH,DDH	√	×	×	×	×
[28]	PKI	SM	CDH	√	√	√	×	×
[29]	AB	SM	CDH	√	×	*	√	*
[30]	CB_PKC	ROM	CDH	√	*	√	√	*
[37]	ID-PKC	SM	CDH	√	√	√	×	×
[38]	ID-PKC	SM	CDH	√	√	√	×	×
[42]	ID-PKC	ROM	CDH	×	×	*	*	√
[43]	ID-PKC	ROM	CDH	√	√	√	√	×
[44]	ID-PKC	SM	CDH	×	*	*	√	×
[45]	ID-PKC	SM	CDH	√	√	√	√	×
[54]	PKI	SM	NGBDH,Many-DH	√	*	*	√	×
[55]	CL-PKC	ROM	CDH	√	√	√	√	√

密钥泄露问题提出了第 1 种基于身份的分层密钥隔离加密算法等.

(3) 2006 年到现在,密钥隔离方案深度研究阶段.这个阶段中密钥隔离效率尤其是可证明安全的研究成为了重点.这个阶段提出了多种标准模型下的密钥隔离方案而且各个方案具备的安全属性越来越多,如 2006 年,为了解决协助者频繁更新密钥导致的密钥泄露概率增加问题提出的平行密钥隔离方案;2008 年,为增强基于身份的密钥隔离方案的安全性提出的第 1 个基于身份的门限密钥隔离方案,特别的 2009 年还出现了针对密钥隔离方案中的信道问题的研究[22].

5　未来工作与结论

对于密码系统来说密钥泄漏是最为致命的攻击.一旦发生了密钥泄漏,密码系统所有安全性将全部丧失.密钥隔离就是解决密钥泄露问题所提出的方案之一.本文首先说明了密钥泄漏导致的安全问题,由此引出密钥隔离方案.本文对密钥隔离的加密、签名以及密钥协商的形式化定义、安全模型以及安全定义进行了描述,还针对目前的密钥隔离方案的研究现状进行了介绍,为日后密钥隔离研究提供帮助.

未来工作包括如下 3 个部分:

(1) 对已有的方案进行扩展,提出其他具有特殊功能的密钥隔离方案.随着应用场景的不断增加,为了适应应用场景的变化,必须对其他场景中未加入密钥隔离性质的密钥方案进行扩展,提出安全性更高使用范围更广的密钥隔离方案.例如当前云技术成为了热点,为了解决云技术的安全性很多密码系统被提出,可搜索加密系统[56-58]就是其中之一.可搜索公钥加密方案是为了解决云存储中用户数据隐秘性以及可搜索性而设计的一种密码系统,而这种系统在面对密钥泄露的情况下仍然是脆弱的,所以可以向这类系统加入密钥隔离等抗密钥泄露技术提高安全性.

(2) 无证书密钥隔离签名与加密方案研究.目前无证书的密钥隔离方案只有签名方案[54-55],虽然无证书的密钥隔离签名方案仍然有研究的必要,但是目前还没有无证书加密方案的相关研究,所以这是密钥隔离研究中新的领域,对无证书的密钥隔离加密的研究非常重要.

(3) 利用双线性对以外的数学工具(RSA、离散对数等)构造高效的方案:双线性对在标准模型下构造密钥隔离方案中广泛使用,但相比其他的数学工具,双线性对的运行效率较低,所以在不使用双线性对的情况下,是否能构造出高效的密钥隔离方案也是一个开放性问题.

总的来说,无论对于签名、加密还是密钥协商的

密钥隔离方案,虽然加密、签名以及密钥协商的实际算法对方案有一定影响,不过各个方案的区别却都主要集中在密钥更新的方法即怎样使得时间片影响到密钥、密钥需要协助者提供怎样的信息以及如何实现密钥更新,所以要得到一个高效的方案,就必须研究密钥更新方式.而且对于一个方案来说,密钥长度等也很重要,因为这也将影响到具体的算法的效率,而密钥长度也受到密钥更新方式的影响.所以研究密钥更新方式是研究密钥隔离方案的核心.以此为突破口,本文后续将针对高效的标准模型下的密钥隔离方案进行研究,得到一个不使用双线性对以及随机预言模型的、更加高效的密钥更新方式从而得到更为高效的密钥隔离方案.并使得其能够被应用于不同情况下的签名、加密以及密钥协商方案中.

参 考 文 献

[1] Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612-613

[2] Desmedt Y, Frankel Y. Threshold cryptosystems//Proceedings of the Advanecs in Cryptology-Crypto'89. California, USA, 1989: 307-315

[3] Ostrovsky R, Yung M. How to withstand mobile virus attacks//Proceedings of the PODC'91. New York, USA, 1991: 51-59

[4] Bellare M, Miner S. A forward-secure digital signature scheme //Proceedings of the Advances in Cryptology-Crypto'99. California, USA, 1999: 431-448

[5] Dodis Y, Katz J, Xu Shouhuai, et al. Key-insulated public-key cryptosystems//Proceedings of the Eurocrypt 2002. Amsterdam, The Netherlands, 2002: 65-82

[6] Itkis G, Reyzin L. SiBIR: Signer-base intrusion-resilient signatures//Proceedings of the Crypto'02. California, USA, 2002: 499-514

[7] Dodis Y, Katz J, Xu Shouhuai, et al. Strong key insulated signature schemes//Proceedings of the PKC 2003. Miami, USA, 2003: 130-144

[8] Bellare M, Palacio A. Protecting against key exposure: Strongly key-insulated encryption with optimal threshold. Applicable Algebra in Engineering, Communication and Computing, 2006, 16(6): 379-396

[9] Hanaoka Y, Hanaoka G, Shikata J, et al. Unconditionally secure key-insulated cryptosystems models, bounds and constructions//Proceedings of the ICICS 2002. Singapore, 2002: 85-96

[10] Cheon J H, Hopper N, Kim Y, et al. Authenticated key-insulated public key encryption and timed-release cryptography. International Financial Cryptography Association (2004), 2004: 307-315

[11] Cheon J H, Hopper N, Kim Y, et al. Timed-release and key-insulated public key encryption//Proceedings of the 10th International Conference on Financial Cryptography and Data Security. Anguilla, British West Indies, 2006: 191-205

[12] Qiu Weidong, Zhou Yaowei, Zhu Bo, et al. Key-insulated encryption based key pre-distribution scheme for WSN//Proceedings of the ISA 2009. New York, USA, 2009: 200-209

[13] Yum D H, Lee P J. Efficient key updating signature schemes based on IBS//Proceedings of the Cryptography and Coding 2003. Cirencester, UK, 2003: 167-182

[14] Koga S, Sakurai K. A distributed online certificate status protocol with a single public key//Proceedings of the PKC 2004. Singapore, 2004: 389-401

[15] González-Deleito N, Markowitch O, Dall'Olio E. A new key-insulated signature scheme//Lopez J, Qing S, Okamoto E eds. Information and Communications Security. Lecture Notes in Computer Science 3269. Berlin Heidelberg: Springer-Verlag, 2004: 465-479

[16] Guillou L C, Quisquater J-J. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory//Proceedings of the EUROCRYPT 1988. Davos, Switzerland, 1988: 123-128

[17] Li Rupeng, Du Xianghua, Li Guowen, et al. Key-insulated group signature scheme with selective revocation//Proceedings of the 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07). Seoul, Korea, 2007: 1057-1063

[18] Li Rupeng, Yu Jia, Wang Jin, et al. Key-insulated group signature scheme with verifier-local revocation//Proceedings of the ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. Qingdao, China, 2007: 273-278

[19] Liu J K, Wong D S. Solutions to key exposure problem in ring signature. International Journal of Network Security, 2008, 6(2): 170-180

[20] Lee Younggyo, Won Dongho. A method for detecting the exposure of a secret key in key-insulated scheme. International Journal of Computer Science and Network Security, 2008, 8(9): 13

[21] Ohtake G, Hanaoka G, Ogawa K. An efficient strong key-insulated signature scheme and its application//Proceedings of the EuroPKI 2008. Trondheim, Norwa, 2008: 150-165

[22] Bellare M, Duan S, Palacio A. Key insulation and intrusion resilience over a public channel//Proceedings of the CT-RSA 2009. San Francisco, USA, 2009: 84-99

[23] Kang Baoyuan, Lu Tong. Cryptanalysis and improvement on key-insulated signature scheme//Proceedings of the 2010 International Conference on Computer and Information Application (ICCIA). Tianjin, China, 2010: 149-151

[24] Seito T, Aikawa T, Shikata J, et al. Information-theoretically secure key-insulated multireceiver authentication codes //Proceedings of the AFRICACRYPT. Stellenbosch, South Africa, 2010: 148-165

[25] Du Haiting, Li Jiguo, Zhang Yichen, et al. Certificate-based key-insulated signature//Proceedings of the ICDKE 2012. Wuyishan, China, 2012: 206-220

[26] Lin Hanyu, Wu Tzongsun, Lee Minglun, et al. New efficient identity-based key-insulated multisignature scheme. International Journal of Machine Learning and Computing, 2013, 3(1): 117-120

[27] Wu Tsuyang, Tseng Yuhmin, Yu Chingwen. ID-based key-insulated signature scheme with batch verifications and its novel application. International Journal of Innovative Computing, Information and Control, 2012, 8(7): 4797-4810

[28] Wan Zhongmei, Li Jiguo, Hong Xuan. Parallel key-insulated signature scheme without random oracles. Journal of Communications and Networks, 2013, 15(3): 252-257

[29] Chen Jianhong, Long Yu, Chen Kefei, et al. Attribute-based key-insulated signature and its applications. Information Sciences, 2014, 275: 57-67

[30] Li Jiguo, Du Haitong, Zhang Yichen, et al. Provably secure certificate-based key-insulated signature scheme. Concurrency and Computation: Practice and Experience, 2014, 26(8): 1546-1560

[31] Seito T, Shikata J. Information-theoretically secure key-insulated key-agreement//Proceedings of the 2011 IEEE Information Theory Workshop (ITW). Paraty, Brazil, 2011: 287-291

[32] Le Zhengyi, Ouyang Yi, Ford J, et al. A hierarchical key-insulated signature scheme in the CA trust model//Proceedings of the 7th International Conference on Information Security (ISC 2004). Palo Alto, USA, 2004: 280-291

[33] Hanaoka Y, Hanaoka G, Shikata J, et al. Identity-based hierarchical strongly key-insulated encryption and its application //Proceedings of the ASIACRYPT. Chennai, India, 2005: 495-514

[34] Hanaoka Y, Hanaoka G, Imai H. Parallel key insulated public key encryption//Proceedings of the PKC 2006. New York, USA, 2006: 105-122

[35] Weng Jian, Liu Shengli, Chen Kefei, et al. Identity-based parallel key-insulated encryption without random oracles: Security notions and construction//Proceedings of the INDOCRYPT. Kolkata, India, 2006: 409- 423

[36] Libert B, Quisquater J-J, Yung M. Parallel key-insulated public key encryption without random oracles//Proceedings of the PKC2007. Beijing, China, 2007: 298-314

[37] Weng Jian, Chen Kefei, Liu Shengli, et al. Identity-based parallel key-insulated signature without random oracles. Journal of Information Science and Engineering, 2008, 24(4): 1143-1157

[38] Wan Zhongmei. A new identity-based parallel key-insulated signature scheme without random oracles//Proceedings of the 2011 4th International Symposium on Computational Intelligence and Design. Hangzhou, China, 2011: 27-30

[39] Ren Yanli, Wang Shuozhong, Zhang Xinpeng, et al. Identity-based parallel key-insulated encryption with multiple long-term keys//Proceedings of the International Conference on ICCE2011, AISC. Chiang Mai, Thailand, 2011: 277-283

[40] Chen Jian-Hong, Chen Ke-Fei, Long Yu, et al. Ciphertext policy attribute-based parallel key-insulated encryption. Journal of Software, 2012, 23(10): 2795-2804(in Chinese) (陈剑洪，陈克非，龙宇等. 密文策略的属性基并行密钥隔离加密. 软件学报，2012，23(10)：2795-2804)

[41] Sahai A. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security//Proceedings of the 40th Annual Symposium on Foundations of Computer Science. New York, USA, 1999: 543-553

[42] Zhou Yuan, Cao Zhenfu, Chai Zhenchuan. Identity-based key insulated signature//Proceedings of the 2nd International Information Security Practice and Experience Conference (ISPEC 2006). Hangzhou, China, 2006: 226-234

[43] Weng Jian, Chen Kefei, Liu Shengli, et al. Identity-based key-insulated signature with secure key-updates//Proceedings of the 6th China International Conference on Information Security and Cryptology. Beijing, China, 2006: 13-26

[44] Weng Jian, Chen Kefei, Liu Shengli, et al. Identity-based key-insulated signature without random oracles//Proceedings of the Computational Intelligence and Security. Harbin, China, 2007: 470-480

[45] Weng Jian, Chen Kefei, Liu Shengli, et al. Identity-based strong key-insulated signature without random oracles. Journal of Software, 2008, 19(6): 1555-1564

[46] Zhang Xiaoping, Gui Weixia. ID-based key-insulated electronic cash system with multiple banks//Proceedings of the 2nd International Conference on Information and Computing Science(ICIC'09). Washington, USA, 2009: 247-249

[47] Wang Changji, Tang Yong, Li Qing. ID-based fair off-line electronic cash system with multiple banks. Journal of Computer Science and Technology, 2007, 22(3): 487-493

[48] Hanaoka G, Weng Jian. Generic constructions of parallel key-insulated encryption//Garay J A, De Prisco R eds. Security and Cryptography for Networks. Lecture Notes in Computer Science 6280. Berlin Heidelberg: Springer-Verlag, 2010: 36-53

[49] Wang Huaqun, Zhang Yuqing. Identity-based strong key-insulated ring signature scheme in the standard model// Proceedings of the 2011 7th International Conference on Mobile Ad-hoc and Sensor Networks. Beijing, China, 2011: 451-455

[50] Lin Hanyu. A novel identity-based key-insulated convertible authenticated encryption scheme. International Journal of Foundations of Computer Science, 2011, 22(3): 739-756

[51] Chen Jianhong, Chen Kefei, Wang Yongtao, et al. Identity-based key-insulated signcryption. Informatica, 2012, 23(1): 27-45

[52] Weng Jian, Liu Shengli, Chen Kefei, et al. Identity-based threshold key-insulated encryption without random oracles// Proceedings of the CT-RSA 2008. San Francisco, USA, 2008: 203-220

[53] Wan Zhongmei, Lai Xuejia, Weng Jian, et al. Identity-based key-insulated proxy signature. Journal of Electronics (China), 2009, 26(6): 853-858

[54] Wan Zhongmei, Lai Xuejia, Weng Jian, et al. Certificateless key-insulated signature without random oracles. Journal of Zhejiang University Science A, 2009, 10(12): 1790-1800

[55] Wan Zhongmei, Lai Xuejia, Weng Jian, et al. Certificateless strong key-insulated signature//Proceedings of the 2011 International Conference on Information Science and Technology (ICIST). Nanjing, China, 2011: 270-276

[56] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search//Proceedings of the Advances in Cryptology-Eurocrypt 2004. International Conference on the Theory and Applications of Cryptographic Techniques. Interlaken, Switzerland, 2004: 506-522

[57] Baek J, Safavi-Naini R, Susilo W. Public key encryption with keyword search revisited//Proceedings of the Computational Science and Its Applications (ICCSA 2008). Perugia, Italy, 2008: 1249-1259

[58] Li Jin, Wang Qian, Wang Cong, et al. Fuzzy keyword search over encrypted data in cloud computing//Proceedings of the INFOCOM. San Diego, USA, 2010: 1-5

QIN Zhi-Guang, born in 1956, Ph. D., professor. His research interests include open system and network security, information system security.

LIU Jing-Jing, born in 1988, M. S. candidate. His research interests include information security and network security.

ZHAO Yang, born in 1973, Ph. D., associate professor. His research interest is information security.

WU Song-Yang, born in 1982, Ph.D., associate professor. His current research interests include information security, and cloud computing.

XIONG Hu, born in 1982, Ph. D., associate professor. His research interests include network security and cryptography.

NIE Xu-Yun, born in 1975, Ph. D., associate professor. His research interests include information security and cryptography.

ZHU Guo-Bin, born in 1981, Ph. D. candidate. His research interests include information security and cryptography.

Background

The safety of the cryptosystem usually depends on the safekeeping of keys. If the secret keys have been leaked, the security of the cryptosystem will be totally broken. Due to the deployment of cryptosystem in the adversarial setting, key leakage will be inevitable. Thus, in order to resist the key leakage attack, extensive researches have already conducted. As one of the approaches which has been initialized to reduce the loss resulted by key leakage, key-insulated mechanism has been proposed and attracted a lot of attention from the information security and cryptography community. This paper analyzes the state-of-the-art of existing key-insulated encryption and signature schemes in terms of the basic concepts, formal definition, security models and security requirements of key-insulated systems, and highlighting the design philosophy of some classic mechanisms, and it is the preparation for the following work.

This paper is partially sponsored by the National Natural Science Foundation of China (61003230, 61370026), Key Project on the Integration of Industry, Education and Research of Guangdong Province (2012B091000054), Applied Basic Research Projects in Sichuan Province (2014JY0041). The aim of these projects is to address the security issues of mobile and computer in the mobile Internet environment, and realize safety store users' keys.

There are a lot of users in our project, which means key leakage may occur to anyone. In order to reduce the loss, we phased in a cryptosystem that is the key-insulated. It provides a method of solving the problem of key leakage.

Our team has been engaged in design and analysis of the digital signature and encryption system for 5 years. We have published more than 40 papers, in which more than 20 were retrieved by SCI. We undertook the relevant national natural science fund projects at the same time.