一种无密钥托管的基于身份的在线/离线加密方案

何能强[1], 李 叶[2], 张 华[2]

[1] 国家计算机网络应急技术处理协调中心, 北京 中国 100029
[2] 北京邮电大学网络与交换技术国家重点实验室, 北京 中国 100876

摘要 随着基于身份的加密算法发展研究, 在线/离线技术被认为是一个可以有效提升密钥生成和加密时计算效率的方法。在离线时, 很大比例的运算可在明确加密消息和接收方的身份之前完成。当在线时, 方案只需要少量的计算便可完成密钥生成和加密。本文提出了一种高效的基于身份的在线/离线加密方案, 首次使用可选择公用外包密钥生成中心(Outsourced key generator, OKG), 解决了之前 PKG 可单独解密出任意密文的密钥托管问题。在本文的方案中, 除非私钥生成中心(Private key generator, PKG)与 OKG 合谋, 否则 PKG 和 OKG 都不能单独解密出密文消息。在基于身份的在线/离线加密系统建立之后, 用户也可根据对所属 PKG 的信任程度选择是否使用公用 OKG, 而不需要 PKG 重新初始化。方案为减少用户的解密计算代价, 可扩展支持云外包解密, 解密算法中的大部分运算可以外包给云完成。除此之外, 对比于其他现行方案, 本方案在密钥生成算法中也可采取在线/离线技术。论文在随机预言机模型下, 证明了本文的方案在弱 l -BDHI 假设下是 IND-ID-CPA 安全的。最后的效率分析表明本文的方案在计算复杂度和存储开销方面都具有优势。

关键词 基于身份的加密; 在线/离线密钥生成和加密; 外包密钥生成中心; 解密可外包; 密钥托管问题; 可证明安全
中图法分类号 TP309.7 DOI 号 10.19363/j.cnki.cn10-1380/tn.2018.03.03

An Identity-Based Online/Offline Encryption Scheme without Key Escrow

HE Nengqiang[1], LI Ye[2], ZHANG Hua[2]

[1] National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), Beijing 100029, China
[2] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract With the development of Identity-Based Cryptograph, the online/offline technology is considered to be a promising way to accelerate the computation of key extraction and encryption, because a large proportion of computation will be pre-computed in the offline phase before knowing the message to be encrypted and recipient's identity. Light computation is required in the online phase for key generation and message encryption. In this paper, we propose a novel efficient identity-based online/offline encryption with public optional Outsourced Key Generator (OKG) scheme. The OKG is applied in our scheme to remove the inherent key escrow problem. Unless the Private Key Generator (PKG) colludes with OKG, neither PKG nor OKG can decrypt the ciphertext independently. Users can according to their confidence of PKG to choose whether to use the public OKG after set up the IBOOE system. To reduce the user's decryption computational cost, this scheme can support outsourced decryption. The most part of decryption computation can be done by outsourcing cloud. Besides, the key generation algorithm can also adopt the technique of online/offline. Furthermore, we present the proposed scheme can get IND-ID-CPA security based on the weak *l*-BDHI assumption in the random oracle model. The efficiency analysis shows that the scheme has advantages in terms of computation complexity and storage overhead.

Key words identity-based encryption; online/offline key generation and encryption; outsourced key generator; outsourced decryption; key escrow; provable security

1 背景

为了移除公钥基础设施(Public key infrastructure, PKI)系统中复杂的证书认证和管理过程, Shamir[1]在 1984 年首次提出了基于身份的加密(Identity- Based Encryption, IBE)。用户的公钥是一个任意长度字符串, 如一个电子邮件地址、电话号码或其他标识符, 代表了用户在 IBE 系统中的身份。当新用户想要加入 IBE

通讯作者: 何能强, 博士, 副高级工程师, Email: hnq@cert.org.cn。
本课题得到国家自然科学基金项目(No. 61502044)资助。
收稿日期: 2017-10-13; 修改日期: 2018-02-02; 定稿日期: 2018-02-09

系统时, 其他用户可与新用户安全通信而不需要认证其证书。基于身份的加密系统工作原理如图 1 所示, 私钥生成中心 PKG 为 Alice 生成私钥, Bob 用 Alice 的邮箱地址作为公钥加密邮件发送给 Alice。在 PKG 生成私钥的过程中就存在着密钥托管问题。

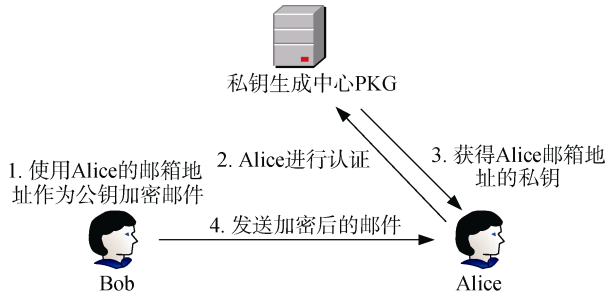

图 1　基于身份的加密系统工作原理[1]

Figure 1　The working principle of the identity-based encryption system[1]

Boneh 和 Franklin 在 2001 年提出了 BF-IBE[2]方案, 他们首次使用椭圆曲线上的双线性对来实现 IBE 系统。在他们方案的基础上, Sakai 和 Kasahara 于 2003 年提出了 SK-IBE[3]方案。与 BF-IBE 方案相比, SK-IBE 方案并不适用于诸如门限密码系统[4]和分层 IBE 系统[5]等许多应用场景。近年来, BF-IBE 方案得到了越来越多的关注。

Even, Goldreich 和 Micali[6]首先提出了在线/离线技术。在他们的数字签名方案中, 签名步骤分为在线和离线两个阶段。在确定签名消息之前运行离线阶段, 在消息被确定之后执行在线阶段。与在线阶段相比, 离线阶段需要更大的计算量(双线性对运算), 在线阶段中应尽可能地减少这样的运算。通过这种方式, 在线阶段只需要少量的计算就可以快速完成。这种方案适用于一些具有低计算能力的设备, 如传感器或移动终端。对于这些设备而言, 大量复杂的计算可以在离线阶段完成。

2008 年, Guo 等人[7]首次将在线/离线技术引入到 IBE 系统方案当中, 并提出了两种基于身份的在线/离线加密(Identity-Based Online/Offline Encryption, IBOOE)算法。在他们的方案中, 大量繁重的计算将在确定具体加密消息和接收方身份之前的离线阶段完成。在确定加密消息和接收方身份后, 在线阶段只需少量计算。由于密文空间太大, Guo 等人提出的这两种在线/离线的 IBE 方案并不适用于轻量级设备。

基于 Boneh 等人[8]和 Gentry[9]的 IBE 方案构造, Guo 等人[7]提出的两个 IBOOE 方案被证明是在无随机预言机下的抗选择密文攻击 (Chosen Ciphertext Attack, CCA)安全。后来, Liu 等人[10]提出了一个更为高效的 IBOOE 方案, 并在随机预言机模型下证明该方案能达到 CCA 安全。随后, Selvi 等人[11]指出了 Liu 等人[10]方案中存在的问题, 在他们的 CCA 安全证明当中存在一个明显的缺陷。与此同时, 在文献[12]中, Selvi 等人提出了一个更为高效的可达到 CCA 安全的在线/离线 IBE 方案。2010 年, 针对无线传感器网络系统, Chu 等人[13]提出了一种新型的 IBOOE 方案, 在离线存储步骤中, 他们移除了 $\mathbb{G}_T$ 中的元素。在那之后, 许多文献[14-18]提出了更为优化的基于身份的在线/离线加密方案。

但是在上述的 IBOOE 方案中, 由于 PKG 可以生成任意用户的私钥, 且可以用它的主密钥解密任意的密文, 系统存在着密钥托管的问题, 当 PKG 被攻破时, 该 IBOOE 系统中所有的用户私钥都将泄露, 致使整个系统的数据面临极大的安全挑战。与此同时, 当用户对 PKG 产生不信任时, 系统也将面临崩溃的状态。

本文为了解决 IBOOE 方案中密钥托管问题, 提出了一种新型高效的基于身份的在线/离线加密方案。在 IBOOE 系统建立之后, 用户也可根据对所属 PKG 的信任程度, 选择是否使用公用 OKG 来解决密钥托管问题, 而且不需要 PKG 重新初始化。另外, 该方案可扩展支持云外包解密。方案旨在为低计算能力的电子设备如传感器或移动终端等提供有效的 IBOOE 方案。大部分的加密运算可在离线阶段完成, 而大部分的解密运算又可外包给云完成。除此之外, 与其它现行 IBOOE 方案不同, 本方案的密钥生成算法也可采用在线/离线技术来提高 PKG 的密钥生成效率。针对用户数量庞大的 IBE 系统, 可通过这种方式减轻 PKG 的计算压力。本文的 IBOOE 方案在随机预言机模型下满足了 IND-ID-CPA 安全性。方案减少了用户在离线阶段时所需的计算量, 同时, 方案在线阶段的计算量也足够小, 可以达到 IBOOE 方案算法的目标。在存储开销和用户通信代价方面, 本文方案也有着明显的提升。

论文其余部分的安排如下: 第二节给出了本文的相关工作。第三节为预备知识的介绍。方案的系统模型与具体方案的构造在第四节和第五节中给出。第六节给出了方案的安全性证明和效率分析。最后, 第七节为本文的结束语。

2　相关工作

自从 Boneh 和 Franklin[2]提出安全高效的使用椭圆曲线上双线性对的基于身份的加密方案之后, 许多 IBE 方案[8,9,19-24]和相关变形方案[25]相继而出。现

在, IBE 方案可以通过素数阶的双线性对[2,3,8,9,19,26]、合数阶的双线性对[23,24]、或者不使用双线性对[20-22,27]来构造。在相同安全性的情况下, 因为椭圆曲线密码学中群的表示较短, 所以在这些构造当中, 基于椭圆曲线的 IBE 方案在计算和实现方面更加高效。例如, 一个 512 位长度的椭圆曲线群可以实现 256 位的安全性, 但相同安全性的 RSA 模数长度至少需要 15360 位[28]。但是对于所有基于双线性对运算的 IBE 方案而言, 加密算法不仅需要椭圆曲线群中的点乘运算, 而且还需要乘法群中的指数运算。

与传统基于双线性对运算的 IBE 方案相比, 为了可以更有效地运行加密算法, 之前的文献提出了两种不同的 IBE 方案(基于身份的在线/离线加密方案和使用陷门离散对数群构造的基于身份的加密方案)。

文献[27]提出了一种使用陷门离散对数(Trapdoor Discrete Log)群构造的 IBE 方案。陷门离线对数群是一个在特定的椭圆曲线上或者是一个在 $\mathbb{Z}_N$ 上定义的最大循环子群, 其中 N 是一个合数。给定任意两个群元素 g 和 h, 如果还给出了陷门信息, 则求解 $h=g^x$ 的离散对数 x 存在多项式时间算法, 否则, 求解 x 最有效率的算法是 Pollard rho 攻击。Paterson 和 Srinivasan[27]研究了如何利用这样一个陷门离散对数群构造 IBE 方案。由于只使用了一种类型的群上的运算(例如 $\mathbb{G}_1$), 所以他们提出的 IBE 方案在加密和解密计算效率方面是非常高效的。但是这种 IBE 方案需要在特定的椭圆曲线上构造, 并且由于使用了陷门计算, 这将导致密钥生成算法的计算效率较低。对比其他基于双线性对运算的 IBE 方案, 这种使用陷门离散对数群所构造的 IBE 方案虽然可以在加密算法里去除 $\mathbb{G}_T$ 中的指数运算, 但是需要使用更加复杂的哈希函数来构造, 所以在方案的实现过程中, 这将带来许多不便。

文献[7]和文献[11]提出了基于身份的在线/离线加密方案。在这种加密方案模型中, 消息发送方可以将加密算法分为离线和在线两个阶段。离线阶段中, 在不明确接收方的身份前, 发送方可以完成尽量多的群运算。在明确接收方身份后的在线阶段, 加密算法只需要一些哈希、模乘和少量的群运算, 这种方案极大减少了确定接收方身份后的加密消息所需时间。IBOOE 方案移除了大量在线阶段时的群运算, 在一定程度上减少了发送方在线计算的时间, 从而显着地节省了实现在线加密算法的硬件成本。

但是, 许多 IBOOE 方案[14,16-21,29]存在密钥托管问题。在 IBOOE 系统中, 所有用户的私钥都由一个可信的 PKG 生成。在这些方案中, PKG 是完全可信的, 但是当PKG进行恶意操作(例如倒卖用户私钥)时, 第三方机构很难进行监督、取证和惩罚, 这对许多 IBOOE 系统的应用和实施构成了极大的安全威胁。

与此同时, 传统的 IBOOE 方案只有一个 PKG, 因此方案将面临如下的两个问题: (1)PKG 需要花费一定的时间和成本并通过一个安全通道给用户传输和更新私钥, 特别是在具有庞大用户数量的大型网络中, PKG 将成为该网络中性能的瓶颈。(2)PKG 将成为网络攻击的首要目标。由于 PKG 中主密钥的存在, PKG 可以生成任意用户的私钥, 一旦 PKG 被攻击成功或者当 PKG 是恶意时, 用户私钥的安全性将荡然无存。所以, 解决 IBOOE 系统中密钥托管的问题变得刻不容缓。

3 预备知识

3.1 符号定义

表 1 给出了本文所用的符号及其含义。

表 1 符号定义

Table 1 Definition of symbols

符号	含义
ID	用户的身份信息
pp	系统的公共参数
op	OKG 的外包参数
msk	系统的主密钥
$omsk$	OKG 的外包主密钥
K_{off}	PKG 的离线私钥
K'_{off}	OKG 的离线私钥
d_{ID}	用户私钥
C_{off}	离线密文
CT	密文

3.2 困难问题

定义 1.双线性映射. $\mathbb{G}$ 是阶为素数 p 的(乘法)循环群, 生成元是 g。$\mathbb{G}_T$ 是阶为素数 p 的(乘法)循环群。当该映射满足以下性质时, 称映射 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 是双线性映射,

(1) 双线性: 对所有的 $u,v\in\mathbb{G}$ 和 $a,b\in\mathbb{Z}_p^*$, 满足 $e(u^a,v^b)=e(u,v)^{ab}$;

(2) 非退化性: $e(g,g)\neq 1$;

(3) 可计算性: 存在一个有效的算法对任何的 $u,v\in\mathbb{G}$, 可计算出 $e(u,v)$。

基于文献[8,10]的 Bilinear Diffie-Hellman Inver-

sion(BDHI)假设如下:

假设 1. l-BDHI 假设. 设 $\mathbb{G}$ 是一个 p 阶循环群, $g\in\mathbb{G}$ 是群的生成元并且 $\beta\in\mathbb{Z}_p^*$。则 l-BDHI 问题是: 给定 $g,g^{\beta},g^{(\beta^2)},...,g^{(\beta^l)}$, 计算 $e(g,g)^{1/\beta}$。

没有一个有效的算法, 能在概率多项式时间内以不可忽略的优势解决 l-BDHI 问题。

假设 2. 弱 l-BDHI 假设. 设 g 和 h 是群 $\mathbb{G}$ 的两个随机生成元, 在 $\mathbb{Z}_p^*$ 随机选择 α。则两个弱 l-BDHI 问题是:

①给定 $g,h,g^{\alpha},g^{(\alpha^2)},...,g^{(\alpha^l)}$, 计算 $e(g,h)^{\frac{1}{\alpha}}$。

②给定 $g,h,g^{\alpha},g^{(\alpha^2)},...,g^{(\alpha^l)}$, 计算 $e(g,h)^{(\alpha^{l+1})}$。

没有一个有效的算法, 能在概率多项式时间内以不可忽略的优势解决这两个弱 l-BDHI 问题。

4 无密钥托管的基于身份的在线/离线加密方案

4.1 方案的形式化定义

本文的 IBOOE 方案在用户选择使用公用外包密钥生成中心 OKG 时, 包含以下七个算法: 系统初始化(*Setup*), OKG 初始化(*OKGSetup*), 离线密钥生成(*OffKeyGen*), 在线密钥生成(*OnKeyGen*), 离线加密(*OffEncrypt*), 在线加密(*OnEncrypt*)和解密(*Decrypt*)。方案的系统框架如图 2 所示。

(1) $Setup(\lambda)\rightarrow(pp,msk)$: 该系统 PKG 输入一个安全参数 λ, 输出公共参数 pp 和主密钥 msk, PKG 保存 msk 作为它的秘密。

(2) $OKGSetup(pp)\rightarrow(op,omsk)$: 公用外包密钥生成中心 OKG 以该 IBOOE 系统的 pp 作为输入并运行初始化算法, 产生并保存针对该系统的外包主密钥 $omsk$ 和外包参数 op, 其中外包参数 op 对该系统中的用户公开。

(3) $OffKeyGen(pp,msk,op,omsk)\rightarrow(K_{off},K'_{off})$ PKG 和 OKG 运行离线密钥生成算法并分别以 $\{msk,pp\}$和$\{omsk,op\}$作为输入, 分别输出并保存离线私钥 K_{off} 和 K'_{off}。

(4) $OnKeyGen(ID,pp,K_{off},K'_{off})\rightarrow d_{ID}$: PKG 和 OKG 分别输入预计算保存的离线私钥 K_{off},K'_{off}, 公共参数 pp 和用户的身份信息 $ID\in\{0,1\}^*$, 输出该用户的私钥 d_{ID}。

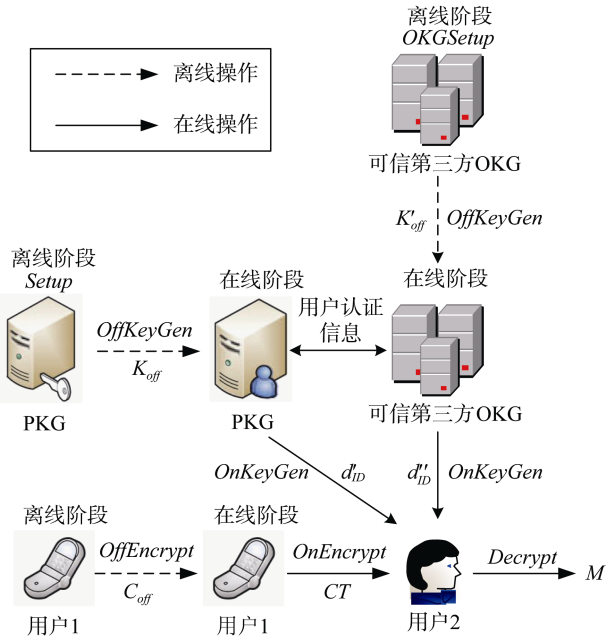

图 2 无密钥托管问题的 IBOOE 方案系统框架

Figure 2 The system framework of the IBOOE scheme without key escrow

(5) $OffEncrypt(pp,op)\rightarrow C_{off}$: 消息发送方(用户 1)执行离线加密算法, 输入公共参数 pp 和外包参数 op, 输出并保存离线密文 C_{off}。

(6) $OnEncrypt(C_{off},M,ID,pp)\rightarrow CT$: 当明确接收方身份后, 消息发送方(用户 1)运行在线加密算法, 输入消息明文 M, 公共参数 pp, 获取保存的离线密文 C_{off} 和接收方的身份信息 $ID\in\{0,1\}^*$, 输出对应的密文 CT。

(7) $Decrypt(CT,d_{ID},pp)\rightarrow M$: 消息接收方(用户 2)运行解密算法, 输入密文 CT, 接收方的私钥 d_{ID} 和公共参数 pp, 如果解密成功, 输出相应的消息明文 M, 否则输出一个拒绝符号 $\perp$。

4.2 方案的安全模型

基于文献[30], 本节定义了方案的安全模型。本文的方案可以满足 IND-ID-CPA 安全性, 允许敌手询问不能用于解密挑战密文的任意用户的私钥。本文方案是基于随机预言机模型证明的(随机预言机模型是指包括攻击者在内的所有协议的参与方, 都有对一个公共的随机预言机的访问权, 例如: 对一个输入 x, 返回一个随机预言 $f(x)$), 正式的安全模型定义如下:

(1) 初始化: 挑战者输入安全参数 λ, 运行系统初始化算法(*Setup*), 将公共参数 pp 发给敌手 $\mathcal{A}$ 并保存主密钥 msk。模拟器 $\mathcal{S}$ 运行 OKG 初始化算法

(*OKGSetup*), 将外包参数 *op* 发给敌手 $\mathcal{A}$ 并保存针对该IBOOE系统的外包主密钥 *omsk* 。这里假设PKG和OKG中至少有一个是未被攻破的。

-对被攻破的 PKG(或者 OKG), $\mathcal{S}$ 将公共参数和主密钥(或者外包参数和外包主密钥)发送给 $\mathcal{A}$ 。

-对未被攻破的 PKG(或者 OKG), $\mathcal{S}$ 将公共参数(或者外包参数)发送给 $\mathcal{A}$ 。

(2) 阶段 1: 敌手 $\mathcal{A}$ 在多项式时间内可以对多个身份 ID_i 发出对应的私钥查询 $q_1,...,q_m$ 。模拟器 $\mathcal{S}$ 通过执行离线密钥生成(*OffKeyGen*)和在线密钥生成(*OnKeyGen*)算法产生对应身份的私钥 d_{ID_i} 并返回给 $\mathcal{A}$ 。

(3) 挑战: 一旦 $\mathcal{A}$ 决定阶段 1 完成, $\mathcal{A}$ 将输出一个想要挑战的身份 ID^*, 但身份 ID^* 不能在阶段 1 的私钥查询中出现过。 $\mathcal{S}$ 提前运行离线加密(*OffEncrypt*)算法生成离线密文 C_{off} 。敌手 $\mathcal{A}$ 提交两个等长的消息 M_0 和 M_1, $\mathcal{S}$ 投掷一个随机的硬币 $b\in\{0,1\}$, 之后 $\mathcal{S}$ 运行在线加密(*OnEncrypt*)算法并返回挑战密文 $CT^* = OnEncrypt(C_{off}, ID^*, pp, M_b)$ 给 $\mathcal{A}$ 。

(4) 阶段2: 对更多的 ID_i 重复阶段1的私钥查询, 要求被查询身份满足 $ID_i \neq ID^*$ 。

(5) 猜测: 敌手 $\mathcal{A}$ 输出一个对 b 的猜测 $b'\in\{0,1\}$, $\mathcal{A}$ 赢得游戏当且仅当 $b'=b$ 。敌手 $\mathcal{A}$ 赢得游戏的优势为:

$$Adv_{\mathcal{A}}(\lambda) = |Pr[b=b'] - \frac{1}{2}|$$

定义 1. 一个IBOOE方案是IND-ID-CPA安全的, 当且仅当不存在多项式有界的敌手能以不可忽略的优势赢得以上游戏。

5 一个新的安全无密钥托管的 IBOOE 方案

基于文献[8,10], 本节提出一个新的安全无密钥托管问题的基于身份的在线/离线加密方案, 并给出方案可外包解密的改进算法。该方案可适用于低计算能力的电子设备, 如传感器或移动终端等。加密和密钥生成算法中的大部分计算可在离线阶段完成, 并且解密算法中的绝大部分计算可由用户安全地外包给云完成。这大大降低了用户端的计算压力。

5.1 方案构造

本方案 7 个算法具体构造如下所示:

(1) $Setup(\lambda)$

系统输入安全参数 λ, 系统参数生成如下: PKG选择一个阶为素数 p 的双线性群 $\mathbb{G}$, 其生成元为 g 。系统定义一个密码学中的哈希函数 $H_1:\{0,1\}^*\to\mathbb{G}$ 。PKG 随机选择两个指数 $\alpha_1, z_1\in\mathbb{Z}_p^*$, 则公共参数 *pp* 和主密钥 *msk* 为:

$$pp = e(g,g)^{\alpha_1}, g^{\frac{1}{z_1}}, H_1, g, g^{z_1} \ , \ msk = \alpha_1, z_1 。$$

其中, 公共参数 *pp* 对系统中用户公开, 主密钥 *msk* 作为秘密由 PKG 安全保存。

(2) $OKGSetup(pp)$

OKG 输入该系统的公共参数 *pp*, OKG 随机选择两个指数 $\alpha_2, z_2\in\mathbb{Z}_p^*$, 计算并公开针对该系统的外包参数 *op*:

$$op = e(g,g)^{\alpha_2}, g^{\frac{1}{z_2}}, g^{z_2}$$

OKG 对该系统的外包主密钥为 $omsk=\{\alpha_2, z_2\}$, 同时 *omsk* 将作为秘密由 OKG 安全保存。

(3) $OffKeyGen(pp, msk, op, omsk)$

①PKG 随机选择 $r_1, r_2\in\mathbb{Z}_p^*$ 并计算 $K_1 = g^{(\alpha_1+r_1)/z_1}$, $K_2' = g^{r_1}$, $K_3 = g^{r_2}$, PKG 的离线私钥为:

$$K_{off} = (r_1, r_2, K_1, K_2', K_3) 。$$

之后, K_{off} 将由 PKG 安全保存。

②OKG 随机选择 $r_3, r_4\in\mathbb{Z}_p^*$ 计算 $K_4 = g^{(\alpha_2+r_3)/z_2}$, $K_5' = g^{r_3}$, $K_6 = g^{r_4}$, OKG 对应的离线私钥为:

$$K_{off}' = (r_3, r_4, K_4, K_5', K_6) 。$$

之后, K_{off}' 将由 OKG 安全保存。

(4) $OnKeyGen(ID, pp, K_{off}, K_{off}')$

PKG 和 OKG 分别输入明确的用户身份信息 $ID\in\{0,1\}^*$ 并读取各自保存的离线私钥 K_{off} 和 K_{off}', 计算并产生用户私钥。

PKG 计算 $K_2 = H_1^{r_2}(ID)\cdot K_2' = g^{r_1}H_1^{r_2}(ID)$, 输出 $d_{ID}'=(K_1, K_2, K_3)$ 并将 d_{ID}' 通过安全信道发送给用户。OKG 计算 $K_5 = H_1^{r_4}(ID)\cdot K_5' = g^{r_3}H_1^{r_4}(ID)$, 输出 $d_{ID}''=(K_4, K_5, K_6)$ 并将 d_{ID}'' 通过安全信道发送给用户。则用户的私钥为:

$$d_{ID} = (d_{ID}', d_{ID}'') = (K_1, K_2, K_3, K_4, K_5, K_6) 。$$

(5) $OffEncrypt(pp, op)$

消息发送方使用公共参数 *pp* 和外包参数 *op* 进

行离线加密。发送方随机选择一个秘密值 $s \in \mathbb{Z}_p^*$，并计算 $C' = e(g,g)^{(\alpha_1+\alpha_2)s}, C_1 = g^{z_1 s}, C_1' = g^{z_2 s}, C_2 = g^s$。发送方的离线密文为:

$$C_{off} = (C', s, C_1, C_1', C_2)。$$

之后, 离线密文 C_{off} 将由发送方安全保存。

(6) $OnEncrypt(C_{off}, M, ID, pp)$

为了将消息 $M \in \mathbb{M}$ 发送给用户身份信息为 $ID \in \{0,1\}^*$ 的接收方, 消息发送方读取离线密文 C_{off} 并计算:

$$C = M \cdot C' = Me(g,g)^{(\alpha_1+\alpha_2)s}, C_3 = H_1^s(ID)$$

则密文 $CT = (C, C_1, C_1', C_2, C_3)$。之后, 密文 CT 可通过信道发送给消息接收方。

(7) $Decrypt(CT, d_{ID}, pp)$

消息接收方收到密文 CT 后, 使用含自己身份的私钥 d_{ID} 解密:

$$D = \frac{e(K_2, C_2)e(K_5, C_2)}{e(K_3, C_3)e(K_6, C_3)},$$

$$E = e(C_1, K_1)e(C_1', K_4)。$$

之后, 接收方通过计算 $\frac{C}{E/D} = M$, 得到消息明文 M。

在 IBOOE 方案中用户选择使用 OKG 的情况下, 上述方案过程如图 3 所示。

发送方	PKG	OKG	接收方
	***Setup*:** $pp = \{e(g,g)^{\alpha_1}, g^{1/z_1}, H_1, g, g^{z_1}\}$ $msk = \{\alpha_1, z_1\}$		
		***OKGSetup*:** $op = \{e(g,g)^{\alpha_2}, g^{1/z_2}, g^{z_2}\}$ $omsk = \{\alpha_2, z_2\}$	
	***OffKeyGen*:** $K_{off} = (r_1, r_2, K_1, K_2', K_3)$	***OffKeyGen*:** $K_{off}' = (r_3, r_4, K_4, K_5', K_6)$	
	***OnKeyGen*:** $d_{ID}' = (K_1, K_2, K_3)$	***OnKeyGen*:** $d_{ID}'' = (K_4, K_5, K_6)$	
***OffEncrypt*:** $C_{off} = (C', s, C_1, C_1', C_2)$ ***OnEncrypt*:** $CT = (C, C_1, C_1', C_2, C_3)$			***Decrypt*:** M

图 3　无密钥托管问题的 IBOOE 方案

Figure 3　The IBOOE scheme without key escrow

发送方	PKG	接收方
	***Setup*:** $pp = \{e(g,g)^{\alpha_1}, g^{1/z_1}, H_1, g, g^{z_1}\}$ $msk = \{\alpha_1, z_1\}$	
	***OffKeyGen*:** $K_{off} = (r_1, r_2, K_1, K_2', K_3)$	
	***OnKeyGen*:** $d_{ID} = (K_1, K_2, K_3)$	
***OffEncrypt*:** $C_{off} = (C', s, C_1, C_2)$ ***OnEncrypt*:** $CT = (C, C_1, C_2, C_3)$		***Decrypt*:** M

图 4　用户完全信任 PKG 时的 IBOOE 方案

Figure 4　The IBOOE scheme when users fully trust PKG

在用户完全信任 PKG 不选择使用 OKG 的情况下, 上述方案移除与 OKG 的所有相关项, 参与方为发送方、接收方和 PKG, 方案具体过程如图 4 所示。

根据是否使用 OKG 时的算法比较, 我们可以看出在 IBOOE 系统建立之后, 当用户选择使用公用 OKG 来解决密钥托管问题时, 针对系统中用户, 只需接收方重新获取解密私钥 d_{ID} 和发送方加密消息 M 时使用外包参数 op 即可, 而不需要 PKG 重新初始化, 在一定程度上减轻了 PKG 的运算压力。

5.2　正确性验证

在 IBOOE 系统中用户选择使用 OKG 的情况下, 接收方可以获得正确的明文。具体验证如下:

$$D = \frac{e(K_2, C_2)e(K_5, C_2)}{e(K_3, C_3)e(K_6, C_3)}$$

$$= \frac{e(g^{r_1} H_1^{r_2}(ID), g^s)e(g^{r_3} H_1^{r_4}(ID), g^s)}{e(g^{r_2}, H_1^s(ID))e(g^{r_4}, H_1^s(ID))}$$

$$= e(g^{r_1}, g^s)e(g^{r_3}, g^s)$$

$$E = e(C_1, K_1)e(C_1', K_4)$$

$$= e(g^{z_1 s}, g^{(\alpha_1+r_1)/z_1})e(g^{z_2 s}, g^{(\alpha_2+r_3)/z_2})$$

$$= e(g,g)^{(\alpha_1+r_1)s} e(g,g)^{(\alpha_2+r_3)s}$$

接收方可得

$$\frac{C}{E/D} =$$

$$\frac{Me(g,g)^{(\alpha_1+\alpha_2)s}}{e(g,g)^{(\alpha_1+r_1)s}e(g,g)^{(\alpha_2+r_3)s}/e(g^{r_1},g^s)e(g^{r_3},g^s)}$$

$$=M$$

在 IBOOE 方案中用户完全信任 PKG 不选择使用 OKG 的情况下, 接收方可以获得正确的明文。具体验证如下:

用户私钥即为: $d_{ID}=(K_1,K_2,K_3)$。

离线密文 C_{off} 即为: $C_{off}=(C'=e(g,g)^{\alpha_1 s},s,C_1,C_2)$。

密文 CT 即为: $CT=(C=Me(g,g)^{\alpha_1 s},C_1,C_2,C_3)$。

解密算法即为: $D=\frac{e(K_2,C_2)}{e(K_3,C_3)}$, $E=e(C_1,K_1)$, 之后, 接收方计算 $\frac{C}{E/D}=M$ 得到消息明文 M。

5.3 扩展方案

本节对提出的用户可选择公用外包密钥生成中心的 IBOOE 方案进行扩展, 使方案在保证安全性的同时支持云外包解密。即使外包的云服务器是半可信的(一方面完成自己的工作, 另一方面会受到来自内部或者外部的攻击, 还可能串通恶意用户窥探用户的文件内容, 获取非法信息), 该扩展方案同样可以保证用户的信息安全, 并且使得用户在解密阶段只需要进行一次指数运算和一次除法运算即可恢复出消息明文 M。扩展方案更加适用于低计算能力的电子设备。

Setup、*OKGSetup*、*OffKeyGen*、*OnKeyGen*、*OffEncrypt*、*OnEncrypt* 算法与 5.1 节中构造相同, 我们不再次赘述, 余下的算法描述如下。

(1) $TKGen(d_{ID})$

接收方输入私钥 $d_{ID}=(K_1,K_2,K_3,K_4,K_5,K_6)$。为了建立转化密钥 TK, 接收方选择一个随机值 $t\in\mathbb{Z}_p^*$ 并计算出转化密钥 $TK=(\widehat{K_1}=K_1^{\frac{1}{t}},\widehat{K_2}=K_2^{\frac{1}{t}},\widehat{K_3}=K_3^{\frac{1}{t}},\widehat{K_4}=K_4^{\frac{1}{t}},\widehat{K_5}=K_5^{\frac{1}{t}},\widehat{K_6}=K_6^{\frac{1}{t}})$, 取回密钥 $RK=t$ 由接收方安全保存。

(2) $Transform(pp,CT,TK)$

接收方将密文 CT 和转化密钥 TK 发送给云端, 云端通过计算:

$$\widehat{D}=\frac{e(\widehat{K_2},C_2)e(\widehat{K_5},C_2)}{e(\widehat{K_3},C_3)e(\widehat{K_6},C_3)}=e(g^{\frac{r_1}{t}},g^s)e(g^{\frac{r_3}{t}},g^s)$$

$$\widehat{E}=e(C_1,\widehat{K_1})e(C_1',\widehat{K_4})=e(g,g)^{\frac{(\alpha_1+r_1)s}{t}}e(g,g)^{\frac{(\alpha_2+r_3)s}{t}}$$

$T_1=C$, $\widehat{T}=\widehat{E}/\widehat{D}=e(g,g)^{\frac{(\alpha_1+\alpha_2)s}{t}}$,

并返回转化密文 $\widehat{CT}=(\widehat{T},T_1)$ 给接收方。

(3) $Dec(pp,CT,\widehat{CT},RK)$

接收方使用取回密钥 RK, 密文 CT 和公共参数 pp 去验证和解密转化密文 $\widehat{CT}$。如果 $T_1\neq C$, 则输出 $\perp$ 表示转化密文未通过验证。如果 $T_1=C$, 则接收方通过计算:

$$T_1/\widehat{T}^t=Me(g,g)^{(\alpha_1+\alpha_2)s}/(e(g,g)^{\frac{(\alpha_1+\alpha_2)s}{t}})^t=M,$$

接收方得到消息明文 M。

6 方案分析

6.1 方案的安全性证明

本节将证明本文构造的 IBOOE 系统可以满足 IND-ID-CPA 安全性。证明中允许敌手可以询问任意用户的私钥 d_{ID}, 只要被询问的用户私钥不能用于解密挑战密文。正式的安全性证明如下。

定理 1. 如果存在一个敌手 $\mathcal{A}$ 能以不可忽略的优势赢得 4.2 节中, 针对提出的 IBOOE 方案所构造的游戏, 则存在一个模拟器 $\mathcal{S}$ 能以不可忽略的优势攻破弱 l-BDHI 假设。

证明. 假设存在一个概率多项式时间的敌手 A 能以不可忽略的优势赢得本文 4.2 节中所描述的游戏。

(1) 初始化: 挑战者运行系统初始化 (λ) 算法并设置问题实例 $g,H_1,g^{(\alpha)},g^{(\alpha^2)},...,g^{(\alpha^l)},T$, 其中 $\alpha\in\mathbb{Z}_p^*$, $g^{(\alpha^i)}\in\mathbb{G}$, $i=1,...,l$, T 为 $e(g,g)^{\frac{1}{\alpha}}$ 或者 $\mathbb{G}_T$ 中的一个随机群元素。PKG 和 OKG 中至少有一个未被攻破, 也就是说对于主密钥 *msk* 和外包主密钥 *omsk* 至少有一个敌手 A 无法获得。

-对被攻破的 PKG(或者 OKG), 模拟器 S 随机选择 $\xi,b\in\mathbb{Z}_p^*$ 并计算 $e(g,g)^{\xi},g^{\frac{1}{b}},g^b$。$S$ 同时发送 (ξ,b) 和 $(e(g,g)^{\xi},g^{\frac{1}{b}},g^b)$ 给敌手 $\mathcal{A}$。

-对未被攻破的 PKG(或者 OKG), 模拟器 S 随机选择 $\xi,b\in\mathbb{Z}_p^*$ 并计算 $T^{\xi},g^{\frac{1}{b}},g^b$。$\mathcal{S}$ 发送 $(T^{\xi},g^{\frac{1}{b}},g^b)$ 给敌手 A。

(2)阶段 1: 敌手 $\mathcal{A}$ 在多项式时间内对多个身份 ID_i 发出对应的私钥查询 $q_1,...,q_m$。如果 PKG(或者

OKG)是被攻破的, $\mathcal{A}$ 可以使用 (ξ,b) 计算出解密私钥组件。如果 PKG(或者 OKG)是未被攻破的, 敌手 $\mathcal{A}$ 进行自己身份 ID 的私钥查询, 模拟器 $\mathcal{S}$ 选取 $r_1...r_4$ 为已知的随机值。解密私钥组件可分为两部分生成。

- PKG 从 $\mathbb{Z}_p$ 中随机选择 r_1, r_2, 解密私钥组件可表示为 $K_1 = g^{(\xi_1+r_1)/b_1}, K_2 = g^{r_1} H_1^{r_2}(ID), K_3 = g^{r_2}$。

- OKG 从 $\mathbb{Z}_p$ 中随机选择 r_3, r_4, 解密私钥组件可表示为 $K_4 = g^{(\xi_2+r_3)/b_2}, K_5 = g^{r_3} H_1^{r_4}(ID), K_6 = g^{r_4}$。

如果敌手 $\mathcal{A}$ 进行非自己身份 ID 的私钥查询, 模拟器 $\mathcal{S}$ 选取 $r_1...r_4$ 为 a^v 加上一些已知的随机值。解密私钥组件可分为两部分生成。

- PKG 设定 $r_1 = a + \eta_1$, $r_2 = a^{\theta_1}$, 其中 η_1 和 θ_1 是从 $\mathbb{Z}_p^*$ 中随机选择的, 解密私钥组件可表示为 $K_1 = g^{(\xi_1+a+\eta_1)/b_1}, K_2 = g^{a+\eta_1} H_1^{a^{\theta_1}}(ID), K_3 = g^{a^{\theta_1}}$。

- OKG 设定 $r_3 = a + \eta_2$, $r_4 = a^{\theta_2}$, 其中 η_2 和 θ_2 是从 $\mathbb{Z}_p^*$ 中随机选择的, 解密私钥组件可表示为 $K_4 = g^{(\xi_2+a+\eta_2)/b_2}, K_5 = g^{a+\eta_2} H_1^{a^{\theta_2}}(ID), K_6 = g^{a^{\theta_2}}$。

(3) 挑战: 敌手 $\mathcal{A}$ 决定结束阶段 1 私钥查询, 并输出一个它想要挑战的身份 ID^*, 身份 ID^* 不能在阶段 1 的私钥查询中出现过。$\mathcal{A}$ 提交两个等长消息 M_0 和 M_1。模拟器 $\mathcal{S}$ 投掷一个随机的硬币 $b \in \{0,1\}$, 建立并返回挑战密文 $CT = (M_b T^{(\xi_1+\xi_2)s}, g^{b_1 s}, g^{b_2 s}, g^s, H_1^s(ID^*))$。如果 $T = e(g,g)^{\frac{1}{\alpha}}$, 则 M_b=M_1; 如果 T 是 $\mathbb{G}_T$ 中的一个随机群元素, 则 M_b=M_0。

(4) 阶段 2: 与阶段 1 相同, 对更多的 ID_i 进行私钥查询, 但要求被查询身份满足 $ID_i \neq ID^*$。

(5) 猜测: 敌手 $\mathcal{A}$ 最终输出一个对 M 的猜测 M'。如果 $M' = M_1$, 模拟器 $\mathcal{S}$ 猜测 $T = e(g,g)^{\frac{1}{\alpha}}$ 是一个元组并输出 1; 否则 $\mathcal{S}$ 猜测 T 是 $\mathbb{G}_T$ 中的一个随机群元素并输出 0。当 T 是一个元组, 模拟器 $\mathcal{S}$ 进行一个完美的仿真, 可得: $\Pr[\mathcal{S}(\vec{r}, T = e(g,g)^{\frac{1}{\alpha}}) = 1] = \frac{1}{2} + Adv_{\mathcal{A}}$。当 T 是 $\mathbb{G}_T$ 中的一个随机群元素, 敌手 $\mathcal{A}$ 获取不到任何有关于 M_b 的信息, 可得: $\Pr[\mathcal{S}(\vec{r}, T = R) = 1] = \frac{1}{2}$。

如果当敌手 $\mathcal{A}$ 能以不可忽略的优势攻破方案, 模拟器 $\mathcal{S}$ 就能以不可忽略的优势攻破弱 l-BDHI 假设。

表 2　安全模型比较

Table 2　The comparison of security model

方案	困难问题	模型	扩展外包解密
文献[7]BB	DBDH	Standard	—
文献[7]G	q-DABDHE	Standard	—
文献[10]	l-BDHI	Random Oracle	—
文献[13]	DBDH	Standard	—
本文方案	弱 l-BDHI	Random Oracle	√

安全模型比较如表 2 所示。本文方案的安全性证明依靠于随机预言机模型。方案在弱 l-BDHI 假设下是 IND-ID-CPA 安全的。随机预言机是一种启发式的证明模型, 该模型中的分析证明比其它模型更加有效, 并且在安全性方面也普遍被人们接受。在特定的情况下, 方案的效率比安全级别更为重要。因此, 本文的安全性证明使用了随机预言机模型。同时, 相比于其他方案, 本文所提出的方案还可支持云外包解密功能, 对于消息的接收方, 大部分的解密计算可以安全地外包给云完成。极大程度地减少了接收方解密的计算代价。

6.2　方案的效率分析

本节在存储开销和计算复杂度方面对所提方案进行了效率分析。在本方案的 *OnEncrypt* 算法中, 用户首先读取离线阶段时计算的离线密文 C_{off}, 然后再进行少量的计算便可完成用户的在线加密过程, 在此过程中, 并不涉及任何双线性对运算。相比于之前的 BF-IBE[2]方案, 本文方案明显降低用户的在线计算量。

E 表示在 $\mathbb{G}$ 或 $\mathbb{G}_T$ 中指数运算的时间, ME 表示在 $\mathbb{G}$ 中的多点乘运算时间, T_e 表示双线性对运算的时间, m_c 表示在 $\mathbb{Z}_p^*$ 中模运算的时间, M 表示在 $\mathbb{G}_T$ 中乘法运算的时间, SE 表示对称密钥加密的时间。n 表示信息空间大小, $\mathcal{S}$ 表示一个强签名[7], 以及 k 表示对称密钥加密 ε 的块大小[13]。本方案所构造的 IBOOE 系统在计算效率、存储开销以及通信代价方面与其他方案相比具有一定优势。

表 3　计算复杂度比较

Table 3　The comparison of computation complexity

方案	离线计算	在线计算
文献[7]BB	$T_e + 6E + 2ME + \mathcal{S}$	$M + 2m_c + \mathcal{S}$
文献[7]G	$4T_e + 4E + 2ME$	$M + 2m_c$
文献[10]	$T_e + 4E + ME$	$3m_c$
文献[13]	$T_e + 3E + 2ME$	$SE + 2m_c$
本文方案	$T_e + 4E$	$M + E$

表 3 在计算复杂度方面将本文方案与其他相关的 IBOOE 方案在离线计算量和在线计算量方面进行了比较。上述方案均在双线性乘法群中实现。通过对离线计算量的比较可得知, 本文所提出的方案在离线阶段时的计算量略低于上述方案, 均在设备可计算范畴内, 满足 IBOOE 方案算法的要求。再从在线阶段要求轻量计算的角度来看, 本文方案可以实现 IBOOE 方案算法的目标。在线阶段时, 本文方案的计算复杂度足够小, 可应用于许多低计算能力的电子设备, 如传感器或移动终端。同时, 本文将在线/离线技术应用到密钥生成算法, 通过这种方式, PKG 可以比其他现有的 IBOOE 方案更快速地生成用户私钥, 当用户数量较为庞大时, 可在一定程度上减轻 PKG 的计算压力。

存储开销比较如表 4 所示。在本文的 IBOOE 方案中, 消息发送方的离线存储开销表示为 C_{off}, PKG 所需离线存储开销表示为 K_{off}。方案中发送方和 PKG 的存储开销分别为 $|\mathbb{Z}_p^*|+3|\mathbb{G}|+|\mathbb{G}_T|$ 和 $2|\mathbb{Z}_p^*|+3|\mathbb{G}|$。就离线存储开销方面, 本文的方案展现出了很好的性能。尽管文献[13]的离线存储开销略低于本文方案, 但是其方案引入了对称密钥加密算法(例如: DES、3DES、IDEA、FEAL、BLOWFISH 等), 发送方与接收方必须都要获得密钥并保持密钥的安全, 这会产生用户密钥管理的问题。

表 4 存储开销比较

Table 4 The comparison of storage overhead

方案	离线存储	密文空间
文献[7]BB	$4\|\mathbb{Z}_p^*\|+\|\mathcal{S}\|+4\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$2\|\mathbb{Z}_p^*\|+2\|\mathcal{S}\|+4\|\mathbb{G}\|+\|\mathbb{G}_T\|$
文献[7]G	$4\|\mathbb{Z}_p^*\|+2\|\mathbb{G}\|+4\|\mathbb{G}_T\|$	$2\|\mathbb{Z}_p^*\|+\|\mathbb{G}\|+4\|\mathbb{G}_T\|$
文献[10]	$6\|\mathbb{Z}_p^*\|+4\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$3\|\mathbb{Z}_p^*\|+4\|\mathbb{G}\|+n$
文献[13]	$3\|\mathbb{Z}_p^*\|+4\|\mathbb{G}\|+k$	$2\|\mathbb{Z}_p^*\|+4\|\mathbb{G}\|+\|\varepsilon\|$
本文方案	$\|\mathbb{Z}_p^*\|+3\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$4\|\mathbb{G}\|+\|\mathbb{G}_T\|$

因为方案中发送方与接收方在信道传输的为密文 CT, 所以密文 CT 所占空间大小可以被看作用户之间的通信代价。因此, 本方案用户之间的通信代价为 $4|\mathbb{G}|+|\mathbb{G}_T|$。本方案密文 CT 所占空间更小, 这在一定程度上降低了传输密文时所需的通信代价(带宽)。

7 结束语

本文利用椭圆曲线上的双线性对构造了一个安全有效的基于身份的在线/离线加密方案。方案可扩展支持云外包解密, 并且应用可选择公用外包密钥生成中心, 使得用户也可根据对所属 PKG 的信任程度, 选择是否使用公用 OKG 来解决密钥托管问题而不需要 PKG 重新初始化。通过安全和效率分析, 与其他现有的 IBOOE 研究成果相比, 本文方案是安全和高效的。本文方案使用了椭圆曲线上的双线性对技术, 但是影响双线性对快速实现的因素有很多, 所以在提高方案的计算速度方面还有着很大的空间, 同时方案在安全性等方面也可继续提升。

致 谢 本文中方案的提出是在北京邮电大学网络技术研究院网络安全中心(国家重点实验室)的大力支持和帮助下完成的, 在此向该中心表示衷心的感谢。

参考文献

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," *Workshop on the Theory and Application of Cryptographic Techniques,* pp. 47-53, 1984.

[2] D. Boneh, and M. Franklin, "Identity-based encryption from the Weil pairing," in *Annual International Cryptology Conference (CRYPTO 2001),* pp. 213-229, 2001.

[3] R. Sakai, and M. Kasahara, "ID based Cryptosystems with Pairing on Elliptic Curve.," *IACR Cryptology ePrint Archive*, 2003.

[4] J. Baek, and Y. Zheng, "Identity-based threshold decryption," in *International Workshop on Public Key Cryptography (PKC 2004),* pp. 262-276, 2004.

[5] C. Gentry, and A. Silverberg, "Hierarchical ID-based cryptography," in *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2002),* pp. 548-566, 2002.

[6] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," *Journal of Cryptology*, vol. 9, no. 1, pp. 35-67, 1996.

[7] F. Guo, Y. Mu, and Z. Chen, "Identity-based online/offline encryption," in *International Conference on Financial Cryptography and Data Security (FC 2008),* pp. 247-261, 2008.

[8] D. Boneh, and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2004),* pp. 223-238, 2004.

[9] C. Gentry, "Practical identity-based encryption without random oracles," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2006),* pp. 445-464, 2006.

[10] J. K. Liu, and J. Zhou, "An efficient identity-based online/offline encryption scheme," in *International Conference on Applied Cryptography and Network Security (ACNS 2009),* pp. 156-167, 2009.

[11] S. S. D. Selvi, S. S. Vivek, and C. P. Rangan, "Identity Based Online/Offline Signcryption Scheme," *IACR Cryptology ePrint Archive*, 2010.

[12] S. S. D. Selvi, S. S. Vivek, and C. P. Rangan, "Identity based online/offline encryption and signcryption schemes revisited," in *Secu-*

rity Aspects in Information Technology (InfoSecHiComNet 2011), pp. 111-127, 2011.

[13] C. K. Chu, J. K. Liu, J. Zhou, F. Bao, and R. H. Deng, "Practical ID-based encryption for wireless sensor network," in *Proc. 5th ACM Symposium on Information, Computer and Communications Security (ACM 2010),* pp. 337-340, 2010.

[14] F. Yan, X. Chen, and Y. Zhang, "Efficient online/offline signcryption without key exposure," I*nternational Journal of Grid and Utility Computing*, vol. 4, no. 1, pp. 85-93, 2013.

[15] J. Li, J. Zhao, and Y. Zhang, "Certificateless online/offline signcryption scheme," *Security and Communication Networks*, vol. 8, no. 11, pp. 1979-1990, 2015.

[16] G. Wang, J. Wang, and Z. Guo, "Online/Offline Self-Updating Encryption," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. 99, no. 12, pp. 2517-2526, 2016.

[17] F. Guo, Y. Mu, W. Susilo, et al, "Optimized identity-based encryption from bilinear pairing for lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 211-220, 2017.

[18] J. Lai, Y. Mu, and F. Guo, "Efficient identity-based online/offline encryption and signcryption with short ciphertext," *International Journal of Information Security*, vol. 16, no. 3, pp. 299-311, 2017.

[19] B. Waters, "Efficient identity-based encryption without random oracles," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005),* pp. 114-127, 2005.

[20] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Lecture Notes in Computer Science,* vol. 2260, pp. 360-363, 2001.

[21] D. Boneh, C. Gentry, and M. Hamburg, "Space-efficient identity based encryption without pairings," in *Foundations of Computer Science (FOCS 2007),* pp. 647-657, 2007.

[22] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. Fortieth Annual ACM Symposium on Theory of Computing (ACM 2008),* pp. 197-206, 2008.

[23] B. Waters, "Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions," in *29th Annual International Cryptology Conference (CRYPTO 2009),* pp. 619-636, 2009.

[24] A. B. Lewko, and B. Waters, "New techniques for dual system encryption and fully secure hibe with short ciphertexts," in *Seventh Theory of Cryptography Conference (TCC 2010),* vol. 5978, pp. 455-479, 2010.

[25] C. I. Fan, L. Y. Huang, and P. H. Ho, "Anonymous multireceiver identity-based encryption," *IEEE Transactions on Computers,* vol. 59, no. 9, pp. 1239-1249, 2010.

[26] L. Chen, and Z. Cheng, "Security proof of sakai-kasahara's identity-based encryption scheme," *IACR Cryptology ePrint Archive,* 2005.

[27] K. G. Paterson, and S. Srinivasan, "On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups," *Designs, Codes and Cryptography,* vol. 52, no. 2, pp. 219-241, 2009.

[28] E. Barker, W. Barker, W. Burr, et al, "Recommendation for key management part 1: General (revision 3)," *NIST special publication,* vol. 800, no. 57, pp. 1-147, 2012.

[29] L. Kwangsu, L. D. Hoon, and P. H. Jong, "Efficient revocable identity-based encryption via subset difference methods," *Designs, Codes and Cryptography,* vol. 85, no. 1, pp. 39-76, 2017.

[30] J. Lai, Y. Mu, F. Guo, and W. Susilo, "Improved identity-based online/offline encryption," in *Australasian Conference on Information Security and Privacy (ACISP),* pp. 160-173, 2015.

何能强 于 2012 年在清华大学信息与通信工程专业获得博士学位。现任国家计算机网络应急技术处理协调中心高级工程师、中国互联网协会网络与信息安全工作委员会副秘书长。研究领域为移动互联网安全，研究兴趣包括移动互联网恶意程序分类识别技术、移动互联网应用程序安全检测技术等。Email: hnq@cert.org.cn

张华 于 2008 年在北京邮电大学密码学专业获得博士学位。现任北京邮电大学副教授。研究领域为网络安全、密码协议。研究兴趣包括：安全数据外包。大数据分析。Email: zhanghua_288@bupt.edu.cn

李叶 于 2015 年在北京邮电大学与伦敦大学玛丽女王学院电信工程及管理专业获得学士学位。现在北京邮电大学计算机科学与技术专业攻读硕士学位。研究领域为信息安全。研究兴趣包括：公钥密码学。Email: samliye@bupt.edu.cn