基于身份加密的装备密钥分布式生成算法

王 宏[1,2] 李建华[1] 崔 琼[1]
(空军工程大学信息与导航学院 西安 710077)[1] (西安通信学院 西安 710106)[2]

摘 要 为解决身份加密体制中单一密钥生成中心易遭受攻击的问题,借鉴网络中心战"去中心化"的思想,针对 Lewko-Waters 身份加密协议,提出了一种分布式密钥生成算法。在算法中,主密钥由密钥生成中心和密钥隐私中心共同掌握,用户密钥在密钥生成中心监管下由分布于网络中的各密钥隐私中心共同生成,有利于增强 Lewko-Waters 协议密钥管理体系的抗毁性、鲁棒性。最后,在标准模型中证明了该方案在选择明文攻击下的密文不可区分性,并进行了算法性能比较分析。

关键词 身份加密,分布式,密钥生成
中图法分类号 TP309 **文献标识码** A

Military Equipment's Distributed Key-generating Algorithm for Identity-based Cryptography

WANG Hong[1,2] LI Jian-hua[1] CUI Qiong[1]
(School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China)[1]
(Xi'an Communications Institute, Xi'an 710106, China)[2]

Abstract According to the decentralization theory of network central warfare, we proposed a distributed private-key extraction algorithm for Lewko-Waters's identity-based encryption because the sole key generating center of identity-based encryption is likely attacked. In this scheme, master key is in charge of both key generating center and key privacy authority. User's private key can be extracted and supervised by key generating center from a number of key privacy authorities distributing all over the network. It could be available to strengthen the survivability and robustness of key management system. Finally we proved their IND-CPA security, i. e. the indistinguishability of ciphertext under chosen plaintext attack, in the normal model and also performed a comparative analysis of the algorithm. As you can see, it can be helpful to accomplish key escrow.

Keywords Identity-based encryption, Distributed key extraction, Key escrow

1 引言

身份加密体制[1](Identity-Based Encryption, IBE)是将用户身份(如身份证号码、驾驶证号码等)直接作为用户公钥,不采用数字证书管理密钥,避免了管理大量的数字证书带来的弊端。IBE 体制中,密钥生成中心(Key Generation Center, KGC)利用公共参数和系统主密钥为用户生成私钥,KGC 掌握所有用户私钥,能够解密所有密文,这成为 IBE 体制中最重要的隐患。为此,最早提出的解决方案是使用门限秘密共享将主密钥分布在多个 KGC 之中,由多个 KGC 共同为用户颁发私钥[2-4],但这种方法会在主密钥秘密门限共享阶段产生大量额外通信开销;Gentry 提出的基于证书加密[5]和 Al-Riyami 等人提出的无证书加密[6]中,用户结合 KGC 的部分私钥选取随机数,生成自己的秘密私钥,避免 KGC 知道用户全部私钥,但用户的公钥已不再是公开的标识自己身份的信息,实际上已经失去身份加密的主要特征;2004 年 Lee 等人[6]提出一个将主密钥分布在 KGC 和密钥隐私中心(Key Privacy Authority, KPA)的密钥生成方案,Gangishetti 等[7]于 2007 年改进该方案,但是 Xu 等[8]指出该方案中存在 KGC 欺骗 KPA 获取用户私钥的可能性;2010 年,Kate 和 Goldberg[9]提出的方案通信复杂度较高,误码率高,无法推广使用;2012 年,郝云芳等[10]针对 Boneh-Boyen1 的 IBE 提出一种安全密钥分发方案,并且证明基于 CDH(Computational Diffie-Hellman)假设条件的安全性,但其并不能广泛推广其它 IBE 体制;2015 年,任艳丽等[11]提出了基于 LW-IBE 体制私钥外包计算协议,将私钥生成外包给不安全服务器,在标准模型下证明了方案的密文不可区分性和外包结果的可验证性,但并未做到 KGC 的"去中心化"。

美军提出的网络中心战,强调作战中心由平台转向网络,将中心虚拟化、隐藏化处理[13]。分布式密钥生成有利于增强密钥的管理保护,适应当前信息化战争"去中心化"的趋势。本文基于 Lewko-Waters 的身份加密体制,提出了包含一个 KGC 和多个 KPA 的密钥分布生成算法,而且 KGC 和 KPA 的角色并未固定到网络节点,可以根据作战需求选择任何节

本文受国家自然科学基金(61401499)资助。
王 宏(1979-),男,博士生,讲师,主要研究方向为装备作战使用与保障,E-mail:whongger2006@sina.com;李建华(1965-),男,博士,教授,主要研究方向为装备作战使用与保障、空天信息系统建设与运用;崔 琼(1990-),女,博士生,主要研究方向为网络化指挥信息系统作战应用。

点充当，使得重要网络节点隐藏化，有效降低了关键网络节点的风险性。

2 算法基础

2.1 合数阶群间的双线性映射

设 p_1, p_2, p_3 为素数，$N=p_1p_2p_3$，G 和 G' 为两个阶为 N 的循环群。映射 $e: G\times G\to G'$，如果满足下列条件，称之为双线性映射[11]。

(1)双线性：对于任意 $u, v\in G, \alpha, \beta\in Z_N$，$e(u^\alpha, v^\beta)=e(u, v)^{\alpha\beta}$；

(2)非退化性：存在 G 的生成元为 g，使得 $e(g,g)$ 为 G' 的生成元；

(3)计算可行性：对于任意 $u, v\in G$，存在 PPT(Probable Polynomial Time)算法计算 $e(u,v)$。

2.2 困难性假设

DBDH(Decisional Bilinear Diffie-Hellman)假设：随机选择 $a, b, c, z, \in Z_p$，p 是群 G 的阶，g 是 G 的生成元，攻击者能够区分五元组 (g, g^a, g^b, g^c, g^z) 和 $(g, g^a, g^b, g^c, g^{abc})$ 的概率很小，可以忽略不计。

2.3 安全模型

本文方案可达到选择明文攻击下的密文不可区分性(Indistinguishability of Ciphertextunder Chosen Plaintext Attack，IND-CPA)，通过挑战者和攻击者的如下交互游戏定义 IND-CPA。

定义 1[2] 对于一个身份加密方案，如果不存在攻击者能以不可忽略的优势在下面的交互游戏中在多项式时间内赢得挑战者，则称此方案具有抗选择明文攻击的密文不可区分性，是语义安全的。攻击者 A 和挑战者 C 之间进行下面的游戏：

(1)Setup：

挑战者 C 输入安全参数，运行初始算法，将系统参数 params 发送给攻击者 A。

(2)Phase1：

攻击者 A 执行多项式次数的适应性询问，即每次询问可以依赖于以前询问的结果，这些询问包括：

Extract 询问：A 选择一个身份 u，C 计算相应身份的私钥 $d_u=\text{Extract}(u)$，并将结果发送给 A。

Decrypt 询问：A 选择一个身份 u 和一个密文 σ。C 首先计算 $d_u=\text{Extract}(u)$，然后计算 $\text{Decrypt}(\sigma, d_u)$，最后返回明文 M 或符号“⊥”(表示解密失败)。

(3)Challenge 阶段：

A 决定结束第一阶段的询问，生成两个相同长度的明文 M_0, M_1 和希望挑战的身份 u^*，其中 u^* 不能是已经执行过 Extract 询问的身份。C 随机选择 $r\in\{0,1\}$，计算 $\sigma^*=Encrypt(M_r, u^*)$，并将结果发送给 A。

(4)Phase2：

A 像在 Phase1 那样执行多项式有限次询问，但是不能对 u^* 执行 Extract 询问，也不能对密文 u^* 执行 Decrypt 询问。

(5)Guess：

A 输出一个值 γ' 作为对 γ 的猜测。如果 $\gamma'=\gamma$，则 A 赢得游戏。

A 赢得挑战的优势定义为 $\text{Advantage}(A)=|P\{\gamma=\gamma'\}-12$。

3 基于 IBE 体制的密钥生成算法

首先回顾 LW-IBE 方案[12]，而后基于多密钥生成中心提出 Lewko-Waters 身份加密体制的密钥生成方案。

3.1 Lewko-Waters 身份加密体制

Setup(λ)：KGC 选择阶为 $N=p_1p_2p_3$ 的双线性群 G，其中 $p_1p_2p_3$ 为大素数。令 G_{p_i} 表示阶为 p_i 的 G 的子群，$i\in\{1,2,3\}$。KGC 选择 $g, u, h\in G_{p_1}$，$\alpha\in Z_n$，则公共参数 $PK=\{g, u, h, e(g,g)^\alpha\}$，KGC 私钥为 $\alpha\in Z_N$ 及 G_{p_3} 的生成元。

KeyGen(MK, ID, PK)：对于身份 $ID\in Z_N$，KGC 随机选择 $r_{ID}\in Z_N$，$R_{11}, R_{12}\in G_{p_3}$，计算 $K_1=g^{r_{ID}}R_{11}$，$K_2=g^\alpha(u^{ID}h)^{r_{ID}}R_{12}$，则身份 ID 对应私钥 $SK_{ID}=(K_1, K_2)$。

Encrypt(M, ID, PK)：对于消息 $M\in G'$，身份 ID，随机选择 $s\in Z_N$，计算 $C_0=Me(g,g)^{\alpha s}$，$C_1=(u^{ID}h)^s$，$C_2=g^s$。最终对应密文 $CT=(C_0, C_1, C_2)$。

Decrypt($CT, SKID, Pk$)：输入 CT，身份 ID，私钥 $SKID$，解密密文如下：

$$\frac{C_0e(C_1,K_1)}{e(C_2,K_2)}=Me(g,g)^{\alpha s}\frac{e((u^{ID}h)^s, g^{r_{ID}}R_{11})}{e(g^s, g^\alpha(u^{ID}h)^{r_{ID}}R_{12})}$$

$$=\frac{Me(g,g)^{\alpha s}}{e(g^s,g^\alpha)}=M$$

3.2 基于 IBE 体制的分布式密钥生成算法

Setup：

(1)杂凑函数 $G: \{0,1\}^*\to F_{p_1}$

KGC 随机选择 $\gamma, \alpha_0\in Z_N$，计算 g^{α_i}，令 $G_\gamma=g^\gamma$，$Q_0=G(ID_{\text{KGC}})$，公共参数 $\text{Params}: \{N, g, u, h, G_\gamma, e(g,g)^{\alpha_0}\}$；

(2)每个 KPA_i 随机选择 k_i, α_i，其中 $i=1,2,\cdots,n$，计算 g^{α_i}，令 $G_{k_i}=g^{k_i}$，$Q_i=G(ID_{KPA_i})$，公开 G_{k_i}；

(3)KGC 计算并发送 $G_{k_i}^\gamma$ 给 KPA_i，KPA_i 验证 $G_{k_i}^\gamma=G_\gamma^{k_i}\pmod{p_1}$，若成立，$KPA_i$ 向 KGC 发送 $(g^{\alpha_i}, G_\gamma^{k_i})$，否则终止运算；

(4)KGC 验证 $G_\gamma^{k_i}=G_{k_i}^\gamma\pmod{p_1}$，若成立，令 $g^\alpha=\prod_{i=0}^{n}g^{\alpha_i\prod_{j\neq i}\frac{-Q_i}{Q_j-Q_i}}$。

KeyGen：

对于身份 $ID\in Z_N$，KGC 随机选择 $r_{ID}\in Z_N$，$R_{11}, R_{12}\in G_{p_3}$，计算 $K_1=g^{r_{ID}}R_{11}$，$K_2=g^\alpha(u^{ID}h)^{r_{ID}}R_{12}$，则身份 ID 对应私钥 $SK_{ID}=(K_1, K_2)$。

其余 Encrypt 和 Decrypt 算法同 Lewko-Waters 身份加密方案。

4 基于 IBE 体制的密钥生成算法分析

首先基于 DBDH 问题证明本文方案的安全性，而后对方案的计算开销进行分析。

4.1 安全性证明

定理 1 假设 DBDH 困难问题没能被攻破，则本文方案完全安全。

证明：定理可以描述如下。

如果攻击者 A 能够攻破本文方案，则模拟器 B 能以不可忽视的概率进行判定 DBDH 游戏。采用反证法，假设攻击者 A 在选择明文安全模式下能以概率 ε 区分 IBE-KE 方案的密文，则可以构造模拟器以优势 $\frac{\varepsilon}{2}$ 进行判定 BDH 游戏。

令 C 代表挑战者，A,B,C 进行判定 BDH 游戏。挑战者 C 随机选择 $\mu\in\{0,1\}$，若 $\mu=0$，则设置 $(A,B,Z)=(g^a,g^b,e(g,g)^{ab})$；若 $\mu=1$，则设置 $(A,B,Z)=(g^a,g^b,e(g,g)^z)$，其中 $(a,b,c)\in Z_{p_1}$。

Setup：模拟器 B 设置公共参数 $PK=\{g,u,h,e(g,g)^\alpha\}$，并且将公共参数发送给攻击者 A。

Phase1：攻击者挑选身份信息 $ID_1,\cdots,ID_m$，进行询问，模拟器运行 KeyGen，发送有关 KGC 和每个 KPA_i 结果，最终生成私钥 $K_1=g^{r_{ID}}R_{11}$，$K_2=g^\alpha(u^{ID}h)^{r_{ID}}R_{12}$，发送给攻击者 A。

Challenge：攻击者 A 认为询问结束后，挑选两个长度相等的明文 M_0，M_1 和 ID^*，其中 ID^* 不能是 $ID_1,\cdots,ID_m$ 中的元素，然后将发送给模拟器 M_0，M_1 和 ID^*，模拟器随机选择 $\tau\in\{0,1\}$，使用 ID^* 加密 M_τ，并发送给攻击者 A，密文为：

$$CT=(C_0,C_1,C_2),C_0=M_\tau Z,C_1=(u^{ID}h)^{\frac{ab}{\alpha}},C_2=g^{\frac{ab}{\alpha}}$$

由于攻击者 A 并不知道 α，因此无法区分 $\frac{ab}{\alpha}$ 和 α，故模拟器 B 很好地扮演了挑战者的角色。

当 $\mu=0$ 时，$C_0=M_\tau Z=M_\tau e(g,g)^{ab}=M_\tau e(g,g)^{\alpha\frac{ab}{\alpha}}$，$C_1=(u^{ID}h)^{\frac{ab}{\alpha}}$，$C_2=g^{\frac{ab}{\alpha}}$，则 CT 是在公钥 ID 和随机参数 $\frac{ab}{\alpha}$ 加密的密文；当 $\mu=1$ 时，$C_0=M_\tau Z=M_\tau e(g,g)^c$，$C_1=(u^{ID}h)^{\frac{ab}{\alpha}}$，$C_2=g^{\frac{ab}{\alpha}}$，$C_0$ 完全是一个随机数，攻击者通过询问不能得到任何有关 M_τ 的信息。

Phase2：攻击者挑选身份信息 $ID_{m+1},\cdots,ID_n$ 进行询问，但是 ID^* 不能在其中，模拟器运行 KeyGen，发送有关 KGC 和每个 KPA_i 结果，最终生成私钥 $K_1=g^{r_{ID}}R_{11}$，$K_2=g^\alpha(u^{ID}h)^{r_{ID}}R_{12}$，发送给攻击者 A。

Guess：攻击者 A 猜测 τ'，如果 $\tau'=\tau$，模拟器 B 回答 $\mu'=0$，表示 (A,B,Z) 为 $(g^a,g^b,e(g,g)^{ab})$；如果 $\tau'\neq\tau$，模拟器 B 回答 $\mu'=1$，表示 (A,B,Z) 为 3 个随机数。

下面分析当 A 攻击成功时，B 成功的概率。

当 $u=1$ 时，攻击者 A 无法获取任何有关 τ 的信息，$P\{\tau'\neq\tau|\mu=1\}=\frac{1}{2}$，即 $P\{\mu'=\mu|\mu=1\}=\frac{1}{2}$；当 $\mu=0$ 时，根据题设条件，攻击者 A 获取任何有关 τ 的信息的概率为 ε，$P\{\tau'=\tau|\mu=0\}=\frac{1}{2}+\varepsilon$，即 $P\{\mu'=\mu|\mu=0\}=\frac{1}{2}+\varepsilon$。

根据全概率公式可得模拟器 B 在判定 BDH 游戏中的猜中的概率为：

$$P\{\mu'=\mu\}=\frac{1}{2}P\{\mu'=\mu|\mu=1\}+\frac{1}{2}P\{\mu'=\mu|\mu=0\}=\frac{1}{2}+\frac{\varepsilon}{2}$$

故模拟器能以优势 $|P\{\mu'=\mu\}-\frac{1}{2}|=\frac{\varepsilon}{2}$ 完成判定 BDH 问题。

4.2 性能分析

计算量是衡量算法优劣性的重要标准，本文方案增加 n 个 PKA 以增强密钥生成的安全性，在表 1 中对直接生成密钥方案和本文方案的计算量进行了比较，其中“n”表示密钥用户数。由表 1 可以看出，如果 KGC 直接为用户生成密钥，可以先对 g^α 进行预计算，再执行 1 次双线性对运算、$2n$ 次模指数运算和 $3n$ 次模乘运算，即可生成用户密钥。如果采用本方案，KGC 的计算量仅仅增加了 1 次拉格朗日插值运算，其它 $PKA_i(i=1,2,\cdots,n)$ 需要预计算 1 次模指数运算和 n 次模指数验证，而且 KGC 和 KPA 可以并行执行运算，因而对于 KGC 来说直接生成密钥和结合 KPA 生成密钥计算量差别很小，便可以解决密钥的托管问题。

表 1 密钥生成方案计算性能比较

	KGC 直接计算私钥	本文方案			
		KGC	PKA_1	…	PKA_n
预计算	m	m	1	…	1
双线性对运算	1	1	0	…	0
模指数	2m	2m	m	…	m
模乘	3m	3m	0	…	0
插值运算	0	1	0	…	0

4.3 仿真分析

利用 CPU 为 Intel Xeon E5-2600（频率最高 2.9GHz）、内存为 128GB 的服务器配置虚拟机。群 G 和 G' 的阶 N 取 480bit，其中分别取 p_1，p_2，p_3 分别取 160bit。当密钥用户数 $m=1000$ 时，配置 1 个 KGC 和 n 个 KPA（$n=1,2,\cdots,10$），KPA 数量和运行时间关系曲线如图 1 所示，当 $n=4$ 时密钥生成所需时间为 105s，系统运行开销最少。实际上 KGC 和 KPA 在工作时，虽然采用并行运算，但随着 KPA 个数的增多，KGC 等待从各个 KPA 发送来密钥碎片的时间就会增加，因而造成时间运行曲线出现拐点（4105），故在密钥生成阶段可以采用 1 个 KGC 配置 4 个 KPA 的最优组合。如图 2 所示，当 KPA 的个数 $n=4$ 时，直接利用 KGC 生成密钥所需时间和采用 KGC+KPA 生成时间基本相当，实际分布式生成密钥仅比直接生成密钥多 1 次插值运算，以较小的运算代价实现了密钥的安全分布式生成。

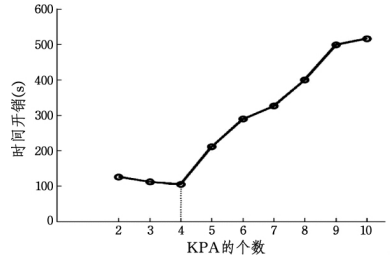

图 1 $m=1000$ 时 KPA 数量和运行时间关系曲线

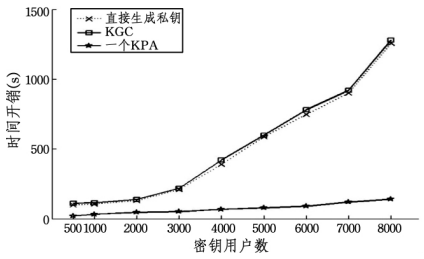

图 2 $n=4$ 时密钥用户数量和运行时间关系曲线

结束语 现代战争中，信息化装备不能脱离密钥保护，密钥管理显得越来越重要，密钥的生成亦至关重要。本文基于身份加密体制，借鉴网络中心战思想，采用“KGC+PKA”结构生成用户密钥。多个 KPA、一个 KGC 的密钥生成模式，即将部分运算外包给多个 KPA，降低了 KGC 的计算开销，提高

（下转第 397 页）

传感器节点发送的感知数据也逐渐增多，导致3种方案中的传感器节点能耗也随之增多。其中SafeQ的能量消耗最大，EPRQ的能量消耗最小，这是因为传感器节点发送的前缀编码数据量要比0-1编码机制产生的数据量更大。然而，在PIRQ方案中，传感器节点不需要发送所有的感知数据给存储节点，降低了能耗开销，但由于加入了完整性保护机制，因此在能耗方面会比EPRQ大一点。

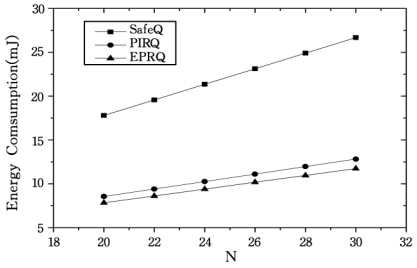

图5　N对感知节点的能量消耗影响

结束语　本文提出了一种能量高效的安全范围查询方法PIRQ。与SafeQ和EPRQ方案相比，PIRQ具有更好的安全性和节能性，但由于引入了完整性保护机制，在能量消耗方面仍然相对较高，在未来仍有不小的改进空间。

参 考 文 献

[1] Gnawali O, Jang K Y, Paek J, et al. The tenet architecture for tiered sensor networks[C]// Proceedings of the 4th International Conference on Embedded Networked Sensor Systems. ACM, 2006:153-166

[2] Ratnasamy S, Karp B, Shenker S, et al. Data-centric storage in sensornets with GHT, a geographic hash table[J]. Mobile Networks and Applications, 2003, 8(4):427-442

[3] Sheng B, Li Q. Verifiable privacy-preserving range query in two-tiered sensor networks[C]// The 27th Conference on Computer Communications(INFOCOM 2008). IEEE, 2008

[4] Chen F, Liu A X. SafeQ: Secure and efficient query processing in sensor networks[C]//2010 Proceedings IEEE INFOCOM. IEEE, 2010:1-9

[5] Chen F, Liu A X. Privacy-and integrity-preserving range queries in sensor networks[J]. IEEE/ACM Transactions on Networking, 2012, 20(6):1774-1787

[6] 戴华，杨庚，肖甫，等. 两层传感网中能量高效的隐私保护范围查询方法[J]. 计算机研究与发展，2015，52(4)：983-993

[7] 窦轶，黄海平，王汝传，等. 两层无线传感器网络安全范围查询协议[J]. 计算机研究与发展，2013，50(6)：1253-1266

[8] 周强，杨庚，李森，等. 一种可检测数据完整性的隐私数据融合算法[J]. 电子与信息学报，2013，35(6)：1277-1283

[9] Groat M M, He W, Forrest S. KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks[C]// 2011 Proceedings IEEE INFOCOM. IEEE, 2011:2024-2032

[10] Rivest R. RFC1321, The MD5 message-digest algorithm request for comments[S]. Cambridge: MIT and RSA Data Security, 1992

[11] Rappaport T S. Wireless communications: principles and practice [M]. New Jersey: Prentice Hall PTR, 1996

[12] 武佩宁. 两层无线传感器网络中安全数据查询协议的研究[D]. 南宁：广西大学，2014

[13] Coman A, Nascimento M A, Sander J. A framework for spatio-temporal query processing over wireless sensor networks[C]// Proceeedings of the 1st International Workshop on Data Management for Sensor Networks: in Conjunction with VLDB 2004. ACM, 2004:104-110

(上接第357页)

了运算效率，又避免了单个KGC被摧毁的风险性，符合联合作战的、以网络为中心的、分布力量结构柔性重组的作战思想，进一步增强了信息装备网络的抗毁性，为后续保密装备网络体系构建奠定了基础。

参 考 文 献

[1] Shamir A. Identity-Based cryptosystems and signature schemes [C]// Advances in Cryptology-CRYPTO'84. Berlin, Heidelberg: Springer-Verlag, 1984:47-53

[2] Boneh D, Franklin M K. Identity-based encryption from the Weilpairing[C]// Proceedings of the 21st Annual International Cryptology Conference onAdvances in Cryptology. LNCS 2139. Berlin, Heidelberg: Springer-Verlag, 2001:213-229

[3] Chen L, Harison K, Soldera D, et al. Applications of multiple trust authorities in pairing based cryptosystems[C]// Proc of the International Conference on Infrastructure Security 2002. Berlin Springer, 2002:260-275

[4] Goldberg K I. A distributed private-key generator for identity-based cryptography[R]. University of Waterloo, 2007

[5] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]// Proc of the 9th International Conference on the Theory and Application of Cryptography and Information Security. Berlin: Springer 2003:452-473

[6] Lee B, Boyd C, Dawson E, et al. Secure key issuing in id-based cryptography[C]// Proc of the 2nd Australasian Information Security Workshop. Austrlia: CRPIT, 2004:251-230

[7] Gangishetti R, Gorantla M C, Das M, et al. Threshold key issuing in identity-based cryptosystems[J]. Computer Standards & Interfaces, 2007, 29(2):260-264

[8] X Chun-xiang, Z Jun-hui, Q Zhi-guang. A Note on Secure Key Issuing in ID-based Cryprography[EB/OL]. http://eprint.iacr.org/2005/180

[9] Kate A, Goldberg I. Asynchronous Distributed Private-Key Generators for Identity-Based Cryptography [EB/OL]. http://eprint.iacr.org/2009/355

[10] 郝云芳，吴静，王立炜. Boneh-Boyen1基于身份加密体制的安全密钥分发[J]. 计算机科学，2012，39(6A)：35-37

[11] 任艳丽，蔡建兴，黄春水，等. 基于身份加密中可验证的私钥生成外包算法[J]. 通信学报，2015，36(11)：1-6

[12] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertext[C]// Micciancio D. ed., Theory of Cryptography, Theory of Cryptography(TCC). LNCS 5978. Zurich, Switzerland: Springer, 2010:455-475

[13] 潘清. 网络中心战装备体系[M]. 北京：国防工业出版社，2010：5-10