Boneh-Boyen$_1$ 基于身份加密体制的安全密钥分发

郝云芳[1] 吴 静[1] 王立炜[2]

(西安培华学院电气信息工程学院 西安 710065)[1] (西安邮电学院电子工程学院 西安 710121)[2]

摘 要 为了提高基于身份加密体制的用户密钥安全性,解决基于身份加密体制中的密钥托管问题成为一个重要课题。提出了一种针对 Boneh-Boyen$_1$ 基于身份加密体制的安全密钥分发方案,方案中系统的主密钥分片分别保存于一个密钥生成中心和多个密钥隐私中心处,用户的私钥生成需要用户收到密钥生成中心和密钥隐私中心发来的多个私钥分片,以避免密钥生成中心获取用户的私钥。在标准模型中证明了密钥分发方案能够保证密钥生成中心无法获取用户的私钥,能够有效解决 Boneh-Boyen$_1$ 基于身份加密方案的密钥托管问题。

关键词 基于身份密码学,密钥托管,安全密钥分发,密钥生成中心,双线性对

中图法分类号 TP309 **文献标识码** A

Secure Key Issuing for Boneh-Boyen$_1$ Identity-based Encryption

HAO Yun-fang[1] WU Jing[1] WANG Li-wei[2]

(Electrical of Information Engineering Institute, Xi'an Peihua University, Xi'an 710065, China)[1]

(School of Electronic Engineering, Xi'an University of Post and Telecommunication, Xi'an 710121, China)[2]

Abstract By making use of user's identity as his public key, identity based cryptosystems have many advantages over traditional PKI based cryptosystems. But identity based cryptosystems also have an inherent drawback of key escrow that the key generation center knows all private keys of users. To improve the security of keys in identity based encryption, how to avoid key escrow problem in identity based encryption becomes a hot issue. A secure key issuing scheme for Boneh-Boyen$_1$ identity based encryption was proposed, in which multiple key privacy authorities are set in addition to the key generation center to protect the privacy of users' private keys. A rigorous security proof in standard model of our secure key issuing protocol was also given. Thus identity based encryption is more usable in practice.

Keywords Identity based cryptography, Key escrow, Secure key issuing, Key generation center, Bilinear pairings

1 引言

基于身份加密(identity based encryption, IBE)体制中,用户使用任意可代表他的公开信息作为公钥,例如他的 email 地址或身份标识,同时密钥生成中心(key generation center, KGC)持有主密钥并为用户生成私钥,因此无需传统公钥加密体制的公钥证书管理,大大提高了效率。由于用户私钥由 KGC 生成,IBE 体制存在一个重大缺陷,就是密钥托管(key escrow)问题,即 KGC 知道所有用户的私钥,因而可以解密系统中任何用户的密文。

为了解决 IBE 体制的密钥托管问题,国内外学者已做了大量研究工作,提出了许多密钥分发方法。最早提出的方法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 同时为用户颁发私钥[1-3],但这种方法会在主密钥秘密共享阶段产生大量额外通信开销,同时每个 KGC 均需验证用户身份,这也需要很大的计算量。Gentry 提出的基于证书加密[4]和 Al-Riyami 等人提出的无证书加密[5]则从另外一个角度解决密钥托管问题:用户选取一个随机秘密值,KGC 为用户生成部分私钥,用户的完整私钥由该部分私钥和自己选取的秘密值生成,从而避免了 KGC 知道用户私钥。用户的公钥是根据系统参数和自己选定的秘密值进行运算生成的,不再是标识用户身份的任意公开信息,实际上这两种方案已经丧失了基于身份密码体制的优点。

2004 年 B. Lee 等人[6]将系统主密钥分布在一个 KGC 和多个密钥隐私中心(key privacy authority, KPA),为了生成私钥,用户需要依次从 KGC 和多个 KPA 处获取部分私钥。2007 年,Gangishetti 等人[7]改进该方案,使用门限方式分布主密钥。但是,Xu Chunxiang 等人[8]指出该方案中存在一个缺陷,即恶意的 KGC 可以欺骗 KPA,仍然具有获取用户私钥的能力。2010 年,B. Lee 进一步对该方案进行改进[9],亦即将证书中心(certificate authority, CA)和 KGC 绑定在一个实体上,以同时提供基于证书和基于身份的加密服务。然而,文献[6,7,9]方案在实际应用中有一个很大的限制:只能应用于全域哈希(full domain hash)[10]的 IBE。在全域哈希的 IBE 中,加、解密均需要将用户的身份标识映射到椭圆曲线上的点,这种映射需要大量的计算并且对椭圆曲线的选取有严格的限定[10],而仅需将用户的身份标识映射为一个整数的非全域哈希 IBE 方案能够提供更高的计算效率,适用范围更广[11,12]。

郝云芳(1952—),女,副教授,主要研究方向为通信电子系统、信息安全,E-mail:haoyunfang_xupt@126.com;吴 静 女,主要研究方向为通信与电子系统;王立炜 男,主要研究方向为计算机网络信息安全。

2010年，Goldberg 和 Katz[13] 提出基于知识的非交互式证明和分布式密钥生成(distributed key generation，DKG)协议的安全密钥分发方法并给出了严格的安全性证明。但DKG协议的使用使得这种方法的通信复杂度极高，在通信量要求严格或误码率较高、通信时延大的场合中无法有效应用。

本文采用单KGC和多KPA的思想，为一种非全域哈希IBE——Boneh-Boyen$_1$ IBE[14]设计了一个密钥安全分发方案，并在标准模型中证明了方案能够有效解决Boneh-Boyen$_1$ IBE中的密钥托管问题。同时，方案具有较低的计算量和通信量，适用于各种应用场景。

2 预备知识

本节介绍本方案需要用到的基本概念和预备知识。本节中均假定 q 为一个大素数，G_1 为一个 q 阶加法循环群，G_2 为一个 q 阶乘法循环群。

2.1 双线性映射

具有以下性质的映射 $e:G_1\times G_1\to G_2$ 称为双线性映射：

(1)双线性性。对于任意的 $P,Q,R\in G_1$，有 $e(P+Q,R)=e(P,R)e(Q,R)$，$e(P,Q+R)=e(P,Q)e(P,R)$。

(2)非退化性。存在 $P,Q\in G_1$，使得 $e(P,Q)\neq 1$。

(3)可计算性。对于任意的 $P,Q\in G_1$，存在有效的算法来计算 $e(P,Q)$ 的值。

2.2 计算 Diffie-Hellman 假定和判定双线性 Diffie-Hellman 假定

计算 Diffie-Hellman(computational Diffie-Hellman，CDH)假定是指：对于任意的 $P\in G_1$ 和任意的 $a,b\in Z_q^*$，给定三元组 (P,aP,bP)，任意概率多项式时间(probabilistic polynomial-time，PPT)算法计算出 abP 的概率可忽略。

判定双线性 Diffie-Hellman(decisional bilinear Diffie-Hellman，DBDH)假定是指：对于任意的 $P\in G_1$，和任意的 $a,b,c\in Z_q^*$，$E\in G_1$，给定五元组 (P,aP,bP,cP,E)，任意 PPT 算法能成功判定 $E=e(P,P)^{abc}$ 是否成立的概率可忽略。

2.3 Boneh-Boyen$_1$ IBE 方案

Boneh-Boyen$_1$ IBE 的详情可以参考文献[14]，这里仅给出概述。Boneh-Boyen$_1$ IBE 由以下4个算法组成：

(1)setup 算法。KGC 选定一个 q 阶加法循环群 G_1，其生成元为 $P\in G_1$、一个 q 阶乘法群 G_2 和一个双线性映射 $e:G_1\times G_1\to G_2$；KGC 选定两个哈希函数 $H_1:\{0,1\}^*\to Z_q^*$ 和 $H_2:G_2\to\{0,1\}^l$，其中 l 表示明文的长度。另外，KGC 随机选定 $\alpha,\beta,\gamma\in Z_q^*$，并计算 $v=e(\alpha P,\beta P)=e(P,P)^{\alpha\beta}$。系统的主密钥为 $\alpha\beta P$，公开参数为 $(G_1,G_2,e,n,P,\alpha P,\beta P,\gamma P,H_1,H_2,v)$。

(2)私钥抽取算法。给定某用户身份标识 ID，KGC 选定一个随机数 $r\in Z_q^*$ 后，计算用户的公钥为 $q_{ID}=H_1(ID)$，用户的私钥为 $D_{ID}=(q_{ID}\,r\alpha P+\alpha\beta P+r\gamma P,rP)=(D_0,D_1)$。

(3)加密算法。令明文为 $M\in\{0,1\}^n$，用公钥 $q_{ID}=H_1(ID)$ 加密过程：随机选择 $s\in Z_q^*$，计算 $k=v^s$，$C_0=sP$，$C_1=q_{ID}(s\alpha P)+s\gamma P$，$C=M\oplus H_2(k)$，密文为三元组 (C,C_0,C_1)。

(4)解密算法。计算 $k=e(C_0,D_0)/e(C_1,D_1)$ 和 $M=C\oplus H_2(k)$，则明文为 M。

3 Boneh-Boyen$_1$ IBE 的安全密钥分发

为了解决密钥托管问题，安全密钥分发方案中除了一个1个 KGC 之外，还需要多个 KPA 实体(假定为 n 个)。Boneh-Boyen$_1$ IBE 中，系统主密钥 $\alpha\beta P$ 可以由两个秘密值 α 和 β 计算出来。本方案中，α 分解为 $n+1$ 秘密值的连积：α_0，α_1，$\cdots\alpha_n$，于是 $\alpha=\prod_{i=0}^{n}\alpha_i$。$\beta$ 分解为 $n+1$ 个秘密值的和：β_0，β_1，$\cdots\beta_n$，于是 $\beta=\sum_{i=0}^{n}\beta_i$。其中 KGC 持有 α_0 和 β_0，KPA_i $(i=1,2,\cdots,n)$ 持有 α_i 和 β_i。最终 $\alpha\beta P=\prod_{i=0}^{n}\alpha_i(\sum_{i=0}^{n}\beta_i)P$。

方案分为系统初始、密钥分发、密钥保护和密钥生成4个阶段。

3.1 系统初始阶段

(1) KGC 选定一个 q 阶加法循环群 G_1，其生成元为 $P\in G_1$、一个 q 阶乘法群 G_2 和一个双线性映射 $e:G_1\times G_1\to G_2$；KGC 选定两个哈希函数 $H_1:\{0,1\}^*\to Z_q^*$ 和 $H_2:G_2\to\{0,1\}^l$，其中 l 表示明文的长度。另外，KGC 随机选定 $\alpha_0,\beta_0,\gamma\in Z_q^*$，并公布参数 $(G_1,G_2,e,n,P,\gamma P,H_1,H_2)$。

(2) 每个 KPA_i $(i=1,2,\cdots,n)$ 随机选择 $\alpha_i,\beta_i,k_i\in Z_q^*$；计算并公开 k_iP。

(3) 记 $(\prod_{m=0}^{i}\alpha_m)P$ 为 P_i $(i=0,1,\cdots,n)$，KGC 与 n 个 KPA 通过以下步骤计算 $\alpha P=\prod_{i=0}^{n}\alpha_iP$。

KGC 计算并发送 $(P_0,\gamma k_1P)$ 给 KPA_1，KPA_1 验证 $e(\gamma k_1P,P)=e(\gamma P,k_1P)$，若不成立则中止，否则 n 个 KPA 依次执行下面步骤：

```
for(i=1;i<=n;i++) {
    KPA_i 计算 P_i=(∏_{m=0}^{i} α_m)P=α_i×P_{i-1};
    if(i<n)
        KPA_i发送 P_i给 KPA_{i+1};
}
```

最后，KPA_n 公布 $P_n=\alpha P$ 作为系统公开参数。

(4) KGC 公布 $e(\alpha P,\beta_0P)$，每个 KPA_i $(i=1,2,\cdots,n)$ 公布 $e(\alpha P,\beta_iP)$，系统公开参数 $e(\alpha P,\beta P)=\prod_{i=0}^{n}e(\alpha P,\beta_iP)$。

(5)具有身份标识 ID 的用户随机选取 $y\in Z_q^*$ 并计算 yP，该用户在密钥分发方案中使用 (yP,y) 作为长期公/私密钥对，避免了文献[7]提出的恶意 KGC 发起的攻击。

3.2 密钥分发阶段

(1) 具有身份标识 ID 的用户随机选取 $x\in Z_q^*$，计算盲因子 $X=xP$，并发送 $(ID,X,y\gamma P)$ 给 KGC 请求部分私钥。

(2)验证 $e(y\gamma P,P)=e(yP,\gamma P)$ 成立后，KGC 随机选取 $r\in Z_q^*$ 并发送 $((q_{ID}r\alpha_0P+\alpha_0\beta_0P),rP,r\gamma X,\alpha_0X)$ 给该用户。

(3)该用户从 KGC 的消息中计算出部分私钥为 $(q_{ID}r\alpha_0+\alpha_0\beta_0)X$，并计算 $\alpha_0P=(x)^{-1}\alpha_0X$。

记 $x(q_{ID}r\alpha_0P+\alpha_0\beta_0P)$ 为 PK_0。

3.3 密钥保护阶段

在该阶段中，具有身份标识 ID 的用户依次请求 KPA_i $(i=1,2,\cdots,n)$ 发送部分私钥以保证最终密钥不为 KGC 所知，记 $(\prod_{m=0}^{i}\alpha_m)X$ 为 X_i $(i=0,1,\cdots,n)$，该阶段具体如下：

```
for(i=1;i<=n;i++){
该用户向 KPA_i 发送(PK_{i-1},yk_iP,X_{i-1},X);
验证 e(yk_iP,P)=e(yP,k_iP)成立后，KPA_i计算 X_i=(∏_{m=0}^{i} α_m)X=
α_iX_{i-1}以及 PK_i=α_iPK_{i-1}+β_i(∏_{m=0}^{i} α_m)X,并将 X_i 和 PK_i 发给该用户;
}
```

3.4 密钥生成阶段

得到 PK_n 后，具有身份标识 ID 的用户计算出私钥为 $(r\gamma P + x^{-1}PK_n, rP) = (q_{ID}\, r\alpha P + \alpha\beta P + r\gamma P, rP)$。

4 安全性证明

本节证明本方案能够解决 Boneh-Boyen$_1$ IBE 的密钥托管问题，即能保证用户私钥的安全性。首先通过“攻击者—挑战者”游戏给出密钥安全性的定义。游戏中攻击者为恶意的 KGC，具有监听所有通信消息的能力，同时具有攻陷某些 KPA 的能力；挑战者是一个理想实体，知道系统中所有的公开及秘密参数，该游戏由 4 个阶段组成：

(1)初始阶段。挑战者和攻击者模拟运行密钥分发方案的系统初始阶段，挑战者将所有系统公开参数发送给攻击者。

(2)攻击者训练阶段。这一阶段中攻击者多次发起两种请求，其一，可以请求一个用户发起安全密钥分发方案的密钥分发、密钥保护和密钥生成阶段；其二，可以请求攻陷某 KPA。挑战者收到前一请求后，模拟运行密钥分发方案的密钥分发、密钥保护和密钥生成阶段，并将模拟运行中的所有交互消息发送给攻击者；挑战者收到后一请求后，将模拟运行中相应 KPA 的内部状态发送给攻击者。

(3)攻击阶段。当训练阶段结束后，攻击者选定某用户的身份标识输出该用户的私钥，或者输出密钥分发方案的主密钥。

定义 1(用户密钥安全性) 在上一游戏中，如果 PPT 攻击者在攻击阶段成功输出某用户私钥的概率可忽略，则称密钥分发方案具有用户密钥安全性。

定义 2(主密钥安全性) 在上一游戏中，如果 PPT 攻击者在攻击阶段成功输出主密钥的概率可忽略，则称密钥分发方案具有主密钥安全性。

显然，用户密钥安全性意味着恶意 KGC 无法获取用户私钥，即密钥分发方案解决了密钥托管问题；另一方面，主密钥安全性则意味着恶意 KGC 无法获取系统主密钥。下面的引理和定理说明了本方案的安全性。

引理 本方案在 KPA_n 未被攻陷的情况下具有主密钥安全性。

证明：假设攻击者可以在未攻陷 KPA_n 的情况下，以不可忽略的概率 ε 在上述游戏中输出主密钥，则可以构造 PPT 算法 B，以概率 ε 解决 CDH 问题。

假定算法 B 的输入为 (P, aP, bP)，B 试图计算并输出 abP，算法 B 构造规则如下所述。B 以上述游戏中的挑战者为子程序，除了以下两点外，在上述游戏中扮演挑战者：

(1)在初始阶段，B 以 aP 和 $bP - q_{ID}rP - \sum_{i=0}^{n-1}\beta_i(aP)$ 分别代替参数 α_nP 和 β_nP。

(2)在攻击者训练阶段，当 KPA_n 需要计算 PK_n 值时，B 以 G_1 上的随机值作为 PK_n 的值，由于 $PK_n = x\alpha(q_{ID}r+\beta)P = \prod_{i=0}^{n-1}\alpha_i x\alpha_n(q_{ID}r + \sum_{i=0}^{n-1}\beta_i + \beta_n)P$，且攻击者无法获取 α_n，β_n 和 x 的值，根据 DBDH 假定，攻击者无法区分 PK_n 和 G_1 上的随机值，因此从攻击者的角度来看，B 完善地扮演了挑战者。

攻击阶段结束后，B 读取攻击者输出的主密钥 MK，若 MK 满足 $e(P, MK) = e(P, aP)^{\prod_{i=0}^{n-1}\alpha_i} e(aP, bP)^{\sum_{i=0}^{n-1}\beta_i \prod_{i=0}^{n-1}\alpha_i}$，$B$ 输出 $((\prod_{i=0}^{n-1}\alpha_i)^{-1}MK + q_{ID}r(aP))$ 作为 abP 的值。由于攻击者可以以不可忽略概率 ε 输出主密钥，同时 $\alpha\beta P = \prod_{i=0}^{n}\alpha_i(\sum_{i=0}^{n}\beta_i)P$ 且 $MK = \alpha\beta P$ 等价于 $abP = ((\prod_{i=0}^{n-1}\alpha_i)^{-1}MK + q_{ID}r(aP))$，因此 B 解决 CDH 问题的概率也等于 ε，这与 CDH 假定矛盾，故引理得证。

定理 本方案在 KPA_n 未被攻陷的情况下具有用户密钥安全性。

证明：假定本方案在 KPA_n 未被攻陷的情况下不具有用户密钥安全性，即攻击者可以以不可忽略概率计算出某公钥为 q_{ID} 用户的私钥，假定为 (M, rP)。由于攻击者同时也是 KGC，故攻击者知道参数 r 和 γ 的值，因此攻击者可以计算出主密钥为 $M - (q_{ID}r\alpha P + r\gamma P)$。这意味着攻击者能以相同的不可忽略的概率计算出主密钥，这违反了上述引理，故本定理得证。

5 性能分析和比较

通信开销和计算量是衡量密钥分发方案性能的重要指标，而安全性假定是衡量密钥分发方案安全性的重要指标。表 1 通过与文献[13]的密钥分发方案在通信开销、计算量、安全性假定方面的比较，来分析本方案的性能。在对比中，方案的密钥分发、密钥保护和密钥生成阶段视为一个阶段：密钥抽取阶段(key extraction stage)。在计算量方面，考虑对运算、标量乘法运算、插值运算 3 种主要的运算；通信开销方面，以消息通信次数作为消息复杂度标准。

从表 1 可以看出，由于文献[13]方案采用的非交互式知识的证明和 DKG 协议引入了大量对运算、标量乘法运算和插值运算，本方案在计算量上具有明显优势；消息复杂度方面，文献[13]方案在初始阶段和密钥抽取阶段均需要交换 $O(n^3)$ 次消息，本方案在两个阶段仅需交换 $O(n)$ 次消息；安全性假定方面，本文方案在标准模型中具有安全性，而文献[13]方案仅在随机预言(random oracle，RO)模型中具有安全性。

表 1 密钥分发方案性能比较

	Goldberg and Katz 的方案[13]		本文方案	
	初始阶段	密钥分发阶段	初始阶段	密钥分发阶段
对运算	2n+1	8n	1	n
标量乘法	$4n^2$	$7n^2$	2n+1	3n+7
插值运算	1	4	0	0
消息复杂度	$O(n^3)$	$O(n^3)$	O(n)	O(n)
安全性假定	RO+CDH 假定		CDH+DBDH 假定	

结束语 本文提出一个用于 Boneh-Boyen$_1$ IBE 的安全密钥分发方案，方案通过在用户私钥生成中引入多个 KPA 避免了 KGC 知道用户私钥，并在标准模型中的 CDH 假定和 DBDH 假定下，证明了方案能够有效解决密钥托管问题。和现有的大多数密钥分发方案只能应用于全域哈希 IBE 相比，本方案可应用于计算效率更高的 Boneh-Boyen$_1$ IBE。和文献[13]的密钥分发方向相比，本方案在计算量和通信开销上具有明显优势，同时安全性更严格。

参 考 文 献

[1] Boneh D, Franklin M. Identity-based encryption from the weil pairing [C]// Proc of the Crypto 2001. Berlin: Springer, 2001: 213-229

(下转第 50 页)

户对已有的信息进行 Hash 运算，也适用于大量数据的检测输入。

接着是 Salt 值的输入，Salt 值的输入过程中一是选择 Salt 值的数据类型，二是输入 Salt 值，可直接在 Salt 值显示窗口中输入十六进制或二进制的 Salt 值。也可用产生随机 Salt 按钮来随机生成一个长度符合要求的 Salt 值。或用导入按钮，导入一个固定的 Salt 值。

最后是 Hash 值的输出，选择 Hash 值输出数据类型，然后点击控制面板里面的执行按钮，那么在 Hash 值显示窗口中将会显示出 Hash 值。

在本系统中的每一个按钮都设计了具体的错误提示，会提示用户具体错在哪里，如何进行修改。例如用户想要随机产生一个 576 比特的二进制信息串，而用户忘记选择信息的数据类型而点击了产生随机数按钮，那么就会弹出错误信息——"请选择数据的类型"。

2.3.3 *输出中间数据*

设计本软件的主要目的之一是为研究 Hash 算法 BLAKE 的内部构造与设计提供一个工具。就像前面提到的，重点研究每一轮的输出以及 G 函数内部构造。研究轮效应就需要将各轮的输出记录下来，然后通过相应的工具进行分析，这里我们可以对随机分析提供足够的数据来源。

用户若对某些中间数据感兴趣，就需要对中间数据输出控制端做出一些选择。首先，选择中间值输出的数据类型(Hex/Bin)；然后输入感兴趣的组数(信息组数的最大值在输入信息之后，点击"BlockMax"按钮，则该信息的最大组数值 N 将显示在旁边的窗口中，查询的时候可在该窗口输入 1～N 之间的任意整数)；再选择在这一分组下的轮数，接着选择具体感兴趣的数据位置。设置好之后，用户只需要点击控制面板的执行按钮，用户感兴趣的数据就会显示在中间数据显示窗口中。

举例来说，如果选择 BLAKE 的类型是 256，16 进制的信息为'00'，16 进制的 Salt 值为'00000000 00000000 00000000 00000000'，数据类型都选择"Hex"，组数输入"1"，轮数选择"所有轮"，中间数据选择"RoundV"，点击控制面板的执行按钮，那么用 BLAKE-256 进行 Hash 运算时压缩函数每一轮的数据与 Hash 值将在各个窗口中显示。此时，图形用户界面的状态如图 3 所示。

用户可根据需要存储相关的数据，只需通过数据控制面板中的存盘选择按钮选择具体需要保存的数据，然后点击控制面板中的存盘按钮进行相关的操作。

结束语 本文在全球公开征集新一代安全 Hash 标准 SHA-3 的最后阶段，对可能成为 SHA-3 标准的 BLAKE 进行了初步的研究，并利用 Matlab 中的 Guide，开发了带有图形用户界面的 BLAKE。利用这个程序可以根据需要很方便地输出 BLAKE 运行的内部结果。这对 BLAKE 的教学以及 BLAKE 的深入研究都具有积极的意义。

参 考 文 献

[1] NIST. Secure Hash Standard[S]. Federal Information Processing Standards Publication(FIPS) 180-2,2002

[2] NIST. Secure Hash Standard[S]. Federal Information Processing Standards Publication(FIPS) 180-3,2008

[3] Aumasson J-P, Henzen L, Meier W, et al. SHA-3 proposal BLAKE* version 1. 3[EB/OL]. http://www. 131002. net/blake/blake. pdf,2010

[4] Biham E, Dunkelman O. A framework for iterative hash functions-HAIFA[R]. ePrint report 2007/278. 2007

[5] Aumasson J-P, Meier W, Phan R C-W. The hash function family LAKE[C]// FSE. 2008

[6] Aumasson J-P, Fischer S, Khazaei S, et al. New features of Latin dances: analysis of Salsa, ChaCha, and Rumba[C]// FSE. 2008

[7] Stinson D R. Cryptography Theory and Practice(Third Edtion)[M]. Taylor & Francis Group, FL, USA, 2006

(上接第 37 页)

[2] Chen L, Harrison 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

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

[4] Gentry C. Certificate-based encryption and the certificate-revocation problem [C]// Proc of Eurocrypt 2003. Berlin: Springer, 2003: 272-291

[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 Cryptology and Information Security. Berlin: Spring, 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. Australia: CRPIT, 2004

[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] Chunxiang X, Junhui Z, Zhiguang Q. A Note on Secure Key Issuing in ID-based Cryptography [EB/OL]. http://eprint. iacr. org/2005/180

[9] Lee B. Unified public key infrastructure supporting both certificate-based and ID-based cryptography [C]// Proc of the 2010 International Conference on Availability, Reliability and Security. Poland: IEEE, 2010: 54-61

[10] Boyen X. A tapestry of identity-Based encryption: practical frameworks compared[J]. International Journal of Applied Cryptography, 2008, 1(1): 3-21

[11] Boyen X. The BB1 identity-based cryptosystem: A standard for encryption and key encapsulation [EB/OL]. http:// grouper. ieee. org/groups/1363

[12] Martin L. Introduction to Identity-Based Encryption [M]. Boston: Artech House, 2008

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

[14] Boneh D, Boyen X. Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles [C]// Proc of EUROCRYPT 2004. Switzerland: Springer, 2004: 223-238