第35卷 第24期 计 算 机 工 程 2009年12月
Vol.35 No.24 Computer Engineering December 2009
·安全技术· 文章编号：1000—3428(2009)24—0174—02 文献标识码：A 中图分类号：TP309.2

密钥托管可控的跨域通信 IBE 模型

王 兴[1]，丁 宏[1]，李 欣[2]
(1. 杭州电子科技大学计算机学院，杭州 310018；2. 公安部第三研究所信息网络安全研发中心，上海 201204)

摘 要：与传统的公钥密码体系相比，基于身份加密(IBE)具有许多优点，但目前提出的 IBE 模型都未能消除密钥托管。针对该问题，提出一种新的 IBE 模型，该模型可以控制密钥托管的范围或完全消除密钥托管，通过区域划分和域间互信，实现跨域互连，并给出在此基础上的对等密钥协商协议。分析结果表明，该模型未增加额外的结构，也未增加密钥协商的计算量或通信开销。

关键词：密钥管理；基于身份加密；密钥托管；密钥协商

IBE Model for Inter-domain Communications with Key Escrow under Control

WANG Xing[1], DING Hong[1], LI Xin[2]
(1. College of Computer & Software, Hangzhou Dianzi University, Hangzhou 310018; 2. Information Network Security Research and Development Center, The Third Research Institute of the Ministry of Public Security, Shanghai 201204)

【Abstract】 Identity-Based Encryption(IBE) provides much more convenience against traditional public key cryptography， but newly proposed schemes can not eliminate key escrow. Aiming at this problem, this paper proposes a new scheme to control key escrow or eliminate it completely. In this model, users are divided into different groups and these groups are associated with each other by inter-trust. A key agreement protocol based on it is provided. Analysis result proves that the model does not need extra infrastructures, and does not increase the cost of computation or communication for key agreement.

【Key words】 key management; Identity-Based Encryption(IBE); key escrow; key agreement

1 概述

相对于传统的公钥密码体系，基于身份加密[1](Identity-Based Encryption, IBE)具有很多优势：用户公钥可以根据用户身份直接计算出来，没有繁琐的证书管理，运维的负担要小得多。只要知道能唯一确定用户身份的信息，任何人都可以给他发送只有他能解密的消息；这样 IBE 就需要一个密钥管理中心，为所有用户发放私钥，用来解密使用身份信息加密的消息。IBE 也有一些缺陷，比如与生俱来的用户私钥被动托管问题，即密钥管理中心能够计算用户的私钥；同时 IBE 的密钥更新和密钥吊销比较麻烦。目前提出的 IBE 公钥管理方案有文献[2]提出的 BF-IBE，文献[3]提出的 HIDE，文献[4]提出的 CBE 以及文献[5]提出的 CLPKC 等。其中，BF-IBE 引用最广。BF-IBE 中所有用户的私钥都可以用主密钥计算出来，即密钥管理中心被动托管所有用户的私钥，可以说整个系统只有主密钥这一个密钥。同时密钥管理中心负责所有的密钥管理工作，负担太大，同时也有“单点失效”的危险。HIDE 将密钥体系分层，分散了密钥管理的负担，并一定程度上缓解了密钥托管的问题，但是层次结构复杂带来了呈线性增长的加解密计算量和通信开销。CBE 和 CLPKC 没有被动密钥托管的问题，但是这 2 个方案不能算是严格意义上的 IBE，用户的公钥不能通过用户身份信息直接计算出来。

在小型系统中，BF-IBE 是不错的选择，密钥管理中心的负载是可以承受的，范围有限、可控制的密钥托管是允许的。但是，如果整个系统跨越多个学科领域，涉及数个行业，而且地域分散行政层次复杂，密钥托管问题就不可接受了。本文提出了一种新的密钥体系构建方式来消除密钥托管。首先将系统内所有用户划分为不同的域，每个域都可以看成是一个小的 IBE 系统。域之间互相建立信任关系，通过信任关系将所有域组成一个大的信任域，同时也是一个全局性的 IBE 系统。该方案将密钥托管控制在一个可控的范围内或完全消除，同时保证用户的公钥依然可以根据用户的身份信息直接计算得到，而且不增加结构复杂度，也不增加系统内加解密运算和密钥协商的运算量和通信开销。

2 相关理论

假设 E 是有限域 F 上的一条椭圆曲线，G_1 是一个 q 阶循环加法群，生成元为 p，q 为大素数。G_2 是 q 阶乘法群。定义双线性映射 $e:G_1\times G_1\to G_2$，其中，G_1 为 $E(F)$ 上点构成的加法群，G_2 为 F 扩展域上的乘法群。e 具有如下属性：

(1)双线性：$\forall P,Q,R\in G_1$，$e(P,Q+R)=e(P,Q)\cdot e(P,R)$，$e(P+Q,R)=e(P,R)\cdot e(Q,R)$。$\forall a,b\in Z_q^*$，$e(aP,bQ)=e(P,Q)^{ab}$。

基金项目：“十一五”国家科技支撑计划基金资助项目(2006BAK15B07)

作者简介：王 兴(1985－)，男，硕士研究生，主研方向：网络信息安全；丁 宏，教授；李 欣，助理研究员、博士

收稿日期：2009-05-04 **E-mail：**htyphoon@126.com

(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 $P,Q\in G_1$，存在一个高效的算法计算 $e(P,Q)$。

对于 $P,aP,bP,cP,Q\in G_1$，$a,b,c\in Z_q^*$，假设以下数学问题是难解的：

(1)离散对数难题(DLP)：给定 P,Q，找到 a 使得 $Q=aP$。

(2) G_1 上的 Diffie-Hellman 计算(CDH)问题：给定 P,aP,bP，计算 abP。

(3)双线性 Diffie-Hellman(BDH)问题：给定 P,aP,bP,cP，计算 $e(P,Q)^{abc}\in G_2$。

3 密钥管理与密钥协商

3.1 密钥组织与密钥管理

系统定义：系统定义为域的集合：$\{D_1,D_2,\cdots,D_n\}$；每一个域 D_i 包括：用户的集合 $\{U_1,U_2,\cdots,U_T\}$，密钥管理中心 KGC_i，基点 P_i，域标识名称 ID_i，初始私钥 s_i，主密钥 SK_i。

(1)选取全局公共系数。全局公共系数在整个系统的初始化时确定，长期有效。确定 E 为有限域 F 上的椭圆曲线，G_1 是生成元为 p，阶为大素数 q 的加法循环群，G_2 是 q 阶的乘法循环群。双线性映射 $e:G_1\times G_1\to G_2$，哈希函数 $H:\{0,1\}^*\to F$，$H_2:\{0,1\}^*\to G_1$。

(2)域参数初始化。域 D_i：KGC_i 选择随机数 $r\in F$ 为 s_i 初始化，基点 $P_i=H_2(ID_i)$，计算 s_iP_i。

(3)域间建立信任关系。D_i 与 D_j 建立信任关系：

1) KGC_i 通过安全认证通道向 KGC_j 请求建立互信；

2) KGC_j 验证请求，如果请求合法则发回 $\{s_jP_i\}$；

3)上述步骤完成单向信任，反向的信任关系依照同样的方式建立。

(4)数个域两两建立互信之后构成一个信任域，定义信任域内域个数为度 d，单个域 D_t 的密钥管理节点 KGC_t 可以计算 D_t 在该信任域内的主密钥：$SK_t=\sum_{i=1}^{d}s_iP_t$ (下标标号为信任域内标号)。

组成的信任域覆盖范围不同，单个域在其中的主密钥也就不同。本文着重讨论 $d=n$ 的情况，即系统内所有域两两互信，构成的信任域包含所有用户。

(5)用户密钥。D_i 的用户 $user1$ 的公钥为：$PK_{user1}=H(ID_{user1})P_i$，其中 $P_i=H_2(ID_i)$；密钥管理节点 KGC_i 为其计算信任域中的私钥：$SK_{user1}=H(ID_{user1})SK_i$。

作为对比，给出用户在 D_i 域内的密钥对：$PK_{user1}=H(ID_{user1})P_i$；$SK^i_{user1}=H(ID_{user1})s_iP_i$。

3.2 密钥协商

假设 D_i 中 $user1$ 与 D_j 内用户 $user2$ 需要建立安全通信链路，其步骤如下：

(1) $user1$ 产生随机数 r_1，发送 r_1PK_{user1} 给 $user2$；

(2) $user2$ 产生随机数 r_2，发送 r_2PK_{user2} 给 $user1$；

(3) $user1$ 计算共享密钥：$K_{user1}=e(r_1SK_{user1},r_2PK_{user1})$；

(4) $user2$ 计算共享密钥：$K_{user2}=e(r_1PK_{user1},r_2SK_{user1})$。

可以验证 $K_{user1}=K_{user2}=e(PK_{user1},PK_{user2})^{r_1r_2\sum_{i=1}^{n}s_i}$。

单向信任：全互联没有建立，D_i 从 D_j 获得了单向信任：s_jP_i，则上述密钥协商过程变为：

(1) $user1$ 从 D_i 获得单向信任关系下的私钥 $SK^{i\&j}_{user1}=H(ID_{user1})s_is_jP_i=s_is_jPK_{user1}$；

(2) $user1$ 产生随机数 r_1，发送 $r_1SK^i_{user1}$ 给 $user2$；

(3) $user2$ 产生随机数 r_2，发送 r_2PK_{user2} 给 $user1$；

(4) $user1$ 计算共享密钥：$K_{user1}=e(r_1SK^{i\&j}_{user1},r_2PK_{user1})$；

(5) $user2$ 计算共享密钥：$K_{user2}=e(r_1SK^i_{user1},r_2SK^j_{user2})$。

可以验证 $K_{user1}=K_{user2}=e(PK_{user1},PK_{user2})^{r_1r_2s_is_j}$。

4 安全性分析及性能评估

4.1 安全性分析

首先假设每个小的域内都采用 BF-IBE 方案来管理。如果将系统内所有用户全划入一个域，那么这个域就是一个 BF-IBE 系统，存在完全的密钥托管；如果每个用户自成一个域，那么一个全互联的信任域就构成了一个无密钥托管的 IBE 系统(稍后证明)。先讨论一般的情况：域间两两互信构成了全局信任域，这时可以把整个系统看成是一个扩展的 BF-IBE：

根密钥：$s_{root}=\sum_{i=1}^{n}s_i$；信任域 D_t 的主密钥相当于根密钥产生的：$SK_t=s_{root}P_t$，公钥即 P_t。

根密钥只是用来说明问题虚拟的，并不真实存在。从根密钥的表达式和单个域主密钥的计算式可以看出，根密钥内包含各个域贡献的随机因子，任意数目小于 n 的域联合起来都不能计算出根密钥。

(1)域主密钥没有被托管。因为根密钥是不存在的，而且根密钥不会泄露，除非所有域的初始密钥都泄露了，这时也就没有秘密了。所以域的主密钥没有被托管。

(2)域主密钥能防范合谋攻击。即使其他的所有域联合起来，再加上 D_t 内的用户节点，也不能合谋破解 D_t 的初始密钥 s_t 和主密钥 PK_t。所有其他节点联合起来能达到如下条件：

1)给定 $\forall r\in\{H(ID_{Ui})\}$，$U_i$ 为 D_t 内用户，都可以得到 rSK_t；

2)给定 $\forall r\in\{P_i\mid i\neq t\}$，$P_i$ 为域的基点，都可以得到 s_tP_i；

由于这 2 个都是难解的椭圆曲线离散对数问题，因此本方案中的域主密钥是能抵抗合谋攻击的。

(3)如果每个用户都自成一个域，那么一个全互联的信任域就构成了一个无密钥托管的 IBE 系统。由(1)和(2)可知，这种条件下的所有用户的密钥都没有被托管，能抵抗合谋攻击。

4.2 性能评估

假设域内采用 BF-IBE 方案来管理密钥。从密钥体系建立过程中用户公私钥的计算方法可以看出，在本文提出的 IBE 模型中，用户公钥总是可以根据身份信息直接计算得到，私钥由其直属密钥管理节点为其产生，这与 BF-IBE 相同；而密钥管理节点仅需维护其初始密钥和主密钥。考虑两种特殊的情况：所有用户划分为一个域和每个用户都自成一个域。所有用户划分为一个域时，只需要一个密钥管理节点，模型变为 BF-IBE。每个用户都自成一个域时，用户自行管理密钥，即维护初始密钥，并通过信任互联获得在公共通信组内的主密钥。与 CBE[4]和 CLPKC[5]相比，本文提出的密钥管理方案消除密钥托管的同时，保证用户公钥仍可以根据身份信息得到，即保留了“基于身份加密”的特性。

(下转第 178 页)