文章编号: 1006-4710(2012)01-0102-04

可用于团队模式的动态广播加密方案

孙瑾, 王晓峰
(西安理工大学 理学院, 陕西 西安 710054)

摘要: 提出一个可用于团队设计模式的动态广播加密方案。通过结合广播加密模型和无证书密码理论,利用身份作为参数,成功解决了方案中私钥泄露的问题。在该方案中每个成员均可以加密和传递设计文档,但只有指定的设计组成员可以解密被加密的文档。分析结果显示该方案在离散对数假设下是安全的,在可以承载公钥密码系统的无线传感器网络中无需额外的硬件设备,故不仅适用于传感器节点而且是其应用领域中一个引人注目的安全结论。

关键词: 广播加密; 无证书公钥系统; 协作设计; 无线传感器网络
中图分类号: TN918.1 **文献标志码**: A

Dynamic Broadcast Encryption Scheme Applicable to Collaborative Design Model

SUN Jin, WANG Xiaofeng
(Faculty of Science, Xi'an University of Technology, Xi'an 710054, China)

Abstract: This paper presents a dynamic broadcast encryption scheme applicable to the collaborative design model. The new scheme uses the ID card as the parameters to successfully solve the private key eschewing problem via combining the broadcast encryption model with the certificateless cryptography theory. In this scheme, every member can encrypt and transmit the designed documents, but it is only the members in the appointed design team who can decrypt the encrypted documents. The analytical results indicate that this scheme is secure under the discrete logarithm assumption and needn't require the additional hardware equipment in the wireless sensor network under the affordable public key cryptography system, whereby this scheme is not only a node applicable to the sensor but also an attractive security conclusion in its applicable realm.

Key words: broadcast encryption; certificateless public key cryptography; collaborative design; wireless sensor networks

团队协作模式是指由多个不同领域的人员彼此合作来完成一个产物,而这一产物将服务于公开的网络。团队协作模式包含多个团队,其相互传递的信息及资料的可信性必须得以保证,这就要求除了指定的团队成员,其他任何人都不能获取所传递的信息。鉴于团队协作模式的动态特性,负责网上构造及分配密钥的可信任授权中心要时时在线是不可能的。虽然可以利用 Diffie-Hellman (DH)密钥交换协议要求通过交换双方的秘密值来构造密钥,但它只适用于一对一的模式,即便能够扩展到多对一的情形,效率问题也仍然存在[1-15]。

广播加密的核心思想是广播者将消息加密并通过广播方式发送给大量用户,其中只有拥有授权的合法用户才可以解密并获得真实信息。目前,这种加密方式在动态无线网络中的应用成为了密码学中一个新的研究热点。国内外学者纷纷涉猎于此,很多具有特殊用途的广播加密方案也被相继提出[4-6],但这些方案都存在明显的不足,比如,所基于的困难性问题太强,并且仅具有 Selective-ID 安全性或安全性依赖于随机预言机模型等[15]。

收稿日期: 2011-10-08
基金项目: 国家自然科学基金资助项目(61173192,60833008);陕西省教育厅自然科学基金资助项目(11JK0505)。
作者简介: 孙瑾(1977-),女,安徽萧县人,讲师,研究方向为公钥广播加密方案的设计与分析。
E-mail: oksunjin@xaut.edu.cn。

网络的公开性是信息传输的一大威胁，动态网络（如无线传感器网、ad hoc 网），由于所有节点都承载着传感、路由及存储数据的任务，自身能量不足却承受着高流通量和存储量的压力而备受关注。动态网络中信息安全问题的关键在于密钥的管理与分配。很多基于对称密码技术的关于密钥管理的方案被提出[7-8]，然而适用于动态网络时高流通量和存储量的压力就凸现出来了。事实上，与对称密码体制相比公钥密码体制（PKC）能提供更多的灵活性和优势。文献[9]、[10]提出在无线传感器网络上 PKC 原型可以快速有效地被实现，这一事实使得在无线传感器网络上讨论安全问题的新方法以及身份型密码方案（IBE）的实现成为可能。随后，文献[11]~[13]预测了 IBE 方案可作为安全结论用于无线传感器网络，然而这些结论在实际应用中的灵活性却没有经过测试。到目前为止，传感器设备上完整的 IBE 方案还没有被提出。

考虑到上述问题，本研究提出一个可用于动态传感器网络的考虑团队设计的广播加密方案。此方案结合无证书加密系统及公钥广播加密模型，结构简单，加密时无需双线性对运算，尤其对低端传感器节点来说减轻了计算负担。在群密钥生成阶段方案不要求用户进行任何的信息交换，方案的安全性建立在离散对数假设这一公认的困难问题上。

1 预备知识

1.1 双线性映射

设 G，G_T 是两个素数 p 阶的循环群，g 是 G 的生成元，a、b 是 Z_p^* 中的元素。双线性映射 $e(\cdot,\cdot)$ 为 $G\times G\to G_T$，并满足以下性质。

1）双线性：$\forall g,h\in G,\hat{e}(g^a,h^b)=\hat{e}(g,h)^{ab}$。

2）非退化性：$\exists g,h\in G$，使得 $\hat{e}(g,h)\neq 1$。

3）可计算性：$\forall g,h\in G$，存在有效算法计算 $\hat{e}(g,h)$。

双线性对可以通过有限域上的超奇异椭圆曲线或超奇异超椭圆曲线中的 Weil 对或 Tate 对推导出来[14]。

1.2 复杂性假设

离散对数问题：

1）DLP（离散对数问题）：设 p 是一个大素数，g 是群 Z_p^* 的一个生成元。对于元素 $y\in Z_p^*$，离散对数问题 DLP 即是找到一个整数 $x\in Z_p^*$，使得 $g^x=y \bmod p$。

2）GDLP（G 群离散对数问题）：设 G 是一个阶为 n 的有限循环群，$g\in G$ 是它的一个生成元。对于元素 $y\in G$，离散对数问题 GDLP 即是找到一个整数 x，使得 $g^x=y$。

离散对数假设为：设 g 是 n 阶有限循环群 G 的一个生成元，元素 $y\in G$。那么寻找一个整数 x 使得 $g^x=y$ 是一个困难问题，即不存在可能的多项式时间算法以不可忽略的优势解决 GDLP 问题。

1.3 动态广播加密方案的定义[15]

在基于身份的广播加密体制（IBBE）中，一个公钥可以对任意多个身份构成的群进行加密，而在其基础上加入动态因素后所得到的动态广播加密体制（DBE）则更具实用性。动态广播加密方案形式上由系统建立、密钥提取、加密和解密四个算法构成，详述如下。

1）系统建立：输入安全参数 λ 及最大接收者的数目 n，输出系统参数和主密钥。

2）密钥生成：输入系统参数及用户序号，输出相应用户的身份标签 lab_i 及解密密钥 dk_i。

3）加密：设用户集合为 $S=(ID_1,\cdots,ID_n)$，撤销用户集合是 $\bar{S}$，广播者用初始加密密钥 ek 首先为 $S\backslash\bar{S}$ 生成 (Hdr,K)，其中，Hdr 称为密文头部，K 称为会话密钥（实际应用中多采用对称密钥），然后利用 K 加密消息 M 得到广播体 C_M 并将 $(Hdr,\bar{S},C_M)$ 发送给每个用户。

4）解密：设用户 ID_i 是诚实用户，$(Hdr,\bar{S},C_M)$ 是其接收到的密文，他首先利用 Hdr 析出 K，然后解密 C_M 恢复明文 M。

2 基于动态网络的身份型广播加密方案

本研究基于文献[5]、[6]提出一种可用于无线传感器网络等动态网络的基于协作模式设计的身份型广播加密方案。新方案结合了基于身份的密码理论和无证书密码技术，依据设计者及设计团队的身份来构造，无需公钥结构，用户的私钥通过密钥生成中心（KGC）和用户共同生成，而 KGC 不知道完整的私钥，只有指定的合法接收者才能解密消息。新方案对从事控制网络安全的传递技术信息的公司来说是很优越的，它在解决了密钥泄漏问题的同时也克服了 KGC 控制私钥的潜在威胁，方案详述如下。

1）系统建立：KGC 生成全球化系统参数。任选值 $r\in Z_p^*$，若 E 表示 F_q 上的一个适合对运算的超奇异椭圆曲线，则随机选择阶为 p 的点 $P\in E(F_q)$，$Q\in E(F_q)$，满足 $Q=rP$。$\hat{e}:E(F_q)\times E(F_q)\to E(F_q)$ 是一个双线性映射，$H_1:\{0,1\}^*\to Z_q^*$ 和 $H_2:F_q\to\{0,1\}^n$ 是两个抗碰撞哈希函数，设 $g=\hat{e}(P,P)$，则系统参数为 $(E(F_q),Q,P,q,n,H_1,H_2)$，主私钥为 r。同时，KGC 任意选择一个传统的对称加密算法 $E(\cdot,\cdot)$（如

AES)用于加密文档,则其相应的解密算法为$D(\cdot,\cdot)$。

2)密钥生成,此过程包括以下两点。

①团队私钥生成:每个团队$i,i=1,\cdots,l$任意推选一名成员作为队长,由其在KGC处登记队身份ID_i以及每个队成员的身份$ID_{ij},j=1,2,\cdots,j_n$,其中ID_{ij}表示团队i中的成员j。KGC为团队i随机选择元素$r_i\in Z_p^*$,计算$sk_i=P^{r_i \bmod p}$,然后KGC保存r_i作为团队i的主密钥,并公开(ID_i,sk_i)作为团队i的公共信息。

②个人私钥生成:团队i中的成员j私下选择随机值$x_{ij}\in Z_p^*$,计算个人部分私钥$d_{ij}=P^{(x_{ij}+H_1(ID_{ij})) \bmod p}$,随后向KGC提供自己的身份$ID_{ij}$及值$d_{ij}$。KGC通过物理方法验证用户的身份,用团队$i$的主密钥$r_i$计算$sk_{ij}=d_{ij}^{\frac{1}{r_i+H_1(ID_i)} \bmod p}$,然后发送给用户$ID_{ij}$,则用户$ID_{ij}$的个人私钥为$(x_{ij},d_{ij},sk_{ij})$。

3)加密:如果某个用户想将文档M安全的广播通知给团队i的成员,那么他首先在系统公共信息列表中找到团队i公开信息(ID_i,sk_i),然后选择随机值$s_i\in E(F_q)$作为加密过程的会话密钥,输入加密机制$E(\cdot,\cdot)$和文档M,得到$C_i=E(s_i,M)$,随机选择值$t\in Z_q^*$并计算广播头部$Hdr_i=(h_{i1},h_{i2})$,其中$h_{i1}=(sk_iP^{H_1(ID_i)})^t$,$h_{i2}=s_i\oplus H_2(g^t)$。最后将密文$(ID_i,Hdr_i,C_i)$广播发送给用户。

4)解密:所有人都可以接收到合法的密文(ID_i,Hdr_i,C_i),但只有团队i中的成员$ID_{ij},j=1,2,\cdots,j_n$可以对其解密。他利用自己的私钥(x_{ij},sk_{ij})首先计算获得会话密钥s_i:$H_2[\hat{e}(sk_{ij},h_{i1}^{\frac{1}{x_{ij}+H_1(ID_{ij})}})]\oplus h_{i2}=s_i$,然后获得被加密的文档$M$:$M=D(s_i,C_i)$。

3 方案的性能分析

3.1 正确性分析

如果成员$ID_{ij},j=1,2,\cdots,j_n$接收到的密文(ID_i,Hdr_i,C_i)是合法密文,那么他可以利用自己的私钥(x_{ij},sk_{ij})获得会话密钥s_i,为:

$$\hat{e}(sk_{ij},h_{i1}^{\frac{1}{x_{ij}+H_1(ID_{ij})}})=$$

$$\hat{e}(d_{ij}^{\frac{1}{r_i+H_1(ID_i)}},(P^{r_i}P^{H_1(ID_i)})^t)^{\frac{1}{x_{ij}+H_1(ID_{ij})}}=$$

$$\hat{e}(P^{\frac{x_{ij}+H_1(ID_{ij})}{r_i+H_1(ID_i)}},P^{(r_i+H_1(ID_i))t})^{\frac{1}{x_{ij}+H_1(ID_{ij})}}=\hat{e}(P,P)^t=g^t$$

3.2 安全性分析

本研究广播加密方案的安全性基于离散对数假设。对其安全性的分析参考文献[6],具体为:

结论1 在离散对数假设下,任何用户都不能得到团队i的主密钥r_i。

首先,从公钥参数信息$sk_i=P^{r_i}$中捕获值$r_i=\log_P sk_{ij} \bmod p$是困难的,如果某用户想这样做,他需要解决离散对数问题。然而,离散对数问题是困难问题,所以通过追溯r_i值来伪造个人私钥几乎是不可能的。

虽然团队i中的成员$ID_{ij},j=1,2,\cdots,j_n$拥有个人密钥$sk_{ij}=d_{ij}^{\frac{1}{r_i+H_1(ID_i)} \bmod p}$及其部分私钥$d_{ij}=P^{(x_{ij}+H_1(ID_{ij})) \bmod p}$,但是他仍然难解$r_i$,因为这是求解离散对数逆问题。

如果用户意图通过密文信息$Hdr_i=(h_{i1},h_{i2})=((sk_iP^{H_1(ID_i)})^t,s_i\oplus H_2(g^t))$获得团队$i$的主密钥$r_i$,那么此问题与求解离散对数问题同样困难。

综上可知,得到团队i的主密钥r_i在离散对数假设下是困难的。

结论2 除了团队i,其它任何团队都无法从密文信息(ID_i,Hdr_i,C_i)中获得团队i的会话密钥。

根据本方案的结构,在所有已收到广播密文(ID_i,Hdr_i,C_i)的成员中,除了团队i中的成员外,其他任何人都无法从广播密文(ID_i,Hdr_i,C_i)中获得秘密值s_i,这是一个离散对数困难问题。因为值s_i和$H_2(g^t)$都是随机的,因而很难从$h_{i2}=s_i\oplus H_2(g^t)$中析出$s_i$。因此,会话密钥$s_i$的随机选择,保证了所设计的方案是前向安全的。

结论3 因为KGC不知道部分私钥,所以所设计的身份型广播加密方案不存在密钥泄漏问题。因此方案可以保证广播信息的安全性。

根据给定团队i中的成员j的身份$ID_{ij},j=1,2,\cdots,j_n$和部分私钥$d_{ij}=P^{(x_{ij}+H_1(ID_{ij})) \bmod p}$,计算$x_{ij}$是离散对数问题。在离散对数假设下求解此值几乎是不可能的。因为KGC得不到私钥的任何一部分值,故本方案能保证广播信息的安全性(在公钥加密体制中KGC是密钥生成中心,由他生成所有私钥所以它是一个潜在的安全隐患,而所设计的方案不存在这一隐患)。

结论4 新方案在离散对数假设下能有效抵抗串谋攻击。

假设团队i的所有合法用户或者其部分成员试图串谋获取团队i的主密钥。即使团队i的所有成员提供它们的个人私钥$sk_{ij}=d_{ij}^{\frac{1}{r_i+H_1(ID_i)} \bmod p}$及$d_{ij}=P^{(x_{ij}+H_1(ID_{ij})) \bmod p}$,攻击者想提取$r_i$仍然是一个离散对数问题。在离散对数假设下解决这一问题是困难的。由此可见,合法用户串谋为某新用户伪造私钥是不可能的,故而新方案是抗串谋攻击安全的。

3.3 效率分析

以下简单分析方案在加密、解密过程中的效率(见表1),并与以往方案进行对比。鉴于双线性对运算计算量大且耗时的特点,本方案在加密过程中只用了一个可以预计算的双线性对计算,解密过程也只需一个双线性对运算,有效剪除了上述消耗,而且解密过程的哈希运算可以预计算,与以往的结论相比,新方案的设计明显节省了密钥的存储空间和计算代价,因此非常有效。另外,新方案的密钥分配方式非常适应于抗节点追踪攻击,同时还提供了良好的安全性,从而为 ad hoc 网、无线传感器网等动态网络提供了一种新颖又简单的密钥分配方式。综上所述,新方案不仅安全有效而且适用于复杂的动态网络环境。

表1 广播加密方案的效率对比

Tab. 1 The efficiency compare on related broadcast encryption schemes

方案	困难假设	私钥长度	密文长度	对运算(加密)	对运算(解密)
BGW1	BDHE	$O(1)$	$O(n)$	1	$\|r\|+1$
文献[4]方案	GDDHE	$O(r)(r<\sqrt{n})$	$O(1)$	0	2
文献[5]方案	DBDH	$O(r)$	$O(1)$	0	2
新方案	GDLP	3	3	0	1

注:在执行预计算的前提下,加密阶段可不需要对运算。表中$|r|$表示接收用户集和的大小。

4 结 论

本研究结合无证书加密系统及公钥广播加密模型,提出了一种基于团队设计的动态广播加密方案。新方案中加入团队密钥生成过程并增加了公共信息列表,不仅适合团队协作模式,而且以身份作为参数,省去了公钥证书的参与,有效避免了密钥泄漏问题以及身份盗取和复制问题。另外,新方案的密钥分配方式非常适用于抗节点追踪攻击,同时提供了良好的安全性,为 ad hoc 网、无线传感器网等动态网络提供了一种新颖又简单的密钥分配方式。

参考文献:

[1] Diffe W, Helllman B M E. New directions in cryptography [J]. IEEE Translation Information Theory, 1976,22(6): 644-654.

[2] Ahmed A H, Ali M, Luis O B. Authenticated group key agreement protocols for Ad hoc wireless network [J]. International Journal of Network Security, 2007, 4(1): 90-98.

[3] Park J H, Lee D H. Security analysis of a multi-receiver identity-based key encapsulation mechanism [J]. IEICE TRANS. Fundamentals, 2009, 92-A (1): 329-331.

[4] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys [C]//Advances in Cryptology-ASIA CRYPT, Malaysia, 2007, 4833: 200-215.

[5] Zhang L Y, Hu Y P, Mu N B. Identity-based broadcast encryption protocol for Ad Hoc networks[C]//IEEE Computer Society, Chengdu:China, 2009: 1619-1623.

[6] Zhang Y L, Zhang J, Zhang Y K. An ID-based broadcast encryption scheme for collaborative design[C]//NSWCTC, 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan:China, 2009, 2:699-702.

[7] Piotr S, Martin C. Tiny IBE: identity-based encryption for heterogeneous sensor networks [C]//IEEE 09, ISSNIP 2009, Melbourne: Australia, 2009: 349-354.

[8] Szczechowiak P, Kargl A, Scott M, et al. On the application of pairing based cryptography to wireless sensor networks[C]//WiSec'09, Second ACM Conference on Wireless Network Security, New York, 2009: 296-311.

[9] Szczechowiak P, Oliveira L, Scott M, et al. Nano ECC: testing the limits of elliptic curve cryptography in sensor networks[C]//EWSN2008, Berlin, 2008, 4913:1-24.

[10] Szczechowiak P, Kargl A, Scott M, et al. On the application of pairing based cryptography to wireless sensor networks[C]//WiSec'09, Second ACM Conference on Wireless Network Security, New York, 2009:1-12.

[11] Doyle B, Bell S, Smeaton A F, et al. Security considerations and key negotiation techniques for power constrained sensor networks [J]. The Computer Journal, 2006, (4/49):443-453.

[12] Yang G, Rong C, Veigner C, et al. Id-based key agreement and encryption for wireless sensor networks [J]. IJCSNS International Journal of Computer Science and Network Security, 2006, 6(5B):43-61.

[13] Oliveira L B, Dahab R, Lopez J, et al. Identity-based encryption for sensor networks [C]//PERCOMW '07, White Plains, 2007:290-294.

[14] Boneh D, Franklin M. Identity based encryption from the Weil pairing [J]. SIAM Journal of Computing, 2001,32: 586-615.

[15] 孙瑾,胡予濮,张乐友. 基于 ad hoc 网的身份型广播加密方案[J]. 计算机科学,2010, 38(2): 46-49.
Sun Jin, Hu Yupu, Zhang Leyou. Identity-based broadcast encryption based on Ad Hoc networks [J]. Computer Science, 2010, 38(2):46-49.

(责任编辑 李虹燕)