类身份广播加密方案*)

王青龙[1] 杨 波[2] 蔡 英[1,3] 韩 臻[1]
(北京交通大学计算机与信息技术学院 北京 100044)[1] (华南农业大学信息学院 广州 510642)[2]
(北京信息科学与技术学院计算机科学与工程系 北京 100085)[3]

摘 要 以身份加密为基础的应用研究在近年得到了快速发展。提出一种新的类身份的广播加密方案。与已有的基于身份的广播加密方案相比较,在保持存储密钥相同的情况下,本方案在计算量和传输开销方面得到了明显改善,有效提高了方案的效率。

关键词 广播加密,身份加密,双线性映射

Like ID-based Broadcast Encryption Scheme

WANG Qing-long[1] YANG Bo[2] CAI Ying[1,3] HAN Zhen[1]
(School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)[1]
(College of Information, South China Agricultural University, Guangzhou 510642, China)[2]
(Department of Computer Science and Engineering, Beijing Information Science and Technology University, Beijing 100101, China)[3]

Abstract In recent years, the applied research of ID-based encryption has developed rapidly. This paper proposed a new like ID-based broadcast encryption. Compared with previous broadcast encryption schemes which employ ID-based encryption, our scheme greatly reduces the cost of transmission overhead and computation while keeps store cost as the same.

Keywords Broadcast encryption, Identity-based encryption, Bilinear pairing

1 概况

广播加密由 Noar 等人于 1992 年首先提出[1],它主要应用于缺乏双向通信信道的场合,如付费电视、网上音视频数据发送、卫星信号发送、CD/DVD 发行等。由于每个用户都可以接收到广播的信息,为了保护服务提供者(DS, Data Supplier)的合法权益,DS 一般对广播的信息进行加密后再发送。合法的预期用户事先从 DS 处获得一组解密钥,因此可以对接收到的信息进行解密;非预期用户因为不拥有相应的解密钥,因而不能对接收到的信息进行解密。当服务提供者提供有多种不同服务时,对应的预期用户一般也是不相同的。另外,同一服务中的预期用户也存在变化,比如有新的用户增加进来或已有用户要取消服务,即预期用户集是动态变化的。如何给用户分配密钥,以满足用户集的动态性,正是广播加密所要解决的问题。

设计广播加密所要考虑的主要问题是在用户存储的解密钥数量和传输开销之间做到平衡。有两种平凡的方法:一种是为所有用户组成的集合的每个子集分配一个密钥,属于该子集的用户拥有分配给该子集的密钥,这样对任意预期用户只需使用由这些预期用户组成的子集对应的密钥加密传输的信息即可;另一种是每个用户存储一个不同的密钥,这样传输一个信息给某些预期用户时,分别用每个用户的密钥对该信息进行加密。第一种方法传输开销最小,但是用户存储的解密钥数量为指数级;第二种方法用户存储的解密钥数量最少,但是传输开销最大,实际上相当于点到对点的单播形式。

广播加密方案中发送的分组数据一般由两部分组成,一般记为 $C=(H,E_k(m))$,其中 H 称为分组头;E 为对称加密算法,m 为待广播信息,k 为对称密钥,称 $E_k(m)$ 为分组体。通过结合分组头提供的信息与自己的解密钥,每个预期用户都能够得出对称密钥 k,进而解密分组体,得到明文信息。

自文献[1]发表后,广播加密的研究很快得到更多人员的研究和关注,相关文献不断发表,其中基于身份加密体制构造的广播加密方案主要有文献[2,4],但是其中文献[4]已被发现存在不安全之处[3],而文献[2]所需的计算量和发送的分组长度都比较大。与已有同类方案相比较,本文的主要贡献是提出的类身份广播加密方案具有更高的效率,在存储量相同的情况下,计算量和通信开销得到了明显改善。

2 双线性映射

设 G_1 为 q 阶加法循环群,G_2 为 q 阶乘法循环群。满足在 G_1 和 G_2 上计算离散对数为困难问题。称 $e:G_1\times G_1\rightarrow G_2$ 为 G_1 到 G_2 的双线性映射,如果满足下述条件:

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

2)非退化性:$\exists P,Q\in G_1$ 满足 $e(P,Q)\neq 1$;

3)可计算性:存在一个有效算法计算 $e(P,Q)$,对 $\forall P,Q\in G_1$。

3 基于身份的加密体制

Boneh 和 Franklin 利用双线性映射构造了一个基于身份的加密方案[5],包括:

参数设置:G_1, G_2, e 意义同上,P 为 G_1 中生成元,KGC (key generation center)秘密选取 $s\in_R Z_q^*$, $H_1:\{0,1\}^*\rightarrow G_1$, $H_2:G_2\rightarrow\{0,1\}^*$ 是两个密码学意义上的 Hash 函数。设

*)基金项目:国家自然科学基金(No. 60372046,60573043),973 研究基金(No. 2007CB307106)。王青龙 博士研究生;杨 波 教授,博士生导师;蔡 英 副教授,博士研究生;韩 臻 教授,博士生导师。

$P_{pub}=sP$，KGC 公开$(G_1,G_2,e,q,P,P_{pub},H_1,H_2)$，保留 s 为秘密。设 ID_i 为用户 i 的公开身份，则 KGC 生成其对应的公钥和私钥分别为 $Q_i=H_1(ID_i)$和 $S_i=sQ_i$。

加密算法：设 m 为待加密消息，KGC 选取 $r\in_R Z_q^*$，

计算 $U=rP,V=m\oplus H_2(e(P_{pub},rQ_i))$。输出密文 $C=(U,V)$。

解密算法：$V\oplus H_2(e(U,S_i))=V\oplus H_2(e(rP,sQ_i))=V\oplus H_2(e(P,Q_i)^{rs})=V\oplus H_2(e(sP,rQ_i))=V\oplus H_2(e(P_{pub},rQ_i))=m$。

4 类身份广播加密方案

G_1,G_2,e,q,P,H_2 意义同上。当用户 u_i 注册时，DS 任选 $a_i\in Z_p^*$，计算 $Q_i=a_iP$ 作为 u_i 的伪身份(在身份加密方案中，Q_i 是对用户公开信息进行 Hash 运算得到的)，任选 $s_i\in Z_p^*$，通过安全信道传送给 u_i 作为其解密钥。N 为已注册用户集合。

加密算法：

设 $m\in G_2$ 为待广播消息，$N_p=\{u_1,u_2,\cdots,u_n\}\subseteq N$ 为预期接收用户集。DS 任选 $r\in Z_p^*$ 并求解满足下述方程组的 $(r_1,r_2,\cdots,r_n)$。

$$(r_1,r_2,\cdots,r_n)\times A=(k,k,\cdots,k) \tag{1}$$

其中 $k\in_R Z_p^*$，$A=\begin{pmatrix} s_1a_1 & a_2 & \cdots & a_n \\ a_1 & s_2a_2 & \cdots & a_n \\ & \cdots & & \\ a_1 & a_2 & \cdots & s_na_n \end{pmatrix}$

DS 计算：$H=(rP,r_1Q_1,r_2Q_2,\cdots,r_nQ_n)$，$E=m\oplus H_2(e(rP,kP))$。发送分组数据 $C=(H,E)$。

解密算法：用户 u_i 接收到分组数据 C 后，按照文献[1]中的方法首先确定出对应自己伪身份的项 r_iQ_i，计算 $E\oplus H_2(e(rP,s_ir_iQ_i+\sum_{j\neq i}r_jQ_j))$，即可得到明文信息 m。

值得注意的是，当预期用户集保持不变时，则发送的分组头中$(r_1P,r_2P,\cdots,r_nP)$也是保持不变的；当预期用户发生改变时，DS 按照(1)式重新计算对应的$(r_1,r_2,\cdots,r_l)$即可(l 为改变后的预期用户数量)。

5 正确性分析

只需证明 $e(rP,s_ir_iQ_i+\sum_{j\neq i}r_jQ_j)=e(rP,kP)$成立，即可证明上述解密过程是正确的。

证明：

$$\begin{aligned} &e(rP,s_ir_iQ_i+\sum_{j\neq i}r_jQ_j)\\ &=e(rP,s_ir_ia_iP+\sum_{j\neq i}r_ja_jP)\\ &=e(rP,kP) \end{aligned} \tag{2}$$

6 安全性分析

(1)非预期用户都不能对广播的消息进行解密，因为只有预期用户才拥有一个对应解密所需的秘密 s_i，$1\leqslant i\leqslant n$，非预期用户在不知道任何秘密 s_i，$1\leqslant i\leqslant n$ 的情况下显然是无法对消息进行解密的。同时，由于满足方程组(1)的解$(r_1,r_2,\cdots,r_n)$是唯一的，因此对应的 s_i，$1\leqslant i\leqslant n$ 也是唯一的，所以非预期用户通过随机方式解密成功的概率只有 $1/q$。同样的原因，任意非预期用户通过共谋也不能对消息进行解密。

(2)由分组数据可知，对同一组预期用户分组头中只有 rP 一项是变化的，而 r 的选取是随机的，是与 r_iQ_i，$1\leqslant i\leqslant n$ 相独立的；再者，非预期用户利用对应的明文可从 E 得到相应的 $H_2(e(rP,kP))$。但是由于 H_2 的单向性，其不能得到 $e(rP,kP)$的任何消息。这样，非预期用户在已知多项式数量的明密文对情况下，仍不能对新的广播信息进行解密。

(3)预期用户不能得到其他预期用户的解密钥。由式(2)知，预期用户 s_i 可以得到 $s_ir_iQ_i+\sum_{j\neq i}r_jQ_j=kP$，但是由于在 G_1 中解离散对数为困难问题，因此 s_i 不能得到对应的 k 和 r_ja_j，$1\leqslant j\leqslant n$，也就无法得到其他预期用户的解密钥。

7 效率分析

本方案中，加密过程需 $n+2$ 次标量乘法运算、一次矩阵运算、一次 weil 配对运算；解密过程需一次标量乘法运算、n 次 G_1 中加法运算、一次 weil 配对运算。在表 1 中我们给出了本方案与其他方案[2,4]广播一次信息所需的加解密运算量和传输分组长度的比较。

结束语 本文给出了一个新的类身份广播加密方案，同现有类似方案相比较，本方案在效率上得到了较大的改善。存在的问题是这些方案的分组长度都与用户数量有关，设计与用户无关的基于身份的广播加密方案尚需进一步研究。

表 1 本方案与文献[2]、[4]的性能比较

	标量乘法次数		Weil 配对次数		加法次数		分组头长度	矩阵运算次数	备注
	加密	解密	加密	解密	加密	解密			
方案[2]	2n	2(n−1)	1	4	*	2(n−1)	2(n−1)+3	DS 计算 2 次	
方案[4]	n+1	n	1	2	2n−2	n−1	n	每个用户计算 1 次	存在不安全
本方案	n+1	1	1	1	*	n	n+1	DS 计算 1 次	

注：“*”表示没有。

参 考 文 献

[1] Fiat A, Naor M. Broadcast encryption. In Advances in Cryptology // Crypto'93. Lecture Notes in Computer Science. Springer Verlag, 1994, 773: 480-491

[2] Lv Xixiang, Yang Bo. Traitor Tracing Using Identity Based Public-key Cryptography. Chinese Journal of Electronics, 2006, 15(4)

[3] Chien Hung-Yu. Comments and corrections: Comments on an Efficient ID-based Broadcast Encryption Scheme. IEEE Trans. on Broadcasting, 2007, 53(4): 809-810

[4] Du X, Wang Y, Ge J, et al. An ID-based broadcast encryption scheme for key distribution. IEEE Trans. on Broadcasting, 2005, 51(2): 264-266

[5] Boneh D, Franklin M. Identity-based encryption from the Weil pairing // Crypto'2001. LNCS 2139. Springer-Verlag, 2001: 213-229