适于任意深度电路结构的紧致属性基广播加密方案

张丽娜[1),2)] 杨 波[1),3)] 周彦伟[1)] 贾艳艳[2)]

[1)](陕西师范大学计算机科学学院 西安 710072)

[2)](西安科技大学计算机科学与技术学院 西安 710054)

[3)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

摘 要 为了简化传统的公钥加密体制,Shamir 于 1984 年提出了基于身份的加密方案.属性密码学由身份密码学发展而来,利用用户属性信息和相应的访问控制策略来替代机制中需要身份参与的运算.基于一般电路来表示访问策略及构造相关的属性密码方案是目前的研究热点和难点.2013 年 Garg 等人利用多线性映射和一般电路来描述访问策略,首次给出了基于一般电路能抵抗回溯攻击的属性基加密方案.受限伪随机函数的概念于 2013 年提出,利用其安全性功能,可以将其与双线性和多线性映射、不可区分性混淆、同态加密等技术相结合,在多种场景得到应用.如何将受限伪随机函数与其他密码技术相结合来构造新兴的密码协议和方案成为受限伪随机函数研究的重要课题.基于 Garg 等人的方案并将受限伪随机函数与基于电路的属性基相结合,文中基于现有的多线性映射给出了一个基于任意深度的一般电路访问结构的广播加密方案.主要创新点在于该方案的一般电路节点的深度 l' 不需要固定于电路的最大深度 l,只需要满足条件 $l'<l$ 即可,实现了一般电路中节点的跨层输入.该方案密文较短,与其他方案相比是密文紧致的,此外该方案不需要广播加密中的报头部件.该方案在标准模型下基于多线性判定性 Diffie-Hellman 假设被证明是具有选择安全性的.尽管在 2016 年的欧洲密码年会上,Hu 等人给出了攻破基于分级编码系统实现多线性映射方法的具体方案,但是基于多线性映射的构造和相关安全性模型仍在进一步完善和发展中.我们相信下阶段会有更实用安全的多线性映射实现方法,因此目前基于多线性映射原语的各类理论研究和实现方案仍具有较大的研究意义.

关键词 多线性映射;基于属性的密码学;选择安全;一般电路;广播加密

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2018.00452

Compact Attribute-Based Broadcast Encryption Scheme for General Circuits with Arbitrary Depth

ZHANG Li-Na[1),2)] YANG Bo[1),3)] ZHOU Yan-Wei[1)] JIA Yan-Yan[2)]

[1)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710072)

[2)](*Department of Computing Science and Technology, Xi'an University of Science and Technology, Xi'an* 710054)

[3)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

Abstract Identity-based encryption (IBE) scheme was proposed by Shamir in 1984 in order to simplify the traditional public key cryptography. Attributed-based encryption scheme is a special type of IBE. The identities could be replaced by the attributes and the corresponding access control policy. Designing access structure and related attribute-based encryption schemes for general circuit is difficult and has been a hot topic. It is really an interesting work to design schemes that be able to realize decryption policies representable as polynomial-size circuits. Based on the existence of multilinear maps, Garg et al. provided the first construction of attribute-based encryption (ABE) for general circuits which could resist the backtracking attack in 2013. Similarly, our

收稿日期:2016-06-02;在线出版日期:2016-12-01.本课题得到国家重点研发计划(2017YFB0802000)、国家自然科学基金(61572303,61772326)、中国科学院信息工程研究所信息安全国家重点实验室开放课题(2017-MS-03)、"十三五"国家密码发展基金(MMJJ20170216)、中央高校基本科研业务费项目(GK201702004)、榆林市科技计划产学研项目(2014CXY-08-01)资助.**张丽娜**,女,1981 年生,博士,副教授,中国计算机学会(CCF)会员,主要研究方向为密码学与信息安全.E-mail:zhangln_ecc@163.com.**杨 波**(通信作者),男,1963 年生,博士,教授,主要研究领域为密码学与信息安全.E-mail:byang@snnu.edu.cn.**周彦伟**,男,1986 年生,博士研究生,主要研究方向为密码学、匿名通信技术等.**贾艳艳**,女,1983 年生,博士,讲师,主要研究方向为密码学与信息安全.

constructions are based on the existence of multilinear maps and it could resist the backtracking attack. The concept of constrained pseudorandom functions (CPRF) were introduced in 2013, since then it had got a wide range of research. With the corresponding security feature, constrained pseudorandom function could be combined with other technologies such as the bilinear and multilinear maps, indistinguishability obfuscation and homomorphic encryption etc. and to be applied in a variety of application situation. Associating with the Garg's scheme and constrained pseudorandom functions, we propose an attribute-based broadcast encryption scheme for general circuits with arbitrary depth. In this scheme the depth of the general circuits l' could be smaller than the maximal depth l, instead of equaling to the maximum and achieve cross layer output. Our main construction exposition is for circuits that are layed and monotonic as usual. How to construct a nonmonotonic access structure is the next step in this research. Comparing to the existing works, the advantages of our scheme are short ciphertext and featuring compactness without adding the broadcast header. Essentially it is a symmetric broadcast encryption scheme and associated with constrained pseudorandom functions. Furthermore our construction is of the key-policy form that the encryption algorithm takes in the description of attributes and message and the key generation algorithm takes in the description of a circuit. Our scheme is proved to be selective security in the standard model under the multilinear decisional Diffie-Hellman assumption. We would have a further exploring on its application scenarios and try to improve its efficiency. Since 2013 multilinear maps serve as a basis for a wide range of cryptographic applications. However, it was found to be insecure in the face of so-called zeroizing attacks that crucially relied on the ability of the adversary to create encodings of 0 by Hu and Jia (Eurocrypt'16) in 2016. This result provides a new opportunity for the study of the realization and application of multi-linear maps in other directions. Some researchers proposed new "weak multilinear map models" that could capture all known polynomial-time attacks on GGH13. We believe that the related results open a stimulating opportunity to study new constructions using a multilinear map abstraction. There would be more practical and secure schemes appeared and building ABE for circuits based on multilinear maps would be one of the most exciting challenges.

Keywords　multilinear maps; attribute based encryption; selective security; general circuits; broadcast encryption

1　引　言

在传统的基于公钥基础设施 PKI(Public Key Infrastructure)的密码体制中,证书的产生、私钥证书的存储和公钥证书的认证等都需要较高的存储开销和安全机制.为了简化传统的公钥密码体制,Shamir 于 1984 年提出了基于身份的加密方案 IBE(Identity-Based Encryption)[1],该设计的概念为不使用任何证书,直接将用户的身份信息(甚至是任意字符串)作为公钥,以此来简化 PKI 中基于证书的密钥管理方案.直到 2001 年才由 Boneh 和 Franklin 提出了第一个比较实用的解决方案,称为 BF_IBE[2],该方案使用 Weil 配对技术,基于有效的可计算双线性映射点群构造,并证明了其安全性在随机预言模型下是适应性选择密文安全.此后,很多有效的基于身份的密码方案被提出和改进,这些公钥认证框架具有无公钥证书的优势,可以利用用户的身份信息如电子邮件地址、手机号码等唯一的身份标识作为公钥,不需要与公钥基础设施相关的各项存储和管理开销,可以节约大量资源,已成为传统公钥体制的有力替代.

属性密码学[3]由身份密码学发展而来,利用用户属性信息和相应的访问控制策略来替代机制中需要身份参与的运算.2006 年 Goyal 等人[4]给出了基于密钥策略的属性基加密方案,该方案基于树形结构设计了访问策略并将其嵌入秘密钥中.此后,基于属性的各类密码方案及其应用得到了广泛研究和发展.由于访问树的结构能够与布尔表达式和电路描述直接对应,因此如何利用一般电路来

表示访问策略是一个有意义的问题. 2013 年 Garg 等人在文献[5]中首次给出了基于一般电路能抵抗回溯攻击的属性基加密方案,该方案利用多线性映射基于一般电路来描述访问策略. 2015 年 Datta 等人[6]基于此方案进行了改进,给出了新的属性基加密方案和签密方案,该方案最大的优点是减少了密文的个数. 同年 Xu 等人[7]基于文献[5]给出了基于一般电路支持代理可验证的属性基混合加密方案. Hu 等人[8]于 2016 年给出了基于一般电路密钥策略的属性加密方案,该方案是支持跨层输出的. 这些方案均为标准模型下选择安全的. 此外,Garg 等人[9]和 Attrapadung[10]分别利用编码技术给出了基于多线性映射和编码的一般电路适应性安全方案. 在 2016 年的欧洲密码年会上,Hu 等人[11]给出了攻破基于分级编码系统实现多线性映射方法的具体方案,并证明了利用基于分级编码系统的多线性映射来构造各类高级密码应用也是不安全的. 此研究结论为多线性映射具体实现在其他方向的研究提供了新的契机,如文献[12]利用不可区分性混淆、同态加密和零知识证明结合基本困难问题来实现多线性映射群. 我们相信下阶段会有更实用安全的多线性映射实现方法,因此目前基于多线性映射原语的各类理论研究和实现方案仍具有较大的研究意义.

2013 年 Boneh 和 Waters[13],Kiayias 等人[14]和 Boyle 等人[15]提出了受限伪随机函数的基本概念. 文献[13]中 Boneh 等人基于双线性对和多线性对给出了受限伪随机函数的三种构造和基于此的三个应用范例,分别是基于左-右谓词结构的密钥交换机制,基于比特-固定谓词结构的广播加密机制和基于电路谓词结构的策略型密钥分发机制. 利用受限伪随机函数的性质,基于电路谓词结构来构造高效的属性基广播加密方案是本文的研究重点.

目前多线性映射和一般电路相结合的高效、实用方案是研究热点之一,如何构造标准模型下的全安全方案及其安全性证明也仍然需要进一步深入探讨,如何将新提出的受限伪随机函数及其性质与各类应用相结合也是值得研究的问题.

2 背景知识

2.1 双线性映射

定义 1[2]. 令 $\mathbb{G}_1$,$\mathbb{G}_2$ 为两个阶为大素数的乘法循环群,$\mathbb{G}_1$ 到 $\mathbb{G}_2$ 的双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$ 应满足如下 3 个性质:

(1) 双线性. 对于任意的 $P,Q\in\mathbb{G}_1$,$a,b\in\mathbb{Z}_p$,有 $e(P^a,Q^b)=e(P,Q)^{ab}$.

(2) 非退化性. 存在 $P\in\mathbb{G}_1$,使得 $e(P,P)\neq 1$.

(3) 可计算性. 对于任意的 $P,Q\in\mathbb{G}_1$,$a,b\in\mathbb{Z}_p$,存在多项式时间的算法能有效计算 $e(P^a,Q^b)\in\mathbb{G}_2$.

2.2 多线性映射

定义 2[16]. 假设存在一个群产生算法 $\mathcal{G}$,通过输入安全参数 λ 和一个正整数 T 来确定其级数,$\mathcal{G}(1^\lambda,\kappa)$ 输出一系列的群 $\boldsymbol{G}=(\mathbb{G}_1,\cdots,\mathbb{G}_\kappa)$,其中每一个群的阶均为大素数 p(这里 $p>2^\lambda$),且 g_i 是 $\mathbb{G}_i$ 的正规生成元,这里记 $g=g_1$.

假设存在一个多线性映射集合 $\{e_{i,j}:\mathbb{G}_i\times\mathbb{G}_j\rightarrow\mathbb{G}_{i+j}\mid i,j\geq 1;i+j\leq\kappa\}$,对于每对有效的 i,j,均存在一系列的双线性映射

$$e_{i,j}(g_i^a,g_j^b)=g_{i+j}^{ab},\ \forall a,b\in\mathbb{Z}_p,$$

则称此映射集合为多线性映射.

假设 1. κ-多线性判定性 Diffie-Hellman(κ-MDDH)假设. 一个挑战者运行 $\mathcal{G}(1^\lambda,\kappa)$ 来生成阶为大素数 p 的一系列群及其对应的生成元,然后选择随机数 $C_1,C_2,\cdots,C_{k+1}\in ZP$. κ-MDDH 假设是指给定 $(g,g^{c_1},\cdots,g^{c_{\kappa+1}})$,区分 T 和 T' 是困难的,其中 $T=g_\kappa^{\prod_{j\in[1,\kappa+1]}c_j}\in\mathbb{G}_\kappa$,$T'$ 为从 $\mathbb{G}_\kappa$ 中随机选择的一个群元素,其获胜优势不会超过基于安全参数 λ 的一个可忽略概率.

2.3 访问结构[17]

设 $\{P_1,\cdots,P_n\}$ 为系统参与者的 n 个属性集合,$\mathbb{A}\subseteq 2^{\{P_1,\cdots,P_n\}}$,$B,C$ 表示属性集合的子集. 假如对于任意的 B,C,若 $B\in\mathbb{A}$ 且 $B\subseteq C$,则 $C\in\mathbb{A}$,则称 $\mathbb{A}$ 是单调的. 访问结构为集合 $\{P_1,\cdots,P_n\}$ 的所有非空子集构成的单调集合,即 $\mathbb{A}\subseteq 2^{\{P_1,\cdots,P_n\}}\setminus\{\phi\}$. 对于 $\forall D\in\mathbb{A}$,称 D 为授权集合,对于 $D\notin\mathbb{A}$,称 D 为非授权集合.

2.4 电 路

本节由 2.3 节给出的访问结构继续给出一般电路的相关概念,并对一般电路[5]的描述进行定义.

电路一般由节点和线路组成. 每个叶子节点对应一个属性,非叶子节点由 AND 门、OR 门和 NOT 门构成,线路则是电路中连接两个节点的连线. 本文所述电路为只包含均为两个输入和一个输出的 AND 门和 OR 门的单调电路,即该电路为只有一个输出门的层级电路. 本文中对于电路的描述用六元组 $f=(n,q,l,A,B,GateType)$ 表示,指该电路有 n 条输入线,q 个输入端口,电路的最大深度为 l,电路的输出线为 $n+1$ 条. 用 w 表示电路中的某个节点,

$A:Gates\to$ Wires/outputwire 表示一个函数，用 $A(w)$ 表示 w 的第一条输入线. 同理，$B(w)$ 表示 w 的第二条输入线. 最后 $GateType:\{\text{AND},\text{OR}\}$ 被用来表示这个电路的类型是与门还是或门. 此外还需要定义一个函数 $depth:W\to\{1,\cdots,l\}$，当 w 是输入端口时，$depth(w)=1$. 当 w 是非输入端口时，用变量 j 表示电路 w 的深度，则 $depth(w)=j$. $f_w(\boldsymbol{x})$ 表示以 w 为根节点的电路输出结果.

下面描述本文中基于一般电路的访问结构，事实上一般电路的描述与访问结构树天然对应[4]. 当电路对应一个映射 $f:\{0,1\}^n\to\{0,1\}$ 时，电路的 n 个输入对应一个 n 维向量 $\boldsymbol{x}\in\{0,1\}^n$，电路根据 $\boldsymbol{x}$ 的取值进行计算，最后电路根节点的输出为 0 或 1，也即当属性集合的向量 $\boldsymbol{x}$ 满足电路描述的访问结构时，$f(\boldsymbol{x})=1$，即根结点的输出为 1.

以下举例说明属性向量与基于一般电路访问结构的对应关系. 如图 1 所示为某一给定的一般电路. 该电路中属性的数量也即电路的输入线数量 $n=5$，输入端口 $q=4$，电路的深度 $l=4$. 非叶子节点类型和相应深度可分别如表 1 所示.

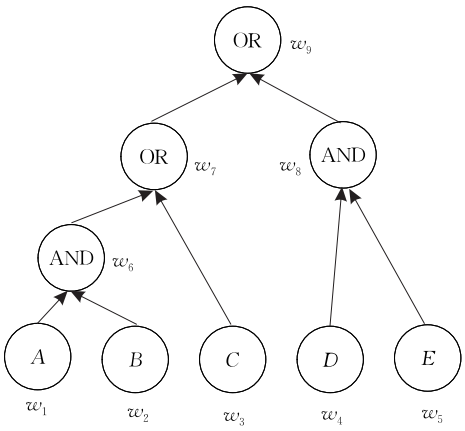

图 1　范例电路

表 1　范例电路中各节点类型及深度

节点类型	节点深度
$GateType(w_6)=\text{AND}$	$depth(w_6)=1$
$GateType(w_7)=\text{AND}$	$depth(w_7)=1$
$GateType(w_8)=\text{OR}$	$depth(w_8)=2$
$GateType(w_9)=\text{OR}$	$depth(w_9)=3$

当属性向量为 $\boldsymbol{x}=(00100)$ 时，对应的中间节点的电路输出可计算得 $f_{w_6}(\boldsymbol{x})=0$，$f_{w_7}(\boldsymbol{x})=1$，$f_{w_8}(\boldsymbol{x})=0$，$f_{w_9}(\boldsymbol{x})=1$，因此可计算根节点对应的输出值 $f(\boldsymbol{x})=f(00100)=1$. 表示对应的属性集合 $\{C\}$ 满足访问结构. 具体情况如图 2 所示.

同理，当属性向量为 $\boldsymbol{x}=(11000)$ 时，对应的电路输出可计算得 $f_{w_6}(\boldsymbol{x})=1$，$f_{w_7}(\boldsymbol{x})=1$，$f_{w_8}(\boldsymbol{x})=0$ 和 $f_{w_9}(\boldsymbol{x})=1$，因此可得 $f(\boldsymbol{x})=f(11000)=1$. 表示对应的属性集合 $\{A,B\}$ 也满足访问结构.

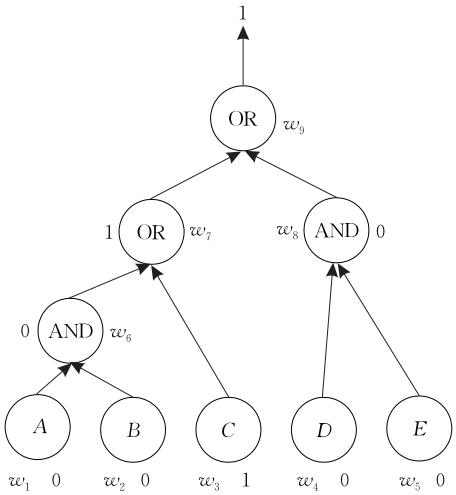

图 2　$x=(00100)$ 时的电路输出范例

但是当属性向量为 $\boldsymbol{x}=(10010)$ 时，对应的电路输出可计算得 $f_{w_6}(\boldsymbol{x})=0$，$f_{w_7}(\boldsymbol{x})=0$，$f_{w_8}(\boldsymbol{x})=0$ 和 $f_{w_9}(\boldsymbol{x})=0$，因此可得 $f(\boldsymbol{x})=f(10010)=0$. 表示对应的属性集合 $\{A,D\}$ 不满足访问结构.

2.5　受限伪随机函数

受限伪随机函数由伪随机函数[18]发展而来，其基本概念于 2013 年分别由文献[13-15]提出. 所谓的受限伪随机函数[13]是指允许从伪随机函数的主密钥 k 中派生出一个受限密钥 k_s，这个受限密钥 k_s 对应于定义域 $\mathcal{X}$ 的一个子集 $S\subseteq\mathcal{X}$. 拥有受限密钥 k_s 的合法用户可以在多项式时间内，对于 $\forall\boldsymbol{x}\in S$ 计算 $F(k,\boldsymbol{x})$. 反之对于没有受限密钥 k_s 的非法用户，无法区分 $F(k,\boldsymbol{x})$ 与任意给定的随机数.

一个基本的受限伪随机函数受限于一个集合 $S\subseteq 2^{\mathcal{X}}$，由一个附加的密钥空间 k_c、两个附加的算法 $F.\text{constrain}$ 和 $F.\text{eval}$ 组成.

$F.\text{constrain}(k,S)$ 算法输入为一个伪随机函数的密钥 k 和集合描述 $S\in\mathcal{S}$，算法输出为受限密钥 $k_s\in k_c$. 对于 $\forall\boldsymbol{x}\in S$，此受限密钥 k_s 可以被用来计算 $F(k,\boldsymbol{x})$，反之当 $\boldsymbol{x}\notin S$ 时，利用 k_s 无法计算 $F(k,\boldsymbol{x})$.

$F.\text{eval}(k_s,\boldsymbol{x})$ 算法输入为受限密钥 $k_s\in k_c$ 和 $\boldsymbol{x}\in S$. 假如 k_s 是伪随机函数的密钥 k 利用算法 $F.\text{constrain}(k,S)$ 派生出的有效受限密钥，则利用 $F.\text{eval}(k_s,\boldsymbol{x})$ 可计算得到 $F(k,\boldsymbol{x})$ 的正确结果. $F.\text{eval}(k_s,\boldsymbol{x})$ 的具体描述如下：

$$F.\text{eval}(k_s,\boldsymbol{x})=\begin{cases}F(k,\boldsymbol{x}), & \boldsymbol{x}\in S\\ \perp, & \text{其他}\end{cases}.$$

定义 3. 比特-固定的受限伪随机函数.

令 $\mathcal{X}=\{0,1\}^n$ 是伪随机函数的定义域. 对于向量 $\boldsymbol{v}\in\{0,1,?\}^n$,令 $S_v\subseteq\mathcal{X}$ 是 n 比特长的字符串,当满足 $\boldsymbol{v}$ 在所有的坐标都有 $v_i\neq?$ 时,可称 S_v 对于 $\boldsymbol{v}$ 是比特-固定的.

由比特-固定的受限伪随机函数定义可知,对于每一个形式为 $\{0,1\}^n$ 的子集 $S\subseteq\mathcal{X}$,均有一个受限密钥 K_S,使得对于 $\boldsymbol{x}\in S$ 能够计算得到 $F(k,\boldsymbol{x})$,但是对于 $\boldsymbol{x}\notin S$ 则无法计算.

定义 4. 比特-固定的谓词结构.

令 $F:K\times\{0,1\}^n\rightarrow\mathcal{Y}$ 是一个伪随机函数. 则可为向量 $\boldsymbol{v}\in\{0,1,?\}^n$ 定义一个谓词结构

$$p_v^{(\mathrm{BF})}:\{0,1\}^n\rightarrow\{0,1\},$$

使得满足特定比特形式的受限密钥 k_v,能够在所有点 $\boldsymbol{x}$ 计算得到 $F(k,\boldsymbol{x})$. 对于所有 $i=1,\cdots,n$,具体结构如下:

$$p_v^{(\mathrm{BF})}(\boldsymbol{x})=1\Leftrightarrow v_i=x_i\text{ 或 }v_i=?.$$

假如 $F:K\times\{0,1\}^n\rightarrow\mathcal{Y}$ 受限于满足谓词结构 $p_v^{(\mathrm{BF})}:\{0,1\}^n\rightarrow\{0,1\}$ 的集合,则称其满足比特-固定的结构.

3 属性基广播加密系统

3.1 模 型

广播加密方案[13,19]由 3 个随机算法组成. 下述方案中 num 表示系统中的用户数目,n 表示系统中用户属性的最大个数,可以通过对系统中每个用户的属性集合描述进行编码,得到长度为 n 的二进制序列串 $\{0,1\}^n$. 方案具体描述如下:

(1) $(bk,(d_1,\cdots,d_m))\leftarrow\mathrm{Setup}(1^\lambda,num)$. 系统建立算法 Setup 的输入为安全参数 λ 和系统最大用户数目 num. 输出为 num 个秘密钥 $d_1,\cdots,d_{num}$ 和一个广播密钥 bk. 对于 $i=1,\cdots,num$,秘密钥 d_i 对应于接收者 i.

(2) $(hdr,k)\leftarrow\mathrm{Encrypt}(bk,S)$. 加密算法 Encrypt 的输入为广播者的密钥 bk 和接收者属性集合描述 S. 算法输出为一对参数 (hdr,k),这里 hdr 为广播数据头,$k\in K$ 是选自密钥空间 K 的消息加密密钥.

令 $m\in\{0,1\}^*$ 为待广播的消息,当广播者需要将消息 m 广播给符合属性集合 S 的用户时,需要先利用加密算法 $(hdr,k)\leftarrow\mathrm{Encrypt}(bk,S)$ 得到加密密钥 k,c_m 是利用对称密钥 k 对消息 m 进行加密得到的密文. 最后广播数据由 (S,hdr,c_m) 组成.

(3) $k\leftarrow\mathrm{Decrypt}(S_i,d_i,S,hdr)$. 解密算法 Decrypt 输入用户 i 所对应的属性集合描述 S_i、用户 i 对应的秘密钥 d_i、接收者属性集合描述 S 以及广播头 hdr. 根据 2.5 节对比特-固定谓词结构的描述,可定义受限集合为合法接收者属性集合 S 所对应的编码,假如对于比特-固定结构的谓词 $p:\{0,1\}^n\rightarrow\{0,1\}$,假如用户属性集合满足 $p(S_i)=1$,则用户能够利用其秘密钥 d_i 通过计算得到对消息进行加密的对称密钥 $k\in K$. 然后用户 i 可以利用 k 来解密广播主体 c_m,恢复其包含的信息 m.

由上述系统模型可知,广播加密算法中所用秘密钥只有广播者自己掌握,因此该方案属于对称广播加密方案. 该广播加密系统是正确的,意味着对于接收者属性集合描述 S 和所有的 $p(S_i)=1$,应满足对任意

$$(bk,(d_1,\cdots,d_n))\xleftarrow{R}\mathrm{Setup}(1^\lambda,n),$$

$$(hdr,k)\xleftarrow{R}\mathrm{Encrypt}(bk,S),$$

则有 $\mathrm{Decrypt}(S_i,d_i,S,hdr)=k$.

3.2 安全性定义

属性基广播加密系统的语义安全[13,19]是指假如一个敌手获得了它对于所选的 $p(S_i)=1$ 对应的接收者秘密钥 d_i,仍不能够攻破用于挑战的接收者属性集合 S_i^* 的广播密文的语义安全. 敌手与挑战者的交互游戏描述如下:

(1) 系统建立阶段. 首先由敌手向挑战者输出一个接收者属性集合描述 S_i^*. 挑战者运行 $(bk,(d_1,\cdots,d_n))\xleftarrow{R}\mathrm{Setup}(1^\lambda,n)$,并将公共参数发送给敌手.

(2) 问询阶段 1. 在本阶段敌手可以向挑战者进行两类问询,具体描述如下:

① $\mathrm{RK}(S_i)$ 是一个接收者秘密钥问询,输入为 S_i,输出为 d_i.

② $\mathrm{SK}(S)$ 是一个加密问询,输入为合法接收者属性集合 S,输出为加密广播消息的对称密钥 k.

这里要求接收者属性集合 S_i 与系统建立阶段确定的待挑战属性集合 S_i^* 不相同.

(3) 挑战阶段. 输入为在系统建立阶段确定的接收者属性集合 S_i^*,选择随机比特 $b\in\{0,1\}$,计算 $k_{1-b}\xleftarrow{R}K$ 和 $(hdr,k_b)\xleftarrow{R}\mathrm{Encrypt}(bk,S)$,然后将 (hdr,k_0,k_1) 返回给攻击者.

(4) 问询阶段 2. 与问询阶段 1 相同.

(5) 猜测阶段. 最后敌手输出一个猜测 b'. 假如 $b=b'$,则敌手赢得游戏,其获胜概率可定义为 $AdvBE_A(\lambda)=|2\Pr[b=b']-1|$.

在上述安全模型中,有两类密钥的问询:一类是

广播接收者的秘密钥问询；另一类是协商出的密钥问询. 事实上，该属性基广播加密系统安全模型中的接收者秘密钥问询谕言机 RK 可直接对应于 2.4 节受限伪随机函数定义中的谕言机 $F.\mathrm{constrain}$，加密问询的谕言机 SK 对应于受限伪随机函数定义中的谕言机 $F.\mathrm{eval}$. 受限伪随机函数的安全性定义具体可见文献[13].

定义 5.　假如对于所有概率多项式时间敌手 $\mathcal{A}$，函数 $AdvBE_A(\lambda)$ 是可忽略不计的，则这个广播加密系统是语义安全的.

4　紧的适于任意深度电路结构的属性基广播加密方案

本文借鉴了受限伪随机函数[13]和文献[6]的设计思路，利用多线性映射将用户的属性在指数上进行联合计算，密文量只有 2 个群元素，相较于以前方案[5,8]在每个密文中为每个属性生成一个群元素参数的方法，在密文的存储量上有显著下降，相较而言密文紧致.

在设计中本文对广播加密系统中每个用户的属性集合描述 S_i 进行编码，得到长度为 n 的二进制序列串 $U_x=\{0,1\}^n$. 编码规则为假定系统中用户属性的最大个数为 n，属性集合可表示为 $\{1,2,\cdots,n\}$. 当用户拥有编号为 i 的属性时，可将 U_x 的第 i 比特位置为 1. 相应的，当用户没有编号为 i 的属性时，可将 U_x 的第 i 比特位置为 0. 设广播加密中合法接收用户的属性集合描述的编码为 $\boldsymbol{x}\in\{0,1\}^n$，用户的属性编码 U_x 受限于合法接收用户的属性编码 $\boldsymbol{x}$，即 $p_x^{(\mathrm{BF})}(U_x)=1$.

在 2.3 节和 2.4 节，给出了访问结构的定义和电路的相关概念. 本方案中电路对应一个映射 $f:\{0,1\}^n\to\{0,1\}$，电路的 n 个输入对应一个 n 维向量 $\boldsymbol{x}\in\{0,1\}^n$，与用户的属性集合描述的编码一致，即当用户拥有第 i 个属性时，电路的第 i 个输入为 1，否则为 0，最后电路根节点的输出为 0 或 1，也即当用户属性集合满足电路描述的访问结构时，则 $f(\boldsymbol{x})=1$，即根结点的输出为 1.

4.1　方案描述

现在我们给出基于一般电路的属性基广播加密的具体方案. 方案中电路节点的深度 l' 不需要固定于电路最大深度 l，只需要满足条件 $l'\le l$ 即可. 本文结合文献[13]中受限伪随机函数的概念，给出了适用于满足 $l'\le l$ 条件下任意深度电路结构的广播加密方案. 方案由四部分组成，分别为 Setup，KeyGen，Encrypt 和 Decrypt，具体方案说明如下：

$\mathrm{Setup}(1^\lambda,n,l)$

系统在初始化时首先输入安全参数 λ，最大属性数目 n 和电路的最大深度 l. 运行 $\mathcal{G}(1^\lambda,\kappa=n+l)$ 输出一系列阶为大素数 p 的群 $\boldsymbol{G}=(\mathbb{G}_1,\cdots,\mathbb{G}_\kappa)$，对应生成元分别为 $g_1,\cdots,g_\kappa$，这里不妨令 $g=g_1$. 随机选择一个指数 $\alpha\in\mathbb{Z}_p$，选择 n 个随机数对 $(d_{1,0},d_{1,1}),\cdots,(d_{n,0},d_{n,1})\in\mathbb{Z}_p^2$，计算 $D_{i,\beta}=g^{d_{i,\beta}}$，这里 $i\in[1,n]$，$\beta\in\{0,1\}$.

系统发布的公开参数 PP 为一系列群 $\boldsymbol{G}$ 的描述和 $\{D_{i,\beta}\}_{i=1,\cdots,n;\beta\in\{0,1\}}$.

主密钥 $MK=g_l^\alpha$ 由系统秘密保存.

$\mathrm{KeyGen}(MK,f=(n,q,l,A,B,GateType))$.

密钥生成算法的输入为公共参数 PP，主密钥 MK 和解密策略的电路描述 f. 该算法首先选择 $n+q-1$ 个随机数 $r_1,\cdots,r_{n+q-1}\in\mathbb{Z}_p$，与电路中的每个节点 w 相对应，然后令 $r_{n+q}=\alpha$，根据 w 的不同类型（可能为输入线，AND 门，或者是 OR 门），生成 w 对应的密钥组件.

(1) Input wire

如果 $w\in[1,n]$，则说明其为第 w 个输入线，密钥生成算法生成相应的密钥组件为

$$K_w=g_2^{r_w d_{w,1}}.$$

(2) OR gate

假如 $w\in Gates$ 且 $GateType(w)=\mathrm{OR}$ 时，设节点 w 的深度为 $j=depth(w)$，$A(w)$ 和 $B(w)$ 的深度分别为 d_1 和 d_2（$1\le d_1,d_2\le j-1$），密钥生成算法选择随机数 $a_w,b_w\in\mathbb{Z}_p$，生成密钥组件为

$$K_{w,1}=g_{j-d_1}^{a_w},\ K_{w,2}=g_{j-d_2}^{b_w},$$
$$K_{w,3}=g_j^{r_w-a_w\cdot r_{A(w)}},\ K_{w,4}=g_j^{r_w-b_w\cdot r_{B(w)}}.$$

(3) AND gate

假如 $w\in Gates$ 且 $GateType(w)=\mathrm{AND}$ 时，同样不妨设节点 w 的深度为 $j=depth(w)$，$A(w)$ 和 $B(w)$ 的深度分别为 d_1 和 d_2（$1\le d_1,d_2\le j-1$），密钥生成算法选择随机数 $a_w,b_w\in\mathbb{Z}_p$，然后生成密钥组件为

$$K_{w,1}=g_{j-d_1}^{a_w},\ K_{w,2}=g_{j-d_2}^{b_w},\ K_{w,3}=g_j^{r_w-a_w\cdot r_{A(w)}-b_w\cdot r_{B(w)}}.$$

$\mathrm{Encrypt}(MK,S)$

该算法的输入参数为主密钥 MK，合法接收用户的属性集合 S，对应的编码为 $\boldsymbol{x}\in\{0,1\}^n$. 令 x_i 表示 $\boldsymbol{x}$ 的第 i 比特，那么可利用主密钥和公共参数生成对称密钥：

$$k=F(MK,\boldsymbol{x})=(g_{\kappa=n+l})^{\alpha\prod_{i\in[1,n]}d_{i,x_i}}.$$

令 C_m 是利用对称密钥 k 对消息 m 进行加密的密文，则最后输出的广播数据为 (S,hdr,c_m). 特别的，在本方案中 hdr 为空.

Decrypt(k_f,S)

算法输入为电路描述 $f=(n,q,l,A,B,GateType)$ 对应的密钥 k_f 和合法接收用户对应的属性集合 S. 这里可设 S 对应的编码为 $\boldsymbol{x}\in\{0,1\}^n$.

本算法的主要目的是利用用户的秘密钥计算出对称密钥 $k=F(MK,\boldsymbol{x})=(g_{\kappa=n+l})^{\alpha\prod_{i\in[1,n]}d_{i,x_i}}$. 利用电路性质，可以从电路的底部开始，由下往上进行计算. 考虑深度为 $l'\leq l$ 的线路 w，如果 $f_w(\boldsymbol{x})=1$，则本算法可利用输入参数计算 $E_w=(g_{j+n})^{r_w\prod_i d_{i,x_i}}$（这里 j 为 w 的深度）作为 k 的中间值，反之如果 $f_w(\boldsymbol{x})=0$，则直接停止计算. 本算法从 E_1 开始，最终计算出 $E_{n+q}=F(MK,\boldsymbol{x})$，即为对称密钥 k 的值.

下面展示当 $f_w(\boldsymbol{x})=1$ 时，本算法如何利用输入参数来计算 E_w，同密钥生成算法类似，也需要根据 w 的不同类型（可能为输入线，AND 门，或者是 OR 门），分 3 种情况进行讨论.

(1) Input wire

假如 $w\in[1,n]$，则说明其为第 w 个输入线，假如 $x_w=f_w(\boldsymbol{x})=1$，则通过公共参数 $D_{i,\beta}=g^{d_{i,\beta}}(i\in[1,n],\beta\in\{0,1\})$ 和密钥 K_w，利用线性对运算可计算：

$$\begin{aligned}E_w&=e(K_w,g_{n-1}^{\prod_{i\in[1,n]\neq w}d_{i,x_i}})\\&=e(g_2^{r_w d_{w,1}},g_{n-1}^{\prod_{i\in[1,n]\neq w}d_{i,x_i}})\\&=g_{n+1}^{r_w\prod_{i\in[1,n]}d_{i,x_i}}.\end{aligned}$$

(2) OR gate

假如 $w\in Gates$ 且 $GateType(w)=\text{OR}$ 时，设节点 w 的深度为 $j=depth(w)$，$A(w)$ 和 $B(w)$ 的深度分别为 d_1 和 d_2（$1\leq d_1,d_2\leq j-1$）. 假如 $f_w(\boldsymbol{x})=1$，则通过公共参数 $D_{i,\beta}=g^{d_{i,\beta}}(i\in[1,n],\beta\in\{0,1\})$ 和相应的密钥组件，利用线性对的运算，可分两种情况进行计算.

当 OR 门的有效输入为 w 的第一条输入线 $A(w)$ 时：

$$\begin{aligned}E_w&=e(E_{A(w)},K_{w,1})\cdot e(g_n^{\prod_{i\in[1,n]}d_{i,x_i}},K_{w,3})\\&=e(g_{n+d_1}^{r_{A(w)}\prod_{i\in[1,n]}d_{i,x_i}},g_{j-d_1}^{a_w})\cdot e(g_n^{\prod_{i\in[1,n]}d_{i,x_i}},g_j^{r_w-a_w\cdot r_{A(w)}})\\&=g_{n+j}^{r_w\prod_{i\in[1,n]}d_{i,x_i}}.\end{aligned}$$

当 OR 门的有效输入为 w 的第 2 条输入线 $B(w)$ 时，同理可计算：

$$\begin{aligned}E_w&=e(E_{B(w)},K_{w,2})\cdot e(g_n^{\prod_{i\in[1,n]}d_{i,x_i}},K_{w,4})\\&=e(g_{n+d_2}^{r_{B(w)}\prod_{i\in[1,n]}d_{i,x_i}},g_{j-d_1}^{b_w})\cdot e(g_n^{\prod_{i\in[1,n]}d_{i,x_i}},g_j^{r_w-b_w\cdot r_{B(w)}})\\&=g_{n+j}^{r_w\prod_{i\in[1,n]}d_{i,x_i}}.\end{aligned}$$

(3) AND gate

假如 $w\in Gates$ 且 $GateType(w)=\text{AND}$ 时，设节点 w 的深度为 $j=depth(w)$，$A(w)$ 和 $B(w)$ 的深度分别为 d_1 和 d_2（$1\leq d_1,d_2\leq j-1$），假如 $f_w(\boldsymbol{x})=1$，则通过公共参数 $D_{i,\beta}=g^{d_{i,\beta}}(i\in[1,n],\beta\in\{0,1\})$ 和相应的密钥组件，利用线性对的运算，可计算：

$$\begin{aligned}E_w&=e(E_{A(w)},K_{w,1})\cdot e(E_{B(w)},K_{w,2})\cdot\\&\quad e(g_n^{\prod_{i\in[1,n]}d_{i,x_i}},K_{w,3})\\&=e(g_{n+d_1}^{r_{A(w)}\prod_{i\in[1,n]}d_{i,x_i}},g_{j-d_1}^{a_w})\cdot(g_{n+d_2}^{r_{B(w)}\prod_{i\in[1,n]}d_{i,x_i}},g_{j-d_2}^{b_w})\cdot\\&\quad e(g_n^{\prod_{i\in[1,n]}d_{i,x_i}},g_j^{r_w-a_w\cdot r_{A(w)}-b_w\cdot r_{B(w)}})\\&=g_{n+j}^{r_w\prod_{i\in[1,n]}d_{i,x_i}}.\end{aligned}$$

当电路深度 $l'=l$ 时，可直接计算 $E_{n+q}=g_{n+l'}^{r_{n+q}\prod_{i\in[1,n]}d_{i,x_i}}=g_{n+l}^{\alpha\prod_{i\in[1,n]}d_{i,x_i}}=F(MK,\boldsymbol{x})$；

当电路深度 $l'<l$ 时，可通过计算得到 $E_{n+q}=g_{n+l'}^{r_{n+q}\prod_{i\in[1,n]}d_{i,x_i}}=g_{n+l'}^{\alpha\prod_{i\in[1,n]}d_{i,x_i}}$，再将 E_{n+q} 与 $g_{l-l'}$ 进行对运算，同样可得到 $g_{n+l}^{\alpha\prod_{i\in[1,n]}d_{i,x_i}}=F(MK,\boldsymbol{x})$.

因此当用户对应的属性集合编码 $\boldsymbol{x}\in\{0,1\}^n$ 满足电路描述即 $f_w(\boldsymbol{x})=1$ 时，本算法输出加密消息的对称密钥 $k\in K$. 用户可以利用对称密钥 k 来解密广播主体 c_m，得到其包含的信息 m.

4.2 安全性证明

现在证明 4.1 节中所给方案的安全性. 我们将展示对于属性个数为 n，任意电路深度为 $l'\leq l$ 的系统，假如 $\kappa=n+l$ 的多线性判定性 Diffie-Hellman（κ-MDDH）假设成立，则通过选择合适的系列群及其相关安全参数，我们构造的算法是安全的.

定理 1. 假如存在一个多项式时间的攻击算法 $\mathcal{A}$ 以优势 $\varepsilon(\lambda)$ 攻破 4.1 节中基于电路结构的属性基广播加密方案，那么必然存在一个多项式时间的敌手 $\mathcal{B}$ 以优势 $\varepsilon(\lambda)/2^n$ 攻破 $\kappa=n+l$ 的多线性判定性 Diffie-Hellman（κ-MDDH）假设.

证明. 算法 $\mathcal{B}$ 收到一个 $\kappa=n+l$-MDDH 的挑战，具体包括：一系列的群描述 $\boldsymbol{G}$，相应的生成元

$g=g_1, g^{c_1}, \cdots, g^{c_{k+1}}$ 和 T，这里 T 的值是 $g_k^{\prod_{j\in[1,k+1]} c_j}$ 或 $\mathbb{G}_\kappa$ 中的一个随机元素. $\mathcal{B}$ 选择一个随机数 $\boldsymbol{x}^*\in\{0,1\}^n$，然后对于 $i\in\{1,2,\cdots,n\}$ 和 $\beta\in\{0,1\}$，选择随机数集合 $z_1,\cdots,z_n$ 来为 $D_{i,\beta}$ 赋值. 其规则为

$$D_{i,\beta}=\begin{cases} g^{c_i}, & x_i^*=\beta \\ g^{z_i}, & x_i^*\neq\beta \end{cases}.$$

通过这种方式，可以将需要进行挑战的 x_i^* 所对应的 $D_{i,\beta}$ 用定理 1 里 κ-MDDH 假设的已知条件 g^{c_i} 来赋值，将不需要进行挑战的普通位所对应的 $D_{i,\beta}$ 用已知的 g^{z_i} 来赋值. 这也意味着，隐含地将秘密钥 $d_{i,\beta}$ 设置为

$$d_{i,\beta}=\begin{cases} c_i, & x_i^*=\beta \\ z_i, & x_i^*\neq\beta \end{cases}.$$

此外也可由上式知，隐含着将主密钥指数上的秘密值 α 设置为 $\alpha=c_{n+1}\cdot c_{n+2}\cdots c_{n+1+l}$.

KeyGen. 在本阶段，攻击者将进行电路描述 $f=(n,q,l',A,B,GateType)$ 所对应的秘密钥问询，这里要求 $f(\boldsymbol{x}^*)=0$. 若 $f(\boldsymbol{x}^*)=1$，则算法终止，并输出一个随机值. 若 $f(\boldsymbol{x}^*)=0$，谕言机输出电路 f 所对应的秘密钥.

下面描述如何为每一个节点 w 构造密钥组件，这里仍然根据 w 的不同类型(可能为输入线、OR 门或者 AND 门)进行讨论.

(1) Input wire

若 $w\in[1,n]$，则说明其为第 w 条输入线.

如果 $f_w(\boldsymbol{x}^*)=1$，则选择随机数 r_w，可直接模拟密钥组件为

$$K_w=e(g^{r_w},D_{i,x_i^*})=g_2^{r_w d_{w,1}}.$$

如果 $f_w(\boldsymbol{x}^*)=0$，则选择随机数 $\eta_w\in\mathbb{Z}_p$，由于 $g^{c_{n+1}}, g^{c_{n+2}}$ 均为假设中的已知条件，通过设置 $g^{r_w}=e(g^{c_{n+1}},g^{c_{n+2}})\cdot g_2^{\eta_w}$ 可以隐含地将 r_w 设置为 $c_{n+1}c_{n+2}+\eta_w$. 由于 η_w 为随机值，因此 r_w 也可看做随机值. 利用选择的随机数 z_i 可模拟密钥组件为

$$K_w=(e(g^{c_{n+1}},g^{c_{n+2}})\cdot g_2^{\eta_w})^{z_i}=g_2^{r_w d_{w,1}}.$$

(2) OR gate

假如 $w\in Gates$ 且 $GateType(w)=\text{OR}$ 时，设节点 w 的深度为 $j=depth(w)$，$A(w)$ 和 $B(w)$ 的深度分别为 d_1 和 d_2 ($1\leq d_1,d_2\leq j-1$).

如果 $f_w(\boldsymbol{x}^*)=1$，则可直接选择随机数 $a_w,b_w,r_w\in\mathbb{Z}_p$，模拟密钥组件为

$$K_{w,1}=g_{j-d_1}^{a_w},\ K_{w,2}=g_{j-d_2}^{b_w},$$
$$K_{w,3}=g_j^{r_w-a_w\cdot r_{A(w)}},\ K_{w,4}=g_j^{r_w-b_w\cdot r_{B(w)}}.$$

如果 $f_w(\boldsymbol{x}^*)=0$，则随机选择 $\eta_w,\varphi_w,\phi_w\in\mathbb{Z}_p$，由于 $g^{c_{n+1}},g^{c_{n+2}},\cdots,g^{c_{n+j+1}}$ 是假设中的已知条件，通过设置 $g^{a_w}=g^{c_{n+j+1}}\cdot g^{\varphi_w}$，$g^{b_w}=g^{c_{n+j+1}}\cdot g^{\phi_w}$ 和 $g_j^{r_w}=e(g^{c_{n+1}},g^{c_{n+2}},\cdots,g^{c_{n+j}})\cdot g_j^{\eta_w}$ 可以隐含设置 $a_w=c_{n+j+1}+\varphi_w$，$b_w=c_{n+j+1}+\phi_w$，也可设置 r_w 为 $c_{n+1}c_{n+2}\cdots c_{n+j}+\eta_w$. 此外利用类似方法还可通过设置 $g_{d_1}^{r_{A(w)}}$ 为 $g_{d_1}^{c_{n+1}c_{n+2}\cdots c_{n+d_1}}\cdot g_{d_1}^{\eta_{A(w)}}$ 隐含设置 $r_{A(w)}$ 为 $c_{n+1}c_{n+2}\cdots c_{n+d_1}+\eta_{A(w)}$. 同样地可隐含设置 $r_{B(w)}$ 为 $c_{n+1}c_{n+2}\cdots c_{n+d_2}+\eta_{B(w)}$. 因此可模拟密钥组件为

$$K_{w,1}=g_{j-d_1}^{a_w}=g_{j-d_1}^{c_{n+j+1}+\varphi_w},$$
$$K_{w,2}=g_{j-d_2}^{b_w}=g_{j-d_2}^{c_{n+j+1}+\phi_w},$$
$$\begin{aligned} K_{w,3}&=g_j^{r_w-a_w\cdot r_{A(w)}}\\ &=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}+\eta_w-(c_{n+j+1}+\varphi_w)\cdot(c_{n+1}c_{n+2}\cdots c_{n+d_1}+\eta_{A(w)})}\\ &=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}}\cdot g_j^{\eta_w}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_1}\cdot c_{n+j+1}})^{-1}\cdot\\ &\quad(g_j^{c_{n+j+1}})^{-\eta_{A(w)}}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_1}})^{-\varphi_w}\cdot(g_j^{\eta_{A(w)}})^{-\varphi_w},\\ K_{w,4}&=g_j^{r_w-b_w\cdot r_{B(w)}}\\ &=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}+\eta_w-(c_{n+j+1}+\phi_w)\cdot(c_{n+1}c_{n+2}\cdots c_{n+d_2}+\eta_{B(w)})}\\ &=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}}\cdot g_j^{\eta_w}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_2}\cdot c_{n+j+1}})^{-1}\cdot\\ &\quad(g_j^{c_{n+j+1}})^{-\eta_{B(w)}}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_2}})^{-\phi_w}\cdot(g_j^{\eta_{B(w)}})^{-\phi_w}. \end{aligned}$$

由于 $g^{c_{n+1}},g^{c_{n+2}},\cdots,g^{c_{n+l+1}}$ 均为假设中的已知条件，η_w,φ_w,ϕ_w 为模拟者自己选取的数值，因此上述密钥组件可通过多次对运算和指数运算得到. 此外由于 η_w,φ_w,ϕ_w 均为随机选取值，因此 a_w,b_w,r_w 也可看做随机值.

(3) AND gate

假如 $w\in Gates$ 且 $GateType(w)=\text{AND}$ 时，同样不妨设节点 w 的深度为 $j=depth(w)$，$A(w)$ 和 $B(w)$ 的深度分别为 d_1 和 d_2，这里要求 $1\leq d_1,d_2\leq j-1$.

如果 $f_w(\boldsymbol{x}^*)=1$，可选择随机数 $a_w,b_w,r_w\in\mathbb{Z}_p$，模拟密钥组件为

$$K_{w,1}=g_{j-d_1}^{a_w},\ K_{w,2}=g_{j-d_2}^{b_w},\ K_{w,3}=g_j^{r_w-a_w\cdot r_{A(w)}-b_w\cdot r_{B(w)}}.$$

如果 $f_w(\boldsymbol{x}^*)=0$，则需要分情况进行讨论.

(1) 若 $f_{A(w)}(\boldsymbol{x}^*)=0$，$f_{B(w)}(\boldsymbol{x}^*)=1$，敌手 $\mathcal{B}$ 选择随机数 $\eta_w,\varphi_w,\phi_w\in\mathbb{Z}_p$，同样的，通过设置 $g^{a_w}=g^{c_{n+j+1}}\cdot g^{\varphi_w}$，$g^{b_w}=g^{c_{n+j+1}}\cdot g^{\phi_w}$ 和 $g_j^{r_w}$ 为 $e(g^{c_{n+1}},g^{c_{n+2}},\cdots,g^{c_{n+j}})\cdot g_j^{\eta_w}$ 可以隐含地设置 r_w 为 $c_{n+1}c_{n+2}\cdots c_{n+j}+\eta_w$，$a_w$ 为 $c_{n+j+1}+\varphi_w$ 和 b_w 为 $c_{n+j+1}+\phi_w$. 通过设置 $g_{d_1}^{r_{A(w)}}=g_{d_1}^{c_{n+1}c_{n+2}\cdots c_{n+d_1}+\eta_{A(w)}}$ 可隐含设置 $r_{A(w)}=c_{n+1}c_{n+2}\cdots c_{n+d_1}+\eta_{A(w)}$，选择随机数 $r_{B(w)}$，可模拟密钥组件为

$$K_{w,1}=g_{j-d_1}^{a_w}=g_{j-d_1}^{c_{n+j+1}+\varphi_w},\ K_{w,2}=g_{j-d_2}^{b_w}=g_{j-d_2}^{c_{n+j+1}+\phi_w},$$

$$\begin{aligned}K_{w,3}&=g_j^{r_w-a_w\cdot r_{A(w)}-b_w\cdot r_{B(w)}}\\&=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}+\eta_w-(c_{n+j+1}+\varphi_w)\cdot(c_{n+1}c_{n+2}\cdots c_{n+d_1}+\eta_{A(w)})-(c_{n+j+1}+\phi_w)\cdot r_{B(w)}}\\&=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}}\cdot g_j^{\eta_w}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_1}\cdot c_{n+j+1}})^{-1}\cdot(g_j^{c_{n+j+1}})^{-\eta_{A(w)}}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_1}})^{-\varphi_w}\cdot\\&\quad(g_j^{\eta_{A(w)}})^{-\varphi_w}\cdot(g_j^{c_{n+j+1}})^{-r_{B(w)}}\cdot(g_j^{\phi_w})^{-r_{B(w)}}.\end{aligned}$$

同样的,由于 $g^{c_{n+1}},g^{c_{n+2}},\cdots,g^{c_{n+l}}$ 均为假设中的已知条件,η_w,φ_w,ϕ_w 为模拟者自己选取的数值,因此上述密钥组件可通过多次对运算和指数运算得到.此外由于 η_w,φ_w,ϕ_w 均为随机选取值,因此 a_w,b_w,r_w 也可看做随机值.

(2)若 $f_{A(w)}(\boldsymbol{x}^*)=1,f_{B(w)}(\boldsymbol{x}^*)=0$,该情况与情况(1)类似,需要将 $A(w)$ 和 $B(w)$ 的角色和参数进行对换.

$$K_{w,1}=g_{j-d_1}^{a_w}=g_{j-d_1}^{c_{n+j+1}+\varphi_w},\ K_{w,2}=g_{j-d_2}^{b_w}=g_{j-d_2}^{c_{n+j+1}+\phi_w}$$

$$\begin{aligned}K_{w,3}&=g_j^{r_w-a_w\cdot r_{A(w)}-b_w\cdot r_{B(w)}}\\&=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}+\eta_w-(c_{n+j+1}+\varphi_w)\cdot r_{A(w)}-(c_{n+j+1}+\phi_w)\cdot(c_{n+1}c_{n+2}\cdots c_{n+d_2}+\eta_{B(w)})}\\&=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}}\cdot g_j^{\eta_w}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_2}\cdot c_{n+j+1}})^{-1}\cdot(g_j^{c_{n+j+1}})^{-r_{A(w)}}\cdot(g_j^{\varphi_w})^{-r_{A(w)}}\cdot\\&\quad(g_j^{c_{n+j+1}})^{-\eta_{B(w)}}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_2}})^{-\phi_w}\cdot(g_j^{\eta_{B(w)}})^{-\phi_w}.\end{aligned}$$

同样的,由于 $g^{c_{n+1}},g^{c_{n+2}},\cdots,g^{c_{n+l}}$ 均为假设中的已知条件,η_w,φ_w,ϕ_w 为模拟者自己选取的数值,因此上述密钥组件可通过多次对运算和指数运算得到.此外由于 η_w,φ_w,ϕ_w 均为随机选取值,因此 a_w,b_w,r_w 也可看做随机值.

(3)若 $f_{A(w)}(\boldsymbol{x}^*)=0,f_{B(w)}(\boldsymbol{x}^*)=0$,敌手 $\mathcal{B}$ 选择随机数 $\eta_w,\varphi_w,\phi_w\in\mathbb{Z}_p$.同样的,通过设置 $g_j^{r_w}=e(g^{c_{n+1}},g^{c_{n+2}},\cdots,g^{c_{n+j}})\cdot g_j^{\eta_w},g^{a_w}=g^{c_{n+j+1}}\cdot g^{\varphi_w}$ 和 $g^{b_w}=g^{c_{n+j+1}}\cdot g^{\phi_w}$ 可隐含设置 r_w 为 $c_{n+1}c_{n+2}\cdots c_{n+j}+\eta_w$,$a_w$ 为 $c_{n+j+1}+\varphi_w$ 和 b_w 为 $c_{n+j+1}+\phi_w$.通过设 $g_{d_1}^{r_{A(w)}}$ 为 $g_{d_1}^{c_{n+1}c_{n+2}\cdots c_{n+d_1}+\eta_{A(w)}}$ 可设 $r_{A(w)}=c_{n+1}c_{n+2}\cdots c_{n+d_1}+\eta_{A(w)}$,通过设置 $g_{d_2}^{r_{B(w)}}$ 为 $g_{d_2}^{c_{n+1}c_{n+2}\cdots c_{n+d_2}+\eta_{B(w)}}$ 隐含将 $c_{n+1}c_{n+2}\cdots c_{n+d_2}+\eta_{B(w)}$ 赋予 $r_{B(w)}$,因此可模拟密钥组件为

$$\begin{aligned}K_{w,1}&=g_{j-d_1}^{a_w}=g_{j-d_1}^{c_{n+j+1}+\varphi_w},\\K_{w,2}&=g_{j-d_2}^{b_w}=g_{j-d_2}^{c_{n+j+1}+\phi_w},\\K_{w,3}&=g_j^{r_w-a_w\cdot r_{A(w)}-b_w\cdot r_{B(w)}}\\&=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j+1}}\cdot g_j^{\eta_w}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_1}\cdot c_{n+j+1}})^{-1}\cdot\\&\quad(g_j^{c_{n+j+1}})^{-\eta_{A(w)}}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_1}})^{-\varphi_w}\cdot(g_j^{\eta_{A(w)}})^{-\varphi_w}\cdot\\&\quad(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_2}\cdot c_{n+j+1}})^{-1}\cdot(g_j^{c_{n+j+1}})^{-\eta_{B(w)}}\cdot\\&\quad(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_2}})^{-\phi_w}\cdot(g_j^{\eta_{B(w)}})^{-\phi_w}.\end{aligned}$$

其过程为敌手 $\mathcal{B}$ 选择随机数 $\eta_w,\varphi_w,\phi_w\in\mathbb{Z}_p$,同样的,通过设置 $g^{a_w}=g^{c_{n+j+1}}\cdot g^{\varphi_w},g^{b_w}=g^{c_{n+j+1}}\cdot g^{\phi_w}$ 和 $g_j^{r_w}$ 为 $e(g^{c_{n+1}},g^{c_{n+2}},\cdots,g^{c_{n+j}})\cdot g_j^{\eta_w}$ 可以隐含地设置 r_w 为 $c_{n+1}c_{n+2}\cdots c_{n+j}+\eta_w$,$a_w$ 为 $c_{n+j+1}+\varphi_w$ 和 b_w 为 $c_{n+j+1}+\phi_w$.通过设置 $g_{d_2}^{r_{B(w)}}=g_{d_2}^{c_{n+1}c_{n+2}\cdots c_{n+d_1}+\eta_{B(w)}}$ 可隐含设置 $r_{B(w)}=c_{n+1}c_{n+2}\cdots c_{n+d_2}+\eta_{B(w)}$,选择随机数 $r_{A(w)}$,可模拟密钥组件为

$$\begin{aligned}K_{w,1}&=g_{j-d_1}^{a_w}=g_{j-d_1}^{c_{n+j+1}+\varphi_w},\ K_{w,2}=g_{j-d_2}^{b_w}=g_{j-d_2}^{c_{n+j+1}+\phi_w}\\K_{w,3}&=g_j^{r_w-a_w\cdot r_{A(w)}-b_w\cdot r_{B(w)}}\\&=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}+\eta_w-(c_{n+j+1}+\varphi_w)\cdot r_{A(w)}-(c_{n+j+1}+\phi_w)\cdot(c_{n+1}c_{n+2}\cdots c_{n+d_2}+\eta_{B(w)})}\\&=g_j^{c_{n+1}c_{n+2}\cdots c_{n+j}}\cdot g_j^{\eta_w}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_2}\cdot c_{n+j+1}})^{-1}\cdot(g_j^{c_{n+j+1}})^{-r_{A(w)}}\cdot(g_j^{\varphi_w})^{-r_{A(w)}}\cdot\\&\quad(g_j^{c_{n+j+1}})^{-\eta_{B(w)}}\cdot(g_j^{c_{n+1}c_{n+2}\cdots c_{n+d_2}})^{-\phi_w}\cdot(g_j^{\eta_{B(w)}})^{-\phi_w}.\end{aligned}$$

同样的,上述密钥组件可通过多次对运算和指数运算得到,a_w,b_w,r_w 也可看做随机值.

Encrypt 在这个阶段攻击者给 $\mathcal{B}$ 一个属性集合编码 $\boldsymbol{x}\in\{0,1\}^n$.可分两种情况进行讨论.

(1)假如 $\boldsymbol{x}=\boldsymbol{x}^*$,$\mathcal{B}$ 终止计算.

(2)假如 $\boldsymbol{x}\neq\boldsymbol{x}^*$,则必然存在某一个 i,使得 $x_i\neq x_i^*$.

算法首先利用假设中的已知条件 $g^{c_{n+1}},g^{c_{n+2}},\cdots,g^{c_{n+l+1}}$ 等进行多次对运算,可得到临时变量 $H=(g_{l+1})^{\alpha}=g_{l+1}^{c_{n+1}\cdot c_{n+2}\cdots c_{n+l+1}}$.对于所有 $j\neq i$,这里 $i\in[1,n]$,利用 $g^{c_1},g^{c_2},\cdots,g^{c_n}$ 可计算 H_{temp} 的值 $(g_{n-1})^{\prod_{j\neq i}d_{j,x_j}}$,然后再利用所选随机数 z_i 对 d_{i,x_i} 进行赋值,即令 $d_{i,x_i}=z_i$ 并将其乘到 H_{temp} 的指数,可得到 $H'=(H_{\text{temp}})^{z_i}=(g_{n-1})^{\prod_{j\in[1,n]}d_{j,x_j}}$,最后计算

$$\begin{aligned}e(H,H')&=e(g_{l+1}^{c_{n+1}\cdot c_{n+2}\cdots c_{n+l+1}},g_{n-1}^{\prod_{j\in[1,n]}d_{j,x_j}})\\&=(g_{\kappa=n+l})^{\alpha\prod_{i\in[1,n]}d_{i,x_i}}.\end{aligned}$$

挑战.最后,攻击者 $\mathcal{A}$ 将输入一个挑战值 $\tilde{\boldsymbol{x}}$.假如 $\tilde{\boldsymbol{x}}\neq\boldsymbol{x}^*$,那么敌手 $\mathcal{B}$ 随机地输出一个猜测 $\delta'\in\{0,1\}$.假如 $\tilde{\boldsymbol{x}}=\boldsymbol{x}^*$,那么 $\mathcal{B}$ 输出 T 作为对此阶段问询的响应.

至此，完成了对敌手$\mathcal{B}$的描述. 由于 T 为 MDDH 元组的一部分，因此真实游戏和敌手$\mathcal{B}$进行的游戏模拟中的 T 具有相同分布. 令 δ 表示 T 是否是一个 MDDH 元组，δ'表示敌手$\mathcal{B}$的输出，则$\mathcal{B}$猜测是正确的概率为

$$\begin{aligned}\Pr[\delta'=\delta]&=\Pr[\delta'=\delta\,|\,abort]\cdot\Pr[abort]+\\&\quad\Pr[\delta'=\delta\,|\,\overline{abort}]\cdot\Pr[\overline{abort}]\\&=\frac{1}{2}(1-2^{-n})+\Pr[\delta'=\delta\,|\,\overline{abort}]\cdot(2^{-n})\\&=\frac{1}{2}(1-2^{-n})+\left(\frac{1}{2}+\varepsilon\right)\cdot(2^{-n})\\&=\frac{1}{2}+\varepsilon\cdot(2^{-n}).\end{aligned}$$

上式中第 2 个等式是由于敌手$\mathcal{B}$在游戏模拟中没有终止的概率是 2^{-n}. 第 3 个等式成立是由于攻击者在给定条件下获胜而不被终止的概率与攻击者获胜的概率是相同的. 由上述式子可知$\mathcal{B}$的获胜优势为 $\varepsilon/2^n$.　　证毕.

5　效率分析

下面将本文方案与文献[5-6,8]中提出的方案进行对比. 表 2 列出了在公共参数、密文量、多线性假设的层数、解密密钥的个数、电路是否支持跨层输出等方面对通信和存储效率进行了对比. 表 3 在算法建立、密钥生成、加密和解密等方面对各方案的计算效率进行了对比.

表 2 中，相关符号的具体含义：n 表示系统属性数量，l 表示电路中的最大深度. κ 表示多线性映射的最大层数，q 表示电路中的门数量，$|PP|$ 表示公共参数的长度，$|CT_x|$ 表示密文的长度，$|SK_f^{(\mathrm{DEC})}|$ 表示秘密钥的长度. MDDH 表示多线性的判定性 Diffie-Hellman 假设.

表 2　相关方案通信和存储对比结果

方案名称	安全性	复杂性假设	$\lvert PP\rvert$	$\lvert CT_x\rvert$	κ	$\lvert SK_f^{(\mathrm{DEC})}\rvert$	是否支持跨层
Garg 方案	选择安全	MDDH	$n+2$	$n+2$	$l+1$	$2n+4q+1$	否
Datta 方案	选择安全	MDDH	$2n+1$	2	$n+l+1$	$n+4q+1$	否
Hu 方案	选择安全	MDDH	$n+2$	$n+2$	$l+1$	$2n+4q+3$	是
本文方案	选择安全	MDDH	$2n+1$	2	$n+l$	$n+4q+1$	是

表 3　相关方案中多线性运算次数对比结果

方案名称	Setup	KeyGen	Encrypt	Decrypt
Garg 方案	$n+2$	$3n+4q+1$	$n+2$	$2n+3q+1$
Datta 方案	$2n+2$	$2n+4q+1$	3	$n+3q+3$
Hu 方案	$n+1$	$3n+4q+3$	$n+2$	$2n+3q+2$
本文方案	$2n+1$	$2n+4q$	2	$n+3q+2$

由表 2 可以看到，(1) 本文的方案密文数量较紧，与 Datta 方案一致，只包括两个群元素，相较于 Garg 方案和 Hu 方案在密文的存储量上有显著下降；(2) 与 Datta 方案相比，本方案支持跨域输出，可以进一步减少 KeyGen 算法中的秘密钥颁发量；(3) 从方案可看出，本文提出的广播加密方案不需要广播头部件，因而可以减少通信数据包结构中的大小，从而降低每次需要传输的数据负荷量，提高通信效率.

表 3 中，相关符号的具体含义：n 表示系统属性数量，q 表示电路中的门数量，表中列出了本方案与文献[5-6,8]中各方案在算法建立、密钥生成、加密和解密等各个阶段中多线性运算的次数. 由于 $g_n^{\prod_{i\in[1,n]}^{d_i,x_i}}$ 可通过预计算得到，本方案与文献[6]的密文量均较为紧致，因此相应地在加密阶段所需要进行的对运算次数也较少.

6　结束语

本文利用受限伪随机函数的性质，实现了基于任意深度电路结构的属性基广播加密方案，该方案在标准模型下基于多线性判定性 Diffie-Hellman (κ-MDDH) 假设被证明是具有选择安全的. 特别的，该方案不需要广播加密中的报头部件，可以有效减少广播加密中每次需要广播的主体，从而节省带宽. 受限伪随机函数是于 2013 年提出的新概念，基于受限伪随机函数的各类构造和相关性质已用于外包计算的研究之中. 如何设计更加简捷高效的基于一般电路的广播加密方案是下一步需要研究的问题. 此外如何结合属性密码，实现基于任意深度一般电路的加密方案和密钥协商方案也是值得探索的问题.

参　考　文　献

[1]　Shamir A. Identity-based cryptosystems and signature schemes

//Proceedings of the 1984 International Cryptology Conference (CRYPTO'1984). Santa Barbara, USA, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing//Proceedings of the 21st Annual International Cryptology Conference (CRYPTO'2001). Santa Barbara, USA, 2001: 213-229

[3] Sahai A, Waters B. Fuzzy identity-based encryption//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'2005). Aarhus, Denmark, 2005: 457-473

[4] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA, 2006: 89-98

[5] Garg S, Gentry C, Halevi S, et al. Attribute-based encryption for circuits from multilinear maps//Proceedings of the 33rd Annual International Cryptology Conference (CRYPTO'2013). Santa Barbara, USA, 2013: 479-499

[6] Datta P, Dutta R, Mukhopadhyay S. Compact attribute-based encryption and signcryption for general circuits from multilinear maps//Proceedings of the 16th International Conference on Cryptology in India. Bangalore, India, 2015: 3-24

[7] Xu J, Wen Q, Li W, et al. Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(1): 119-129

[8] Hu Peng, Gao Hai-Ying. Key-policy attribute-based encryption scheme for general circuits. Journal of Software, 2016, 27(6): 1498-1510(in Chinese)
(胡鹏, 高海英. 一种实现一般电路的密钥策略的属性加密方案. 软件学报, 2016, 27(6): 1498-1510)

[9] Garg S, Gentry C, Halevi S, et al. Fully secure attribute based encryption from multilinear maps. Cryptology ePrint Archive: IACR, Report 2014/622, 2014

[10] Attrapadung N. Fully secure and succinct attribute based encryption for circuits from multi-linear maps. Cryptology ePrint Archive: IACR, Report 2014/772, 2014

[11] Hu Y, Jia H. Cryptanalysis of GGH map//Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'2016). Vienna, Austria, 2016: 537-565

[12] Albrecht M R, Farshim P, Hofheinz D, et al. Multilinear maps from obfuscation//Proceedings of the 13th Theory of Cryptography Conference. Tel Aviv, Israel, 2016: 446-473

[13] Boneh D, Waters B. Constrained pseudorandom functions and their applications//Proceedings of the 19th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'2013). Bangalore, India, 2013: 280-300

[14] Kiayias A, Papadopoulos S, Triandopoulos N, et al. Delegatable pseudorandom functions and applications//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS'13). New York, USA, 2013: 669-684

[15] Boyle E, Goldwasser S, Ivan I. Functional signatures and pseudorandom functions//Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography (PKC'2014). Buenos Aires, Argentina, 2014: 501-519

[16] Garg S, Gentry C, Halevi S. Candidate multilinear maps from ideal lattices//Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'2013). Athens, Greece, 2013: 1-17

[17] Beimel A. Secure Schemes for Secret Sharing and Key Distribution [Ph. D. dissertation]. Israel Institute of Technology, Technion, Haifa, Israel, 1996

[18] Goldreich O, Goldwasser S, Micali S. How to construct random functions. Journal of the ACM, 1986, 33(4): 792-807

[19] Fiat A, Naor M. Broadcast encryption//Proceedings of the 13th Annual International Cryptology Conference (CRYPTO'93). Santa Barbara, USA, 1993: 480-491

ZHANG Li-Na, born in 1981, Ph.D., associate professor. Her research interests include cryptography and information security.

YANG Bo, born in 1963, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and information security.

ZHOU Yan-Wei, born in 1986, Ph. D. candidate. His research interests include cryptography and anonymous communication.

JIA Yan-Yan, born in 1983, Ph.D., lecturer. Her research interests include cryptography and information security.

Background

Identity-based encryption (IBE) scheme was proposed by Shamir in 1984 in order to simplify the traditional public key cryptography. IBE provides a public-key encryption mechanism where the public key is the identity to the client and even an arbitrary string. Attributed-based encryption scheme is a special type of IBE. The identities could be instead by the attributes and the corresponding access control policy.

It is an interesting work to design schemes that be able to realize decryption policies representable as polynomial-size circuits. In 2013, Garg et al. provided the first construction of attribute-based encryption (ABE) for general circuits which could resist the backtracking attack. Then many related schemes were proposed. In 2015 Datta et al. presented a key-policy scheme supporting general polynomial-size circuit realizable decryption policies and the ciphertexts were short. In 2016, Hu et al. proposed a key-policy scheme for general circuits and achieved cross layer output.

We propose an attribute-based broadcast encryption scheme for general circuits with arbitrary depth based on the Garg's scheme. Our scheme has short ciphertexts and does not require the broadcast header. Essentially it is a symmetric broadcast encryption scheme and associated with constrained pseudorandom functions. Our scheme is proved to achieve selective security in the standard model under the multilinear decisional Diffie-Hellman assumption. We would have a further exploring on its application scenarios and try to improve its efficiency. This work is supported by the National Key R&D Program of China (2017YFB0802000), the National Natural Science Foundation of China (61572303, 61772326), the National Cryptography Development Fund during the 13th Five-year Plan Period (MMJJ20170216), the Foundation of State Key Laboratory of Information Security (2017-MS-03), the Fundamental Research Funds for the Central Universities (GK201702004) and the Science and Technology Program of Yulin (2014CXY-08-01).