# 具有固定长度密文的广播加密方案

国佃利[1],杨鹏飞[1],刘家磊[2],王 萍[3],宋宁宁[1]
(1.中国电子信息产业集团有限公司第六研究所,北京 100083;
2.安阳师范学院 软件学院,河南 安阳 455000;3.中国联合网络通信有限公司北京市分公司,北京 100052)

**摘 要**:广播加密方案可建立一对多的密态数据传输通道,消息发送者可在执行加密操作前创建授权用户集合,惟有授权用户才能对接收到的广播密态数据进行解密。利用素数阶非对称双线性映射构造了标准模型下静态安全的公钥广播加密方案,密文扩展量与用户密钥扩展量为 $O(1)$,公钥扩展量为 $O(N)$($N$ 表示广播加密系统内用户总数)。与之前相关方案相比,该方案能够在简单的非交互式安全假设下取得标准模型下静态安全性,并且取得最优化的密文与用户密钥扩展量。

**关键词**:广播加密;标准模型;静态安全性;参数扩展量
**中图分类号**:TN914;TP309.7 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.200857

**中文引用格式**:国佃利,杨鹏飞,刘家磊,等. 具有固定长度密文的广播加密方案[J].电子技术应用,2021,47(9):55-58.
**英文引用格式**:Guo Dianli,Yang Pengfei,Liu Jialei,et al. Broadcasting encryption scheme with constant ciphertext overhead[J]. Application of Electronic Technique,2021,47(9):55-58.

## Broadcasting encryption scheme with constant ciphertext overhead

Guo Dianli[1],Yang Pengfei[1],Liu Jialei[2],Wang Ping[3],Song Ningning[1]
(1.The 6th Research Institute of China Electronics Corporation,Beijing 10083,China;
2.School of Software Engineering,Anyang Normal University,Anyang 455000,China;
3.China Unicom Beijing Branch,Beijing 100052,China)

**Abstract**:Broadcasting encryption enables to establish a secrecy channel for distributing ciphered messages, the broadcaster adaptively chooses the set of authorized users before executing encryption operation, and only the authorized users could decrypt the received ciphered broadcast. This paper devises a public key broadcasting encryption construction with prime order asymmetric bilinear maps and proves it is static secure in the standard model. In the proposed construction, the overhead of ciphertexts and user secret keys are $O(1)$, the public key overhead is $O(N)$ in the total user number $N$. Compared with other related constructions, the proposal achieves static security based on non-interactive security assumption with the optimal overhead of ciphertexst and user secret keys.

**Key words**:broadcasting encryption;standard model;static security;overhead

## 0 引言

广播作为数据传输的重要方式,在有线电视、卫星通信、移动通信、计算机通信中有着广泛的应用。广播加密继承了广播中“一对多”的数据传输形式,是一种在不安全的信道中向指数量级用户发送密态数据的密码技术,指定授权集合中的用户可恢复出加密密钥,进而完成密态数据转换。即使全部非授权用户贡献出用户密钥,也无法通过获得广播数据加密密钥,该广播加密方案被认为能够抵抗完全合谋攻击。

广播加密方案的安全性可根据攻击模型定义分为两种类型:静态安全性与自适应安全性,满足上述两种安全性的方案均能够抵抗完全合谋攻击。在静态安全模型中,攻击者在知晓系统公钥前需公布挑战的授权集合,而自适应安全模型中则没有类似限制,实现自适应安全性往往需要牺牲部分加解密效率及大幅提升参数扩展量。实时数据广播加密系统是目前广播加密最为广阔的应用方向,如何提升其加解密效率与降低参数扩展量是亟待解决的关键问题。

平凡的广播加密方案的设计结构满足低存储空间需求和高安全性,能够抵抗完全合谋攻击。然而,平凡的广播加密方案有着极其庞大的密文扩展量。Fiat 和 Naor[1] 在 1993 年提出了第一个广播加密方案,在该方案中用户数量为 $N$,密文扩展量为 $N(t\log^2 t\log N)$。值得注意的是,该方案仅仅能够抵抗不超过 $t$ 个用户发起的合谋攻击。显然,作者希望通过降低安全等级的方式以寻求降低平凡的广播加密方案中庞大的密文扩展量。2005 年,

Boneh、Gentry 和 Waters[2]利用素数阶对称双线性映射构造了可抵抗完全合谋攻击的广播加密方案，密文扩展量与密钥的扩展量都为 $O(1)$，但系统公钥扩展量随着用户总数 $N$ 线性增长。Gentry 和 Waters[3]在 2009 年提出了新的广播加密方案，引入了半静态安全性，期望通过“双密钥”策略将半静态安全性转化为自适应安全性，该方案的密文的扩展量为 $O(1)$。同年，Waters[4]基于对偶系统加密构造了适应性安全的广播加密方案，其密文扩展量为 $O(1)$，但系统公钥和用户密钥扩展量都为 $O(N)$。随后，多个研究人员利用多重线性映射构造了参数扩展量极低的广播加密方案[5-7]，但随着胡予濮教授[8]攻破了 GGH 多重线性映射密码方案，基于该方案的广播加密方案均不再成立，在此不一一介绍。2015 年，Kim 等人[9]提出了基于身份的适应性安全的广播加密方案，但该方案的系统公钥和用户密钥均随着最大接收者总数线性增长，也就意味着即使授权集合中仅包含一个用户，也无法降低依据初始设定的最大接收者数量形成的各类参数扩展量。2019 年与 2020 年，Guo 等人[10-11]分别提出了带认证性质的基于公钥的广播加密方案，并分别给出了静态安全性与自适应安全性证明，由于需要实现对消息发送者的鉴权认证，该方案的密文与密钥扩展量扩张十分庞大。

本文利用素数阶非对称双线性映射构造了基于公钥的广播加密方案，密文扩展量与用户密钥扩展量均为最优化的常数级别，公钥扩展量随着系统用户总数增加线性增长，随后在标准模型下基于非交互式的安全假设(co-Diffie-Hellman 假设)给出了静态安全性的证明。

本文首先简要描述素数阶非对称双线性映射及 co-Diffie-Hellman 安全假设。随之，提出了一个新的广播加密方案，并证明了方案的静态安全性。

## 1 基础知识

下面简要描述素数阶非对称双线性映射以及判定性 co-Diffie-Hellman 问题的定义[12-14]。

### 1.1 素数阶非对称双线性映射

映射 $e:G_1\times G_2\rightarrow G_T$ 为素数阶段非对称双线性映射，其中 $G_1$、$G_2$ 和 $G_T$ 为 3 个阶为大素数 $p$ 的乘法循环群，满足以下 3 种特性。

(1)双线性特性：对于 $\forall g\in G_1$，$\forall h\in G_2$ 和 $\forall a,b\in Z_p$，有等式 $e(g^a,h^b)=e(g,h)^{ab}$ 成立。

(2)非退化特性：$\exists g\in G_1$，$\exists h\in G_2$，满足 $e(g,h)\neq 1$。

(3)高效计算特性：对于 $\forall g\in G_1$，$\forall h\in G_2$，能够高效地计算 $e(g,h)\in G_T$。

### 1.2 判定性 co-Diffie-Hellman 问题

利用安全参数 $\lambda$ 素数阶非对称双线性群生成器输出 3 个阶为 $q$ 的乘法循环群 $G_1$、$G_2$ 和 $G_T$，以及非对称双线性映射 $e:G_1\times G_2\rightarrow G_T$。给定攻击者 $D=\{G_1,G_2,G_T,e,g^a,h,h^b,T\}$，其中 $g\in G_1$，$h\in G_2$，$a,b\in Z_p$。通过判定输出 $\beta\in\{0,1\}$ 区分 $T$ 为 $g^{ab}$ 或者为循环群 $G_1$ 中的一个随机的生成元。

定义 1 如果判定性 co-Diffie-Hellman 问题在多项式时间内是难解的，即不存在多项式时间算法能够以不可忽略的优势 $\varepsilon$ 解决该问题。

## 2 广播加密方案

### 2.1 广播加密系统定义

广播加密方案包括以下 4 个随机化算法：Setup，KeyGen，Enc，Dec[13]。

(1)Setup$(N,\lambda)$，该算法以用户总数 $N$ 为输入，输出结果为公私钥对<PK，msk>。

(2)KeyGen(msk，$u$)，该算法主私钥和用户身份 $u\in[1,N]$ 为输入，输出结果为用户 $u$ 的私钥 $\mathrm{sk}_u$。

(3)Enc($S$，PK)，加密算法以授权集合 $S\subseteq[1,N]$ 和公钥为输入，输出结果为(Hdr，$K$)，其中 Hdr 被称为头文件，$K$ 为消息加密密钥。

消息 $M$ 利用对称加密方案在密钥 $K$ 作用下加密为密文 $C$，最后广播密文为$\{S,\mathrm{Hdr},C\}$。

(4)Dec(PK，$u$，$\mathrm{SK}_u$，$S$，Hdr)，解密算法需要输入公钥 PK、授权集合 $S$、用户身份 $u$、用户密钥 $\mathrm{sk}_u$ 以及密文头文件 Hdr。如果 $u\in S$，输出消息加密密钥 $K$；否则，输出 $\perp$。最后，用户 $u$ 利用密钥 $K$ 解密 $C$ 获取广播消息 $M$。

在解密算法中，对于 $S\subseteq[1,N]$ 以及 $u\in S$，如果(PK，msk)是由 Setup$(N,\lambda)$生成，$\mathrm{sk}_u$ 是由密钥生成算法 KeyGen(msk，$u$)生成，(Hdr，$K$)是由加密算法 Enc($S$，PK)生成，那么 Decrypt(PK，$S$，$u$，$\mathrm{sk}_u$，Hdr)$=K$。

### 2.2 广播加密方案构造

本小节在素数阶的非对称双线性群中构造了一个包含 $N$ 个用户的静态安全的广播加密方案，密文与用户密钥扩展量为 $O(1)$，公钥扩展量为 $O(N)$。新构造的静态安全的广播加密方案主要包括 Setup、KeyGen、Enc、Dec 4 个算法。

(1)Setup$(N,\lambda)$，输入用户总数 $N$ 与安全参数 $\lambda$。算法生成两个阶同为大素数 $p$ 的双线性群 $G_1$ 和 $G_2$，随机选取生成元 $g\in G_1$，$h\in G_2$，并选取随机数 $\alpha,\gamma\in Z_p$，同时依次计算 $h_i=h^{(\alpha^i)}(i=1,2,\cdots,N,N+2,\cdots,2N)$，$v\in g^{\gamma}$。最终输出系统公钥参数 $\mathrm{PK}=\{h,h_1,h_2,\cdots,h_N,h_{N+2},\cdots,h_{2N},v\}$ 以及主私钥 $\mathrm{msk}=\{\gamma,\alpha\}$。

(2)KeyGen(msk，$i$)，输入用户身份标识 $i\in[1,N]$，输出该用户的私钥 $\mathrm{sk}_i=g_i^{\gamma}=g^{(\gamma\alpha^i)}$。

(3)Enc($S$，PK)，广播者任意选取广播用户添加至授权用户集合 $S\subseteq[1,N]$，在加密算法中输入系统公钥及授权用户集合 $S$，随后加密算法随机选取数值 $t\in Z_p$，并计算消息加密密钥 $K$ 与头文件 Hdr，$K=e(\mathrm{sk}_i,h_{N-i+1})^t=e(g,h)^{(t\gamma\alpha^{N+1})}$，$\mathrm{Hdr}=(C_0,C_1)=(v^t,(\prod_{k\in S}h_{N+1-k})^t)$。

最后，广播者利用对称加密算法对广播内容进行加密，在消息加密密钥作用下计算得到广播密文 $C=\mathrm{SymEnc}(M,K)$。

(4)Dec(PK,$j$,$sk_j$,$S$,Hdr),输入接收者的身份标识$j$、接收者私钥$sk_j$、系统公钥、授权集合$S$及密文头文件Hdr。如果接收者$j\in S$,解密算法按照如下算式计算消息加密密钥$K$;否则,输出$\perp$。

$$K=\frac{e(sk_j,C_1)}{e(\prod_{k\in S,k\neq j}h_{N+1-k+j},C_0)} \tag{1}$$

如果接收者属于授权用户集合,其可利用已得到的消息加密密钥$K$解密广播密文获得广播消息$M$=SymDec($C$,$K$)。

## 3 安全性证明

### 3.1 静态安全性模型

在静态安全性模型中,敌手$A$被允许适应性地查询挑战集合$S^*$外的用户私钥,意味着敌手能够掌握除挑战集合$S^*$外的所有用户私钥,因此隐式地模拟了完全合谋攻击。具体的静态安全性模型定义如下所示:

(1)Init,敌手$A$公开想要挑战的目标用户集合$S^*$。

(2)Setup,挑战者运行初始化算法Setup($N$,$\lambda$),并将算法输出的系统公钥PK发送给敌手$A$。

(3)Secret Key Queries,随后敌手$A$被赋予查询用户私钥的权利,如果被查询用户$i\in S^*$时,挑战者立即终止该实验;否则挑战者运行密钥生成算法KeyGen(msk,$i$),并将生成用户密钥$sk_i$发送给敌手$A$。如果敌手$A$重复查询用户$i$的密钥时,挑战者不再运行密钥生成算法,只将已生成的用户密钥$sk_i$发送给敌手$A$。

(4)Challenge,挑战者运行加密算法$(Hdr^*,K_0^*)\xleftarrow{R}Enc(S^*,PK)$,得到头文件$Hdr^*$和相应的消息加密密钥$K_0^*$。随后挑战者在密钥空间中随机选取密钥$K_1^*$以及随机选取比特$\beta\in\{0,1\}$,并将$(Hdr^*,K_\beta^*)$发送给敌手$A$。

(5)More Secret Key Queries,敌手$A$获取$(Hdr^*,K_\beta^*)$后被允许继续查询挑战集合$S^*$外的用户密钥。

(6)Guess,如果挑战者在密钥查询阶段没有终止实验,敌手$A$需返回对比特$\beta$的猜测$\beta'\in\{0,1\}$。

如果敌手在Guess阶段返回的猜测$\beta'$与挑战者在Challenge阶段随机选取的比特$\beta$一致,则意味着敌手$A$赢得了该实验,并攻破了广播加密方案。

定义2 令敌手$A$能够赢得广播加密方案的优势$Adv^{BE}_{A,N,\lambda}=|Pr[\beta'=\beta]-1/2|$,对于任意多项式时间的敌手$A$,如果$Adv^{BE}_{A,N,\lambda}$是一个关于$\lambda$的可忽略的函数,该广播加密方案可满足静态安全性。

### 3.2 静态安全性证明

基于上述定义的静态安全性定义,在标准模型下证明了本文构造的广播加密方案在判定性co-Diffie-Hellman假设下满足静态安全性。判定性co-Diffie-Hellman假设为一般性静态安全假设,其与敌手所做的密钥查询次数无关,将广播加密方案的安全性归约至此类安全性假设更为合理。

定理1 如果不存在多项式时间敌手$A$能够以不可忽略的优势解决判定性co-Diffie-Hellman问题,本文中构造的广播加密方案满足静态安全性。

证明:本小节利用反证法证明定理1,即如果多项式时间敌手$A$可在不可忽略的优势下攻破新构造的广播加密方案,那么就能够依托该敌手打造解决判定性co-Diffie-Hellman问题的算法$B$。算法$B$通过已取得的$\{G_1,G_1,G_T,e,g^a,h,h^b,T\}$与敌手$A$进行多轮次的交互模拟实验。

首先,敌手$A$选取目标用户集合$S^*$,并将其发送给算法$B$。值得注意的是,算法$B$在该试验中承担挑战者的角色。

随后,算法$B$选取随机数$\alpha\in Z_p$,并计算$h_i=h^{(\alpha^i)}$,$i=1,2,\cdots,N,N+2,\cdots,2N$。随后令$v=g^a$,并将计算得到的参数$\{h,h_1,h_2,\cdots,h_N,h_{N+2},\cdots,h_{2N},v\}$发送给敌手$A$。由于$g^a$的随机性隐含了数值$a$的随机特性,算法$B$使用$a$模拟了系统主密钥,但无法确定其准确数值。即使敌手$A$对上述公共参数后进行分析,也无法区分其与真实方案中的系统公钥的差别。

敌手$A$在接下来的实验中被允许查询目标用户集合$S^*$外的用户私钥,$A$可将用户身份发送给算法$B$,随后$B$利用已选取的随机数$\alpha\in Z_p$以及$g^a$计算得到$sk_i=(g^a)^{\alpha^i}$。值得注意的是,如果敌手$A$重复查询同一个用户的私钥,算法$B$只能返回第一次计算得到的私钥。

在挑战阶段,算法$B$在目标用户集合$S^*$作用下计算挑战密文头及对应的消息加密密钥:

$$K=e(T,h)^{\alpha^{N+1}} \tag{2}$$

$$Hdr=(C_0^*,C_1^*)=(T,h^{b\sum_{k\in S^*}\alpha^{N+1-k}}) \tag{3}$$

敌手$A$获取挑战密文头与消息加密密钥后,会根据已得到的信息返回算法$B$一个比特值$\beta$,算法$B$用于解决判定性co-Diffie-Hellman问题。

通过以上实验交互,算法$B$借助敌手$A$的能力实现了对于新提出的广播加密方案的模拟,并在其中嵌入了判定性co-Diffie-Hellman问题,一旦算法$B$能够以不可忽略的优势解决判定性co-Diffie-Hellman问题,那么敌手$A$就能够以同样的优势攻破新提出的广播加密方案。通过反证法得出结论,由于判定性co-Diffie-Hellman问题在多项式时间内是难解的,因此本文提出的广播加密方案满足静态安全性。

## 4 结论

本文利用素数阶非对称双线性映射设计了一个满足静态安全性的广播加密方案,其中密文扩展量与用户密钥扩展量均为固定长度,系统公钥扩展量随着用户总数线性增长,随后给出了形式化的安全性证明。新提出的广播加密方案系统公钥扩展量仍十分庞大,在未来的研究中希望通过采用新的密码学工具及安全假设构造

更为安全的广播加密方案，在保证参数扩展量优化的同时进一步提升安全特性。

## 参考文献

[1] FIAT A，NAOR M.Broadcast encryption[C]//Proc.of the 13th Annual International Cryptology Conference，Berlin Heidelberg：Springer，1993：480-491.

[2] BONEH D，GENTRY C，WATERS B.Collusion resistant broadcast encryption with short ciphertexts and private keys[C]//Proc.of the 25th Annual International Cryptology Conference，Berlin Heidelberg：Springer，2005：258-275.

[3] GENTRY C，WATERS B.Adaptive security in broadcast encryption systems(with short ciphertexts)[C]//Proc.of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques，Berlin Heidelberg：Springer，2009：171-188.

[4] WATERS B.Dual system encryption：realizing fully secure ibe and hibe under simple assumptions[C]//Proc.of the 29th Annual International Cryptology Conference，Berlin Heidelberg：Springer，2009：619-636.

[5] BONEH D，WATERS B，ZHANDRY M.Low overhead broadcast encryption from multilinear maps[C]//Proc.of the 34th Annual International Cryptology Conference，Berlin Heidelberg：Springer，2014：206-223.

[6] ZHANDRY M.Adaptively secure broadcast encryption with small system parameters[J].IACR Cryptology ePrint Archive，2014：757.

[7] GUO D，WEN Q，LI W，et al.Adaptively secure broadcast encryption with constant ciphertexts[J].IEEE Transactions on Broadcasting，2016，62(3)：709-715.

[8] Hu Yupu，Jia Huiwen.Cryptanalysis of GGH map[C]//Proc.of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques，Berlin Heidelberg：Springer，2016：537-565.

[9] KIM J，SUSILO W，MAN H A，et al.Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext[J].IEEE Transactions on Information Forensics & Security，2015，10(3)：679-693.

[10] GUO D，WEN Q，JIN Z，et al.Authenticated public key broadcast encryption with short ciphertext[J].Multimedia Tools and Applications，2019，78：23399-23414.

[11] GUO D，WEN Q，LI W，et al.Adaptively secure broadcast encryption with authenticated content distributors[J].Multimedia Tools and Applications，2020，79：7889-7910.

[12] BONEH D，FRANKLIN M.Identity based encryption from the Weil pairing[C]//Proc.of the 24th Annual International Cryptology Conference，Berlin Heidelberg：Springer，2001：213-229.

[13] BONEH D，GENTRY C，LYNN B，et al.Aggregate and verifiably encrypted signatures from bilinear maps[C]//Proc.of the 22nd International Conference on Theory and Applications of Cryptographic Techniques，Berlin Heidelberg：Springer，2003：416-432.

[14] BONEH D，LYNN B，SHACHAM H.Short signatures from the weil pairing[J].Journal of Cryptology，2004，17(4)：297-319.

（收稿日期：2020-08-20）

作者简介：

国佃利(1988-)，男，博士，工程师，主要研究方向：移动通信、广播加密。

刘家磊(1982-)，通信作者，男，博士，讲师，主要研究方向：服务计算、云计算、移动边缘计算，E-mail：01850@aynu.edu.cn。

王萍(1990-)，女，硕士，助理工程师，主要研究方向：移动通信、企业安全评估。

扫码下载电子文档

（上接第 54 页）

[6] KNUTH D E，MORRIS J H，PRATT V R.Fast pattern matchingin strings[J].SIAM J.Comput.，1977，6(1)：323-350.

[7] WU S，MANBER U.A fast algorithm for multipattern searching[Z].Report TR-94-17，Department of Computer Science，University of Arizona，Tucson，AZ，1994.

[8] ROMAN E，AMBLER S.Mastering enterprise JavaBeans[M].Wiley Publishing，2002.

[9] JOHNSON R.Expert one-on-one J2EE development without EJB[M].Wiley Publishing，2004.

[10] JOHNSON R.Expert one-on-one J2EE design and development[M].WroxsPress，2003.

[11] 巫喜红，凌捷.BM 模式匹配算法剖析[J].计算机工程与设计，2007(1)：29-31.

[12] 陈新驰，韩建民，贾洞.基于 AC 自动机的多模式匹配算法 FACA[J].计算机工程，2012，38(11)：173-176.

[13] 陈洪涛，王法玉，靳彩园，等.多模式匹配算法的应用与改进[J].中国科技信息，2019，618(23)：78-80.

[14] 孙强，辛阳，陈林顺.AC 多模式匹配算法的优化与应用[J].中国科技论文在线，2011，6(1)：45-48.

[15] 董世博，李训根，殷珍珍.一种改进的字符串多模式匹配算法[J].计算机工程与应用，2013，49(8)：133-137.

（收稿日期：2020-09-23）

作者简介：

滕斌(1993-)，男，硕士研究生，主要研究方向：计算机视觉、图像处理。

林志贤(1975-)，通信作者，男，博士，教授，博士生导师，主要研究方向：信息显示技术、平板显示驱动系统及图像处理，E-mail：lzx2005000@163.com。

扫码下载电子文档

# 版权声明