中国科学: 信息科学 2010 年 第 40 卷 第 2 期: 371～380
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

抗窃听的安全网络编码

罗明星[①②③*], 杨义先[①②③], 王励成[①②③], 钮心忻[①②③]

① 北京邮电大学网络与交换技术国家重点实验室信息安全中心, 北京 100876;
② 北京邮电大学网络与信息攻防技术教育部重点实验室, 北京 100876;
③ 北京邮电大学灾备技术国家工程实验室, 北京 100876
* 通信作者. E-mail: luomxgg@yahoo.com.cn

收稿日期: 2009–06–07; 接受日期: 2009–11–10
国家自然科学基金与香港研究资助局联合科研基金 (批准号: 60731160626)、高等学校学科创新引智计划 (批准号: B08004)、国家自然科学基金 (批准号: 60821001, 90718001) 和中央高校基本科研业务 (批准号: BUPT2009RC0220) 资助项目

摘要 文中构造信息论意义下的安全网络编码以抗窃听攻击. 基于广义攻击模型和 all-or-nothing 变换, 构造广义组合网络上的安全网络编码, 其安全性由网络容量和窃听集的最小割共同决定. 进而, 此结论被推广到任意单信源有向无圈网络. 与已有结论相比, 这种安全网络编码无额外加密开销, 也无传输容量损失.

关键词
all-or-nothing 变换
安全网络编码
窃听

1 引言

Ahlswede 等 [1] 首先提出网络编码, 其特征体现在网络中间节点的每个输出信息都是所有输入信息的函数. 各种编码函数刻画不同类型的网络编码, 如线性函数和随机线性函数分别对应于线性网络编码和随机线性网络编码 [1~3]. 众所周知, 很容易构造单信源有向无圈网络上的达到不同最大流最小界层次的线性网络编码, 如多播、广播、散布、通有和静态网络编码等 [1,3,4]. Jaggi 等 [5] 提出一个针对任意无圈网络的有效构造方法. 若无中心机构, 为恢复网络容量和可达速率, Ho 等 [2] 提出随机线性网络编码, 并证明以分布式方式构造此网络编码. Koetter 等 [6] 提出基于系统理论的网络编码的代数框架, 将已有结果扩展到任意网络, 并证明带延迟有圈网络的时不变网络编码的可达性. 此网络编码也达到其网络的最大流最小割界.

为实现基于网络编码的安全通信, 如下两类攻击模式已被广泛讨论. 第一类称为窃听攻击, 即一些节点出于好奇或获取消息的目的窃听一些网络联接. 对于好奇的节点, 随机线性网络编码具有内在的安全功能 [7]. 若给定窃听集合, Cai 等 [8] 证明在单信源有向无圈网络上存在信息论意义下的安全线性网络编码 (以下简称信息论安全网络编码). 利用码字的代数结构, 可将此结果推广到一些多信源网络 [9,10]. Feldman 等 [11] 给出文献 [8] 中的一等价问题, 即寻找满足广义距离的线性码. Bhattad 和 Narayanan[12] 提出刻画安全性的不同标准, 即假设窃听者不能获取任何未编码或原始的数据则称为安全. 此安全问题被转化为概率优化问题 [13]. 然而, 最坏窃听者可窃听除合法通信者共享的密钥外的所有传输数据. 针对此类窃听者, 与随机线性网络编码可达的保密性相比实际安全网络编码方案 [14] 可达一般安全. 此方案提供一种开发内在安全性的方式, 以减少安全通信所需的加密操作. 此外, 文

引用格式: 罗明星, 杨义先, 王励成, 等. 抗窃听的安全网络编码. 中国科学: 信息科学, 2010, 40: 371–380

献 [15] 也证明此方案可达到信息论安全而无损解码概率. 第二类攻击模式称为拜占庭攻击, 即攻击者可能会修改编码数据. 为解决此问题, Koetter 和 Kschischang [16] 提出秩距离纠错码, 然后扩展到信道可提供部分信息—有关传输数据的擦除和偏移信息 [17]. 与此同时, 一些网络纠错码也被提出 [18~21]. Ho 等 [22] 结合密码学提出一信息论框架以检测拜占庭攻击. Charles 等 [23] 提出一同构签名方案. 该方案被用来构造基于配对的网络编码. 最近, 文献 [24] 提出一签名方案以检测给定数据是否属于某原始消息空间. Boneh 等 [25] 提出两签名方案以提供抗污染攻击的加密保护.

本文主要考虑窃听攻击, 目的在于克服已有安全网络编码的主要缺陷, 即随机密钥的传输冗余和窃听集的特定限制 [8~12,18~21]. 通过定义广义攻击模型以刻画实际窃听者. 为构造信息论安全网络编码, 本文推广了由 Stinson[26] 提出的 all-or-nothing 变换. 此变换可达信息论安全而非计算安全 [27]. 基于此信息论安全变换, 我们构造了广义组合网络上的安全网络编码, 其安全性可由网络容量和窃听集的最小割完全刻画. 进而, 此结论被推广于任意单信源有向无圈网络. 在窃听者不能获取任何传输信息意义下, 网络编码 [8~10] 可提供强安全, 而从本文的信息论安全网络编码窃听者也不能获取任何原始消息 [12,26,27]. Cai 等定义的传统窃听模型 [8~10] 要求在构建安全网络编码之前给定窃听集, 本文只限制窃听集的最小割而无其他约束. 即使在相同的窃听集条件下, 本文的安全网络编码无任何传输冗余, 而文献 [8 ~ 10] 需要放弃部分带宽以传输安全密钥. 当然, 文献 [8 ~ 11, 18 ~ 21] 的另一个动机在于研究最佳网络纠错码, 以纠正一些随机错误或注入错误, 这超出本文讨论范围. 弱安全网络编码 [12] 不仅依赖于给定的多播网络编码, 而且每一次完整会话也不安全, 然而本文无需给定任何网络编码就能构造信息论安全多播、广播、散布、通用和静态网络编码. 此外, 本文也讨论一些广义组合网络, 并提出多项式复杂度算法以构造任意单信源有限无圈网络的安全网络编码, 最后给出由随机线性网络编码构造安全网络编码的成功概率.

本文安排如下. 第 2 节给出一些准备知识. 第 3 节讨论广义组合网络的安全网络编码. 第 4 节讨论任意单信源有限无圈网络的安全网络编码. 第 5 节给出随机线性网络编码方案. 第 6 节给出一些例子. 第 7 节总结全文.

2 预备

此节给出安全通信的图模型、攻击模型、all-or-nothing 变换等必要记号和术语.

2.1 图模型

基于 Ahlswede[1] 等和 Cai 等 [8] 的模型, 一个图代表一个有向多图, 即所有边有方向, 并允许节点之间多条边相连. 记 $\mathcal{G}$ 为一个图, 其节点集为 $\mathcal{V}(\mathcal{G})$, 边集为 $\mathcal{E}(\mathcal{G})$. 假设 $\mathcal{E}(\mathcal{G}) \subset \mathcal{V}(\mathcal{G}) \times \mathcal{V}(\mathcal{G}) \times \mathbb{N}$, 其中第 3 个分量用以区别两节点之间的不同边. 对于 $A, B \subset \mathcal{V}(\mathcal{G})$, 记 (A, B) 为 $\mathcal{G}$ 中起于 A 中节点止于 B 中节点的所有边集. 记 $(a, B) := (\{a\}, B)$, $(A, b) := (A, \{b\})$.

对于节点 u, v, 若 $(u, v) \in \mathcal{E}(\mathcal{G})$, 则称 u 为 v 的父节点; 若 $(v, u) \in \mathcal{E}(\mathcal{G})$, 则称 u 为 v 的子节点. 对于 $e = (u, v)$, 令 $\mathrm{tail}(e) = u$, $\mathrm{head}(e) = v$. $\mathrm{In}(v)$ 和 $\mathrm{Out}(v)$ 分别代表节点 v 的输入边集和输出边集.

一个单源多播网络 $\mathcal{N} = (\mathcal{G}, s, T)$ 由一有向多图 $\mathcal{G}$、一信源节点 s 和一信宿节点集 $T \not\ni s$ (每个节点的最大流不小于网络容量) 构成. 信源节点将消息多播给 T 的所有节点.

2.2 攻击模型

在一个无圈网络中, 若将所有最大流不小于网络容量的节点定义为通信方, 其他节点和边定义为

参与方, 那么通信的目的就在于通信方给参与方安全传输消息. 在此情形下, 参与方不限个数. 作为参与方的传输边仅传输消息, 而节点则需对输入消息作必要运算以完成传输协议, 这些特殊运算依赖于传输方案, 如随机线性组合、确定线性组合或非线性运算分别相应于随机线性网络编码、确定线性网络编码或非线性网络编码.

攻击模型描述如下:

1. 场景: 一个单信源多播网络 $\mathcal{N}=(\mathcal{G},s,T)$, 其中 T 为所有最大流不小于网络容量 ω 的节点集, ω 为信源向信宿的多播速率. 信源 s 向所有信宿多播消息 $\{\alpha_1,\ldots,\alpha_\omega\}$.

2. 攻击者: 攻击者在会话前选择一窃听集 $A\subset\mathcal{G}$ 满足 min-cut$(A)<\omega$, 其中 min-cut(A) 表示 A 的最小割 (从信源到 A 的最大不相邻道路数 [28]).

3. 攻击目标:

$$\text{Output}(\mathcal{N},A)\cap\{\alpha_1,\ldots,\alpha_\omega\}\neq\emptyset,$$

即攻击者想获取 $\{\alpha_1,\ldots,\alpha_\omega\}$ 的部分消息.

不失一般性, 本文假设窃听者在会话前选择窃听集 $A\subset\mathcal{G}$. 信源和信宿都不知道 A, 但在一次完整会话过程中 A 是固定不变的. 窃听者控制 A 中的所有对象, 他可以窃听流经的所有数据. 由于信宿不能为窃听者, 安全传输可定义为 T 中所有节点能正确恢复消息 $\{\alpha_1,\ldots,\alpha_\omega\}$, 同时窃听者不能获取任何消息.

2.3 All-or-nothing 变换

Rivest[27] 首先定义如下 all-or-nothing 变换.

函数 ϕ 为 $\mathbb{X}^m$ 到 $\mathbb{X}^m$ 的 all-or-nothing 变换如果它满足如下性质:

1. ϕ 为双射.

2. 如果固定 m 个输出值 $y_1,\ldots,y_m$ 中的任意 $m-1$ 个, 任何一输入值 $x_i(1\leqslant i\leqslant m)$ 都完全待定, 其中 $\mathbb{X}$ 为一有限符号集, m 为正整数.

为表述结论, 我们定义如下广义 all-or-nothing 变换.

定义 1 记 $X_1,\ldots,X_m,Y_1,\ldots,Y_n(n\leqslant m)$ 为一些取值于有限集 $\mathbb{X}$ 的随机变量 (可以非独立或非一致分布). 广义 all-or-nothing 变换 ϕ 可通过熵函数 H 表述如下:

1. $H(Y_1,\ldots,Y_n|X_1,\ldots,X_m)=0$.

2. 若 $n=m$, $H(X_1,\ldots,X_m|Y_1,\ldots,Y_m)=0$.

3. 对于所有 $i,j,1\leqslant i\leqslant m,1\leqslant j\leqslant n$, $H(X_i|Y_1,\ldots,Y_{j-1},Y_{j+1},\ldots,Y_n)=H(X_i)$.

当 $n=m$ 时, 此广义 all-or-nothing 变换即为 Stinson[26] 所定义的 all-or-nothing 变换. 此处的广义变换是信息论安全的, 而非计算安全 [27]. 对于一基于有限域 $\mathbb{F}_q$ 的 all-or-nothing 变换, 如果每个 y_i 是 $x_1,\ldots,x_m$ 的 $\mathbb{F}_q$-线性函数, 则此变换是线性的. 如下定理给出线性 all-or-nothing 变换的有效构造方法.

定理 1 假设 $\boldsymbol{M}$ 为 $m\times m$ 可逆矩阵, 其元素属于 $\mathbb{F}_q^*$, 则由 $\phi(\boldsymbol{x})=\boldsymbol{M}^{-1}\boldsymbol{x}$ 所定义的函数 $\phi:\mathbb{F}_q^m\to\mathbb{F}_q^m$ 为线性 all-or-nothing 变换, 其中上指标 -1 表示矩阵逆 (见文献 [26] 定理 2.1).

由定义 1 的条件 3 可知, 从 $n<m$ 个方程不能解出输入值 x_i, 因此可得如下广义线性 all-or-nothing 变换的判断定理.

定理 2 记 $\phi:\mathbb{F}^m\to\mathbb{F}^n$, $\phi(\boldsymbol{x})=\boldsymbol{M}_{n\times m}\boldsymbol{x}$, $\mathbb{F}$ 为一有限域. ϕ 为广义线性 all-or-nothing 变换 $(n<m)$ 当且仅当通过删除 $\boldsymbol{M}_{n\times m}$ 的第 i 列所得的行向量集线性独立, 或 $\boldsymbol{M}_{n\times m}$ 的行向量集线性相

关, 并且对 $i=1,\ldots,m$ 通过删除 $\boldsymbol{M}_{n\times m}$ 的第 i 列所得的行向量集线性相关.

证明 由广义 all-or-nothing 变换的定义, 对 $i=1,\ldots,m$, 若通过删除 $\boldsymbol{M}_{n\times m}$ 的第 i 列所得的行向量集线性独立, 那么 $\phi(\boldsymbol{x})=\boldsymbol{M}_{n\times m}\boldsymbol{x}$ 为广义线性 all-or-nothing 变换. 同时若 $\boldsymbol{M}_{n\times m}$ 的行向量集线性相关, 并且通过删除 $\boldsymbol{M}_{n\times m}$ 的第 i 列所得的行向量集线性相关, 则存在一些变换使得 $\boldsymbol{M}_{n\times m}$ 可表示为 $(\boldsymbol{0};\hat{M}_{(n-1)\times m})$, 其中 $\hat{\boldsymbol{M}}_{(n-1)\times m}$ 为 $(n-1)\times m$ 矩阵. 因此由 $y_1,\ldots,y_n$ 不能得到 $x_1,\ldots,x_m$. 类似可证条件的必要性.

2.4 安全网络编码

在介绍安全网络编码之前, 首先给出线性网络码的全局描述 [3,4].

定义 2 对于一个无圈网络, 一个基于有限域 $\mathbb{F}$ 的 ω–维线性网络码可由每个信道对 (d,e) 的特定常数 $k_{d,e}$ 和信道 e 上的特定 ω–维列向量 $\boldsymbol{f}_e$ 共同描述如下:

1. $\boldsymbol{f}_e=\sum_{d\in \mathrm{In}(t)} k_{d,e}\boldsymbol{f}_d$, $e\in \mathrm{Out}(t)$.

2. ω 条虚拟信道 $e\in \mathrm{In}(s)$ 上的向量 $\boldsymbol{f}_e$ 构成向量空间 $\mathbb{F}^\omega$ 的一组标准基, $\boldsymbol{f}_e$ 称为信道 e 的全局编码核.

定义 3 考虑多播网络 $\mathcal{N}=(\mathcal{G},s,T)$, 多播消息为 $\{\alpha_1,\ldots,\alpha_\omega\}$. 线性网络码是信息论安全的网络码当且仅当满足 $\text{min-cut}(A)<\omega$ 的任意攻击者不能获取任何原始消息 α_i, $i=1,\ldots,\omega$, 其中 A 为窃听集.

由定义 1, 此处的安全性不同于以前给定窃听集的安全性. 本文考虑构造任意单信源有向无圈网络上的信息论安全网络编码, 且仅限制窃听集的最小割.

3 组合型网络上的安全网络编码

组合网络因其简单性和对称性被广泛运用于网络设计、组合设计、编码、密码学等领域 [28]. 此节给出两类广义组合网络, 并设计相应的安全多播网络编码. I 型 $\binom{m}{n}$ 组合网络满足如下条件:

1. 第 1 层只有一个节点, 且为信源.

2. 第 2 层有 m 节点, 且每个节点和信源相连.

3. 第 3 层的每个节点有不多于 n 条输入边, 且每条输入边源自第 2 层的不同节点.

如果第 3 层有 C_m^n(不考虑顺序, 从 m 个不同球中选出 n 球个的组合数) 个节点, 并且第 3 层的每个节点有 n 条输入边, 那么如上所定义的组合型网络即为经典 $\binom{m}{n}$ 组合网络. 由此定义可知组合型网络为有向无圈网络, 第 6 节将给出一些例子.

下面给出 I 型 $\binom{m}{n}$ 组合网络上的安全网络编码.

定理 3 考虑 I 型 $\binom{m}{n}$ 组合网络, 假设对每个窃听集 A 有$\text{min-cut}(A)<n$, 则存在信息论安全网络编码多播消息 $\{\alpha_1,\ldots,\alpha_n\}$.

证明 考虑矩阵

$$\boldsymbol{V}_{n\times(q-1)}=\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & x_1 & \cdots & x_{q-2}\\ \vdots & \vdots & \vdots & \vdots\\ 1 & x_1^{n-1} & \cdots & x_{q-2}^{n-1}\end{pmatrix},$$

其中 $x_i(i=1,\ldots,q-2)\in\mathbb{F}_q-\{0,1\}$ 互不相同.

由于

$$\det\begin{pmatrix}1 & \cdots & 1\\ x_1 & \cdots & x_{n-1}\\ \vdots & \vdots & \vdots\\ x_1^{n-1} & \cdots & x_{n-1}^{n-1}\end{pmatrix}=\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\neq 0 \mod q,$$

$\boldsymbol{V}_{n\times(q-1)}$ 的任意 $k\,(1\leqslant k\leqslant n)$ 列线性独立, 因此, 由 $\boldsymbol{V}_{n\times(q-1)}$ 的列向量所构成的矩阵可诱导广义线性 all-or-nothing 变换 (即一矩阵可定义一线性 all-or-nothing 变换, 参考定理 1). 令 $\boldsymbol{V}_{n\times(q-1)}$ 为信源的全局编码核矩阵 (虚拟边上的)$(q\gg n)$(q 远大于 n). 将 $\boldsymbol{V}_{n\times(q-1)}$ 的列向量定义为信源输出边上的全局编码核向量, 而其他边由输入边直接确定. 从组合型网络的定义可知此网络编码能实现多播消息 $\{\alpha_1,\ldots,\alpha_n\}$, 其原因在于 $\boldsymbol{V}_{n\times(q-1)}$ 的任意 n 列非退化, 即第 3 层中有 n 条输入边的节点均可恢复所有消息. 与此同时, 满足 min-cut$(A)<n$ 的任意窃听者均不能获取任何原始消息 (窃听者最多可得 min-cut(A) 个线性独立的方程, 而从这些方程不能解出任何 $\alpha_i, i=1,\ldots,n$, 参考定理 2). 因此, 存在信息论安全网络编码多播消息 $\{\alpha_1,\ldots,\alpha_n\}$.

现在, 考虑 II 型 $\binom{m}{n}$ 组合网络, 它满足如下条件:

1. 第 1 层只有一个节点, 且为信源.

2. 第 2 层有 m 节点, 且每个节点和信源相连.

3. 第 3 层的每个节点有不多于 n 条输入边, 且每条输入边源自第 2 层的不同节点.

4. 第 4 层中的每个节点有不多于 n 条输入边, 且每条输入边源自第 3 层的不同节点.

与 I 型组合网络类似, 可得如下定理.

定理 4 考虑 II $\binom{m}{n}$ 组合网络, 若对每个窃听集 A 有min-cut$(A)<n$, 则存在信息论安全网络编码多播消息 $\{\alpha_1,\ldots,\alpha_n\}$.

由定理 3 和附录中的引理 A1 可得此定理的证明.

4 安全线性网络编码

此节考虑任意单信源有向无圈网络上的安全网络编码. 与第 3 节的组合网络相比, 任意有限无圈网络上的安全网络编码还依赖于网络拓扑.

令 $\lambda_{\mathcal{N}}$ 表示所有中间节点 (除信源和信宿外) 的最小输入边数 (非 1 的), 即

$$\lambda_{\mathcal{N}}=\min_{v\in\mathcal{V}\backslash T}\{|\mathrm{In}(v)|,\text{s.t. }|\mathrm{In}(v)|\neq 1\}. \tag{1}$$

结合已有算法 [5,8] 和广义 all-or-nothing 变换可得如下定理.

定理 5 考虑无圈多播网络 $\mathcal{N}=(\mathcal{G},s,T)$, 若对每个窃听集 A 有min-cut$(A)<\lambda_{\mathcal{N}}$, 则存在信息论安全网络编码多播消息 $\{\alpha_1,\ldots,\alpha_n\}$.

证明 对于任意无圈多播网络, 由最大流最小割定理和已有结论 [5,8], 存在线性网络编码多播消息 $\{\alpha_1,\ldots,\alpha_\omega\}$ 给 T 的每个节点. 此网络码没考虑安全性. 事实上, 记此线性码为 $\mathcal{C}$. 由全局编码核的定义 [4] 可得信源 s 的编码核矩阵为 $(\boldsymbol{I}_{\omega\times\omega}\,\boldsymbol{M}_{\omega\times(l-\omega)})$, 其中 $\boldsymbol{M}_{\omega\times(l-\omega)}$ 为 $\omega\times(l-\omega)$ 矩阵, l 表示

信源 s 的输出边数. 窃听者通过窃听信源的输出边可得部分原始消息. 这样, 出于安全性考虑必须重新构造信源 s 的编码核矩阵.

以下从代数组合理论或拟阵理论 [28] 来构造信源 s 的编码核矩阵. 令

$$\boldsymbol{V}_{\omega\times n}=\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & x_1 & \cdots & x_n\\ \vdots & \vdots & \vdots & \vdots\\ 1 & x_1^{\omega-1} & \cdots & x_n^{\omega-1}\end{pmatrix},$$

其中 $x_i(i=1,\ldots,n)\in\mathbb{F}-\{0,1\}$ 互不相同. 由拟阵和 MDS 码的等价性, $\boldsymbol{V}_{\omega\times n}$ 为某拟阵的向量表示. 进而, 由有限域理论若 $x_i\neq 0$ 有 $x_i^j\neq 0$, 且若 $\mathbb{F}$ 充分大则 $n\geqslant l$.

设 $\boldsymbol{V}_{\omega\times l}$ 为信源 s 的编码核矩阵. 基于已有算法 [4,5], 我们给出如下安全多播算法.

此算法构造单信源有向无圈网络上的一基于大数域 $\mathbb{F}$ 的 ω– 维安全线性多播, 其中 $\eta=|T|$ 表示 max-flow$(t)\geqslant\omega$ 的信宿数, L_k 表示连向信宿 t_j 的一条道路.

一信道序列 $e_1,\ldots,e_l$ 称为连向节点 t_k 的道路如果满足 $e_1\in\mathrm{Out}(s), e_l\in\mathrm{In}(t_k)$, 并且 (e_j,e_{j+1}) 是一个邻接对, $1\leqslant j\leqslant l-1$. 对于每个 $k, 1\leqslant k\leqslant\eta$, 存在 ω 条边不相邻的道路 $L_{k,1},\ldots,L_{k,\omega}$ 连向 t_k, 这里共有 $\eta\omega$ 条类似道路. 在网络上定义一个自上向下的顺序. 下面的程序给出每条信道 e 的全局编码核向量 $\boldsymbol{f}_e$.

算法 1

利用 $\boldsymbol{V}_{\omega\times\ell}$ 的列向量初始化所有信道 $e_{j,i}$ 的全局编码核.
for (从上向下顺序中的每个节点 t)
  for (每条信道 $e\in\mathrm{Out}(t)$)
    1. 对于信道 e, 若信道 e 在道路 $L_{j,i}$ 上则定义一指标 "对" (j,i).[a)]
    2. 选择一向量 $\boldsymbol{w}\in V_t$ 使得 $\phi(\boldsymbol{x})=\boldsymbol{M}\boldsymbol{x}$ 为广义线性 all-or-nothing 变换, 其中对每个指标对 (j,i), $\boldsymbol{M}=(\boldsymbol{w},\boldsymbol{f}_{e_{j,i}},k\neq i)$.
  $\boldsymbol{f}_e=\boldsymbol{w}$.

注 a) 对每个 j, 最多存在一指标对 (j,i). 因为节点 t 按从上向下顺序选择, 若 (j,i) 为一指标对, 则递归可得 $e_{j,i}\in\mathrm{In}(t)$, 且满足 $\boldsymbol{f}_{e_{j,i}}\in V_t$. 从算法后面的解释可得 $\boldsymbol{f}_{e_{j,i}}\in V_t\setminus\langle\{\boldsymbol{f}_{e_{j,k}};k\neq i\}\rangle$, 并且 $\boldsymbol{f}_{e_{j,i}}$ 满足安全性要求.

在继续证明之前, 需要证明算法中 $\boldsymbol{w}$ 的存在性. 事实上, 令 $\dim(V_t)=\nu$. 对每个指标对 (j,i) 因为 $\boldsymbol{f}_{e_{j,i}}\in V_t\setminus\langle\{\boldsymbol{f}_{e_{j,k}}:k\neq i\}\rangle$, 从而有 $\dim(V_t\cap\langle\{\boldsymbol{f}_{e_{j,k}}:k\neq i\}\rangle)\leqslant\nu-1$, 这样 $|V_t\cap(\cup_{(q,i)}\langle\{\boldsymbol{f}_{e_{j,k}}:k\neq i\}\rangle)|\leqslant\eta|\mathbb{F}|^{\nu-1}<|\mathbb{F}|^{\nu}=|V_t|$. 因此, 存在 $\boldsymbol{w}\in V_t$ 使得对每个指标对 (j,i) [4,5] 有 $\boldsymbol{w}\notin\langle\{\boldsymbol{f}_{e_{j,i}};k\neq i\}\rangle$. 若 $\nu=\omega$, 从附录引理 A1 可得 $\boldsymbol{w}$. 若 $\nu<\omega$, 从 $\lambda_{\mathcal{N}}$ 的假设有 $\nu\geqslant\lambda_{\mathcal{N}}$. 记 B 为任意 $m-1$ 条信道的集合, $1\leqslant m\leqslant\nu$, 满足 $\{\boldsymbol{f}_e,e\in B\}$ 线性无关, 并且 $V_t\not\subset V_B$. 以下将寻找 $\boldsymbol{w}\in V_t\setminus(\cup_{(q,i)}\langle\{\boldsymbol{f}_{e_{j,k}}:k\neq i\}\rangle)$, 满足对任意 B, $\boldsymbol{M}_B:=(\boldsymbol{w},\boldsymbol{f}_e,e\in B)$ 能诱导一广义线性 all-or-nothing 变换. 从附录引理 A2 的证明 (对所有满足 min-cut$(B)\leqslant\nu-1$ 的窃听集 B, 利用附录不等式 (A1)) 和通有网络编码的构造 [4], 对充分大 q, 可得 $|V_t\cap((\cup_B V_B)\cup(\cup_B\boldsymbol{M}'_B))|\leqslant\sum_{\jmath=1}^{\nu}C_{|\mathcal{E}|-1}^{\jmath-1}q^{\nu-1}+\sum_{\jmath=1}^{\nu}C_{|\mathcal{E}|-1}^{\jmath-1}\omega q^{\jmath-1}<q^{\nu}=|V_t|$, 其中, $\boldsymbol{M}'_B$ 表示 B 中信道上的全局编码核向量构成的矩阵, 并且能诱导一广义线性 all-or-nothing 变换. 从而完成存在性证明.

现在继续证明定理. 预乘的矩阵 (即信源的编码核矩阵) 可定以一广义线性 all-or-nothing 变换, 故可达信息论安全 [26]. 进而, 从上算法可知, 最小割小于 $\lambda_{\mathcal{N}}$ 的窃听者不能得到任何原始消息 (不能对角化编码系数矩阵), 从而如上所得多播网络编码是信息论安全的 [4,5].

复杂度分析 网络共 $|\mathcal{E}|$ 条信道. 在算法的第一个 "for" 循环中, 对于每个信道 e 最多有 η 指标对, 从而对于整个算法, 最多有 $|\mathcal{E}|\eta$ 个指标对, 并需要证实 $\sum_{k=1}^{\omega-1} C_{|\mathcal{E}|-1}^{k-1}$ 个可能的广义线性 all-or-nothing 变换. 由此不难推出对固定 ω 此算法为 $|\mathcal{E}|$ 的多项式算法 [5].

5 安全随机线性网络编码

考虑任意单信源有向无圈网络的安全多播问题. 若从有限域 $\mathbb{F}_q$ 中随机选取部分或所有编码系数 $\{k_{d,e}, \boldsymbol{f}_d\}$ 来构造网络编码, 并且其他编码系数如果存在则固定不变 [2], 那么此网络编码为随机线性网络编码, 其中 $q > d$.

定理 6 考虑无圈多播网络 $\mathcal{N} = (\mathcal{G}, s, T)$, 假设对于任意窃听集 A 满足$\text{min-cut}(A) < \lambda_{\mathcal{N}}$, 则一个随机线性网络编码为信息论安全网络编码的概率不小于 $(q-d)^{\eta}(q-\lambda_{\mathcal{N}}(\lambda_{\mathcal{N}}+1)+1)^{|\mathcal{E}|}/q^{\eta+|\mathcal{E}|}$, 其中 η 表示导向任意信宿的信息流上的随机编码系数的最大个数, $\lambda_{\mathcal{N}}$ 由 (1) 式定义.

证明 由定理 2[2], 存在随机线性网络编码使得每个信宿能以不小于 $(1-d/q)^{\eta}$ 的概率恢复消息 $\{\alpha_1, \ldots, \alpha_n\}$, η 表示导向任意信宿的信息流上的随机编码系数的最大个数. 结合附录引理 A3 和定理 5 中的算法 (随机选择局部编码系数), 可知随机线性网络编码为信息论安全网络编码的概率不小于 $(q-d)^{\eta}(q-\lambda_{\mathcal{N}}(\lambda_{\mathcal{N}}+1)+1)^{|\mathcal{E}|}/q^{\eta+|\mathcal{E}|}$.

6 例子

此节给出一些例子以说明本文结论.

例 1 考虑图 1 所示 I 型 $(\frac{7}{3})$ 组合网络, 将一个 Vandermonde 矩阵定义为信源 s 的编码核矩阵, 则可得一个信息论安全网络编码多播消息 $\{a, b, c\}$, 即对于任意 $\text{min-cut}(A) < 3$ 的窃听者得不到任何原始消息, 其中 A 为窃听集. 这里 $\boldsymbol{e}_i = (1, \beta_i, \beta_i^2)^{\mathrm{T}}$, $i = 1, \ldots, 7$, $\beta_i \in \mathbb{F}_q^*$. 由 Vandermonde 矩阵的性质可证明网络编码的安全性.

例 2 考虑图 2 所示网络, 其全局编码核位于边上, 其中 $\boldsymbol{e}_i = (1, \gamma_i, \gamma_i^2)^{\mathrm{T}} (i = 1, \ldots, 4)$ 和 $(1, \beta_j, \beta_j^2)^{\mathrm{T}} (j = 1, \ldots, 12)$ 分别为信道 $(u_5, t_1), (u_5, t_2), (u_5, t_4)$, $(u_6, t_1), (u_6, t_3), (u_6, t_4), (u_7, t_1), (u_7, t_2)$, $(u_7, t_3), (u_8, t_2), (u_8, t_3)$ 和 (u_8, t_4) 的全局编码核向量, $\gamma_i, \beta_j \in \mathbb{F}_q^*$. 由于 $|\text{In}(u_i)| = 1$ 节点 $u_i (i = 1, \ldots, 4)$ 仅需路由. 由 Vandermonde 矩阵的性质可证明此网络编码达到信息论安全, 即对于任意 $\text{min-cut}(A) < 3$ 的窃听者得不到任何原始消息, 其中 A 为窃听集.

例 3 考虑图 3(a) 所示网络, 其通信目的在于向节点 t_1, t_2, t_3 多播消息 $\{a, b, c\}$. 通过采用 v_4 和 v_5 的等价形式, 以及删除无用节点 v_8 可得等价图 3(b). 这里, 出于方便假设 v_i 的所有输出边的全局编码核向量相同. 如果不考虑安全问题, 则很容易构造网络编码多播消息, 如 $\boldsymbol{e}_1 = (1, 0, 0)^{\mathrm{T}}, \boldsymbol{e}_2 = (0, 1, 0)^{\mathrm{T}}, \boldsymbol{e}_3 = (0, 0, 1)^{\mathrm{T}}, \boldsymbol{e}_4 = (1, 1, 0)^{\mathrm{T}}$ 和 $\boldsymbol{e}_5 = (0, 1, 1)^{\mathrm{T}}$. 信宿 $t_i (i = 1, 2, 3)$ 的解码矩阵分别为 $(\boldsymbol{e}_1 \quad \boldsymbol{e}_2 \quad \boldsymbol{e}_1 + \boldsymbol{e}_2), (\boldsymbol{e}_2 \quad \boldsymbol{e}_1 + \boldsymbol{e}_2 \quad \boldsymbol{e}_2 + \boldsymbol{e}_3)$ 和 $(\boldsymbol{e}_1 \quad \boldsymbol{e}_2 + \boldsymbol{e}_3 \quad \boldsymbol{e}_3)$, 因为这些矩阵都非退化, 从而每个信宿均可恢复所有消息.

如果存在窃听者, 则此网络编码不安全. 例如窃听者可窃听信道 $v_1 v_4'$, $v_2 v_6$ 或 $v_3 t_3$ 以获取相应的部分原始消息 a, b 或 c. 因此必须设计其他安全网络编码. 注意到 $\lambda_{\mathcal{N}} = 2$, 对于充分大素数域 $\mathbb{F}$, 设

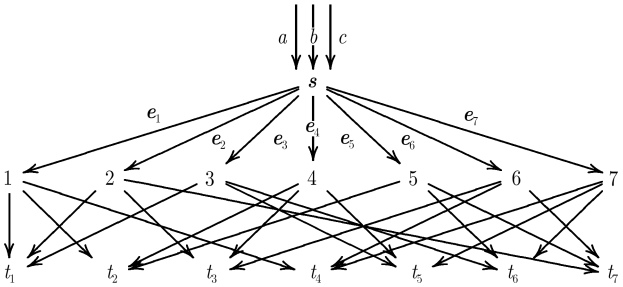


图 1　I 型 $(\frac{7}{3})$ 组合网络

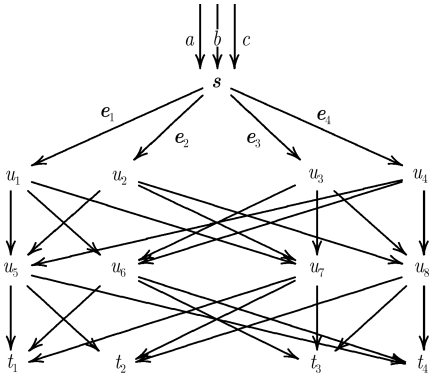
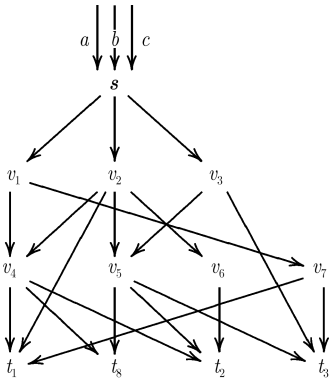
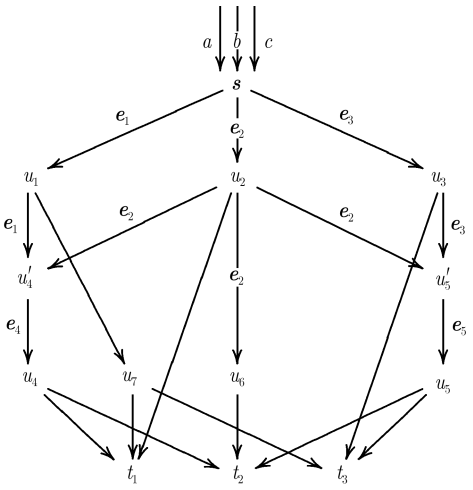


图 2　II 型 $(\frac{4}{3})$ 组合网络



(a) 带 4 个信宿的多播网络



(b) 图 (a) 的等价形式

图 3

$\boldsymbol{e}_1 = (6,-6,2)^{\mathrm{T}}, \boldsymbol{e}_2 = (-6,8,-3)^{\mathrm{T}}, \boldsymbol{e}_3 = (1,-2,1)^{\mathrm{T}}, \boldsymbol{e}_4 = \boldsymbol{e}_1 + \boldsymbol{e}_2 = (0,2,-1)^{\mathrm{T}}$ 和 $\boldsymbol{e}_5 = \boldsymbol{e}_2 + 3\boldsymbol{e}_3 = (-3,2,0)^{\mathrm{T}}$, 则可得一个安全网络编码使得任意 min-cut$(A) < 2$ 的窃听者都不能得到任何原始消息, 其中 A 为窃听集.

7　总结

本文给出信息论安全多播网络编码. 基于广义攻击模型和广义 all-or-nothing 变换, 我们证明在广义组合网络上存在信息论安全多播网络编码. 此结论也被推广到任意单信源有向无圈网络. 除窃听集的最小割限制外, 本文的安全网络编码没有放弃任何网络容量 (在蔡和杨的结论中用来传输额外的安全密钥). 定理 3 ~ 5 与密码学的门限方案相似, 其窃听的成功性由输入边的最小值和网络容量共同决定. 此外, 本文结论也可推广到其他线性网络编码, 如广播、散布、通有.

对于既有窃听者又有拜占庭攻击者的通信网络, 很难利用一种方法构造信息论安全网络编码而无损网络容量. 然而, 本文提供了一种混合信息的好方法, 且无传输冗余. 基于此特点, 结合简单 Hash 函数可以设计其他经济、可行的安全多播网络编码以抗击拜占庭攻击. 此结论已包括在其他论文中. 将来, 怎么结合诸如加密或 Hash 函数等密码学方法来实现安全性和传输效率的平衡不失为有趣问题.

致谢 感谢胡正名教授的宝贵意见.

参考文献

1 Ahlswede R, Cai N, Li S Y R, et al. Network information flow. IEEE Trans Inform Theor, 2000, 46: 1204–1216
2 Ho T, Médard M, Koetter R, et al. A random linear network coding approach to multicast. IEEE Trans Inform Theor, 2006, 52: 4413–4430
3 Li S Y R, Yeung R W, Cai N. Linear network coding. IEEE Trans Inform Theor, 2003, 49: 371–381
4 Yeung R W. Information Theory and Network Coding. Hongkong: Springer, 2008
5 Jaggi S, Sanders P, Chou P A, et al. Polynomial time algorithms for multicast network code construction. IEEE Trans Inform Theor, 2003, 51: 1973–1982
6 Koetter R, Médard M. An algebraic approach to network coding. IEEE/ACM Trans Netw, 2003, 11: 782–795
7 Lima L, Médard M, Barros J. Random linear network coding: a free cypher? In: Proceedings of the IEEE International Symposium on Information Theory. Nice: IEEE, 2007. 546–550
8 Cai N, Yeung R W. Secure network coding. In: Proceedings of the IEEE International Symposium on Information Theory. Lausanne: IEEE, 2002. 323
9 Cai N, Yeung R W. A security condition for multi-source linear network coding. In: IEEE International Symposium on Information Theory (ISIT). Nice: IEEE, 2007. 24–29
10 Yeung R W, Cai N. On the optimality of a construction of secure network codes. In: IEEE International Symposium on Information Theory (ISIT). Toronto: IEEE, 2008. 166–170
11 Feldman J, Malkin T, Servedio R A, et al. On the capacity of secure network coding. In: Proceedings of the 42nd Annual Allerton Conference on Communication, Control, and Computing, 2004. 388–401
12 Bhattad K, Narayanan K. Weakly secure network coding. In: Proceedings of the 1st Workshop on Network Coding, Theory, and Applications (NetCod), 2005. 148–153
13 Tan J, Médard M. Secure network coding with a cost criterion. In: Proceedings of the 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt'06), 2006. 1–6
14 Vilela J P, Lima L, Barros J. Lightweight security for network coding. In: IEEE International Conference on Communications, 2008. 1750–1754
15 Lima L, Vilela J P, Barros J, et al. An information-theoretic cryptanalysis of network coding is protecting the code enough? In: International Symposium on Information Theory and Its Applications (ISITA), 2008. 1–6
16 Koetter R, Kschischang F. Coding for errors and erasures in random network coding. IEEE Trans Inform Theor, 2008, 54: 3579–3591
17 Silva D, Kschischang F, Koetter R. A rank-metric approach to error control in random network coding. In: IEEE Information Theory Workshop on Information Theory for Wireless Networks, 2007. 1–5
18 Jaggi S, Langberg M, Katti S, et al. Resilient network coding in the presence of Byzantine adversaries. IEEE Trans Inform Theor, 2008, 54: 2596–2603
19 Cai N, Yeung R W. Network coding and error ecorrection. In: Proceedings of 2002 IEEE Information Theory Workshop, 2002 . 323
20 Yeung R W, Cai N. Network error correction, I: basic concepts and upper bounds. Commun Inf Syst, 2006, 6: 19–35
21 Zhang Z. Linear network error correction coding in packet networks. IEEE Trans Inform Theor, 2008, 54: 209–218
22 Ho T, Leong B, Koetter R, et al. Byzantine modification detection in multicast networks using randomized network coding. In: Proceedings of International Symposium on Information Theory (ISIT), 2004. 144
23 Charles D, Jain K, Lauter K. Signatures for network coding. In: Proceedings of the 40th Annual Conference on Information Sciences and Systems. Princeton, 2006. 857–863
24 Zhao F, Kalker T, Médard M, et al. Signatures for content distribution with network coding. In: International Symposium on Information Theory (ISIT). Nice, 2007. 556–560
25 Boneh D, Freeman D, Katz J, et al. Signing a linear subspace: signature schemes for network coding. In: Proceedings of PKC, 2009. 68–87
26 Stinson D R. Something about all or nothing (transforms). Des Code Crypt, 2001, 22: 133–138

27 Rivest R L. All-or-nothing Encryption and the package transform. In: Biham E, ed. Fast Software Encryption, LNCS 1267. Berlin: Springer, 1997. 210–218

28 West D B. Introduction to Graph Theory. 2nd ed. New Jersey: Prentice Hall, 2001

附录 A

以下给出一些必要的引理及其证明.

引理 A1 若 $\phi(\boldsymbol{x})=\boldsymbol{M}_{n\times n}\boldsymbol{x}$ 为线性空间 $\mathbb{F}_q^n$ 到 $\mathbb{F}_q^n$ 的线性 all-or-nothing 变换, 则存在 all-or-nothing 变换 $\varphi(\boldsymbol{x})=\boldsymbol{M}'_{n\times n}\boldsymbol{x}$ 使得 $\boldsymbol{M}'_{n\times n}$ 和 $\boldsymbol{M}_{n\times n}$ 有 $i\,(1\leqslant i\leqslant n)$ 个不同列向量, 其中 q 充分大.

证明 通过递归来寻找 $\boldsymbol{M}'_{n\times n}$. 记 $\boldsymbol{M}_{n\times n}=(\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n)$. 首先, 证明存在一些常数 $a_1,\ldots,a_n$ 使得矩阵 $(\sum_{i=1}^n a_i\boldsymbol{v}_i,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_n)^{-1}$ 诱导一个线性 all-or-nothing 变换. 事实上, 若对于每个 $1\leqslant i,j\leqslant n$ 有 $\det(\boldsymbol{M}_{ij})\neq 0$ 则 $\varphi(\boldsymbol{x})=\boldsymbol{M}'_{n\times n}\boldsymbol{x}$ 为一线性 all-or-nothing 变换, 其因为在于 $\boldsymbol{M}_{n\times n}^{-1}=(\det(\boldsymbol{M}_{ij}))_{n\times n}/\det(\boldsymbol{M}_{n\times n})$ 没有零分量 (参考定理 1), 这里 $\boldsymbol{M}_{ij}$ 表示删除矩阵 $(\sum_{i=1}^n a_i\boldsymbol{v}_i,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_n)^{-1}$ 第 i 行和第 j 列所得的子矩阵. 因此, 只需找到一些常数 $a_1,\ldots,a_n$ 使得 $\boldsymbol{w}=\sum_{i=1}^n a_i\boldsymbol{v}_i$ 满足对于所有 $1\leqslant i,j\leqslant n$ 有 $f(\boldsymbol{w})_{ij}:=\det(\boldsymbol{M}_{ij})\not\equiv 0 \mod q$ 和 $f(\boldsymbol{w}):=\det(\sum_{i=1}^n a_i\boldsymbol{v}_i,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_n)\not\equiv 0 \mod q$. 而对于每个 $1\leqslant i,j\leqslant n$, 由行列式的多线性知 $f(\boldsymbol{w})_{ij}\equiv 0 \mod q$ 定义 $\mathbb{F}_q^n$ 的一超平面, 其变量为 $a_1,\ldots,a_n$, 即有 $|\{\boldsymbol{w}:f(\boldsymbol{w})_{ij}\not\equiv 0 \mod q\}|=q^{n-1}$ 和 $|\{\boldsymbol{w}:f(\boldsymbol{w})\equiv 0 \mod q\}|=q^{n-1}$. 故 $|\cup_{(i,j)\neq(k,1),1\leqslant k\leqslant n}\{\mathbf{w}:f(\boldsymbol{w})_{ij}\equiv 0 \mod q\}|\leqslant(n(n-1)+1)q^{n-1}$. 又因为 $\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n$ 线性无关, 则 $|\{\sum_{i=1}^n a_i\boldsymbol{v}_i,a_i\in\mathbb{F}_q\}|=q^n$. 当 q 充分大时, 有 $(n(n-1)+1)q^{n-1}<q^n$, 即 $\{\sum_{i=1}^n a_i\boldsymbol{v}_i,a_i\in\mathbb{F}_q\}-(\cup_{(i,j)\neq(k,1),1\leqslant k\leqslant n}A_{ij})\neq\emptyset$, 其中 $A_{ij}=\{\boldsymbol{w}:f(\boldsymbol{w})_{ij}\equiv 0 \mod q\}$. 从而证明常数 $a_1,\ldots,a_n$ 的存在性.

现在, 假设已找到向量 $\boldsymbol{v}'_1,\ldots,\boldsymbol{v}'_k\in\mathbb{F}_q^n$ 使得 $(\boldsymbol{v}'_1,\ldots,\boldsymbol{v}'_k,\ldots,\boldsymbol{v}_n)^{-1}$ 诱导一个线性 all-or-nothing 变换. 为完成证明, 只需找到一些常数 $a_1,\ldots,a_n$ 使得矩阵 $(\boldsymbol{v}'_1,\ldots,\boldsymbol{v}'_k,\sum_{i=1}^n a_i\boldsymbol{v}_i,\boldsymbol{v}_{k+2},\ldots,\boldsymbol{v}_n)^{-1}$ 诱导一个线性 all-or-nothing 变换. 从上面的证明可知, 这等价于寻找常数 $a_1,\ldots,a_n$ 使得 $\boldsymbol{w}=\sum_{i=1}^n a_i\boldsymbol{v}_i$ 满足 $|\{\sum_{i=1}^n a_i\boldsymbol{v}_i,a_i\in\mathbb{F}_q\}-(\cup_{(u,v)\neq(s,1),1\leqslant s\leqslant n}A_{uv})|-k>0$, $A_{uv}=\{\boldsymbol{w}:f(\boldsymbol{w})_{uv}\equiv 0 \mod q\}$. 这里对于所有 $1\leqslant i,j\leqslant n$ 有 $f(\boldsymbol{w})_{\iota\tau}:=\det(\boldsymbol{M}'_{\iota\tau})$, 且 $f(\boldsymbol{w}):=\det(\boldsymbol{v}'_1,\ldots,\boldsymbol{v}'_k,\sum_{i=1}^n a_i\boldsymbol{v}_i,\boldsymbol{v}_{k+2},\ldots,\boldsymbol{v}_n)$, $\boldsymbol{M}'_{\iota\tau}$ 表示删除矩阵 $(\boldsymbol{v}'_1,\ldots,\boldsymbol{v}'_k,\sum_{i=1}^n a_i\boldsymbol{v}_i,\boldsymbol{v}_{k+2},\ldots,\boldsymbol{v}_n)^{-1}$ 第 ι 行和第 τ 列所得的子矩阵. 通过类似证明可得结论.

引理 A2 若 $\phi(\boldsymbol{x})=\boldsymbol{M}_{n\times m}\boldsymbol{x}$ 为线性空间 $\mathbb{F}_q^m$ 到 $\mathbb{F}_q^n$ 的广义线性 all-or-nothing 变换, 则存在广义线性 all-or-nothing 变换 $\varphi(\boldsymbol{x})=\boldsymbol{M}'_{n\times m}\boldsymbol{x}$ 使得 $\boldsymbol{M}'_{n\times m}$ 和 $\boldsymbol{M}_{n\times m}$ 有 $i\,(1\leqslant i\leqslant m)$ 个不同列向量, 其中 q 充分大.

证明 通过递归来证明此引理. 记 $\boldsymbol{M}_{n\times m}:=(\boldsymbol{v}_1,\ldots,\boldsymbol{v}_m)$, 其列向量为 $\boldsymbol{v}_i\in\mathbb{F}_q^n$. 首先证明存在常数 $a_1,\ldots,a_n$ 使得 $(\sum_{i=1}^m a_i\boldsymbol{v}_i,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_m)$ 诱导线性空间 $\mathbb{F}_q^m$ 到 $\mathbb{F}_q^n$ 的广义线性 all-or-nothing 变换. 令 $\boldsymbol{v}'_1=\sum_{k=1}^m a_k\boldsymbol{v}_k$, 对每个 $i=1,\ldots,n$. 因为 $|\langle\boldsymbol{v}_{2i},\ldots,\boldsymbol{v}_{mi}\rangle=\mathrm{span}(\boldsymbol{v}_{2i},\ldots,\boldsymbol{v}_{mi})|=q^{m-1}$, 故 $|\cup_{i=1}^n\langle\boldsymbol{v}_{2i},\ldots,\boldsymbol{v}_{mi}\rangle|\leqslant nq^{m-1}$. 从而有

$$|\cup_{i=1}^n\langle\boldsymbol{v}_{2i},\ldots,\boldsymbol{v}_{mi}\rangle|\leqslant nq^{m-1}<q^m \tag{A1}$$

和 $|\{\boldsymbol{v}'_1,a_1,\ldots,a_m\in\mathbb{F}_q\}|=q^m$, 这里 $\boldsymbol{v}_{ji}$ 表示删除 $\boldsymbol{v}_j$ 的第 i 个分量所得的向量. 从定理 2 可知, 存在向量 $\boldsymbol{v}'_1$ 使得 $(\boldsymbol{v}'_1,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_m)$ 诱导一个广义线性 all-or-nothing 变换.

现在, 假设存在 $\boldsymbol{M}'_{n\times m}$ 使得 $\boldsymbol{M}'_{n\times m}$ 和 $\boldsymbol{M}_{n\times m}$ 有 $k-1$ 个不同的列向量. 以下只需要证明对于 k 结论成立. 事实上, 对充分大 q, 注意 $|\cup_{i=1}^n\langle\boldsymbol{v}'_{1i},\ldots,\boldsymbol{v}'_{k-1\,i},\boldsymbol{v}'_{ki},\ldots,\boldsymbol{v}_{mi}\rangle\cup\{\boldsymbol{v}_j,j=1,\ldots,k-1\}|\leqslant nq^{m-1}+k-1<q^m=|\{\boldsymbol{v}'_k,a_1,\ldots,a_m\in\mathbb{F}_q\}|$. 通过相似于上面的证明即可得结论.

引理 A3 若 $\phi(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}$ 为线性空间 $\mathbb{F}_q^n$ 到 $\mathbb{F}_q^m$ 的广义线性 all-or-nothing 变换, 那么 $\varphi(\boldsymbol{x})=\boldsymbol{A}'\boldsymbol{x}$ 为广义线性 all-or-nothing 变换的概率不小于 $(q+1-m(m+1))^c/q^c$, 其中 $c=C_n^m$, 矩阵 $\boldsymbol{A}'=(\sum_{i=1}^m a_i\boldsymbol{v}_i,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_k)$, $\boldsymbol{A}=(\boldsymbol{v}_1,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_m)$, a_i 随机选于 $\mathbb{F}_q$.

从引理 A1 和 A2 可以得此引理的证明.