云南大学学报（自然科学版），2006，28（3）：201～205　　CN 53－1045/N　ISSN 0258－7971
Journal of Yunnan University

密钥覆盖问题的 NP 完全性证明*

陆正福，洪孙焱
（云南大学 数学系，云南 昆明　650091）

摘要：给出了密钥覆盖问题的模型建立过程，并从顶点覆盖问题的判定形式出发，证明了密钥覆盖问题的判定形式是 NP 完全问题，为组通信安全的研究，尤其是多播安全的研究奠定了更为坚实的基础.

关键词：组密钥管理；组合优化；计算复杂性；顶点覆盖问题；密钥覆盖问题
中图分类号：TP 393　　**文献标识码**：A　　**文章编号**：0258－7971(2006)03－0201－05

组密钥管理是组通信安全中的核心问题，是保证组通信的保密性与真实性、可追踪性的基础[1～5]，可应用在 IP 网络的多播(包括网络层和应用层)、无线网络的自组网、大规模分布式计算系统中.组密钥管理包括组密钥的生成、分发、更新等环节，其关键是组密钥的更新，因为大规模动态组的密钥更新所引起的计算量和通信量决定了密钥服务系统性能优化程度和可扩展性，从而成为研究重点.针对多播组密钥管理，已有一批中外学者发表了研究结果，其中用户分组和密钥多级分层[1,2,6]是其中的 2 类最有代表性和影响力的方案.本文研究后者的组合算法问题.

密钥多级分层的数学本质是构造性的，它可以一般化地描述为密钥覆盖问题(KCP)，其可行方案的设计是一类组合设计问题，并伴随着代价最小化的目标，从而是一个组合优化问题.KCP 问题可以追溯到 C K Wong 等在文献[1,2]中的工作，该文指出，KCP 是一个 NP 困难问题，并指出集合覆盖问题 SCP 可以在多项式时间内归约为 KCP，但未给出证明.后来的有关文献，均以 KCP 是 NP 困难问题为研究前提，设计特殊模型和相应的协议，亦未见到有关 KCP 复杂性的证明.我们经过研究发现，将组密钥更新表达为组合优化意义上的 KCP 不是简单明了的，需加以适当的问题转化，并证明其计算复杂性.

一个组合优化问题的计算复杂性研究的通常途径是研究该组合优化问题所对应的判定问题.本文的研究工作就是按照这样的做法，从顶点覆盖问题 VCP 的判定形式(记为 VCP(D)[7])出发，证明了密钥覆盖问题 KCP 的判定形式(类似地记为 KCP(D))是 NP 完全的.

本文的贡献在于从理论上系统地研究了组密钥更新中的复杂性：首先，明确给出了组密钥更新到 KCP 的转化；其次，给出了关于 KCP 的判定问题的 NP 完全性的一个严格证明；此外，我们是从 VCP 出发来证明的，而不是文献[1,2]所提及的 SCP，这个证明途径表明，解 VCP 的近似算法可以略加演变用于 KCP 的研究，丰富了解决 KCP 的方法.

1　概念和术语的引入

关于计算复杂性理论的基本概念，可以参见文献[7～10].为了本文第 3 节证明的概念铺垫的需要，先给出一些必要的关于 NP 完全性的概念和术语.

1.1　NP 完全性的基本概念

定义 1　对任一判定问题 $\prod$，称 $\prod$ 属于 NP 类(记为 $\prod \in$ NP)，如果对它存在一个多项式时间算法 A(猜想检验算法)，其复杂性的多项式为 $p()$，使得：I 为 $\prod$ 的“是”实例，当且仅当存在一

* 收稿日期：2005－04－04
基金项目：国家自然科学基金资助项目(10561009)；云南省自然科学基金资助项目(2002F0012M)；云南大学理(工)科校级重点科研项目资助(2003Z010C).
作者简介：陆正福(1965－　)，男，安徽人，副教授，主要从事协议工程、信息安全和网络计算等方面的研究.

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

个猜想 $c(I)$,在 $p(|I|)$ 时间内对输入$(I, c(I))$得到答案"是".其中 $|I|$ 表示 I 的输入长度.

注解[10]:上述 NP 类的定义的关键在于"多项式时间可检验性",即对每个"是"实例 I,都存在一个 $c(I)$,用来证实 I 为一个"是"实例,而且检验 $c(I)$ 所需的时间不超过 $p(|I|)$.不涉及求 $c(I)$ 的问题.如何求 $c(I)$ 恰好是一些判定问题的原优化问题的困难之所在,因此从方法学的角度看,将组合优化问题转换为判定问题是必要的.

定义 2[1] 对任一判定问题 $\prod$,若 $\prod \in$ NP,且对所有别的问题 $\prod'$,均可多项式变换为 $\prod$(记为 $\prod' \propto \prod$),则称 $\prod$ 为 NP 完全的(NPC).

1971 年发表的著名的 Cook 定理建立了第 1 个 NPC 问题(可满足性问题),奠定了 NP 完全性的理论基础.有了第一个 NPC 问题后,若要证明一个判定问题属于 NPC,不需直接按照定义 2 去证明,只需证明:$\prod \in$ NP,且有某 NP 完全问题 $\prod' \propto \prod$.其中的关键是多项式变换.这些是 NPC 完全性理论中证明的关键.

文献[9]建立了如图 1 所示的基本 NPC 问题的结构图,其中的箭头表达了从一个问题到另一个问题的多项式变换关系,即从 CIRCUIT－SAT 出发,证明了 SAT,3－CNF－SAT,CLIQUE,VERTEX－COVER 等问题为 NPC 问题.

图 1 中的 VERTEX－COVER(顶点覆盖)是本文第 3 节证明的基础.

NP 完全性的研究是针对判定问题的,然而很多现实问题是以组合优化问题形式给出的,但给定一个界之后便可转化为判定问题.

1.2 安全多播组的概念 C K Wong 等在文献[1,2]中引入了密钥图的概念.在密钥图中,安全多播组可形式化定义为 1 个三元组 (U, K, R),其中 U 是有限非空成员集合,K 是有限非空密钥集合,R 为 U 和 K 之间的二元关系,$R \subset U \times K$,成员 $u(u \in U)$ 拥有密钥 $k(k \in K)$ 当且仅当$(u, k) \in R$.

在安全多播组中,密钥集 K 包括 3 类密钥:组密钥,用户专用密钥,辅助密钥.组密钥用 k_G 表示,是多播组所共享的密钥.用户专用密钥用 k_u 表示,k_u 是用户 u 专用的不为其他用户共享的密钥.辅助密钥集用 K_A 表示,K_A 是为方便密钥管理而引入的密钥集.安全多播组采用其组密钥进行加密通信.出于安全性的考虑,安全多播组需要完成组密钥管理方面的工作,其核心是组密钥和辅助密钥更新等.在更新过程中,需要用已有的未泄密的辅助密钥乃至专用密钥去加密新密钥(组密钥乃至辅助密钥),这种用于加密其它密钥的密钥称之为 KEK,密钥更新的关键就在于 KEK 的选择.

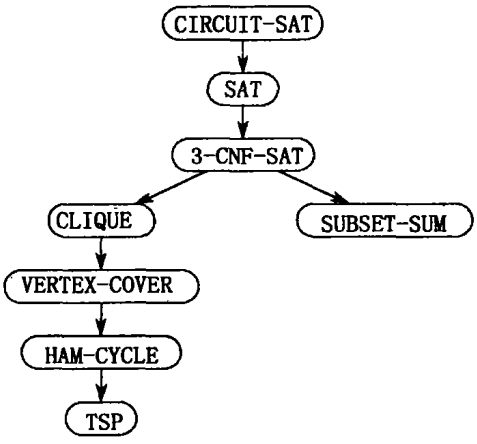

图 1 NPC 问题的结构

Fig.1 The structure of NPC

对于每个安全多播组(U, K, R),定义如下 2 个函数:keyset() 和 userset():

$$\forall u \in U, \text{keyset}(u) = \{k \mid (u, k) \in R\},$$
$$\forall S \subset U, \text{keyset}(S) = \bigcup_{u \in S} \text{keyset}(u),$$
$$\forall k \in K, \text{userset}(k) = \{u \mid (u, k) \in R\},$$
$$\forall M \subset K, \text{userset}(M) = \bigcup_{k \in M} \text{keyset}(k).$$

直观上,keyset() 表示成员或成员组所拥有的密钥集,userset() 表示拥有给出密钥或密钥组的多播成员集合.在安全多播组中一般有唯一的 1 个密钥 k_G 满足

$$\text{userset}(k_G) = U,$$

这实际上就是组密钥.

2 密钥覆盖问题的组合优化模型

为了第 3 节的证明,本节给出从组密钥更新转化为密钥覆盖问题 KCP 的形式化定义的模型建立过程.

为保证多播组的安全性,当某成员 u 主动离开多播组或者 u 被怀疑有泄密嫌疑而被逐出多播组时,成员 u 所拥有且被其他成员所共享的所有密钥都需要更新.假设 k 是这样的一个密钥,为了替换

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

密钥 k,群组管理员随机产生新的密钥 k_{new} 并将其发送给 userset(k) 中除了 u 外的每一个成员.为了安全地执行这一过程,群组管理员需要在 K 中确定一个密钥子集 K' 来加密 k_{new},这个密钥子集 K' 需满足 userset(K') = userset(k) \ {u}.为了使得密钥分配的工作量最小,群组管理员需要寻找 1 个尽可能小的 K'.这种密钥更新过程可以概括为:已知 1 个安全多播组(U, K, R) 和 U 的子集 S,在 K 中确定一个最小子集 K' 使得 userset(K') = S.

用户 u 离开,需要更新的密钥集记为 A_u = keyset(u) \ k_u, 令 U_u = userset(A_u), K_{all} = keyset(U_u),我们考虑由 K_{all} 节点构成的密钥图,若其中的连通分支只包含 U_u 成员的专用密钥,则用 U_u 的专用密钥作为KEK来加密新密钥,而在其他连通分支中能用成员专用密钥作为 KEK 的,也可以用辅助密钥(或组密钥) 替代之,而这样需要的 KEK 更少.因而,不考虑密钥集中的专用密钥并不影响问题的本质,设 K_{U_u} 为 U_u 成员的专用密钥集,令 K_u = K_{all} \ K_{U_u}.这样我们的目标便是要在 K_u 中寻找最小子集 K',用 K' 中的密钥去加密 k_{new} 等秘密消息,以达到安全更新的目的.

K' 是未泄密的,A_u 是泄密的,可以用 K' 中的密钥作为 KEK 去加密需要更新的 A_u(A_u 中包含了组密钥),由于 U_u = userset(A_u) 是已知的,而 K_u = K_{all} \ K_{U_u} 可计算得到,于是密钥更新的讨论可局限在新的忽略了专用密钥的安全多播组(U_u, K_u, R_u) 上讨论,其中,$R_u \subset U_u \times K_u$ 是由 u 离开所诱导出的关系.以上的简化处理和概念转化对第 3 节证明是必不可少的.

到此,我们便可以给出密钥覆盖的定义.

定义 3　密钥覆盖(KEY－COVER):在安全多播组(U_u, K_u, R_u) 中,若 $K' \subset K_u$,满足 userset(K') = U_u,则称 K' 是(U_u, K_u, R_u) 的一个密钥覆盖.其中,K' 中密钥的个数称之为密钥覆盖的大小.

定义 4　密钥覆盖问题(KCP):在给定的安全多播组中求最小的密钥覆盖.

KCP 陈述为判定问题,记为 KCP(D),即为确定给定多播组中是否存在 1 个大小不超过给定正整数 N 的密钥覆盖.可以形式化定义 KCP(D) 如下:

定义 5　KCP(D) = {〈(U_u, K_u, R_u), N〉:安全多播组(U_u, K_u, R_u) 有 1 个大小不超过 N 的密钥覆盖}.

3　KCP 计算复杂性证明

我们要证明 KCP(D) ∈ NPC,为此我们分 4 步完成[1]:① 证明 KCP(D) ∈ NP;② 选取一个已知的 NPC 问题:VCP(D);③ 构造 1 个从 VCP(D) 到 KCP(D) 的变换 f;④ 证明 f 为 1 个多项式变换.

首先我们完成证明步骤 ①.

命题 1　KCP(D) ∈ NP.

证明　我们可按照定义 1 及其注解来证明 KCP(D) 是属于 NP 类的.

对于判定问题 KCP(D),取 I 为其"是" 实例〈(U_u, K_u, R_u), N〉, c(I) 是有关的猜想:密钥子集 $K' \subset K_u$ 是大小不超过 N 的密钥覆盖,可以设计这样的猜想检验算法:逐一检查 R_u 中的每个元素,若某元素的第 2 分量属于 K',则选中其第 1 分量;若选中的所有第 1 分量的并集等于 K_u,则证实了猜想.这样的猜想检验算法具有线性复杂度.按照定义 1,有 KCP(D) ∈ NP.证毕.

接下来,完成步骤 ②.我们选取 1 个已知的 NPC 问题:顶点覆盖的判定形式 VCP(D).为此,先给出顶点覆盖的定义.

定义 6　顶点覆盖:给定无向图 G = (V, E),若存在 $V' \subset V$,使得 ∀(u, v) ∈ E,有 u ∈ V' 或 $v \in V'$,则称 V' 为 G 的 1 个顶点覆盖.其中 V' 中的顶点个数称为顶点覆盖的大小,如图 2,{z, w} 即为给出图的 1 个顶点覆盖,其大小为 2.

定义 7　顶点覆盖问题(VCP):给定无向图 G = (V, E),求 G 的最小顶点覆盖.

给定 1 个正整数 $N \leqslant |V|$,问 G 中是否存在 1 个大小不超过 N 的顶点覆盖?这便是 VCP 的判定形式,记为 VCP(D),其形式化描述如下:

定义 8　VCP(D) = {〈G, N〉:G 存在大小不超过 N 的密钥覆盖,其中 $N \leqslant |V|$}.

引理 1　VCP(D) ∈ NPC.

引理 1 的证明详见文献[7,9].

本文将从 VCP(D) 出发,证明密钥覆盖问题 KCP 的判定形式可多项式变换为顶点覆盖问题 VCP 的判定形式 KCP(D).

下面,我们完成步骤 ③④.

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

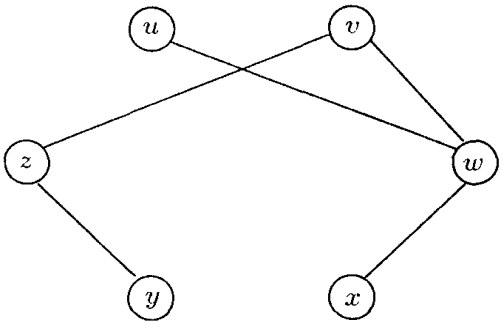

图 2 顶点覆盖

Fig. 2 The example of VCP

命题 2 $VCP(D) \propto KCP(D)$

证明 任取 VCP(D) 的 1 个实例:〈$G=(V,E)$, N〉. 定义 edgeset(v)($v \in V$) 为与顶点 v 关联的边的集合.

令 $U_u = E$, $K_u = V$, 且令 $R_u = \{(u,k) \mid u \in \text{edgeset}(v), u \in U_u, k \in U_u, v = k, v \in V\}$. 如此则构造了一个 KCP($D$) 的实例:〈($U_u$, K_u, R_u), N〉(其中 $v = k$ 表示 v 与 k 对应).

假设〈$G=(V,E)$, N〉有 1 个答案为是的顶点覆盖 V', 我们令 $K' = V'$, 则我们构造的实例〈(U_u, K_u, R_u), N〉也有 1 个答案为是的密钥覆盖 K'. 因为:$\forall u \in U_u$, 取 $e \in E$: e = u, 设(v_1, v_2) = e, 由假设知 v_1 和 v_2 中有 1 个属于 V', 不妨设 $v_1 \in V'$, 则 $e \in \text{edgeset}(v_1)$, 取 $k \in K_u$: $k = v_1$, 于是由 R_u 的构造方法知 $(u,k) \in R_u$, 即 $u \in \text{userset}(K')$, 由 u 是任取的知 K' 为(U_u, K_u, R_u) 的 1 个大小为 N 的密钥覆盖.

假设〈$G=(V,E)$, N〉的答案为否, 则我们构造的实例〈(U_u, K_u, R_u), N〉的答案也为否. 我们用反正法证明之:

假设〈(U_u, K_u, R_u), N〉有 1 个答案为是的密钥覆盖 K', 令 $V' = K'$, 则 $\forall e \in E$, 取 $u \in U_u$: $u = e$, 由假设知 $u \in \text{userset}(K')$, 不妨设 $u \in \text{userset}(k)$, 则 $(u,k) \in R$, 取 $v \in V'$: v = k, 从而 $e \in \text{edgeset}(v)$, 即对任意 $e \in E$, 我们已在 V' 中找到一点 v, 使得 v 为 e 的顶点, 从而〈$G=(V,E)$, N〉有 1 个答案为是的顶点覆盖 V', 矛盾.

综上, 任意 VCP 的实例都能与 1 个 KCP 的实例对应, 且能保持"是"与"否"答案不变.

上述构造和变换都能在多项式时间内完成, 其关键是与顶点关联的边的集合的构造.

从而 $VCP(D) \propto KCP(D)$. 证毕.

定理 1 $KCP(D) \in NPC$

证明 由命题 1、引理 1 及命题 2 得证.

至此, NPC 的结构图增加了 KEY—COVER (密钥覆盖)结点, 如图 3.

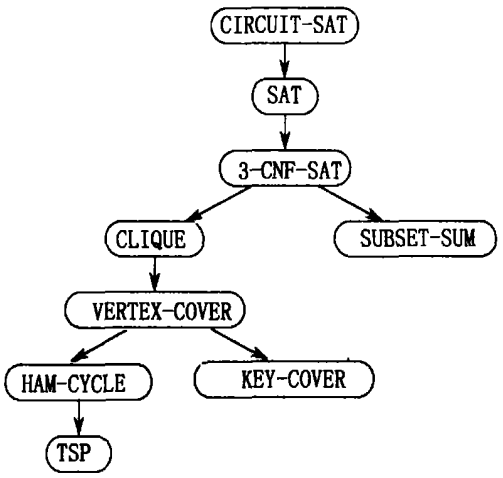

图 3 扩充的 NPC 结构

Fig. 3 Extended structure of NPC

4 结 论

有大量的研究工作(包括标准化工作)是围绕密钥多级分层展开的. 密钥多级分层类别的组密钥更新方案在支持多播的网络中更为受到重视[3].

从计算复杂性理论研究的角度看, 我们对密钥多级分层类别的组密钥更新所产生的密钥覆盖问题 KCP 进行了计算复杂性方面的研究, 从顶点覆盖出发, 证明了 KCP 的判定形式 KCP(D)属于 NPC 类. 这项研究工作在一定程度上是对密钥覆盖问题理论研究的完善, 也进一步丰富了 NPC 问题. 从组通信安全的角度看, 不论组通信基于何种实现方式:网络层多播、P2P 多播、单播、(无线)广播等, 只要涉及密钥的多级分层[3], 即引入组密钥和专用密钥以外的辅助密钥, 密钥的更新就会涉及密钥覆盖问题, 而通过上述的证明可知, 作为组合优化问题, KCP 不存在有效算法(否则 KCP(D)就存在有效算法, 与 $KCP(D) \in NPC$ 矛盾), KCP 要作为 1 个 NP 困难问题(NPH)来处理. 因此, 需要寻求近似的算法、特殊的模型等, 以期能够在多项式时间内给出满意的近似解.

总之, 本文的理论价值在于给出了 KCP 问题模型的准确定义、KCP 的复杂性的 1 个严格证明, 其实用意义在于证明过程揭示了 1 类通过 VCP 近

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

似算法设计 KCP 近似算法的设计思路.关于 VCP 近似算法的设计参见文献[11].

致谢:本文作者感谢多届"多播安全理论"、"计算机网络中的数学问题"等讨论班的老师和同学的讨论和建议.

参考文献:

[1] WONG C K, GOUDA M, LAM S. Secure group communications using key graphs[J]. Proceedings of ACM SIGCOMM '98, 1998, 28(4): 68-79.

[2] WONG C K, GOUDA M, LAM S. Secure group communications using key graphs[J]. IEEE/ACM Trans on Networking, 2000, 8(1): 16-30.

[3] 陆正福,李亚东,何英. IP 多播组密钥管理方案的分类体系研究[J]. 计算机工程与科学, 2004, 26(10): 23-26, 33.

[4] 陆正福,叶锐,王国栋. 基于移动代理的多播水印协议[J]. 云南大学学报:自然科学版, 2004, 26(4): 306-311.

[5] 陆正福,叶锐,王国栋. 多播水印协议 MAMWP 的 BAN 逻辑分析[J]. 云南大学学报:自然科学版, 2005, 27(1): 18-21.

[6] 陆正福,李亚东,于光德. 多播安全中批量密铜更新问题研究[J]. 云南大学学报:自然科学版, 2002, 24(15): 335-340.

[7] PAPADIMITRIOU C H. Computational Complexity [M]. Boston: Addison Wesley, 2004.

[8] GAREY M R, JOHNSON D S. Computers and intractability: a guide to the theory of NP-Completeness [M]. W H Freeman, 1979.

[9] CORMEN T H, LEISERSON C E, RIVEST R L. Introduction to algorithms [M]. Cambridge: MIT Press, 1989.

[10] 孙惠泉. 图论及其应用[M]. 北京:科学出版社, 2004.

[11] DORIT S Hochbaum. Approximation algorithms for NP — hard problems [M]. Boston: PWS Publishing Company, 1997.

On the proof of the NP-completeness of key covering problem in the group rekeying

LU Zheng-fu, HONG Sun-yan

(Department of Mathematics, Yunnan University, Kunming 650091, China)

Abstract: The process of modeling the key covering problem is preserted. And the NP-completeness of the decision version for the key covering problem is proved as well. Our proof is given based on the decision version of the vetex covering problem. Therefore, the further research on group security, especially for the multicast security, can have much solod foundation.

Key words: group key management; combinatorial optimization; computational complexity; vertex covering problem; key covering problem

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net