

基于独立集问题的零知识证明研究

王平水

(安徽财经大学 网络中心, 安徽 蚌埠 233041)

摘要: 零知识证明已经成为信息安全领域身份认证的关键技术之一。为了避免已知零知识证明系统的图同构问题, 提出了一种知识的计算零知识证明系统, 其安全性建立在 NPC 独立集问题上。该算法的构造基于离散对数问题的困难性, 从而保证了系统的合理性、完全性、计算零知识性。并从计算复杂度和通信复杂度两方面对系统及其算法参数的选取进行了分析。理论证明, 该系统是可行有效的。

关键词: 零知识证明; 独立集; 离散对数; 计算零知识性

中图分类号: TP18

文献标识码: A

文章编号: 1673-629X(2007)09-0055-03

Study on Zero-Knowledge Proof Based on Independent Set Problem

WANG Ping-shui

(Network Center of Anhui University of Finance & Economics, Bengbu 233041, China)

Abstract: Zero-knowledge proof has been one of the key technologies to be applied in identity authentication in the fields of information security. To avoid the use of the graph isomorphism problem in the known zero-knowledge proof systems, an efficient computational zero-knowledge proof of knowledge whose security relies on the NP-Completeness of the independent set problem is presented here. The proposed algorithm is constructed from a bit commitment scheme based on the hardness of the discrete logarithm problem, which guarantees the fulfillment of soundness, completeness and computational zero-knowledge properties. The system and its algorithm parameter choice were analyzed from two aspects of computational complexity and communication complexity. It was proved theoretically that the system is feasible and effective.

Key words: zero-knowledge proof; independent set problem; discrete logarithm; computational complexity

0 引言

零知识证明(ZKP)技术是由 Goldwasser 等人在 20 世纪 80 年代初提出的^[1], 已经成为现代密码学中研究的热点问题之一。自从该概念提出以来, 已有大量事实表明其在复杂性理论、信息加密和身份认证中是非常有用的。文中所讨论的计算零知识证明技术在单向函数存在的假设条件下, 可用于任一 NP 问题^[2]。

关于零知识证明的最重要的实验结果是: 完美的零知识的存在, 使得 NPC 问题存在多项式时间算法^[3]。由于图论作为 NP 问题的主要来源, 一些基于不同的图问题如同构、不同构、聚类、独立集等的计算零知识证明技术在国内文献中被纷纷提出。这些方法最主要的缺点之一是: 在一定程度上都与图同构这

一最基本的问题有关, 并且其计算复杂性尚未可知, 甚至该问题对于大多数随机图来讲是较为容易的^[4]。所谓图同构, 是指如果两张图除点的名字不同外其他都一样, 对于一个非常大的图, 找出两个图是否同构是很难的, 这是 NP 完全问题之一。

鉴于此, 文中提出了一种新的基于独立集问题(以下简称 ISP)的计算零知识证明系统, 其安全性建立在离散对数问题(以下简称 DLP)的难解性上^[5]。

1 概念和定义

零知识证明本质上是一种密码协议, 这种协议的一方称为证明者, 他试图使被称为验证者的另一方相信某个论断是正确的, 但却不向验证者提供任何有用的信息。Goldwasser 等人提出的零知识证明是交互式的, 也就是证明者和验证者之间必须进行交互, 才能实现零知识性。在交互式零知识证明的研究中, 目前人们最关心的基本模型有两种^[6]:

收稿日期: 2006-11-20

基金项目: 安徽省教育厅自然科学基金资助项目(2006KJ017C)

作者简介: 王平水(1972-), 男, 安徽蚌埠人, 副教授, 硕士, 主要研究领域为符号计算与网络信息安全。

一种是 GMR 模型,在这种模型中,证明者具有无限的计算能力,验证者具有多项式时间的计算能力,证明指的是语言成员问题,即输入 I 是否是语言 L 的一个成员。GMR 的零知识证明不是真正的零知识证明,因为在证明中,证明者向验证者揭露了知识的 1 比特,即 $I \in L$,除此之外,再没有任何其他附加的信息泄露给验证者,通常称这种交互式零知识证明为成员或定理的零知识证明。

另一种是 FFS 模型,在这种模型中,证明者和验证者均具有多项式时间的计算能力,证明者的目的不是向验证者证明 $I \in L$,而是证明他知道 I 关于 L 的状况。FFS 的零知识证明才是真正的零知识证明,因为在证明中,验证者没有得到任何信息,他连 $I \in L$ 还是 $I \notin L$ 都不知道,但他相信这个证明,通常称这种交互式零知识证明为知识或身份的零知识证明,文中所研究和讨论的就属于该类,即知识的零知识证明。

文中所提出的算法涉及到两个方面的基本问题:离散对数问题和独立集问题^[7]。

一方面,离散对数问题可描述为:设 p 为一素数, g 为乘法群 Z_p^* 的一个生成元, $x \in Z_p, y \in Z_p^*$, 定义离散对数 $y = \text{DLP}_{p,g}(x); g^x = x \pmod{p}$, 该问题属 NPI 类,没有多项式时间算法。

另一方面,独立集问题 ISP 属 NPC 问题,可定义为:给定一个无向图 $G = (V, E)$, 其中 $V = \{v_1, v_2, \dots, v_n\}$ 是图 G 的顶点集, $E = \{e_1, e_2, \dots, e_m\} \subseteq V \times V$ 是图 G 的边集,称 V 的一个子集 $I \subseteq V$ 为独立集,如果它的顶点两两互不相邻。

我们注意到,一个有用的方法隐含在图 G 的独立集中,即启发式算法^[8],该方法可用于文中所提出算法实例中。求解 ISP 有很多方法,如随机搜索算法(Random Search Algorithms)、随机贪婪算法(Random Greedy Algorithms)或随机阈值算法(Random Threshold Algorithms)等。由于最近在网络安全中的深入研究工作^[8]对网络通信协议的设计做出了重要贡献,即给出了 ISP 上有效的零知识证明的定义,作为文中所提出算法的基础 ISP 的选择看来就十分方便。

作为文中算法的基础,以下简单说明一下求解独立集问题 ISP 的三种常用方法^[9]。

(1) 随机搜索算法 RSA。

- ① 令 $V(G) = V; I = \emptyset$;
- ② 如果 $V(G) = \emptyset$, 则停止并输出 I ; 否则从 $V(G)$ 中任取一个顶点 v ;
- ③ 计算 $I = I \cup \{v\}; G = G - \{v\} \cup N(v)$, 其中 $N(v)$ 表示顶点 v 在 G 中的邻集; 转第 ② 步。

显然由这一算法得到的 I 是独立集, 这个算法不

能保证能得到一个满意的解。这是由于第 ② 步中对顶点 v 的任意选取造成的。如果对 v 的选取作一定限制, 就可能得到一个确定性的结果。一个自然的想法是选取度最小的顶点加入到当前的独立集, 这样就得到下面的以最小度作为贪婪指标的随机贪婪算法。

(2) 随机贪婪算法 RGA。

- ① 令 $V(G) = V; I = \emptyset$;
- ② 如果 $V(G) = \emptyset$, 则停止并输出 I ; 否则从图 G 中选取一个度最小的顶点 v ;
- ③ 计算 $I = I \cup \{v\}; G = G - \{v\} \cup N(v)$; 转第 ② 步。

这个算法中如果有若干个度最小的顶点, 则可从 G 中随机选取一个。

(3) 随机阈值算法 RTA。

顾名思义, 随机阈值算法就是采用了一个阈值函数来判断是否接受一个顶点加入当前的独立集。具体算法描述如下:

- ① 令 $V(G) = V; I = \emptyset$;
- ② 如果 $V(G) = \emptyset$, 则停止并输出 I ; 否则从 $V(G)$ 中任取一个顶点 v ;
- ③ 计算顶点 v 的阈值 $A(v)$, 如果 $A(v) \geq 0$, 则 $I = I \cup \{v\}; G = G - \{v\} \cup N(v)$;
- ④ 转第 ② 步。

2 算法描述

所提出的基于独立集问题 ISP 的知识的计算零知识证明系统使用了一个基于 DLP 的秘密承诺方案。算法设计中证明者 A 的输入为一个随机图 $G = (V, E)$ 和一个整数 k , 其目标是使 B 相信, 他知道图 G 的一个大小为 k 的独立集, 但 B 又无法获取除此之外的其他任何有用信息。

在预处理阶段, A 随机产生一个含有 n 个顶点的图 G 和一个嵌入的大小为 k 的秘密独立集 I , 并公布他的输入 (G, k) 。秘密的独立集 I 实际上可用作 A 的秘密身份, 因为隐藏该独立集 I 需多项式时间。在执行过程中, 每一次交互证明者 A 均随机产生一个 c 色图 G , 其独立集 I 的 k 个顶点同色, 且该颜色不同于图 G 中其它任何顶点。必须指出的是, 颜色数 c 值的大小不受任何其它值的限制, 因此, 颜色 c 的计算可在多项式时间内完成。

A 的秘密承诺由 c 个 n 维空间向量 $a_i = (a_i^j), a_i^j \in \{0, 1\}, i = 1, 2, \dots, c, j = 1, 2, \dots, n$ 构成: 每一标记颜色 i 且与顶点 j 相邻的位置记权值为 1, 其余记权值为 0。每一 c 色顶点集的阶可由向量 a_i 的平均权值 $W_H(a_i)$ (该值为非零值) 给出, 该值在本算法中起特殊作

用。初始化阶段, A 和 B 共同协商选定整数 m 和 c , 素数 $p_i (i=1, 2, \dots, c)$, $Z_{p_i}^*$ 的生成元 g_i , 随机整数 $r_i \in Z_{p_i}^*$ 。之后, 算法按如下四步交互执行 m 次:

1) 承诺: 证明者 A 产生向量 $a_i = (a_i^1, a_i^2, \dots, a_i^n)$, $i=1, 2, \dots, c$, 选取秘密随机整数 $y_j \in Z_{p_{j-1}}, j=1, 2, \dots, n$, 其中 $p = \min_{i=1, 2, \dots, c} \{p_i\}$, 并通过向验证者 B 传送一 n 维向量 $V_i = ((r_i^j \cdot g_j^y) \bmod p_i), (i=1, 2, \dots, c, j=1, 2, \dots, n)$ 来提交这些参数。

2) 挑战: B 随机选取一二进制位 b 发送给 A , 如果 $b=0$, 同时发送两个随机的相邻顶点 v 和 w 。

3) 响应: 如果 $b=0$, A 发送给 B 秘密整数 y_v 和 y_w ; 否则, 发送整数 $y = \sum_{j=1}^n y_j$ 和 $W_H(a_i) = \sum_{j=1}^n a_i^j, i=1, 2, \dots, c$ 。

4) 验证: B 检验 A 提供的数值是否正确:

(1) 当 $b=0$ 时, 由 V_i^v 和 $V_i^w (i=1, 2, \dots, c)$, B 检验: 仅存在两个不同向量, 其构成与顶点 v 和 w 有关, 且值为 1 (即 $\exists! h, l \in \{1, 2, \dots, c\} | h \neq l, a_h^v = a_l^w = 1$);

(2) 当 $b=1$ 时, B 检验:

$$\sum_{i=1}^c W_H(a_i) = n,$$

$$\exists i \in \{1, 2, \dots, c\} | W_H(a_i) = k,$$

$$\forall i \in \{1, 2, \dots, c\} | (\sum_{j=1}^n r_i^j \cdot g_j^y) = (r_i^{W_H(a_i)} \cdot g_i^y) \bmod p_i$$

3 复杂性分析

随机产生包含 n 个顶点的图 G 及其大小为 k 的独立集 I 时间复杂度为 $O((n-k)^2)$ 。通过著名的贪婪启发式算法完成颜色填充在最坏情况下时间复杂度为 $O(n^3)$ 。为了构建离散对数问题实例, 证明者 A 需要产生素数 c 并进行 $c \cdot n$ 次模幂运算时间复杂度为 $O(c \cdot n \cdot \log^2 l)$, 其中 $l = \max_{i=1, 2, \dots, c} \{p_i\}$ 。对 B 的响应, 当 $b=0$ 时, 需常量时间; 当 $b=1$ 时, 需线性时间。因此, 证明者 A 的计算复杂度可估计为 $O(n^3)$, 相应地, 验证者 B 进行指数运算的计算复杂度为 $O(c \cdot \log^2 l)$ 。至于通信复杂度, 在预处理阶段证明者 A 需公布随机图 $G = (V, E)$, 其大小为 $O(|E| \cdot \log(n))$, 此外, 提交的向量由 $n \cdot c$ 个整数组成, 对双方挑战的响应由两个整数组成, 因此相应算法的通信复杂度为 $O(m \cdot c \cdot \log(n))$ 。一个值得特别关注的问题是参数 n, c, p_i 等

的选取, 为确保方案的安全性, 图 G 的大小 n 和素数 p_i 应足够大, 然而, 为了降低通信复杂度, 颜色值 c 较小时是非常方便的。另外, 随机图 G 的产生和计算机表示也是非常重要的因素, 为确保 ISP 的困难性, 产生随机图 G 时, 建议 n 的值应大于 1000, 即 $n > 1000$ 。

4 结论

零知识证明技术已被广泛应用于复杂性理论、信息加密、身份认证等诸多领域。文中在研究已知的基于 ISP 的零知识证明的特点的基础上, 提出了一种新的基于 ISP 的知识的计算零知识证明系统, 该系统所采用的算法避免了已知零知识证明系统中的图同构问题, 其安全性建立在 NPC 独立集问题上, 从计算复杂度和通信复杂度两方面对系统进行了分析, 并从系统安全的角度对算法中参数的选取进行了总结。理论分析表明, 该系统是可行有效的, 其执行效率还有待实践中加以检验。

参考文献:

- [1] Goldwasser S, Micali S, Rackoff C. The Knowledge Complexity of Interactive Proof System[C]//In: Proc. 17th Annual ACM STOC 85. Providence, Rhode Island: [s. n.], 1985: 291-304.
- [2] Goldreich O, Micali S, Wigderson A. How to Prove All NP Statements in Zero-Knowledge, and a Methodology of Cryptographic Protocol Design [C]//In: Crypto'86. Berlin: Springer-Verlag, 1987: 171-185.
- [3] Fortnow L. The Complexity of Perfect Zero-Knowledge [C]//In: Proc. 19th Annual ACM STOC 87. New York: [s. n.], 1987: 204-209.
- [4] Fortin S. The Graph Isomorphism Problem[R]. In: Technical Report TR96-20. Canada: University of Alberta, 1996: 1-25.
- [5] 杨波. 现代密码学[M]. 北京: 清华大学出版社, 2003: 143-148.
- [6] 冯登国, 裴定一. 密码学引论[M]. 北京: 科学出版社, 1999: 36-55.
- [7] 卿斯汉. 安全协议[M]. 北京: 清华大学出版社, 2005: 212-220.
- [8] Brockington M, Culberson J. Camouflaging Independent Sets in Quasi-random Graphs[C]//In: Cliques, Coloring and Satisfiability. New York: AMS, 1994: 75-88.
- [9] 戎文晋. 最大独立集问题及其成长算法的研究[D]. 太原: 太原理工大学, 2004: 1-5.