一个自授权系统及问题的知识复杂性*

徐寿怀 张根度 朱 洪

(复旦大学计算机科学系 上海 200433)

E-mail: shxu@ms.fudan.edu.cn

摘要 基于图同构零知识证明的标识-鉴别-签名系统,提出了一个解决自授权问题的方法.与以前的方法相比,虽然两者都是基于对主秘密的逐步暴露来实现的,但前者是基于图同构置换来实现的,而后者是基于类似于秘密共享的思想来实现的.在研究给出的自授权系统的安全性时,定义了问题级的知识复杂性、实际知识复杂性和计算知识复杂性.应把它们作为协议知识复杂性的上界.

关键词 零知识证明,图同构,知识复杂性,自授权系统.

中图法分类号 TP14

在很多情况下,要把主密钥(或秘密)存放在安全的环境中,由它派生出二级密钥,它在指定的时间内起着主密钥的作用.如何限制合法的用户把这种二级密钥任意地送给别人使用呢?一个方法是,当用户进行一次自授权时,必须暴露有关主密钥的部分信息[1,2].

Goldreich 等人在文献[1]中提出了解决该问题要实现的两个目标:① 危害最小化,即任何一个二级密钥的失密对主密钥造成的危害要尽量小;② 可控制的授权,每次授权总是伴随着主密钥的部分信息的泄露.主密钥的泄露有突变(阈值模式)和渐变(每次泄露主密钥的若干有效位)两种方法,并提出了基于零知识证明的解,而知识的零知识证明[3]是基于离散对数求解的困难性的.

本文基于图同构零知识证明的标识-鉴别-签名系统,构造了一种新的自授权系统,其渐变解是自然的.在交互式协议中定量的知识复杂性[4,5]的启发下,我们提出了基于问题求解搜索空间的知识复杂性定义,并认为该复杂性界应是协议知识复杂性界的上界,可代替目前被承认的协议的知识复杂性的通信复杂性上界[5].

1 基于图同构零知识证明的标识-鉴别-签名系统

传统的标识-鉴别-签名系统都是基于计算数论中的难题(如求离散对数或因子分解)的.本文提出了一个基于一对公开的同构图的零知识证明的标识-鉴别-签名系统的自授权系统.

构造 1. 基于一对公开的同构图的标识-鉴别-签名模式由下述的标识生成、身份鉴别、数字签名和签名验证这4个(概率)多项式时间算法组成.

标识生成. 对输入的安全参数 1^n,输出一个四元组$(o,p,f,\{g_i\}_{i\in N})$,其中 o 是一对顶点数为 n 的同构图(G_0,G_1),p 是 G_0 到 G_1 的一个同构映射,$\{g_i\}_{i\in N}$是一个$\{0,1\}^*\to\{0,1\}^*$的单向置换簇,f 定义为对 G_1 施加一个同构映射 π,π 是用单向置换簇生成的$\{0,1,\ldots,n-1\}$上的置换 $permu(x)$,即 $f(\pi,(G_0,G_1))=\pi(G_1)$.假设存在一种安全的方法把$(o,p,f,\{g_i\}_{i\in N})$分配给用户 P,其中只有 P 才知道 p,其余的都是公开的.

身份鉴别. 当用户 P 要与用户 V 通信时,P 通过向 V 零知识地证明他知道(G_0,G_1)的同构 p.

数字签名. 对给定的报文 x,用户 P 首先用与"标识生成"中相同的方法生成 $\sigma=permu(x)$,再计算

---

* 本文研究得到国家自然科学基金和国家863高科技项目基金资助.作者徐寿怀,1970年生,博士生,主要研究领域为计算机网络安全,安全电子商务,电子货币.张根度,1937年生,教授,博士生导师,主要研究领域为计算机网络,信息工程和安全.朱洪,1939年生,教授,博士生导师,主要研究领域为算法设计和分析,计算复杂性,信息安全.

本文通讯联系人:徐寿怀,上海 200433,复旦大学计算机科学系

本文 1997-12-16 收到原稿,1998-03-03 收到修改稿

$\beta=\sigma(G_1)$,对报文 x,用户 P 的签名就是该 β,它被附加在 x 的后面(也可以不把该签名附加在报文中传送. 当 V 收到报文后,按同样的算法计算,得到一个新的 β',而 P 提供的零知识证明是关于"$G_0\cong\beta$"的,若该证明不能使 V 接受"$G_0\cong\beta'$",即说明或者报文在传输过程中被篡改而使得 $\beta\neq\beta'$,或者 P 在抵赖. 无论何种原因,该报文都被抛弃). 显然,P 知道 G_0 与 β 是同构的.

签名验证. 用户 V 验证该签名时,需要用户 P 零知识地证明该 β 与 G_0 同构. 由于 $\{g_i\}_{i\in N}$ 是公开的,V 在收到可能被篡改了的报文 x' 后,计算 $\sigma'=permu(x')$,然后计算 $\beta'=\sigma'(G_1)$. 若 $\beta'\neq\beta$,则抛弃该被篡改过的报文,否则,通过 P 零知识地证明 G_0 与 β 同构.

在构造 1 中的标识生成部分假设有一个可靠的第三方来完成标识生成和分发的工作. 实际上,也可以不依赖于可信的第三方的存在,即对一个给定的安全参数,每个用户生成自己的标识等信息,然后向某个机构(如公钥目录机构)登记即可. 关于这方面研究的更新的结果,将另文发表.

2　基于同构图标识的自授权系统模型

在基于同构图标识的零知识证明系统中,为了实现可控制扩散的需求,当合法用户每进行一次自授权时,就必须给出同构中的一个顶点对偶,形式见构造 3. 这样,经至多为顶点数次数的自授权后,该用户的秘密就全部泄露了.

构造 2. (基于一对公开图的图同构零知识证明系统的自授权系统模型)设合法用户拥有的公私钥对为(sk,pk)*.

授权生成. 用户生成一个二级钥对(sk_l,pk_l)**,然后生成一个可供验证者验证的带下标的标记 tag_l,l 表示本次授权的一个标号. tag_l 将使验证者相信它的确是由该合法用户生成的. 此时,在新得到的公私钥系统中不再有包括原来密钥的秘密信息.

授权验证. 当一个持有(sk_l,pk_l)的用户请求服务时,服务提供者将根据 tag_l 来验证其合法性. 当验证者确信该授权是合法的,则提供服务,称此三元组(sk_l,pk_l,tag_l)是合法的.

用户通过非法的手段得到三元组(sk_l,pk_l,tag_l)后,他至多能在该授权规定的范围(如该授权或三元组的有效期)内享受服务,但合法用户的主密钥却并未被暴露.

3　基于一对公开的同构图的自授权系统构造

3.1　基于一对公开的同构图的自授权系统构造

在本节给出的实例中,二级标识-鉴别-签名系统仍然是基于一对公开的同构图的.

构造 3. (基于一对公开图的图同构零知识证明系统的自授权系统)设合法用户已按构造 1 生成相应的系统,他拥有的公私钥对(sk,pk)同构造 2. (G_0,G_1)是其同构图对或标识,每个图的顶点标识为 0,1,2,...,$n-1$,n 为顶点数.

授权生成. 令 l 表示本次授权的下标,它表示这次授权必须暴露的在该秘密的同构置换中 G_0 的标号为 l 的点对应于 G_1 中的点的标号 l'. 形式地说,若 $G_1=\pi(G_0)$,则 $\pi(l)=l'$. 然后,生成本次授权的一个标记(二进串) tag_l,该标记是关于 NP 断言"存在 G_0 和 G_1 的同构置换 π,即 $G_1=\pi(G_0)$,且 $\pi(l)=l'$"的一个非交互式零知识证明. 最后,用户利用构造 2 生成一个二级钥对(sk_l,pk_l),其中 pk_l 是一对同构图,其顶点数是安全参数的一个函数,sk_l 是这一对图的同构置换. 这个二级钥对将在其有效期内起着与原来的主钥对相同的功能和作用.

授权验证. 当一个持有(sk_l,pk_l)的用户请求服务时,服务提供者将根据 tag_l 表示的非交互式零知识证明来验证三元组(sk_l,pk_l,tag_l)是否合法.

---

* 此时,公钥就是一对同构图,私钥就是两图的同构.

** 此二级密码应用的模式可以独立于原来的应用模式. 如,若仍然采用原来的基于图同构的零知识证明模式时,则公钥为一对图,私钥是图的同构;若采用传统的公钥模式如 RSA 时,则公私钥的概念就是传统意义上的定义.

3.2 基于一对公开的同构图的自授权系统构造的正确性

构造3的正确性由下述定理保证.

定理1. (1) 任何NP断言都存在零知识交互式证明系统[6];(2) 任何零知识交互式证明系统都可变换成非交互式零知识证明系统[7].

3.3 基于一对公开的同构图的自授权系统构造的实际安全性

当给定两个图时,要判断它们是否同构,搜索空间为$n!$.根据Stirling公式易知,当$n=128$时,穷尽搜索是不可行的.

显然,验证了足够多的二级钥的验证者能容易地计算出合法用户的主密钥.但当n足够大(如$n=128$)时,暴露一个构造3中的点对不会泄露整个同构置换.当我们从某个Oracle处得知的置换中某个对应顶点的度数为d时,问题求解的搜索空间从$n!$降为$d!\cdot(n-d-1)!$,因此,在选择要暴露的同构置换中的点对时,要满足危害最小化,所选中的点的顺序应以度数的增序进行.

对给定规模的图,安全自授权的次数取决于当时实际的计算能力和图的特征.例如,当规模为30的图同构的搜索是可接受的时候,对一个规模为n的图而言,进行自授权的次数的上界为$(n-30)$,实用建议的次数为$(n-60)$.

4 定性的和定量的知识复杂性

4.1 协议的知识复杂性

Goldwasser[8]等人在1985年首次提出了交互式证明系统的知识复杂性概念.知识复杂性是关于验证方通过交互时获得计算意义上的好处的一个测度,即在交互后可能得到的东西.知识复杂性*、信息熵和通信复杂性是不同的测度.通信复杂性是指双方的通信量的量度[5].关于定量的知识复杂性,Goldreich等人[5]认为:可以用协议的通信复杂性作为协议的知识复杂性的上界.在基于通信复杂性界是可计算的假设下得到知识复杂性应当位于区间$[0,poly(\cdot)]$中.

目前,关于协议的知识复杂性的形式有3种不同的定义.称证明者P泄露了至多$k(|x|)$比特的知识,如果在交互后验证者V能计算出来的任何东西,他都能通过查询Oracle至多$k(|x|)$比特后计算出来.基于空间测度的复杂性是指,一个图灵机成功地模拟一个真实的交互的良好子空间的一个量度.基于暗示的复杂性是指,一个图灵机能够有效地模拟一个真正的交互时需要从其他地方获得的最小暗示的长度.有关以往的定量知识复杂性研究的部分综述可详见文献[5].

4.2 问题的知识复杂性

本文给出的应用系统涉及的是问题级的知识复杂性而不是协议级的知识复杂性,用问题的知识复杂性作为协议的知识复杂性上界是更为合理的.

一般地,对两个顶点数为n的图,与知识复杂性有关的问题,我们至少关心:(1) 问题本身的知识复杂性是多少?(2) 当一个Oracle告诉我们关于此两图的同构时,我们获得的知识有多少?(3) 当我们像在构造3中那样获得置换中的一个点对时,获得了多少知识?

给定图的顶点编号,如$0,1,2,\ldots,n-1$,1个置换只需$n\cdot\log(n)$位就能完全确定.当$n=128$时,有$n\cdot\log(n)=896$比特的知识.我们给出:

定义1. 问题的知识复杂性就是精确表示该问题的解所必需的最短二进制串的长度.

对因子分解而言,设$n=p_1^{e_1}\ldots p_j^{e_j}$,其中$p_i$是不同的素数,$e_i>0,i=1,2,\ldots,j$,则该问题的知识复杂性为$\sum_{i=1}^{j}\log(p_i)$.上例中精确地表示了一个置换需$n\cdot\log(n)$比特,当得到该896个比特的知识时,问题的解就唯一地确定了.但在实际问题中,并不需要知道全部的$n\cdot\log(n)$比特的知识时,可能就足以计算出图的同构.因为当搜索空间足够小时,可以直接得到问题的解.因此,需要定义问题的实际知识复杂性,其上界是问题的知识复杂

* 知识复杂性总是基于计算复杂性来定义的,即知识复杂性与计算能力有关.

性.多大的搜索空间才算是有计算难度的?这不仅与现实机器的计算能力有关,还与所基于的问题中涉及的对象(如图)的特点有关.由于我们讨论的是最坏的性状复杂性,在上面的图同构中,如果定义 $3*10^{32}$(相当于搜索 30 个顶点的图的同构)是当前能力下的可计算的搜索空间,则问题求解时,若搜索空间不超过该空间的大小,则该问题在当前计算能力下可以解决,从而此时再查询 Oracle 时获得的知识复杂性为 0.这样,当从 Oracle 处获得知识,使搜索空间逐步减小到该空间界时,就获得了问题的全部知识.

定义 2. 设初始的问题求解搜索空间为 s_0,考虑该问题时实际计算能力所处理的空间为 s',当从一个 Oracle 处获得某种知识后,问题求解的搜索空间降为 $s_1 \geqslant s'$,则称该问题的实际知识复杂性为 $\log(s_0)$ 比特,称从 Oracle 处获得到的知识复杂性即计算知识复杂性,为 $-\log(\frac{s_1}{s_0})$ 比特.

在图同构例中,问题的实际知识复杂性的上界为问题的知识复杂性,即对足够大的 n,$\frac{(n-1)(n-2)}{2} > n\log(n) > \log(n!) \approx 716$.当我们从某个 Oracle 处得知的置换中某个对应顶点的度数为 d 时,则获得的知识复杂性的量度为 $-\log(\frac{k! \cdot (n-k-1)!}{n!}) \geqslant -\log(\frac{(n-1)!}{n!}) = \log n$.这与直觉是相符合的,因为我们不仅得到了该点对本身的对应,还得到了其相邻点的某种对应关系.当我们从某个 Oracle 处获得的知识使问题的搜索空间降为可计算时,我们从该 Oracle 处获得的知识至少为 $-\log(\frac{30!}{128!}) \approx 716-108=606$.

例:设 1 个 512 比特的 Blum 数 $n=pq$,则相应的因子分解问题的知识复杂性为 $\log p+\log q=512$,而通信复杂性 $\geqslant \log p+\log q=512$.该问题的实际知识复杂性的上界为 $\log(\sqrt{n} \cdot \log \sqrt{n})=264$ 比特.

5 结论和讨论

本文基于图同构零知识证明的标识-鉴别-签名系统,提出了一个解决自授权问题的方法.与文献[5]中提出的方法相比,前者是基于图同构置换来实现的,而后者是基于类似于秘密共享的思想来实现的.

在研究自授权系统的安全性时,我们得到了一个意外的结果,即问题的知识复杂性定义.我们定义了问题级的知识复杂性、实际知识复杂性和计算知识复杂性.我们认为,把它们作为协议知识复杂性的上界是合理的.

参考文献

1 Goldreich O, Pfitmann B, Rivest R L. Self-delegation with Controlled Propagation-or-What if You Lose Your Laptop. http://www.mit.edu, 1997

2 Dwork C, Lotspiech J, Naor M. Digital signets: self-enforcing protection of digital information(preliminary version). In: Leighton F T ed. Proceedings of the 28th ACM Symposium on Theory of Computing. New York: ACM Press, 1996. 489～498

3 Bellare M, Goldreich O. On defining proofs of knowledge. In: Brickell E F ed. Proceedings of the CRYPTO, Lecture Notes in Computer Science 740. Berlin: Springer-Verlag, 1992. 390～420

4 Goldreich O, Petrank E. Quantifying knowledge complexity. In: Sipser M ed. Proceedings of IEEE Symposium on Foundations of Computer Science. Los Alamitors, California: IEEE Computer Society Press, 1991. 59～68

5 Goldreich O, Petrank E. Quantifying Knowledge Complexity. http://www.mit.edu, 1997

6 Ben-Or M, Goldreich O, Goldwasser S *et al*. Everything provable is provable in zero-knowledge. In: Goldwasser S ed. Proceedings of CRYPTO, Lecture Notes in Computer Science 403. Berlin: Springer-Verlag, 1988. 37～46

7 Blum M, Feldman P, Micali S. Non-interactive zero-knowledge and its applications(extended abstract). In: Ullman J D ed. Proceedings of the 20th ACM Symposium on Theory of Computing. New York: ACM Press, 1988. 103～112

8 Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proofs. In: Pipenger N ed. Proceedings of the 17th ACM Symposium on Theory of Computing. New York: ACM Press, 1985. 291～304

One Self-delegation Scheme and the Knowledge Complexity of Problems

XU Shou huai ZHANG Gen-du ZHU Hong

(*Department of Computer Science Fudan University Shanghai* 200433)

Abstract A solution to the problem of self-delegation using the identification-authentication-signature scheme based on the graph isomorphism problem is proposed in this paper. The major difference from the traditional solutions is that it is based on the graph isomorphism rather than computing numeric theory problem, though they all leak out secret information little by little. The knowledge complexity of problems, the including knowledge complexity, the practical knowledge complexity, and the computing knowledge complexity are also defined. In the authors' opinion, these definitions should be used as the upper bound of knowledge complexity of protocols.

Key words Zero-knowledge proof, graph isomorphism, knowledge complexity, self-delegation system.