随机归约的五步完美零知识证明系统*

臧斌宇[1] 周玉林[2] 熊鹏荣[2] 朱 洪[3]

[1](复旦大学并行处理中心 上海 200433)

[2](江西上饶师范专科学校数学系 上饶 334001)

[3](复旦大学计算机科学系 上海 200433)

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

摘要 构造了一个完美零知识的五步交互证明系统,该系统不依赖于任何(复杂性和计算能力)假设,在该系统中,证明者可具有有限或无限的计算能力.

关键词 完备性,可靠性,零知识,完美零知识证明系统,随机归约.

中图法分类号 TP301

目前,没有任何假设的零知识证明系统是极少的.文献[1]给出了一个没有任何假设的完美零知识五步交互证明系统,该系统是建立在图同构问题上的证明系统,这是目前所见的没有任何假设的交互次数最少的完美零知识证明系统.但该系统要求证明者的计算能力无限.对证明系统没有附加假设这类问题,Tompa和Woll[2]曾给出平均归约的概念使其一般化.目前已有几个四步完美零知识证明系统,但都附加了假设,且缺乏一般性.Sakurai[3]曾给出二次剩余上的零知识四步证明系统,该系统虽然没有任何假设,但它不是语言的证明系统(在$x\notin R_N$时,证明者也能说服验证者接受该语言,即该协议只有在正确的输入下才是完美零知识证明系统).

平方剩余是否存在没有附加假设条件的四步完美零知识证明系统这个问题,至今还没有解决,也没有找到其他没有附加条件和假设的四步完美零知识证明系统.

本文给出的完美零知识五步证明系统,不需有任何复杂性假设和对证明者附加任何计算能力假设.我们的证明系统中的证明者可具有有限的计算能力,比文献[1]的条件弱(文献[1]中证明者由于计算能力无限,故可据此获得说服验证者的知识就多),比文献[1]适应面广(因为随机归约问题是平方剩余问题、离散对数问题、图同构问题等的一般化).我们的结论适合任何零知识证明机构.

1 协议的描述

本文用到的概念有:交互证明系统、完备性、可靠性和完美零知识性,可参阅文献[2,4],随机归约性概念出自文献[2].

设R满足下述条件:

(1) R是随机自归约的;

(2) 存在一概率多项式时间$|N^{O(1)}$算法,对给定的N,x,y决定(x,y)是否属于R_N;

(3) 存在一概率多项式时间$|N^{O(1)}$算法,对输入N,输出随机对$(x,y)\in R_N$,这里,x在R_N上为均匀分布,y在$R_N(x)$上为随机的均匀分布,这些条件与文献[2]中相同.

在条件(1)~(3)满足的假设下,我们来构造一个五步协议.

---

* 本文研究得到国家自然科学基金资助.作者**臧斌宇**,1963年生,在职博士生,副教授,主要研究领域为并行处理.**周玉林**,1962年生,讲师,主要研究领域为算法理论.**熊鹏荣**,1961年生,讲师,主要研究领域为算法分析与设计.**朱洪**,1939年生,教授,博士生导师,主要研究领域为算法分析与设计.

本文通讯联系人:朱洪,上海 200433,上海复旦大学计算机科学系理论组

本文1997-05-19收到原稿,1998-01-23收到修改稿

五步证明协议:该协议的公共输入是(N,x),证明者的辅助输入是y,$(x,y)\in R_N$,k为安全系数,

(1) P:随机地均匀地选择$(\bar{x}_i,\bar{y}_i)\in R_N$,$i=1,\ldots,k$,送$\alpha_1=(\bar{x}_1,\ldots,\bar{x}_k)$给$V$;

(2) V:随机地均匀地选择$b_i\in\{0,1\}$,$i=1,\ldots,k$,

如果$b_i=0$,则计算$u_i=A(N,\bar{x}_i,g)$,让$w_i=\bar{g}_i$

(这里,g是V的随机源,$\bar{g}_i$是V在计算u_i时消耗掉的g的有限前缀);

如果$b_i=1$,则随机地、均匀地选择$(u_i,v_i)\in R_N$,让$w_i=v_i$.

送$\beta_1=(u_1,\ldots,u_k)$给P;{V将位元b_i掩盖在u_i中,用u_i提交位b_i};

(3) P:计算$x_i=A(N,x,r)$,设$\bar{r}_i$是P在计算x_i中消耗掉的P的随机源的有限前缀,

P根据$(N,x,y,\bar{r}_i)$计算x_i的某个证据y_i,$i=1,\ldots,k$,送$\alpha_2=(x_1,\ldots,x_k)$给$V$;

(4) V:送$\beta_2=(w_1,\ldots,w_k)$给P;{V揭掩盖};

(5) P:根据计算揭掩盖并应答:

如果$u_i=A(N,\bar{x}_i,w_i)$,则得$b_i=0$;如果$(u_i,w_i)\in R_N$,则得$b_i=1$.

若$b_i=0$,则令$z_i=\bar{r}_i$;若$b_i=1$,则令$z_i=y_i$,$i=1,\ldots,k$.

送$\alpha_3=(\bar{y}_1,\ldots,\bar{y}_k)(z_1,\ldots,z_k)$给$V$;

(6) V:检验P的报文α_3的正确性,即:

检验关系$(x_i,y_i)\in R_N$,

如果$b_i=0$,则检验等式$x_i=A(N,x,z_i)$;

如果$b_i=1$,则检验关系$(x_i,z_i)\in R_N$,$i=1,\ldots,k$.

如果这些条件都满足,则V接受且停机;否则,V拒绝,输出"P欺骗"且停机.

2　协议的证明

定理 1. 上述协议满足协议的完备性.

证明:当$x\in L_R$时,显然,当P以$y\in R_N(x)$为辅助输入,只要P,V按协议执行,则V必接受. □

定理 2. 上述协议满足协议的可靠性.

证明:我们描述一个多项式时间的知识提取器M,该知识提取器在平均时间$|N|^{O(1)}$内停机,且其输出y满足$(x,y)\in R_N$的概率与P'通过交互说服V使V接受的概率最多相差$|x|^{-\omega(1)}$.

我们先分析一下,M怎样才能获得x的一个证据,一个可行的方法是让M获得两轮不同的V能接受的报文,$\alpha_1-\beta_1-\alpha_2-\beta_2-\alpha_3$与$\alpha_1-\beta_1-\alpha_2-\beta'_2-\alpha'_3$,其中$\alpha_1=(x_1,\ldots,x_k)$,$\beta_1=(u_1,\ldots,u_k)$,$\alpha_2=(x_1,\ldots,x_k)$,$\beta_2=(w_1,\ldots,w_k)$,$\alpha_3=(\bar{y}_1,\ldots,\bar{y}_k)(z_1,\ldots,z_k)$,$\beta'_2=(w'_1,\ldots,w'_k)$,$\alpha'_3=(\bar{y}'_1,\ldots,\bar{y}'_k)(z'_1,\ldots,z'_k)$,设$M$通过$\beta_2$,$\beta'_2$揭开的掩盖位分别是$(b_1,\ldots,b_k)$,$(b'_1,\ldots,b'_k)$,且有某个$j$,使得$b_j\neq b'_j$,由对称性,不妨设$b_j=0$,$b'_j=1$,则有$x_i=A(N,x,z_i)$与$(x_i,z'_i)\in R_N$同时成立,这样,$x$的某个证据即可通过$(N,x,z_i,z'_i)$算出(随机归约定义中的$R_2$,见文献[2]).

为了让M获得两次不同的报文,M必须先得到一"变色龙"$\beta_1=(u_1,\ldots,u_k)$,* 然后才能随心所欲地揭开掩盖,以期获得两轮不同的报文.

由以上分析,M执行过程可分为3部分:

第1部分:模拟.该部分的目的,是获得$(\bar{x}_1,\ldots,\bar{x}_k)$,$(\bar{y}_1,\ldots,\bar{y}_k)$,其中$(\bar{x}_i,\bar{y}_i)\in R_N$,该部分实际上是使下面的两部分的$(u_1,\ldots,u_k)$成为"变色龙",在该部分中,$M$模拟诚实的$V$忠实地执行整个协议,与$P'$交互(即调用$P'$作为子程序),若$V$拒绝则$M$拒绝,输出$P'$欺骗,否则$M$执行第2部分.设$M$在协议的第(1)句获得

---

* 这里仅作简单的解释.所谓的"变色龙"是一位掩盖集,该位掩盖集可由掩盖者随心所欲地揭开.也即,掩盖者想让某位揭开后呈"0",他就可以按某种方式揭开使其呈"0",想让该位揭开后呈"1",他就可以按另一种方式揭开使其呈"1";而对非掩盖者,只有当其已经知道$\bar{x}_1,\ldots,\bar{x}_k$对应的证据$\bar{y}_1,\ldots,y_k$时,$\beta_1=(u_1,\ldots,u_k)$才是它手下的"变色龙".

$(\bar{x}_1,\ldots,\bar{x}_k)$,在协议的第(5)句获得$(\bar{y}_1,\ldots,\bar{y}_k)$.

第2部分:获得一组报文$\alpha_1-\beta_1-\alpha_2-\beta_2-\alpha_3$(其中$\alpha_1$在第1部分已得到).该部分组成如下:

REPEAT

将P'的工作带、通讯带设置成第1部分模拟时执行完协议的(1)后的状态,即从协议的(2)开始执行,此时,M已有$(\bar{x}_1,\ldots,\bar{x}_k)$,$(\bar{y}_1,\ldots,\bar{y}_k)$,其中$(\bar{x}_i,\bar{y}_i)\in R_N$.

(2′) M计算$u_i=A(N,\bar{x}_i,g)$.这里,g是M的随机源,$\bar{g}_i$是M在计算u_i时消耗掉的g的有限前缀.

根据$(N,\bar{x}_i,\bar{y}_i,\bar{g}_i)$计算$v_i$,使得$(u_i,v_i)\in R_N$,

送$\beta_1=(u_1,\ldots,u_k)$给P'{注意,此时$(u_1,\ldots,u_k)$已是M掌握的"变色龙"};

(3′) 让P'送$\alpha_2=(x_1,\ldots,x_k)$;

(4′) M随机地、均匀地选择$b_i\in\{0,1\}$,$i=1,\ldots,k$,

如果$b_i=0$,则让$w_i=\bar{g}_i$,

如果$b_i=1$,则让$w_i=v_i$,送$\beta_2=(w_1,\ldots,w_k)$给P';{M随心所欲地揭掩盖};

(5′) 让P'送$\alpha_3=(\bar{y}_1,\ldots,\bar{y}_k)(z_1,\ldots,z_k)$;

(6′) M对P'的报文α_3进行检验,即:

检验关系$(\bar{x}_i,\bar{y}_i)\in R_N$,

如果$b_i=0$,则检验$x_i=A(N,x,z_i)$,

如果$b_i=1$,则检验关系$(x_i,z_i)\in R_N$,$i=1,\ldots,k$;

UNTIL α_3通过M的检验.

这一部分执行完后,M得到报文$\alpha_1-\beta_1-\alpha_2-\beta_2-\alpha_3$,且其中的$\beta_1=(u_1,\ldots,u_k)$是"变色龙".现让$M$进入第3部分.

第3部分:在上述"变色龙"$\beta_1=(u_1,\ldots,u_k)$及问题集$\alpha_2=(x_1,\ldots,x_3)$下找另一组报文$\alpha_1-\beta_1-\alpha_2-\beta'_2-\alpha'_3$,其中$\alpha_1-\beta_1-\alpha_2$是前面已经得到的.该部分内容如下:

将P'的工作带、通讯带设置成第2部分执行完(3′)后的状态,即M从协议的(4)开始执行,

REPEAT

(4″) M随机地选择$b'_i\in\{0,1\}$,$i=1,\ldots,k$,

如果$b'_i=0$,则让$w'_i=\bar{g}_i$,如果$b'_i=1$,则让$w'_i=v_i$,送$\beta'_2=(w'_1,\ldots,w'_k)$给$P'$;

(5″) 让P'送$\alpha'_3=(\bar{y}'_1,\ldots,\bar{y}'_k)(z'_1,\ldots,z'_k)$给$M$;

(6″) M检验P'的报文α_3,即:

检验关系$(\bar{x}_i,\bar{y}'_i)\in R_N$,

如果$b_i=0$,则检验等式$x_i=A(N,x,z'_i)$,

如果$b_i=1$,则检验关系$(x_i,z'_i)\in R_N$,$i=1,\ldots,k$,

UNTIL (6)中的α_3通过检验或循环将所有的$(b_1,\ldots,b_k)$遍历完毕.

(7″) 如果所有的$(b_1,\ldots,b_k)$被遍历完毕,则M停机,不输出任何东西.

否则,M从成功获得的两组不同的报文中计算x的证据y,M输出x的证据y且停机.

当M执行完第3部分后,M要么输出$y\in R_N(x)$后停机,要么停机不输出.下面,我们证明M平均执行的时间是多项式的,然后证明M计算出$y\in R_N(x)$的概率不小于$p-2^{-k}$.这里,p是M通过第1部分的概率,即设

$$\text{Prob}\ (V_P(N,x,s)(N,x)\ \text{接受})=p.$$

首先,M在第1部分模拟(P',V)的时间是多项式的,M模拟之后立即停机的概率为$(1-p)$,因此,M执行后两个部分的概率为p.当M进入第2部分,M反复执行直到M模拟的V再次接受(N,x)为止,因此,M执行第2部分循环的平均次数为$1/p$.当M进入第3部分时,$(\bar{x}_1,\ldots,\bar{x}_k)(u_1,\ldots,u_k)(x_1,\ldots,x_k)$已固定,假设$(P',V)$在这些已固定量下接受$(N,x)$的概率为$q$,那么$M$退出第2部分以后,选择这些固定量的概率不超过$D^{-1}q\sum_{j=0}^{\infty}(1-p)^j=\frac{q}{Dp}$,这里$D$是所有的$(u_1,\ldots,u_k)$的个数.设$q=i_1/2^k$(对$q$解释,$2^k$为所有可能的$(b_1,\ldots,b_k)$

的数目,i_1 为 2^k 个$(b_1,\ldots,b_k)$中 P'能给予正确应答的数目),那么固定这些量之后,M 在第 3 部分的平均执行次数为$(2^k-1)/(i_1-1)$(假设此时 $i_1>1$,M 在第 2 部分成功之后,在第 3 部分重新获得一组 P'能正确应答的$(b'_1,\ldots,b'_k)$的概率为$(i_1-1)/(2^k-1)$),所以 M 执行第 3 部分的平均次数不超过 $\sum_{a_1,\ldots,a_k}\frac{i_1}{2^kDp}\cdot\frac{2^k-1}{i_1-1}\leqslant 2/p$. 所以,$M$ 执行第 2 部分和第 3 部分的总的平均次数为 $p(1/p+2/p)=3$,因此,M 是平均多项式时间的.

如果 M 模拟成功(其概率为 p),那么只有当 $i_1=1$,即 $q=2^{-k}$时 M 才求不出 $y\in R_N(x)$,而 M 在退出第 1 部分时,选择这些固定量的概率不超过 $\sum_{a_1,\ldots,a_k}D^{-1}q/p=2^{-k}/p$,因此,$M$ 成功地求出 $y\in R_N(x)$的概率不小于 $p(1-2^{-k}/p)=p-2^{-k}$. 由于 $k=\omega(\log|x|)$,因此 M 满足条件. □

至于协议是完美零知识的,其证明几乎与文献[1]相同,在此从略.

由上述分析,我们已得:

定理 3. 上述协议是完美零知识的五步知识证明系统. □

参考文献

1 Bellare M, Micali S, Ostrovsky R. Perfect zero knowledge in constant rounds. In: Gabow H N ed. Proceeding of the 22nd Annua. ACM Symposium on the Theory of Computing. New York, NY: ACM Press, 1990. 482～493

2 Tompa M, Woll H. Random self-reducibility and zero knowledge interactive proofs of possession of information. In: Leighton F T ed. Proceeding of the 28th Symposium on Foundation of Computer Science. Los Alamitos, CA: IEEE Computer Society, 1987. 427～482

3 Sakurai K. On separating proofs of knowledge from proofs of membership of languages and its application to secure identification schemes. Lecture Notes in Computer Science, 1995,(959):496～509

4 Feige U, Fiat A, Shamir A. Zero knowledge proofs of identity. In: Aho A V ed. Proceedings of the 19th Annual ACM Symposium on the Theory of Computing. New York, NY: ACM Press, 1987. 210～217

Perfect Zero Knowledge Proof System with Five Moves for Random Reducibility

ZANG Bin-yu[1]　ZHOU Yu-lin[2]　XIONG Peng-rong[2]　ZHU Hong[3]

[1](*Parallel Processing Institute　Fudan University　Shanghai*　200433)

[2](*Department of Mathematics　Shangrao Teachers' College　Shangrao*　334001)

[3](*Department of Computer Science　Fudan University　Shanghai*　200433)

Abstract　A perfect zero knowledge proof with five moves which doesn't rely on any assumption is constructed in this paper. In this proof system, the prover can have either unlimited or limited computing power.

Key words　Completeness, soundness, zero knowledge, perfect zero knowledge proof system, random reducibility.