一种关于离散根问题的完美零知识证明系统

钟 鸣, 杨义先
(北京邮电大学信息安全中心, 北京 100876)

摘 要: 本文提出了一种关于离散根问题的完美零知识证明系统, 并且其零知识性不依赖于任何前提假设. 我们的工作提供了完美零知识证明系统以非平凡方式存在(对于不在 BPP 中的语言存在)的进一步证据.

关键词: 交互式证明; 完美零知识性; 离散根; 诺言问题
中图分类号: TN911.22 文献标识码: A 文章编号: 0372-2112 (2002) 04-0519-04

A Perfect Zero-Knowledge Proof System for the Discrete Root Problem

ZHONG Ming, YANG Yi-xian
(*Information Security Center, Beijing University of Posts and Telecomm, Beijing* 100876, *China*)

Abstract: This paper presents a perfect zero-knowledge proof system for a decision problem which is computationally equivalent to the Discrete Root Problem, and its zero-knowledge property does not rely on any assumptions. Thus we provide additional evidence to the belief that perfect zero-knowledge proof systems exist in a non-trivial manner (i.e., for language not in BPP).

Key words: interactive proofs; perfect zero-knowledge; discrete root; promise problem

1 引言

Goldwasser 最早在文[1]中提出了零知识证明的概念, 即验证者(verifier)在参与了零知识证明过程后, 任何能在多项式时间内计算出的信息, 也能在多项式时间后被验证者独立计算出, 只要他相信命题的真实性.

对零知识证明系统的定义主要考虑两种不同的概率分布:

(1) 在执行完与证明者(prover)的交互过程后, 由多项式时间的验证者生成的概率分布.

(2) 一台概率多项式时间自动机在基于待证明命题正确性的前提下生成的概率分布.

由此产生了不同的关于零知识证明系统的定义:

(1) 完美的零知识证明系统: 在这种系统中上述两种分布完全相同.

(2) 计算性(统计性)的零知识证明系统: 在这种系统中上述两种分布在多项式时间内不可分辨, 即两种分布不能被任何概率多项式时间的测试区分开.

在单向函数存在的前提下, Goldreich 等[2]证明了对于任何 NP 语言都存在计算性的零知识证明系统, 从而解决了关于计算性的零知识证明系统的存在情况问题. 但是关于完美的零知识证明系统的存在性问题情况却有所不同. 显然, 对于任何属于 BPP 范围内的语言都存在平凡的完美的零知识证明系统. 但对于非平凡的完美零知识证明系统(即对于不在 BPP 范围内的语言的完美零知识证明系统)的存在问题, 还远未得到彻底解决. 在前人的研究工作中已经提出了几种非平凡的完美零知识证明系统, 包括关于二次剩余问题[1]、图同构[2]和离散对数问题[3]的完美零知识证明系统.

文[3]利用诺言问题进行了证明, 本文通过使用与文[3]相同的证明方法, 提出了一种关于离散根问题的完美零知识证明系统, 从而进一步提供了关于完美零知识证明系统在非平凡的方式下存在的证据, 而且和文[3]一样, 我们的零知识证明系统也不依赖于任何前提假设.

令 n 是两个足够大的素数的乘积, 其因数分解情况保密. 而 e 是小于 n 的素数. 则离散根问题就是在给定 n, e 和 y 的情况下求出整数 x 使得 $y = x^e \bmod n$. DRP 问题被普遍认为是难解问题, 解决 DRP 问题等同与因数分解问题.

定义 $DRP_{\varepsilon(n)}$ 问题如下: 设 $y = x^e \bmod n$, 且 x 位于区间 $[1, \varepsilon(n) \cdot n]$ 或区间 $[\lceil n/2 \rceil, \lceil n/2 \rceil + \varepsilon(n) \cdot n]$ 中, 这里 $m^{-o(1)} < \varepsilon(n) < m^{-1}$ ($m = \log_2 n$). 则 $DRP_{\varepsilon(n)}$ 问题就是指确定 $x \leq \lceil n/2 \rceil$ 是否成立, 即判断 x 究竟属于哪个区间.

在第四节中, 提出了一种关于 $DRP_{\varepsilon(n)}$ 问题的完美零知识证明系统. 根据 $DRP_{\varepsilon(n)}$ 问题和 DRP 问题的计算等同性, 我们就拥有了关于与 DRP 问题同等困难的问题的完美零知识证明系统.

收稿日期: 2000-10-10; 修回日期: 2001-03-10
基金项目: 国家自然科学基金(No. 69772035, 69882002); 国家重点基础研究发展规划项目(No. G1999035805)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2 符号和定义

设 S 是一个集合, 则 $r \in_R S$ 是指 r 以均匀的概率分布从 S 的所有元素中随机选出的.

诺言问题(promise problem)[4]是指一对谓词 (P, Q), 这里 P 被称作"诺言"而 Q 被称作"询问". 如果一个图灵机 M 对于所有满足 $P(z)$ 的 z 停止, 并输出"yes"当且仅当 $Q(z)$ 也满足时, 则 M 就"解决"了这个诺言问题 (P, Q).

定义 1[3] 一个关于诺言问题 (P, Q) 的交互式证明系统是指满足如下条件的交互式图灵机对 $\langle P, V\rangle$:

(1) V 是一个与 P 分享输入的多项式时间自动机, P 与 V 能通过通信磁带相互通信.

(2)完备性(completeness): 对于任何常数 $c > 0$ 和所有足够长的 z, 若 $P(z) \wedge Q(z)$, 则有: $Prob(V$ 在与 P 交互后接受 $z) \geq 1 - |z|^{-c}$.

(3)正确性(soundness): 对于任何常数 $c > 0$ 和所有足够长的 z, 若 $P(z) \wedge \neg Q(z)$, 则有: $Prob(V$ 在与 P 交互后拒绝 $z) \geq 1 - |z|^{-c}$.

定义 2[3] 设 $\langle P, V\rangle$ 是关于诺言问题 (P, Q) 的交互式证明系统, V^* 是独立的验证者. 用 $\langle P, V^*\rangle(z)$ 来表示当 V^* 与 P 关于相同的输入 z 进行交互时, 它的所有只读磁带(包括随机磁带)的分布. 当对于任何多项式时间验证者 V^*, 都存在多项式时间自动机 M_{V^*} 使得对于所有满足 $P(z) \wedge Q(z)$ 的 z, 概率分布 $M_{V^*}(z)$ 与 $\langle P, V^*\rangle(z)$ 完全相同时, 则把 $\langle P, V\rangle$ 称为关于 (P, Q) 的完美零知识证明系统.

定义 3 令 n 是两个足够大的素数的乘积, 其因数分解情况保密. 而 e 是小于 n 的素数, $y \in Z_n^*$. 则 DRP 问题的定义如下:

输入: n, e, y.

输出: $x \in [1, n-1]$ 使得 $y \equiv x^e \bmod n$. (使用符号 $x = Dy^{1/e} \bmod n$)

定义谓词 Q 如下:

$$Q(n, e, y) \Leftrightarrow Dy^{1/e} \bmod n \in [\lceil n/2 \rceil, n-1]$$

令 $m^{-O(1)} < \varepsilon(n) < m^{-1}$ 时 $(m = \log_2 n)$, 则定义谓词 $P_{\varepsilon(n)}$ 如下:

$$P_{\varepsilon(n)}(n, e, y) \Leftrightarrow Dy^{1/e} \bmod n \in [1, \varepsilon(n) \cdot n] \text{ or } Dy^{1/e} \bmod n \in [\lceil n/2 \rceil + 1, \lceil n/2 \rceil + \varepsilon(n) \cdot n]$$

当 n、e 一定时也把 $Q(n, e, y)$、$P_{\varepsilon(n)}(n, e, y)$ 写作 $Q(y)$、$P_{\varepsilon(n)}(y)$.

可以看到, 由 $(P_{\varepsilon(n)}, Q)$ 定义的诺言问题就相当于 $DRP_{\varepsilon(n)}$ 问题.

3 DRP 问题和 $DRP_{\varepsilon(n)}$ 问题的计算等同性

引理 1 若 $D(2^e \cdot y)^{1/e} \bmod n \in [s_1, s_2]$, 则 $Dy^{1/e} \bmod n$ 必然属于两个区间之一, 即区间 $[\lceil \frac{s_1}{2} \rceil, \lceil \frac{s_2}{2} \rceil]$ 和区间 $[\lceil \frac{s_1+n}{2} \rceil, \lceil \frac{s_2+n}{2} \rceil]$.

定理 1 当 $m^{-O(1)} < \varepsilon(n) < m^{-1}$ 时 $(m = \log_2 n)$, DRP 问题和 $DRP_{\varepsilon(n)}$ 问题计算性等价, 即它们能在多项式时间内相互转换.

证明 显然, 如果我们知道如何解决 DRP 问题, 就能在多项式时间内解决 $DRP_{\varepsilon(n)}$ 问题, 因此只需证明在知道如何解决 $DRP_{\varepsilon(n)}$ 问题的情况下, 就能在多项式时间内解决 DRP 问题. 我们的证明是通过提出一种能够在多项式时间内解决问题的算法, 该算法使用的工具是一个与 $DRP_{\varepsilon(n)}$ 问题对应的预言(oracle)自动机 $HALF(n, y, s)$.

$HALF_e(n, y, s)$ 的定义如下:

$$HALF_e(n, y, s) = 0, Dy^{1/e} \bmod n \in [\lceil s/2 \rceil, \lceil s/2 \rceil + \varepsilon(n) \cdot n]$$

$$HALF_e(n, y, s) = 1, Dy^{1/e} \bmod n \in [\lceil \frac{s+n}{2} \rceil, \lceil \frac{s+n}{2} \rceil + \varepsilon(n) \cdot n]$$

$HALF_e(n, y, s) = ?$, 其他情况.

令 $m = \log_2 n$, 这里 $m^{-O(1)} < \varepsilon(n) < m^{-1}$, 而且"?"表示在这种情况下因为 $HALF_e(n, y, s)$ 无法正确判断, 因此可能输出 0 或者 1. 下述算法用 $HALF_e(n, y, s)$ 来解决 DRP 问题:

(1)令 $m = \log_2 n - 1$.

(2)计算 $y_1 \leftarrow y, y_2 \leftarrow 2^e \cdot y_1, y_3 \leftarrow 2^e \cdot y_2, \cdots, y_{m+1} \leftarrow 2^e \cdot y_m$.

(3)令 $c \leftarrow 0$.

(4)令 $s_1 \leftarrow c \cdot \varepsilon(n) \cdot (n), s_2 \leftarrow (n+1) \cdot \varepsilon(n) \cdot n$.

(5)对于 j 从 m 到 1 进行如下操作:

a. 如果 $HALF_e(n, y, s_1) = 0$, 则什么也不做.

否则 $s_1 \leftarrow s_1 + n, s_2 \leftarrow s_2 + n$

b. 计算 $s_1 \leftarrow \lceil s_1/2 \rceil, s_2 \leftarrow \lceil s_2/2 \rceil$

(6)对于 i 从 s_1 到 s_2 进行如下操作:

如果 $y = i^e \bmod n$ 则终止算法执行, 输出 i.

(7) $c \leftarrow c + 1$, 然后转到第(3)步执行.

该算法通过在 $1/\varepsilon(n)$ 个长度为 $\varepsilon(n) \cdot (n)$ 的区间中, 对 $Dy_{m+1}^{1/e} \bmod n = 2^m \cdot Dy^{1/e} \bmod n$ 进行计算搜索来发现 $Dy^{1/e} \bmod n$. 当搜索到正确的区间的时候, 根据引理 1, 能在 m 步内迅速发现 $Dy^{1/e} \bmod n$. 因为当 $Dy_i^{1/e} \bmod n$ 在一个间距为 d 的区间内时, $Dy_{i-1}^{1/e} \bmod n$ 属于两个长度为 $d/2$ 的区间内. 我们利用自动机 $HALF_e$ 来确定 $Dy_i^{1/e-1} \bmod n$ 所属的区间, 因此在最多 $m = \log_2 n - 1$ 步后就能将对 $Dy^{1/e} \bmod n$ 的搜索压缩在一个长度为 2 的区间内. 然后就可以检查该区间内的数是否是 $Dy^{1/e} \bmod n$. 如果都不满足的话, 说明搜索开始时 $Dy_{m+1}^{1/e} \bmod n$ 所在的区间是错误的, 要继续测试下一区间. 因为这里只有 $1/\varepsilon(n)$ 个即多项式数量的区间, 且对每个区间的搜索代价 $m = \log_2 n$ 也是多项式的. 所以可以看到我们的算法能在多项式时间内执行结束.

4 关于 $DRP_{\varepsilon(n)}$ 问题的完美零知识证明系统

如下协议被重复执行 $m = \log_2 n$ 次(除非 V 拒绝或 P 提前终止协议), 每一次执行时的随机数生成相互独立. 随机选取 $\varepsilon(n)$ 满足 $m^{-O(1)} < \varepsilon(n) < m^{-1}$ 时:

(1) V 选择 $b \in_R \{0, 1\}$ 和 $r \in_R [1, \min(\sqrt{\frac{n}{k+1}}, \sqrt{km})]$, 计

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

算 $\alpha = y^{b} \cdot r^{e} \bmod n$ 并将 α 送给 P. 除 α 外 V 还计算其它 m 对整数,第 i 对整数用 α_i 来表示. α_i 的构造过程是: V 选择 $b_i \in_R \{0, 1\}$ 和 $r_{i,0}, r_{i,1} \in_R [1, \min(\sqrt{\frac{n}{k+1}}, \sqrt{km})]$, 然后计算 $\alpha_{i,0} = y^{b_i} \cdot r_{i,b_i}^{e} \bmod n$, $\alpha_{i,1} = y^{b_i \oplus 1} \cdot r_{i,b_i \oplus 1}^{e} \bmod n$, 而 $\alpha_i = (\alpha_{i,0}, \alpha_{i,1})$. V 将这 m 对整数送给 P.

(2) P 以对于所有 2^m 个子集均匀的概率分布随机选择一子集 $I \subseteq \{1, 2, \cdots, m\}$ 并送给 V.

(3) V 给 P $\{(b_i, r_{i,0}, r_{i,1}): i \in I\}$ 及 $\{(b_i' = b_i \oplus b \oplus 1, r_i' = r \cdot r_{i, b \oplus 1}): i \in \bar{I}\}$.

(4) 对于每一个 $i \in I$, P 检查 α_i 是否是正确生成的, 而对于每一个 $i \in \bar{I}$, P 检查是否 $r_i' \in [1, \min(\frac{n}{k+1}, km)]$ 且 $y \cdot (r_i')^{e} = \alpha \cdot \alpha_{i, b_i'}$. 对于任何错误 P 都将停止协议的执行, 否则 P 计算 $\beta = H_k(\alpha)$ 并将 β 送给 V.

(5) 如果 $\beta \neq b$, 则 V 拒绝接受 P 的证明, 否则继续执行.

如果 V 不拒绝地执行完所有个回合, 则 V 接受 P 的证明.

定理 2　令 $m^{-O(1)} < \varepsilon(n) < m^{-1}$ 时 $(m = \log_2 n)$, 则协议一关于 $\mathrm{DRP}_{\varepsilon(n)}$ 问题构成一个完美的零知识交互式证明系统.

证明　(令 x 代表 $D_y^{1/e}$, 我们首先证明协议一关于 $\mathrm{DRP}_{\varepsilon(n)}$ 问题构成一个交互式证明系统, 然后再证明它的完美零知识性)

完备性: 若 $S(y) \wedge H_k(y)$, 则 $x \in [\sqrt{kn} + 1, \sqrt{kn + \varepsilon(n) \cdot n}]$. 另外 V 选择 $r \in_R [1, \min(\sqrt{\frac{n}{k+1}}, \sqrt{km})]$, 则当 $b = 0$ 时, 有

$$\alpha^{1/e} = r \in [1, \sqrt{\frac{n}{k+1}}] \subseteq [1, \sqrt{kn}]$$

当 $b = 1$ 时, 有

$$\alpha^{1/e} = xr \in [\sqrt{kn}, n \cdot \sqrt{\frac{k + \varepsilon(n)}{k+1}}] \subseteq [\sqrt{kn}, n]$$

因此 $\beta = H_k(\alpha) = b$, 这就意味着在这种情况下 P 总能使 V 接受自己的证明.

正确性: 若 $S(y) \wedge \neg H_k(y)$, 则 $x \in [1, \sqrt{\varepsilon(n) \cdot n}]$. 另外 V 选择 $r \in_R [1, \min(\sqrt{\frac{n}{k+1}}, \sqrt{km})]$, 则当 $b = 0$ 时, 有

$$\alpha^{1/e} = r \in [1, \sqrt{\frac{n}{k+1}}] \subseteq [1, \sqrt{kn}]$$

当 $b = 1$ 时有

$$\alpha^{1/e} = xr \in [\sqrt{kn}, \sqrt{kn \cdot \varepsilon(n) \cdot m}] \subseteq [1, \sqrt{kn}]$$

则对于不诚实的证明者 P^* 来说, V 经过一个回合后不拒绝接受 P^* 的证明的概率为:

$$Prob(P^*(\alpha) = b) = 1/2$$

因而 P^* 无法得到任何额外信息来欺骗 V, 使 V 相信 $x \in [\sqrt{kn} + 1, \sqrt{kn + \varepsilon(n) \cdot n}]$. 在每一回合中 P^* 能够成功欺骗 V 的概率为 $1/2$, 因此在所有 m 个回合中 P^* 都能够成功欺骗 V 的概率为 $1/2^m$.

零知识性: 对于所有的多项式时间交互自动机 V^*, 提出一个自动机 M_{V^*} 使得对于所有满足 $P_{\varepsilon(n)}(n, e, y) \wedge Q(n, e, y)$ 的输入都有: $M_{V^*}(n, e, y) = \langle P, V^* \rangle (n, e, y)$ 成立. 其中 M_{V^*} 能把 V^* 作为子例程使用.

M_{V^*} 的设计思想在于使得 V^* 能够产出所有计算 $H_k(\alpha)$ 必须的信息. 通过以不变的随机磁带输入(random tape)执行 V^* 多次, 这样 V^* 送出相同的 α 和 $\alpha_1, \cdots, \alpha_m$. 从而对每一整数对 α_i, M_{V^*} 能在一次试验中获得 $\{b_i, r_{i,0}, r_{i,1}\}$, 而在另一次试验中获得 $\{b_i', r_i'\}$. M_{V^*} 检查这些信息是否是通过正确的方式构成的, 如果是的话, M_{V^*} 就获得了足够的计算 $H_k(\alpha)$ 的信息.

下面就是对 M_{V^*} 的详细描述. M_{V^*} 在开始执行时为 V^* 选择随机磁带输入 $s \in_R \{0, 1\}^q$, 这里 $q = poly(|n, e, y|)$ 是 V^* 对于当前输入的运行时间上限. M_{V^*} 把 s 放在它的记录磁带上并执行如下协议 $m = \log_2 n$ 个回合.

回合 j:

(1) M_{V^*} 首先模仿前面和 V^* 的 $j-1$ 个回合的通信, 然后以输入 (n, e, y) 和 s 启动 V^*. 然后 M_{V^*} 从与 V^* 的通信磁带上读取 α 和 $\alpha_1, \cdots, \alpha_m$. M_{V^*} 随机选择子集 $I \subseteq \{1, 2, \cdots, m\}$, 然后把它放在 V^* 的通信磁带及自己的记录磁带上.

(2) M_{V^*} 从 V^* 的通信磁带上读取 $\{(b_i, r_{i,0}, r_{i,1}): i \in I\}$, $\{(b'_i, r'_i): i \in \bar{I}\}$. 对于每一个 $i \in I$, P 检查 α_i 是否是正确生成的, 而对于每一个 $i \in \bar{I}$, P 检查是否 $r_i' \in [1, \min(\frac{n}{k+1}, km)]$ 且 $y \cdot (r_i')^{e} = \alpha \cdot \alpha_{i, b_i'}$. 如果发现任何错误则 M_{V^*} 终止执行协议, 否则继续执行.

(3)这一步的目的是发现 $H_k(\alpha)$, 这是通过反复执行下面各步直到发现 $H_k(\alpha)$ 为止来实现的:

a. M_{V^*} 随机选择不同于 I 的子集 $K \subseteq \{1, 2, \cdots, m\}$, 然后 M_{V^*} 以相同的输入、相同的随机磁带 s 和相同的已成功模仿的所有回合启动 V^*. M_{V^*} 将 K 置于 V^* 的只读通信磁带上, 随后 M_{V^*} 就能从 V^* 的通信磁带上读取 $\{(\delta_i, s_{i,0}, s_{i,1}): i \in K\}$ 和 $\{(\delta_i', s_i'): i \in \bar{K}\}$.

b. M_{V^*} 检查收到的信息是否是正确生成的, 如果不是的话, 则 M_{V^*} 返回到上一步. 否则 M_{V^*} 寻找 i 使得 i 满足 $i \in I \cap \bar{K}$ 或 $i \in \bar{I} \cap K$. 因为 $I \neq K$, 所以这样的 i 是存在的. 不失一般性, 假设 $i \in I \cap \bar{K}$. 从而 i 对应于一个整数对 α_i, 使得 V^* (在不同的试验中)曾分别送出 $\{b_i, r_{i,0}, r_{r,1}\}$ 和 $\{b_i', r_i'\}$. 既然所有的信息都曾被 M_{V^*} 检查过并确认正确. M_{V^*} 现在可以计算出 $\beta = b_i \oplus \delta_i' \oplus 1$.

c. 并行于(a)和(b)的执行, M_{V^*} 利用穷举搜索来尝试发现 $H_k(\alpha)$.

(4) 在成功发现 β 以后, M_{V^*} 把 β 添加到它的记录磁带上, 完成 j 第个回合的执行.

在所有的回合都执行完成后, M_{V^*} 输出它的记录磁带并停止.

现在证明上述构造的正确性. 首先证明 M_{V^*} 能在多项式时间内执行结束, 其次, 证明 M_{V^*} 执行时产生的输出分布与 V^* 在与 P 交互时产生的磁带输出分布完全相同. 只要上述

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

两点能够得到证明, 我们的协议的零知识性也就得到了证明.

命题 1 自动机 M_{V^*} 能在多项式时间内执行结束.

证明 考虑当给定随机磁带 s 和前面 $j-1$ 个回合时, V^* 在第 j 个回合的期望执行时间. 当 V^* 对于集 $I\subseteq\{1, 2, \cdots, m\}$ 和随机磁带 s 回答正确时我们把 I 称作"好的". 我们用 g_s 来表示对应于 s 的所有"好的"子集的个数. 显然 $0\leqslant g_s\leqslant 2^m$. 要计算 V^* 在第 j 个回合的期望执行时间, 需要考虑以下三种情况:

(1) $(g_s\geqslant 2)$. 在 M_{V^*} 执行时, 如果在第一步中挑选的子集 I 是"好的"的话, 就必须考虑另一子集 K 也是"好的"的概率. 而如果在第一步中挑选的子集 I 不是"好的"的话, 本回合就将立即结束. 因此回合 j 的期望执行步数是:

$$\frac{g_s}{2^m}\left(\left(\frac{g_s-1}{2^m-1}\right)^{-1}+1\right)+\frac{2^m-g_s}{2^m}\cdot 1<\frac{g_s}{g_s-1}+1\leqslant 3$$

(2) $(g_s=1)$. M_{V^*} 在第一步中挑选的子集 I 是"好的"的概率只有 2^{-m}, 此时只能通过穷举搜索来发现 β, 而在其它情况下本回合都将立即结束. 因此, M_{V^*} 在第 j 个回合的期望执行步数上限为 $1+(n-1)\cdot 2^{-m}\leqslant 2$ 步.

(3) $(g_s=0)$. 因为 M_{V^*} 在第一步中挑选的子集 I 始终都是"坏的", 因此 M_{V^*} 都将立即结束执行.

综上所述有 M_{V^*} 能在多项式时间内执行结束.

命题 2 概率分布 $M_{V^*}(n, e, y)$ 和分布 $<P_{V^*}>(n, e, y)$ 完全相同.

证明 两个分布都包括一个随机的 s 及一系列的元素, 其中每一个元素是 $\{I, \beta\}$ (当 I 是"好的"时) 或就仅仅是 I (当 I 是"坏的"时). 在 $<P, V^*>(n, e, y)$ 中, 有 $\beta=H_k(\alpha)$ $(\alpha=V^*(n, e, y, s))$, 需要证明在 $M_{V^*}(n, e, y)$ 中也是这样. 就是说, 证明当 I 是"好的"时 M_{V^*} 能成功发现 $H_k(\alpha)$, 通过穷举搜索或发现 i 使得对于它 $\{b_i, r_{i,0}, r_{i,1}\}$ 和 $\{\delta_i', s_i'\}$ 都是正确生成的, 即:

$$(a)\ r_{i,0}, r_{i,1}\in\left[1, \min\left(\sqrt{\frac{n}{k+1}}, \sqrt{km}\right)\right]$$

$$(b)\ s_i'=r\cdot r_{i,b_i\oplus 1}\in\left[1, \min\left(\frac{n}{k+1}, km\right)\right]$$

$$(c)\ \alpha_{i,j}=y^{b_i\oplus j}\cdot(r_{i,b_i\oplus j})^e$$

$$(d)\ y\cdot(s_i')^e=\alpha\cdot\alpha_{i,\delta_i'}$$

在这种情况下有(通过(c)和(d)):

$$H_k(\alpha)=H_k(y\cdot(s_i')^e(\alpha_{i,\delta_i'})^{-1})$$
$$=H_k(y^{b_i\oplus\delta_i'}(r_{i,b_i\oplus\delta_i'})^e)^{-1})$$
$$=H_k(y^{b_i\oplus\delta_i'\oplus 1}\cdot(s_i'/r_{i,b_i\oplus\delta_i'})^e)$$

最后, 通过(a)和(b)有, $s_i'/r_{i,b_i\oplus\delta_i'}\in\left[1, \min\left(\sqrt{\frac{n}{k+1}}, \sqrt{km}\right)\right]$. 另外又有 $Dy^{1/e}\bmod n\in[\sqrt{kn}+1, \sqrt{kn+\varepsilon(n)\cdot n}]$, 因此有 $H_k(\alpha)=H_k(y^{b_i\oplus\delta_i'\oplus 1})=b_i\oplus\delta'_i+1$.

这正是 M_{V^*} 计算 $H_k(\alpha)$ 的方式. 这就完成了对于多项式时间验证者的零知识性的证明.

5 结束语

本文提出了一种不基于任何假设的关于 DRP 问题的完美零知识证明系统, 并对其完备性、正确性和零知识性进行了证明. 我们的工作对于完美零知识证明系统在非平凡方式下的存在情况的研究具有一定的价值. 在下一步的工作中, 我们将致力于把我们的协议从 DRP 问题推广到广义的条件下, 即在任何有限阿贝尔群中的求根问题.

参考文献:

[1] Goldwasser S, S Micali, C Rackoff. The knowledge complexity of interactive proof system [J]. SIAM J Comput, 1989, 18(1): 186–208.

[2] Goldreich O, et al. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design [J]. J Assoc Comput Math, 1991, 38(1): 691–729.

[3] Goldreich O, et al. A perfect zero-knowledge proof system for a problem equivalent to the discrete logarithm [J]. J Cryptology, 1993, 6(1): 97–116.

[4] Even S, Goldreich O, Y Yacobi. The complexity of promise problems with applications to public-key cryptography [J]. Inform Control, 1984, 61: 159–173.

作者简介:

钟 鸣 男, 1978 年生于四川绵阳市, 1996 年毕业于西安交通大学计算机系, 获工学学士学位, 现于北京邮电大学信息工程学院攻读博士学位, 主要研究方向为信息安全与电子商务.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net