# 一种基于离散对数问题的零知识证明协议

夏东岳

北京市第四中学　北京

【摘要】本文参考前人对于零知识证明问题相关研究，得出了若干设计协议的结论和方式。在此基础上，以降低零知识证明协议的欺骗概率为目标，使用离散对数问题作为数学支撑，结合分割选择技术作为基础进行设计。在最终验证环节引入一个随机数作为创新点，以及分割选择验证环节采取相邻数作差更为复杂的协议算法，设计出一种新式的零知识证明协议。经过对多种情况的假设进行推导，得到不同前提下的欺骗方案设计，运用概率积事件求出最终欺骗概率，与前人的成果进行比较，达成降低欺骗概率的目标。针对此协议还提出了个性化设计方案以降低协议欺骗概率，以及给出未来协议的应用和发展方向。

【关键词】零知识证明；离散对数；密码学

【收稿日期】2024 年 1 月 18 日　【出刊日期】2024 年 3 月 21 日　【DOI】10.12208/j.aam.20240007

## A zero-knowledge proof protocol based on discrete logarithm problem

*Dongyue Xia*

*Beijing No. 4 Middle School, Beijing*

【**Abstract**】In this paper, some conclusions and methods of designing protocols are obtained by referring to previous researches on zero-knowledge proof. On this basis, aiming at reducing the deception probability of the zero-knowledge proof protocol, the discrete logarithm problem is used as the mathematical support and the cut and choose technique is used as the basis for the design. A new zero-knowledge proof protocol is designed by introducing a random number as the innovation point in the final verification process and using a more complicated protocol algorithm to cut and choose process. After deducing the hypothesis of various situations, the deception scheme design under different premises is obtained. The final deception probability is obtained by using probability product events, and the goal of reducing the deception probability is achieved by comparing with the previous achievements. A personalized design scheme is proposed to reduce the probability of deception, and the future application and development direction of the protocol are given.

【**Keywords**】Zero-knowledge proof; Discrete logarithm; Cryptography

## 1 引言

### 1.1 背景介绍

在现代信息时代下，身份验证已经成为无法忽视的一环。无论是区块链应用中交易双方身份的真实性验证，还是军事上各种高级权限申请上的验证，都面临着伪造身份，窃取信息等安全性问题出现。现如今，解决此类问题有经典的数字签名，数字证书等加密协议解决问题，也有零知识证明协议、最小泄露证明协议等从逻辑上更加复杂的方式解决问题。本文着手于零知识证明协议进行设计。

零知识证明（Zero-knowledge proof）的解释是“证明某一个事实并且不泄露知识”，此问题最早是在 1985 年由 S。 Goldwasser，S。 Micali 和 C。 Rackoff 在 *The Knowledge Complexity of Interactive Proof Systems* [5] 一文中进行研究的，使用零知识证明用于身份验证最早是由 Uriel Feige，Amos Fiat 和 Adi Shamir[7,8] 提出的。此问题具有 2 个特征：可靠性和不可欺骗性。假设现在有一人 Peggy 想向另一人 Victor 进行零知识证

明验证，可靠性是指 Victor 无法从 Peggy 提供的证明中得到任何有利于自己得到知识的信息；不可欺骗性是指如果 Peggy 并不知道知识，她无法通过零知识证明协议向 Victor 证明自己拥有这个知识。

Michael Rabin [6] 是首个在零知识证明中使用分割选择（cut and choose）的技术的人，此技术将验证过程分为 2 类，使得 Peggy 一方不能重复猜出验证要求，进而降低欺骗概率。

在前人的算法中，可靠性的保障主要在于将已知知识进行转化，从而 Victor 无法得到知识的原有形式。不可欺骗性是同时基于数学问题和分割选择技术，如图同构问题、哈密顿圈问题、因子分解问题、离散对数问题等，Peggy 一方很难在短时间内破解此类问题（NP 或 NP 完全问题）；并将验证要求分割成 2 类，通过验证次数的增加，在验证 $n$ 次下，达到欺骗概率为 $\frac{1}{2^n}$。

在前人的论文中[1-4]，可总结出以下结论：唯一可能泄露知识的步骤在分割选择验证之后，即最终验证环节，可靠性的分析只需分析这一环节是否有泄露可能即可；降低欺骗概率的方式除增加协议重复次数以外，也可以增加一次验证所需要的数据量，对数据进行分割选择验证；欺骗协议的设计逻辑一般是和协议逻辑正好相反，先保证最终验证环节的通过，再根据伪造的数据通过分割选择验证，即欺骗协议是倒推逻辑。

1.2 协议创新

本协议在欺骗概率量级突破到 $\frac{1}{n2^n}$，这一种新式的证明协议是具有开拓性的，具体的创新点及其原因分析如下：

（1）在最终验证环节引入随机数，而前人论文 [1] 并未达到此效果的原因是在该论文 $c_i=1$ 一类验证中，将一个数据作为标准，其他数据都与这一个数据进行做差运算完成验证，致其欺骗协议在倒推中只需预测 $C=\{c_1,c_2,.....,c_n\}$ 即可。本协议在欺骗时不仅需要预测出 $C=\{c_1,c_2,.....,c_n\}$，还需要预测出 $e_t$ 才可完成欺骗。

（2）在 $c_i=1$ 一类验证中，采取去中心化的验证，不以一个数据作为标准，而是以两两相邻数据的差值 $r_{e_j}-r_{e_{j-i}}\equiv\Delta_{e_j}(\mathrm{mod}\ p)(e_0=e_v)$ 作为标准，使得欺骗时无法简单找到伪造起点，还需考虑 $c_i=1$ 一类中数据的互相关系才能欺骗。

（3）分割选择验证环节中不验证全部数据，只随机选择一个数据：

$K=\{k_1,k_2,.....,k_n\}$ 进行验证，降低运行时间成本，可在相同时间内增加数据量 $n$，进一步降低欺骗概率。

（4）协议只需 1 个原根，不需要提前准备多个原根，在寻找原根的时间成本上进一步降低。

（5）提出了个性化的设计，可以通过增加最终验证环节的验证个数进一步提高随机数带来的安全性收益。例如当 $e_t$ 验证个数提高到 2 个时，此时理论上欺骗概率可降低至 $\frac{1}{n(n-1)2^{n-1}}$，可以应对更高程度的验证需求。

## 2 预备知识

2.1 完全剩余系与简化剩余系

给定一个正整数 $n$，从模 $n$ 的每种余数类中各取一个元素，组成的集合记作 $S_n=\{i\mid i\in N,i\in[0,n-1]\}$，$S_n$ 称作模 $n$ 的完全剩余系。将 $S_n$ 中与 $n$ 互素的数取出组成新集合 $S_n^*=\{i\mid i\in S_n,(i,n)=1\}$，$S_n^*$ 称作模 $n$ 的简化剩余系。

2.2 原根

对于素数 $p$，取 $a\in S_p^*$，若满足关于 $x$ 的同余方程 $a^x\equiv 1(\mathrm{mod}\ p)$ 的最小正整数解为 $x=p-1$，则称 $a$ 是模 $p$ 的原根。且根据原根存在性定理，对于素数 $p$，一定存在模 $p$ 的原根。

2.3 离散对数及离散对数问题

对于一个素数 $p$，设 $a$ 是模 $p$ 的原根，$b\in S_p^*$，则满足存在唯一的整数 $x_0(0\le x_0\le p-1)$ 使得 $a^{x_0}\equiv b(\mathrm{mod}\ p)$，则指数 $x_0$ 称为 $b$ 的以 $a$ 为底的离散对数。当给定一个素数 $p$，设 $a$ 是模 $p$ 的原根，

$b \in S_p^*$，求出满足 $a^x \equiv b(\mathrm{mod}\ p)$ 的解 $x_0$ 的问题称为离散对数问题。在现阶段离散对数问题尚未有多项式时间解。

## 3 零知识证明协议

### 3.1 协议设计

给定一个大素数 $p$，设 $a$ 是模 $p$ 的原根，$b \in S_p^*$。当 Peggy 知道 $a^x \equiv b(\mathrm{mod}\ p)$ 的解 $x_0$，向 Victor 进行证明：

（1）Peggy 秘密生成随机整数数列 $R = \{r_1, r_2, ....., r_n\}$。

（2）Peggy 计算出矩阵 $M = \begin{bmatrix} m_{11} & m_{12} & ..... & m_{1n} \\ m_{21} & m_{22} & ..... & m_{2n} \\ ..... & ..... & ..... & ..... \\ m_{n1} & m_{n2} & ..... & m_{nn} \end{bmatrix}$ 发送至 Victor，

其中 $a^{r_i r_j} \equiv m_{ij}(\mathrm{mod}\ p)$。

（3）Peggy 和 Victor 根据掷硬币协议生成随机数

$C = \{c_1, c_2, ....., c_n\}(c_i \in \{0,1\}, i = 1,2,.....n)$。

将随机数分为 $D$，$E$ 两组满足：

$D = \{i \mid c_i = 0, 1 \le i \le n\}$，$E = \{i \mid c_i = 1, 1 \le i \le n\}$；

记作 $D = \{d_1, d_2, ....., d_u\}$，$E = \{e_1, e_2, ....., e_v\}$；

显然 $u + v = n$。

（4）Peggy 和 Victor 共同生成随机下标序列

$K = \{k_1, k_2, ....., k_n\}$，其中满足 $c_{k_i} = 0$。

（5）若 $c_i = 0$，Peggy 发送 $r_{k_i}$，$r_i$ 至 Victor。

若 $c_i = 1$，设下标 $e_j = i$；

Peggy 计算 $r_{e_j} - r_{e_{j-i}} \equiv \Delta_{e_j}(\mathrm{mod}\ p)(e_0 = e_v)$ 发送至 Victor。

（6）若 $c_i = 0$，Victor 验证 $m_{ik_i} \equiv a^{r_{k_i} r_l}(\mathrm{mod}\ p)$。

若 $c_i = 1$，Victor 验证 $\dfrac{m_{e_j k_i}}{m_{e_{j-1} k_i}} \equiv a^{r_{k_i} \Delta_{e_j}}(\mathrm{mod}\ p)$。

（7）（5）-（6）两步循环直至 $i$ 从 1 遍历至 $n$ 结束。

（8）操作结束后，Victor 随机选择下标数列 $E$ 中的一个数 $e_t$，

Peggy 计算 $z \equiv x_0 - r_{e_t}(\mathrm{mod}\ p-1)$ 发送给 Victor。

（9）Victor 验证 $a^{zr_i} \equiv \dfrac{b^{r_i}}{m_{ie_t}}(\mathrm{mod}\ p)(i = 1,2,.....,n)$。

### 3.2 协议分析

可靠性分析：由协议第（8）步知，Victor 唯一能获取关于 $x_0$ 的信息只有 $z \equiv x_0 - r_{e_t}(\mathrm{mod}\ p-1)$。

而 Victor 无法获取 $r_{e_t}$，协议可靠。

不可欺骗性分析：假设 Peggy 不知道 $x_0$，由于只有 $r_{d_i}$ 暴露给 Victor，依据此性质，在预测出所有的 $C$，$e_t$（在欺骗方案中为作区分记作 $g_t$）的条件下可以向 Victor 欺骗，欺骗方案如下（为以示区别，协议中实时产生的数据名称沿用协议中的名称，预测的数据名称采用下文欺骗方案中的名称）：

（1）Peggy 秘密生成随机整数数列 $R = \{r_1, r_2, ....., r_n\}$，并根据预测，

将 $C$ 提前分为 $F$，$G$ 两组，其中 $F=\{i \mid c_i=0,1\le i\le n\}$

$G=\{i \mid c_i=1,1\le i\le n\}$；记作 $F=\{f_1,f_2,.....,f_u\}$，$G=\{g_1,g_2,.....,g_v\}$；

显然 $u+v=n$。

（2）对于 $F$ 组，Peggy 计算 $m_{ij}\equiv a^{r_i r_j}(\bmod p)(i,j\in F)$。

（3）对于 $G$ 组，Peggy 生成随机数 y，并计算

$m_{ig_t}=m_{g_i i}\equiv\dfrac{b^{r_i}}{a^{y}}(\bmod p)(i\in F)$。

（4）Peggy 秘密生成随机数列 $\Delta=\{\delta_1,\delta_2,.....\delta_v\}(\sum_{i=1}^{v}\delta_i=0)$，并计算

$m_{g_{(t+j+1)}i}=m_{ig_{(t+j+1)}}\equiv m_{ig_{(t+j)}}a^{r_i\delta_{t+j+1}}(\bmod p)$，其中下标按模 $v$ 处理。

用上述方案得到的数据可完成协议验证。

由于矩阵 $M$ 在协议验证前已经发送至 Victor，若预测不准确，有以下情况 Peggy 将无法通过协议验证：

（1）预测 $c_i=1$ 但 $c_i=0$，此时设 $g_j=i$，已发送的矩阵 $M$ 中

$m_{g_j k_i}\equiv m_{g_{j-1}k_i}a^{r_{k_i}\delta_j}(\bmod p)$，Peggy 需找到 $r_i$ 满足

$$a^{r_i r_{k_i}}\equiv m_{g_j k_i}(\bmod p)$$

此为离散对数问题，没有多项式时间解。

（2）预测 $c_i=0$ 但 $c_i=1$，此时设 $e_j=i$，已发送的矩阵 $M$ 中

$m_{e_j k_i}\equiv a^{r_i r_{k_i}}(\bmod p)$，Peggy 需找到 $\delta_j$ 满足

$$a^{\delta_j k_i}\equiv\frac{m_{ik_i}}{m_{e_{j-1}k_i}}(\bmod p)$$

此为离散对数问题，没有多项式时间解。

（3）$g_t$ 预测错误，则协议第（9）步中 Peggy 需找到 $z$ 满足：

$$a^{zr_i}\equiv\frac{b^{r_i}}{m_{ie_t}}(\bmod p)$$

此为离散对数问题，没有多项式时间解。

综上，预测 $C$ 和 $e_t$ 事件独立，准确预测每一个 $c_i$ 概率为 $\dfrac{1}{2}$，准确预测 $C$ 概率为 $\dfrac{1}{2^n}$，准确预测 $e_t$ 概率为 $\dfrac{1}{n}$，二者同时预测准确，即协议欺骗率为 $\dfrac{1}{n2^n}$。

### 3.3 个性化设计

通过增加最终验证中 $e_t$ 的验证个数和验证次数，可增加协议的安全性。

## 4 研究期望

离散对数问题是当今比较难解决的问题，将离散对数和零知识证明等其他应用密码学分支结合起来，可应用在各种场景中的身份识别。比如可以应用在银行和客户的身份验证中，银行的一个分行统一使用一个大模数 $p$，为每一个客户分发一个特别的离散对数问题，离散对数解作为客户的特征身份。每当客户申请对自己的银行账户做出改变时候，调用零知识证明协议进行身份验证。

针对不同受信等级的账户，提供不同的数据量、验证次数或改变最终验证环节的验证个数。冻结账户则可以统一改变客户的离散对数问题，用银行的一个不对外公布的离散对数问题进行替换，使其不会被攻破。

也可以尝试进一步优化分割选择步骤，提出基于 3 个及以上选项的分割选择验证协议，发展新型的零知识证明协议。还可加入单向函数，使欺骗方案难以通过倒推进行设计实践。

## 参考文献

[1] 李曦 王道顺.多项式函数根的零知识证明协议[J].清华大学学报,2009,49(7):999-1002.

[2] Bruce Sehneier. Applied cryptography: Protocols, Algorithms, and Source Code in C[M].北京:机械工业出版社,2014.1:71-83.

[3] 欧海文 叶顶锋 杨君辉 戴宗铎.关于同时基于因子分解与离散对数问题的签名体制[J]. 通信学报,2004.10, 25(10): 143-147.

[4] 韩德, 郑素文.基于椭圆曲线群上的零知识证明[J]. 装甲兵工程学院学报, 2010.12,24(6):92-94.

[5] S. Goldwasser, S. Micali, C. Rackoff. The Knowledge Complexity of Interactive Proof Systems[J].Proceedings of the 17th ACM Symposium on Theory of Computing, 1985:291-304.

[6] M.O. Rabin. Digital Signatures[J].Foundations of Secure Communication, New York: Academic Press, 1978:155-168.

[7] A. Fiat, A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems[J].Advances in Cryptology_CRYPTO ’86 Proceedings, Springer-Verlag, 1987:186-194.

[8] A. Fiat, A. Shamir. Unforgeable Proofs of Identity[J].Proceedings of Securicom 87, Paris, 1987:147-153.