

# 一种基于二次剩余的抛掷硬币方案

杨晓莉, 左祥建

(陕西师范大学 计算机科学学院, 陕西 西安 710119)

**摘要:** 硬币抛掷在密码学和现实生活中都有重要的应用。比如篮球比赛或足球比赛, 裁判用硬币抛掷的正反面来决定哪边先开球。然后裁判抛掷硬币, 如果硬币是正面, 那么甲方从左往右攻; 反之, 乙方从左往右攻。这个实验就是一种简单的硬币抛掷协议。然而, 对于不在同一地方的两人来说, 如何公平地抛掷硬币, 就是一个有待研究的问题了。研究了两方抛掷硬币的一个推广问题—多方抛掷硬币问题, 构造了这个问题的解决方案。该方案基于 Goldwasser-Micali 概率加密算法的异或同态性和因子分子的困难性, 对多人抛掷硬币的结果进行异或运算, 实现了安全多方计算, 保证了多人抛掷硬币的安全性和公平性。并对该方案进行了安全性分析和复杂度分析。

**关键词:** 密码学; 安全多方计算; 硬币抛掷; 概率加密; 异或同态性

**中图分类号:** TP309

**文献标识码:** A

**文章编号:** 1673-629X(2016)09-0139-04

doi: 10.3969/j.issn.1673-629X.2016.09.031

## A Coin Toss Protocol Based on Quadratic Residue

YANG Xiao-li, ZUO Xiang-jian

(School of Computer Science, Shaanxi Normal University, Xi'an 710119, China)

**Abstract:** The coin toss has important applications in both cryptography and information security. For example, in a basketball match or a football match, the referee decides which team to play first by the result of a coin toss, then judges the toss of a coin. If a coin is positive, the party A attacks from left to right; conversely, party B does from left to right. This experiment is a kind of simple coin drop agreement. However, for two people not in the same place, how to fairly toss a coin is a problem to be researched. Studies an extended problem of a coin toss; multi-party coin toss protocol, and constructs a solution to it. This scheme is based on the XOR homomorphism of Goldwasser-Micali probabilistic encryption algorithm and difficulty of factor molecules, and is exclusive or operation to the results of many people toss of a coin, guaranteeing the security and fairness in secure multiparty coin toss. It proves that these protocols are analyzed in security and complexity.

**Key words:** cryptography; secure multi-party computation; coin toss; probabilistic encryption; XOR homomorphism

## 0 引言

随着互联网的发展, 不仅给人们的生活提供了便利, 同时也带来了不少麻烦, 比如说个人信息泄漏、信息破坏、信息污染, 这些都是信息安全问题<sup>[1-2]</sup>。信息安全问题是当今社会谈论的热点问题之一。因此, 解决信息安全问题是学者研究的重要问题。

密码学中会遇到两方比较猜测结果的问题, 可是双方都不想让对方知道自已的信息, 这就是密码学和信息安全中的多方保密计算<sup>[3]</sup>, 抛掷硬币方案是安全多方计算的一个应用特例。Blum 在 1982 年通过调制解调器引入抛掷公平硬币问题<sup>[4]</sup>, 利用位比特协议解决了两个人抛掷硬币问题; Ben 等在 1990 年提出了硬

币抛掷问题<sup>[5]</sup>; Lindell 等在 2003 年提出两方安全抛掷硬币问题<sup>[6]</sup>; 余堃也在 2003 年提出了公平硬币抛掷协议<sup>[7]</sup>。但是这些协议仅限于两方, 没有解决多方参与抛掷硬币问题。

文中提出一种多方参与抛掷硬币方案, 此方案与两方参与抛硬币方案相比, 具有普遍适用性, 增加了游戏的趣味性, 保证了多方参与抛掷硬币的安全性。

全同态加密是指在 2009 年 IBM 公司的克雷格·金特里 (Craig Gentry) 发表了一篇文章<sup>[8]</sup>, 公布了一项关于密码学的全新发现: 一项真正的突破。他发现, 对加密的数据进行处理得到一个输出, 将这一输出进行解密, 其结果与用同一方法处理未加密的原始数据得

收稿日期: 2015-08-18

修回日期: 2016-01-06

网络出版时间: 2016-08-23

基金项目: 国家中央高校基本科研业务费专项资金项目 (GK201504017); 包头市科技计划项目 (2014S2004-2-1-15)

作者简介: 杨晓莉 (1989-), 女, 硕士研究生, 研究方向为密码学与信息安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20160823.1343.028.html>

到的输出结果是一样的。这样不影响明文数据的机密性,同态加密方法在多方保密计算中发挥了重要的作用。文中运用了 Goldwasser 概率加密的异或同态性,在不暴露明文的情况下,对密文进行异或得出的结果与对明文异或得出的结果相同,高效地解决了多方抛硬币问题。

## 1 预备知识

### 1.1 二次剩余

定义 1: 设  $n$  是正整数, 若同余式  $x^2 \equiv a \pmod{n}$ ,  $(a, n) = 1$  有解, 则  $a$  叫模  $n$  的二次剩余; 否则  $a$  叫模  $n$  的非二次剩余<sup>[9]</sup>。

定义 2: 设  $p$  是素数, 定义勒让德符号 (Legendre)<sup>[10]</sup>:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{若 } a \text{ 是模 } p \text{ 的二次剩余} \\ -1, & \text{若 } a \text{ 是模 } p \text{ 的二次非剩余} \\ 0, & \text{若 } p \mid a \end{cases}$$

设  $n$  是正整数,  $n = pq$ , 若满足勒让德符号  $\left(\frac{a}{p}\right) = 1$ ,  $\left(\frac{a}{q}\right) = 1$ , 就是说  $a$  是模  $p$  的二次剩余,  $a$  也是模  $q$  的二次剩余, 则  $a$  叫做模  $n$  的二次剩余; 否则,  $a$  叫做  $n$  的二次非剩余。

### 1.2 Goldwasser 公钥加密系统

1984 年, S. Goldwasser 与 S. Micali 提出了一种新的概率加密体制<sup>[11]</sup>, 首次将随机比特的概率思想运用到公钥密码体制。每次加密是针对每个明文选取一个随机数计算出相应的密文。该加密体制对同一明文进行两次加密时得到的密文不同, Goldwasser-Micali 算法主要是对 0, 1 进行加密, 解决了 RSA 算法的缺陷, 即因 RSA 算法的不足而提出。该体制的加密利用合数模二次剩余逐次加密, 是第一个具有语义安全性的类同态加密方案。

Goldwasser-Micali 公钥加密系统是基于二次剩余的比特承诺协议, 包含以下算法:

密钥生成: 随机选取大素数  $p, q$ , 计算  $n = pq$ , 随机选取一个正整数  $t$  满足勒让德符号:  $\left(\frac{t}{p}\right) = \left(\frac{t}{q}\right) = -1$ , 即  $t$  是模  $p, q$  的二次非剩余。公开密钥是  $(n, t)$ , 私钥是  $(p, q)$ 。

加密: 设有待加密的二进制表示的明文:  $m = m_1 m_2 \cdots m_n$ 。对每个明文比特  $m_i$ , 随机选择整数  $r_i: 1 \leq r_i \leq n-1$ , 计算:

$$E(m_i) = \begin{cases} tr_i^2, & m_i = 1 \\ r_i^2, & m_i = 0 \end{cases}$$

得到密文  $E(m) = (E(m_1), E(m_2), \cdots, E(m_n))$ 。

解密: 设密文  $E(m) = (E(m_1), E(m_2), \cdots, E(m_n))$ 。对每个密文  $E(m_i)$ , 先计算出勒让德符号  $\left(\frac{E(m_i)}{p}\right)$  和  $\left(\frac{E(m_i)}{q}\right)$  的值, 然后令

$$m_i = \begin{cases} 0, & \text{若 } \left(\frac{E(m_i)}{p}\right) = \left(\frac{E(m_i)}{q}\right) = 1 \\ 1, & \text{若 } \left(\frac{E(m_i)}{p}\right) = \left(\frac{E(m_i)}{q}\right) = -1 \end{cases}$$

得到解密出的明文为  $m = m_1 m_2 \cdots m_n$ 。

### 1.3 同态加密

异或同态性: 给定明文  $m_1, m_2$ ,  $E(m_1) \times E(m_2) = t^{m_1} r_1^2 t^{m_2} r_2^2 = t^{m_1+m_2} (r_1 r_2)^2 = E(m_1 \oplus m_2)$ , 由此可知 Goldwasser 加密系统满足异或同态性, 支持任意多次异或同态操作, 即对任意的消息  $m_1, m_2, \cdots, m_n$  有:

$$E(m_1) \times E(m_2) \times \cdots \times E(m_n) = E(m_1 \oplus m_2 \oplus \cdots \oplus m_n)$$

即 Goldwasser 加密系统的同态性仅适用于异或操作。

例如:

(1) 当  $m_1 = 1, m_2 = 0$  时,  $E(m_1) = tr_1^2 \bmod n, E(m_2) = r_2^2 \bmod n$ ,  $E(m_1) \times E(m_2) = tr_1^2 r_2^2 \bmod n = E(m_1 \oplus m_2) = 1, m_1 \oplus m_2 = 1 \oplus 0 = 1$ 。

(2) 当  $m_1 = 1, m_2 = 1$  时,  $E(m_1) = tr_1^2 \bmod n, E(m_2) = tr_2^2 \bmod n$ ,  $E(m_1) \times E(m_2) = t^2 r_1^2 r_2^2 \bmod n = E(m_1 \oplus m_2) = 0, m_1 \oplus m_2 = 1 \oplus 1 = 0$ 。

(3) 当  $m_1 = 0, m_2 = 0$  时,  $E(m_1) = r_1^2 \bmod n, E(m_2) = r_2^2 \bmod n$ ,  $E(m_1) \times E(m_2) = r_1^2 r_2^2 \bmod n = E(m_1 \oplus m_2) = 0, m_1 \oplus m_2 = 0 \oplus 0 = 0$ 。

## 2 问题与解决方案

### 2.1 两人参与抛硬币方案的协议

协议 1: 两方参与抛硬币的一般步骤:

- (1) Alice 必须在 Bob 猜测之前抛币。
- (2) Bob 猜测后, Alice 不能再抛币。
- (3) Bob 猜测前不能知道硬币怎样落地。

协议 2: Alice 和 Bob 在玩一个抛硬币游戏, 下面提出了两个人的游戏过程协议<sup>[12]</sup>:

(1) 由 Alice 发送一对大素数  $p, q$  的乘积  $n = pq$  给 Bob。

(2) Bob 在  $Z_n^*$  中随机选取一个小于  $\frac{n}{2}$  的  $r$ , 然后发送  $a = r^2 \bmod n$  给 Alice。

(3) Alice 验证  $a$  是否为模  $n$  的二次剩余, 若满足  $\left(\frac{a}{p}\right) = 1, \left(\frac{a}{q}\right) = 1$ , 则  $a$  是模  $p$  的二次剩余, 也是模  $q$

的二次剩余,计算  $r^2 \equiv a \pmod n$ , 计算出四个根, 分别是  $r_1, n - r_1, r_2, n - r_2$ , 其中  $r_1 < r_2 < \frac{n}{2}$ , 然后 Alice 随机猜测 Bob 选择的是  $r_1, r_2$  中的哪一个, 并把猜测结果 0, 1 发送给 Bob (大的用 1 表示, 小的用 0 表示)。

(4) Bob 收到 0 或 1 后将第 2 步选择的  $r$  发送给 Alice。

(5) Alice 验证  $r \in Z_n^* \wedge \{r_1, r_2\}$ , Alice 根据第 3 步和接收到的  $r$  可以知道她的猜测是否正确, 将  $p, q$  值传送给 Bob。

(6) Bob 检验  $p, q$  是否为两个不同的素数, 且验证  $n = pq$  是否成立。根据  $r^2 \equiv a \pmod n$ , 计算出  $\{r_1, r_2\}$ , Bob 知道他和 Alice 的游戏最后谁胜利了。

2.2 多方参与抛掷硬币协议

2.2.1 方案的基本思想一

$n$  个参与者  $P_1, P_2, \dots, P_n$  每人产生 1 比特信息, 并对各自的 1 比特信息  $m_1, m_2, \dots, m_n$  分别加密, 通过对各自的猜测值的密文进行保密的异或运算产生一个随机数  $m_0$ , 利用 Goldwasser 概率加密算法的异或同态性。这个随机数  $m_0$  就是硬币抛掷的结果。

协议 3: 多方保密确定硬币结果。

输入:  $n$  个参与者  $P_1, P_2, \dots, P_n$  的猜测值分别是  $m_1, m_2, \dots, m_n$ 。

输出: 硬币结果  $m_0$ 。

(1)  $P_1, P_2, \dots, P_n$  用 Goldwasser-Micali 概率加密算法分别对  $m_1, m_2, \dots, m_n$  进行加密, 得到

$$E(m_i) = \begin{cases} tr_i^2, & m_i = 1 \\ r_i^2, & m_i = 0 \end{cases}$$

(2)  $P_1$  将加密结果  $E(m_1)$  发送给  $P_2$ ,  $P_2$  做运算  $E(m_1) \times E(m_2)$ , 并把结果发送给  $P_3$ ,  $P_3$  做运算  $E(m_1) \times E(m_2) \times E(m_3)$ , 并把结果发送给  $P_4$ , 依次类推,  $P_{n-1}$  做运算  $E(m_1) \times E(m_2) \times \dots \times E(m_{n-1})$ , 并把结果发送给  $P_n$ ,  $P_n$  做运算  $E(m_1) \times E(m_2) \times \dots \times E(m_{n-1}) \times E(m_n)$ , 并把结果发送给  $P_1$ 。

(3)  $P_1$  由 Goldwasser 概率加密的异或同态性得出  $E(m_1) \times E(m_2) \times \dots \times E(m_n) = E(m_1 \oplus m_2 \oplus \dots \oplus m_n)$ ,  $P_1$  对  $P_n$  发来的结果用勒让德判断是否为二次剩余, 如果是, 那么硬币结果为  $m_0 = 0$ , 否则, 硬币结果为  $m_0 = 1$ , 并将  $m_0$  公布给其他参与者。

(4)  $P_1$  公布  $p, q$  的值, 其他参与者验证  $P_1$  公布结果的正确性。

2.2.2 方案的基本思想二

$n$  个参与者  $P_1, P_2, \dots, P_n$  每人产生  $n$  比特信息, 并对各自的  $n$  比特信息  $m_1, m_2, \dots, m_n$  分别加密, 通过对各自的猜测值的密文进行保密的异或运算产生  $n$  比特

信息  $m_0$ , 利用 Goldwasser 概率加密算法的异或同态性, 这个  $n$  比特  $m_0$  就是硬币抛掷的结果。此方法与上述运算方法相同。

2.3 实例验证

(1) 设有 4 个参与者  $P_1, P_2, P_3, P_4$  的猜测值是  $m_1 = 1, m_2 = 0, m_3 = 0, m_4 = 1$ ,  $P_1, P_2, P_3, P_4$  对各自的猜测结果分别加密为  $E(m_1) = tr_1^2 \pmod n, E(m_2) = r_2^2 \pmod n, E(m_3) = r_3^2 \pmod n, E(m_4) = tr_4^2 \pmod n$ 。

(2)  $P_1$  将加密结果  $E(m_1) = tr_1^2 \pmod n$  发送给  $P_2$ ,  $P_2$  计算  $E(m_1) \times E(m_2) = tr_1^2 r_2^2 \pmod n$ , 并把结果发送给  $P_3$ ,  $P_3$  计算  $E(m_1) \times E(m_2) \times E(m_3) = tr_1^2 r_2^2 r_3^2 \pmod n$ , 并把结果发送给  $P_4$ ,  $P_4$  计算  $E(m_1) \times E(m_2) \times E(m_3) \times E(m_4) = t^2 r_1^2 r_2^2 r_3^2 \pmod n$ , 则由异或同态性得  $E(m_1 \oplus m_2 \oplus \dots \oplus m_n) = t^2 r_1^2 r_2^2 r_3^2 \pmod n$ , 并把结果发送给  $P_1$ 。

(3)  $P_1$  判断勒让德符号  $\left(\frac{E(m_1)E(m_2)E(m_3)E(m_4)}{p}\right) = \left(\frac{E(m_1)E(m_2)E(m_3)E(m_4)}{q}\right) = 1$ , 由加密同态性:  $m_0 = m_1 \oplus m_2 \oplus m_3 \oplus m_4 = 0$ , 并将结果公布给  $P_2, P_3, P_4$ 。

(4)  $P_1$  公布  $p, q$  的值, 其他参与者验证  $P_1$  公布结果的正确性。

3 性能分析

3.1 安全性分析

在数论中, 对于  $n$  的任意二次剩余  $r$ , 求  $r$  使得  $r^2 \equiv a \pmod n$  的困难性相当于对  $n$  进行因子分解的困难性, 特别是当  $n$  为  $10^{200}$  量级且满足  $n \equiv 1 \pmod 8$  时, 求解二次剩余是难题, 协议 3 是基于二次剩余的, 该协议的安全性依赖于大整数分解这个困难性问题<sup>[13]</sup>。

协议 3 是多方参与确定硬币的结果, 参与者通过对猜测值进行异或运算得出硬币结果, 这个结果是一个随机数, 参与者不确定随机数是 0 还是 1, 也没必要故意看别人的猜测值, 所以该方案在对猜测值进行加密并传递的过程是安全的。  $P_1$  用私钥解密并把结果和私钥公布, 在这个环节, 其他参与者如果不相信  $P_1$  公布的结果, 可以用私钥验证。

综上所述, 协议 3 的整个过程都是安全的。

3.2 复杂度分析

计算复杂度: 协议 2 需要 Bob 计算  $r^2 \equiv a \pmod n$ , 进行一次模  $n$  运算得到  $a$ , Alice 通过两次勒让德符号验证  $a$  是模  $n$  的二次剩余, 再做一次模  $n$  运算, Bob 最终验证结果需要做一次  $r^2 \equiv a \pmod n$  运算, 所以协议 2 的计算复杂度是  $O(3)$ 。协议 3 每人平均对自己的猜测

结果用 Goldwasser 加密算法<sup>[14]</sup>加密一次,然后除  $P_1$  外都要做一次乘法运算,  $P_n$  把运算结果发送给  $P_1$ ,并判断一次勒让德符号,得出一个异或结果  $m_0$ ,并将  $m_0$  公布给其他参与者,协议 3 的计算复杂度是  $O(2)$ ,协议 3 比协议 2 的计算复杂度低。

通信复杂度:衡量通信复杂度的指标是协议交换信息的比特数或者通信轮数,在多方保密计算研究中通常用轮数。协议 2 中 Alice 和 Bob 的通信轮数为 5,协议 3 中  $n$  个人的通信轮数为  $n+1$ ,但是协议 3 是多方抛掷硬币,通信复杂度必然会高,总体来说协议 3 比协议 2 通信复杂性低。

## 4 结束语

公平抛掷硬币协议是一种模拟抛掷硬币协议,一般采用单向函数的抛掷协议和公开密钥密码学的协议,但是这些协议均仅限于两方,对多方没有普遍适用性。文中研究了多方抛掷硬币的多方保密计算,提出了一种新的解决方案。该方案运用了 Goldwasser 概率加密因子分解的困难假设和异或同态性,并对其进行了安全性分析和复杂性分析,满足多方保密的安全性需求。

## 参考文献:

- [1] Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness[J]. MIS Quarterly, 2010, 34(3): 523-548.
- [2] Siponen M, Mahmood M A, Pahlila S. Employees' adherence to information security policies: an exploratory field study[J]. Information & Management, 2014, 51(2): 217-224.
- [3] cation protocol [C]//Proc of the IEEE international conference on RFID. Las Vegas: IEEE, 2008: 97-104.
- [9] Deursen T, Radomirovic S. Untraceable RFID protocols are not trivially composable: attacks on the envision of EC-RAC[R]. Luxembourg: University of Luxembourg, 2009.
- [10] Lee Y, Batina L, Verbaauwhede I. Privacy challenges in RFID systems [C]//Proc of the internet of things 2010. Berlin: Springer, 2010: 397-407.
- [11] Lv C, Li H, Ma J, et al. Vulnerability analysis of elliptic curve cryptography-based RFID authentication protocols[J]. Transactions on Emerging Telecommunications Technologies, 2012, 23(7): 618-624.
- [12] Liao Y P, Hsiao C M. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol[J]. Ad Hoc Networks, 2014, 18(7): 133-146.

- [3] Du W, Atallah M J. Secure multi-party computation problems and their applications: a review and open problems [C]//Raskin V, Greenwald S J, Timmerman B, et al. Proceedings of new security paradigms workshop 2001. New York: ACM Press, 2001: 13-22.
- [4] Blum M. Coin flipping by telephone: a protocol for solving impossible problems [C]//Proceedings of the 24th IEEE computer conference. [s. l.]: IEEE, 1982: 133-137.
- [5] Ben-Or M, Linial N. Collective coin flipping [M]//Randomness and computation. New York: Academic Press, 1990: 91-115.
- [6] Lindell Y. Parallel coin-tossing and constant-round secure two-party computation [J]. Journal of Cryptology, 2003, 16(3): 143-184.
- [7] 余 堃, 沈 仟, 周明天. 背包问题在硬币抛掷协议上的研究[J]. 电子科技大学学报, 2003, 32(4): 417-419.
- [8] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE [J]. SIAM Journal on Computing, 2014, 43(2): 831-871.
- [9] 陈恭亮. 信息安全数学基础 [M]. 北京: 清华大学出版社, 2004: 82-83.
- [10] Koblitz N. A course in number theory and cryptography [M]. [s. l.]: Springer Science and Business Media, 1994.
- [11] Goldwasser S, Micali S. Probabilistic encryption [J]. Journal of Computer and System Sciences, 1984, 28(2): 270-299.
- [12] Schneier B, 吴世忠, 祝世雄, 等. 应用密码学: 协议、算法与 C 源程序 [M]. 北京: 机械工业出版社, 2000: 387-388.
- [13] 李子臣, 戴一奇. 二次剩余密码体制的安全性分析 [J]. 清华大学学报: 自然科学版, 2001, 41(7): 80-82.
- [14] Goldwasser S. Multi party computations: past and present [C]//Proceedings of the sixteenth annual ACM symposium on principles of distributed computing. [s. l.]: ACM, 1997: 1-6.
- [13] Zhao Z. A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem [J]. Journal of Medical Systems, 2014, 38(5): 1-7.
- [14] He D B, Kumar N, Chilamkurti N, et al. Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol [J]. Journal of Medical Systems, 2014, 38(10): 1-6.
- [15] 李荣荣, 寇建涛, 董 刚, 等. 面向智慧园区的 RFID 系统信息安全认证方案 [J]. 电信科学, 2016, 32(2): 164-169.
- [16] Godor G, Giczi N, Imre S. Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems—performance analysis by simulations [C]//Proc of the IEEE international conference on wireless communications, networking and information security. Beijing: IEEE, 2010: 650-657.