基于雅克比符号的公平硬币抛掷方案

高丽丽,王红愿
(陕西师范大学 计算机科学学院,陕西 西安 710062)

摘 要:在现实生活中,往往碰到许多难以抉择的问题,这时,往往倾向于用抛硬币的方式解决。比如足球比赛,比赛开始前,两方足球队的队长各选一面来决定各自的半场。然后裁判抛掷硬币,如果硬币正面,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。文中基于雅克比符号的运算性质以及因子分解的困难性,给出了一种安全高效的公平硬币抛掷问题的解决方案。与已有方案相比,该方案计算简单,且克服了单向散列函数难构造的问题。

关键词:公平硬币抛掷;雅克比符号;安全通信
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2013)01-0131-04
doi:10.3969/j.issn.1673-629X.2013.01.33

Fair Coin Tossing Scheme Based on Jacobi Symbol

GAO Li-li, WANG Hong-yuan
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: In real life, tend to encounter many difficult choices, by this time, tend to solve by coin toss. Such as the football match, before the match, the captain of two sides of the football team chooses one side to decide their half-court, then judge the toss of a coin, if a coin is positive, then party a from left to right attack; conversely, party b from left to right attack. 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, which is a research remains to be the problem. Based on operational properties and the difficulty of factorization for Jacobi symbols, give the solution to the problem of a safe and effective and fair coin tossing. Compared with the existing program, the program is simple, and to overcome the problem of a one-way hash function is difficult to construct.

Key words: fair coin toss; Jacobi symbol; secure communication

0 引 言

二十一世纪是信息化世纪,随着信息技术的发展,通信变得简单、便捷,但在便利的同时,也增添了不少麻烦。比如说,通信过程中,信息被截取,以致泄露隐私等等。为了在享受便利信息的同时,保护隐私,最大限度的减少或避免因信息泄密、破坏安全问题所造成的损失及影响,是目前急需解决的一项具有重大意义的课题,这时,就需对通信的方法进行研究。在这篇文章中,将以一个简单的消息传递例子——硬币抛掷问题,来设计一种可行的、有效的安全通信方法。

在现实生活中,常常因为一件小事而争执不休,这时候,往往用抛硬币的方式解决,认为这种方式是公平的。因为能够同时看到抛掷硬币的结果,并且公认抛掷硬币的结果是随机出现的。下面,来考虑这样一个场景:两个人在电话中为一件小事争执不休,他们最后决定通过抛掷硬币的方式来解决问题。在这个场景中,争执不休的两个人不在同一个地方,他们不能亲眼见证抛掷结果,不得不通过相互通信来得知抛掷结果。那么,问题就有可能出现了,在通信过程中,其中一方就很可能出现欺骗行为。比如,抛掷硬币方会对他的抛掷硬币的结果进行欺骗,告诉对方对其有利的结果;或者,可以安装一个摄像头,把抛掷硬币的过程给录下来,然而,这时抛掷硬币方可以抛掷多次,然后把对其有利的那段录像发送给另一方。为了避免抛掷硬币过程中出现欺骗,实现传输过程中的安全性,就提出了这样一个问题:怎样才能实现公平地抛掷硬币? 这就是这篇文章中需要解决的问题。

收稿日期:2012-04-29;**修回日期**:2012-08-03
基金项目:国家自然科学基金资助项目(61070189)
作者简介:高丽丽(1988-),女,硕士,研究方向为密码学与信息安全;导师:李顺东,教授,研究方向为密码学与信息安全。

1 预备知识及问题的引入

1.1 雅克比符号

雅克比符号(Jacobi Symbol),写作 $J(a,n)$,是勒

让德符号的合数模的一般化表示,它定义在任意整数 a 和奇整数 n 上。这个函数首先出现在素数测试中。雅克比符号是基于 n 的除数的余数化简集上的函数,可按下列方法计算:

定义 1: $J(a,n)$ 只定义在 n 为奇数的情况下。

定义 2: $J(0,n)=0$。

定义 3: 如果 n 是素数,且 n 能整除以 a,那么 $J(a,n)=0$。

定义 4: 如果 n 是素数,且 a 是模 n 的一个二次剩余,那么 $J(a,n)=1$。

定义 5: 如果 n 是素数,且 a 是模 n 的一个非二次剩余,那么 $J(a,n)=-1$。

雅克比符号具有以下性质:

性质 1: 若 a 与 n 不互素,则 $J(a/n)=0$。

性质 2: $J(a/(n1*n2))=J(a/n1)*J(a/n2)$。

性质 3: 若 $\gcd(n1,n2)=1$ 且 $n1$ 或 $n2=1\bmod 4$,则 $J(n1/n2)=J(n2/n1)$;

若 $\gcd(n1,n2)=1$ 且 $n1,n2=3\bmod 4$,则 $J(n1/n2)=-J(n2/n1)$。

1.2 问题的引入

考虑到生活中的实际情况,夏天就要到了,不在同一地方的 Alice 和 Bob 都打算去买一把太阳伞。这时,Carol 说她那多一把,可以给 Alice 和 Bob 中的其中一人。可是,问题出现了,伞只有一把,可是两人都想得到这把伞,该怎么办呢? C 这时给出了一个主意,她要求两人通过电话抛硬币的方式来解决:由 Alice 抛掷硬币,Bob 来猜结果,如果 Bob 猜对了则这把伞属于 Bob,否则属于 Alice。

对于上面提出的问题,最容易想到的方案便是,Alice 抛掷完硬币后,让 Bob 先把猜测的结果告诉她,由她来验证猜测的结果是否正确,并把结果再告诉 Bob。这种方案给了 Alice 很大的权力——Alice 完全可以谎报抛掷结果,而 Bob 也不能看到真正的结果。这种方案如果在通信的双方互不信任的情况下,是不可行的。

对于上述所提到的方案的缺陷,有不少学者对这个问题进行了研究,为了避免上述的漏洞,Alice 提出的问题最好是二选一的问题,两个选项都有可能成为答案,概率各占 50%;而回答这个问题没有任何技巧,只能凭借猜测;而答案也必须是唯一的,并且很容易验证答案的正确性。比如,问题可以设定为某一天的某某报纸头条新闻中的句号的个数是奇数还是偶数,或者新华字典中某一页的第几个字的笔画数是奇数还是偶数等等。可以要求,A 提出这样的问题后,B 必须立即作答。而面对这样的问题,B 没有任何答题技巧可言,只能瞎猜一个。之后两人便可花时间验证答案的正确性。另外,还需要的就是方案不具有可重复性。因此,许多工作者进行了研究[1~4],有了以下思路。

一般来说,抛掷硬币协议需要具有如下的性质:

第一,Alice 必须在 Bob 猜测之前抛掷硬币;

第二,在听到 Bob 的猜测后,Alice 不能再抛掷硬币;

第三,Bob 在猜测之前不能知道硬币怎么落地的。

基于上面的思路,为了能够达到公平地通信,解决硬币抛掷问题,已有不少工作者在这方面做出了卓越成效的工作[5~8]。其中就目前的研究状况来看,以下两种方法可用来实现符号上述所提到的性质的协议:使用单向函数的抛掷硬币协议以及使用公开密钥密码术的抛掷硬币协议。

1.3 相关协议

根据以前的研究,主要有以下两种协议[9,10]:

方案 0:使用单向函数的抛掷硬币协议。

如果 Alice 和 Bob 能找到一个信任的单向函数,则可达成以下协议:

(1) Alice 选择一个随机数 x,她计算 $y=f(x)$,这里 $f(x)$ 是单向函数;

(2) Alice 将 y 发送给 Bob;

(3) Bob 对 x 的奇偶性进行猜测,并将猜测结果发送给 Alice;

(4) 如果 Bob 的猜测正确,则抛掷硬币结果为正面;否则,为反面。Alice 公布结果,并将 x 发送给 Bob;

(5) Bob 通过计算 $f(x)$ 进行验证。

在该协议中,安全性主要取决于单向函数。例如,如果 Alice 能够找到 x 和 x',满足 x 为偶数而 x' 为奇数,且 $y=f(x)=f(x')$,那么 Alice 每次都能够欺骗 Bob。然而,满足条件的单向函数并不容易找到,这就是该协议中需要解决的非常重要的难题。

方案 1:使用公开密钥密码术的抛掷硬币协议。

在该方案中,Alice 和 Bob 达成如下协议:

(1) Alice 和 Bob 都产生一个公开密钥/私人密钥对;

(2) Alice 产生两个消息,其一表示正面,另一个表示反面。这些消息中包含有某个唯一的随机串,以便以后能够验证其在协议中的真实性。Alice 用她的公开密钥分别将两个消息进行加密,并以随机的顺序把它们发送给 Bob;

(3) Bob 由于不能读懂其中任意一消息,他随机地选择一个。他用他的公开密钥加密并回送给 Alice;

(4) Alice 由于不能读懂送回给她的消息,就用她的私人密钥解密并会送给 Bob;

(5) Bob 用他的私人密钥解密消息,得到抛掷硬币结果。他将解密后的消息送给 Alice;

(6) Alice 读抛掷硬币结果,并验证随机串的正确性;

(7) Alice 和 Bob 出示他们的密钥对以便双方能验证对方没有欺诈。

这个协议是自我实施的。任意一方都能即时检测对方的欺诈,不需要可信的第三方介入实际的协议和协议完成后的任何仲裁。下面看看协议是如何工作的:

如果 Alice 想欺骗,强制为正面,她有三种可能的方法影响结果。首先,她可以在第(2)步中加密两个"正面"消息。然而,对于这种欺骗方法,Bob 可以在第(7)步,Alice 出示她的密钥时,发现 Alice 进行了欺骗;其次,Alice 在第(4)步时用一些其他的密钥解密消息,将产生的一些乱七八糟的无用的消息。对于这种欺骗方法,Bob 可以在第(5)步中发现;最后,Alice 可在第(6)步中否认消息的有效性。然而,当在第(7)步,Alice 不能证明消息无效时,Bob 就可以发现 Alice 已经进行了欺骗了。

如果 Bob 想欺骗并强制为"反面",他的选择性不大。他可以在第(3)步中不正确地加密一个消息,但 Alice 在第(6)步查看最终的消息时就可以发现它;他可以在第(5)步中进行不适当的操作,但这也会导致乱七八糟的无用的消息,Alice 可在第(6)步中发现;他可以声称由于 Alice 那方面的欺诈使他不能适当地完成第(5)步的操作,但这种形式的欺诈能在第(7)步中发现;最后,他可能在第(5)步中给 Alice 一个"反面"的消息,而不管他解密获得的消息是什么,但 Alice 能在第(6)步中立即检查消息的真实性。

根据以上的分析,该协议即安全又有效,但它需要算法满足交换律,即:DK1EK2EK1M = EK2(M)。

一般来说,对于对称算法这个特性并不满足,故该协议具有一定的局限性。

2　抛掷方案

基于上一部分所提到的方案的缺点,在这里研究了一种新的抛掷方案——使用雅克比符号进行设置。已知 Alice 进行抛掷硬币,Bob 进行猜测,设置方案如下:

(1) Alice 首先选两个大素数 p 和 q,其中 $p \equiv 1 \bmod 4$,$q \equiv 3 \bmod 4$。计算 $n = pq$ 的值;然后再选一个与 p 及 q 均不相同的大素数 a,并计算雅克比符号 $J(a/n)$;

(2) 将 $J(a/n)$ 的值及 n 值发送给 Bob;

(3) Bob 对 a 的值进行猜测:猜测 $a \equiv 1 \bmod 4$ 还是 $a \equiv 3 \bmod 4$;

(4) 若 Bob 猜测正确,则抛掷硬币结果为正面;若 Bob 猜测错误,则抛掷硬币结果为反面。Alice 公布结果,并将 a 发送给 Bob;

(5) Bob 进行验证。

在这个方案中,Alice 提出的问题是二选一的问题:$a \equiv 1 \bmod 4$ 还是 $a \equiv 3 \bmod 4$。并且,两个选项都有可能成为答案,概率各占 1/2;而 Bob 在回答时,没有任何技巧,只能凭借猜测。另外,该方案具有可重复性。

3　方案分析

3.1　安全性分析

在抛掷硬币的过程中,Alice 和 Bob 都可能进行欺骗,下面就这两种情况分别进行分析。

情况一:Alice 进行欺骗。

Alice 如果想要进行欺骗,在第(4)步中,对这两个不同情况下的 a 值,她需得到相同的雅克比符号值。而这是不可能的,下面进行证明:

因为

$p \equiv 1 \bmod 4$,$q \equiv 3 \bmod 4$,$n = pq$

显然

$n \equiv 3 \bmod 4$

又因为 a 与 p 和 q 均不相同,且 p,q 及 a 均为素数,故 $\gcd(a,n) = 1$。由雅克比符号的性质 3 以及 $n \equiv 3 \bmod 4$ 可知,$J(a/n)$ 的值取决于 a 的情况,对于 a 值情况的不同,所得到的结果也不同。

综上所述,Alice 不可进行欺骗。

情况二:Bob 进行欺骗。

若 Bob 想进行欺骗,那他就不得不试图得知 a 的情况。由于 a 总共就有两种情况,正好与硬币抛掷的两种结果相对应,所以相对于 Bob 来说,他就不得不对 a 值的情况进行猜测,且猜对的概率为 1/2,符合现实中对硬币抛掷情况的猜测概率。

3.2　计算方法分析

对于雅克比符号的计算,采用迭代公式:

$Ja,n = J(a \bmod n, n)$

进行计算。该算法运用迭代,计算比较简便。

4　结束语

抛掷硬币是日常生活中屡见不鲜的一个实验。实验的结果不是正面就是反面。而且出现正面和反面的概率都是随机并且相等的,因此生活中经常以抛掷硬币的方式来解决一个问题。而在网络中,就可以以一枚虚拟的硬币来进行硬币协议。公平抛掷硬币协议是一种模拟抛掷硬币的协议,可以采用单向函数、使用公开密钥密码术的抛掷硬币协议来实现公平抛掷硬币协议。然而,上述方法都有一定的局限性,所以文中提出了一种新的方法来实现抛掷硬币协议。

密码协议是信息和通讯安全技术的重要内容,而密码的应用已经从军事、政府和外交迅速扩展到了工业、商业和金融等领域,而对于密码协议的研究也越来越重要。而在文中,提出了一种抛掷硬币协议,这种协议比较简单便捷地解决硬币抛掷问题的方法——基于雅克比符号的硬币抛掷问题的解决方法,这种方法能够使得不相互信任的双方通过抛掷硬币的方式,对于争执的问题达成共识。硬币抛掷问题的解决有着很大的意义[11,12],比如,通过硬币抛掷协议,可以使得 Alice 和 Bob 产生随机会话密钥,以便双方都不能影响密钥产生的结果,从而完成 Alice 和 Bob 在网络上交换邮件消息或其他通信。

参考文献:

[1] Ambainis A, Buhrman H, Dodis Y, et al. Multiparty quantum coin flipping[C]//Proceeding of the 19th Annual IEEE Conference on Computational Complexity. [s. l.]:[s. n.],2004:250-259.

[2] Saks M. A robust noncryptographic protocol for collective coin flipping[J]. SIAM Journal on Discrete Mathematics, 1989, 2(2):240-244.

[3] Ben O M, Linial N. Collective coin flapping[J]. Advances in Computing Research: Randomness and Computation, 1989(5):91-115.

[4] Alon N, Naor M. Coin-flipping games immune against linear-sized coalitions[J]. SIAM Journal on Computing, 1993, 22(2):403-417.

[5] 吴晓平. 信息安全数学基础[M]. 北京:国防工业出版社,2009:66-69.

[6] Ambainis A. A new protocol and lower bounds for quantum coin flipping[J]. Journal of Computer System Sciences, 2004, 68(2):398-416.

[7] Gordon S D, Hazay C, Katz J, et al. Complete fairness in secure two-party computation[C]//Proceedings of the 40th Annual ACM Symposium on Theory of Computing. [s. l.]:[s. n.],2008:413-422.

[8] Lindell Y. Parallel coin-tossing and constant-round secure two-party computation[J]. Journal of Cryptology, 2003, 16(3):143-184.

[9] Scheneier B. 应用密码学-协议、算法与 C 源程序[M]. 吴世忠,祝世雄,张文郑,等译. 北京:机械工业出版社,2010:62-65.

[10] 李顺东. 现代密码学:理论、方法与研究前沿[M]. 北京:科学出版社,2008:143-144.

[11] 付潇潇,王世民. 基于 RSA 加密算法的扑克游戏[J]. 北京工商大学学报(自然科学版),2007(5):60-63.

[12] 佘 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.

(上接第 130 页)

理、垃圾邮件过滤等领域有着广泛的应用,是解决网络信息过载的有效途径之一。运用语义的知识来进行文本分类是目前国内外学者研究的热点。文中提出了一种基于语义距离的文本分类方法,首先利用 CHI 特征选择方法进行文本特征选择,然后利用词语之间的距离计算代表类别的特征向量集合,最后通过计算文本特征向量和类别特征向量之间的语义距离来确定文本类别[13,14]。实验结果取得了较高的准确率,但该方法受词语相似度计算结果的影响,如果能进一步提高词语之间的相似度计算的准确率,将得到更好的结果。

参考文献:

[1] Zhang W, Taketoshi Y, Tang X J. Text Classification Based on Multi-word with Support Vector Machine[J]. Knowledge-based Systems, 2008, 21(8):879-886.

[2] Chen Y T, Chen M C. Using Chi-square Statistics to Measure Similarities for Text Categorization[J]. Expert Systems with Applications, 2011, 38(40):3085-3090.

[3] Wang Jun, Zhou Yiming. A Novel Text Representation Model for Text Classification[C]//First International Conference on Intelligent Networks and Intelligent Systems. [s. l.]:[s. n.], 2008:702-705.

[4] 杨金柱,刘金岭. 基于词语上下文的文本分类研究[J]. 计算机技术与发展,2011,21(8):145-148.

[5] 鲁 婷,王 浩,姚洪亮. 一种基于中心文档的 KNN 中文文本分类算法[J]. 计算机工程与应用,2011,47(2):127-130.

[6] 张 苗,张德贤. 多类支持向量机文本分类方法[J]. 计算机技术与发展,2008,18(3):139-141.

[7] 姜 鹤,陈丽亚. SVM 文本分类中一种新的特征提取方法[J]. 计算机技术与发展,2010,20(3):17-19.

[8] 林 伟,孟凡荣,王志晓. 基于概念特征的语义文本分类[J]. 计算机工程与应用,2011,47(28):139-142.

[9] 刘 群,李素建. 基于知网的词汇语义相似度计算[C]//第三届汉语词汇语义学研讨会. 台北:出版者不详,2002.

[10] 董振东. 知网[DB/OL]. 2012. http://www. keenage. com.

[11] Wu Zhibiao, Martha P. Verb Semantics and Lexical Selection[C]//Proceedings of the 32nd Annual Meeting of the Association for Computational Linguistics. New Mexico: Association for Computational Linguistics, 1994:133-138.

[12] 胡 涛,刘怀亮. 中文文本分类中一种基于语义的特征降维方法[J]. 现代情报,2011,31(11):46-50.

[13] 张培颖. 基于句子特征和语义距离的文本摘要技术[J]. 微计算机应用,2009(7):84-89.

[14] 宋 玲,马 军,连 莉. 文档相似度综合计算研究[J]. 计算机工程与应用,2006,42(30):160-163.

基于雅克比符号的公平硬币抛掷方案

作者： 高丽丽， 王红愿
作者单位： 陕西师范大学 计算机科学学院,陕西 西安 710062
刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2013(1)