非交互式零知识及其应用*

Manuel Blum等

【摘要】本文提出：任何零知识证明中的交互作用都可以通过共享一个公用的短随机串来代替。我们用这一结果构造了能防止选择性密文攻击的一流的公开密钥密码体制。

一、引 言

最近，S.Goldwasser，S.Micali和G.Rackoff三人(简称GMR)证明了在没有就某问题给出最少提示的情况下，也有可能证明某些定理是正确的。这是根据零知识证明系统中多少存在的悖论概念被严格形式化的。

尽管存在着保密加密方案，但这些证明系统还远不能成为一种罕见的、异乎寻常的事件。事实上，根据这种假设，〔GMW〕证明了NP中的任何一种语言都拥有零知识证明系统。实际上，正如Ben—Or，Goldreich，Goldwasser，Hastad，Micali和Rogaway〔BGGHMR〕近来所证明的那样，对IP中的所有语言来说，情况也是如此。此外，正如Blum〔B_2〕所指出的那样，任何定理都承认传递零知识的证明，而不是暴露自己的长度。

业已证明，零知识证明对复杂性理论和密码学都非常有用。例如，在复杂性理论方面，通过Fortnow〔F〕和Boppana、Hastad〔BH〕的研究结果可以看出，零知识能给我们提供一种方法，使我们相信某些语言不是NP完全的。在密码学方面，零知识证明在最近证明的、具有诚实多数的协议的完备性定理方面发挥了重要的作用〔GMW2〕。零知识证明还产生出经严格分析的识别方案〔S〕，其效果与传说的识别方案一样。

尽管零知识有着广泛的适用性，但它仍然是一种使人感到好奇的概念：

使零知识证明起作用的是什么？

以下三个主要特性能把所有已知的零知识证明系统与更传统的系统区别开：

1)“交互作用”：证明者和检验者能相互对话。

2)“隐藏随机化”：检验者投掷的硬币是证明者所不知道的。因此，证明者要对检验者投掷的硬币进行预测是不可能的。

3)“计算上的困难性”：证明者在某证明中设置了其它某一问题的计算上的困难性。

乍一看，所有这三条似乎都是必不可少的。本文在提取零知识证明的精华方面迈出

*资料来源："Non Interactive Zero—knowldge and Its Application"Submitted to 1988 STOC (宋云生译 朱甫臣校).

了重要的第一步。我们证明，只存在计算上的困难性(例如区分2素数积与3素数积 的难度)可使上述第一个特性(交互作用)无关紧要。并可消除第二个特性(随机性) 的保密度。这就是说，如果证明者和检验者共享一个公用随机串，证明者就能以非交互的、然而却是零知识的方式使检验者相信他所发现的任何一种定理的有效性。更确切地说，对任何常数c和d来说，共享一个k比特长的随机串使证明者P能以零知识方式向一个多(k)一时间检验者非交互式地证明k^d大小的任意k^c个定理；即不从V那里读出任何报文。

我们把P和V当成两个学数学的学生。P在玩了一会“头尾游戏”之后，便到世界各地旅行去了。在旅行期间，P继续进行他的数学研究。每发现一个定理，他就给V寄一张明信片，以零知识方式证明他所发现的新定理的正确性。注意，这是一个必不可少的非交互作用过程；具体地说，这只是从P到V的单向交互作用。事实上即使V愿意给P回信或与P通话，他也不能做到，因为P没有固定的(或可预报的)地址。在V给P的回信到达某地点之前，P也许早已离开了。

1. 我们的模型与老的模型的比较

尽管仍不改变零知识定义，但证明者和检验者的计算方法有了明显的变化。注意：共享一个随机串σ与能够进行交互作用相比，是一个“弱条件”。事实上，如果P和V能够相互配合，那么用通过电话投掷硬币的方法，就能构成一个公用随机串[B]；但反之却是不成立的。

此外还要注意：与前面介绍的第二个特性相比，共享一个公用随机串是一个“缓当得多的条件”。事实上，我们的证明者能看到检验者所有的硬币投掷。注意，我们的条件比双方存取一个随机标志还要弱。在后一种情况下，事实上所进行的所有硬币投掷证明者都能看到。但将要投掷哪些硬币他仍然是无法预测的。相反，我们的模型使证明者能“预先”知道所有的硬币投掷。也就是说，我们证明的零知识性不依赖于σ的保密性或不可预测性，而依赖于其比特“很好地混合”！这一奇妙的特点使我们的结果很可能具有适用性。例如，该国家所有的图书馆都拥有由RAND公司制定的同样的随机表付本。因此，我们可以认为自己已处于设想的情景之中了。

2. 我们的研究结果所具有的强度

正如我们所说的那样，如果随机串σ是一个真正的随机串，那么可以保证，我们证明系统中所证明的所有定理都是正确的，而且是零知识的。我们当然可以提出：如果σ事实上并不真正是随机选择的，那么情况将会怎样？幸运的是，σ的随机性不好会扰乱我们定理的零知识性，而“不影响定理的正确性。”也就是说，对几乎所有随机性不好的σ来说，不存在任何可被检验者接受的错误论点。这确实是一个重要的特性。因为我们从来就不能肯定我们自然随机源的质量。遗憾的是，由于篇幅的限制，我们不能对这个问题和类似的观点作详细地说明。不过，我们想在下面给出此结论的重要推论。

3. 我们结果的应用

非交互式零知识有一个很值得注意的应用，即它能按迪菲和赫尔曼的方式构成能防止选择密文攻击的加密方案。自从出现了以复杂性理论为基础的密码学以来，上述加密方案是否存在一直是一个基本上没有解决的问题。本文将在第三节讨论这方面的应用。

二、我们的解决办法

1. 复杂性假设

我们先叙述一种足以提供非交互式零知识的复杂性假设。为清楚起见，我们不打算选择这种“最小”假设。同样，我们也不把多项式时间内的效率情况考虑在内。

令C_k^2（C_k^3）表示长度为k的2（3）个相异素数所有复合整数乘积的集合，令$B=\{B_k\}$表示组合电路的一个族，其中B_k有2k个布尔输入和一个布尔输出；令$P_k^B(q_k)$表示在输入$C_k^2(C_k^3)$中一个随机选择的复合数时B_k输出“1”的概率。于是我们假设，对所有多项式界限的B，以及所有正常数C和足够大的k来说，有

$$\left| P_k^B - q_k^B \right| < k^{-c} .$$

2. 数论评论

雅可比符号函数$(\frac{x}{n})$是多项式时间可计算的。如果$n\in C_k^2$（$n\in C_k^3$），则Z_n^*中有一个半的元素雅可比符号为1。另一半元素可划分成2（4）个等价类。在这2（4）个等价类中，如果两个元素具有相同的模n的每个素因子的二次特征，我们就将这两个元素定义为等价元素。这等于说它们的积是模n的一个平方。区分这些等价类中的成员关系与确定模复合数的二次剩余性一样困难。这一假设比假设确定二次剩余性是困难的要强些（因此，我们可以在不增加假设集合的情况下，使用以二次剩余性为基础的协议）。

3. 中间解决办法

我们先讨论一种方法，即当输入一个保密参数k时，首先允许P和V进入交互阶段（在此阶段中，P和V能相互通话）。然后，P以非交互方式、以零知识方式向V证明他所需要的那些定理。P通常具有无穷的计算能力，V则是多时间的。同样，不失一般性完全有可能考虑这样一种情况：P想证明的定理是关于图的4可着色性（如果已知对P的输入图输入适当的4种颜色，那么P实际上可以是多项式时间的）。

确切地说，当输入一个保密参数k时，对某个固定的$C>0$来说，P和V在交互阶段执行k^c步。然后，对任何$d、e>0$的常数，若已知大小为k^{-}，$G_1,G_2\cdots\cdots$的任意k^{c-d}个4可着色图，P都可以非交互式地、以零知识方式向V证明。这些G_i是4可着色的。我们强调在交互阶段，P还不知道（还没有作为输入给出）这些G_i。

交互阶段所采用的算法

我们在下面假设P和V都有一个作为输入的一元整数k。

1）P随机地选择一个整数$n\in C_k^3$。

2）P以交互方式向V证明n是三个不同素数的积。

3）P和V决定一个随机选择的k比特串ρ。

由于语言$\{ C_k^3 \mid k\in N \}$属于NP，且所有的NP都有零识识证明，因此第2步是很

容易实行的。用通过电话投掷硬币的方法实现第3步也是很容易的。如果使用基于整数因子分解难度的[B_1]中的协议，我们就不需要介绍任何其它的假设了[1]。

非交互阶段所采用的算法

下面我们假设P和V已完成了具有参数k的交互阶段。于是k、n和p都是p和V的公用输入。Gen是一个密码上很强的伪随机比特发生器[BM][Y]（在不增加假设的情况下，Gen就是[BBS]中提出的那种基于二次剩余性的伪随机比特发生器。实际上这种发生器是建立在如[ACGS]中所示的因子分解基础之上的）。作为附加的输入，P拥有任意4可着色图集合。G在下面是这些输入图的任意一个。

P的程序

1）给Z_n^*的雅可比符号1元素的等价类编成1到4号。

2）决定G的4种颜色。

3）对G中的任一顶点v，如果v着色为i，那么就在i类中随机地选择一个元素e_v，并用e_v来标记v。

4）将标记的G发给V。

5）对G中的每一个边(u，v)随机地选择$y_{u,v}\in Z_n^*$，使得e_u、e_v、$y_{u,v}$模n是一个平方，然后计算它的随机平方根$x_{u,v}$，并将$y_{u,v}$和$x_{u,v}$发送给V。

6）对每个$y_{u,v}$，在输入p时，输出Gen的下一k^h个比特（h在这里是后面将要确定的一个常数），将这些比特组合成每块为k比特的相邻块，让我来看一下表示雅可比符号为1的Z_n^*中元素的所有块：对表示一个模n平方的每个块，将它的一个随机平方根发送给V；对于与$y_{u,v}$处于同一等价类的每个块，将它与$y_{u,v}$乘积的平方根发送给V。

V的程序

1）检验G的所有标号都是Z_n^*的雅可比符号1元素。

2）对所有(u、v)边，检验$x_{v,u}$是e_u、e_v、$y_{u,v}$模n的一个平方根。

3）对每一个y_u，检验已接收到正确平方根的块，是否多于其相连块的$\frac{k^h}{5}$，以及是否多于其它块"乘"$y_{u,v}$的$\frac{k^h}{5}$。

4）如果所有检验均通过，则"承认"G是4可着色的。

首先要注意，这种通信方式是单向的，即从P到V。第二，V的所有计算都可以在概率多项式时间内完成。第三，如果G是4可着色的，且P和V按照其程序执行，则V将承认G，其概率实质上为1。因此，为了证明以下所说的是一个证明系统，我们只需要说明：V以优势概率不承认任何不是4可着色的G。首先，由于n已成功地通过了交互阶段，因此以实质上为1的概率证明，n是三个不同素数的积。其次，以实质上等于1的概率证明，与每个$y_{u,v}$有关的块序列在4个等价类的每个等价类中所含的元素均大于$\frac{k^h}{5}$。事实上，模n的雅可比符号1元素的随机序列"访问"每一等价类的概率为$\frac{1}{4}$。由于Gen的种子（seed）与真正的随机种子（seed）是多项式不可辨别的，因此这对从

Gen的输出中提取的块来说，实际上也是成立的(难以捉摸的一点是：即使在我们的应用中Gen的种子ρ是不保密的，情况也是如此。事实上，如果随机种子始终是保密的，那么所有的有效检验统计特性都适用于Gen的输出；如果随机种子是公开的，则我们感兴趣的特殊的统计特性就不可能“消失”！)。如果$\frac{k^h}{5}$块“乘”$y_{u,v}$有模n平方根，那么它们都属于与y_u相同的等价类。事实上很容易看到，当且仅当Z_n^*中两个元素的乘积是一个平方时，这两个元素属于同一类。此外，如果其它的$\frac{k^h}{5}$个元素本身就有模n平方根，那么以实质上为1概率证明，$y_{u,v}$是一个模n非平方（否则$\frac{2\cdot k^h}{5}$块便是模n平方，而不是所希望的$\frac{k^h}{4}$块)。最后，如果$y_{u,v}$是一个模n非平方，则边（n、v）的着色是恰当的；也就是说，e_u和e_v属于不同的类。事实上，由于e_u、e_v、$y_{u,v}$有一个平方根，因此（e_u、e_v）属于与y_u相同的类；如果e_u和e_v属于相同的类，则它们的乘积就是一个平方，$y_{u,v}$也是如此。每条边都恰当地着了色，G也是这样。

现在我们必须证明上述证明系统是零知识的。也就是说，存在着一种有效的模拟器。在已知4可着色图的任一序列(但不是它们的颜色！)和任何(也许是骗取的)概率多项式时间检验者V'的情况下，这种模拟器能产生一种概率分布，这种概率分布与V'同P通话时将“看到的”概率分布是计算上不可辨别的。V'所看到的是交互阶段的硬币投掷序列(非交互阶段的硬币投掷是不值得模拟的)，以及交互阶段和非交互阶段来自P的信息。零知识证明是一个非常棘手的问题。我们只对高级阶段进行了概述，没有涉及更详细的内容。尽管我们在本文中指出了该证明的哪些部分是容易的，哪些部分是困难的。

检验者从P处接收的第一个信息便是C_k^3的一个随机成员。模拟器则随机地产生两个素数，并将两素数相乘，以产生C_k^2的一个随机成员。至此，在已知我们假设的情况下，这样做就能愚弄任一多项式界限的裁判了。然而，与P交互时，检验者也可以产生一个与C_k^3中的成员证明有关的（消息、硬币投掷）对。而模拟器则在输入$n\in C_k^2$时产生一个（消息、硬币投掷）对，它看上去就象是$n\in C_k^3$的“证明”（虽然在交互证明系统中，任何人都不能向检验者证明一个假定理。但模拟器的这种能力比乍看上去的要好一些。事实上，证明系统只能保证你在参与证明时不被欺骗！完全不同的是，裁判员不参与证明，但却由其它人(要么是P，要么是V，或者是模拟器)向他传递（消息——硬币投掷）对。这种解释也许不能使上述观点变得很直观，但却有希望更令人相信。总之这个观点是很微妙的。另外，从旁观者的角度来看，产生不能与真证明相区分的假证明的能力，不是由现有的特殊代数问题所造成的。正如我们将在终稿文章中所证明的那样，它适用于任何一条定理，且适用于使用任何一种加密方案！）。其次，模拟器产生检验者将在硬币投掷协议中所看到的随机数（这一步并不难）。这一步一旦实现，模拟

器就处于工作状态。事实上，在非交互部分，模拟器将用模n（$\in C_k^2$）平方来标记任何图G的所有顶点。也就是说，对每个顶点u_i，他都联系一个随机选择的平方e_u（任何一个有效的裁判都不能否决这种标记，因为我们在假设中所应用的二次剩余性的难度是很大的）。于是，对每一边（u、v），他都联系一个随机选择的平方y_u。此时，模拟器可根据其随机种子，正确地运行Gen，以获得一个伪随机k^h长的块序列。由于n是两个素数的乘积，因此这些块中大约有一半雅可比符号为1的元素是模n平方的。对随机选择的那一半来说，模拟器将求一个平方根。求平方根是很容易的，因为他是以因子分解的方式选择n的。对剩余一半的每个块，他求其和$y_{u,v}$的乘积的平方根。这样做可以再次愚弄裁判员，因为他不能有效地确定二次剩余性。

注意：对一单个定理的证明（C_k^3 中的成员关系）进行伪造使我们能对其它任何数量的定理的证明进行伪造。这就是选择区分两个素数乘积与三个素数乘积的计算困难性的原因之一。

4.从中间解决办法到理想的解决办法

通过对共享一个随机串使P能以零知识方式非交互方式地向V证明C_k^3中的成员关系进行证明，我们得到一个理想的解决办法（这要注意交互阶段的第一步和第二步。第三步自然也要注意。比如说取共享串的一半）。这是选择复杂性假设的第二个理由（直到现在，我们还不知道怎样用共享随机串来证明识别语言的成员关系。）非交互式地以零知识方式证明C_k^3中的成员关系是不清楚的（证明C_k^2中的成员关系是很容易的。所以，只要证明在将共享串分块后，其中有$\frac{1}{k}$的块是模n平方就足够了）。这一非交互式零知识证明将在终稿文章中给出。现在让我们来讨论上述结论的一个重要推论。

三、一个长期以来未解决的问题现在解决了

公开密钥密码体制概念是以复杂性理论为基础的密码学中最好的体制之一。正如迪菲和赫尔曼［DH］所提出的那样，每个用户U将一串P_v公开，而将相联系的S_v串保密起来。另一个用户为了秘密地将消息m发给V，必须先计算$y=E(P_v, m)$，然后发送y；用户V一收到y，就计算$D(S_v, y)$，以还原m；这里E和D都是所选择的多项式时间算法，以使得对其它任何用户来说，要根据y计算m将是不可行的。

注意：在这一方案中，其它任何用户都可以被看成是“被动的”敌手，他试图仅仅根据对输入y和P_v进行计算还原m。这种敌手的攻击实际上是一种普通的攻击。文献中还介绍了其它几种类型的攻击。人们普遍认为：“选择密文攻击”是所有普通攻击中最强的一种攻击。在这种攻击中，敌手试图通过询问和接收他所选择的密文脱密来破译密码体制。里夫斯特已证明，拉宾的密码方案（对一个被动敌手来说，如果消息是均匀选择的给定长度的字符串，那么该方案的破译正如因子分解一样困难。）很容易遭受这种攻击。确实，这种攻击对在大银行从事脱密工作的所有雇员来说，也是可行的。拉宾(R)方案是一种精心设计的方案，其保密性相当于被动的敌手对因子进行分解。但这种方案

却经不起选择密文的攻击。因此，用拉宾方案便能很好地举例说明这种攻击的能力。由于人们已注意到这一现象，因此试图设计一些不易遭受这种攻击的密码体制，但这些努力均未获得成功。文献［GMT］提出了一种积极的解决办法，即在加密过程中，只允许合法的收方和发方交互作用。然而自1978年以来，对标准的迪菲—赫尔曼模式来说，不易遭受选择密文攻击的密码体制的存在仍然是一个未解决的问题。

非交互式零知识证明使我们能最终解决上述问题。现将我们的解决办法的实质（而不是详细内容）作以下非形式地描述。

需要给用户v发送y和σ两个串，而不是消息m的加密y。这里，σ是关于y的脱密知识的零知识和非交互式证明。“脱密设备”（读脱密函数）检验σ是否使人信服y的脱密。如果使人信服，便输出m，否则便什么也不输出。注意，此时能使用脱密设备可证明是有利的。事实上，我们只有在向脱密设备提供密文（我们能证明我们知道这些密文的脱密）时，脱密设备才能输出这些脱密的内容！换句话说，脱密设备只能用来输出我们已知道的东西。有关这一有效应用的详细情况将在终稿文章中讨论。

（对正规的设备和证明需要给予关照。例如，可将脱密设备用作为一种外部信息源，以检验给定串σ是否是“正确的知识证明”因此，应特别注意证明这种外部信息源是不能起帮助作用的。在终稿文章中，我们将主要证明：如果能在不用m作为输入的情况下产生一个合法的（y，σ）对，那么在只输入y和Pu时就很容易脱密所有的消息。）

SCP2：多级保密通信处理器

据《Software World》报道：英国正在对其研制出的多级保密通信处理器（SCP2）进行鉴定，准备在军事部门、政府机构和经过特许的商业部门中推广应用。这种处理器也叫作多级保密可信计算基地（TCB），具有良好的保密性能，能够广泛应用于网际互连。其设计精细，已经到了诸如安全保护、保密前端一类的端口一级。

GEC Computer Limited公司为其编制了专用系统软件，该软件在GEC公司的41系列微型计算机上运行。使用该处理器时，不需要在每一级安全访问机构上都单独设立一台机器，它能够在保证整体安全性的同时，让人们有效地使用连结在同一个网络中的网内资源。SCP2在计算机系统内的不同保密级别上分离数据，同时允许数据按管理安全策略在不同的保密级别之间传送。此外，它还带有允许网际互连的标准通信规约。

据厂家称：这是在美国之外，第一个达到类似于美国国防部的可信（Trusted）计算机鉴定标准B3的微处理器。

有关人士估计，随着对多级保密及其网络实现方面问题研究的深入，GEC Computer Limited公司有可能把加密、灵巧卡验证和先进的存取控制方法结合在一起。

罗昭武　供稿