

安全计算协议

(扩展摘要)

Andrew C. Yao

加州大学伯克利分校，加利福尼亚州 94720

1 引言

两个百万富翁想知道谁更富有；然而，他们不希望无意中发现关于对方财富的任何额外信息。他们如何进行这样的对话？

这是一个普遍问题的特例。假设有 m 个人希望计算函数 $f(x_1, x_2, x_3, \dots, x_m)$ 的值，该函数是 m 个有界范围的整数变量 x_i 的整数值函数。假设最初第 P_i 个人知道 x_i 的值，而不知道其他 x 的值。他们是否可能通过彼此之间的通信来计算 f 的值，而不过度泄露关于各自变量值的任何信息？百万富翁问题对应于 $m = 2$ 且 $f(x_1, x_2) = 1$ 当 $x_1 < x_2$ ，否则为 0 的情况。在本文中，我们将给出这个一般问题的精确表述，并描述三种使用单向函数（即易于计算但难以求逆的函数）来解决它的方法。这些结果可应用于秘密投票、数据库的私人查询、不经意谈判、心理扑克等。我们还将讨论复杂性问题“计算需要交换多少位”，并描述防止参与者作弊的方法。最后，我们研究“什么是单向函数无法完成的”这个问题。

在描述这些结果之前，我们希望通过在下一节首先考虑安全计算的统一视角，来将这项工作置于背景中。

2 安全计算的统一视角

自从1976年首次提出单向函数（Diffie和Hellman [1]）以来，它们已被用于两种类型的应用。第一种涉及消息的加密和传输，以使其对窃听者和破坏者来说不可读和不可篡改[1, 2, 3, 4]。第二种应用包括“心理扑克”（Shamir等人[5]），其中两个玩家通过电话线通信发牌，以及“抛硬币”（Blum [6]），其中两个相互怀疑的方要生成一个无偏比特。我们期望有一个统一的框架，能够关联所有这些应用，并为证明协议安全性开发通用的证明技术。更根本的是，如果我们想要理解单向函数的内在能力和局限性，这样的框架是必不可少的。例如，

如果没有精确的模型，就很难回答诸如“三个相互怀疑的方是否可能交互式地生成一个偏差为 $1/e$ 的比特？”这样的问题。

为了回应这一需求，我们提议采用以下观点。拥有私有变量 i 和 j 的双方 Alice 和 Bob，希望进行通信，使得 Alice 可以评估函数 $f(i, j)$ ，Bob 可以评估函数 $g(i, j)$ 。通信线上可能存在一些窃听者或破坏者。协议的目的将是设计一个供 Alice 和 Bob 遵循的算法，使得某些安全约束（针对破坏者）和隐私约束（Alice 可能不希望透露 i 的确切值）能够得到满足。

在一个极端情况下，当计算部分是微不足道的，例如如果 $f = \text{常数}$ 且 $g(i, j) = i$ ，那么我们得到前面提到的第一种应用，其基本关注点是窃听和破坏。在另一个极端，当可以忽略此类外部威胁，但 f 和 g 的计算是重要的时，我们就得到了本文将要研究的问题。（心理扑克和抛硬币代表了该问题的随机版本，也将被讨论。）请注意，尽管我们在上述描述中使用了 Alice 和 Bob，但所有讨论都可以扩展到 m 方通信的情况。

自然地将这两个特例放在一起讨论是合适的。然而，由于篇幅考虑，我们在此仅报告对应于没有外部破坏者的计算密集型情况的结果。另一种情况的结果将在别处报告。

3 确定性计算

3.1 百万富翁问题的解决方案

在此摘要中，我们将只详细描述我们拥有的三个解决方案中的一个。

为明确起见，假设 Alice 有 i 百万，Bob 有 j 百万，其中 $1 < i, j < 10$ 。我们需要一个协议让他们决定是否 $i < j$ ，并且这也是他们最终（除了自己的值之外）唯一知道的事情。设 M 为所有 N 位非负整数的集合， Q_N 为从 M 到 M 的所有一一对应函数的集合。设 E_a 为 Alice 的公钥，通过从 Q_N 中随机选择一个元素生成。

协议进行如下：

1. Bob 选择一个随机的 N 位整数，并私下计算 $E_a(x)$ 的值；将结果称为 k 。
2. Bob 发送数字 $k - j + 1$ 给 Alice；
3. Alice 私下计算 $y_u = D_a(k - j + u)$ 的值，其中 $u = 1, 2, \dots, 10$ 。
4. Alice 生成一个 $N/2$ 位的随机素数 p ，并计算所有 u 对应的 $z_u = y_u \pmod p$ ；
如果所有 z_u 在模 p 意义下至少相差 2，则停止；否则生成另一个随机素数并重复该过程，直到所有 z_u 至少相差 2；令 p, z_u 表示这组最终的数字；
5. Alice 将素数 p 和以下 10 个数字发送给 Bob： z_1, z_2, \dots, z_i ，接着是
 $z_i + 1, z_{i+1} + 1, \dots, z_{10} + 1$ ；上述数字应在模 p 意义下解释。
6. Bob 查看从 Alice 发送来的第 j 个数字（不计算 p ），如果它等于 $x \pmod p$ ，则判定 $i \geq j$ ，否则判定 $i < j$ 。
7. Bob 将结论告诉 Alice。

该协议显然能使 Alice 和 Bob 正确决定谁更富有。为了证明它满足双方无法获得关于对方财富的更多信息的要求，我们需要定义一个将在第 3.2 节完成的精确模型。这里我们将非正式地论证为什么要求得到满足。

首先，Alice 不会知道关于 Bob 财富 j 的任何信息，除了 Bob 告诉她的最终结果所隐含的对 j 的约束，因为来自 Bob 的唯一其他信息是 Bob 知道对于某个介于 $k - j + 1$ 到 $k - j + 10$ 之间的 s ， $D_a(s)$ 的值。由于函数 E_a 是随机的，所有 10 种可能性都是等可能的。

Bob 知道什么？他知道 y_j （即 x ），因此也知道 z_j 。然而，他没有关于其他 z_u 值的信息，通过查看 Alice 发送给他的数字，他无法判断它们是 z_u 还是 $z_u + 1$ 。

论证尚未完成，因为 Alice 或 Bob 可能试图通过更多计算来推断另一个人的值。例如，Bob 可能尝试随机选择一个数字 t 并检查 $E_a(t) = k - j + 9$ 是否成立；如果成功，那么他就知道 y_9 的值为 t ，并且知道 z_9 的值，这使他能够查明是否 $i \geq 9$ 。如果 $i \geq j$ 是先前结论的结果，这将是 Bob 不应该发现的额外信息。因此，还必须在正式定义中包含，参与者不仅不会因为协议指定的交换而获得信息，而且他们无法在合理的时间内进行计算以获得此信息。在第 3.2 节给出的正式定义中，我们将精确地定义这一点。

人们可能已经注意到，某些方可能在过程中作弊，即偏离商定的协议。例如，Bob 可能在最后一步对 Alice 撒谎，告诉 Alice 错误的结论。是否有一种设计协议的方法，使得成功作弊的机会变得极小，而不泄露 i 和 j 的值？我们将在第 3.3 节表明这是可能的。（请注意，这比 Shamir 等人[5]中心理扑克协议中使用的可验证性要求更强。）

我们还有另外两个基于不同原理的百万富翁问题解决方案。其中第一个假设 Alice 和 Bob 各自拥有一个私有单向函数，这些函数满足交换性，即 $E_a E_b(x) = E_b E_a(x)$ 。另一个解决方案利用了 Goldwasser 和 Micali [2] 发明的概率加密方法。

3.2 一般问题的模型

由于这三个解决方案的安全性基于不同的假设，必须为每个解决方案详细指定精确的模型。在本摘要中，我们将只给出对应于第一个解决方案的模型。

为简单起见，我们将只给出当 f 为 0-1 值且 $m = 2$ (Alice 和 Bob) 时的定义和结果。将结果推广到一般 m 的情况将在第 5 节简要讨论。一般情况的证明涉及额外的技术复杂性，并且存在额外的安全考虑，例如可能的“共谋”，这在 2 人情况下是不存在的。

协议。假设 Alice 有一个公共单向函数 E_a ，其反函数 D_a 只有 Alice 知道；类似地，Bob 有一个公共的 E_b ，和一个私有的反函数 D_b 。假设 E_a 和 E_b 是独立且随机地从 Q_N （所有可能的 N 位整数上的一一对应函数的集合）中抽取的。计算函数 $f(i, j)$ 的协议 A 确切地规定 Alice 和 Bob 应如何进行通信，如下所示。Alice 和 Bob 交替地向对方发送字符串。每次 Bob 完成传输后，Alice 检查她目前拥有的信息，这些信息由一些字符串序列 $\alpha_1, \alpha_2, \dots, \alpha_t$ 以及字符串之间的一些关系（例如 $E_b(\alpha_3) = \alpha_9$, α_8 有奇数个 1）组成；根据迄今为止她和 Bob 之间传输的比特，协议规定她应如何私下计算字符串 $\alpha_{t+1}, \alpha_{t+2}, \dots, \alpha_s$ ，其中每个新字符串 α_u 是较早字符串的函数，或者是形式为 $E_a(y)$ 、 $E_b(y)$ 或 $D_a(y)$ 的函数，其中 y 是已获得的字符串。选择应用哪个函数，或者是否计算 E_b 或 D_a ，通常是概率性的，即她将基于一些抛硬币的结果来决定计算 $E(4)$ ，或者计算 $\alpha_2 + 3\alpha_8$ 。完成此计算后，她将向 Bob 发送一个字符串，同样，该字符串是概率性选择的。现在轮到 Bob 根据协议计算字符串并发送字符串。我们约定有一个特殊符号，其出现意味着协议执行结束。到那时，协议会指示每个参与者私下计算函数值 f 。最后，我们要求，在一个协议中，Bob 和 Alice 对 E 和 D 的总评估次数以 $O(N^k)$ 为界，其中 k 是预先选择的整数。

隐私约束。设 $\epsilon, \delta > 0$ ，且 $f(i, j)$ 是一个 0-1 值函数。假设最初所有 (i, j) 值对都是等可能的。假设 Bob 和 Alice 根据协议忠实地进行计算。最后，Alice 原则上可以从她计算出的函数值 v 和她所拥有的字符串中，计算 j 值的概率分布；称之为 $p_i(j)$ 。如果满足以下条件，则称协议满足 (ϵ, δ) -隐私约束：

1. 对于 $j \in G_i$, $p_i(j) = \frac{1}{|G_i|}(1 + O(\epsilon))$, 否则为 0, 其中 G_i 是满足 $f(i, j) = v$ 的 j 的集合,
2. 如果 Alice 之后尝试执行不超过 $O(N^k)$ 次 E 和 D 的评估的更多计算，那么以至少 $1 - \delta$ 的概率，她仍将得到上述关于 j 的分布，并且
3. 上述要求对 Bob 也同样成立。

定理 1 对于任何 $\epsilon, \delta > 0$ 和任何函数 f , 存在一个计算 f 的协议满足 (ϵ, δ) -隐私约束。

可以考虑初始 (i, j) 分布不均匀的更一般情况。我们在此不深入讨论。在第 4 节中, 这成为概率计算的特例。

3.3 附加要求

(A) 复杂性。 如果 i, j 的范围 n 变大, 之前给出的百万富翁问题解决方案将变得不切实际, 因为传输的比特数与 n 成正比。一个有趣的问题是, 确定任何计算满足 (ϵ, δ) -隐私约束的 f 的协议所需的最小比特数。可以想象, 有些函数在没有隐私要求的情况下很容易计算, 但在额外的隐私约束下变得不可行。幸运的是, 我们可以证明情况并非如此。设 A 为一个协议, 令 $T(A)$ 表示使用 A 时 Alice 和 Bob 之间交换的最大比特数。

定理 2 设 $1 > \epsilon, \delta > 0$, 且 $f(i, j)$ 是一个 0-1 函数。如果 f 可以通过大小为 $C(f)$ 的布尔电路计算, 那么存在一个计算 f 的协议 A , 满足 (ϵ, δ) -隐私约束, 并且:

$$T(A) = O\left(C(f) \log \frac{1}{\epsilon\delta}\right).$$

事实上, 如果 f 可以通过图灵机在时间 S 内计算, 那么协议可以实现, 使得 Alice 和 Bob 都有图灵机算法以 $O(S \log(1/\epsilon\delta))$ 的时间界限执行该协议。

然而, 存在一些函数在隐私约束下需要在 Bob 和 Alice 之间传输指数级的比特数。设 F_n 是 0-1 值函数 $f(i, j)$ 的族, 其中 i 和 j 是 n 位整数。显然, 在没有隐私约束的情况下, 最多传输 n 比特信息就可以计算 f (参见 Yao [7] 的进一步讨论)。

定理 3 设 $\frac{1}{5} > \epsilon, \delta > 0$ 为固定值。设 f 是 F_n 中的一个随机元素, 那么任何计算 f 且满足 (ϵ, δ) -隐私约束的协议 A , 对于所有大的 n , 必须有 $T(A) > 2^{n/2}$ 。

(B) 相互怀疑的参与者。 到目前为止的讨论都假设 Bob 和 Alice 遵守商定协议规定的规则。如果他们中的任何一方可能为了获得额外信息或误导对方得到错误答案而作弊呢? 确实, 使用我们的协议, 如果在事后有一个验证阶段, 要求双方揭示他们所有的私有计算, 任何作弊行为都会被发现。然而, 这将迫使双方透露他们的变量。正如将在后面给出的应用中变得清楚的那样, 这有时可能是一个严重的缺点。以下结果表明, 可以在不要求任何一方透露变量的情况下阻止作弊。

由于协议永远无法禁止 Alice (或 Bob) 表现得好像她有一个不同的变量值 i' , 协议最多能确保这是 Alice (或 Bob) 唯一能做的作弊。

定义 1 考虑协议执行中的一个实例。如果 Alice 的行为与任何 i 值都不一致, 而 Bob 没有检测到, 我们将其视为 Alice 的一次成功作弊。Bob 的成功作弊类似定义。

定理 4 设 $1 > \gamma > 0$ 。在定理 2 的相同假设下, 存在一个计算 f 的协议 A , 使得

1. $T(A) = O\left(C(f) \log \frac{1}{\epsilon\delta\gamma} \log \frac{1}{\gamma}\right)$, 并且
2. 如果一个参与者按照 A 行事, 则另一参与者成功作弊的概率至多为 γ 。

3.4 应用

秘密投票。假设一个由 m 名成员组成的委员会希望决定一项是-否行动。每个成员写一个意见 x_i , 最终行动可以看作是函数 $f(x_1, x_2, x_3, \dots, x_m)$ 。本文获得的结果意味着, 可以在不知道任何其他成员意见的情况下就最终行动 f 达成一致。此外, 该协议使任何人成功作弊的可能性非常小。

不经意谈判。假设 Alice 试图向 Bob 出售一栋房子。原则上, 每人心中都有一个谈判策略。如果我们将 Alice 的所有可能策略编号为 A_1, A_2, \dots, A_t , 将 Bob 的策略编号为 B_1, B_2, \dots, B_u , 那么一旦确定了实际使用的策略 A_i, B_j , 结果 (无交易, 或以 x 美元出售, ...) 就确定了。将结果写为 $f(i, j)$, 那么可以不经意地进行谈判, 即 Alice 不会获得关于 Bob 谈判策略的任何信息, 除了它与结果一致, 反之亦然。

数据库的私人查询。我们已经证明的定理可以扩展到每个人 P_i 计算不同函数 f_i 的情况。特别地, Alice 可能希望计算函数 $f(i, j)$, 而 Bob 希望计算一个平凡函数 $g(i, j) = \text{常数}$, 这意味着 Bob 最终对 i 一无所知。如果我们将 Bob 视为一个状态为 j 的数据库查询系统, 而 Alice 正在询问查询号 i , 那么 Alice 可以在不知道数据库中任何其他数据的情况下获得查询的答案, 而数据库系统不知道 Alice 查询了什么。

4 概率计算

让我们考虑有两个参与方 Bob 和 Alice 的情况 ($m = 2$)。设 V 和 W 为有限集合。从 $V \times W$ 到区间 $[0, 1]$ 的函数 p 称为概率密度, 如果 $p(v, w)$ 对 v 和 w 的和等于 1。令 $P(V, W)$ 为所有此类概率密度的集合。

设 I, J 为有限整数集。令 $F = \{f_{ij} | i \in I, j \in J\} \subseteq P(V, W)$ 为一个概率密度族。最初, Alice 知道 $i \in I$ 的值, Bob 知道 $j \in J$; (i, j) 的值服从某个初始概率密度 $q \in P(I, J)$ 。他们希望在他们之间传递消息, 以便最终 Alice 以概率 $f_{ij}(v, w)$ 获得值 $v \in V$, Bob 获得值 $w \in W$ 。隐私约束是, Alice 可以获得的关于 j 和 w 的信息不超过从她的 i 和 v 值可以推断出的信息 (加上对 Bob 的相应约束)。这个陈述可以根据 q 和 F 精确表述; 我们在此省略其完全一般性, 仅以特例 $q = \text{常数}$ 为例说明。在这个特殊情况下, 根据隐私约束, Alice 可以从她所做的计算推断出的分布 $h(w)$ 应等于

$$\frac{1}{|J|} \sum_{j \in J} \frac{f_{ij}(v, w)}{\sum_{x \in W} f_{ij}(v, x)}$$

例如, 心理扑克将对应于以下情况: $I = J = \{0\}$, q 是常数, $V = W$ 是 $\{1, 2, \dots, 52\}$ 的所有 5 元素子集的集合,

$f_{00}(v, w)$ 在 v 和 w 不相交时为 0, 否则等于常数。

第 3 节的结果可以推广到概率情况。基本上, 当施加隐私约束时, 合理的概率计算仍然是可行的。我们在此不给出细节。

我们的一个有趣推论是, 心理扑克可以用任何通用的公钥系统进行。它与 Shamir 等人的解决方案[5]的不同之处在于, 我们不需要使用的单向函数具有交换性, 并且我们可以使用公钥系统来玩它 (而不是使用私钥)。(已知有一种使用具有公开密钥的特殊单向函数来玩心理扑克的解决方案[2], 但该解决方案依赖于所涉及单向函数的特殊属性。) 此外, 当牌的数量增加时, 本解决方案使用的比特数要少得多。假设我们有一副 n 张牌, Alice 和 Bob 想轮流从牌堆中抽取一张随机牌。所有先前已知的解决方案在 Bob 和 Alice 之间传输 cn 比特的信息, 而我们的方案只需要大约 $c(\log n)^2$ 比特。

5 推广到 m 方情况

当 m 方 A_1, A_2, \dots, A_m 协作计算函数 $f(x_1, x_2, \dots, x_m)$ 时，可能有多方共谋作弊。我们将表明，即使在最严格的约束下，也能满足以下意义：无论有多少参与者可能共谋，任何作弊行为都会被所有诚实方检测和识别（即使有多达 $m - 1$ 个不诚实者试图帮助掩盖）。我们现在使其精确化。

设 V 是函数 $f(x_1, x_2, \dots, x_m)$ 的值域，其中 $x_i \in X_i$ 。对于任何非空 $K \subseteq \{1, 2, \dots, m\}$ ，定义 $H_K = X_{t_1} \times X_{t_2} \times \dots \times X_{t_{|K|}}$ ，其中 $\{t_1, t_2, \dots, t_{|K|}\} = K$ 。令 $K' = \{1, 2, \dots, m\} - K$ ，并类似地定义 $H_{K'}$ 。对于任何 $i \in H_K$ 和 $v \in V$ ，令 $G_i(v) \subseteq H_K$ 为所有 $j \in H_K$ 的集合，使得（唯一的向量） $x = (x_1, x_2, \dots, x_m)$ （其在 $H_{K'}$ 和 H_K 上的投影分别等于 i 和 j ）满足 $f(x) = v$ 。令 $q_{i,v}(j) = 1/|G_i(v)|$ 对于 $j \in G_i(v)$ ，否则为 0。（如果 K' 中的所有参与者 A_r 共谋推断其他参与者的变量值的概率分布，并且除了他们自己的变量值 i 之外，唯一可用的信息是函数 f 的值为 v ，那么 $q_{i,v}(j)$ 就是他们可以推断出的分布。）设 $\epsilon, \delta > 0$ 。如果对于每个非空 K ，即使允许 K 中的参与者私下执行多项式于 $T(A)$ 的计算量，他们以至少 $1 - \delta$ 的概率推断出的关于 j 的分布等于 $q_{i,v}(j)(1 + O(\epsilon))$ ，则称协议 A 满足 (ϵ, δ) -私有约束。 K' 的一次成功作弊（相对于协议 A ）是 A 执行的一个实例，其中至少有一个参与者 A_r ($r \in K'$) 的行为与任何 $x_r \in X_r$ 不一致，且未被 K 中的所有参与者检测到。

定理 5 对于任何 $\epsilon, \delta, \gamma > 0$ ，存在一个计算 f 的协议 A ，它满足 (ϵ, δ) -私有约束，并且具有以下性质：对于任何 $K' \neq \{1, \dots, m\}$ ， K' 成功作弊的概率不能超过 γ 。

上述定理中 $T(A)$ 的值为 $O(|X_1| \cdot |X_2| \cdot \dots \cdot |X_m| \cdot |V|)$ ，这通常是几乎最优的，如下一个定理所示。

定理 6 存在一些函数 f ，对于它们，任何满足定理 5 条件的协议 A 必须有
$$T(A) = \Omega\left((|X_1| \cdot |X_2| \cdot \dots \cdot |X_m|)^{1/4}\right).$$

在特殊情况下，可以设计出运行时间比定理 5 给出的界限更好的协议。例如，奇偶函数 $f(x_1, x_2, \dots, x_m) = x_1 \oplus x_2 \oplus \dots \oplus x_m$ 和计票函数 $f(x_1, x_2, \dots, x_m) = \#$ （其中 x 是布尔变量）都有满足定理 5 的协议，且运行时间是 m 的多项式。

我们上面考虑的安全措施是一种强措施。对于一些目的，不太严格的措施就足够了。（例如，可能只要求没有子集 K' 能够强制计算结果是某个特定值。）在这种不太严格的要求下，有时可以设计出运行时间更好的协议。例如，有一个运行时间为 $O(p(m) \log q)$ 的协议，其中 $p(m)$ 是一个多项式，供 m 方计算函数

$f(x_1, x_2, \dots, x_m) = x_1 + x_2 + \dots + x_m \pmod{q}$ ，其安全标准仅比定理 5 中给出的稍宽松。

6 什么是无法完成的？

存在一些安全约束是任何协议都无法实现的。我们这里只提两个结果。

第一个不可能性结果对本文给出的所有三个模型都有效。假设 m 个人试图生成一个偏差为 α 的比特。对于 $m > 2$ ，很容易看到如何做到。例如 A 生成一个随机无偏比特 α_1 并发送给 B ， B 生成一个随机 α_2 并发送给 C ， C 生成一个随机 α_3 并发送给 A 。现在令 $\alpha = \alpha_1 + \alpha_2 + \alpha_3$ ，我们得到一个无偏的 α ，其性质是，即使其中一个人通过生成有偏比特作弊，它仍然是无偏的。让我们称一个生成偏差为 α 的比特的协议是稳健的，如果即使有人作弊，偏差仍然是正确的。

定理 7 没有一个具有有限 $T(A)$ 的、生成一个超越数偏差 α 的比特的协议 A 可以是稳健的。

第二个结果对第 3.2 节定义的模型有效。假设 Alice 和 Bob 希望交换一对解 x, y , 满足 $E_a(x) = 1$ 和 $E_b(y) = 1$ 。是否存在一个协议, 使得诚实方不会被双重欺骗, 即在没有得到对方秘密的情况下被骗走自己的秘密。

定理 8 设 A 为任何交换秘密的协议。那么 Alice 或 Bob 将能够以至少 $1/2$ 的概率成功双重欺骗。

值得一提的是, 在同一模型中可以进行不同类型的秘密交换。假设 Alice 想知道 $E_b(y) = w$ 的解 y , Bob 想知道 $E_a(x) = u$ 的解 x , 但 Bob 不知道 w 的值, Alice 不知道 u 。设 N 为加密函数 E_a 和 E_b 操作的比特数。

定理 9 设 $\epsilon > 0$ 为固定值。存在一个运行时间为 N 的多项式的协议 A , 用于交换秘密 $D_b(w)$ 和 $D_a(u)$, 并且在该协议下, 任何人成功双重欺骗的概率以 ϵ 为界。

以前曾考虑过不同种类的秘密交换。Blum [6] 表明, 可以用极小的作弊机会交换大合数的因子 (一种特殊类型的秘密)。Even (私人通信, 1981) 也设计了一些用于交换秘密的协议。

参考文献

-
- [1] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644-654, 1976.
 - [2] S. Goldwasser and S. Micali. Probabilistic encryption and how to play mental poker keeping secret all partial information. In *Proceedings of the 14th ACM Symposium on Theory of Computing (STOC'82)*, pages 365-377, San Francisco, CA, USA, May 1982.
 - [3] M. O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical Report LCS/TR-212, Massachusetts Institute of Technology, 1979.
 - [4] R. L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and publickey cryptosystems. *Communications of the ACM*, 21(2):120-126, February 1978.
 - [5] Adi Shamir, R. L. Rivest, and Leonard M. Adleman. Mental poker. Technical Report LCS/TR-125, Massachusetts Institute of Technology, April 1979.
 - [6] Manuel Blum. Three applications of the oblivious transfer: Part I: Coin flipping by telephone; part II: How to exchange secrets; part III: How to send certified electronic mail. Technical report, University of California, Berkeley, CA, USA, 1981.
 - [7] Andrew C. Yao. Some complexity questions related to distributive computing. In *Conference Record of the 11th ACM Symposium on Theory of Computing (STOC'79)*, pages 209-213, Atlanta, GA, USA, April 1979.