陷门函数的理论与应用

（扩展摘要）

Andrew C. Yao

计算机科学系

加利福尼亚大学

伯克利，加利福尼亚 94720

摘要

本文的目的是引入一种新的信息理论并探索其应用。利用现代计算复杂性理论，我们研究了通过可行计算可以访问的信息概念。

在本文的第一部分，我们奠定了该理论的基础，并为密码学和伪随机数生成建立了一个框架。在第二部分，我们研究了陷门函数的概念，并考察了此类函数在密码学、伪随机数生成以及抽象复杂性理论中的应用。

第一部分：计算信息理论

1. 引言

时至今日，香农的信息定义（以熵为单位）已被普遍接受为统计事件的正确度量[22]。它具备许多理想的性质，并且已被证明是唯一可能满足这些性质的定义（见香农[22]）。它出现在几个重要定理中，总是提供自然的解释。那么，我们为什么要修改这个基本定义，从而修改整个理论呢？

答案是，粗略地说，有时提取一个字符串中包含的香农信息可能需要天文数字般的计算量；在这种情况下，信息论得出的结论可能变得无关紧要。为了更精确地说明这一点，让我们先回顾一下香农理论中的一些基本事实。

设 $\Sigma = \{a_{1}, a_{2}, \ldots, a_{s}\}$ 是一个字母表，即一个有限的符号集合，p 是 Σ 上的概率密度，$p_{i} = p(a_{i})$。考虑一个设备 S，它随机地一次生成一个符号的无限序列 $b_{1}b_{2}b_{3}\ldots$，其中每个 b_{j} 根据 p 独立分布。称这样的设备 S 为信源，并令 S 的熵为 $H(S) = \sum_{i} p_{i} \log_{2}(1 / p_{i})$。可以将 $H(S)$ 视为 S 生成的每个输出符号中包含的不确定性或信息量。下一定理将证明这是一个合理的解释。

假设两个人 A 和 B 相距很远，A 这边有一个信源 S，以及一个 A 可以通过其向 B 发送二进制比特的通信媒介。A 通知 B 由 S 生成的字符串的最有效方式（就最小化发送比特数而言）是什么？更精确地说，假设 A 想要发送 S 输出的连续 n 个符号，L_{n} 即 A 必须发送的最小期望比特数是多少？（关于 L_{n} 的精确定义，参见 [22]）。

香农第一定理[22]。$\lim_{n\to \infty}\frac{L_n}{n} = H(S)$

事实上，以下成立：

换句话说，描述 S 输出的一个符号所需的最小平均比特数为 $H(S)$。

这是信息论中的两个基本定理之一；我们稍后将回顾另一个。但现在，我们已经准备好详细说明计算考量如何可能影响信息论提供的结论。

例 1。设 Σ 为所有 k 位二进制字符串的集合，其中 $k = 10^4$。对于任意 100 位整数 x 和 m，令 $\alpha_{x,m}$ 表示字符串 $c_1c_2\ldots c_k$，其中 $c_j = \text{模 } m \text{ 下 } (x^j) \text{ 的奇偶性}$。设 $\Lambda \subseteq \Sigma$ 为多重集 $\{\alpha_{x,m} \mid x, m\}$。因此，$|\Lambda| = 2^{200}$ 且 $|\Sigma| = 2^{10000}$。考虑 Σ 上的信源 S，其分布密度 $p(y) = 1 / |\Lambda|$ 若 $y \in \Lambda$，否则 $p(y) = 0$。显然，$H(S) \leq \log_2 |\Lambda| = 200$。香农第一定理指出，原则上 A 可以使用 $nH(S) = 200n$ 比特向 B 发送 S 的 n 个输出符号。事实上，A 可以简单地将每个输出 $\alpha_{x,m}$ 表示为 200 位字符串 xm。然而，为了做到这一点，A 必须从 10000 位字符串 $\alpha_{x,m}$ 计算出 x 和 m，因为 A 只知道后者。这并不明显能够在合理的计算时间内完成。

上述例子仅用于证明香农第一定理不能立即保证使用每信源输出 $H(S)$ 比特的计算上可行的编码。我们不知道这个特定问题的真正答案。

我们现在回顾更多信息论内容。再次假设 A 希望通知 B 信源 S 的输出。然而这一次，A 和 B 之间的通信媒介 C，虽然仍然传输 0,1 信号，但是不完美的，因为存在概率 q 使得“0”信号被接收为“1”，同样存在概率 q 使得“1”被接收为“0”。在文献中，C 被称为二进制对称信道，或 BSC。为了通过信道 C 通信 S 的 n 个输出比特，必须发送多少比特？由于如果 $q > 0$ 则错误不可避免，我们感兴趣的是将错误概率保持在任何预先指定的水平 $\epsilon > 0$ 以下。

令 $I = \{0,1\}$，$J = \{0,1\}$ 表示 C 的输入和输出字母表。长度为 m 的码是子集 $E \subseteq I^m$；解码规则是函数 $f: J^m \mapsto I^m$。对于任何 $x \in E$，令 $P(x)$ 为当 x 输入到 C 时，如果接收到 y 则 $f(y) \neq x$ 的概率。将 C 的容量定义为 $capacity(C) = 1 - q \log_2(1/q) - (1 - q) \log_2(1/(1 - q))$。

香农第二定理[22]。对于任何 $R < \text{capacity}(C)$ 和 $\epsilon > 0$，存在（对于足够大的 m）一个长度为 m 的码 E 和一个解码规则 f，使得 (a) $|E| \geq 2^{Rm}$，(b) 对所有 $x \in E$，$P(x) < \epsilon$。

比率 $(\log_2|E|)/m$ 被称为码 E 的速率，因为当使用码 E 时，它是每通过信道发送一比特所通信的平均消息比特数。

存在上述定理的逆命题。本质上，它们表明以速率 $R > \text{capacity}(C)$ 传输是不可能的，除非使错误 $\epsilon \to 1$。

香农第二定理对于比 BSC 更一般的信道也成立。定义信道 C 为一个 $r \times t$ 矩阵 (v_{ij})，满足 $v_{ij} \geq 0$ 且 $\sum_{j} v_{ij} = 1$。解释是 C 有一个输入字母表 $I = \{b_1, b_2, \ldots, b_r\}$ 和一个输出字母表 $J = \{c_1, c_2, \ldots, c_k\}$，使得如果输入 b_i，则输出将是 c_j，概率为 v_{ij}。可以证明，对于正确定义的容量 (C)，香农定理成立。我们请读者参考信息论教科书（例如[8]）了解细节。

理论上，香农第二定理使得可以通过穷举搜索长度为 $1, 2, \ldots$ 的所有可能码，在 $O(1)$ 时间内构造具有给定速率 $R < \text{capacity}(C)$ 和错误界 $\epsilon > 0$ 的显式码。然而，这样的过程在实际计算上是不可行的。寻找实用码的研究有大量文献[8]，并且在实现给定 R 和 ϵ 的码所需的时间和存储需求方面也有改进的理论结果（Ziv[26]）。因此，计算复杂性确实已经在信息论中受到了很多关注。然而，我们感兴趣的计算方面则截然不同。就我们的目的而言，经典信道的编码问题基本上已经解决。我们主要感兴趣的是当信源变得非经典时的情况，即字母表大小不能再被视为常数，如例1所示，以及当信道变得非经典时的情况，我们稍后会看到。

2. 有效熵

给定一个具有大字母表的信源 S，如例1所示，我们应该如何定义其输出中包含的信息？我们将采用这样的观点：以计算上可行的方式描述一个输出所需的最小平均比特数是适当的度量。换句话说，我们将把香农第一定理视为一个定义。

我们考虑以下情况。信源有一个字母表，其符号是有限二进制字符串，平均长度为 n（比如 $n \approx 200$）。人员 A 有兴趣向 B 通信 S 的 n^t 个输出符号的序列 σ（t 是一个固定整数，比如 $t = 3$）。问题是，A 能在合理的时间量内（比如在 n^k 时间内，对于某个固定的 k）计算出多短的字符串 ρ，使得 B 在接收到 ρ 后能在合理的时间量内恢复 σ？为了精确定义这个概念，我们借助了成熟的计算复杂性理论。在该理论中，计算问题的复杂性是通过随着输入长度变大算法的渐进行为来度量的。为了将理论结果应用于特定长度的输入，我们默认假设该长度足够大，可以使用渐近结果。例如，假设理论上可以证明某个形式逻辑系统的判定问题具有复杂性 $\Omega(2^{2^n})$，即，任何用于该判定问题的算法 T 必须具有运行时间 $\geq C_T 2^{2^n}$，对于某个常数 $C_T > 0$。那么我们将认为，对于公式大小 $n \approx 1000$，任何合理的算法必须对某些输入公式使用时间 $\approx 2^{2^{1000}}$。采用这种方法，我们需要考虑的不是一个信源，而是一个信源序列，并关注感兴趣量的渐近行为。

定义 1。设 Σ 是一个固定的有限字母表。一个信源 S 是 Σ^{+} 上的概率分布 p，具有有限的期望长度 $\beta(S) = \sum_{x} p(x)|x|$。一个信源集合 S 是信源序列 $S_{1}, S_{2}, \ldots$，具有概率分布 $p_{1}, p_{2}, \ldots$，使得对于某个固定的 $t_{2} > t_{1} > 0$，$p_{n}(y) > 0$ 意味着 $n^{t_{1}} < |y| < n^{t_{2}}$。

注。最后一个假设并非必需，但有助于简化后续讨论；我们感兴趣的大多数应用都满足它。

在下文中，概率算法指的是总是停机的概率多带图灵机[9]。或者可以将其视为总是停机的随机访问计算机上的程序，因为我们只证明多项式不变的结果。

符号。我们将使用符号 $O(v(n))$ 表示任何函数 $f(n)$，它比 $1 / n^t$ 对于每个固定的 t 更快地趋近于零。

以下定义精确地指定了 A 如何被允许对来自 S^n 的 n^k（对于某个 $k > 0$）个输出符号序列进行编码，以及 B 如何解码它。

定义 2。设 $t, k > 0$ 为任意固定数。S 的 (t, k)-编码是一个概率算法三元组 $M = (M_A, M_B, M_C)$，满足以下属性：

(a) 给定输入 $\alpha = (n, x_1, x_2, \ldots, x_{n^k})$，其中对于所有 i 有 $p_n(x_i) > 0$，算法 M_A 将在时间 $O(n^t)$ 内停机，并在 M_A 的输出带上留下某个二进制字符串 β；令 $q_n(\alpha)$ 表示 β 的概率分布；

(b) 给定输入对 (n,β)，其中 β 根据 $q(\alpha)$ 分布，算法 M_B 将在时间 $O(n^t)$ 内停机，并以概率 $1 - O(v(n))$ 在 M_B 的输出带上留下字符串 α；

(c) 令 $b > 0$ 为任意固定数。给定 n 和任何字符串 $\beta = \beta_{1}\beta_{2}\ldots \beta_{u}$，其中每个 β_{i} 是 M_A 对于某个 α_{i} 的可能输出，且 $u = O(n^{b})$，算法 M_C 在时间 $O(n^{b'})$ 内停机（对于某个固定的 b'），并以错误概率 $O(v(n))$ 正确输出 $\beta_{1}\beta_{2}\ldots \beta_{u}$。

定义 $\ell_{n}(\alpha)$ 为 β 在 $q_{n}(\alpha)$ 上的期望长度。令 $p_{n}(\alpha) = p_{n}(x_{1})p_{n}(x_{2})\ldots p_{n}(x_{n^{k}})$。令 $\ell_{n}(\mathcal{M};\mathcal{S}) = \sum_{\alpha}p_{n}(\alpha)\ell_{n}(\alpha) / n^{k}$，即 $\mathcal{M}$ 用于编码 S_{n} 的一个输出符号 x 的平均比特数。

注。属性 (a) 和 (b) 规定编码和解码可以在多项式计算时间内完成，且错误为 $O(v(n))$。属性 (c) 大致说明该码是一个唯一可解码码，意思是，为了传输信源 S_n 的 $u \cdot n^k$ 个输出，可以分别编码每个 n^k 段，然后将 u 个块连接起来进行传输。

定义 3。S 的 (t,k)-熵序列是一个序列 $w_{1}, w_{2}, \ldots$，使得存在 S 的一个 (t,k)-编码 $\mathcal{M}$，满足 $\ell_{n}(\mathcal{M}; S) = w_{n}$。

只有 w_{n} 的渐近行为是令人感兴趣的，因为对于任何固定的 n，我们可以选择具有足够多状态的 M 使得 $w_{n} = H(S_{n})$，即 S_{n} 的香农熵。

定义 4。我们说有效熵 $H_{c}(S)$ 小于 $g(n)$，或用符号表示为 $H_{c}(S) \leq g(n)$，如果存在 $t, k > 0$ 和 S 的一个 (t, k)-熵序列 $\langle w_{n} \rangle$，使得对于所有足够大的 n，$w_{n} \leq g(n)$。

类似地，如果对于每个固定的 $t, k > 0$，S 的每个 (t, k)-熵序列 $\langle w_{n} \rangle$ 对所有足够大的 n 满足 $w_{n} \geq h(n)$，则我们记 $H_{c}(S) \leq h(n)$。我们还将使用诸如 $H_{c}(S) = O(g(n)), \Omega h(n)), \Theta(f(n))$ 等符号。

因此，我们使用术语“信源集合的有效熵”与我们谈论“判定问题的计算复杂性”的精神相同；两者都不是明确定义的量，但可以作为有用的简写。然而，在某些情况下，我们有足够紧密的上下界来写出诸如 $H_{c}(S; n) = g(n) + O(\log n)$ 的等式。一个重要的情况是对应于随机数的信源集合。

定义 5。真随机数集合 $\mathcal{T}_0$ 是信源集合 $S_{1}, S_{2}, \ldots$，其中 S_{n} 被定义为概率分布 $p_n(x) = 2^{-n}$ 若 $|x| = n$，否则为 0。

定理 1。对于任何信源集合 S，$H_{c}(S;n)\geq H(S_{n}) + O(v(n))$

推论。$H_{c}(\mathcal{T}_{0};n) = n + O(v(n))$

上述定理中出现了加性 $O(v(n))$，因为我们在定义2中允许了 $O(v(n))$ 的概率错误。推论中等式的形式具有特殊的意义，这将在第5节中变得清晰。

是否存在有效熵远大于其香农熵的信源集合？答案是肯定的。设 $g(n)$ 是任何趋近于无穷的单调函数，且 $(\log_2 n)^2 < g(n) < n$。

例 2。可以证明，以下信源集合 $S = S_1, S_2, \ldots$ 具有 $H(S_n) = g(n)$，而 $H_c(S; n) = n + O(v(n))$。设 $\alpha_1, \alpha_2, \ldots$ 为一个二进制字符串序列，其中 α_n 的长度为 $n \cdot 2^{g(n)}$ 并且具有最大的 Kolmogroff-Chaitin 信息[6][14]。将 α_n 写为 $\alpha_{n1}\alpha_{n2}\ldots\alpha_{nG(n)}$，其中 $G(n) = 2^{g(n)}$，且 $|\alpha_{ni}| = n$；令 S_n 由 $p(x) = 2^{-g(n)}$ 若 $x = \alpha_{ni}$ 对某个 i 定义，否则为 0。事实上，使用算法信息的相对化版本（由 Levin 定义），不难修改上述定义以得到一个可构造的 S。

3. 可靠传输

信息论的核心是香农第二定理，该定理指出，信道 C 可以以每信道转移 R 比特的速率可靠地传输信息，前提是 $R < \text{capacity}(C)$。此外，速率 $R > \text{capacity}(C)$ 是不可能实现的。我们面临的自然问题是：信道传输计算信息的速度能有多快？在本节中，我们将研究这个问题的一个方面，即：信道 C 能否以速率 R 比特（$R > \text{capacity}(C)$）可靠地传输计算信息？（我们创造了术语“比特”作为有效熵的单位。）

让我们首先更精确地定义上述问题。由于细节与定义2相似，我们将非正式地陈述定义。与香农情况下码及其速率的定义方式相比，我们需要定义相对于信源集合的码和速率的概念。

定义 6。设 $S = \langle S_n \rangle$ 为一个信源集合，C 为一个具有输入输出符号集 I 和 J 的信道。S 在 C 上的 (t,k)-编码方案是一个概率算法三元组 $\mathcal{M} = (M_A, M_B, M_C)$，它们总是在多项式时间 $O(n^t)$ 内停机。对于任何 n 和来自 S_n 的 n^k 个输出的字符串 α，编码器 M_A 随机计算一个字符串 $\beta \in I^*$，通过信道 C 发送它；解码器 M_B 获取产生的输出字符串 $\gamma \in J^*$ 并计算一个字符串 δ。要求是，当对 α 的概率分布以及 M_A, M_B 和 C 的所有随机移动取平均时，$\delta \neq \alpha$ 的概率是 $O(v(n))$ 阶的。字符串 γ（来自信道 C 的输出）由算法 M_c 唯一地解码（如定义2），同样允许失败概率 $O(v(n))$。

定义2可以视为定义6的特例。S 的 (t,k)-编码本质上是 S 在信道 C 上的 (t,k)-编码方案，其中 C 是交叉概率 $q = 0$ 的二进制对称信道。

定义 7。在之前的定义中，令 $\ell_{n}(\mathcal{M};\mathcal{S};\mathcal{C})$ 为 $|\beta| / n^{k}$ 的期望值，当输入到 M_A 的 α 由信源 S_{n} 概率生成时。

因此，$\ell_{n}(\mathcal{M};S;C)$ 是 $\mathcal{M}$ 为通过信道 C 可靠传输信源 S_{n} 的一个输出符号而使用的平均信道符号数。为了了解“速率”——码的传统性能度量——对应什么，让我们暂时假设 $\chi_c(S;n)$ 具有急剧的渐近行为（例如 $\chi_c(S;n) = \sqrt{n} + O(n^{1/5})$）。在这种情况下，$\mathcal{M}$（对于 S 在 C 上）的速率的自然定义是

那么，是否可能以高于信道容量的速率可靠地传输计算信息的问题就变成了“是否存在 $\mathcal{M}$ 和一个固定的 $\epsilon > 0$，使得 $\lambda_{c}(S; n) > (\text{capacity}(C) + \epsilon)\ell_{n}(\mathcal{M}; S; C)$？”。

下一个定理说答案是“否”。（即使 $\lambda_{c}(S; n)$ 没有被急剧确定，该定理的陈述也有效。）

定理 2。设 $\mathcal{M}$ 为信源集合 S 在信道 C 上的编码方案。则对于任何固定的 $\epsilon > 0$，存在 S 的一个熵序列 $\langle w_n \rangle$，使得

对于所有足够大的 $\pmb{n}$。

推论。如果 $\mathcal{H}_c(S; n) \geq h(n)$，则

对于所有足够大的 n。

这个定理的证明相当复杂。我们在这里不深入讨论。

从美学角度来看，让我们提两个原因说明定理2对于我们的理论很重要。首先，如果该定理为假，我们将有一个信道（比如容量等于2），其每个信道输入符号最多只能携带2比特的香农信息，但可能携带更多，比如2.4比特的计算信息。对于传输计算信息而言，香农第二定理的自然解释将会丢失。我们还必须接受，即使在简单情况下，并非所有比特都是相同的。

第二点是，定理为真并没有明显的原因。考虑具有 $\chi_c(S; n) \approx \sqrt{n}$ 的信源集合 S 的编码。可以想象，码字可能分布得非常稀疏，以至于如果我们使用相同的编码在具有小交叉概率 q 的 BSC 上传输，信道传输后的位移码字仍然相距甚远。因此，没有纯粹的组合障碍阻止编码对于 BSC 仍然有效，并保持高于定理2所允许的速率。事实上，在基于复杂性类型的推理之后，在新环境中获得了一致的解释，这使我们确信我们的定义是正确的。

4. 不可区分性

设 S 和 S' 是两个信源，它们在 Σ^{+} 上具有已知的不同概率分布 p 和 p'，其中 Σ 是固定字母表。假设给你一个模拟其中一个信源的盒子，但没有告诉你模拟的是哪个信源。盒子将根据底层分布，在每次请求时发出一个字符串。你能有把握地分辨出盒子正在模拟哪个信源吗？

对于经典信源，答案是“是”，因为总是可以获取足够的输出，并观察任何特定字符串 v（满足 $p(v) \neq p(v')$）的出现频率。然而，在非经典情况下，问题更为复杂。即使 p 和 p' 有很大差异，比如对于所有长度为 n 的 v 有 $p(v) = |\Sigma|^{-n}$，而 $p'(v) = 1 / |T|$，其中 $T \subseteq \Sigma^n$ 且 $|T| = |\Sigma|^{\sqrt{n}}$，也不明显存在一种方法可以决定哪个替代情况是真实的（如果我们使用上述针对经典信源提到的方法，将需要天文数字般的观测次数）。我们现在精确定义我们所说的两个不可区分信源的含义。

定义 8。设 $S = \langle S_n \rangle$，$S' = \langle S'_n \rangle$ 为两个信源集合。(S, S') 的见证算法 M 是一个概率算法，对于某个固定的 t, k 和 $\epsilon > 0$，以下属性成立：

(a) 对于任何输入 (n, α)，其中 $\alpha = (x_1, x_2, \ldots, x_{n^k})$ 是 S_n 的 n^k 个输出的序列，算法 M 在时间 $O(n^t)$ 内停机并留下布尔输出 $M(n, \alpha)$；令 $f_n(M, S)$ 为当 α 由 S_n 概率生成时 $M(n, \alpha) = 1$ 的概率；

(b) 类似地，令 $f_{n}(M,S^{\prime})$ 为 $S^{\prime}$ 的相应概率；

(c) 存在一个无限的（不同的）值序列 $n_1, n_2, \ldots$，使得

定义 9。如果不存在 S 和 S' 的见证算法，则称两个信源集合 S 和 S' 是不可区分的。

请注意，见证算法可能不是决定盒子是在模拟信源 S 还是 S' 的合适算法，因为条件 (c) 仅保证 S 和 S' 对于 n 的某些值表现不同。见证算法的定义旨在确保两个不可区分的信源对于任何测试，当 $n \to \infty$ 时表现几乎相同。

存在具有非常不同底层概率分布的不可区分信源集合。事实上，例2中定义的集合 $\mathcal{S}$ 和真随机数集合 τ_0（定义5）是不可区分的。原因将在下一节中变得清晰。

5. 伪随机数理论

字符串中随机性概念的研究受到了相当大的关注（见 Knuth [13]）。有两类结果：第一类处理“什么是随机序列”的问题，第二类处理伪随机数生成的问题。前者关注单个序列的属性，并且已通过许多研究者的工作得到满意解答（例如，Kolmogroff[14], Chaitin[6], Martin-Lof[15], Levin[27], Meyer and McCreight[16]）；我们将对后一个问题感兴趣。

伪随机数的需求出现在许多场合，如模拟、抽样、密码学等。对于特定应用，应如何选择伪随机数生成器？在文献中，有许多提出的生成伪随机数的方法，并且有各种统计测试可用于衡量所提出方案的强度。如果在某个应用中，可以隔离一些能保证成功的简单随机性属性，那么可以使用基于所需随机性属性的统计测试来筛选和选择适当的生成器。然而，这种情况很少见。此外，特定伪随机数生成器在特定统计测试下的性能通常难以通过分析确定，并且常常依赖于经验证据。

如果存在一个适合所有应用的伪随机数生成器，那不是很好吗？在本节中，我们将建立一个讨论伪随机数的框架，并引入完美伪随机数生成器的概念。在本文的第二部分，我们将展示一类生成器，它们有强有力的理论证据表明是完美的。

就我们的目的而言，伪随机数生成器是一种算法，它接受一些真随机比特并确定性地生成一个长得多的比特序列。例如，一个可能的线性同余生成器是随机选择四个 n 位数 m, a, c, X_0，并通过 $X_{j+1} = (aX_j + c) \bmod m$ 生成一个 n^3 位序列 $\rho = X_1X_2 \cdots X_{n^3}$。我们可以将最终字符串的概率分布视为一个信源。伪随机数生成器的强度可以作为信源的一个属性来研究，而不考虑它是如何生成的。让我们首先看看如何根据信源来形式化这一点。

定义 10。如果所有满足 $p_n(x) > 0$ 的字符串 x 都具有相同的长度 $\xi(n)$，并且进一步对于所有 n 有 $\xi(n) < \xi(n + 1)$，则称信源集合 $S = \langle p_n \rangle$ 是均匀的。称 $\xi(n)$ 为 S 的长度函数。

为简单起见，在本节的其余部分，我们假设字母表为 $\{0,1\}$。注意，根据定义，对于某个 $t_1, t_2 > 0$，有 $n^{t_1} < \xi(n) < n^{t_2}$。

设 $\xi(n)$ 为一个整数值函数，且 $\xi(n) < \xi(n + 1)$。定义 τ_{ξ} 为信源集合 $\langle S_n \rangle$，其中 S_n 是对应于 $\xi(n)$ 位随机数的信源。

定义 11。如果 S 和 T_{ξ} 是不可区分的，则称具有长度函数 $\xi(n)$ 的均匀信源集合 S 是完美的。

我们想强调，均匀信源集合不一定对应于伪随机数生成器，因为底层分布可能不是由少量随机比特生成的。在转向定义伪随机数生成器的任务之前，我们想更深入地探索“完美”的属性。

统计测试的概念如何融入这个图景？让我们严谨地定义这个术语。

定义 12。多项式统计测试是一个概率算法 M，它仅接受形式为 $(x_1, x_2, \ldots, x_{N^k})$ 的输入，其中每个 x_i 是一个 N 位数，在时间 $O(N^t)$ 内停机，并输出一个二进制字符串 y，其中 t 和 k 是某个固定的正整数。

定义 13。在上述定义中，令 $\eta(N, y)$ 为当输入 x_i 是独立的 N 位数时 y 作为输出出现的概率。对于任何具有长度函数 ξ 的均匀信源集合 S，令 $\eta_M(N, y; S)$ 为当输入 x_i 由信源 S_n 生成时（其中 $N = \xi(n)$）y 作为输出出现的概率。（仅当 $N = \xi(n)$ 对某个 n 成立时，$\eta_M(N, y; S)$ 才有定义。）

非正式地说，测试 M 从信源集合 S 中获取 N^k 个 N 位输出，并计算一个量 y。这个量 y 通常用于产生一个分数 $s = f(y, N)$（通过查表或另一个计算），它表示应拒绝 S 为非随机的置信水平（参见例如[13]）。

定义 14。设 M 为一个多项式统计测试，S 为一个均匀信源集合。如果对所有 y 有 $\eta_{M}(N, y; S) - \eta_{M}(N, y) = O(v(N))$，则我们说 S 通过了统计测试 M。

定理 3。一个均匀信源集合 S 是完美的，当且仅当 S 通过了每个多项式统计测试。

这建立了统计测试与我们关于完美信源集合的定义之间的联系。到目前为止，我们完全根据计算复杂性讨论了“完美”这个概念。下一个结果表明，我们也可以用计算信息来表达它。

定理 4。一个均匀信源集合 S 是完美的，当且仅当 $\chi_c(S; n) = n + O(v(n))$。

定理1推论中等式的重要性现在应该变得清晰了：它刻画了完美信源集合的特征。从定理4还可以得出，例2中的 S 是一个完美信源集合，因此与 τ_0 不可区分。

我们通过在当前设置下定义伪随机数生成器来结束本节。

定义 15。伪随机数生成器 G 是一个概率算法，使得给定输入整数 k 和 n，它

(a) 在多项式时间 $\mathbf{n}$ 内停机，

(b) 使用 $O(n)$ 个真随机比特，并且

(c) 输出一个长度为 n^k 的二进制字符串 α。

对于每个 k，上述生成器 G 定义了一个自然的信源集合 $\mathcal{W}_k(G) = \langle S_n \rangle$，其中 S_n 是输出 α（长度为 n^k）的信源，其概率与 G 相同（当 n 为输入时）。

定义 16。如果对于每个固定的 k，$\mathcal{W}_k(G)$ 都是一个完美信源集合，则称伪随机数生成器 G 是完美的。

6. 互信息与独立性

我们首先回顾香农理论中的互信息和独立性概念。设 $Q = (T, p)$ 为一个概率空间，其中 T 是一个有限样本空间，p 是 T 上的概率分布。对于任何随机变量 $X: T \mapsto V_X$，其中可能值的数量 $|V_X|$ 是有限的，令 X 的熵为

其中 $p_X(x) = \sum_{X(t) = x} p(t)$ 是 $X = x$ 的概率。我们可以将 $H(X)$ 视为对 X 值的单次观察给我们的平均信息量。信源 S 的熵 $H(S)$ 可以作为特殊情况获得，当 S 既是样本空间又是随机变量时。

设 Y 是 Q 上的另一个随机变量。给定 Y 时 X 的条件熵定义为

即，当 Y 的值已知时，对 X 的一次观察给我们的平均信息量。Y 关于 X 的互信息是 $I(X,Y) = H(X) - H(X|Y)$。一个有趣的事实是互信息是对称的，即 $I(X,Y) = I(Y,X)$。从量上说，这意味着如果知道 Y 的值告诉你关于 X 值的一些信息，那么知道 X 的值也大致告诉你关于 Y 的相同数量的信息。

如果 $I(X, Y) = 0$，则称两个随机变量 X 和 Y 是独立的。可以证明这与概率论中该术语的传统用法一致，即对于所有 x, y，$Pr\{X = x, Y = y\} = Pr\{X = x\} \cdot Pr\{Y = y\}$。

现在让我们定义我们理论中的相应概念。与定义有效熵一样，我们从一个例子开始，说明当考虑计算努力时，需要不同的定义。

考虑样本空间 T，它包含两个顶点集之间所有具有 1000 个节点的二分图 G，并假设所有这样的图以相等的概率出现。令 X 和 Y 为由 $Y(G) = G$ 和 $X(G) =$ G 中完美匹配的数量（模3）定义的随机变量。显然，由于可以从 G 的值计算出 X 的值，所以 $H(X|Y) = 0$。因此，$I(X,Y) = H(X)$；我们可以说 Y 包含了关于 X 的所有香农信息。然而，我们不知道从 G 计算 X 的有效方法，并且可以想象（在平均意义下）不存在有效算法。如果是后一种情况，那么我们可以认为 Y 包含的关于 X 的香农信息是（至少部分）无法通过可行计算访问的。因此，显然需要一个不同的 $H(X|Y)$ 定义来表达这种可能性。

我们不知道对于上述讨论的特定问题是否存在有效算法（它是 NP 难的，参见[24]）。可以构造能够严格证明存在这种现象的例子。

让我们尝试捕捉有效条件熵的概念。考虑字母表 Σ 上的信源集合 $S = \langle S_n \rangle$。S 上的随机变量 X 是一个序列 $\langle X_n \rangle$，其中 X_n 是 S_n（被视为概率空间）上的随机变量，其值在 Σ^+ 中。假设信源 S_n 发出 n^k 个输出符号的序列 $\alpha_1, \alpha_2, \ldots, \alpha_{n^k}$，人员 A 被告知 $X(\alpha_i)$ 和 $Y(\alpha_i)$ 的值（$1 \leq i \leq n^k$），而人员 B 仅被告知 $Y(\alpha_i)$ 的值（$1 \leq i \leq n^k$）。现在，如果 A 想要告知 B 关于 $X(\alpha_i)$（$1 \leq i \leq n^k$）的值，A 必须发送给 B 的最小平均比特数是多少？注意，当 Y 是常数且 $X(\alpha_i) = \alpha_i$ 时，该问题简化为定义有效熵时面临的问题。

由于细节与定义2-4相似，我们将非正式地陈述这些定义。X 相对于 Y 的 (t,k)-编码是一个概率算法三元组 $\mathcal{M} = (M_A,M_B,M_C)$，其中编码器 M_A 接受输入 $\alpha = (n,x_1,x_2,\ldots ,x_{n^k},y_1,y_2,\ldots ,y_{n^k})$ 并计算某个二进制字符串 β，如果将此 β 连同 n 和 $y_{1},y_{2},\ldots ,y_{n^{k}}$ 一起输入解码器 M_B，将使 M_B 能够以错误概率 $O(v(n))$ 恢复字符串 $x_{1},x_{2},\ldots ,x_{n^{k}}$；此外，码字 β 由算法 M_C 唯一地解码；算法 M_A,M_B,M_C 都在 $O(n^{t})$ 时间内停机。令 $\ell_n(\mathcal{M};X|Y)$ 表示 $|\beta | / n^{k}$ 的平均值，即 $\mathcal{M}$ 用于编码 X 的一个值 x 的平均比特数。$X|Y$ 的 (t,k)-条件熵序列是一个序列 $\langle w_n\rangle$，使得存在 X 相对于 Y 的 (t,k)-编码，满足 $\ell_n(\mathcal{M};X|Y) = w_n$。我们使用缩写 $H_{C}(X_{n}|Y_{n})\leq g(n)$，$H_{C}

(X_{n}|Y_{n}) = g(n) + O(h(n))$ 等，方式与定义4相同。我们将使用术语 $X|Y$ 的有效条件熵来表示 $H_{C}(X|Y)$。

我们现在转向互信息的问题。

定义 17。设 $g(n)$ 和 $h(n)$ 为任意函数。如果以下为真，则我们将记 $I_C(X_n|Y_n) \leq g(n)$：对于 $X|Y$ 的任何条件熵序列 $\langle w_n \rangle$，存在 X 的一个熵序列 $\langle w_n' \rangle$，使得对于所有足够大的 n，有 $w_n' \leq w_n + g(n)$。类似地可以定义诸如 $I_C(X_n|Y_n) = O(g(n))$，$I_C(X_n|Y_n) \geq h(n)$ 等表达式。

通常，$I_C(X_n|Y_n)$ 不是对称的，这与经典互信息的情况相反。事实上，这种不对称属性对于公钥密码学的可能性至关重要（见第二部分 §5）。然而，在一个重要的特殊情况下，I_C 几乎是对称的。

定理 5。$I_C(X_n|Y_n) = O(v(n))$ 当且仅当 $I_C(Y_n|X_n) = O(v(n))$。

定义 18。如果 $I_C(X_n|Y_n) = O(v(n))$，则称 X 和 Y 是有效独立的。

在经典情况下，对独立性有另一种描述，即 $Pr\{X = x, Y = y\} = Pr\{X = x\} \cdot Pr\{Y = y\}$。是否存在类似物？对于给定的 X 和 Y，让我们定义两个新的信源集合 $S' = \langle S_n' \rangle$ 和 $S'' = \langle S_n'' \rangle$。信源 S_n' 通过以下过程概率地输出字符串 (x, y)：让 S_n 概率生成一个输出 α，然后定义 $x = X(\alpha)$，$y = Y(\alpha)$。信源 S_n'' 通过以下过程输出 (x, y)：让 S_n 独立生成两个输出字符串 α_1, α_2 并定义 $x = X(\alpha_1)$，$y = Y(\alpha_2)$。我们将 S' 记为 $S(X + Y)$，将 S'' 记为 $S(X \times Y)$。

定理 6。设 X 和 Y 为信源集合 S 上的随机变量。则 X 和 Y 是有效独立的，当且仅当 $S(X + Y)$ 和 $S(X \times Y)$ 是不可区分的。

定理6意味着，对于所有足够大的 n，任何多项式时间测试都必然无法检测到有效独立的 X, Y 之间的任何相关性。它还意味着，观察 $y_1, y_2, \ldots, y_{n^k}$ 将不会为预测 $x_1, x_2, \ldots, x_{n^k}$ 的任何函数的值带来明显的优势。

7. 密码学理论

在[23]中，香农基于信息论发展了密码学的数学理论。利用我们开发的工具，我们准备给出一个基于计算复杂性理论的替代基础。

由于篇幅限制，我们将在这个摘要中只给出一个基本的说明。考虑一个传统的密码系统，其中两个用户 A 和 B 共享一个来自大密钥空间 $\mathcal{K}$ 的秘密密钥 K。令 $E(K, M)$ 为加密算法，$D(K, M)$ 为解密算法，即 $D(K, E(K, M)) = M$。令 p 和 q 分别为消息 M 和密钥 K 的概率分布。假设窃听者窃听线路并获取密文 $J = E(K, M)$。他能发现多少关于明文 M 的信息？

香农在[23]中讨论了这种情况。将 K, M, J 视为随机变量。那么 $I(M, J) = H(M) - H(M|J)$ 将是窃听者获得的关于 M 的信息量。无条件安全系统是满足 $H(M) = H(M|J)$ 的系统。有人指出，如果 $H(K) < H(M)$，则无法实现无条件安全。因此，如果我们有 200 位长的密钥和 10^6 位的消息，那么很可能我们无法拥有无条件安全系统。然而，香农指出应该考虑计算复杂性方面。让我们看看如何处理这个问题。

由于我们的理论处理渐近行为，它仅适用于可以轻松放大或缩小的密码系统。为明确起见，假设对于每个 n，系统具有 n 位密钥 K_{n}，n^{4} 位消息 M_{n} 以及一对加解密函数 $E_{n}(K_{n}, M_{n})$，$D_{n}(K_{n}, J_{n})$。密钥 K_{n} 和消息 M_{n} 根据某些概率分布 p_{n} 和 q_{n} 分布。让我们考虑定义如下的概率空间 Q_{n}：样本空间是所有可能的 $(K_{n}, M_{n}, E_{n}(K_{n}, M_{n}))$ 值的集合，并且 $p_{n}(K_{n} = k) \cdot q_{n}(M_{n} = m)$ 是分配给点 $(k, m, E_{n}(k, m))$ 的概率。令 $Q = \langle Q_{n} \rangle$，则 K, M 和 $J = E(K, M)$ 成为信源集合 Q 上的随机变量。我们通过要求 $H_{C}(M) \approx H_{C}(M|J)$，或 $I_{C}(M_{n}|J_{n}) = O(v(n))$ 来定义系统的计算安全性。也就是说，如果随机变量 M 和 J 是计算独立的，则称系统是计算安全的。根据上一节末尾的讨论，在安全系统上，当 n 很大时，窃听者无法从密文中了解到任何关于 M 的信息。

第二部分：陷门函数及其应用

1. 引言

单向函数和陷门函数的概念由 Diffie 和 Hellman [7] 提出，作为一种新型密码学的基础。自那时起，已经发现了许多实现和应用。然而，“什么是陷门函数？”这个问题至今尚未得到令人满意的回答。第二部分的目的是基于第一部分中开发的计算信息论，提出单向函数和陷门函数的精确定义，并展示改进的结果和新的应用。具体来说，我们将展示任何陷门函数都可用于产生如第一部分定义的安全加密方案，并且也许更令人惊讶的是，可用于生成将通过任何可行统计测试的“完美”伪随机数。我们还给出了一个新的函数，它是一个陷门函数，假设大整数分解在计算上是不可行的。最后，将展示单向函数存在性对抽象复杂性理论的一个有趣影响。

2. 背景

2.1 加密

Diffie 和 Hellman [7] 发明了用于发送秘密消息的公钥加密概念。在该方案中，每个用户 A 将一个公钥 K_A 放入公共文件中的加密函数 E_{K_A}，并将私钥 K'_A 保留为解密函数 $D_{K'_A}$ 的私有信息。这对 (K_A, K'_A) 具有这样的性质：对于 E_{K_A} 定义域中的任何 x，$D_{K'_A}(E_{K_A}(x)) = x$。任何希望发送消息 x 给 A 的人都可以将其加密为 $E_{K_A}(x)$，然后 A 通过将 $D_{K'_A}$ 应用于 $E_{K_A}(x)$ 来恢复 x。为了使该方案正常工作，应满足以下属性：

(a) 给定 K_A 和 $\pmb{x}$，$E_{K_A}(x)$ 的值应该易于计算；给定 $K_A^\prime$ 和 $\pmb{y}$，$D_{K_A^\prime}(y)$ 的值应该易于计算；

(b) 给定 $E_{K_A}(x)$，找到 $\pmb{x}$ 在计算上是困难的；

(c) 随机对 (K_A, K_A') 应该易于生成。

由于这些函数 $E_{K_A}(x)$ 易于计算但难以逆推，因此被称为陷门函数。

Rivest、Shamir 和 Adleman（RSA 方案 [20]）提出了一个具体的实现。在他们的方案中，用户 A 生成两个随机素数 p 和 q，以及一个整数 s，满足 $\gcd(s, \phi(N)) = 1$，其中 $N = p \cdot q$，$\phi(n)$ 是欧拉 totient 函数。令 N 为公钥 K_A，$r = s^{-1} \mod \phi(N)$ 为私钥 K'_A。函数 $E_{K_A}(x) = x^s \mod N$ 用作加密函数，而 $D_{K_A}(x) = x^r \mod N$ 用作解密函数。

Rabin [19] 提出了 RSA 方案的一个变体。他没有使用 $x^s \bmod N$，而是定义了 $E_{K_A}(x) = x^2 \bmod N$，解密对于知道 N 因式分解的用户 A 来说是容易的。一个有趣的事实是，成功地对任何 ϵ 比例的 x 逆推 $E_{K_A}(x)$，将使得人们能够在随机多项式时间内对 N 进行因式分解。

Goldwasser 和 Micali [10] 提出了上述方案的两个潜在问题：

(a) 即使 $E_{K_A}(x)$ 通常难以逆推，但当 x 具有特殊形式时，它可能很容易；

(b) 人们可能能够从 $E_{K_A}(x)$ 推断出关于 $\pmb{x}$ 的一些部分信息。

他们提出了一个没有这些困难的方案。该方案逐比特加密整个消息，其中单个比特的加密基于判定整数 y 是否是模 N 的二次剩余的复杂性。我们在此概述该方法。

设 $N = p \cdot q$ 为两个 n 位素数的乘积。用 Z_N^* 表示集合 $\{x \mid 1 \leq x \leq N, \gcd(x, N) = 1\}$，并令 $A_N^* \subseteq Z_N^*$ 为包含那些雅可比符号 $(x / N) = 1$ 的 x 的子集。A_N^* 的一半成员是二次剩余，一半是非剩余。

用户 A 生成一个随机的 n 位合数 $N = p \cdot q$（由两个素数组成），并将 N 连同 A_N^* 中的一个非剩余 y 放入公共文件中。假设 B 想要发送一个比特 b 给 A。那么 B 将随机生成一个 $x \in Z_N^*$，并在 $b = 0$ 时发送 $x^2 \mod N$，在 $b = 1$ 时发送 $yx^2 \mod N$。因此，A 可以通过查明接收到的数字是否是二次剩余来决定 $b = 0$ 还是 1。不知道 N 因式分解的窃听者将难以决定 b 是什么。

像这样对于一个给定消息随机产生密文的方案，被称为概率加密[10]。

Goldwasser 和 Micali [10] 表明，在下面的假设 GM 下，对于任何固定的 $0 < \epsilon < 1$，对手将无法以 $1/2 + \epsilon$ 或更高的概率正确猜测 b 的值。

定义 19。令 $C_{n,\epsilon}$ 为任何电路的最小规模，该电路对于具有两个素因子的所有 n 位整数 N 的 ϵ 部分，能正确判定模 N 的二次剩余性。

假设 GM：对于任何固定多项式 Q 和任何固定的 $0 < \epsilon < 1$，$C_{n,\epsilon} > Q(n)$ 渐近成立。

2.2 伪随机数生成

使用伪随机数生成器作为近似的一次一密是秘密通信的常见模式。Shamir [21] 考虑了以下问题。假设两个人 A 和 B 共享一个共同的秘密种子 s，并使用一个共同的伪随机数生成器。为了让 A 向 B 发送明文块 $y_1, y_2, \ldots$，A 可以使用 s 生成一个伪随机数序列 $x_1, x_2, \ldots$，并向 B 发送密文 $x_1 \oplus y_1, x_2 \oplus y_2, \ldots$。由于 B 可以生成序列 $x_1, x_2, \ldots$，这些可以很容易地被 B 解码。现在想象一下，当对手有一些关于明文的侧面信息，使他能够找出 $x_1, x_2, \ldots$ 的几个初

始值。基于这些值，对手可能能够生成其余的 x 序列，从而破解密文。Shamir 提出了一个问题：能否设计一个具有以下属性的伪随机数生成器：即使知道 $x_1, x_2, \ldots, x_k$，仍然难以计算 x_{k+1}？基于 RSA 方案是安全的假设，Shamir 给出了一个满足此要求的伪随机数生成器。

Shamir 的方案不能保证下一个比特难以计算（即使下一个字难以计算）。Blum 和 Micali [5] 最近基于离散对数问题构建了一个更强的伪随机数生成器。（他们还给出了一个关于单向函数的准则，在此准则下该构造将有效。）令 $k > 0$ 为任意整数。该生成器使用 $O(n)$ 个真随机比特，并生成一个序列 $x_{1}, x_{2}, \ldots, x_{n^{k}}$，在下面的假设 BM 下，具有以下属性：令 $G_{n,j,\epsilon}$ 为任何具有 j 个布尔输入的电路的最小规模，当 $x_{1}, x_{2}, \ldots, x_{j}$ 的值输入到电路时，该电路能够以 $\frac{1}{2} + \epsilon$ 或更高的概率正确输出 x_{j+1} 的值。则对于任何固定多项式 Q，$G_{n,j,\epsilon} > Q(n)$ 渐近成立。

为了描述所需的假设，令 p 为一个素数，g 为循环乘法群 $A_p = \{1, 2, \ldots, p - 1\}$ 的一个生成元。对于 $y \in A_p$，令 $f(p, g, y)$ 为满足 $g^x \bmod p = y$ 的值 $x \in A_p$。如果一个具有三个 n 位输入 a, b 和 c 的布尔电路解决了 p 的离散对数问题，如果对于所有 g 和 y，当 $a = p, b = g$ 且 $c = y$ 时，其输出等于 $f(p, g, y)$。令 $I_{n,\epsilon}$ 为任何电路的最小规模，该电路解决了所有 n 位素数 p 的 ϵ 部分的离散对数问题。

假设 BM：对于任何固定多项式 Q 和任何固定的 $0 < \epsilon < 1$，$I_{n,\epsilon} > Q(n)$ 渐近成立。

2.3 讨论

在前面的综述背景下，有几个问题似乎值得进一步考虑。

(a) [10] 中的概率加密方案和 [5] 中的伪随机序列生成都利用了所采用单向函数的特殊属性。是否有通用程序可以利用任何陷门函数进行加密和生成伪随机数？

(b) [5] 中的伪随机数序列对于任何固定的 $\epsilon > 0$ 是逐比特无偏的，因此解决了 Shamir 提出的问题。然而，密码分析员可能采用不同的程序来分析伪随机数生成器。例如，他可能反向工作，检查最后几个比特以尝试重建前面的比特。（确实，[5] 中方案生成的序列如果反向读取是否具有相同的无偏属性仍然是开放的。）能否构造一个能够经受密码分析员任何破解伪随机序列尝试的伪随机序列？在更广泛的背景下，能否构造可用于密码学以外应用的伪随机序列？

(c) 能否削弱假设 BM 和假设 GM 中的假设，使得不是要求任何算法不能解决任何固定 ϵ 部分的实例，而是只要求没有算法能解决，比如说，一半的实例？

我们将在接下来两节中对所有上述问题给出肯定的回答。

3. 单向函数

在本节中，我们形式化单向函数的概念，并展示如何使用它们来构建完美的伪随机数生成器以及实现安全的传统密码系统。

将单向函数 f 视为谜题 Z 中使用的 1-1 函数是有帮助的。在每次游戏中，Z 根据某个分布 $p_n(x)$ 选择一个随机的 n 位数 x，并向我们展示 $f(x)$ 的值。我们被挑战去找到 x，并有一个按钮可以请求帮助。如果最终我们请求帮助的次数占一定比例，则函数 f 将是单向的。

定义 20。令 $P = \langle p_n \rangle$ 为 Σ^{+} 上的概率分布序列，其中 p_n 的支持（即集合 $\{x \mid p_n(x) \neq 0\}$）仅包含长度为 $\theta(n)$ 的字符串。如果存在一个概率算法 M，给定输入 n，将在 n 的多项式时间内停机，并以满足 $\| h - p_n \| = O(v(n))$ 的概率分布 $h(x)$ 输出一个 x，则我们将称 P 为多项式时间分布集合。符号：$\| h - p_n \| = \sum_{x} |h(x) - p_n(x)|$。

定义 21。令 f 为从 V 到 Σ^* 的 1-1 函数，其中 $V \subseteq \Sigma^*$。令 $P = \langle p_n \rangle$ 为一个多项式时间分布集合，使得每个 p_n 的支持是 V 的一个子集。将 f 在 P 下的相关集合定义为信源集合 $Q^{f,P} = \langle Q_n \rangle$，其中信源 $Q_n = (T, q_n)$ 的样本空间为 $T = \{(x, f(x)) \mid x \in V\}$，分布 $q_n(\tau) = p_n(x)$ 对于 $\tau = (x, f(x))$。令 $X^{f,P} = \langle X_n \rangle$ 和 $Y^{f,P} = \langle Y_n \rangle$ 为 $Q^{f,P}$ 上的两个随机变量，定义为对于 $\tau = (x, f(x)) \in Q_n$，$X_n(\tau) = x$ 且 $Y_n(\tau) = f(x)$。

定义 22。如果存在一个多项式时间分布集合 P，使得对于某个固定的 t，$H_{C}(X_{n}^{f,P}|Y_{n}^{f,P}) = \Omega(1/n^{t})$，则称 1-1 函数 f 是单向的。

该定义的要点是，在分布 p_{m} 下，为了从 $f(x)$ 恢复 $\pmb{x}$，需要一些比特的信息。下一个定理直接从复杂性角度给出了另一种描述。

定义 23。令 f 和 P 如定义 21 中所述。定义 $P^{f} = \langle p_{n}^{f} \rangle$，其中 $p_{n}^{f}(y) = p_{n}(f^{-1}(y))$。

定理 7。一个 1-1 函数 f 是单向的，当且仅当存在一个多项式时间分布集合 P，使得以下成立：对于任何概率算法，在输入 n 和 y（y 根据 $p_n^f(y)$ 分布）时，在 n 的多项式时间内停机并输出 x，$x \neq f^{-1}(y)$ 的概率对于某个 t 是 $\Omega(1/n^t)$。

当单向函数具有一些附加属性时，它们变得更加有趣。例如，如果一个单向函数具有某种不变性，那么它可以用来构造一个完美的伪随机数生成器，从而构建一个安全的传统密码系统；如果它拥有一个密钥加一个逆密钥，那么它就成为一个陷门函数，并可用于构建概率公钥密码系统。

具有不变性属性的单向函数

定义 24。如果在定义 22 中，我们还有 $P^f = P$，那么我们称 f 为稳定单向函数。

定理 8。任何稳定单向函数 f 都可以用来构造一个完美的伪随机数生成器 G_f。

注。该构造是显式的，意思是，如果给出了 f 和 P 的所有相关概率算法的描述，那么 G_f 的描述是直接的。

定理 8 的推论。任何稳定单向函数 f 都可以用来构造一个计算安全的密码系统。（见第一部分的 §7）

注。伪随机数生成器的种子被用作共同的私钥。这是计算安全的一次一密的实现。

带密钥的单向函数

我们将使用离散对数问题作为例子来说明我们的结果。

例 3. 离散对数函数

令 (G*{n} = {(p, g, m) \mid p \text{ 是一个 } n \text{ 位素数, } g) 是 (A*{p} })。定义 (V = \bigcup_{n} G_{n})，和 (f: V \mapsto V) 为 $f(x) = (p, g, g^{m} \bmod p)$ 如果 $x = (p, g, m)$。

我们将 (p, g)（x 中在 f 下保持不变的部分）视为密钥。考虑那些以两个步骤生成 x 的分布 P 是有用的：首先生成密钥 (p, g)，然后是剩余部分 m。下面定义的 $\langle p_n \rangle$ 给出了这样一个 P。令

如果 $K = (p, g)$ 是一个可能的密钥，则 $p_n'(K) = 0$ 否则。令 $p_{n,K}'' = 1 / (p - 1)$ 若 $m \in A_p$，否则为 0。最后，对于 $x = (K, m)$，定义 $p_n(x) = p_n'(K) \cdot p_{n,k}''(m)$。

符号。我们将扩展定义 20，并说序列 $\langle p_{n,K}^{\prime\prime}(m)\rangle$ 是一个多项式时间分布集合，如果 $p_{n,K}^{\prime\prime}(m) \neq 0$ 意味着 $m = \theta(n)$，并且如果存在一个概率算法，给定 n 和 K，在 n 的多项式时间内停机，并输出一个字符串 z，其概率分布 $h(z)$ 满足 $\| h - p_{n,k}^{\prime\prime}\| = O(v(n))$。

定义 25。如果 f 的定义域 V 具有形式 $V \subseteq \Sigma_1^* \times \Sigma_2^*$ 并且存在一个多项式时间分布集合 $P = \langle p_n \rangle$ 具有以下属性，则称单向函数 f 拥有一个密钥：

(a) P 使得 f 成为如定义 22 中的单向函数，

(b) 如果 $x = (K, z)$，则 $p_n(x) = p_n'(K) \cdot p_{n,K}''(z)$，其中 $\langle p_n' \rangle$ 和 $\langle p_{n,K}'' \rangle$ 是多项式时间分布集合，

(c) 对于 $x = (K, z)$，$f(x)$ 可以写成形式 $(K, f_{K}^{\prime\prime}(z))$。

4. 陷门函数与加密

陷门函数基本上是一个带有密钥 K 的单向函数，使得同时可以轻松创建一个逆密钥 K'，但是无法从 K 推断出 K'。我们将不在本摘要中给出正式定义。

概率公钥密码系统（PPKC）是一种密码系统，其中用户 A 在公共文件中有一个 n 位密钥 K，同时将密钥 K' 作为私有信息保留。为了发送一个比特 $b \in \{0,1\}$，B 将使用 b 和 K 概率计算一个字符串 $\pmb{x}$ 并将其发送给 $\pmb{A}$。密钥的生成方式使得，凭借 K' 的知识，$\pmb{A}$ 可以唯一地恢复 b。

让我们称一个 PPKC 是安全的，如果对于具有偏差 $p \geq 1/2$ 的 b，对手无法在多项式时间内从 K 和 x 中以超过 $p + O(v(n))$ 的概率正确猜测 b 的值。

定理 9。任何陷门函数都可以用来构建一个安全的 PPKC。

对大合数进行因式分解是一个长期抵制有效解决方案的问题。因此，它将是构建 PPKC 或伪随机数生成器的最合适基础。下面我们提出一个新的陷门函数，它也是一个稳定的单向函数，假设因式分解在待描述的适当意义下是困难的。令 T_{n} 为所有整数 $N = p \cdot q$ 的集合，其中 p 和 q 是 n 位素数，且 $p \equiv q \equiv 3 \mod 4$。

因式分解的难解性假设：

对于任何尝试对整数进行因式分解的多项式时间概率算法 M，存在一个 n_0，使得对于所有 $n \geq n_0$，M 将无法对 T_n 中至少 $1 / n^{10}$ 的成员进行因式分解。

注。可以用任何预先确定的 t 的 $1 / n^t$ 替换 $1 / n^{10}$。

一个基于因式分解的陷门

我们通过生成两个随机的 n 位素数 p, q（$p \equiv q \equiv 3 \bmod 4$），并设置 $K = N \left(\equiv p \cdot q \right)$ 和 $K' = \{p, q\}$ 来生成一对密钥 (K, K')。陷门函数 f 定义为：对于 $z \in A_N^*$，如果 z 是偶数，则 $f(N, z) = z^2 \bmod N$，如果 z 是奇数，则 $f(N, z) = -z^2 \bmod N$。

有趣的是，上面定义的基于因式分解的陷门函数也导致了一个简单的伪随机数生成器。可以证明，如果二次剩余问题是困难的，那么这个生成器是完美的。

一个二次剩余伪随机数生成器

令 $n > 0$ 和 $k > 0$。我们将描述如何使用 $O(n(\log n)^2)$ 个真随机比特生成一个长度为 n^k 比特的序列 β。

我们首先描述一个生成准随机序列 α 的过程：从 T_{n} 中随机选取一个 N，以及一个随机的 m（$1 \leq m \leq N - 1$），然后通过 $z_{1} = m$，$z_{i + 1} = f(N, z_{i})$ 计算以下数字序列 $z_{1}, z_{2}, \ldots, z_{n^{k}}$。令 $\alpha = \alpha_{1} \alpha_{2} \cdots \alpha_{n^{k}}$，其中 α_{i} 就是 z_{i} 的奇偶性。

为了获得 β，我们重复上述过程以获得 $t = (\log_2 n)^2$ 个准随机字符串 $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t)}$。现在令 $\beta = \alpha^{(1)} \oplus \alpha^{(2)} \oplus \dots \oplus \alpha^{(t)}$，其中 $\oplus$ 表示按位异或。对于固定的 k 和大的 n，如此生成的伪随机序列 β 将与其随机序列不可区分，假设二次剩余性是困难的。

5. 是什么使陷门函数起作用？

深入理解前两节的结果是很有趣的。正如我们将看到的，如果我们跟踪各种字符串中包含的计算信息并考虑如何操纵这些信息，这些结果可以自然地推导出来。在本摘要中，我们将对使用陷门函数进行加密给出这样的分析。

为明确起见，考虑一个单向函数 f，它将 n 位字符串映射到 n 位字符串（对于每个 n），并令 $\langle p_n \rangle$ 是使 f 成为单向的分布集合。对于给定的 n，f 可以被视为具有大字母表的信道，实际上具有 2^n 个输入符号和 2^n 个输出符号。因此，f 是一个非经典信道，我们必须考虑可访问信息而不是香农信息。

令 (X_{n},Y_{n}) 表示对应于 $(x,f(x))$ 的随机变量对，其中 x 根据 p_n 分布。让我们通过假设一方 A 在信道 f 的输入端，以概率 $p_n(x)$ 跨信道向另一方 B 发送字符串 x 来戏剧化这一情况，B 接收到字符串 $f(x)$。显然，香农条件熵 $H(Y_{n}|X_{n})$ 和 $H(X_{n}|Y_{n})$ 都是 0，经典地 f 是一个无噪声信道。然而，当我们考虑可访问信息时，我们发现 $H_{C}(Y_{n}|X_{n})$ 仍然是 0，但 $H_{C}(X_{n}|Y_{n})$ 是 $\Omega(1/n^{t})$。也就是说，A 对 B 接收到什么没有不确定性，但 B 对 A 发送了什么至少有一些不确定性，诚然，不确定性可能小到 $1/n^{t}$ 比特。因此，从 B 的角度来看，他处于一个噪声至少为 $1/n^{t}$ 的噪声信道的接收端，这在多项式时间计算中是一个不可忽略的量。

现在让我们以稍微不同的方式可视化上述图景。假设 f 实际上是一个陷门函数，而第三方 G 是秘密密钥的所有者，而 A 实际上是在将 x 作为 $f(x)$ 传输给 G。对 G 来说，这是一个清晰的信道，因为他有秘密密钥来解码 $f(x)$。现在 B 的角色是一个窃听者，他没有秘密密钥，试图用低档设备窃听线路。但是这种情况在经典信息论中有一个确切的类比，称为 Wyner 窃听信道[25]。Wyner 表明，即使 B 信道中的噪声很小，A 也可以通过适当地编码他的消息来放大噪声。例如，假设 B 有一个交叉概率为 10^{-4} 的二进制对称信道，并且 A 将一个比特 b 编码为一个随机的 10^{6} 位字符串 α，使得当且仅当 $b = 0$ 时，α 具有偶数个 1。那么，在传输的比特中，B 可以以高置信度猜测每个单独比特的值，但 B 知道他将在大约 100 个比特的值上出错。估计他是错过了偶数个比特还是奇数个比特变得困难。事实上，已经证明这种方案确实会完全使 B 对 b 的真实值感到困惑。

在我们的情况下，噪声有点像 n^{-t}，而 α 长度的近似估计大约是 n^t，这很大，但可以在多项式时间内完成。

详细跟踪伪随机数生成中的信息核算也很有趣；我们将把这留给完整的论文。

6. 抽象复杂性理论中的一个定理

令 R 为在随机多项式时间内可解的判定问题类，如 Adleman [1] 中所定义。R 与确定性复杂性层次结构之间的关系一直是相当感兴趣的主题（Adleman [1], Aleiunas, et. al. [3], Bennett and Gill [4], Gill [9]）。两个众所周知的结果是，R 中的任何判定问题都可以由多项式规模的布尔电路计算[1]，并且明显的关系 $R \subseteq \bigcup_{\epsilon > 0} DTIME(2^{n^{\epsilon}})$ 成立，其中 $DTIME(g(n))$ 是在确定性时间 $g(n)$ 内可解的问题类。在本节中，我们将在单向函数存在的假设下，证明后一种关系的更强形式。（本节中单向函数的定义将与前面几节的定义有所不同。）

令 f 为定义在 $\{0,1\}^*$ 子集上的 1-1 满射函数。假设 $P = \langle p_n \rangle$ 是一个在 f 下不变的多项式时间分布集合。如果一个布尔电路 C 在 p_n 下逆推 f，如果 $\sum_{y \in T} p_n(y) > 1/2$，其中 T 是 C 给出输出 $f^{-1}(y)$ 的输入字符串 y 的集合。令 $B_n(f, P)$ 为在 p_n 下逆推 f 的最小电路的大小。

定义 26。如果存在一个 P，使得对于任何多项式 Q，$B_{n}(f, P) > Q(n)$ 渐近成立，则称 f 为强单向函数。

本节的主要定理如下。

定理 10。如果存在任何强单向函数，则

这个公式意味着，对于 R 中的任何判定问题和任何 $\epsilon > 0$，存在一个确定性图灵机在时间 $O(2^{n^{\epsilon}})$ 内解决它。有趣的是，这是一个非均匀复杂性的下界对均匀复杂性的上界有影响的情况（参见 Karp and Lipton[], Pippenger [17], Pippenger and Fischer [18]）。

如果整数因式分解是困难的，或者离散对数问题在适当意义下是困难的，则定理 10 的假设将得到满足。令 $F(n)$ 为任何布尔电路的最小规模，该电路可以对具有两个 n 位素因子的 $2n$ 位合数 N 的 $4/5$ 部分进行因式分解。

因式分解的强难解性假设：对于任何固定多项式 Q，$F(n) > Q(n)$ 渐近成立。

定理 10 的推论。在因式分解的强难解性假设下，

显然，如果离散对数问题在假设 BM 的意义上是困难的，定理 10 也成立。然而，在这种情况下，一个弱得多的假设就足够了。我们将在下面陈述该结果作为定理 11。

定义 27。令 p 为一个 n 位素数，g 为 A_p 的任何生成元。离散对数问题 $D_{p,g}$ 是：给定输入 $y \in A_p$，找到满足 $g^x \bmod p = y$ 的 x。

令 $\ell(D_{p,g})$ 为求解 $D_{p,g}$ 的最小布尔电路规模。定义 $L(n)$ 为 $\max\{\ell(D_{p,g}) \mid \log_2(p + 1) \leq n\}$。我们做出以下假设：

离散对数的难解性假设：对于任何固定多项式 Q，$L(n) > Q(n)$ 渐近成立。

请注意，这个假设比假设 BM 弱。事实上，与本文其余部分不同，它不涉及平均情况复杂性。

定理 11。在离散对数的难解性假设下，我们有

离散对数问题是一个经典的数论问题，对此没有已知的有效算法。该问题的难解性假设，以某种形式，一直是几种密码协议的基础（Diffie and Hellman [7], Blum and Micali [5]）。到目前为止，已知的最佳算法[2]运行时间大约为 $2^{\sqrt{n}}$。如果离散对数问题实际上具有比多项式高得多的复杂性，那么我们可以获得比定理 2 更强的结果。例如，有：

定理 $12'$。如果对于某个固定的 $\epsilon > 0$ 和所有 n，$L(n) > 2^{n^c}$，则对于某个常数 $c > 0$，$R \subseteq DTIME(2^{(\log n)^c})$。

参考文献

[1] L. Adleman, "Two theorems on random polynomial time," Proc. 19th IEEE Symp. on Foundations of Computer Science, Ann Arbor, Michigan, Oct. 1978, 75-83.

[2] L. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," Proc. 20th IEEE Symp. on Foundations of Computer Science, Puerto Rico, Oct. 1979, 55-60.

[3] R. Aleliunas, R. M. Karp, R. J. Lipton, L. Lovasz, C. Rachoff, "Random walks, universal sequences, and the complexity of maze problems," Proc. 20th IEEE Symp. on Foundations of Computer Science, Puerto Rico, Oct. 1979, 218-223.

[4] C. H. Bennett and J. Gill, "Relative to a random oracle, PA = NPA = co-NPA with probability 1," SIAM J. on Computing 10 (1981), 96-113.

[5] M. Blum and S. Micali, "How to generate cryptographically strong sequences of pseudo random bits," this proceedings.

[6] G. Chaitin, "A theory of program size formally identical to information theory," Journal of ACM 22 (1975), 329-340.

[7] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. on Inform. Theory IT-22, 6 (1976), 644-654.

[8] R. Gallager, Information Theory and Reliable Communication, Wiley, New York, 1968.

[9] J. Gill, "Computational complexity of probabilistic Turing machines," SIAM J. om Computing 6 (1977), 675-695.

[10] S. Goldwasser and S. Micali, "Probabilistic encryption and how to play mental poker keeping secret all partial information," Proc. 14th ACM Symp. on Theory of Computing, San Francisco, May 1982.

[11] J. E. Hopcroft and J. D. Ullman, Introduction to Automata Theory, Languages, and Computation, Addison-Wesley, Reading, Mass., 1979.

[12] R. M. Karp and R. J. Lipton, "Some connections between nonuniform and uniform complexity classes," Proc. 12th ACM Symp. on Theory of Computing, Los Angeles, April 1980, 302-309.

[13] D. E. Knuth, The Art of Computer Programming, Vol. 2, Addison-Wesley, Reading, Mass., second edition, 1981.

[14] A. N. Kolmogorov, "Three approaches to the concept of the amount of information," Probl. Pered. Inf. (Probl. of Inf. Transm.) 1/1 (1965).

[15] P. Martin-Lof, "The definition of random sequences," Information and Control 9 (1966), 602-619.

[16] A. R. Meyer and E. M. McCreight, "Computability complex and pseudorandom zero-one valued functions," in Theory of Machines and Computations, Z. Kohavi and A. Paz, eds., Academic Press, New York 1971, 19-42.

[17] N. Pippenger, "On simultaneous resource bounds," Proc. 20th IEEE Symp. on Foundations of Computer Science, Puerto Rico, Oct. 1979, 307-311.

[18] N. Pippenger and M. J. Fischer, "Relations among complexity measures," Journal of ACM 26 (1979), 361-381.

[19] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," MIT/LCS/TR-212, 1979.

[20] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of ACM 21 (1978), 120-126.

[21] A. Shamir, presented at Crypto-81, Santa Barbara, 1981.

[22] C. E. Shannon, "A mathematica theory of communication," Bell System Technical Journal, 27 (1948), Part I, 479-523, Part II, 623-656.

[23] C. E. Shannon, "Communicatin theory of secrecy systems," Bell System Technical Journal 28 (1949), 656-715,

[24] L. Valiant, "The complexity of computing the permanent," Theoretical Computer Science 8 (1979), 189-201.

[25] A. D. Wyner, "The wire-tap channel," Bell System Technical Journal 54 (1975), 1355-1387.

[26] J. Ziv, IEEE Transaction on Information (1965).

[27] A. K. Zvonkin and L. A. Levin, "The complexity of finite objects and the algorithmic concepts of information and randomness," Uspekhi Mat. Nauk (Russian Math. Surveys 25/6 (1970), 83-124.

专业术语英汉对照表

英文术语	中文翻译
Trapdoor Functions	陷门函数
Computational Complexity	计算复杂性
Information Theory	信息论
Shannon's Theorem	香农定理
Entropy	熵
Effective Entropy	有效熵
Source / Source Ensemble	信源 / 信源集合
Probabilistic Algorithm	概率算法
Polynomial-time	多项式时间
Indistinguishability	不可区分性
Pseudorandom Number Generator	伪随机数生成器
Perfect Pseudorandom Generator	完美伪随机数生成器
Statistical Test	统计测试
Mutual Information	互信息
Effective Independence	有效独立性
Cryptography	密码学
Public Key Encryption	公钥加密
Probabilistic Encryption	概率加密
One-way Function	单向函数
Stable One-way Function	稳定单向函数
Key	密钥
Discrete Logarithm	离散对数
Factoring	因式分解
Quadratic Residue	二次剩余

英文术语	中文翻译
Binary Symmetric Channel (BSC)	二进制对称信道
Channel Capacity	信道容量
Rate (of a code)	（码的）速率
Random Variable	随机变量
Conditional Entropy	条件熵
Abstract Complexity Theory	抽象复杂性理论
Deterministic Turing Machine (DTIME)	确定性图灵机
Random Polynomial Time (R)	随机多项式时间
Boolean Circuit	布尔电路
Average-case Complexity	平均情况复杂性
Worst-case Complexity	最坏情况复杂性