摘要

隨機性已被證實在資訊科學的許多領域都是非常有用的，然而我們通常只能獲得不夠完美的隨機源。退而求其次地，我們可以利用一個決定性的函數，稱為萃取器(extractor)，從一些可取樣的弱隨機源中萃取出真正的隨機元。我們說一個弱隨機源的 statistical min-entropy 為 k 則表示每個字串出現的機率都不會超過 2^{-k}。在近幾十年中，針對各種隨機源的萃取器被廣泛的討論，且有許多重要的結果。

我們首先考慮針對獨立符號隨機源(independent-symbol sources)的萃取器。一個 (n,D,k)-來源，其為一個在[D]^n ([D]={1,2,...,N}) 上的分布 $X=(X_1,\cdots,X_n)$，其中 $X_1,\cdots,X_n$ 是彼此獨立的，且 X 的 min-entropy 是 k。[LLT06]提出一個針對此種隨機源的萃取器，其可看成是在一個圖形上作隨機散步(random walk)。我們發現在此隨機散步中每一步所對應的矩陣為一個特殊的矩陣，稱為循環矩陣(circulant matrix)。我們利用已知的循環矩陣的性質簡化此種萃取器的分析，並獲得一個更好的結果。

此外，本計劃由計算性的角度出發，考慮一個條件的來源(f(X)|X)，其中 X 是一個在 $\{0,1\}^{n_1}$ 的分布，而 $f:\{0,1\}^{n_1}\to\{0,1\}^n$ 為某個函數。假設當輸入 x 是依照分布 X 所產生時，任何大小為 2^k 的電路最多只有 2^{-k} 的機率可以猜對 f(x)時，則我們說這種條件分布(f(X)|X)擁有 computational min-entropy k。我們首先證明無法從單一個只擁有 computational min-entropy 的來源中萃取出一個隨機元。接著我們證明可從一個只擁有 computational min-entropy 與另一個擁有 statistical min-entropy 的隨機源中萃取出隨機元。更進一步地，我們亦證明可從兩個只擁有 computational min-entropy 的隨機源中萃取出隨機元。這可看成是把原先在 statistical setting 中針對多隨機源萃取器的研究延伸到 computational setting。我們把建造此種萃取器的工作轉成是一個在學習理論上的問題: 利用任何一個分布在對手雜訊(adversarial noise)的模型下學習線性函數。針對此問題，我們亦提出一個學習演算法。

關鍵詞: 獨立符號來源，循環矩陣，兩個隨機源的萃取器，computational min-entropy，學習線性函數

Abstract

Randomness has become a useful resource in computer science. However, random sources we have access to are usually imperfect. We say that a weak source has statistical min-entropy k if every string occurs with probability at most 2^{-k}. From such weak sources, we would like to use a deterministic function, called an extractor, to extract some almost perfect randomness. During the past decade, the research about extractors for various kinds of sources has received much attention, and obtains many important results.

We first consider independent-symbol sources. A distribution $X=(X_1,...,X_n)$ over the set $[D]^n$ ($[D]=\{1,2,...,D\}$) is a (n,D,k)-source if the n symbols $X_1,...,X_n$ are independent, and the min-entropy of X is k. Lee et. al. [LLT06] proposed an extractor for independent-symbol sources, which can be seen as a random walk on a graph. We observe that the corresponding matrix of each step in this random walk is a circulant matrix. We simplify the analysis of the extractors using the properties of circulant matrices, and obtain a better bound.

We also study the task of deterministically extracting randomness from sources containing computational entropy. The sources we consider have the form of a conditional distribution $(f(X)|X)$, for some function f and some distribution X, and we say that such a source has computational min-entropy k if any circuit of size 2^k can only predict f(x) correctly with probability at most 2^{-k} given input x sampled from X. We first show that it is impossible to have a seedless extractor to extract from one single source of this kind. Then we show that it becomes possible if we are allowed a seed which is weakly random (instead of perfectly random) but contains some statistical min-entropy, or even a seed which is not random at all but contains some computational min-entropy. This can be seen as a step toward extending the study of multi-source extractors from the traditional, statistical setting to a computational setting. We reduce the task of constructing such extractors to a problem in learning theory: learning linear functions under arbitrary distribution with adversarial noise. For this problem, we provide a learning algorithm, which may have interest of its own.

Keywords: independent-symbol sources，circulant matrix，two-source extractor，computational min-entropy，learning linear functions

(一) 研究計畫之背景

I. 萃取器 (Extractors)

隨機性(Randomness)已被證實在資訊科學(computer science)的許多領域都是非常有用的。舉個例子來說，在密碼學上，我們常使用隨機性來隱藏秘密，以避免在傳輸的過程中被第三者竊聽而洩露資訊。此外，在許多情況下，使用隨機演算法(probabilistic algorithm)比我們已知的傳統決定性演算法(deterministic algorithm)在時間以及空間的複雜度(time and space complexity)上來的更有效率[MR95, Gol98]。而這些隨機演算法都需要使用所謂的"真正的隨機元(truly random bits)"。不幸地，在真實的世界中並不存在真正的隨機元，因此，我們只能退而求其次地使用一個決定性的函數(deterministic function)從一些可取樣的弱隨機源(weak random sources)中萃取出真正的隨機元，其中，弱隨機源所能保證的事只有任一個字串出現的機率都不會非常高。如果我們說一個弱隨機源的 statistical min-entropy 為 k 則表示每個字串出現的機率都不會超過 2^{-k}，直觀地我們認為這樣的弱來源"包含" k 個隨機元。

1988 年時，Chor 等人證明不存在一個決定性的函數(deterministic function)可以從單一個 statistical min-entropy < n 的弱隨機源中萃取出一個隨機元[CG88]。於是，研究者們試圖在單一個弱隨機源外，再加上一個很短(相較於弱隨機源的長度)的真正隨機元，以萃取出隨機元。我們稱這個很短的真正隨機元為種子(seed)，而這種萃取器為種子萃取器(seeded extractor)。在近幾十年來，國內外的理論學家們都致力於建造出使用最少種子，而能從各種弱隨機源中萃取出非常靠近真正隨機元的種子萃取器，如[ILL89、Zuc97、RSW00、RVW00、TSZS01、TSUZ01]等。最後終於造出了幾近完美的種子萃取器[LRVW03]。

然而在使用種子萃取器時，我們仍然需要種子，其為一些真正的隨機元。在一些應用中，我們可以解決此問題(比如在解隨機 BPP 問題中列舉所有可能的種子)，而在其他應用中，則又回歸到最初的問題: 如何獲得一些真正的隨機元呢? 這個爭議讓學者們轉而建造不需種子輔助的萃取器，即決定性萃取器(deterministic extractors or seedless extractors)。

當弱隨機源擁有某些特殊的性質時，我們確實可以從一個隨機源中萃取隨機元。一個(n, k)-固定某些位元的來源 (A (n,k)-bit fixing source) 為一個在 $\{0,1\}^n$ 的分布 $X=(X_1,\cdots,X_n)$，其中 n-k 個位元是固定的，而其餘的 k 個位元則是均等的(uniform)且彼此獨立的(independent)。Kamp 等人[KZ03]提出從一個固定某些位元的來源中萃取出一些隨機元的方法，而 Gabizon 等人則在 2004 年提出改進的方法使之萃取出幾乎所有隨機源所含的隨機性[GRS04]。

此外，我們亦可從兩個甚至多個弱隨機源中不使用種子而直接萃取出很靠近均等分布(uniform distribution)的隨機元。針對兩個弱隨機源，研究者們致力於放寬對此兩個隨機源的 statistical min-entropy 的限制[CG88、DO03、DEOR04、LLTT05、Raz05]，最後，Bourgain 造出只要兩個 statistical min-entropy 均略小於 n/2 的弱隨機源即可萃取出Ω(n)個隨機元的萃取器[Bou05]。而另一方面，理論學家們也設法從越少個且含有越少 statistical min-entropy 的隨機源中萃取出隨機元[BIW04、BKS+05、Raz05]。

事實上，固定某些位元的來源以及多個隨機源的來源可以下列觀點看成是兩種極端。這兩種來源均包含多個部分而且這些部份彼此都是獨立的。固定某些位元的來源可看成是包含許多個部份，且每個部分只有單一個隨機或者為固定的位元。而多個隨機源的來源則可看成包含相對少數個部份，可是每個部份為多個位元且含足夠數量的隨機元。本計劃考慮一個介於其中的來源，稱為獨立

符號的來源(independent-symbol source)，寫成 (n,D,k)-來源，其為一個在$[D]^n$($[D]=\{1,2,...,N\}$)上的分布$X=(X_1,\cdots,X_n)$，其中$X_1,\cdots,X_n$是彼此獨立的，且 X 的 min-entropy 是 k。 我們不難看出一個(n, k)-固定某些位元的來源其實就是一個(n,2,k)-來源。換句話說，固定某些位元的來源只是我們所考慮的獨立符號來源的一個特例。而對較小的 n 及較大的 D，此種來源即可涵蓋多個隨機源的來源。Kamp 等人[KRVZ06]及 Lee 等人[LLT06]均提出從一個獨立符號來源中萃取出幾乎所有隨機性的萃取器。

II. Computational min-entropy

在過去的文獻中，大多是考慮那些在統計上仍有隨機性(亦即 statistical min-entropy 不為 0)的隨機源。在本計劃中，我們將換個角度，考慮那些在統計上並不具有任何的隨機性，但在那些計算複雜度有所限制的觀察者而言仍有些許隨機性的隨機源。換句話說，我們將從傳統的統計觀點，轉換為計算觀點。由於這些隨機源在統計上本就不具任何的隨機元，因此我們也必須將萃取器的輸出限制稍作修改。相對於在原本的定義中，我們要求萃取器的輸出要在統計上(亦即不限制計算複雜度的觀察者眼中)極靠近真正的隨機元，現在我們只要求這些輸出在那些計算複雜度有限的觀察者眼中看似隨機即可。值得注意的是，這些輸出有可能在統計上是距離真正隨機元極遠的，甚或是根本不具任何隨機性的。事實上，在密碼學中，尤其是有關利用 one-way functions 建造 pseudo-random generators 的研究中，已經有一些隱含的結果存在[Yao82, GL89, HILL99]。

何謂"看似隨機"呢? 事實上，已經有一個非常好的"看似幾乎隨機"的定義[Yao82]，但關於一個隨機源"看來有些隨機"的定義以及衡量此隨機源中隨機性之測量值的定義仍不清楚。目前有一些看似合理的定義，但目前已有些證據可以證明這些定義之間有不一致之處[BSW03, HLR07]。

III. 學習 parity 函數的演算法(Algorithms for learning parity functions)

在計算學習理論(computational learning theory)中，學習 parity 函數是一個最基本的問題。令$x=(x_1,\cdots,x_n)\in\{0,1\}^n$，則一個 parity 函數是一個對某個$T\subseteq\{1,2,\cdots,n\}$的函數$f(x)=\bigoplus_{i\in T}x_i$。在此學習模型(learning model)中，我們有一個想學習的函數$f:\{0,1\}^n\to\{0,1\}$，以及一個在$\{0,1\}^n$上的分佈 W，從中我們可以取樣 w 並獲得訓練樣本(training example)(w,q(w))，其中 q 為某個函數。如果我們得到的樣本都是正確的，亦即$q(w)=f(w),\forall w$時，則我們可以對 W 作多次取樣後利用所獲得的訓練樣本作高斯消去法(Gaussian elimination)則可獲得我們想要學習的函數 f。但是當我們所獲得的樣本可能被雜訊影響而變得不一定正確時，如何從此種模型中學習函數 f 就變成一個具有挑戰性的問題了。一般廣被討論的是以下的兩種雜訊模型: 隨機雜訊(random noise)跟對手雜訊(adversarial noise)。在隨機雜訊的模型中，針對每一個訓練樣本都是獨立的並且最多有η的機率使得 q(w)≠f(w)。而在對手雜訊的模型中則是當 w 是依照分布 W 所取樣時，最多有η比例的 w 使得 q(w)≠f(w)。不難看出，隨機雜訊模型要比對手雜訊模型更容易分析。另外，對手雜訊的模型亦可看成是不可知的模型(agnostic model)[KSS94]，而此種模型確實符合我們在現實生

活中所可能遭遇的現象。

針對在隨機雜訊模型中學習一個有 n 個變數的 parity 函數且$\eta \le 1/2-\Omega(1)$的問題，目前最好的結果為 Blum, Kalai,和 Wasserman[BKW03]於 2003 年提出的一個需要$2^{O\left(\frac{n}{\log n}\right)}$個樣本且時間複雜度為$2^{O\left(\frac{n}{\log n}\right)}$的演算法，更值得一提的是此演算法對任何分布 W 都是有效的。而在對手雜訊模型中，此問題跟條列解碼(list decode) Hadamard codes 有關。然而目前已知的結果都只能作用在 W 為一個均等分布的情況[GL89, FGKP06]。最近，Feldman 等人[FGKP06]証明當 W 為一個均等分布時，則可以利用針對隨機雜訊模型的演算法來造出針對對手雜訊模型的演算法。因此利用上述[BKW03]的演算法，則可以得到一個需要$2^{O\left(\frac{n}{\log n}\right)}$個樣本且時間複雜度為$2^{O\left(\frac{n}{\log n}\right)}$的演算法，但其中 W 為一個均等分布。

（二）研究目的

一、探討循環矩陣(circulant matrices)與獨立符號來源萃取器的特性與關係

[LLT06] 中針對獨立符號來源的萃取器即是利用在一個圖形上作隨機散步（random walk）的方法來萃取隨機元。我們發現在此隨機散步中每一步所對應的矩陣為一個特殊的矩陣，稱為循環矩陣(circulant matrix)[Dav79]，其為一個形式為$P=\begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ p_n & p_1 & \cdots & p_{n-1} \\ \vdots & \vdots & & \vdots \\ p_2 & p_3 & \cdots & p_1 \end{pmatrix}$的矩陣，其中$\sum_i p_i = 1$。我們希望能利用已知的關於循環矩陣的特性來簡化針對獨立符號來源萃取器的分析，並希望能獲得一個更好的結果。

二、建造出針對 computational min-entropy 的隨機源的萃取器:

在本計劃中，我們考慮採用[HLR07]中的定義來計算一個隨機源在計算上的隨機量。我們在這裡所考慮的來源是一個條件的型式(f(X)|X)，其中 X 是一個在$\{0,1\}^{n_1}$的分布，而$f:\{0,1\}^{n_1}\to\{0,1\}^{n}$為某個函數。假設當輸入是依照分布 X 所產生時，任何大小為2^k的電路最多只有2^{-k}的機率可以猜對 f 的函數值時，則我們說這種條件分布(f(X)|X)擁有 computational min-entropy k。當 f 是一個決定性的函數時，亦即 f(x)的值完全由 x 所決定，則當給定 x 之後，f(x)並不具有任何在統計上的隨機性。然而，依照我們的定義，只要函數 f 是很難計算的，則(f(X)|X)還是可以擁有很大的 computational min-entropy，使得我們可以從中萃取隨機元。更準確地說，從一個分佈 f(X)中，我們希望能萃取出一些隨機性，

使得即使在給定 X 時，這些隨機性在某些大小的電路看來幾乎是非常隨機的。

我們首先會考慮是否可以從單一個只擁有 computational min-entropy 的隨機源中萃取出隨機元。

接下來，由於已經知道如何從兩個擁有 statistical min-entropy 的隨機源的萃取出隨機元，本計劃考慮放寬對隨機源的限制，試著從一個擁有 statistical min-entropy 以及另一個只擁有 computational min-entropy 的兩個隨機源中萃取出隨機元。跟著我們進一步放寬對隨機源的限制，希望能從兩個都只擁有 computational min-entropy 的隨機源中萃取出隨機元。

(三) 研究方法與結果

A. 利用循環矩陣的特性來簡化針對獨立符號來源萃取器的證明:

由於在[LLT06]中的隨機散步其每一步所對應的矩陣即為一個循環矩陣(circulant matrix)，且此種矩陣的特徵向量 (eigenvectors) 是互相垂直的，我們即可利用此矩陣的特徵值 (eigenvalues) 來幫助我們證明每走一步後所得到的分布都會比原先的分布更接近均等分布，且得到一個比[LLT06]更好的結果。更精確地說，我們考慮在$\mathbb{Z}_M$上做隨機散步，目前的分布為 $P=(P_1, \ldots, P_M)$, $U=(1/M, \ldots, 1/M)$為均等分布，而利用一個 min-entropy 為 k 的來源 X_i 走一步隨機散步之後所得到的分布為 P'。在[LLT06]中，我們可以證明

$$\|P'-U\|_2^2 \le \|P-U\|_2^2 \cdot \left(1-\frac{k}{4M^2 \log D}\right) \le \|P-U\|_2^2 \cdot e^{-\frac{k}{4M^2 \log D}}.$$

然而，利用循環矩陣的特性，我們可以證明

$$\|P'-U\|_2^2 \le \|P-U\|_2^2 \cdot e^{-2\frac{2^{2k}-1}{M^2-1}}.$$

B. 建造出針對擁有 computational min-entropy 的隨機源的萃取器:

我們首先利用隨機方法證明無法從單一個長度為 n，computational min-entropy 為 n-2 的隨機源中萃取出隨機元，即使我們僅希望萃取出一個隨機元。

接著我們考慮[LLTT05]中針對兩個弱隨機源的萃取器 $Ext:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$，其中 m|n。在[LLTT05]中，我們把任何一個 $v \in \{0,1\}^n$，看成一個 ℓ-dimensional vector $(v_1,\ldots,v_l)$，其中 ℓ=n/m，而定義 $Ext(x,y) \equiv \langle x,y \rangle_m = \sum_i x_i \cdot y_i \pmod m$。我們希望能證明對任何一個只擁有 computational min-entropy 的隨機源(V|X)與另一個擁有 statistical min-entropy 的隨機源 W，任何的小電路都無法分辨$(X,W,\langle V,W \rangle_m)$以及$(X,W,U)$。我們利用反證法，假設存在一個小電路可以分辨$(X,W,\langle V,W \rangle_m)$以及$(X,W,U)$。則可以推得會存在一台推測器 (predictor)

Q 使得對許多的(x,v)，給定 x,w 之後，Q 有足夠的機率可以猜對$\langle v,w\rangle_m$的值。給定一對此種(x,v)，我們希望能有足夠的機率可以從 x 猜對 v。而這個問題可以轉化成由一些有誤差的訓練樣本，即(w,q(w))其中 q(w)=Q(x,w)，中學習一個線性函數$\langle v,\cdot\rangle_m$的問題。對此，我們建造了一個可以輸出所有可能的線性函數之學習演算法(詳見項目(三)C.)。最後我們從這些可能的線性函數中隨機選一個當我們的輸出，我們可以證明此輸出所包含的函數並不會太多，因此有足夠的機率會猜中正確的 v，而這就會跟(V|X)有足夠 computational min-entropy 的假設相矛盾。由以上的方法，我們可以證明[LLTT05]中的萃取器可以從一個擁有 computational min-entropy 為$k_1 = n-k+O(k/\log k)$的隨機源與另一個擁有 statistical min-entropy 為 k 的隨機源中萃取出隨機元。

最後我們考慮由兩個只擁有 computational min-entropy 的隨機源萃取出隨機元。我們發現如果一個隨機源 (W|Y) 擁有 computational min-entropy k，則 W 所擁有的 statistical min-entropy 至少為 k。經由以上的觀察，我們就可以利用上述的証明方式證明[LLTT05]的萃取器亦可從一個擁有 computational min-entropy 為$k_1 = n-k+O(k/\log k)$的隨機源與另一個擁有 computational min-entropy 為 k 的隨機源中萃取出隨機元。

C. 利用任何分布來學習一個線性函數

給定任何一個 statistical min-entropy 為 k 的隨機源 W，我們提出一個需要 $K=2^{O(k/\log k)}$ 個訓練樣本(w,q(w))，時間複雜度為$2^{n-k+O(k/\log k)}$，且有很大機率會輸出一個包含所有滿足$\Pr_{w\in W}[q(w)\neq v(w)]\le 1-2^{-O(\sqrt{k/\log k})}$的線性函數 v 的學習演算法。我們注意到，把 v 看成$(v_1,\ldots,v_\ell)$，則每一個訓練樣本(w,q(w))，可以給我們一個線性方程式$w_1v_1+\ldots+w_\ell v_\ell=q(w)$，所以我們的問題可以轉化成是去解一個有$2^{O(k/\log k)}$個方程式的線性方程組$[W^{(0)}|q^{(0)}]$，其中 $W^{(0)}$是一個 $K\times\ell$ 的矩陣，而$q^{(0)}$是一個 K-dimensional vector，且滿足對每一個訓練樣本(w,q(w))，$W^{(0)}$有一列為 w，而$q^{(0)}$有一個元素為 q(w)。我們的學習演算法包含兩個階段: Forward phase (如 Figure 1) 和 Backward Phase (如 Figure 2)，其中 d=k/mT，而 T 及 L 為適當的參數。

Figure 1: FORWARD PHASE

1. For t from 1 to T do
   (a) Partition the equations of $[W^{(t-1)}|q^{(t-1)}]$ into at most 2^{md} groups according to their first blocks in $W^{(t)}$ (same block value in the same group).
   (b) Within each group, randomly select an equation which we call pivot.
   (c) Within each group, subtract each equation by the pivot.
   (d) Remove the pivots and delete the first block from each equation. Let $[W^{(t)}|q^{(t)}]$ be the resulting system of equations.

Figure 2: BACKWARD PHASE

1. Set $V^{(T)} = \mathbb{F}^{(n-k)/m}$, and set $V^{(t)} = \emptyset$ for $0 \le t \le T-1$.
2. For t from $T-1$ down to 0 do
   (a) For any $z \in \mathbb{F}^d \times V^{(t+1)}$ which is δ_t-good for $[W^{(t)}|q^{(t)}]$, include z into $V^{(t)}$ if $|V^{(t)}| \le L$, and break otherwise.
3. Output $V^{(0)}$.

最後我們證明任何一個滿足 $\Pr_{w\in W}[q(w)\neq v(w)]\le 1-2^{-O(\sqrt{k/\log k})}$ 的 v 都有足夠的機率會被包含在 $V^{(0)}$ 中，而我們可以經由重複以上過程多次且輸出所有 $V^{(0)}$ 之聯集的方法來提高此成功機率。

計畫成果自評

一、我們利用循環矩陣的特性來簡化針對獨立符號來源萃取器的證明並獲得一個更好的結果。

二、由計算的角度，我們發現無法從一個只擁有 computational min-entropy 的隨機源中萃取出一個隨機元。

三、我們能證明[LLTT05]所提出的針對兩個弱隨機源的萃取器也是一個針對兩個只擁有 computational min-entropy 的隨機源的萃取器。

四、我們提出一個可利用任何分布來學習線性函數的學習演算法。

已完成的論文

- C.J. Lee, C.J. Lu, S.C. Tsai. Extracting Computational Entropy and Learning Noisy Linear Functions. COCOON 2009.

参考文献

[BIW04] B. Barak, R. Impagliazzo, and A. Wigderson. Extracting Ranodmness from Few Independent Sources. FOCS 2004.

[BKS+05] B.Barak, G. Kindler, R. Shaltiel, B. Sudakov, A. Wigderson. Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers and Extractors. In *Proc. 37th STOC*. ACM, 2005.

[BKW03] A. Blum, A. Kalai, and H. Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. J. ACM, 50(4):506-519,2003.

[BSW03] B. Barak, R. Shaltiel, and A. Wigderson. Computational Analogues of Entropy. In RANDOM-APPROX 2003, 200-215.

[Bou05] J. Bourgain. More on the sum-product phenomenon in prime fields and its applications. International Journal of Number Theory, 1:1-32, 2005.

[CG88] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. SIAM Journal on Computing. 17(2):230-261, 1988.

[Dav79] P. J. Davis. Circulant matrices. John Wiley, 1979.

[DO03] Y. Dodis, R. Oliveira. On Extracting Private Randomness over a Public Channel. RANDOM-APPROX 2003, 252-263.

[DEOR04] Y. Dodis, A. Elbaz, R. Oliveira, R. Raz. Improved Randomness Extraction from Two Independent Sources. RANDOM-APPROX 2004.

[FGKP06] V. Feldman, P. Gopalan, S. Khot, and A. K. Ponnuswami. New results for learning noisy parities and halfspaces. In Proc. 47th IEEE Symposium on Foundations of Computer Science(FOCS'06), 2006.

[GL89] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In Proc. 21st Annual ACM Symposium on Theory of Computing (STOC'89),1989.

[Gol98] O. Goldreich. Modern Cryptography, Probabilistic Proofs and Pseudorandomness. Springer-Verlag, Algorithms and Combinatorics, 1998.

[GRS04] A. Gabizon, R. Raz and R. Shaltiel. Deterministic extractors for bit-fixing sources by obtaining an independent seed. In Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, 2004.

[HILL99] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. SIAM J. Comput., 28(4):1364--1396, 1999.

[HLR07] C. Y. Hsiao, C. J. Lu, and L. Reyzin. Conditional computational entropy, or toward separating pseudoentropy form compressibility. In Proc. Advances in Cryptology-EUROCRYPT07, 2007.

[ILL89] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudorandom generation from one-way functions. In Proceedings of the 21st ACM Symposium on Theory of Computing, 1989.

[KRVZ06] J. Kamp, A. Rao, S. Vadhan, and D. Zuckerman. Deterministic Extractors

for Small-Space Sources. In Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC '06), pages 691-700, May 2006.

[KSS94] M. Kearns, R. Schapire, and L.Sellie. Toward efficient agnostic learning. Machine Learning, 17(2/3): 115-142, 1994.

[KZ03] J. Kamp and D. Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. In Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, 2003.

[LLTT05] C. J. Lee, C. J. Lu, S. C. Tsai, and W. G. Tzeng. Extracting randomness from n independent weak random sources. IEEE Transactions on Information Theory (SCI), 51(6) 2224-2227, 2005.

[LLT06] C. J. Lee, C. J. Lu, and S. C. Tsai, Deterministic extractors for independent-symbol sources. In Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP), pages 84-95, 2006.

[LRVW03] C. J. Lu, O. Reingold, S. Vadhan, and A. Wigderson. Extractors: Optimal up to Constant Factors. In Proceedings of the 35th ACM Symposium on Theory of Computing, pages 601-611, 2003.

[MR95] R. Motwani and P. Raghavan. Randomized algorithms. Cambridge University press, 1995.

[Raz05] R. Raz. Extractors with Weak Random Seeds. Proceeding of the 37th STOC, 2005, pp. 11-20.

[RSW00] O. Reingold, R. Shaltiel, and A. Wigderson. Extracting randomness via repeated condensing. In Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science, 2000.

[RVW00] O. Reigold, S. Vadhan, and A. Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science, 2000.

[TSUZ01] A. Ta-Shma, C. Umans, and D. Zuckerman. Loss-less condensers, unbalanced expanders, and extractors. In Proceedings of the 33rd Annual ACM Symposium on Theory of Computing, 2001.

[TSZS01] A. Ta-Shma, D. Zucherman and S. Safra. Extractors from Reed-Muller codes. In Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science, 2001.

[Yao82] A. Yao. Theory and applications of trapdoor functions. In Proc. 23rd Annual Symposium on Foundations of Computer Science (FOCS'82), 1982.

[Zuc97] D. Zuckerman. Randomness-optimal oblivious sampling. Random Structures and Algorithms, 11:345-367, 1997.