On the impact of cryptographic thinking on TCS and beyond

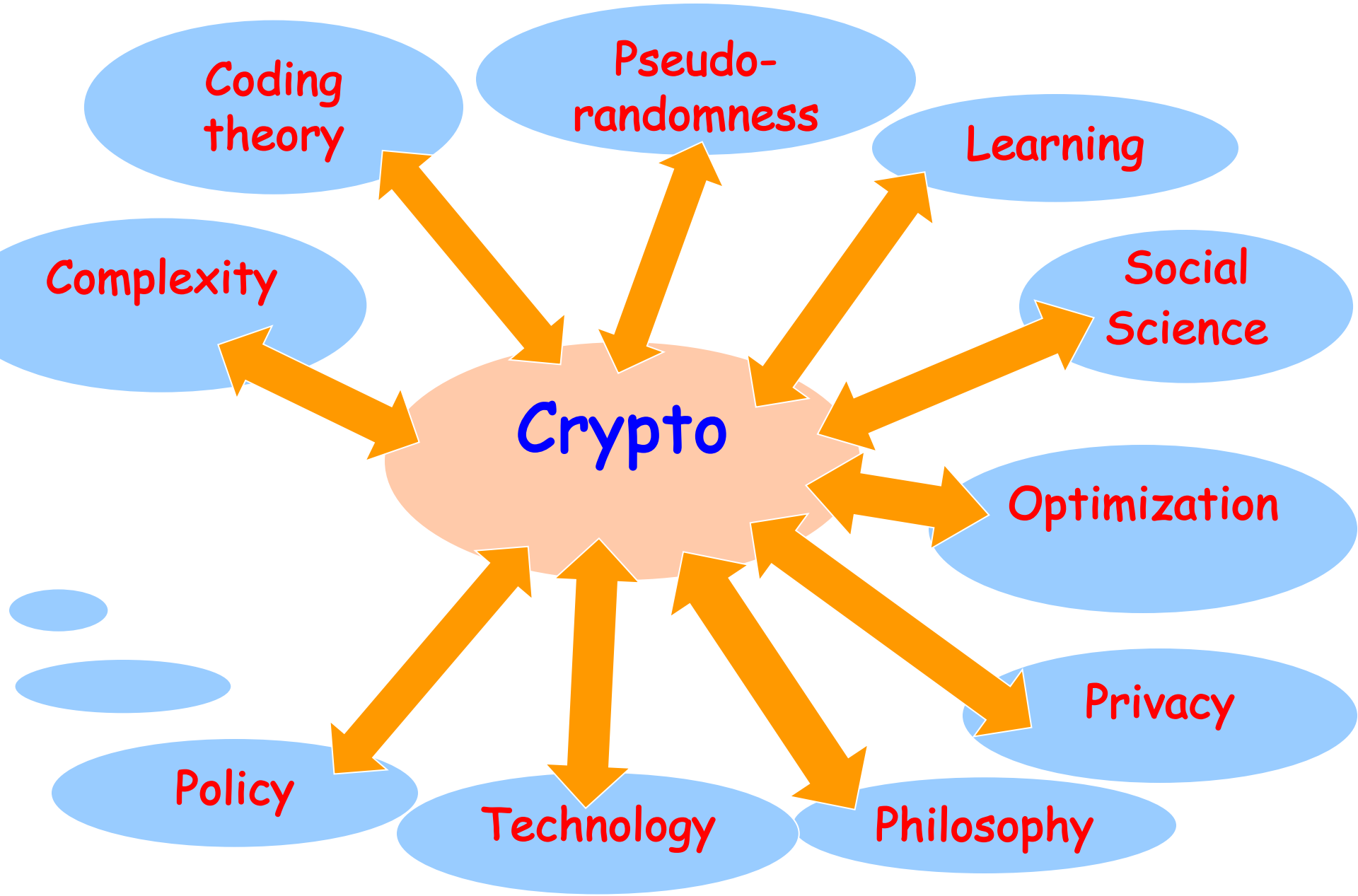
Avi Wigderson
Institute for Advanced Study

Reflection

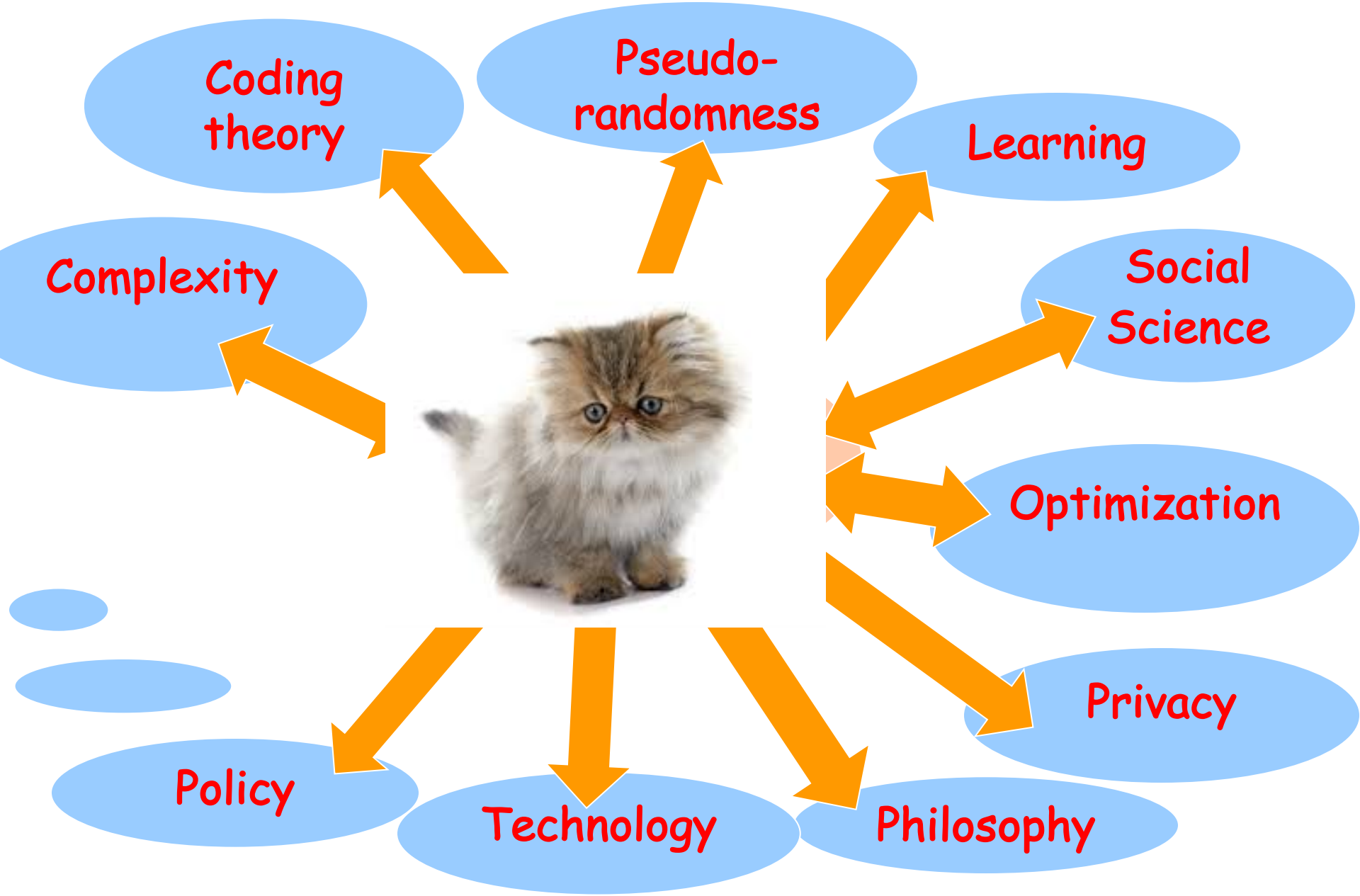
Long time since my crypto days (so there may be a bias on older examples; there are many newer ones!)

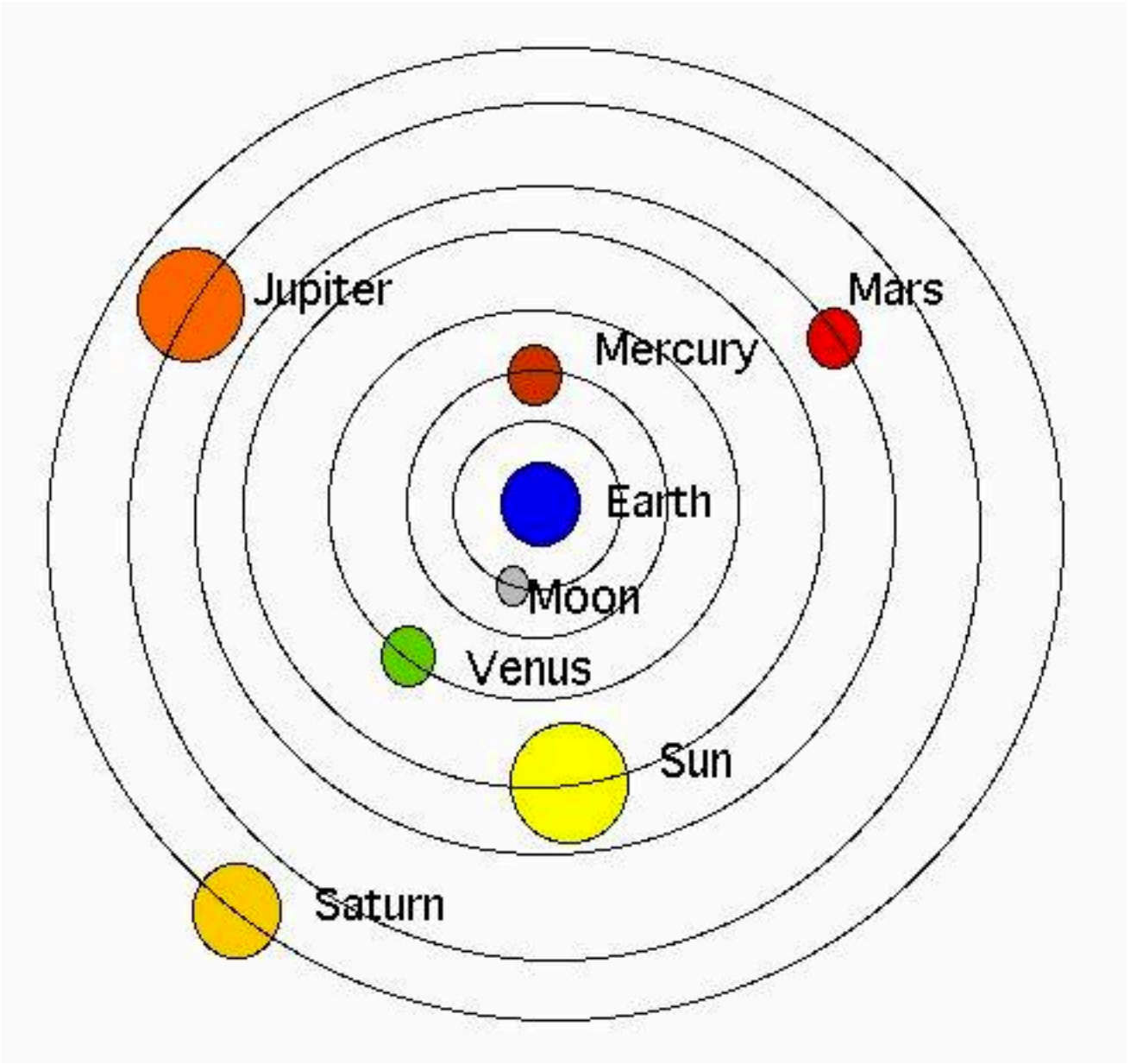
Crypto had a formative impact on my scientific development (so I am biased to giving it credit)

I could easily give other talks on outside impact on crypto (but not today)



Matches made in heaven


Coding theory
Pseudo-randomness
Learning
Complexity
Social Science
Optimization
Privacy
Policy
Technology
Philosophy



Ptolemy's geocentric model

On the impact of cryptographic thinking on TCS and beyond

Many examples

Spirit

Crazy 80's motto of crypto:

Impossible? Let's do it!

- PKCs, Signatures
- Exchanging secrets
- Joint coin flipping
- Oblivious transfer
- Poker over the telephone
- …

Still goes on and on:

- Signatures from 1-way fns
- Non-BB ZK
- Non-malleable encryption
- Homomorphic encryption
- Obfuscation
- …

General

Modeling: CS is a modeling science.
Crypto may be the most prolific.

Reductions: TCS is the art of reduction!
Crypto is probably the toughest testbed.

Adversarial thinking:
[Kerckhoff'1883] [Shannon'1949] "One ought to design (crypto-) systems assuming that the enemy will immediately gain full familiarity with them."
Everywhere in Algorithms and Complexity, impact on Statistics, Optimization, Control Theory,...

Randomness

Crypto → High level understandings

- Randomness is a resource
- Pseudo-randomness
- Hardness vs. randomness

Pseudo-randomness

Randomness is a resource!
Statistics, Probabilistic algorithms,…
PRGs, Statistical tests [Knuth vol. 2]

[Vernam'17] One-Time Pad: Long random string
[Shamir'81] Short random seed →(det)→ Long OTP

Computational-based pseudo-randomness
[Shamir'81,Blum-Micali'82,Yao'82….] [Sipser'79]
If you cannot tell it apart from random, it is random!

Computational indistinguishability
Modern crypto, PR generators, PR objects,…

Derandomization

[Blum-Micali'81, Yao'82]

∃ Trapdoor fn ➔ BPP ⊆ DTIME (exp(n^{ϵ}))

Hardness ➔ Deandomization

[Ajtay-W'85] Unc

[Nisan'88] Far

[Nisan-W'88] Co

∃ Hard fn for C ➔

Different settings

[Reingold'05] SL=L

Paradigm: det. alg design

Converse?? [Tell'18]

[Kabanets-Impagliazzo'00]

[Impagliazzo-W'88,...] Tighter connections

E ⊄ Subexp/poly ➔ BPP = P

Hardness amplification

Worst-case to average-case

- RSR (Random self-reducibility)
- Arithmetization

XOR lemmas

Random self-reducibility

Crypto needs average-case hardness!
When worst-case hardness ➔ avg-case hardness?

Discrete logarithm mod p (g generator of $(Z_p)^*$)

Assume efficient $A(g^y) = y$ whp over random y.
Given g^x , pick random r, compute $A(g^x g^r)-r = x$ whp

What other functions can we do this for?
Quadratic residuosity mod N=pq

[Ajtai'96] Finding short vertors in lattices
[Regev'05] LWE (Learning With Errors)
➔ Cryptosystems

Arithmetization

$h:\{0,1\}^n \to \{0,1\}$ hard in worst case
h multilinear polynomial over any field F
$h^*: F^n \to F$ hard on average! (interpolation)

[Lipton'89]
[Blum-Kannan'89] Program checking

[Beaver-Feigenbaum'90]
Instance hiding ([Shamir'79] secret sharing)

Avalanche… IP=PSPACE, MIP=NEXP, PCP=NP,…

Worst-case vs. Avg-case for NP-complete problems?

XOR lemmas

Amplifying error probability → $\frac{1}{2}$ (constructing hard-core bit, reducing advantage over random guess)

Info-theoretic inspiration – reducing coin bias

$\Pr[X] < \frac{1}{2}(1+\delta) \Rightarrow \Pr[X \oplus Y] < \frac{1}{2}(1+\delta^2)$ X,Y indep, $\delta \in (0,1)$

[Yao'82,Levin'82] $f:\{0,1\}^n \to \{0,1\}$, $X=f(x)$, $Y=f(y)$

$\Pr[C(x) \text{ predicts } X] < \frac{1}{2}(1+\delta) \Rightarrow |C| < s$

$\Pr[C'(x,y) \text{ predicts } X \oplus Y] < \frac{1}{2}(1+\delta^2+\epsilon) \quad |C'| < \epsilon s$

Many different proofs, many computational settings

Crypto, PRGs, Algorithms, Circuit complexity, PCPs..

Coding Theory ← Crypto

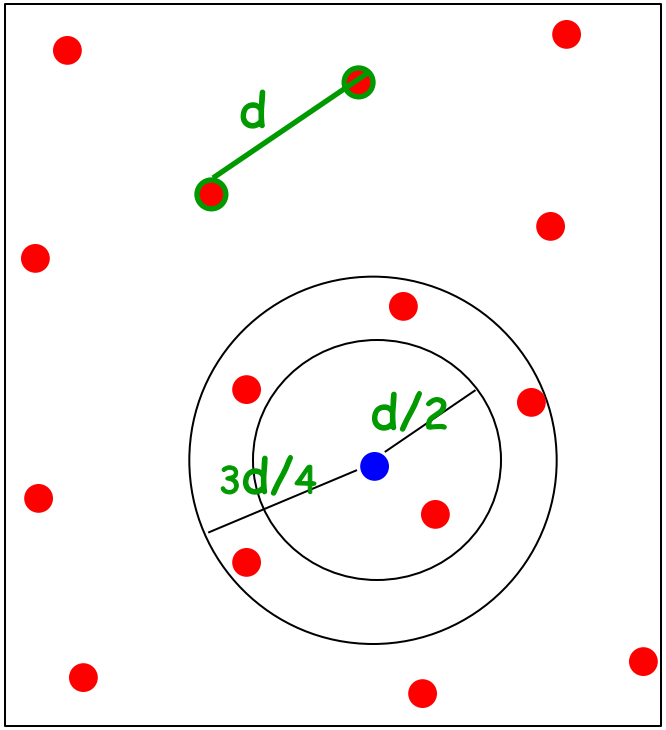
Error-correcting codes:
protecting communication from noise

- List decoding
- Local decoding

Naturally arose in crypto – new twist

Huge impact, great interaction
between TCS and Coding/Info theory

List decoding

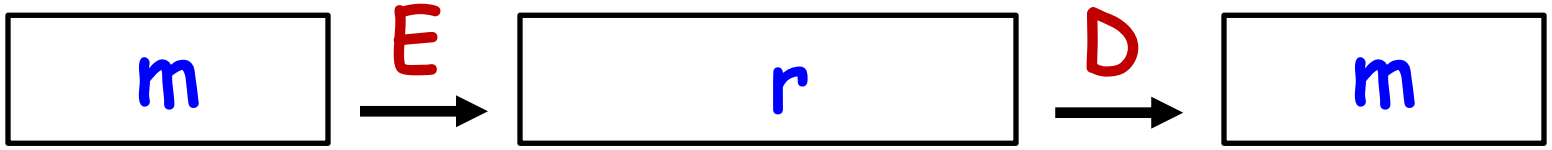


Unique decoding: one
[Elias'57] List decoding: few
Combinatorial bounds

[Goldreich-Levin'89] Crypto:
Efficient construction of a hard-core bit
([Elias] = list decoding of Hadamard codes)

→ Algorithms+tight bounds for many codes
→ Crypto, Extractors, PCPs, Complexity…

Local decoding



Global decoding: $m=D(r)$, $time(D)=poly(|r|,|m|)$

Crypto motivations: hard-core bit, program testing, arithmetization, …. $|r|,|m| \sim exp(n)$

Local decoding $time(D)<poly(n)=polylog(|r|,|m|)$

$\forall i\ m_i = D(r_{j1}, r_{j2},\dots, r_{jq})$, $1<q<n$ D randomized!

→ Local Testing, Property Testing, Sub-linear Algs →Statistics, Opt, Streaming, Big-Data,…

Gleaning global properties from a small samples

Interactive proofs

Written proofs:
Math: proof systems, proof theory
CS: NP, NEXP, RE,…

Probabilistic
Interactive proofs: Allow more power and new properties of proofs, impossible in written ones!

- IP Single prover
- MIP Many provers
- Delegation: "efficient" provers
- Quantum analogs

IP → computational complexity

[Goldwasser-Micali-Rackoff'85]
Define IP to capture crypto interactions tasks (+ZK)

IP as a complexity class – can it prove more than NP

[Lund-Fortnow-Karloff-Nisan'90, Shamir'91]
IP = PSPACE (use arithemtization)

[Babai'85] (motivated by group theory problems)
Defined *Arthur-Merlin games:* (IP with public coins)

→ [Goldwasser-Sipser'86] public coins = private coins
→ Classes MA, AM (constant rounds), just above NP

MIP → computational complexity++

[BenOr-Goldwasser-Kilian-W'88]
Defined MIP (for cryptographic reasons)

MIP as a complexity class – what can it prove?

[Babai-Fortnow-Lund'90] MIP = NEXP

[FRS'88, BFLS'91,AS'92,ALMSS'92] PCP = NP

[Feige-Goldwasser-Lovasz-Safra-Szegedy'90]
PCPs → Hardness of approximation
Revolution in Optimization
& Crypto & Coding & Lower bounds &...

Quantum proof systems

Both prover(s) and verifier are quantum

One prover: QIP
[Jain-Ji-Updahyay-Watrous'09]
QIP = PSPACE

Many provers: MIP* (= QMIP)
[…,Ji-Natarajan-Vidick-Wright-Yuen'20]
MIP* = RE (←→ Halting problem is equivalent to approx. the value of a non-local game!)
(→ Connes embedding conjecture in von-Neumann algebras is false!)

IP → Delegation

~~Infinitely powerful prover~~ → Efficient prover!

[Brasad-Chaum-Crepeau'86] ZK argument systems

Efficient prover, but much stronger than verifier!

Think: Program checking, Cloud computing

[Goldwasser-Kalai-Rothblum'09'] No assumptions!

TISP[poly(n),log(n)] prover, TISP[O~(n),log(n)] verifier

[Kalai-Raz-Rothblum'13]

poly(n) prover, O~(n) verifier

Think: Quantum computing

[Mahadev'18] Quantum prover, Classical verifier

Testing scientific theories…

Zero-Knowledge Proofs

- Birth of MIP
- Practical, societal, scientific impacts
- Statistical ZK

ZK ➔ MIP

[Goldwasser-Micali-Rackoff'85] IP
Define & exemplify ZK proofs

[Goldreich-Micali-W'86]
1-way functions ➔ NP ⊆ ZK

Prove NP ⊆ ZK without computational assumptions?

[BenOr-Goldwasser-Kilian-W'89] MIP
Introduce 2-prover (and multi-prover) systems.
Physical separation ➔ NP ⊆ ZK

ZK: external impacts

Inspire the imagination!

[Moni+Yael Naor, Reingold] Child education

Societal: Physical ZK proofs:

[Barak-Glaser-Goldstone'14] Nuclear disarmament

[Fisch-Freund-Naor] Anonymous DNA testing,…

Physics: Quantum SZK proofs:

[Harlow-Hayden'13] Black-hole firewall paradox,…

Integrating complexity into scientific theories

Practical ZK proofs:

- Anonymous cash, Blockchains, Public ledgers …

Computational models ➔ Info-theoretic models

(the counterintuitive direction)

- Completeness theorems
- Full information models

Completeness theorems

[Yao'86,Goldreich-Micali-W'87] (computational)

Assume < n/2 players are bad.

∃ Trapdoor fns ➔ Every n-player crypto task has a private and secure protocol

Most basic primitive: Pairwise private communication ➔ "Everything"

(info-theoretic)

[BenOr-Goldwasser-W'88, Chaum-Crepeau-Damgard'88]

Assume < n/3 players are bad.

Pairwise private channels ➔ Every n-player function has a private and secure protocol

Distributed computation (other networks)

Techniques → Simpler (LWE based) hom encryption

Full information model

What if you do not even assume private comm?
What if everyone knows everything?

Coin flipping/elections/leader election →
[BenOr –Linial'86,…]
Influences of players in Boolean functions.
→ Game theory, Analysis of Boolean functions

Completeness thms→
[Linial-Goldwasser-Goldreich'95]
Fault-tolerant computation in the full information model.

Crypto →
Social science, Policy, Law

Differential Privacy
→ adaptive data analysis

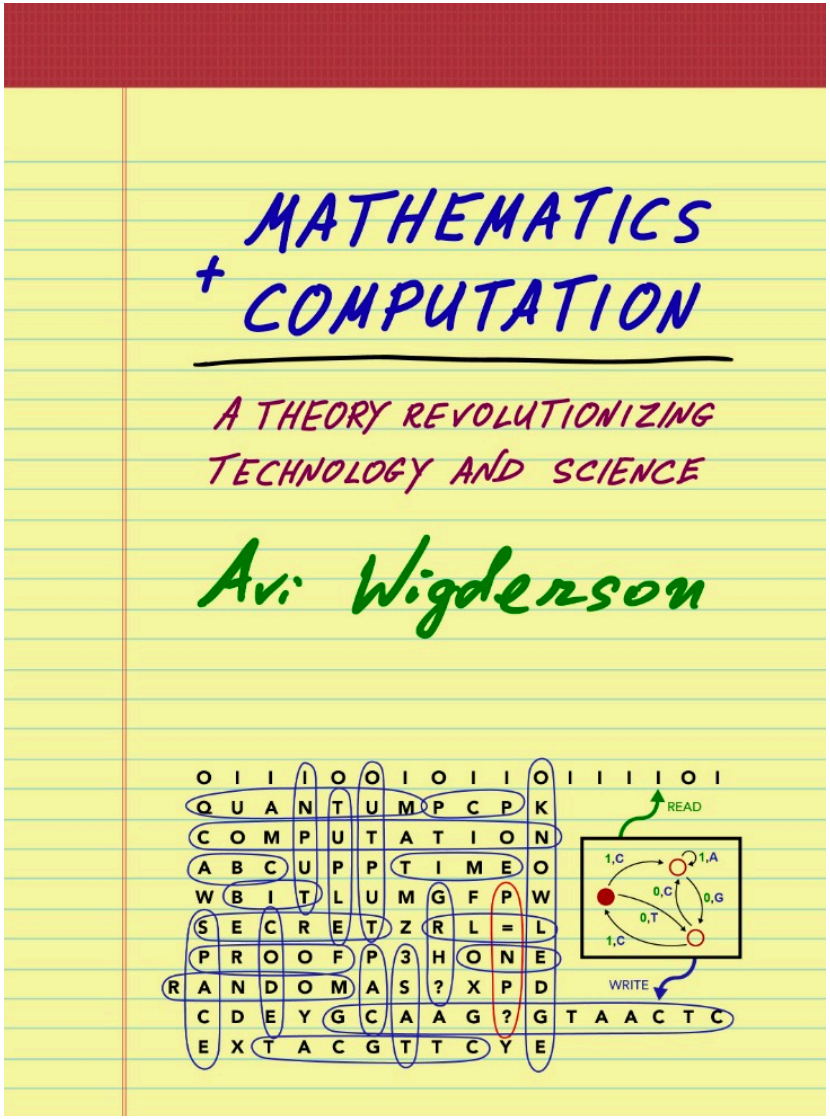
Fairness of algorithms
→ …

Crypto → Philosophy

Collusion
Interaction
Knowledge
Privacy
Proof
Randomness
Simultaneity
Secret
Verification
…

Novel, formal meanings & uses

Book ad



- Published by Princeton University Press

- Free (forever) on my website

- Comments welcome!