Computational-Statistical Bit-Security

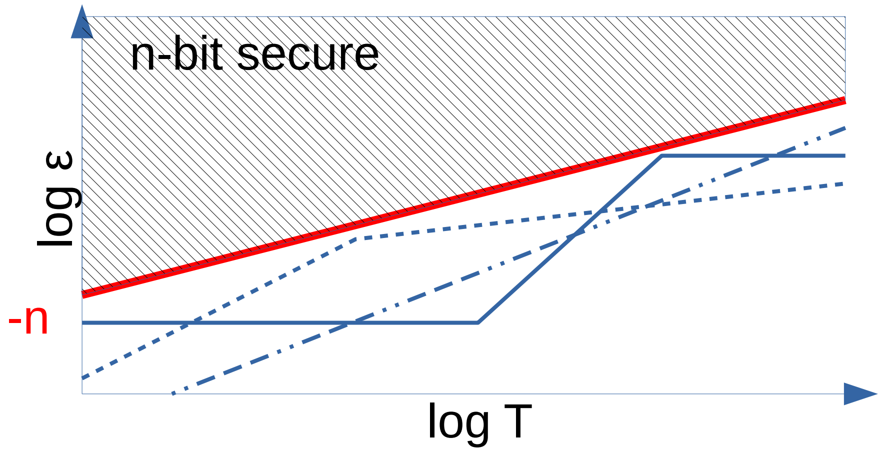
Daniele Micciancio
Mark Schultz-Wu

(UC San Diego)

Theory of Cryptography Conference – TCC 2024
December 2024

Quantifying Security

- Security of cryptography is measured in “bits”
  - e.g., 128-bit secure, 256-bit secure, etc.
  - Intuition: cost of brute force attack on n-bit key
- Formal definition for search problems:
  - Adversary A
  - $\varepsilon(A) = \Pr\{A = k\}$
  - $T(A)$ = Runtime/Cost
  - $T(A)/\varepsilon(A) \geq 2^n$

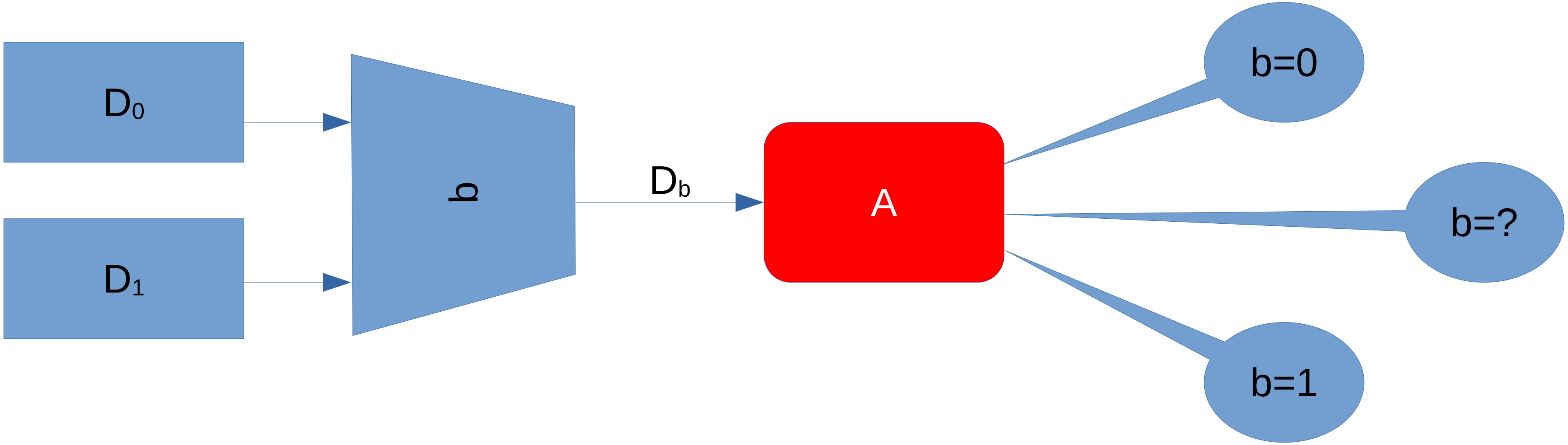


What about decision problems?

- Distinguishing games:
  - goal: recover secret bit $b \in \{0,1\}$
  - PRG, PRF, IND-CPA, IND-CCA, ZK, ….
- $T(A)/\delta$ for $\delta=(2\varepsilon-1)= \varepsilon-(1-\varepsilon)$ does not work:
  - G(x) can be more secure as PRG than as OWF
  - against intuition that PRG is a stronger security requirement than OWF
- Is there a better definition for δ?

Bit-security of decision problems

- First formal definition: [**M.**,Walter'18]
  - Uses $\delta=(\varepsilon-\varepsilon')^2/(\varepsilon+\varepsilon')$ [Levin], where ε' = Pr{A=(1-b)}
  - Adversaries can output 0,1 or "?", so $\varepsilon+\varepsilon'\leq 1$



Follow up work

- [Watanabe,Yasunaga’21,’23]
  - Alternative definition with “operational interpretation”
  - Does not need “?” output symbol
- [Lee’24],[WY’24],[Veliche,Aggarwal,Ming’24]
- Applications:
  - [Abla,Liu,Wang,Wang’21]: IBE
  - [Li,**M.**,Sorrell,**S.**’22]: approximate FHE

Our work

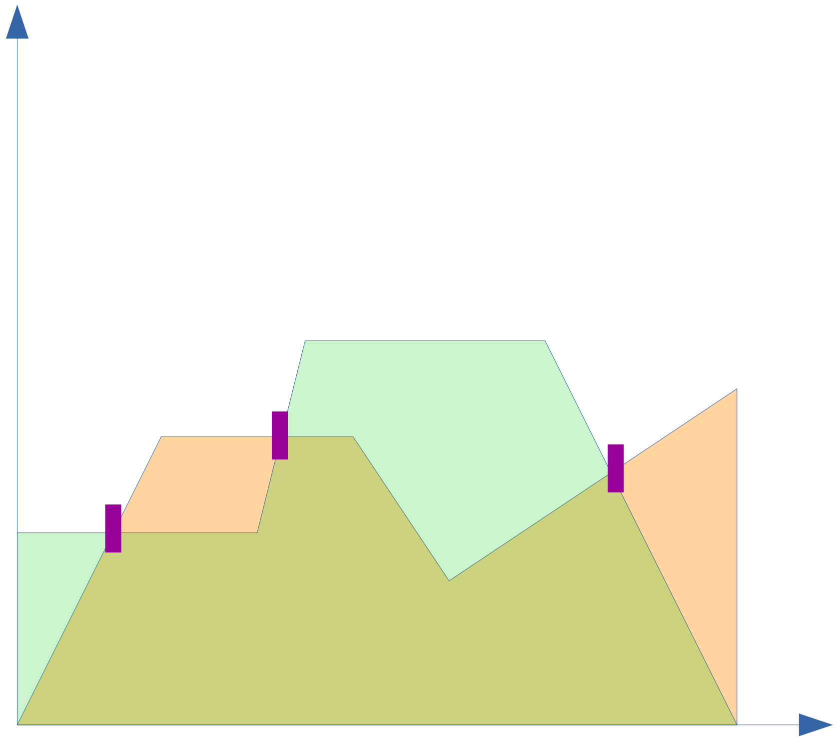
- Characterize optimal statistical adversaries
- Clarify equivalence of MW and WY definition
- Toolbox for (c,s)-security [LMSS'22]
  - Distribution replacement theorem
  - (c,s)-hybrid argument
- Techniques: fuzzy adversaries
  - Output $\sigma \in [-1,1]$: decision=sign(σ), confidence=$|\sigma| \in [0,1]$
  - Still equivalent to "aborting" MW {0,1,?}-adversary

Statistical security

- Statistical (aka, information theoretic) security:
  - Small ε(A) , regardless of running time T(A)
  - unconditional: no computational assumptions!
  - easier to analyze
- Related to dissimilarity between distributions
  - Total Variation (TV) distance
  - KL diveregence, Renyi divergence, etc.
  - Hellinger distance
- Implies computational security

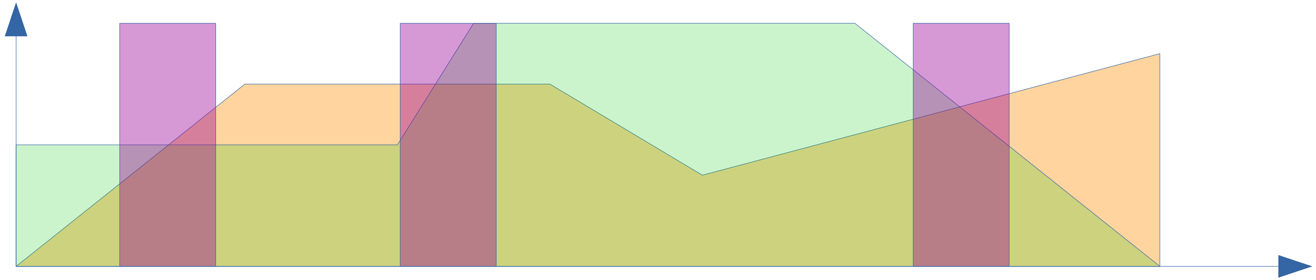
Optimal (statistical) distinguisher

- x ← D[0] or D[1]
- A(x)= 0 or 1
  - D[A(x)]≥D[1-A(x)]
- A(x) = 0, 1 or ?
  - When should A output ?
  - D[0]=D[1]
  - D[0]≈D[1], but how close?



Structure of Optimal Distinguisher

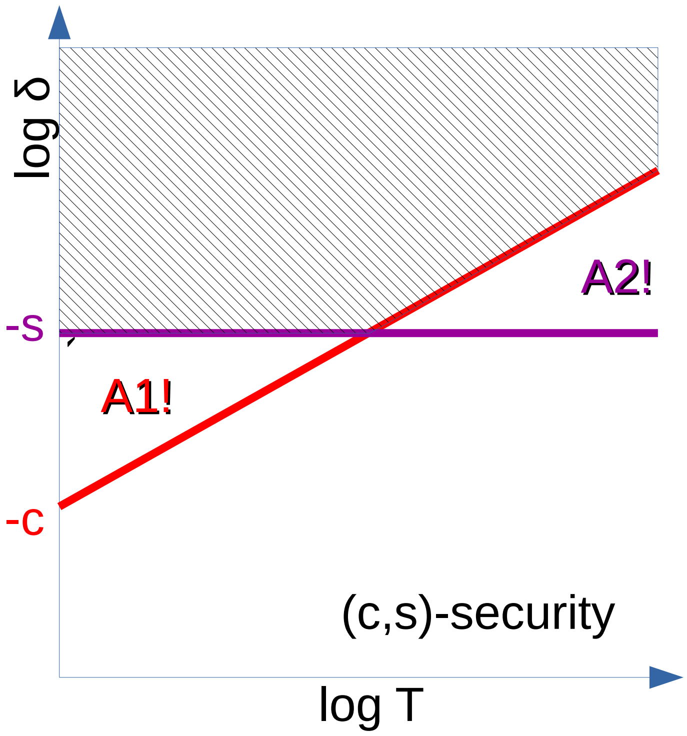
- WLOG, may assume A is deterministic
  - may seem obvious, but it is a convexity property
- Optimal A is a “threshold” adversary
  - Output ? if $|\log \Pr\{D0\} - \log \Pr\{D1\}| < \tau$
  - $\tau = \log(4/(3-2\varepsilon^*) - 1) \le \log 3$, where $\varepsilon^*=\varepsilon/(\varepsilon+\varepsilon')$



Computational/Statistical security

- [LMSS'21] (c,s)-security:

  for all
  - either $\delta(A) \leq 2^{-s}$
  - or $T(A)/\delta(A) \geq 2^{c}$
- Note: a function can be
  - neither c-bits comp. security, nor 2-bits stat. secure
  - and still be (c,s)-secure



Distribution replacement

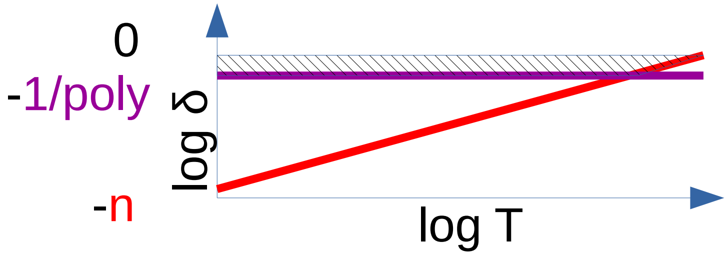
- Let $G^X = (G_0^X, G_1^X)$ be a decision game parametrized by a distribution X
  - If G^X is (c,s)-secure, and
  - (X,Y) are (c,s)-indistinguishable
  - then G^Y is also (c',s')-secure, for c'≈c, s'≈s
- E.g., X easy to analyze, Y easy to sample
- Generalizes previous results which assumed
  - (X,Y) are statistically close [MW18]
  - (X,Y) are computationally indistinguishable [Y21]

Hybrid argument

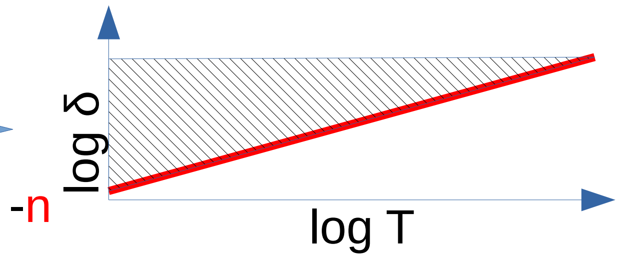
- Sequence of games H_0, H_1, … ,H_n
  - If (H_i,H_{i+1}) are (c,s)-indistinguishable,
  - then (H_0,H_n) are (c',s')-indistinguishable
- E.g., construction achieving (H_0,H_n)-security using several cryptographic primitives
  - Each (H_i,H_{i+1}) is proved using one of the primitives
  - Some primitives are computationally c-bit secure
  - Others are statistically s-bit secure

Relation to other talks

- [WY’24] hardness amplification

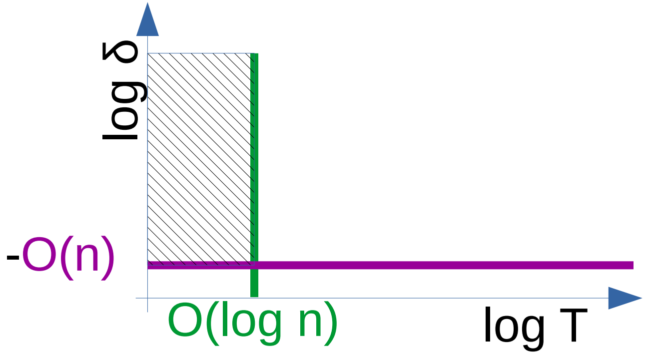


weak unpredictabilty = (n,1/poly(n))-security



strong unpredictabilty = (n,n)-security

- [VAM’24]:
  - assumes $T \leq poly(n)$
  - shows $\delta \leq exp(-n)$



Conclusion

- Bit security (in all its c, s and (c,s) flavors)
  - useful, both in theory and practice
  - usable, not much harder than traditional proofs
- TODO: use it!

Questions?