Computational Entropy: Recent results and applications

Leonid Reyzin

June 24, 2015
Bertinoro, Italy
Entropy

Entropy of a single value \( w = \log (\text{surprise}) = \log \frac{1}{\Pr[w]} \)

\[= -\log \Pr[w]\]

Shannon entropy: average of log (surprise) = \[-\mathbb{E} \log \Pr[w] \]

\( w \in W \)

(measures compressibility of iid strings of symbols from \( W \),
because each element can be compressed to its entropy)
guessability and entropy

There are many ways to measure entropy

Q: If I want to guess your hidden value (password/plaintext) which entropy do I care about?

A: minentropy = $- \log \left( \text{Pr [adversary predicts sample]} \right)$

$$H_\infty(W) = - \log \max_w \text{Pr}[w]$$

(we’ll briefly consider other notions later)
what is minentropy good for?

• Passwords
• Message authentication
**what is minentropy good for?**

- Passwords
- Message authentication

**Key**

\[ w = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{GF}(2^{n/2}) \times \mathbb{GF}(2^{n/2}) \]

**MAC**

\[ \text{MAC}_{a,b}(m) = \sigma = am + b \]

[Wegman-Carter ‘81]
what is minentropy good for?

- Passwords
- Message authentication

Let $|a,b| = n$, $H_\infty(a,b) = k$

Let “entropy gap” $n - k = g$

Security: $k - n/2 = n/2 - g$ [Maurer-Wolf ‘03]
what is minentropy good for?

- Passwords
- Message authentication: \( \text{MAC}_{a,b}(m) = \sigma = am + b \)
- Secret key/randomness extraction (\( \Rightarrow \) encryption, etc.)

\[ \text{minentropy } k \]

\[ w \rightarrow \text{Ext} \rightarrow R \]

\[ \text{seed } i \]

reusable

jointly uniform (\( \epsilon \)-close)

note two different views of extractors

[Santha-Vazirani 1986,…]:

poor quality randomness $w$ → Ext → indistinguishable from uniform

[Wyner 1975,…]:

randomness $w$ (maybe uniform) → Ext → indistinguishable from uniform given leakage

What is the right value for $H_\infty(W)$ in this case?

Lemma: $H_\infty(W | Y = y) \geq H_\infty(W) - \log 1/\Pr[y]$ 

So we can measure it for each $y$… but we don’t know $y$
defining conditional entropy $H_\infty(W \mid Y)$

- E.g., $W$ is uniform over $\{0,1\}^n$, $Y =$ Hamming Weight($W$)
  
  $\Pr[Y = n/2] > 1/(2\sqrt{n}) \Rightarrow H_\infty(W \mid Y = n/2) \geq n - \frac{1}{2} \log n - 1$
  
  $\Pr[Y = n] = 2^{-n} \Rightarrow H_\infty(W \mid Y = 0) = n - n = 0$

- But what about $H_\infty(W \mid Y)$?

- Recall: minentropy $= - \log$ (predictability)
  
  $H_\infty(W) = - \log \max_W \Pr[w]$

- What’s the probability of predicting $W$ given $Y$?
  
  $H_\infty(W \mid Y) = - \log \mathbb{E} \max_Y \Pr[w \mid Y=y]$ 

  “average minentropy” but not average of minentropy:
  
  if min-entropy is 0 half the time, and 1000 half the time, you get $\log (2^0 + 2^{-1000})/2 \approx - \log 1/2 = 1$. [Dodis-Ostrovsky -R-Smith ‘04]
defining conditional entropy $H_{\infty}(W \mid Y)$

- E.g., $W$ is uniform over $\{0,1\}^n$, $Y = \text{Hamming Weight}(W)$
  
  $\Pr[Y = n/2] > 1/(2\sqrt{n}) \implies H_{\infty}(W \mid Y = n/2) \geq n - \frac{1}{2} \log n - 1$
  
  $\Pr[Y = n] = 2^{-n} \implies H_{\infty}(W \mid Y = 0) = n - n = 0$

- But what about $H_{\infty}(W \mid Y)$?

- Recall: minentropy $= - \log \text{(predictability)}$
  
  $H_{\infty}(W) = - \log \max_{W} \Pr[w]$

- What’s the probability of predicting $W$ given $Y$?

  $H_{\infty}(W \mid Y) = - \log \mathbb{E} \max_{y} \Pr[w \mid Y = y]$

  [Dodis-Ostrovsky -R-Smith ‘04]

Lemma: $H_{\infty}(W \mid Y = y) \geq H_{\infty}(W) - \log 1/\Pr[y]$
defining conditional entropy $H_\infty(W \mid Y)$

- E.g., $W$ is uniform over $\{0,1\}^n$, $Y = \text{Hamming Weight}(W)$
  \[
  \text{Pr}[Y = n/2] > 1/(2\sqrt{n}) \Rightarrow H_\infty(W \mid Y = n/2) \geq n - \frac{1}{2} \log n - 1
  \]
  \[
  \text{Pr}[Y = n] = 2^{-n} \Rightarrow H_\infty(W \mid Y = 0) = n - n = 0
  \]

- But what about $H_\infty(W \mid Y)$?

Thm: if $Y$ is over $\{0,1\}^b$, then $H_\infty(W \mid Y) \geq H_\infty(W) - b$
what is $H_{\infty}(W \mid Y)$ good for?

- **Passwords**
  - Prob. of guessing by adversary who knows $Y$: $2^{-H_{\infty}(W \mid Y)}$

- **Message authentication**
  - If key is $W$ and adversary knows $Y$: security $= H_{\infty}(W \mid Y) - n/2$

- **Secret key/randomness extraction ($\Rightarrow$ encryption, etc.)**
  - All extractors work [Vadhan ‘11]

$$H_{\infty}(W \mid Y) = k$$

- $w$ to $\text{Ext}$
- seed $i$ to $\text{Ext}$
- $R$ from $\text{Ext}$

jointly $\epsilon$-close to uniform given $Y$
If (conditional) min-entropy is so useful in information-theoretic crypto, what about computational analogues?
**computational entropy (HILL)**

Min-Entropy

\[ H_\infty(W) = -\log \max_{w \in W} \Pr[w] \]

[Håstad, Impagliazzo, Levin, Luby]:

\[ H_{\delta,s}^{\text{HILL}}(W) \geq k \text{ if } \exists Z \text{ such that } H_\infty(Z) = k \text{ and } W \approx_{\delta,s} Z \]

Two more parameters relating to what \( \approx \) means

-- maximum size \( s \) of distinguishing circuit \( D \)

-- maximum advantage \( \delta \) with which \( D \) will distinguish
what is HILL entropy good for?

$H^{\text{HILL}}_{\delta, s}(W) \geq k$ if $\exists Z$ such that $H_{\infty}(Z) = k$ and $W \approx_{\delta, s} Z$

- Many uses: indistinguishability is a powerful notion.
- In the proofs, substitute $Z$ for $W$; a bounded adversary won’t notice

$$H_{\infty}(W) = |x|$$

$$H^{\text{HILL}}(W) = |w|$$
what is HILL entropy good for?

\[ H^{\text{HILL}}_{\delta, s}(W) \geq k \text{ if } \exists Z \text{ such that } H_\infty(Z) = k \text{ and } W \approx_{\delta, s} Z \]

- Many uses: indistinguishability is a powerful notion.
- In the proofs, substitute \( Z \) for \( W \);

a bounded adversary won’t notice

\[ \text{HILL entropy } k \]

\[ \hat{w} \quad \text{Ext} \quad R \]

\[ \text{seed } i \]

looks \((\varepsilon + \delta)\)-close to uniform to circuits of size \( s \)
what about conditional?

\[ H_{\delta,s}^{\text{HILL}}(W) \geq k \text{ if } \exists Z \text{ such that } H_{\infty}(Z) = k \text{ and } W \approx_{\delta,s} Z \]

Very common:

- entropic secret: \( g^{ab} \) | observer knows \( g^a, g^b \)
- entropic secret: \( SK \) | observer knows leakage
- entropic secret: \( \text{Sign}_{SK}(m) \) | observer knows \( PK \)
- entropic secret: \( \text{PRG}(x) \) | observer knows \( \text{Enc}(x) \)
**how does conditioning reduce HILL entropy?**

\[
H_{\delta,s}^{\text{HILL}}(W) \geq k \text{ if } \exists Z \text{ such that } H_{\infty}(Z) = k \text{ and } W \approx_{\delta,s} Z
\]

Recall min-entropy:

\[
H_{\infty}(W \mid Y = y) \geq H_{\infty}(W) - \log \frac{1}{\Pr[y]}
\]
**how does conditioning reduce HILL entropy?**

\[ H_{\delta,s}^{\text{HILL}}(W) \geq k \text{ if } \exists Z \text{ such that } H_{\infty}(Z) = k \text{ and } W \approx_{\delta,s} Z \]

Recall min-entropy:

\[ H_{\infty}(W \mid Y = y) \geq H_{\infty}(W) - \log \frac{1}{\Pr[y]} \]

**Theorem** [Fuller O’Neill-R’12] same holds for computational entropy:

\[ H_{\delta/\Pr[y],s}^{\text{metric*}}(W \mid Y = y) \geq H_{\delta,s}^{\text{metric*}}(W) - \log \frac{1}{\Pr[y]} \]

(variant of Dense Model Theorem of [Green-Tao ‘04, Tao-Ziegler ‘06, Gowers ‘08, Reingold-Trevisan-Tulsiani-Vadhan ‘08, Dziembowski-Pietrzak ’08, Zhang ‘12, Vadhan-Zheng ‘13])

**Warning:** this is not \( H_{\text{HILL}} \)!

Weaker entropy notion: a different \( Z \) for each distinguisher

\[ H_{\delta,s}^{\text{metric*}}(W) \geq k \text{ if } \forall \text{ distinguisher } D \exists Z \text{ s.t. } H_{\infty}(Z) = k \text{ and } W \approx_{D,Z} \]

(moreover, \( D \) is limited to deterministic [0,1] distinguishers)

It can be converted to \( H_{\text{HILL}} \) with a loss in circuit size \( s \)

[Barak-Shaltiel-Wigderson ‘03, Vadhan-Zheng ‘12, Skórski ’15]
how does conditioning reduce HILL entropy?

Long story, but simple message:

\[ H_{\delta/\Pr[y],s}^{\text{metric}*} (W | Y = y) \geq H_{\delta,s}^{\text{metric}*} (W) - \log 1/\Pr[y] \]

It can be converted to \( H^{\text{HILL}} \) with a loss in circuit size \( s \)

necessary [Pietrzak-Skórski’16]

[Barak-Shaltiel-Wigderson ‘03, Vadhan-Zheng ’12, Skórski ’15]
what is $H^{HILL}(W \mid y)$ good for?

Deterministic Encryption

• Usual PK encryption is randomized
  (two ciphertexts of the same plaintext will be different)

• Problem: building deterministic public-key encryption
  (makes encrypted search much easier, for example)

• Shouldn’t be possible: adversary can guess-and-test $m$

• Possible if $m$ comes from distribution $M$ that has entropy!
  [Bellare-Boldyreva-O’Neill ’07]

• Security defn: can compute as much without $c$ as with $c$
  as long as $H_\infty(M)$ is high enough
what is $H^{HILL}(W \mid y)$ good for?

Deterministic PK Encryption (secure if $m$ has entropy)

- How to build from normal encryption?

  $$m \rightarrow r \rightarrow PK \rightarrow r \rightarrow Enc \rightarrow c$$

- Idea: get $r$ from $m$, because $m$ has entropy
- Tool: trapdoor function $f$ (e.g., RSA) with hardcore bits

  $$x \rightarrow f \rightarrow f(x) \leadsto x \text{ can be recovered given } f^{-1}$$
  $$hc \leadsto r \text{ looks uniform given } f(x)$$
**what is $H^{HILL}(W | y)$ good for?**

Deterministic PK Encryption

- How to build from normal encryption?

  $$\begin{align*}
  m & \rightarrow \text{Enc} \\
  r & \rightarrow \text{Enc} \\
  PK & \rightarrow \text{Enc}
  \end{align*}$$

- Idea: get $r$ from $m$, because $m$ has entropy
- Tool: trapdoor function $f$ (e.g., RSA) with hardcore bits

$$\begin{align*}
  x & \rightarrow f \\
  hc & \rightarrow f(x) \\
  & \rightarrow r
  \end{align*}$$
what is $H^{\text{Hill}}(W \mid y)$ good for?

Deterministic PK Encryption

• How to build from normal encryption?

\[ m \rightarrow r \rightarrow PK \]
\[ \text{Enc} \rightarrow c \]

• Idea: get $r$ from $m$, because $m$ has entropy

• Tool: trapdoor function $f$ (e.g., RSA) with hardcore bits

\[ x = m \rightarrow f \rightarrow f(x) \rightarrow hc \rightarrow r \rightarrow PK \rightarrow \text{Enc} \rightarrow c \]

• Add $f$ to $PK$, $f^{-1}$ to $SK$
what is $H^{HILL} (W \mid y)$ good for?

Deterministic PK Encryption

Problem: $r$ may reveal parts of $m$ and Enc doesn’t hide $r$

Need: “robust” $hc$ to hide input — i.e., looks uniform for $M \mid y$, $\forall y$ with $\Pr[y] \geq \frac{1}{4}$.

(follows from “indistinguishability implies semantic security”)

Construction of robust $hc$ [Fuller-O’Neill-R ‘12]:
what is $H^{HILL}(W | y)$ good for?

Proof of robust $hc$ construction

Need: “robust” $hc$ to hide input — i.e., looks uniform for $M | y$, $orall y$ with $\Pr[y] \geq \frac{1}{4}$.
what is $H^{HILL}(W \mid y)$ good for?

Proof of robust $hc$ construction

Need: “robust” $hc$ to hide input — i.e., looks uniform for $M \mid y$, $\forall y$ with $Pr[y] \geq \frac{1}{4}$. 
what is $H^{HILL}(W | y)$ good for?

Proof of robust $hc$ construction

$M \rightarrow f \rightarrow f(M) \rightarrow r$

has true entropy

know: looks uniform given $f(M)$
what is $H^{HILL} (W \mid y)$ good for?

Proof of robust $hc$ construction

\[ M \rightarrow_{hc} f \rightarrow f(M) \rightarrow r \]

has HILL entropy
what is $H^{\text{HILL}} (W \mid y)$ good for?

Proof of robust $hc$ construction

$M \mid y \rightarrow f \rightarrow f(M \mid y)$

$hc \rightarrow r$

has HILL entropy, but reduced by $\Pr[y]$ (computational leakage lemma)
what is $H^{\text{HILL}}(W | y)$ good for?

Proof of robust $hc$ construction

Proof:

$\begin{align*}
M | y & \xrightarrow{hc} r \\
 & \xrightarrow{f} f(M | y)
\end{align*}$

has HILL entropy even given $f(M | y)$

(information-theoretic leakage lemma)
what is $H^{HILL}(W|y)$ good for?

Proof of robust $hc$ construction

know: has HILL entropy conditioned on $f(M|y)$

hence: looks uniform given $f(M|y)$

so Ext works!

Q.E.D.
what about conditioning on average?

<table>
<thead>
<tr>
<th>entropic secret: $g^{ab}$</th>
<th>observer knows $g^a, g^b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>entropic secret: $SK$</td>
<td>observer knows leakage</td>
</tr>
<tr>
<td>entropic secret: $\text{Sign}_{SK}(m)$</td>
<td>observer knows $PK$</td>
</tr>
<tr>
<td>entropic secret: $\text{PRG}(x)$</td>
<td>observer knows $\text{Enc}(x)$</td>
</tr>
</tbody>
</table>

Again, we may not want to reason about specific values of $Y$. 
average computational entropy

Def [Hsiao-Lu-R ‘04]:  $H_{\delta,s}^{\text{HILL}}(W \mid Y) \geq k$ if $\exists Z$ such that $H_{\infty}(Z \mid Y) = k$ and $(W, Y) \approx (Z, Y)$  
Note: $W$ changes, not $Y$

More Relaxed Def:  $H_{\delta,s}^{\text{HILL-rlx}}(W \mid Y) \geq k$ if $\exists Z, T$ s.t. $H_{\infty}(Z \mid T) = k$ and $(W, Y) \approx (Z, T)$

(more permissive; seems sufficient for known applications)

Can similarly define metric*(-rlx): allow different $Z$ (and $T$) for each $D$, where $D$ is deterministic $[0,1]$; convert to HILL with loss in $s$

Recall: if $Y$ is over $\{0,1\}^b$, then  

$$H_{\infty}(W \mid Y) \geq H_{\infty}(W) - b$$

Theorem [Fuller-O’Neill-R ‘12]:  $H_{\delta,2^b,s}^{\text{metric*}}(W \mid Y) \geq H_{\delta,s}^{\text{metric*}}(W) - b$

Theorem [Pietrzak-Skórski’15]:  $H_{\delta, s/2i^b,2^b}^{\text{metric*}}(W \mid Y) \geq H_{\delta,s}^{\text{metric*}}(W) - b$
chain rule

Def [Hsiao-Lu-R ‘04]: $H_{\delta,s}^{\text{HILL}}(W \mid Y) \geq k$ if $\exists Z$ such that $H_{\infty}(Z \mid Y) = k$ and $(W, Y) \approx (Z, Y)$ Note: $W$ changes, not $Y$

More Relaxed Def: $H_{\delta,s}^{\text{HILL-rlx}}(W \mid Y) \geq k$ if $\exists Z, T$ s. t. $H_{\infty}(Z \mid T) = k$ and $(W, Y) \approx (Z, T)$

(more permissive; seems sufficient for known applications)

What about $H(W \mid X, Y) \geq H(W \mid X) - b$? (works for min-entropy!)

NO for HILL! [Krenn-Pietrzak-Wadia-Wichs’14]

YES if $Z$ is samplable given $Y$ [Chung-Kalai-Lu-Raz ’11, memory delegation]

YES for HILL-rlx


Proof: $Y$ can be simulated by $S(W)$, so $(W, X, S(W)) \approx (Z, T, S(Z))$
what is $H^{HILL}(W \mid Y)$ good for?

Suppose I am worried about side-channel attacks: some information leaks to the adversary.

Given $x$, which is uniformly distributed, we can use a Pseudorandom Generator (PRG) to produce a uniformly looking output $w$.
what is $H^{\text{Hill}} (W \mid Y)$ good for?

Suppose I am worried about side-channel attacks: some information leaks to the adversary.
Suppose I am worried about side-channel attacks: some information leaks to the adversary

\[ H^{\text{HILL}}(W | Y) \] good for?

- Used in [Dziembowski-Pietrzak '08] leakage-resilient stream cipher
- Can also be used for key derivation from weak randomness (alternative approach in [Dodis-Yu '13])

\[ H^{\text{HILL}}(W|\text{leakage}) = |w| - b \]
Suppose I am worried about side-channel attacks: some information leaks to the adversary.

**what is $H^{HILL}(W | Y)$ good for?**

Uniform-looking $w$
what is $H^{HILL} (W | Y)$ good for?

Suppose I am worried about side-channel attacks: some information leaks to the adversary

have only $H^{HILL}$ and independence

uniform $x$

key

$w_{PRF}$

uniform $b$ bits of leakage

uniform looking $w$
Suppose I am worried about side-channel attacks: some information leaks to the adversary

have only $H^{\text{HILL}}$

and independence

uniform

uniform

uniform-looking $w$

$H^{\text{HILL}}(W \mid \text{leakage})$
is high enough iterate this construction

$\bullet$ Used by [Pietrzak ‘09] leakage-resilient stream cipher

$\bullet$ See [Skórski arXiv:1505.06765] for analysis + refs to follow-up work
computational entropy and privacy

- Computational differential privacy
  [Mironov-Pandey-Reingold-Vadhan ‘09]
  – Prove two definitions of privacy equivalent using a variant of dense model theorem / leakage lemma

- Privacy of votes [Bernhard-Cortier-Pereira-Warinschi ‘12]

[Hsiao-Lu-R ‘04] Def: \( H(W \mid Y) \geq k \) if \( \exists Z \) such that \( H_\infty(Z \mid Y) = k \) and \( (W, Y) \approx (Z, Y) \)

More Relaxed Def: \( H(W \mid Y) \geq k \) if \( \exists Z, T \) such that \( H_\infty(Z \mid T) = k \) and \( (W, Y) \approx (Z, T) \)

[BCPW’12] Def: \( H(W \mid Y) \geq k \) if \( \exists T \) such that \( H_\infty(W \mid T) = k \) and \( (W, Y) \approx (Z, T) \)
unpredictability entropy

Why should computational min-entropy be defined through indistinguishability? Why not model unpredictability directly?

[Hsiao-Lu-R. ‘04]

\[ H_{s_{\text{Unp}}}(W | Z) \geq k \text{ if for all } \forall A \text{ of size } s, \Pr[A(z) = w] \leq 2^{-k} \]

Lemma: \[ H_{s_{\text{Unp}}}(W | X, Y) \geq H_{s_{\text{Unp}}}(W | X) - b \]
what is $H^{Unp}(W \mid Z)$ good for?

$H^{Unp}_s(W \mid Z) \geq k$ if for all $\forall A$ of size $s$, $\Pr[A(z) = w] \leq 2^{-k}$

Examples:

- **Diffie-Hellman**: $g^{ab} \mid g^a, g^b$
- **One-Way Functions**: $x \mid f(x)$
- **Signatures**: $Sign_{SK}(m) \mid PK$

$H^{HILL}=0$
**what is $H_{Unp}^W(Z)$ good for?**

$H^k_{Unp}(W|Z) \geq k$ if for all $\forall A$ of size $s$, $\Pr[A(z) = w] \leq 2^{-k}$

- Hardcore bit results (e.g., [Goldreich&Levin, Ta-Shma&Zuckerman]) are often stated for OWF, but work any time you have $H^k_{Unp}$

- Leakage-resilient crypto (assuming strong hardness) [Brakerski-Kalai-Katz-Vaikuntanathan ’10]

- Almost full $H^k_{Unp} \Rightarrow H^{HILL}$ [Skórski-Golovnev-Pietrzak ’15]
  - $H^k_{unp}$ can sometimes be condensed to almost full, get almost full $H^{HILL}$

- A variant of $H^k_{Unp}$ (based on KL-divergence from $W$ to $A(Z)$) $\Rightarrow$ Shannon variant of $H^{HILL}$ (when $W$ is short) [Vadhan-Zheng ‘12]
  - If $f$ is a OWF, then the version of $H^k_{unp}$ holds bitwise, for $x_i | f(x), x_1 \ldots x_{i-1}$
  - Hence, get Shannon variant of $H^{HILL}$
  - Shannon-entropy can be converted to min-entropy by parallel repetition
  - Result: PRG from OWF (simple construction, shorter seed)
the last slide

Conditional entropy is naturally everywhere
Computational conditional entropy is a natural extension

Uses so far

- Deterministic encryption
- Memory delegation
- Privacy amplification/fuzzy extractors
- Leakage-resilient crypto
- Differential privacy
- Voting
- PRGs

Field is maturing, should enable new uses
Thank you!