Equivocations, Exponents and Second-Order Rates under Various Rényi Information Measures

Vincent Y. F. Tan

Joint work with Masahito Hayashi (Nagoya University and NUS)

NUS
National University of Singapore

arXiv 1504.02536 (IT Transactions revised)

IMS Workshop on Mathematics of IT Cryptography

The Main Question We Ask

$$A^n \;\text{———}\; E^n$$

The Main Question We Ask

$$
\begin{tikzcd}
A^n \arrow[r, dash] \arrow[d, "f_n"'] & E^n \arrow[d] \\
f_n(A^n) & E^n
\end{tikzcd}
$$

The Main Question We Ask

$$
\begin{tikzcd}
A^n \arrow[r, dash] \arrow[d, "f_n"'] & E^n \arrow[d] \\
f_n(A^n) & E^n
\end{tikzcd}
$$

- Fundamental limits of applying a hash function f_n to a source A^n

The Main Question We Ask

$$
\begin{tikzcd}
A^n \arrow[r, dash] \arrow[d, "f_n"'] & E^n \arrow[d] \\
f_n(A^n) & E^n
\end{tikzcd}
$$

- Fundamental limits of applying a hash function f_n to a source A^n
- Source A^n is correlated to E^n; their joint distribution is

$$P_{AE}^n(a^n, e^n) = \prod_{i=1}^{n} P_{AE}(a_i, e_i)$$

The Main Question We Ask

$$
\begin{tikzcd}
A^n \arrow[r, dash] \arrow[d, "f_n"'] & E^n \arrow[d] \\
f_n(A^n) & E^n
\end{tikzcd}
$$

- Fundamental limits of applying a hash function f_n to a source A^n
- Source A^n is correlated to E^n; their joint distribution is

$$P_{AE}^n(a^n, e^n) = \prod_{i=1}^n P_{AE}(a_i, e_i)$$

- Information-theoretic security: After application of f_n, how independent is A^n from E^n and how uniform is it for a given rate

$$R = \frac{1}{n} \log \|f_n\|$$

Measuring Independence and Uniformity

- We can measure dependence using the mutual information

$$I(A \wedge E) = D(P_{AE} \| P_A \times P_E).$$

We take $A \equiv f(A^n)$ and $E \equiv E^n$ later.

Measuring Independence and Uniformity

- We can measure dependence using the mutual information

$$I(A \wedge E) = D(P_{AE} \| P_A \times P_E).$$

We take $A \equiv f(A^n)$ and $E \equiv E^n$ later.

- We can measure dependence and non-uniformity using the relative entropy

$$\begin{aligned} &D(P_{AE} \| P_{\mathrm{mix},\mathcal{A}} \times P_E) \\ &\quad = \log |\mathcal{A}| - H(A|E) \\ &\quad = I(A \wedge E) + D(P_A \| P_{\mathrm{mix},\mathcal{A}}) \end{aligned}$$

where $P_{\mathrm{mix},\mathcal{A}}$ is the uniform distribution on $\mathcal{A}$

Measuring Independence and Uniformity

- We can measure dependence using the mutual information

$$I(A \wedge E) = D(P_{AE} \| P_A \times P_E).$$

We take $A \equiv f(A^n)$ and $E \equiv E^n$ later.

- We can measure dependence and non-uniformity using the relative entropy

$$\begin{aligned} & D(P_{AE} \| P_{\mathrm{mix},\mathcal{A}} \times P_E) \\ & \quad = \log |\mathcal{A}| - H(A|E) \\ & \quad = I(A \wedge E) + D(P_A \| P_{\mathrm{mix},\mathcal{A}}) \end{aligned}$$

where $P_{\mathrm{mix},\mathcal{A}}$ is the uniform distribution on $\mathcal{A}$

- Csiszár and Narayan (2004) considered $D(P_{AE} \| P_{\mathrm{mix},\mathcal{A}} \times P_E)$

Measuring Independence and Uniformity

- We can measure dependence using the mutual information

$$I(A \wedge E) = D(P_{AE} \| P_A \times P_E).$$

We take $A \equiv f(A^n)$ and $E \equiv E^n$ later.

- We can measure dependence and non-uniformity using the relative entropy

$$\begin{aligned} & D(P_{AE} \| P_{\mathrm{mix},\mathcal{A}} \times P_E) \\ & \quad = \log |\mathcal{A}| - H(A|E) \\ & \quad = I(A \wedge E) + D(P_A \| P_{\mathrm{mix},\mathcal{A}}) \end{aligned}$$

where $P_{\mathrm{mix},\mathcal{A}}$ is the uniform distribution on $\mathcal{A}$

- Csiszár and Narayan (2004) considered $D(P_{AE} \| P_{\mathrm{mix},\mathcal{A}} \times P_E)$
- These are Shannon information measures

Rényi Information Measures

- The Rényi divergence of order $1+s$ is

$$D_{1+s}(P\|Q) := \frac{1}{s} \log \sum_a P(a)^{1+s} Q(a)^{-s}$$

Rényi Information Measures

- The Rényi divergence of order $1+s$ is

$$D_{1+s}(P\|Q) := \frac{1}{s}\log\sum_{a} P(a)^{1+s}Q(a)^{-s}$$

- Recover relative entropy as $s \to 0$, i.e.,

$$\lim_{s\to 0} D_{1+s}(P\|Q) = D(P\|Q).$$

Rényi Information Measures

- The Rényi divergence of order $1+s$ is

$$D_{1+s}(P\|Q) := \frac{1}{s} \log \sum_a P(a)^{1+s} Q(a)^{-s}$$

- Recover relative entropy as $s \to 0$, i.e.,

$$\lim_{s\to 0} D_{1+s}(P\|Q) = D(P\|Q).$$

- Conditional Rényi entropy 1:

$$H_{1+s}(A|E|P_{AE}\|Q_E) := -D_{1+s}(P_{AE}\|I_A \times Q_E)$$
$$H_{1+s}(A|E) := H_{1+s}(A|E|P_{AE}\|P_E)$$

- Conditional Rényi entropy 2 (Gallager form):

$$H_{1+s}^{\uparrow}(A|E) := -\frac{1+s}{s}\log\sum_{e}\left(\sum_{a}P_{AE}(a,e)^{1+s}\right)^{\frac{1}{1+s}}$$

Rényi Information Measures

- Conditional Rényi entropy 2 (Gallager form):

$$H^{\uparrow}_{1+s}(A|E) := -\frac{1+s}{s}\log\sum_e\left(\sum_a P_{AE}(a,e)^{1+s}\right)^{\frac{1}{1+s}}$$

Related to the Gallager's source coding with side-information exponent function

$$\phi(s) := \log\sum_e\left(\sum_a P_{AE}(a,e)^{\frac{1}{1-s}}\right)^{1-s}$$

See Fehr and Berens (2014) for other definitions of conditional Rényi entropies.

Rényi Information Measures

- Conditional Rényi entropy 2 (Gallager form):

$$H^{\uparrow}_{1+s}(A|E) := -\frac{1+s}{s} \log \sum_{e} \left(\sum_{a} P_{AE}(a,e)^{1+s} \right)^{\frac{1}{1+s}}$$

  Related to the Gallager's source coding with side-information exponent function

$$\phi(s) := \log \sum_{e} \left(\sum_{a} P_{AE}(a,e)^{\frac{1}{1-s}} \right)^{1-s}$$

  See Fehr and Berens (2014) for other definitions of conditional Rényi entropies.

- Easy to check that

$$\max_{Q_E \in \mathcal{P}(\mathcal{E})} H_{1+s}(A|E|P_{AE}\|Q_E) = H^{\uparrow}_{1+s}(A|E).$$

Generalized Security Rényi Information Measures

- Security measure based on Conditional Rényi entropy 1:

$$C_{1+s}(A|E) := \log |\mathcal{A}| - H_{1+s}(A|E)$$

Generalized Security Rényi Information Measures

- Security measure based on Conditional Rényi entropy 1:

$$C_{1+s}(A|E) := \log|\mathcal{A}| - H_{1+s}(A|E)$$

- Security measure based on Conditional Rényi entropy 2:

$$C^{\uparrow}_{1+s}(A|E) := \log|\mathcal{A}| - H^{\uparrow}_{1+s}(A|E)$$

Generalized Security Rényi Information Measures

- Security measure based on Conditional Rényi entropy 1:

$$C_{1+s}(A|E) := \log|\mathcal{A}| - H_{1+s}(A|E)$$

- Security measure based on Conditional Rényi entropy 2:

$$C^{\uparrow}_{1+s}(A|E) := \log|\mathcal{A}| - H^{\uparrow}_{1+s}(A|E)$$

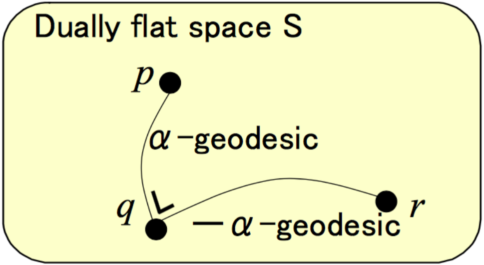
- When $s = 0$, these reduce to the information security measure based on relative entropy

$$C_1(A|E) = D(P_{AE} \| P_{\mathrm{mix},\mathcal{A}} \times P_E) = \log|\mathcal{A}| - H(A|E)$$

Remarks on Generalized Security Criteria I

Can show that

$$C_{1+s}(A|E) = I_{1+s}^{(\mathrm{Sibson})}(E \wedge A) + D_{1+s}(Q_A^{(s)} \| P_{\mathrm{mix},\mathcal{A}})$$



Generalized Pythagorean theorem in information geometry for Rényi entropy. Fig. from S. Akaho.

Remarks on Generalized Security Criteria I

- We can also show that

$$C^{\uparrow}_{1+s}(A|E) = I^{(\mathrm{Arimoto})}_{1+s}(A \wedge E) + D_{1+s}(P_A \| P_{\mathrm{mix},\mathcal{A}}).$$

Remarks on Generalized Security Criteria I

- We can also show that

$$C^{\uparrow}_{1+s}(A|E) = I^{(\mathrm{Arimoto})}_{1+s}(A \wedge E) + D_{1+s}(P_A \| P_{\mathrm{mix},\mathcal{A}}).$$

- Both these relations generalize the Shannon-theoretic relation which is attained as $s \to 0$:

$$C_1(A|E) = I(A \wedge E) + D(P_A \| P_{\mathrm{mix},\mathcal{A}}).$$

Remarks on Generalized Security Criteria I

- We can also show that

$$C^{\uparrow}_{1+s}(A|E) = I^{(\text{Arimoto})}_{1+s}(A \wedge E) + D_{1+s}(P_A \| P_{\text{mix},\mathcal{A}}).$$

- Both these relations generalize the Shannon-theoretic relation which is attained as $s \to 0$:

$$C_1(A|E) = I(A \wedge E) + D(P_A \| P_{\text{mix},\mathcal{A}}).$$

- If $C_1(A|E)$ is small A is approximately independent of E and A is close to uniform.

Motivations for Generalized Security Measures

- Iwamoto and Shikata (2014): Measure equivocation using these generalized security measures

Motivations for Generalized Security Measures

- Iwamoto and Shikata (2014): Measure equivocation using these generalized security measures
- Cryptography and Quantum Key Distribution (QKD), the collision entropy

  $$H_2(A) = -\log \sum_a P_A(a)^2$$

  and min-entropy

  $$H_{\min}(A) = -\log \max_a P_A(a)$$

  are important; cf. leftover hash lemma

Motivations for Generalized Security Measures

- Iwamoto and Shikata (2014): Measure equivocation using these generalized security measures
- Cryptography and Quantum Key Distribution (QKD), the collision entropy

  $$H_2(A) = -\log \sum_a P_A(a)^2$$

  and min-entropy

  $$H_{\min}(A) = -\log \max_a P_A(a)$$

  are important; cf. leftover hash lemma
- Dodis and Yu (2013): Overcoming weak expectations where bounds provided are based on Rényi entropies

Motivations for Generalized Security Measures

- Iwamoto and Shikata (2014): Measure equivocation using these generalized security measures

- Cryptography and Quantum Key Distribution (QKD), the collision entropy

$$H_2(A) = -\log \sum_a P_A(a)^2$$

and min-entropy

$$H_{\min}(A) = -\log \max_a P_A(a)$$

are important; cf. leftover hash lemma

- Dodis and Yu (2013): Overcoming weak expectations where bounds provided are based on Rényi entropies

- Error exponents for information-theoretic security problems

Families of Hash Functions

Definition

A random hash function f_X is a stochastic map from $\mathcal{A}$ to $\mathcal{M} = \{1, \dots, M\}$ where X governs the stochastic behavior of f_X.

Families of Hash Functions

Definition

A random hash function f_X is a stochastic map from $\mathcal{A}$ to $\mathcal{M} = \{1, \ldots, M\}$ where X governs the stochastic behavior of f_X.

Definition

A random hash function is called ϵ-almost universal$_2$ [Carter and Wegman (1979)] if for all distinct $a_1, a_2 \in \mathcal{A}$,

$$\Pr(f_X(a_1) = f_X(a_2)) \le \epsilon M^{-1}.$$

Families of Hash Functions

Definition

A random hash function f_X is a stochastic map from $\mathcal{A}$ to $\mathcal{M} = \{1, \ldots, M\}$ where X governs the stochastic behavior of f_X.

Definition

A random hash function is called ϵ-almost universal$_2$ [Carter and Wegman (1979)] if for all distinct $a_1, a_2 \in \mathcal{A}$,

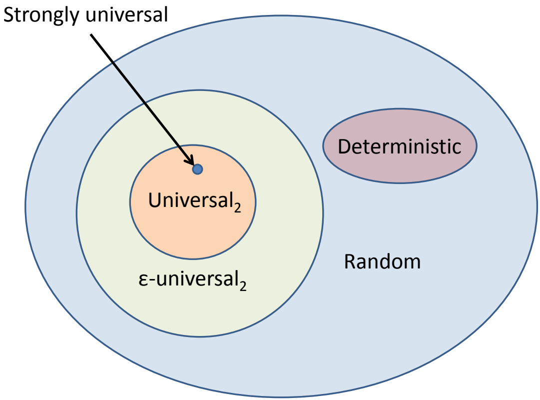
$$\Pr(f_X(a_1) = f_X(a_2)) \leq \epsilon M^{-1}.$$

Definition

A random hash function is called strongly universal when the random variables $\{f_X(a) : a \in \mathcal{A}\}$ are independent and

$$\Pr(f_X(a) = m) = M^{-1}, \quad \forall\, a \in \mathcal{A}, m \in \mathcal{M}.$$

Families of Hash Functions



Hierarchy of hash functions.

Sequences of Hash Functions

Sequence of hash functions $\{f_{X_n} : \mathcal{A}^n \to [e^{nR}]\}_{n=1}^{\infty}$

Sequence of hash functions $\{f_{X_n} : \mathcal{A}^n \to [e^{nR}]\}_{n=1}^{\infty}$

$$\begin{tikzcd}
A^n \arrow[r, dash] \arrow[d, "f_{X_n}"'] & E^n \arrow[d] & X_n \arrow[d] \\
f_{X_n}(A^n) \arrow[r, dash, dashed] \arrow[rr, dash, dashed, bend right] & E^n & X_n
\end{tikzcd}$$

Sequence of hash functions $\{f_{X_n} : \mathcal{A}^n \to [e^{nR}]\}_{n=1}^{\infty}$

$$
\begin{tikzcd}
A^n \arrow[r, dash] \arrow[d, "f_{X_n}"'] & E^n \arrow[d] & X_n \arrow[d] \\
f_{X_n}(A^n) \arrow[r, dash, dashed] \arrow[rr, dash, dashed, bend right] & E^n & X_n
\end{tikzcd}
$$

$\{X_n\}$: Sequence of common randomness independent of (A^n, E^n)

Asymptotics of Equivocation I

Define the averages of the security indices (over X_n) as

$$C_{1+s} := C_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$
$$C^{\uparrow}_{1+s} := C^{\uparrow}_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$

where the random variables are evaluated as $P^n_{AE} \times P_{X_n}$.

Asymptotics of Equivocation I

Define the averages of the security indices (over X_n) as

$$C_{1+s} := C_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$
$$C^{\uparrow}_{1+s} := C^{\uparrow}_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$

where the random variables are evaluated as $P^n_{AE} \times P_{X_n}$.

Theorem

Let $M_n = \|f_{X_n}\| = \lfloor e^{nR} \rfloor$. For any $s \in [0,1]$, we have

$$\lim_{n\to\infty} \frac{1}{n} \inf_{f_{X_n}} C_{1+s} = |R - H_{1+s}(A|E)|^+,$$
$$\lim_{n\to\infty} \frac{1}{n} \inf_{f_{X_n}} C^{\uparrow}_{1+s} = |R - H^{\uparrow}_{1+s}(A|E)|^+.$$

Infima are over all random hash functions and achieved by any sequence of ϵ-almost universal$_2$ hash functions.

Asymptotics of Equivocation II

Theorem

Let $M_n = \|f_{X_n}\| = \lfloor e^{nR} \rfloor$*. For any* $s \in (0,1]$*, we have*

$$\lim_{n\to\infty} \frac{1}{n} \inf_{f_{X_n}} C_{1-s} = \begin{cases} R - H_{1-s}(A|E) & R \geq \hat{R}_{-s} \\ \max_{t\in[0,s]} \frac{t}{s}(R - H_{1-t}(A|E)) & R \leq \hat{R}_{-s} \end{cases} .$$

Asymptotics of Equivocation II

Theorem

Let $M_n = \|f_{X_n}\| = \lfloor e^{nR} \rfloor$*. For any* $s \in (0,1]$*, we have*

$$\lim_{n \to \infty} \frac{1}{n} \inf_{f_{X_n}} C_{1-s} = \begin{cases} R - H_{1-s}(A|E) & R \geq \hat{R}_{-s} \\ \max_{t \in [0,s]} \frac{t}{s}(R - H_{1-t}(A|E)) & R \leq \hat{R}_{-s} \end{cases} .$$

- Here $\hat{R}_s$ is some cutoff rate defined as

$$\hat{R}_s := \frac{\mathrm{d}}{\mathrm{d}t} tH_{1+t}(A|E)\Big|_{t=s}$$

and similarly for $\hat{R}_s^{\uparrow}$.

Asymptotics of Equivocation II

Theorem

Let $M_n = \|f_{X_n}\| = \lfloor e^{nR} \rfloor$. *For any* $s \in (0,1]$, *we have*

$$\lim_{n\to\infty} \frac{1}{n} \inf_{f_{X_n}} C_{1-s} = \begin{cases} R - H_{1-s}(A|E) & R \geq \hat{R}_{-s} \\ \max_{t\in[0,s]} \frac{t}{s}(R - H_{1-t}(A|E)) & R \leq \hat{R}_{-s} \end{cases} .$$

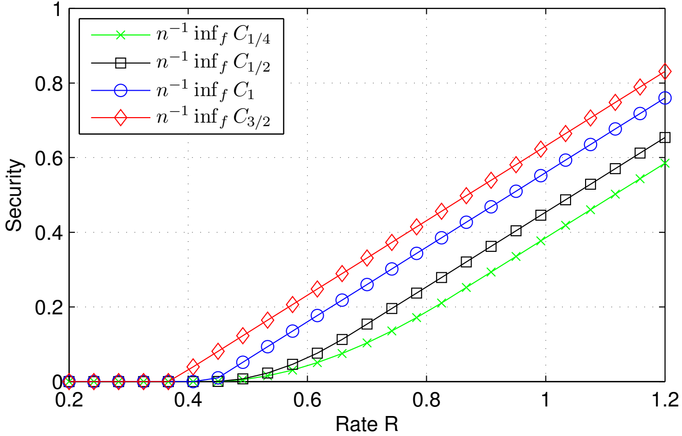
- Here $\hat{R}_s$ is some cutoff rate defined as

$$\hat{R}_s := \frac{\mathrm{d}}{\mathrm{d}t}\, tH_{1+t}(A|E)\bigg|_{t=s}$$

  and similarly for $\hat{R}_s^{\uparrow}$.

- Similar behavior for $C_{1-s}^{\uparrow}$

Asymptotics of Equivocation : Illustration



Security measures $\frac{1}{n}C_{1+s}$ and $\frac{1}{n}C_{1-s}$ for source $\begin{bmatrix} 0.7 & 0.1 \\ 0.1 & 0.1 \end{bmatrix}$

Optimal Key Generation Rate

Corollary

We have

$$\sup\left\{R : \lim_{n\to\infty} \inf_{f:\mathcal{A}^n\to[e^{nR}]} \frac{C_{1+s}}{n} = 0\right\} = \begin{cases} H_{1+s}(A|E) & \textit{if } s \in (0,1] \\ H(A|E) & \textit{if } s \in [-1,0] \end{cases}$$

Optimal Key Generation Rate

Corollary

We have

$$\sup\left\{R : \lim_{n\to\infty} \inf_{f:\mathcal{A}^n\to[e^{nR}]} \frac{C_{1+s}}{n} = 0\right\} = \begin{cases} H_{1+s}(A|E) & \textit{if } s \in (0,1] \\ H(A|E) & \textit{if } s \in [-1,0] \end{cases}$$

- Maximum key generation rate changes depending on sign of s

Optimal Key Generation Rate

Corollary

We have

$$\sup\left\{R : \lim_{n\to\infty} \inf_{f:\mathcal{A}^n\to[e^{nR}]} \frac{C_{1+s}}{n} = 0\right\} = \begin{cases} H_{1+s}(A|E) & \textit{if } s \in (0,1] \\ H(A|E) & \textit{if } s \in [-1,0] \end{cases}$$

- Maximum key generation rate changes depending on sign of s
- When $s \in (0,1]$, it is H_{1+s}
- When $s \in [-1,0]$, it is H, independent of s

Optimal Key Generation Rate

Corollary

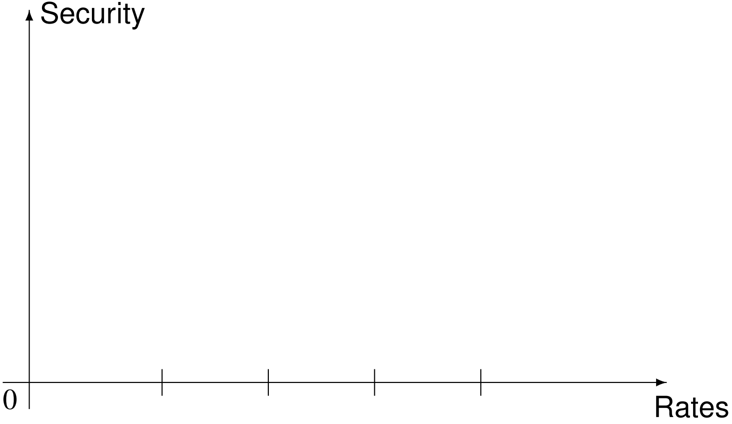
We have

$$\sup\left\{R : \lim_{n\to\infty} \inf_{f:\mathcal{A}^n\to[e^{nR}]} \frac{C_{1+s}}{n} = 0\right\} = \begin{cases} H_{1+s}(A|E) & \text{if } s\in(0,1] \\ H(A|E) & \text{if } s\in[-1,0] \end{cases}$$

- Maximum key generation rate changes depending on sign of s
- When $s \in (0,1]$, it is H_{1+s}
- When $s \in [-1,0]$, it is H, independent of s
- Similar behavior for $C^{\uparrow}_{1+s}$

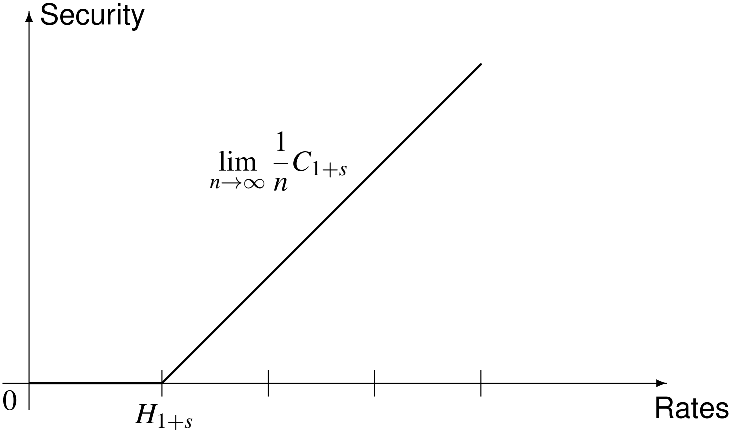
Summary of Behavior of Equivocations

Schematic showing the relation between the various entropies and the transition rate $\hat{R}_{-s}$.



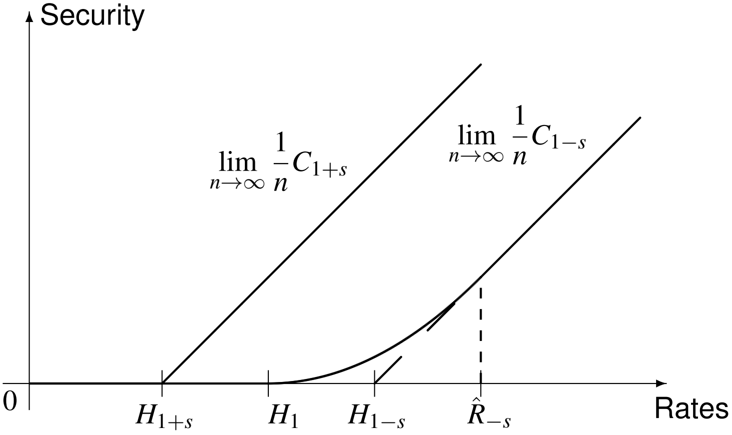
Summary of Behavior of Equivocations

Schematic showing the relation between the various entropies and the transition rate $\hat{R}_{-s}$.



Summary of Behavior of Equivocations

Schematic showing the relation between the various entropies and the transition rate $\hat{R}_{-s}$.



Exponential Behavior of Rényi Security Measures

- Previously, we were interested in

$$\frac{1}{n} C_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$

and the same for the Gallager version.

Exponential Behavior of Rényi Security Measures

- Previously, we were interested in

$$\frac{1}{n} C_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$

and the same for the Gallager version.

- We know below the optimal key generation rate, $\frac{1}{n} C_{1+s}$ and $\frac{1}{n} C^{\uparrow}_{1+s}$ tend to zero

Exponential Behavior of Rényi Security Measures

- Previously, we were interested in

$$\frac{1}{n} C_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$

  and the same for the Gallager version.

- We know below the optimal key generation rate, $\frac{1}{n} C_{1+s}$ and $\frac{1}{n} C_{1+s}^{\uparrow}$ tend to zero

- How fast do they tend to zero, i.e., we seek limiting behavior of the exponent

$$-\frac{1}{n} \log C_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$

Exponential Behavior of Rényi Security Measures

Theorem

Let $M_n = \|f_{X_n}\| = \lfloor e^{nR} \rfloor$. *For* $s \in [0,1]$, *we have*

$$\lim_{n\to\infty} -\frac{1}{n} \log \inf_{f_{X_n}} C_{1+s} = \max_{t\in[s,1]} tH_{1+t}(A|E) - tR$$

$$\lim_{n\to\infty} -\frac{1}{n} \log \inf_{f_{X_n}} C_{1-s} = \max_{t\in[0,1]} tH_{1+t}(A|E) - tR$$

Exponential Behavior of Rényi Security Measures

Theorem

Let $M_n = \|f_{X_n}\| = \lfloor e^{nR} \rfloor$*. For* $s \in [0,1]$*, we have*

$$\lim_{n\to\infty} -\frac{1}{n} \log \inf_{f_{X_n}} C_{1+s} = \max_{t\in[s,1]} tH_{1+t}(A|E) - tR$$

$$\lim_{n\to\infty} -\frac{1}{n} \log \inf_{f_{X_n}} C_{1-s} = \max_{t\in[0,1]} tH_{1+t}(A|E) - tR$$

Similar behavior for Gallager forms.

Illustration of Exponents

Illustration of the exponential decays of $C_{1/2}, C_1, C_{3/2}$, and $C_{7/4}$. Also indicated are the zero-crossings.

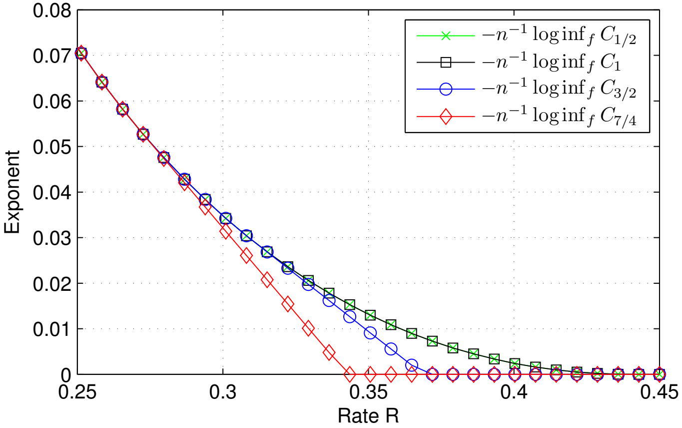


Illustration of Exponents

Illustration of the exponential decays of $C_{1/2}, C_1, C_{3/2}$, and $C_{7/4}$.
Also indicated are the zero-crossings.

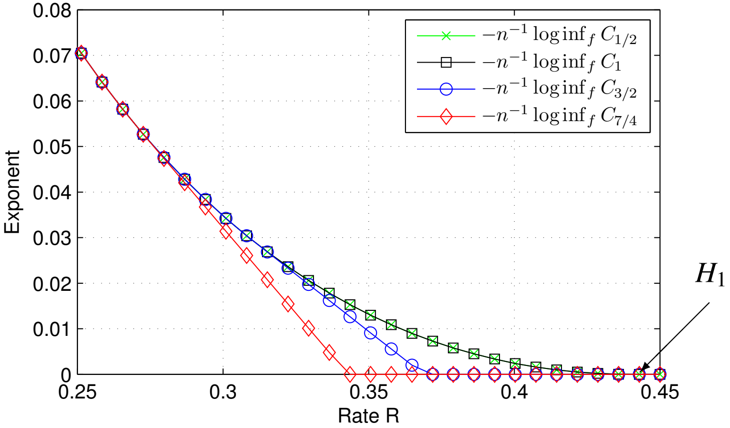


Illustration of Exponents

Illustration of the exponential decays of $C_{1/2}, C_1, C_{3/2}$, and $C_{7/4}$.
Also indicated are the zero-crossings.

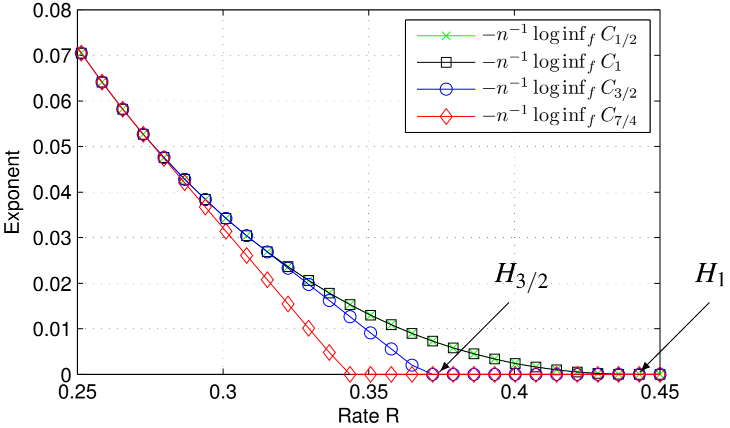
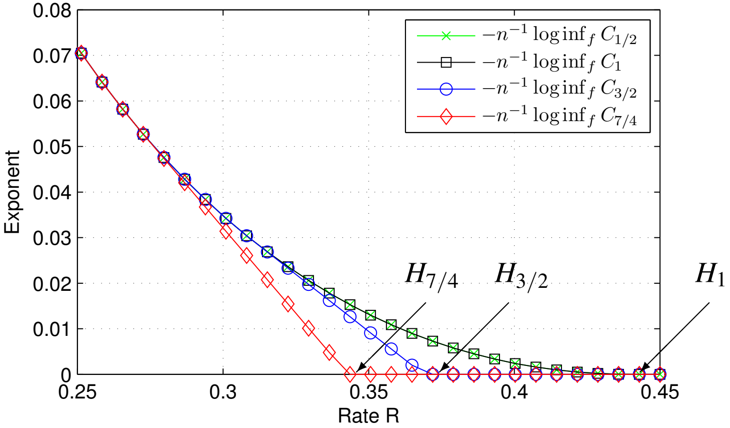


Illustration of Exponents

Illustration of the exponential decays of $C_{1/2}, C_1, C_{3/2}$, and $C_{7/4}$. Also indicated are the zero-crossings.



Remarks on Exponents

- Proof ideas based on new non-asymptotic bounds and large deviation evaluations

Remarks on Exponents

- Proof ideas based on new non-asymptotic bounds and large deviation evaluations
- E.g., Cramer's theorem and various forms of the Gärtner-Ellis theorems

Remarks on Exponents

- Proof ideas based on new non-asymptotic bounds and large deviation evaluations
- E.g., Cramer's theorem and various forms of the Gärtner-Ellis theorems
- Non-asymptotic bounds are improved versions of Bennett et al.'s (1999) bounds for the leftover hash lemma stated in terms of the Rényi entropy of order 2

Second-Order Asymptotics

Now we assume that the key size M_n satisfies

$$\log M_n = nH(A|E) + \sqrt{n}L$$

for some $L \in \mathbb{R}$. This is called the second-order regime.

Second-Order Asymptotics

Now we assume that the key size M_n satisfies

$$\log M_n = nH(A|E) + \sqrt{n}L$$

for some $L \in \mathbb{R}$. This is called the second-order regime.

Theorem

For random hash functions $f_{X_n} : \mathcal{A}^n \to \{1, \ldots, M_n\}$, we have

$$\lim_{n\to\infty} \frac{1}{\sqrt{n}} \inf_{f_{X_n}} C_1(f_{X_n}(A^n)|E^n, X_n) = \int_{-\infty}^{L/\sqrt{V}} \frac{L - \sqrt{V}x}{\sqrt{2\pi}} \mathrm{e}^{-x^2/2}\, \mathrm{d}x$$

where the conditional varentropy is defined as

$$V = V(A|E) = \mathrm{var}\left[-\log P_{A|E}(A|E)\right].$$

Second-Order Asymptotics

Now we assume that the key size M_n satisfies

$$\log M_n = nH(A|E) + \sqrt{n}L$$

for some $L \in \mathbb{R}$. This is called the second-order regime.

Theorem

For random hash functions $f_{X_n} : \mathcal{A}^n \to \{1, \ldots, M_n\}$, *we have*

$$\lim_{n\to\infty} \frac{1}{\sqrt{n}} \inf_{f_{X_n}} C_1(f_{X_n}(A^n)|E^n, X_n) = \int_{-\infty}^{L/\sqrt{V}} \frac{L - \sqrt{V}x}{\sqrt{2\pi}} \mathrm{e}^{-x^2/2}\, \mathrm{d}x$$

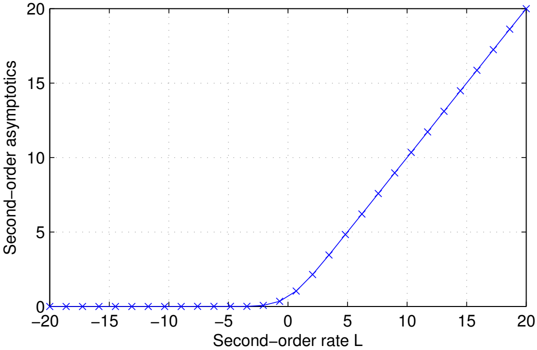
where the conditional varentropy is defined as

$$V = V(A|E) = \mathrm{var}\left[-\log P_{A|E}(A|E)\right].$$

Here, we make use of central limit theorem ideas.

Second-Order Asymptotics: Illustration

$$\lim_{n\to\infty} \frac{1}{\sqrt{n}} \inf_{f_{X_n}} C_1(f_{X_n}(A^n)|E^n, X_n) = \int_{-\infty}^{L/\sqrt{V}} \frac{L-\sqrt{V}x}{\sqrt{2\pi}} \mathrm{e}^{-x^2/2}\,\mathrm{d}x$$



Summary

- We have conducted a detailed study of the asymptotic behavior of

$$C_{1+s} := \log M_n - H_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$
$$C^{\uparrow}_{1+s} := \log M_n - H^{\uparrow}_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$

their exponents, and second-order asymptotics.

$$\begin{tikzcd}
A^n \arrow[r, dash] \arrow[d, "f_{X_n}"'] & E^n \arrow[d] & X_n \arrow[d] \\
f_{X_n}(A^n) \arrow[r, dash, dashed] \arrow[rr, dash, dashed, bend right] & E^n & X_n
\end{tikzcd}$$

Summary

- We have conducted a detailed study of the asymptotic behavior of

$$C_{1+s} := \log M_n - H_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$
$$C^{\uparrow}_{1+s} := \log M_n - H^{\uparrow}_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$

their exponents, and second-order asymptotics.

$$\begin{tikzcd}
A^n \arrow[r, dash] \arrow[d, "f_{X_n}"'] & E^n \arrow[d] & X_n \arrow[d] \\
f_{X_n}(A^n) \arrow[r, dash, dashed] \arrow[rr, dash, dashed, bend right] & E^n & X_n
\end{tikzcd}$$

- Optimal key generation rate has a surprising behavior which depends on the sign of s.

Summary

- We have conducted a detailed study of the asymptotic behavior of

$$C_{1+s} := \log M_n - H_{1+s}(f_{X_n}(A^n)|E^n, X_n)$$
$$C_{1+s}^{\uparrow} := \log M_n - H_{1+s}^{\uparrow}(f_{X_n}(A^n)|E^n, X_n)$$

their exponents, and second-order asymptotics.

$$\begin{tikzcd}
A^n \arrow[r, dash] \arrow[d, "f_{X_n}"'] & E^n \arrow[d] & X_n \arrow[d] \\
f_{X_n}(A^n) \arrow[r, dash, dashed] \arrow[rr, dash, dashed, bend right] & E^n & X_n
\end{tikzcd}$$

- Optimal key generation rate has a surprising behavior which depends on the sign of s.
- For more results, consult the full version: `arxiv.org/abs/1504.02536` (IT Transactions revised)