

Estimating Min-Entropy For Large Output Spaces

Darryl Buller, Aaron Kaufer Information Assurance Directorate National Security Agency



- Background
- Our goal
- Using Bayesian Networks
- Optimizing with a Genetic Algorithm
- Computing Min-Entropy
- Examples













- Source of randomness can be quantified by its entropy
- Min-entropy measurement is useful for cryptographic applications

•
$$H_{\infty} = -\log_2[Max\{\Pr[S = s_i]\}]$$

- Corresponds to cost of optimal guessing attack
- Other measures of entropy can be misleading for these applications





When data from entropy source is processed by a mixing function, we focus our analysis on the raw entropy source data







- Suppose we have sample data from an entropy source
- We wish to find a statistical model and estimate the source's min-entropy
- Sample data is a sequence {s₁, s₂, ..., s_L}, each s_i an *n*-bit value sampled from an output space X





- SP 800-90B has techniques for typical cases that satisfy the following two assumptions:
 - Output space X is reasonably small
 - Sample size L is large enough to detect non-IID properties (if they exist)





- What if output space is very large; e.g., each s_i is dozens or hundreds of bits?
- Example: n = 50 bits, where 15th bit tends to match 43rd bit, or 17th bit is influenced by 3rd, 8th, and 31st bits, etc...
- Feasible sample sizes are far too small for us to fully understand the source and search for non-IID properties













Our Goal

Given *n* bit positions having an unknown joint distribution on 2^{*n*} possible values:

- 1. Compactly represent the essence of the joint distribution
- 2. Identify dependencies among bit positions
- 3. Estimate probability of most likely *n*-bit value; this lets us estimate min-entropy











- Definition: Directed acyclic graph (DAG) whose nodes are random variables and edges indicate dependence
- Variables can depend on multiple other variables (in our case, each bit is a variable)





Example:

- Suppose X consists of 4-bit outputs
- A possible BN would be:

 $\Pr[x_1, x_2, x_3, x_4] = \Pr[x_2] \Pr[x_3] \Pr[x_1 | x_2, x_3] \Pr[x_4 | x_1, x_3]$







- Given sample data, we want to find a BN that best explains the sample data
- Use resulting BN to estimate min-entropy
- But how do we find the best BN given our data?











- Optimization technique inspired by biology
- Represent a candidate solution as a "genome" (BN in our case)
- Maintain sequence of populations of candidate solutions
- Define fitness function that measures the quality of a particular genome





- The process:
 - 1. Randomly generate initial population of candidate solutions
 - 2. Repeatedly create new generation based on previous generation
- The goal is to eventually find the best-scoring candidate solution
- How does this work?





- In biology, crossover and mutation result in changes that affect fitness
- Increased fitness is rewarded by selection population increasingly resembles optimal solution
- Decreased fitness is penalized candidates are less likely to influence subsequent generations





• Our implementation ...





Genome: Encodes the details of a specific candidate solution

- Each candidate is a binary nxn adjacency matrix
- -A(i,j) = 1 iff bit *j* is statistically dependent on bit *i*







- Build conditional probability tables from the sample data as specified by the adjacency matrix
 x₂
 x₃
- For this example, we need

 1x2 table for Pr[x₂]
 1x2 table for Pr[x₃]
 4x2 table for Pr[x₁|x₂, x₃]
 4x2 table for Pr[x₄|x₁, x₃]







Crossover: produces two offspring by combining features of two parents

- Randomly pick a crossover point
- Join top part of one adjacency matrix and bottom part of the other, and vice-versa





- Note that crossover often results in an invalid BN due to cycles
- Need a "de-cycling" step children still contain characteristics of both parents





Mutation: A random change in a candidate's adjacency matrix

- 1. Add an edge
- 2. Remove an edge
- 3. Move an edge destination
- 4. Move an edge origin
- 5. Reverse an edge







Selection: Rewards high-fitness candidates by giving them a higher chance of selection to influence next generation:

- 1. Elitist selection: Directly copy most fit candidate to next generation
- 2. Fill remainder of next generation using rank selection to choose pairs of parents for crossover



- Fitness function: allows comparison of candidate solutions
- We use the Bayes Information Criterion (BIC)
- BIC rewards larger likelihood and simpler models; a smaller BIC is better (fitness-wise)

$$BIC = \mathbf{k} \ln \mathbf{N} - 2 \ln \mathbf{L}$$

k: # of free parameters

- N: # of sample outputs
- L: likelihood of observed samples given the BN





For the following BN: 1x2 table for Pr[x₂] 1x2 table for Pr[x₃] 4x2 table for Pr[x₁|x₂, x₃] 4x2 table for Pr[x₄|x₁, x₃]
k = 1 + 1 + 4 + 4 = 10







Min-Entropy







Min-Entropy

- Use Max-Product Variable Elimination algorithm
 to find the MAP of a BN
- Generalization of Viterbi algorithm













Example 1

4-8	11-15		18-22		25-29	
-----	-------	--	-------	--	-------	--

- 32-bit blocks; sample size 15,000
- Bits 4-8, 11-15, 18-22, 25-29 follow biased joint distribution on 5-bit values
- All other bits unbiased and independent
- Actual min-entropy is 17.2877...





GENERATION #1 / 5000

ADJACENCY MATRIX:







GENERATION #25 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

01	ı—	_						 								*			_			 		
02	*									*														
03	1																			*				
04	1					*	*																	
05	1											*			*								*	
06	· *	*			*		*							*									*	
07	i				*																			
08	Ì																							
09	Ì																		*			*		
10	i																							
11	i					*					*													
12	i																							
13	Ì											*												
14	i							*	*		*												*	
15	Ì																							
16	Ì																							
17	1						*																*	
18	I	*							*							*								
19	Ì																*							
20	1																					*		
21	1																	*			*			
22	1												*											
23	1																		*					
24	1		*																					
25	1																			*			*	
26	1																							
27	1				*																	*		
28	I			*	*										*				*			*		*
29	1																							
30	l i																							
31	1																							
32	I																	*						

BIC: 726693.810980





GENERATION #50 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

								 					·							 		<u> </u>
01																						*
02	I *									*												
03																			*			
04				*	,	*	*															
05												*			*							
06	*	*		4			*							*							*	
07				*																		
80	l i																					
09	l i																			*		
10																						
11	l i					*					*											
12																						
13	l –								*			*										
14	I							*	*		*											
15	l i																					
16	l –																					
17	I																*					
18	l i	*							*						4	r						
19	l i															*						
20																				*		
21	l –																*					
22	l i												*									
23	l i																	*				
24	I		*																			
25	I						ب												*		*	
26	l i																					
27	l i									*							*		*	*		
28	l i			ب ب											*			*		*		*
29	l i																					
30	l –																					
31	l i																					
32	l –																,	*				

BIC: 710074.763608





GENERATION #75 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

	_						 		 														 			
01	1																									
02	I.	*									*															
03	L																									
04	L					*	*	*																		
05	1													*			*									
06	1	*	*			*		*								*									*	
07	Í.					*		*																		
80	Í.																									
09	Í.																						*			
10	i -																									
11	Í.						*						*													
12	Í.												*													
13	1									*				*												
14	Í.								*	*			*													
15	Í.																									
16	1																									
17	I.																									
18	Í.		*							*								*								
19	1																		*							
20	1																							*		
21	Í.																			*						
22	1														-	r	*									
23	L																									
24	L			*																						
25	1																					*	*		*	
26	L.																									*
27	L.											*								*		*	*			
28	1				*	*											*				*		*			
29	L																									
30	L																									
31	I.																									
32	L																									

BIC: 699140.036300





GENERATION #100 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

01	ı—	_				 _		 	_						 										 		
02	*										*																
03	Í.																										
04	Í.				*	*	*																				
05	l l													*		-	ł.										
06	*	*		*	*		*																			*	
07	i i				*		*																				
80	1																										
09	1																								*		
10	1																										
11	1					*							*														
12	1												*														
13	1									*			*	*													
14	1								*	*			*														
15	1																										
16	1																										
17	I																				*						
18	1	*								*						-	k 1	*									
19	1																		*								
20	1																								*		
21	1																			*							
22	1														*	-	le la										
23	1																										
24	1		*																								
25																							*	*	*	*	
26																											
27												*								*			*		*		
28	1			*	*																	*			*		
29																											
30																											
31																											
32																											

BIC: 683288.866511




GENERATION #125 / 5000

ADJACENCY MATRIX:

	0	1	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01 02		*	_	_	_	_	_	_	_	_	_	—	_		—	—	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	—
03 04	i					*		*	*																								
05	İ.																*																
)6)7	1	*	*		*	*			*																							*	
	1																																







BIC: 682658.487793





GENERATION #150 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	·—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
02	i *												*																			
03	i –																															
04	i –				*		*	*																								
05	i –															*																
06	i *	*		*	*			*																							*	
07	i –				*			*																								
08	i –																															
09	i –																															
10	i –																															
11	i						*								*																	
12	i														*																	
13	i –											*			*																	
14	i i										*	*			*																	
15	Í.																															
16	Í.	*																														
17	1																															
18	1											*									*											
19	1																*					*										
20	1																	*												*		
21	1																															
22	1																	*		*												
23	1																															
24	1		*																													
25	1																									*	*		*			
26	1																												*			*
27	1													*									*			*			*			
28	1				*															*					*		*		*			
29	1																															
30	1																															
31	1																															
32	1																															





GENERATION #175 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	I	_	—	—	—	_	_	—	—	—	—	—	—	_	—	_	_	_	—	—	—	—	—	_	_	—	_	_	—	—	—	—
02	*												*																			
03	l –																															
04	l i				*			*																								
05	l –															*																
06	I *	*		*	*			*																								
07	I			*	*			*																								
80	l i																															
09																																
10	l i																															
11							*					*			*																	
12															*																	
13												*			*																	
14											*	*			*																	
15																																
16																																
10	1											ىلە									ىلە											
10	1											-					÷	÷			-	4										
20	1																	*												*		
21	1																															
22	1																	*		*												
23	1																															
24	i		*																													
25	i																									*	*		*			
26	i																												*			*
27	i																						*			*			*			
28	i																			*					*		*		*			
29	1																															
30	I																															
31	I																															
32	I .																															

BIC: 675213.747863





GENERATION #200 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	·—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	_	—	—	_	—	—	—	_	—	—	—	—	—	—	_
02	i *												*																			
03	1																															
04	1				*			*																								
05	1															*																
06	I *	*		*	*			*																								
07	1			*	*			*																								
80	1																															
09	1																															
10	1																															
11	1											*			*																	
12	1														*																	
13	1										*	*			*																	
14											*	*			*																	
15	1																															
16																																
17	!																															
18	!											*									*											
19	<u>!</u>																-				ىلە									4		
20	-																															
22	÷ –																	*		*												
22	1																															
24	1		*																													
25	÷ .																									*	*		*			
26	i –																												*			*
27	i –																						*			*			*			
28	i –																			*					*		*		*			
29	i –																															
30	i																															
31	1																															
32	1																															

BIC: 674206.774448





GENERATION #225 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

		 				 		 						 	 				 			 		 _
01	1																							
02	* ۱										*													
03	1																							
04	1				*		*																	
05	1												*											
06	I *	*		*	*		*																	
07	I			*	*		*																	
80	1																							
09	1																							
10	I																							
11	1									*		*												
12	1											*												
13	1								ł.	*		*												
14	1							-	tr.	*		*												
15	I																							
16	1																							
17	1																							
18	I														*	*								
19	1													*		*	*							
20	I															*							*	
21	1																							
22	I													*	*									
23	I																							
24	1		*																					
25	1																			*	*	*		
26	1																					*		ł.
27	1																	*		*		*		
28	1														*				*	*	*	*		
29	1																							
30	1																							
31	I																							
32	1																							

BIC: 658522.184421





GENERATION #250 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	ı—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—		_	—	—	—	—	—	—
02	I *												*																			
03	1																															
04	1				*			*																								
05	1															*																
06	I *			*	*			*																								
07	1			*	*			*																								
80	1																															
09	1																															
10	1																															
11	1											*			*																	
12	1														*																	
13	I										*	*			*																	
14	1										*	*			*																	
15	!																															
16	!																															
10	<u>.</u>																			÷	÷											
10	-																	*			*	*										
20	-																				*									*		
21	: -																															
22	: -																	*		*												
23	i –																															
24	i –																															
25	i –																									*	*		*			
26	i –																												*			
27	i –																									*			*			
28	i																			*					*	*	*		*			
29	1																															
30	1																															
31	I.																															
32	1																															

BIC: 658468.903248





GENERATION #275 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	·—	—	—	—	_	—	_	—	—	_	_	—	_	—	—	—	—	—	—	—	_	—	—	—	_	_	_	—	_	_	—	—
02	i												*																			
03	i i																															
04	Í.				*			*																								
05	Í.															*																
06	I *			*	*			*																								
07	1			*	*			*																								
80	1																															
09	1																															
10	1																															
11	1											*			*																	
12	1														*																	
13	1										*	*			*																	
14	1										*	*			*																	
15	1																															
16	1																															
17	1																															
18	1																			*	*											
19	I																	*			*	*										
20																					*											
21	!																															
22	!																	*		*												
23																																
24	<u>.</u>																															
25																										-	-		- -			
20																										÷			-			
27																									÷	-	÷		÷			
20																																
20	1																															
30	1																															
31	<u>.</u>																															

32 |

BIC: 658377.735340





GENERATION #300 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	ı—	—	_		—	_	_	_	_			_	_	_	_		_	_	_	_		_	_			_	_	_	_			
02	I.																															
03	1																															
04	1				*			*																								
05	1															*																
06	1			*	*			*																								
07	1			*	*			*																								
08	1																															
09	I																															
10																																
11	!											*																				
12	!														*																	
13											- -	Ť																				
15	-										-	-																				
16	-																															
17	÷ –																		*													
18	i –																			*	*											
19	i –																	*			*	*										
20	i –																				*											
21	i –																															
22	i –																	*		*												
23	i																															
24	Í.																															
25	1																									*	*		*			
26	1																												*			
27	1																									*			*			
28	1																								*	*	*		*			
29	1																															
30	1																															
31	1																															
32	1																															

BIC: 658342.568077





GENERATION #325 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	·—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
02	i –																															
03	l l																															
04	1				*			*																								
05	1															*																
06	1			*	*			*																								
07	1			*	*			*																								
80	1																															
09	!																															
10	!																															
12	!											~			Ť																	
12											*	*			-																	
14											*	*			*																	
15	1																															
16	i i																															
17	i –																		*													
18	i i																			*	*											
19	1																	*			*	*										
20	I.																				*											
21	1																															
22	1																	*		*	*											
23	I																															
24	!																															
25	!																									*	*		*			
26	!																									ىلە						
27	-																								÷	ī	÷		ī			
20	-																															
30	1																															
31	1																															
<u> </u>																																

32 |

BIC: 657256.585419





GENERATION #350 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	0.7	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	·—	—	—	—	—	_	—	—	—		_	_	_	_	_	_	_	_	_	_	_	_	—	—	_	_	_	_	_	—	—	—
02	i i																															
03	i i																															
04	i –				*			*																								
05	i –															*																
06	1			*	*			*																								
07	1			*	*			*																								
80	1																															
09	1																															
10	1																															
11	1											*			*																	
12	1														*																	
13	1										*	*			*																	
14	1										*	*			*																	
15	1																															
16	1																															
17	1																		*													
18	1																			*	*											
19	1																	*			*	*										
20	1																				*											
21	1																															
22	1																	*		*	*											
23	I																															
24																																
25																										*	*		*			
26	!																															
27	!																															
28	!																								*	*	*		*			
29	<u>!</u>																															
30	1																															
31	1																															
32																																

BIC: 657256.585419





GENERATION #375 / 5000

ADJACENCY MATRIX:

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
ı—				_	_	_	_	—	_	_	—	_	_	_			—			_	_	_	_		_	—	_	_	_		
I .																															
!																															
				*			*								÷																
			*	*			*								-																
i i			*	*			*																								
i i																															
i i																															
Ì																															
I I											*			*																	
I														*																	
l –										*	*			*																	
I										*	*			*																	
l																															
!																															
																		~	4	ъ											
																	*		-	*	*										
																				*											
i i																															
i i																	*		*	*											
i																															
I																															
1																									*	*		*			
I .																															
1																									*			*			
I .																								*	*	*		*			
l																									*						
1																															





GENERATION #400 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01 02 04 05 06 07 08 09 10 11 23 14 15 16 7 8 9 20 22 23 24 25		02	03	04 *	05 *	•	07	80 * *	09	10	**	12 * *	13	14	15 * *	16	17	*	19 *	20 *	21 	*	23	24	25	26	27	28	29	30	31	32
26	į –																															
28	I I																								*	*	*		*			
29	1																									*						
31	 																															
32	I.																															

BIC: 657254.405126





GENERATION #425 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	ı—	—	—	—	—	—	—	—	—		—	—	—	—	—	—	—	—	—	—		—	—	—	—	—	—	—	—	—	—	—
02	i –																															
03	1																															
04	1							*																								
05	1			*				*																								
06	1			*	*			*																								
07	1			*	*			*																								
80	1																															
09	1																															
10																																
11	!											*			*																	
12	! · ·																															
13	<u>.</u>																															
14	÷ .											-			-																	
16	÷ –						*																									
17	÷ –																		*													
18	÷ –																			*	*											
19	÷ .																	*		*	*	*										
20	i –																				*											
21	i –																															
22	i –																	*		*	*											
23	i –																															
24	i –																															
25	1																									*	*		*			
26	1																															
27	1																									*			*			
28	1																								*	*	*		*			
29	1																									*						
30	1																															
31	1																															
32	1																															





GENERATION	#450 /	5000
------------	--------	------

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	·—	—	—	—	_	—	—	—	—	—	_	_	—	—	_		_		_	—		—	_	_		_	_		_	_		—
02	i																															
03	i i																															
04	1							*																								
05	1			*				*																								
06	1			*	*			*																								
07	1			*	*			*																								
80	1																															
09	1																															
10	1																															
11	1											*			*																	
12	1														*																	
13	1										*	*			*																	
14	1										*	*			*																	
15	1																															
16	1																															
17	!																		*													
18	!																															
19	<u>.</u>																	-		~	Ţ	~										
20	-																				-											
22	-																	*		*	*											
22	÷ –																															
24	1																															
25	÷ –																									*	*		*			
26	÷ –																															
27	i –																									*			*			
28	i –																								*	*	*		*			
29	i –																									*						
30	i																															
31	i																															
22	1																															

32 |

BIC: 651783.140737





GENERATION	#475 /	5000
------------	--------	------

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	·—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
02	i –																															
03	i –																															
04	i i							*																								
05	i –			*				*																								
06	i –			*	*			*																								
07	i –			*	*			*																								
80	i –																															
09	i -																															
10	i –																															
11	Í.											*			*																	
12	1														*																	
13	1										*	*			*																	
14	1										*	*			*																	
15	1																															
16	1																															
17	1																		*													
18	1																			*	*											
19	1																	*		*	*	*										
20	1																				*											
21	1																															
22	1																	*		*	*											
23	1																															
24	1																															
25	1																									*	*		*			
26	1																															
27	1																									*			*			
28	1																								*	*	*		*			
29	1																									*						
30	1																															
31	1																															
32	1																															

BIC: 651783.140737





GENERATION #500 / 5000

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
01	, —	—	—	—	—	—	_	_	_			—	—	—	—		—		_	—	—	—	—	—		_	—	—	_	_	—	—
02	i –																															
03	i –																															
04	i –							*																								
05	i –			*				*																								
06	i –			*	*			*																								
07	i –			*	*			*																								
08	i –																															
09	i –																															
10	i –																															
11	i –											*			*																	
12	i –														*																	
13	i –										*	*			*																	
14	i –										*	*			*																	
15	Í.																															
16	1																															
17	1																		*													
18	1																			*	*											
19	1																	*		*	*	*										
20	1																				*											
21	1																															
22	1																	*		*	*											
23	1																															
24	1																															
25	1																									*	*		*			
26	1																															
27	1																									*			*			
28	1																								*	*	*		*			
29	1																									*						
30	1																															
31	1																															
32	1																															

BIC: 651783.140737





BEST	-FI	T 1	10DE	сь:																												
ADJA	CEN	ICY	мал	RI	۲:																											
01 02 03 04 05 06 07 08 09 10 11	01 	02 —	03 —	04 —	(: 	06	07	08 	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
12 13 14 15 16 17 18 19 20 21 22 23 24	12 * * 12 * * 13 * * 14 * * 15 * * 16 * * 17 * * 18 * * 19 * * 20 * * 21 * * 22 * * 23 * * 24 * * 25 * *																															
25 26 27 28 29 30 31 32	 																								*	*	*		*			
BIC:	65	5178	33.1	407	737																											
Writ	ing	j BE	CST-	FI	C MO	DDEI	i to	"e	dge	s.c	ut"	• • •	•																			
Comp	uti	ng	Mir	1-Er	itro	ру	Est	ima	te																							
ESTI	MAT	ED	MIN	I EI	TRO	PY	: 1	7.0	506	47																					F	
									Info	orma	tion	Assı	uran	ce Di	recto	orate	// 0	Confid	dence	e in (Cybei	rspac	e									2

Example 2



- 20-bit blocks; sample size 15,000
- Bit 3 dependent on 1; 7 on 5; 8 on 4 and 6; 12 and 14 on 10
- All other bits unbiased and independent
- Actual min-entropy is 16.3104...





GENERATION #1 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 578019.435300





GENERATION #25 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 570684.444407





GENERATION #50 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



()



GENERATION #75 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



())



GENERATION #100 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 570455.316561





GENERATION #125 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20







GENERATION #150 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 570455.316561





GENERATION #175 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 570455.316561





GENERATION #200 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 570443.807480





GENERATION #225 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 570443.807480





GENERATION #250 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 570432.721112





GENERATION #275 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 570432.721112





GENERATION #300 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



BIC: 570432.721112





GENERATION #325 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20





Information Assurance Directorate // Confidence in Cyberspace

IAT

GENERATION #350 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20







GENERATION #375 / 5000 ADJACENCY MATRIX: 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 01 | 02 | 03 | * 04 | * 05 | *

- 08 | 09 | 10 | * * 11 | 12 | 13 |
- 14 | * 15 |
- 16 | 17 |
- 18 |
- 19 | 20 |
- 20 |

BIC: 570432.721112



07



GENERATION #400 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20







GENERATION #425 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20




GENERATION #450 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20





Information Assurance Directorate // Confidence in Cyberspace

IAT

GENERATION #475 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20



00 🛞

Information Assurance Directorate // Confidence in Cyberspace



GENERATION #500 / 5000

ADJACENCY MATRIX:

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20





Information Assurance Directorate // Confidence in Cyberspace



BEST-FIT MODEL:

ADJACENCY MATRIX:

	01	02	03	04	05	06	07	80	09	10	11	12	13	14	15	16	17	18	19	20
01 02 03 04 05 06 07 08 09 10 11 12 13 14								*				*		*						
15 16 17 18 19 20	 																			
BIC: 570432.721112 Writing BEST-FIT MODEL to "edges.out"																				
Computing Min-Entropy Estimate																				
ESTI	MAT	ED	MIN	EN	TRC	PY	: 1	6.2	512	61										~
					li	nforma	tion As	surance	e Direc	torate ,	// Confi	dence i	n Cyber	space						IN

References

Koller, D. and N. Friedman (2009). *Probabilistic Graphical Models, Principles and Techniques*. Cambridge, Massachusetts: The MIT Press.



