

### Pseudo-Entanglement is Necessary for EFI Pairs

Manuel Goulão with David Elkouss

Portugal Crypto Day - 13th of December of 2024



Introduction

Fundamentals of Cryptography

EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

Discussion

#### Contents

#### Introduction

Fundamentals of Cryptography

EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

Discussion

- · What systems may we *implement*?
- · Perfect encryption
- · All messages are valid: Zero information!
- Key as long as the message. . .
- · Key can only be used once.....

	ABCDEFGHIJELMNOPGESTUVWXYZ
	ZYXWVUTSRQPONMLKJINGFEDCBA
	B ABCDEFGHIJELMNOFGESTUVWXY2
	"YXWVUTSRGPONMLKJINGFEDCBAZ
LFHHY ZAHSS JENXE SYNFE KOZAT	C ABCDEFGHIJELMNOPGRETUVWXYZ
	XWVUTSREPONMLXJIHOFEDCBAZY
	D ABCDEFGEIJELMNOFGESTUVWXYZ
***** 37680 ***** 3**** *****	WVUTSRGFORMLKJIRGFEDCBAZTX
	* ABCDEFORIJELENOFURETUVWXTZ
PODTE JJLVJ XFEHL HPLEA ZXVZY	YUTSAAFUNALETIAUFEDUBAETAW
	P TTANAPONILI INOPEDCE INVEST
TRUIS TRUET BRENS HERET SZYSZ	ANCHEVANTINT WYOPANETURWYY
	O TEROPORMINI INGREDCHATYNWYD
	ANCEFFANTIFIANCEARETUVWY
ETJEF OBIER PRIVY YTKER ATOPE	" SROPONMLEJINGFEDCBALTEWVUT
	ABCDEFORIJELMNOFGRATUVWXYZ
	B B B PONMLEJ I HGFEDCBAZYXWVUTS
	. ABCDEFGHIJKLMNOPGRETUVWXYZ
	GPONMINJINGFEDCBAZYXWVUTSR
VIIUJ TERRI GHRDE YOVRJ ROCEY	- ABCDEFGHIJELMNOFQESTUVWXYZ
	PONMLEJINOFEDCBAZYXWVUTSRQ
ALSE WHITE CALLY BUTEN JUINP	A BCDEFGHIJELMNOFGESTUVWXYZ
	ONMLEJINGFEDCBAZTXWVUTERGF
	M ABCDEFORIJELMNOFGRETUVWXYZ
	NMLK2 ING 7 EDCBAZYXWVUT BAGPO
	N ABCDEFORIJELMNOFGESTUWWETE
KANDER OZJIH DBREY BRUVE LFBRT	MLKJINGFEDCBALTXWYUTSKUPDA
	0
	INCOMPOSITION OF A STREET OF A
	P KIINGFEDCBAZTXWYUTSBOPONML
	- ABCDEFGELJELMNOPGESTUVWYYZ
NGONG ZUBZB EPVJI NCIXY PBTEX	9 JINGFEDCBAZYXWVUTEBGPONMLK
	- ABCDEFGEIJELMNOFGESTUVWXYZ
	* INGFEDCBAZYXWVUTBRGPONMLKJ
	- ABCDEFGRIJELMNOPGRSTUVWXYZ
	"HGFEDCBAZYXWYUTSRGFONMLKJI
POFRI ACFAA NLTKE DANDA BAINU	- ABCDEFGHIJKLMNOPGRSTUVWXYZ
	GFEDCBAZTXWVUTSRGFONMLKJIK
	** ABCDEFORIJELMNOFGRETUVWXYZ
	FEDCBAZYXWVUTERQPONMLEJING
	V ABCDEFORIJELMNOFGBBTUVWXTZ
ATEFS INFOU STRVE ITIPO RUCER	EDCHALTAWYUTSAGFUNALEJIHUF
PRARE ARALG BYLLS COTHE GOREN	I BORRESS AND
	X CRAST WYUTEBOPONNLEJINOFED
	ANCONFANTINIANOPOLETIUNTY
FSENA UDTLB UNKAN NAKNE TZVXN	Y BATTXWVUTERGPONMLKJINGFEDC
	ABCHTTONIJELMNOPOBETHUWYVE
USESS JERFY NTURN SCTEM OFLET	Z ABCDEFONIJKLMNOFORSTUVWXYZ

NSA One-Time Pad (Source: Wikimedia)

- · What systems may we *implement*?
- · Perfect encryption
- · All messages are valid: Zero information!
- · Key as long as the message. . .
- · Key can only be used once.....

																									-		-	_	-	_		-				_									_
																						-			1.3	C	DI	: 7	G	ж	1.	2	Ľ	×	NC	17	0	R		T	σ,	1	73	Y	Z
					•		•••																	A 2	ΞŦ.	x	ē ī	÷	Ŧ	5	ñċ	5	ō	N I		. 2	c 3	ī	ñ.	ā i	;;	έĒ	P C	÷.	11
																								-	1	Ċ.	6 1		O.	ŵ	Ÿ7	12	Ť.	2	80	17	12	ΩŔ,	1			16	7 2	Ŷ	<b>%</b>
																									r x	÷	ŪΫ	-		ñ.	õ i	0		×		ć i	17	Ŧ	ā	÷	÷ ;	ò ē	5	12	ΞL
	-				-				- 1		۰.				-						-					÷.	÷ 1	r é	ā	÷		nü	-		20			æ	*	24			-6	-6	ζI.
۰.	,	۳	*	۰	z	٠	×	٠	٠			×	x		٠	۰			•		•	.,	• •	C 3		23				*	:;	. 3	5			15		2	а.	5.	23	12		4	÷.
																										-	-	-1	- 2-	뵨	-	-6		÷.,	14	-	-8	~	-	84	<u></u>	68	.8	æ	41
										-						-				ъ.				D 1		0		1	•	프	11		-	-	NC	12	. 5	- 25		Ξ.	0.0		<u>م</u>	Ξ	Ξ١
٠	•	•		•	-		۶	٠	•	•	v	٠	۰	•	٠	•			•	٠	ь.	•••		- 9	<u> </u>	<u>v</u> .	τ.		•	2	0)		11	х.		. 25	10	x	x	D	с з		. z	T	<b>A</b> 1
																								· A		0	D X	.,	0	x	13	x	Ľ.	×:	NO		- 6	x	8	51	σ.	/w	/ 🗙	¥	21
									а.							•						• 1		~ v	10	T	5.2	. 9	7	0	83	11	ж	1	13	: 0		x	D	¢.;		. 2	X	x	w
	-	•		۰.	٠	•	٠	•	•	-		•	•	•		•	•	•		•	-		• •			0:	DX	7	0	н	n	x	1	X.	N C	12		ж	T	Ŧ1	0.8	18	72	Y	ΞI.
																								F 8	7 .	6		1.2	0	x	йİ	. 2	3	T I	K Q	. 7	ΥĒ	D	Q.	ā.	ι.	4 12	x	ŵ	ΨÌ.
τ.		u			×									•	ы.						2		• •			71	2		6	v	75		10.7	ŝ	20	18	. 77	18	121	24	34	14	14	υ	÷L.
	-			-				~	•		۰.	-		•					•	•				0 7			5 F	6	2	Ξ.	ī.	3	7		Ξž	1	'n	ā	я.	11		ŕ 7	-	÷	61
																									-	8-	24	÷	-	θ.	**	-6	- 14		1	c R	18	÷	æ	84	ы	-77	10	÷	31
£	٧	J.	٠		٠	٠	x				к.	τ.	¥	۷	٧	τ.	к.		κ.	٠	τ.			ha 🕈		21	2 2	1		۰.	21		***	21	22	12	. 2	•		5.3	2.2			2	21
-		-		-		-		-	-		-						-			-				-	- T-	•	- 1	2		<u>.</u>	0.1	4	-	2	_				<b>a</b> .	<u>.</u>				<u>_</u>	21
																								T A		с:	DΣ	,	•	н	.,	x	L	к.	<b>x</b> 0	12	- 9	ж	8	51	79		x	x	<b>Z</b> I.
	н	c	J,	ж.		٠			*	٠	н	z	z			٠	2	۷		c	۷				L Q.	<b>7</b> 1	<u> </u>	N	1.1	x.	,,	ж	0	23	εп	.0			Ζ.	x:	κ		υ	т	8I.
																										<u>c 3</u>	5 2	y	61	к	r7	x	17	en	10	- 12	- 0	ж	87	ŧ٦	77	14	12	¥	ži.
																								1 6		ō i	N N	ĽŻ.	x	3	11	0	7	E :	ĎČ	8		Ŧ	Ŷ.	ż١	٧Ý	/ΰ	Ŧ	ŝ	8
۷	r	1	U	J	٠	٠	٠	٠	z	۰			D		٧	۰	v	۸.			٥	٤ 4		-	30	21	1.2	y	ል	ŵ.	77	v	1.1	a٦	270	- 10		v	21	n	70	Λē	v	v	£1.
							-																	1× 7	0	23	47		51	γ.				67	n ž		. 7	÷	2	2	6 ÷	. 7	7	ñ	21
																									-8-	a-c	248	÷	÷.	ē-	-	÷	÷4	i.	-2	æ	-2	4	<del>9</del> 4	24		-	Æ	2	21
	٠	ь.	۰	κ.		н	x	١.		c	٠	1	Ð	۷		0	۳.	κ.		z	Ð	z.		L 3			: 5			<u>a</u>	11	- 2	**	2	19	-5	. =	-	2.3	53	<u></u>		ā	x	<u>e</u> t -
																								- 0	28.	м.	6.8	ы.		л.			<u>.</u>			عد	12	<u>.</u>	w	<u>.</u>	- 1		2	2	51
																								M A		٥3	5 8	Y	01	ĸ	17	х	ы	K 3	• 0		۰.	ж	8.3	53	7 V	w	x	¥	Z
٥	1	N	۰		c		•		ĸ	٠	٠	٠	۷	٠.	c	٠	۳	٠	۰	1	٠	.,	• •	C_ N	LM.	IJ	κ 2	1	<b>X</b> (	٥.		D	C 1		1.2	x	x	w	¥ 1	21		. 8		۶.	0
																								N A		85	5 Z	Ŧ	67	80	7	x	17	20	70	7	76	х	81	n	ΥŸ	W	T	¥	ž[
															-									· M	11.1	κ.	11	н	01	<b>r</b> :	εn	C	31	6.3	t ¥	×	w	v	01		1.28	. 0	7	Ö.	н.
۰.	÷	٠	z		٠	z	٠		-	•	٠	۰	c	۰.	٠	٠	٠	۲	κ.	۰.	,	•	ι.	-		81	18	Ŷ	81	r	2	¥	Ŧ	n	16	18	12	÷	81	- 1	10	10	ŵ	Ÿ	21
		•																						0 7			: 5	'n.	**	Ξ.	ñ ñ	5	11		: :		,÷	÷.	÷ ;		: 2		8	÷.	<b>2</b> 1
					-	-	а.	-										ы.				• •			-0-	64	ю	÷	÷۲	BH	н	ø	e.	ы	HR	æ	æ	÷	÷	н	ы	16	w	6	81
	-				٠	٠		•			•		٠	•	•	•	٠	•	•	•	۰.		•••	18 3		* :	: 2	4	21	2	::	~	**	24		.2		=	23	12	: 1	. 2	0	۵	21
																								<u> </u>	м.	ы	1.2	s	84		64	۵	84	ы	14		-¥-	х.	84	24	ы.	-16	a	æ	81
		-					-		-	-	-							۰.		-				la ^		C 3	2 8	τ	0,	к.		×	-	6.2	10	×.		ж.	81	53	7 9	w	х	х.	<u>ē</u> )
۰	٠	٠	•	•	z	v	٠		•	•		•	•	•		٠	٠	•	۰.		•		• •	- 1	11	жs	22	х	21	<u>c ;</u>		x	x	<u>c s</u>	vv	v	л.	ж.	8.		• 0	с <b>н</b>	м	ы	81
																										01	5 8	r	0)	K.	5	x	13	o	10	Ŧ	0	х	57	er,	77	w	×	Y	2)
w															ε.			•		ы.				· ī		ā i	řΧ	D.	ē.)	Ξ.	i. 2	x	x١	23	10	Ŧ.	۰.	8	ā١	11	Ń	а	z.	x.	и.
•	•	•	٠	•			•	۰.	-	-	•	•	-	-		-	•	•		•	-			-		81	5 E	Ŧ	<u>a</u> 3	<b>6</b> - 1	-	¥	17	o	10	æ	6	81	67	F₹	rv.	- 92	¥	Y	21
																								18 V	0	77	iπ	è	17	Ă İ	żΫ	ÿ	÷	ĩ١	17	а.	×.	0	ž i	άŝ	ιŵ.	εĒ.	÷	ž.	ΞL
						e				×	ь.							ь.		٠	٠	۱.	4 U		÷.	н	Hű	÷	<del>.</del> 4	н	н	ø	ñ	÷	ŀŔ	÷	*	e:	н		ю	-	÷	ŵ	21
•	٠		~	•		٠	۰.	•	-		•	۰.	•	•	•	-				-				T 2		2.5	22	٤.		24	12	2	**		: 2	2		с.	22	52	12	=	÷	а.	<u>- 12</u>
																									44	84	44	4	84	2	-4	ő	44	64	-8	4	4	64	24	и	N	4	۰	۵ł	81
					۰.						•							υ.		٠	٠			Y A		сı	58	r	03	к.)		ж	1.1	Ω	10	æ		8	8.3	13	/ Y	w	×	x	ē) -
~	-	•		-		-				-		-	-	-										- 1		<u>P.5</u>	2.8	۰	Ξ.	L		<u>x</u>	0.1					0	<u> </u>	88		<u>.</u>	z.	а.	21
																								w A		C 3	58	7	03		•	x	L)	o	10	×	•	8	83	83	77	w	×	¥.	21
٠		٠	٠				٠				٠		۷		1	٧			8	٠	J.	с 1	C K	ι' x	D	c 3		z	γ3	x١	v٧	υ	τ,		۱a		0	м:	ж3	42	: 3	x	ж	0	P1 -
-		•		•	-																					87		¥	01	0		¥	1.1	7	10	Ŧ	-	50	-	12		-	Y	Ŧ	81
																								W D	C1	87	ίž	÷.	x١	ē,	70	Ť	¥ 1	i i	١ř	õ	8	M.	Εŝ	23	i	ú	ď.	8	81
٠	٠	٠	٠	٠		٠	٠	x	٠	٠	٠	L.	1	×		٠	τ.		e	۰	٠			⊢Ť	-	÷Ϋ	÷Ŧ	ŵ	÷.	1	÷	ŵ	-1	-	÷Ŕ	÷	с÷,	÷1	e-i	÷	гŵ	-10	÷	÷	#1 -
1	1	1	1	2		1		1	۰.	2	1	1	1											X 2	53	11	: 5	4	24	24	14	*	۳1	. 1	: 2	5	3	51	÷ 3	13	4	a	\$	41	8I -
																								6	-4	24	LZ.	۰	- 1	- 1	-4	4	-	-4	~	4	-	24	24	4	-0	4	۲.	24	a -
		٠			v			L.		υ	н	ĸ	٠		н	٠	٠	H		٠	z	۷ :		¥ A	20	υI	2.2	₫.;	01	53	11	×	73	- 2	22	٤.	9	ð١	83	73	Ľ	*	ž	x.	<u>81</u>
	1	1						1																- 3	Α.	z٦	r X	w	¥ !	C 1		*	a)	• •	, #	×	30	*		: *	10	1	*	v	
																					-				31	Ċ1	5 E	T	07	C	7	x	13	73	10	Σ	•	87	67	ert.	۲V	w	x	7	21
υ	4	٠	٠	٠	J	×			٧	н	۰	v	N	н	٠	¢	۳	×		۰	۲	6	8 7	1ª A	21	ŶĴ	ŧŵ	٠	τ.	r i	١Â	á	70	<b>,</b> ,	IŇ	z.	×	3	I İ	łŌ	١Ż	x	ñ	C	11
																									-	-	-	÷	-	-	-	÷	_	_	-	-	-	-	~	-	-	-	-	-	

NSA One-Time Pad (Source: Wikimedia)

- · What systems may we *implement*?
- · Perfect encryption
- · All messages are valid: Zero information!
- · Key as long as the message. . .
- · Key can only be used once.....

																									-			_	-	_		-				_									_
																						-			1.3	C	DI	: 7	G	ж	1.	2	Ľ	×	NC	17	0			T	σ,	1	73	Y	Z
					•		•••																	A 2	ΞŦ.	x:	ē ī	÷	Ŧ	5	ñ i	5	ō	N I		. 2	c 3	ī	ñ.	ā i	;;	έĒ	P C	ā	11
																								-	1	Ċ.	6 1		O.	ŵ	Ÿ7	12	Ť.	2	80	17	12	ΩŔ,	1			16	7 2	Ŷ	<b>%</b>
																									r x	÷	ŪΫ	-		ñ.	õ i	0		×		ć i	17	Ŧ	ā	÷		ò ē	5	12	ΞL
	-				-				- 1		۰.				-						-					÷.	÷ 1	r é		÷		nü	-		20			æ	*	24			-6	-6	ζI.
۰.	,	۳	*	۰	z	٠	×	٠	٠			×	x		٠	۰			•		•	.,	• •	C 3		23				*	:;	. 3	5			15		2	а.	5.	23	12		4	÷.
																										-	-	-1	- 2-	뵨	-	-6		÷.,	14	-	-8	~	4	84	<u>_</u>	68	.8	æ	41
										-						-				ъ.				D 1		0		1	•	프	11		-	-	NC	12	- 5	- 25		Ξ.	0.0		<u>م</u>	Ξ	Ξ١
٠	•	•		•	-		۶	٠	•	•	v	٠	۰	•	٠	•			•	٠	ь.	•••		- 9	<u> </u>	<u>v</u> .	τ.		•	2	0)		11	х.		. 25	10	x	x	D	с з		. z	T	<b>Æ</b> 1
																								· A		0	D X	.,	0	x	13	x	Ľ.	×:	NO		- 6	x	8	51	σ.	/w	/*	¥	21
									а.							•						• 1		~ v	10	T	5.2	. 9	7	0	83	11	ж	1	13	: 0		x	D	¢.;		. 2	X	x	w
	-	•		۰.	٠	•	٠	•	•	-	•	•	•	•		•	•	•		•	-		• •			0:	D X	7	0	н	n	x	1	X.	N C	12		ж	T	Ŧ1	0.8	18	72	Y	ΞI.
																								F 8	7 .	6		1.2	0	x	йİ	. 2	3	T I	K Q	. 7	ΥĒ	D	C.	ā.	ι.	4 12	x	ŵ	ΨÌ.
τ.		u			×									•	ы.						2		• •			71	2		6	v	75		10.7	ŝ	20	18	. 77	18	121	24	34	14	14	υ	÷L.
	-			-				~	•		۰.	-		•					•	•				0 7			5 F	6	2	Ξ.	ī.	3	7		Ξž	1	'n	ā	я.	11		ŕ 7	-	÷	61
																									-	8-	24	÷	-	θ.	**	-6	- 14		1	c R	18	÷	æ	84	ы	-77	10	÷	31
£	٧	J.	٠		٠	٠	×				к.	τ.	¥	٧	٧	τ.	к.		κ.	٠	τ.			ha 🕈		21	2 2	1		۰.	21		***	21	22	12	. 2	•		5.3	2.2			2	21
-		-		-		-		-	-		-						-			-				-	- T-	•	- 1	2		<u>.</u>	0.1	4	-	2	_				<b>a</b> .	<u>.</u>				<u>_</u>	21
																								T A		с:	DΣ	,	•	н	.,	x	L	к.	<b>x</b> 0	12	- 9	ж	8	51	79		x	x	<b>Z</b> I.
	н	c	J,	κ.		٠			*	٠	н	z	z			٠	z	۷		c	۷			· .	L Q.	<b>7</b> 1	<u> </u>	N	1.1	x.	,,	ж	0	23	εп	.0			Ζ.	x:	κ		υ	т	8I.
																										<u>c 3</u>	5 2	y	61	к	r7	x	17	en	10	- 12	- 0	ж	87	ŧ٦	77	14	12	¥	ži.
																								1 6		ō i	N N	ĽŻ.	x	3	11	0	7	E :	ĎČ	8		Ŧ	Ŷ.	ż١	٧Ý	/ΰ	Ŧ	ŝ	8
۷	r	1	υ	J	٠	٠	٠	٠	z	۰			D		٧	۰	v	۸.			٥	٤ 4		-	30	21	1.2	y	6	ŵ.	77	v	1.1	a٦	270	- 10		v	21	n	70	Λē	v	v	£1.
							-																	1× 7	0	23	47		51	γ.				67	n ž		. 7	÷	2	2	6 ÷	. 7	7	ñ	21
																									-8-	a-c	248	÷	÷.	ē-	-	÷	÷4	i.	-2	æ	-2	4	<del>9</del> 4	24		-	Æ	2	21
	٠	ь.	۰	κ.		н	x	١.		c	٠	1	Ð	۷	٠	0	۳.	κ.		z	Ð	z.		12 2			: 5			<u>a</u>	11	- 2	**	2	19	-5	. =	-	2.3	53	<u></u>		ā	x	<u>e</u> t -
																								- 0	28.	м.	6.8	ы.		л.			<u>.</u>			عد	12	<u>.</u>	w	<u>.</u>	- 1		2	2	51
																								M A		٥3	5 8	Y	01	ĸ	17	х	ы	K 3	• 0		۰.	ж	8.3	53	7 V	w	x	¥	Z
٥	1	N	۰		c		•		ĸ	٠	٠	٠	٧	٠.	c	٠	۳	٠	۰	1	٠	.,	• •	C_ N	LM.	IJ	κ 2	1	<b>X</b> (	٥.		D	C 1		1.2	x	x	w	¥ 1	21		. 8		۶.	0
																								N A		85	5 Z	Ŧ	67	80	7	x	17	20	70	7	76	х	81	n	ΥŸ	W	T	¥	ž[
															-									· M	11.1	κ.	11	н	01	<b>r</b> :	εn	C	31	6.3	t ¥	×	w	v	01		1.28	. 0	7	Ö.	н.
۰.	÷	٠	z		٠	z	٠		-	•	٠	۰	c	۰.	٠	٠	٠	۲	κ.	۰.	,	•	ι.	-		81	ιæ	Ŷ	81	r	2	¥	Ŧi	n	16	18	12	÷	27	- 1	10	10	ŵ	Ÿ	21
		•																						0 7			: 5	'n.	**	Ξ.	ñ ñ	5	11		: :		,÷	÷.	÷ ;		: 2		8	÷.	<b>2</b> 1
					-	-	а.	-										ы.				• •			-0-	64	ю	÷	÷۲	BH	н	ø	e.	ы	HR	æ	æ	÷	÷	н	ы	16	w	6	81
	-				٠	٠		•			•	•	٠	•	•	•	٠	•	•	•	۰.		•••	18 3		* :	: 2	4	21	2	::	~	**	24		.2		=	23	12	: 1	. 2	0	۵	21
																								<u> </u>	ч <b>с</b> .,	ы	1.2	s	84		64	۵	84	ы	1.0		-¥-	х.	84	24	ы.	-16	a	æ	81
		-					-		-	-	-							۰.		-				la ^		C 3	2 8	τ	0,	к.		×	-	6.2	10	×.		ж.	81	53	7 9	w	х	х.	<u>ē</u> )
۰	٠	٠	•	•	z	v	٠		•	•		•	•	•		٠	٠	•	۰.		•		• •	- 1	11	жs	22	х	21	<u>c ;</u>		x	x	<u>c s</u>	vv	v	л.	ж.	8.		• 0	с <b>н</b>	м	ы	81
																									. 3	01	5 8	r	0)	K.	5	x	13	o	10	Ŧ	0	х	57	er,	77	w	×	Y	2)
w															ε.			•		ы.				· ī		ā i	řΧ	D.	ē.)	Ξ.	i. 2	x	x١	23	10	Ŧ.	۰.	8	ā١	11	Ń	а	z.	x.	и.
•	•	•	٠	•			•	۰.	-	-	•	•	-	-		-	•	•		•	-			-		81	5 E	Ŧ	<u>a</u> 3	<b>6</b> - 1	-	¥	17	o	10	æ	6	81	67	F₹	rv.	- 92	¥	Y	21
																								18 V	0	77	iπ	è	17	Ă İ	żΫ	ÿ	÷	ĩ١	17	а.	×.	0	ž i	άŝ	ΠŇ.	εĒ.	÷	ž.	ΞL
						e				×	ь.							ь.		٠	٠	۱.	4 U		÷.	н	Hű	÷	<del>.</del> 4	н	н	ø	ñ	÷	ŀŔ	÷	*	e:	н		ю	-	÷	ŵ	21
•	٠		~	•		٠	۰.	•	-		•	۰.	•	•	•	-				-				T 2		2.5	22	٤.		24	12	2	**		: 2	2		с.	22	52	12	=	÷	а.	<u>- 12</u>
																									44	84	44	4	84	2	-4	ő	44	64	-8	4	4	64	24	и	N	4	۰	۵ł	81
					۰.						•							υ.		٠	٠			Y . A		сı	58	r	03	к.)		ж	1.1	Ω	10	æ		8	8.3	13	/ Y	w	×	x	ē) -
~	-	•		-		-				-		-	-	-										- 1		<u>P.5</u>	2.8	۰	Ξ.	L		<u>x</u>	0.1					0	<u> </u>	88		<u>.</u>	z.	а.	21
																								w A		C 3	58	7	03	1	•	x	L)	o	10	×	•	8	83	83	77	w	×	¥.	21
٠		٠	٠				٠				٠		۷		1	٧			8	٠	J.	с 1	C K	ι' x	D	c 3		z	γ3	x١	v٧	υ	τ,		۱a		0	м:	ж3	42	: 3	x	ж	0	P1 -
-		•		•	-																					87		¥	01	0		¥	1.1	7	10	Ŧ	-	50	-	12		-	Y	Ŧ	81
																								W D	C1	87	ίž	÷.	x١	ē,	70	Ť	¥ 1	i i	١ř	õ	8	M.	Εŝ	23	i	ú	ď.	8	81
٠	٠	٠	٠	٠		٠	٠	x	٠	٠	٠	L.	1	×		٠	τ.		e	۰	٠			⊢Ť	-	÷Ϋ	÷Ŧ	ŵ	÷.	1	÷	ŵ	-1	-	÷Ŕ	÷	с÷,	÷1	e-i	÷	гŵ	-10	÷	÷	#1 -
1	1	1	1	2		1		1	۰.	2	1	1	1											X 2	53	11	: 5	4	24	24	14	*	۳1	. 1	: 2	5	3	51	÷ 3	13	4	a	\$	41	8I -
																								6	-4	24	LZ.	۰	- 1	- 1	-4	4		-4	~	4	-	24	24	4	-0	4	۲.	24	a -
		٠			v			L.		υ	н	ĸ	٠		н	٠	٠	H		٠	z	۷ :		¥ A	20	υI	2.2	₫.;	01	53	11	×	73	- 2	22	٤.	9	ð١	83	73	Ľ	*	ž	x.	<u>81</u>
	1	1						1																- 3	Α.	z٦	r X	w	¥ !	C 1		*	a)	• •	, #	×	30	*		: *	10	1	*	v	
																					-				31	Ċ1	5 E	T	07	C	7	x	13	73	10	Σ	•	87	67	ert.	۲V	w	x	7	21
υ	4	٠	٠	٠	J	×			٧	н	۰	v	N	н	٠	¢	۳	×		۰	۲	6	8 7	1ª A	21	ŶĴ	ŧŵ	٠	τ.	r i	١Â	á	70	<b>,</b> ,	IŇ	z.	×	3	I İ	łŌ	١Ż	x	ñ	C	11
																									-	-	-	÷	-	-	-	÷	_	_	-	-	-	-	~	-	-	-	-	-	

NSA One-Time Pad (Source: Wikimedia)

- · What systems may we *implement*?
- · Perfect encryption
- · All messages are valid: Zero information!
- $\cdot\,$  Key as long as the message. . .
- · Key can only be used once.....

																		••			-	-	ABCDEFGHIJELMNOPGRETUWWXYZ
																							ZYXWVUTSBOPONMLKJINGFEDCBA
																							ABCDFFGWIJFFIWWOPOPEFTUWWY
																							"YXWYUTNBOPONNINJIWOYTDCBAZ
	_						-	- 1						-								-	INCOTONITY INCOMPANY
ч.	•	*	•		•		٠				×	x		٠	۰						•	τ.	C ABCDETGAISELAAOFGABIOVWAIA
																							XWVUISAUFONMLAJIMUFEDUBALI
	-	-							-												-	£	D ABCDEFGEIJELMNOFGESTUVWXYZ
۷		ĸ	τ,	۰.	,,	۰c	٠	•		v	٠	۳	٠		•	κ.	• •	•	• •		. 6	۰.	" WVUTSROPONMLKJINGFEDCBAZYX
																							. ABCDEFGHIJELMNOFGRETUVWYYZ
-	-	-							-	-													" VUTSBOPONNLYJINGFEDCRAZYXW
•	0	₽	•	•			٠	-		,	٠	×	L.	•	٠	L	• •	•				٠	ABODEEAWIIEIWWORAEEWWWWW
																							TTANGPONNININGFEDORISYTWY
									-														INCOMPTONY INTOTACE STRUCTURES
2	•	٠	•	•	•		•	•	-	٠	•	•		~	۰.	•		•	•••			•	o Anophi Salis than of the TUY WITA
																							TERUFURMENTINUFEDURALTEWVU
								-		~				~									ABCDEFGHIJELMNOPGRETUVWXYZ
٠	۰.	•	•		•		٠	•	•	•		•				•	•	•	•			•	" SROPONMLKJINGFEDCBAZTXWVUT
																							- ABCDEFORIJELMNOFORSTUVWXYZ
																	۰.				n.		B B B B B B B B B B B B B B B B B B B
-		•		•				•	-		•	•	-	-		•					-		ABCDEFONT J XI MNOPONATUTWYY
																							A BOXWINI VIINOFFDOBIEVYNYDTEB
¥			а.											*		•						٠	
		•				-		-	-			-	-		-						-		
																							FURMERIANTERCARTATION
		ь.				1 1	1		c	٠	1	Ð	۷		D	T I		•	2 6	13	H		L ASCDEFONIJELMNOFGESTUVWXYZ
		-																					- ONMLEJINGFEDUBALTXWVUTBRGF
																							M ABCDEFORIJKLMNOFGRETUVWXYZ
۰	1	N	•		: •					٠	٠	٧		c	٠	۳		•				•	
																							M ABCDEFORIJELMNOFGRETUVWXYZ
								-	-	-	-		-										"MLKJINGFEDCBAZYXWVUTSBGFON
2	÷	2		•	• •			-		٠		6	τ.		•	٠	•	•			•		- ABCDEFORIJELMNOFGESTUVWXYZ
																							LEJINGFEDCBAZYXWVUTSRGFONM
															ы.	•	υ.						- ABCDEFGELJELENOPOBETUVWYYZ
	-	-						-	•	-		•				•			•			-	* KIINGFEDCBAZYXWYUTEBOPONML
																							ABODYYOWI /VIWNOBOBE TUUWYYY
									ĸ		٧	4			e	z	ж 1			. 1			10 11000000000000000000000000000000000
						-																	118071000000000000000000000000000000000
																							A ABCDEFGHIJELMNOFGASTUVWXYZ
۷		1					٠			٠	٠	٠	4	L.		z	• •		υ.			κ.	- INGFEDCHALTAWYUTHAGFUNMLAJ
																							ABCDEFGRIJELMNOPGRSTUVWXYZ
																							" HOFEDCBAZYXWVUTSRQFONMLKJI
	۰		. :		16		٠	٠	•	r.	۰	ĸ	ε.	•	٠		• •	•	.,	. 1	•	v	_ ABCDEFGHIJKLMNOFGRSTUVWXYZ
																							T OFEDCRAZYXWVUTSRGFONMLXJIK
								-			-												ABCDEFORIJELMNOFGRETUVWXYZ
۰	ĸ	τ.	• •		. •	• •	٠			۷	٠	٠			•	٠	•	•	• •			•	FEDCBAZYXWYUTARGPONMLKJIRO
																							A BOOK FOWLINT WHO NO BERTHWAY
	_	1								-	-												V TROBATY XWYUTABAPONNI FIINOF
٠	۰	٠		•		•••					•	۰	•	٠		•	•		•	• •		•	THE REPORT OF THE OWNER OF THE WORKS
																							W CASHERS BUILT ANNUL SOLUTION
											۰.		۰.										DURALIANTOLIKAPONALETTAUFA
٠	•	٠	- 1		• •			-			*	*	-		1	۰.	- 1		• •			-	ABCDEFORIJELMNOFGRETUVWXYZ
																							- CHAZYXWVUTSRGFORMLEJIEOFED
						۰.	1.		u		×	٠		н	٠	٠			• 3	٤.			ABCDEFGEIJELMNOFGESTUVWXYZ
^	-	-	- 1	- '				2			^	1	~										BAZYXWVUTERGFONMLKJINGFEDC
																							- ABCDEFORIJELMNOFGESTUVWYYZ
υ	٠	٠	•	۰.	,,			۲	н	т	v	N	н	٠	c	۳		•	• •	• •		۳	AZYXWVUTSRGPONMLKJINGFEDCH
																							And and and the second s

NSA One-Time Pad (Source: Wikimedia)

- · What systems may we *implement*?
- · Perfect encryption
- · All messages are valid: Zero information!
- $\cdot\,$  Key as long as the message. . .
- $\cdot\,$  Key can only be used once.....

																									-			_	-	_		-				_									_
																						-			1.3	C	DI	: 7	G	ж	1.	2	Ľ	×	NC	17	0	R		T	σ,	~	73	Y	Z
					•		•••																	A 2	ΞŦ.	x:	ē ī	÷	Ŧ	5	ñ i	5	ō	N I		. 2	c 3	ī	ñ.	ā i	;;	έĒ	P C	ā	11
																								-	1	Ċ.	6 1		O.	ŵ	Ÿ7	12	Ť.	2	80	17	12	ΩŔ,	1			16	7 2	Ŷ	<b>%</b>
																									r x	÷	ŪΫ	-		ñ.	õ i	0		×		ć i	17	Ŧ	ā	÷		ò ē	5	12	ΞL
	-				-				- 1		۰.				-						-					÷.	÷ 1	r é	ā	÷		nü	-		20			æ	*	24			-6	-6	ζI.
۰.	,	۳	*	۰	z	٠	×	٠	٠			×	x		٠	۰			•		•	.,	• •	C 3		23				*	:;	. 3	5			15		2	а.	5.	23	12		4	÷.
																										-	-	-1	- 2-	뵨	-	-6		÷.,	14	-	-8	~	4	84	<u>_</u>	68	.8	æ	41
										-						-				ъ.				D 1		0		1	•	프	11		-	-	NC	12	- 5	- 25		Ξ.	0.0		<u>م</u>	Ξ	Ξ١
٠	•	•		•	-		۶	٠	•	•	v	٠	۰	•	٠	•			•	٠	ь.	•••		- 9	<u> </u>	<u>v</u> .	τ.		•	2	0)		11	x		. 25	10	x	x	D	с з		. z	T	<b>A</b> 1
																								· A		0	D X	.,	0	x	13	x	Ľ.	×:	NO		- 6	x	8	51	σ.	/w	/*	¥	21
									а.							•						• 1		~ v	10	T	5.2	. 9	7	0	83	11	ж	1	13	: 0		x	D	¢.;		. 2	X	x	w
	-	•		۰.	٠	•	٠	•	•	-	•	•	•	•		•	•	•		•	-		• •			0:	DX	7	0	Ħ	n	x	1	X.	N C	77			T	Ŧ1	0.8	18	72	Y	ΞI.
																								F 8	7 .	6		1.2	0	x	йİ	. 2	3	T I	K Q	. 7	ΥĒ	D	Q.	ā.	ι.	4 12	x	ŵ	ΨÌ.
τ.		u			×									•	ы.						2		• •			71	2		6	v	75		10.7	ŝ	20	18	. 77	18	121	24	34	14	14	υ	÷L.
	-			-				~	•		۰.	-		•					•	•				0 7			5 F	6	2	Ξ.	ī.	3	7		Ξž	1	'n	ā	я.	11		ŕ 7	-	÷	61
																									-	8-	24	÷	-	θ.	**	-6	- 14		1	c R	18	÷	æ	84	ы	-77	10	÷	31
£	٧	J.	٠		٠	٠	x				к.	τ.	¥	٧	٧	τ.	к.		κ.	٠	τ.			ha 🕈		21	2 2	1		۰.	21		***	21	22	12	. 2	•		5.3	2.2			2	21
-		-		-		-		-	-		-						-			-				-	- T-	•	- 1	2		<u>.</u>	0.1	4	-	2	_				<b>a</b> .	<u>.</u>				<u>_</u>	21
																								T A		с:	DΣ	,	•	н	.,	x	L	к.	<b>x</b> 0	12	- 9	ж	8	51	79		x	x	<b>Z</b> I.
	н	c	J,	ж.		٠			*	٠	н	z	z			٠	z	۷		c	۷			· .		<b>7</b> 1	<u> </u>	N	1.1	x.	,,	ж	0	23	εп	.0			Ζ.	x:	κ		υ	т	8I.
																										<u>c 3</u>	5 2	y	61	к	r7	x	17	en	10	- 12	- 0	ж	87	ŧ٦	77	14	12	¥	ži.
																								1 6		ō i	N N	ĽŻ.	x	3	11	0	7	E :	ĎČ	8		Ŧ	Ŷ.	ż١	٧Ý	/ΰ	Ŧ	ŝ	8
۷	r	1	υ	J	٠	٠	٠		z	۰			D		٧	۰	v	۸.			٥	٤ 4		-	30	21	1.2	y	ል	ŵ.	77	v	1.1	a٦	270	- 10		v	21	n	70	Λē	v	v	£1.
							-																	1× 7	0	23	47		51	γ.				67	n ž		. 7	÷	2	2	6 ÷	. 7	7	ñ	21
																								<u> </u>	-8-	a-c	248	÷	÷.	ē-	-	÷	÷4	i.	-2	æ	-2	4	<del>9</del> 4	24		-	Æ	2	21
	٠	ь.	۰	κ.		н	x	١.		c	٠	1	Ð	۷		0	۳.	κ.		z	Ð	z.		L 3			: 5			<u>a</u>	11	- 2	**	2	19	-5	. =	-	2.3	53	<u></u>		ā	x	<u>e</u> t -
																								- 0	28.	м.	6.8	ы.		л.			<u>.</u>			عد	12	<u>.</u>	w	<u>.</u>	- 1		2	2	<u>.</u>
																								M A		٥3	5 8	Y	01	ĸ	17	х	ы	K 3	• 0		۰.	ж	8.3	53	7 V	w	x	¥	Z
٥	1	N	۰		c		•		ĸ	٠	٠	٠	٧	٠.	c	٠	۳	٠	۰	1	٠	.,	• •	C_ N	LM.	IJ	κ 2	1	<b>X</b> (	٥.		D	C 1		1.2	x	x	w	¥ 1	21		. 8		۶.	0
																								N A		85	5 Z	Ŧ	67	80	7	x	17	20	70	7	76	х	81	n	ΥŸ	W	T	¥	ž[
															-									· M	11.1	κ.	11	н	01	<b>r</b> :	εn	C	31	6.3	t ¥	×	w	v	01		1.28	. 0	7	Ö.	н.
۰.	÷	٠	z		٠	z	٠		-	•	٠	۰	c	۰.	٠	٠	٠	۲	κ.	۰.	,	•	ι.	-		81	ιæ	Ŷ	81	r	2	¥	Ŧi	n	16	18	12	÷	27	- 1	10	10	ŵ	Ÿ	21
		•																						0 7			: 5	'n.	**	Ξ.	ñ ñ	5	11		: :		,÷	÷.	÷ ;		: 2		8	÷.	<b>2</b> 1
					-	-	а.	-										ы.				• •			-0-	64	ю	÷	÷۲	BH	н	ø	e.	ы	HR	æ	æ	÷	÷	н	ы	16	w	6	81
	-				٠	٠		•			•		٠	•	•	•	٠	•	•	•	۰.		•••	18 3		* :	: 2	4	21	2	::	~	**	24		.2		=	23	12	: 1	. 2	0	۵	21
																								<u> </u>	ч <b>с</b> .,	ы	1.2	s	84		64	۵	84	ы	1.0		-¥-	х.	84	24	ы.	-16	a	æ	81
		-					-		-	-	-							۰.		-				la ^		C 3	2 8	τ	0,	к.		×	-	6.2	10	×.		ж.	81	53	7 9	w	х	х.	<u>ē</u> )
۰	٠	٠	•	•	z	v	٠		•	•		•	•	•		٠	٠	•	۰.		•		• •	- 1	11	жs	22	х	21	<u>c ;</u>		x	x	<u>c s</u>	vv	v	л.	ж.	8.		• 0	с <b>н</b>	м	ы	81
																									. 3	01	5 8	r	0)	K.	5	x	13	o	10	Ŧ	0	х	57	er,	77	w	×	Y	2)
w															ε.			•		ы.				· ī		ā i	řΧ	D.	ē.)	Ξ.	i. 2	x	x١	23	10	Ŧ.	۰.	8	ā١	11	Ń	а	z.	x.	и.
•	•	•	٠	•			•	۰.	-	-	•	•	-	-		-	•	•		•	-			-		81	5 E	Ŧ	<u>a</u> 3	<b>6</b> - 1	-	¥	17	o	10	æ	6	81	67	F₹	rv.	- 92	¥	Y	21
																								18 V	0	77	iπ	è	17	Ă İ	żΫ	ÿ	÷	ĩ١	17	а.	×.	0	ž i	άŝ	ιŵ.	εĒ.	÷	ž.	ΞL
						e				×	ь.							ь.		٠	٠	۱.	4 U		÷.	н	Hű	÷	<del>~</del> (	н	н	ø	ñ	÷	ŀŔ	÷	*	e:	н		ю	-	÷	ŵ	21
•	٠		~	•		٠	۰.	•	-		•	۰.	•	•	•	-				-				T 2		2.5	22	٤.		24	12	2	**		: 2	2		с.	22	52	12	=	÷	а.	<u>- 12</u>
																									44	84	44	4	84	2	-4	ő	44	64	-8	4	4	64	24	и	N	4	۰	۵ł	81
					۰.						•							υ.		٠	٠			Y A		сı	58	r	03	к.)		ж	1.1	Ω	10	æ		8	8.3	13	/ Y	w	×	x	ē) -
~	-	•		-		-				-		-	-	-										- 1		<u>P.5</u>	2.8	۰	Ξ.	L		<u>x</u>	0.1					0	<u> </u>	88		<u>.</u>	z.	а.	21
																								w A		C 3	58	7	03	1	•	x	L)	o	10	×	•	8	83	83	77	w	×	¥.	21
٠		٠	٠				٠				٠		۷		1	٧			8	٠	J.	с 1	C K	ι' x	D	c 3		z	γ3	x١	v٧	υ	τ,		۱a		0	м:	ж3	42	: 3	x	ж	0	P1 -
-		•		•	-																					87		¥	01	0		¥	1.1	7	10	Ŧ	-	50	-	12		-	Y	Ŧ	81
																								W D	C1	87	ίž	÷.	x١	ē,	70	Ť	¥ 1	i i	١ř	õ	8	M.	Εŝ	23	i	ú	ď.	8	81
٠	٠	٠	٠	٠		٠	٠	x	٠	٠	٠	L.	1	×		٠	τ.		e	۰	٠			⊢Ť	-	÷Ϋ	÷Ŧ	ŵ	÷.	1	÷	ŵ	-1	-	÷Ŕ	÷	с÷,	÷1	e-i	÷	гŵ	-10	÷	÷	#1 -
1	1	1	1	2		1		1	۰.	2	1	1	1											X 2	53	11	: 5	4	24	24	14	*	۳1	. 1	: 2	5	3	51	÷ 3	13	4	a	\$	41	8I -
																								6	-4	24	LZ.	۰	- 1	- 1	-4	4	-	-4	~	4	-	24	24	4	-0	4	۲.	24	a -
		٠			v			L.		υ	н	ĸ	٠		н	٠	٠	H		٠	z	۷ :		¥ A	20	υI	2.2	₫.;	01	53	11	×	73	- 2	22	٤.	9	ð١	83	73	Ľ	*	ž	x.	<u>81</u>
	1	1						1																- 3	Α.	z٦	r X	w	¥ !	C 1		*	a)	• •	, #	×	30	*		: *	10	1	*	v	
																					-				31	Ċ1	5 E	T	07	C	7	x	13	73	10	Σ	•	87	67	ert.	۲V	w	x	7	21
υ	4	٠	٠	٠	J	×			٧	н	۰	v	N	н	٠	¢	۳	×		۰	۲	6	8 7	1ª A	21	ŶĴ	ŧŵ	٠	τ.	r i	١Â	á	70	<b>,</b> ,	IŇ	z.	×	3	I İ	łŌ	١Ż	x	ñ	C	11
																									-	-	-	÷	-	-	-	÷	_	_	-	-	-	-	~	-	-	-	-	-	

NSA One-Time Pad (Source: Wikimedia)

- · What systems may we *implement*?
- · Perfect encryption
- · All messages are valid: Zero information!
- $\cdot\,$  Key as long as the message. . .
- $\cdot\,$  Key can only be used once.....

																			_	ABCDEFGELITINNOPORETURNYYT
٠	••	•••	•••	•••	••	••	•••	•••	• • •	•••	•••	•••			•••	•••			-	
																				ELANT CIDENT CHALLES THUF EDUBA
																				B ABCDEFORIJELMNOFGRSTUVWXYZ
																				TXWVUTSRGPONMLXJINGFEDCBAZ
μ.				2				4	•			٠	Υ.				o z			- ABCDEFGHIJELMNOFGRETUVWXYZ
-				-	- 1		-	-	-			-			-			-	-	YWYUTSBOPONNI.YJINOPPOCBARY
																				ANCERPONT INTERACTOR CONTRACTOR OF
	•			14	•															p anoprioritation and the state
•	-	•		•		••	•	~	•	• •	•	•	•				•		•	WVUTSAUFURMLAJIAUFEDUBALTA
																				* ABCDEFGHIJELMNOFGRETUVWXYZ
									-										-	" VUTSROPONNLKJINGFEDCBAZYXW
•	•	• •		-		••	-	•	•	• •			•		••		• •	•		- ABCDEFONIJELMNOPOBETUVWYY
																				TTANGPONNIN/INOFEDCELEVEN
	•												Ξ.							INCOMPTONIC INCOMPTONIC
۰.	•	•••		•	•	•••	•	-	•	• •		~	•	•	•		• •		•	
																				TERUFURNERSINGFEDURALTEWVU
	-			-			-	-				-	- 1						-	ABCDEFGHIJELMNOPGESTUVWXYZ
	τ.			٠	•				•	•	π.	۰	τ.			•			•	* SEGFONMLEJINGFEDCBAITEWVUT
																				ABCDETOWIJELWNOPONATUWWYYZ
				-				-				-						÷.,		I BOROWNINI TITROFFICELEYYWYTE
٠	•	ς					٠	٠				٠	• •						•	Far On ALAST HOT LOODALIZATO
																				, ABCDEFGHIJKLMNOPGRATUVWXYZ
																				GPONMLEJINOFEDCBAZYXWVUTSR
۳	1	1 4	11		• •			۰	•	R D		۳	۰	۰.			ο c	•	۰.	- ABCDEFGHIJKLMNOFGESTUVWXYZ
																				* FORMLEJINOFEDCBAEYXWYUTSBQ
																				ABCOPPONITESTWOODOBESTOWEY
					н :	. 1		c	٠	10	٧.		0	т.		21	8 2			L ANCDEFORISELMNOFMENTUVWATE
																				- ONMLEJIROFEDUBALTXWVUTBAMF
																				ABCDEFORIJKLMNOFGRETUVWXYZ
٥	1			¢					٠		14	c	•	* 4					v	"NMLEJING7EDCBAZYXWVUTSRGPO
																				. ABCDEFONIJKLMNOFGRETUVWXYE
																				P ULLITE CEED CELTER PURCHAGE COOL
٤.	-	s 2		۰	Ζ.			Ð				٠	•	• •		- L I			۰.	ALL STANKER STANLASTON STANLASTON
2		κ.																		O ABCDEFORIJELMNOFGESTUVWITE
																				LKJINGFEDCBAZYXWVUTSRGFONM
		٢,		٠	• 1			1					u ·	٧١	ιε.	υ				. ABCDEFGHIJELMNOFGRETUVWXYZ
	_																			T NILLARREAR AND AND THE SCOOL OF
																				KI I HUTEDUBALIAWYUTBAUFURMU
																				A CONTRACTOR OF
	_												•		×					G ABCDEFGHIJELMNOFGRSTUVWXYZ
		• •	•	z				ĸ	,	۰.			c		۲	•	• •		×	A A C DEFGRIJELMNOFGASTUVWXYZ JINGFEDCBAZYXWVUTBAGFONMLK
		• •	•	z			•	ĸ	•	۰.		*	¢		۲	•	• •		×	G ABCDEFGHIJKLMNOPGBSTUVWXYZ 3 ABCDEFGHIJKLMNOPGBSTUVWXYZ 3 ABCDEFGHIJKLMNOPGBSTUVWXYZ
۷.		•••	•	2			:		:				•		•		• •		*	G ABCDEFGRIJELMNOFGRITUVWXY 3 JHOFEDCBAZYXWVUTBRQPONMLK 8 ABCDEFGRIJELMNOFGRITUVWXY 8 ABCDEFGRIJELMNOFGRITUVWXY 1 HOFEDCBAZYXWVUTBRQPONMLKJ
۷		• •		z H			:	8 6			•								*	ABCDEFGELIKLMNOFGETUVWYT     ACTINGFEDCBAZYWVTTBRGFONMLX     ASCDEFGEJIKLMNOFGETUVWYT     INGFEDCBAZYWVTTBRGFONMLX     ASCDEFGEJIKLMNOFGETUVWYT
۷	E			2 H				к 4			•	•			•				*	
-				2 H				•			•		•		•				*	A 1 D 1 Y 1 D C B 4 Y 2 C B 4 H D V C B 4 R D V W Y 1 C B 4 H D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C B 4 R D V C C C B 4 R D V C C B A D V C C B 4 R D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V C C B A D V
•				2 H 0			:	к 4 ж		•••	•	N L 0					* *		*	A 3 C D 5 C C C C C C C C C C C C C C C C C
•		10		2 H 8				к 4 ж		•••		N L 0							×	A         1         0         1         0         1         0
-				2 H				•											*	G         A         C         A
	E 0   E			2 H .			:	• •											*	
	E 0			2 H .			:	•	-							•			*	
	E 0			х н • .															*	
	E E T			2 H A L Z								N L D M I	C				8 1 8 1 8 1 8 1 8 1 8 1 8 1 8 1 8 1 8 1		*	
	E 0 E			2 H e L Z				•					с ж ж				* 1 * 1 * 1		× ×	
	E 0 E			2 H . L . Z	0 0			•					C						*	
		• • • • • • • •		z x a L z J			• • • • •			• •			с ж ж ч				8 7 K U A 1 C P		*	
	e • •	0 N 1 0 N 1		2 H A L Z J			• • • •			* . * * * *			C			•	8 7 K U A 1 C P		х х х х	
		0 N 1 0 1 N 1 N		2 H A L Z J			• • • •						C		•		8 7 K U A 1 U C P	с н х	* * * * *	
		a N 1 0 7 N 1 N		х н <b>а</b> L X J J						• J							8 7 K U A 1 C P U C A 2 V		* * * *	
	E 7 8	a N 1 0 7 N 1 N 4 P		х н е L X J J	0 0	. 2 							с ж ж ч		•		8 7 8 0 8 0 8 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9	E 	* * *	
	E 7 5	0 N 1 0 7 N 1 P		х н а L х J J						• • • • • •		N L D M I 4 H	с ж ж ч		•		8 7 8 0 8 0 8 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9 0 9	к н к	* * *	
				х н е L х J J J															* * * * * * *	

NSA One-Time Pad (Source: Wikimedia)

#### · Make *computational* assumptions

- · Limit computational resources
- · 1. Make problems intricate
- · 2. Make *hardness* assumptions
- · Security is assumed, not proven

AES round (Source: Wikimedia)

Used everywhere in the information-world

### $b^x = a \mod q$ Find x

Discrete logarithm problem

- · Make *computational* assumptions
- · Limit computational resources
- · 1. Make problems intricate
- · 2. Make *hardness* assumptions
- · Security is assumed, not proven

AES round (Source: Wikimedia)

Used everywhere in the information-world

### $b^x = a \mod q$ Find x

Discrete logarithm problem

- · Make *computational* assumptions
- · Limit computational resources
- · 1. Make problems intricate
- · 2. Make *hardness* assumptions
- · Security is assumed, not proven



AES round (Source: Wikimedia)

 $b^x = a \mod q$ Find x

Discrete logarithm problem

- · Make *computational* assumptions
- · Limit computational resources
- · 1. Make problems intricate
- · 2. Make *hardness* assumptions
- · Security is assumed, not proven



AES round (Source: Wikimedia)

 $b^x = a \mod q$ Find x

Discrete logarithm problem

- · Make *computational* assumptions
- · Limit computational resources
- · 1. Make problems intricate
- · 2. Make *hardness* assumptions
- $\cdot\,$  Security is assumed, not proven



(Source: Wikimedia)

 $b^x = a \mod q$ Find x

Discrete logarithm problem

- · Make *computational* assumptions
- · Limit computational resources
- · 1. Make problems intricate
- · 2. Make *hardness* assumptions
- $\cdot$  Security is assumed, not proven



AES round (Source: Wikimedia)

 $b^x = a \mod q$ Find x

Discrete logarithm problem

#### · Existence of *pseudo-entanglement is necessary for EFI pairs*

- · Constructive result: weakest construction of pseudo-entangled states (not PRSs)
- · Polynomial amplification of pseudo-entanglement
- · New candidate for *minimal assumption* for computational cryptography
- · Connection between *computational hardness/cryptography and physics*

- · Existence of *pseudo-entanglement is necessary for EFI pairs*
- · Constructive result: weakest construction of pseudo-entangled states (not PRSs)
- · Polynomial amplification of pseudo-entanglement
- · New candidate for *minimal assumption* for computational cryptography
- · Connection between *computational hardness/cryptography and physics*

- · Existence of *pseudo-entanglement is necessary for EFI pairs*
- · Constructive result: weakest construction of pseudo-entangled states (not PRSs)
- · Polynomial amplification of pseudo-entanglement
- · New candidate for *minimal assumption* for computational cryptography
- · Connection between *computational hardness/cryptography and physics*

- · Existence of *pseudo-entanglement is necessary for EFI pairs*
- · Constructive result: weakest construction of pseudo-entangled states (not PRSs)
- · Polynomial *amplification of pseudo-entanglement*
- · New candidate for *minimal assumption* for computational cryptography
- · Connection between *computational hardness/cryptography and physics*

- · Existence of *pseudo-entanglement is necessary for EFI pairs*
- · Constructive result: weakest construction of pseudo-entangled states (not PRSs)
- · Polynomial *amplification of pseudo-entanglement*
- · New candidate for *minimal assumption* for computational cryptography
- · Connection between computational hardness/cryptography and physics

#### Contents

Introduction

#### Fundamentals of Cryptography

EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

Discussion

Classical Cryptography



Classical Cryptography



# Quantum Cryptography



# Quantum Cryptography



# Quantum Cryptography



- · Impossibility of many Information-Theoretic protocols
- Classical (computational) cryptography  $\Longrightarrow \mathbf{P} \neq \mathbf{NP}$
- · Quantum resources  $\implies$  weaker Commitments, OT, QKD, ...
- · Assume correctness of the Laws of Physics
- · New computational world: Quantum Cryptography, but no Classical Cryptography

- · Impossibility of many Information-Theoretic protocols
- $\cdot$  Classical (computational) cryptography  $\Longrightarrow \mathbf{P} 
  eq \mathbf{NP}$
- · Quantum resources  $\implies$  weaker Commitments, OT, QKD, ...
- · Assume correctness of the Laws of Physics
- · New computational world: Quantum Cryptography, but no Classical Cryptography

- · Impossibility of many Information-Theoretic protocols
- $\cdot$  Classical (computational) cryptography  $\Longrightarrow \mathbf{P} 
  eq \mathbf{NP}$
- · *Quantum resources*  $\implies$  weaker Commitments, OT, QKD, ...
- · Assume correctness of the Laws of Physics
- · New computational world: Quantum Cryptography, but no Classical Cryptography

- · Impossibility of many Information-Theoretic protocols
- · Classical (computational) cryptography  $\Longrightarrow \mathbf{P} 
  eq \mathbf{NP}$
- · *Quantum resources*  $\implies$  weaker Commitments, OT, QKD, ...
- · Assume correctness of the Laws of Physics
- · New computational world: Quantum Cryptography, but no Classical Cryptography

- · Impossibility of many Information-Theoretic protocols
- · Classical (computational) cryptography  $\Longrightarrow \mathbf{P} 
  eq \mathbf{NP}$
- · *Quantum resources*  $\implies$  weaker Commitments, OT, QKD, ...
- · Assume correctness of the Laws of Physics
- · New computational world: Quantum Cryptography, but no Classical Cryptography

- · Impossibility of many Information-Theoretic protocols
- · Classical (computational) cryptography  $\Longrightarrow \mathbf{P} \neq \mathbf{NP}$
- · *Quantum resources*  $\implies$  weaker Commitments, OT, QKD, ...
- · Assume correctness of the Laws of Physics
- · New computational world: Quantum Cryptography, but no Classical Cryptography

#### Contents

Introduction

#### Fundamentals of Cryptography

#### EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

Discussion

### Weaker Primitives

· One-Way Functions



· Pseudo-Random Generator



 $\begin{array}{l} \mathsf{OWF} \Longrightarrow \mathsf{PRSG} \\ \mathsf{PRSG} \nleftrightarrow (\mathsf{oracle red.}) \ \mathsf{OWF} \end{array}$ 

Pseudo-Random State Generator

- $\cdot$  Efficient gen. (QPT):  $G_n(k) = \ket{\psi_k}$
- · Pseudo-random:  $G_n(k)^{\otimes p(n)} \approx_c |H\rangle^{\otimes p(n)}$

### Weaker Primitives

· One-Way Functions



· Pseudo-Random Generator



 $OWF \implies PRSG$  $PRSG \implies (oracle red.) OWF$ 

#### Pseudo-Random State Generator

- $\cdot$  Efficient gen. (QPT):  $G_n(k) = \ket{\psi_k}$
- · Pseudo-random:  $G_n(k)^{\otimes p(n)} \approx_c |H\rangle^{\otimes p(n)}$

### Weaker Primitives

· One-Way Functions



· Pseudo-Random Generator



Pseudo-Random State Generator

- $\cdot$  Efficient gen. (QPT):  $G_n(k) = \ket{\psi_k}$
- · Pseudo-random:  $G_n(k)^{\otimes p(n)} \approx_c |H\rangle^{\otimes p(n)}$

$$\label{eq:owf} \begin{array}{l} \mathsf{OWF} \Longrightarrow \mathsf{PRSG} \\ \\ \mathsf{PRSG} \not\Longrightarrow \text{(oracle red.) OWF} \end{array}$$
Mixed *n*-qubit states  $\rho_0, \rho_1$ 

- $\cdot$  Efficiently preparable: QPT  $\mathcal{U}_0, \mathcal{U}_1$
- $\cdot$  statistically Far:  $\mathsf{TD}(
  ho_0,
  ho_1)=1-arepsilon$
- $\cdot$  computationally Indistinguishable:  $ho_0pprox_c
  ho_1$





Mixed *n*-qubit states  $\rho_0, \rho_1$ 

- · Efficiently preparable: QPT  $\mathcal{U}_0, \mathcal{U}_1$
- · statistically Far:  $\mathsf{TD}(
  ho_0,
  ho_1)=1-arepsilon$
- $\cdot$  computationally Indistinguishable:  $ho_0pprox_c
  ho_1$





Mixed *n*-qubit states  $\rho_0, \rho_1$ 

- · Efficiently preparable: QPT  $\mathcal{U}_0, \mathcal{U}_1$
- · statistically Far:  $\mathsf{TD}(\rho_0, \rho_1) = 1 \varepsilon$
- $\cdot$  computationally Indistinguishable:  $ho_0pprox_c
  ho_1$





Mixed *n*-qubit states  $\rho_0, \rho_1$ 

- · Efficiently preparable: QPT  $\mathcal{U}_0, \mathcal{U}_1$
- · statistically Far:  $\mathsf{TD}(\rho_0, \rho_1) = 1 \varepsilon$
- $\cdot$  computationally Indistinguishable:  $\rho_0 \approx_c \rho_1$





Mixed *n*-qubit states  $\rho_0, \rho_1$ 

- · Efficiently preparable: QPT  $\mathcal{U}_0, \mathcal{U}_1$
- · statistically Far:  $\mathsf{TD}(\rho_0, \rho_1) = 1 \varepsilon$
- · computationally Indistinguishable:  $\rho_0 \approx_c \rho_1$





$$\mathsf{EFI} \; \mathsf{Pairs} \Longleftrightarrow \mathsf{Commitments} \Longleftrightarrow \mathsf{OT} \Longleftrightarrow \mathsf{MPC}$$

Probability ensembles  $X = \{X_n\}_n, Y = \{Y_n\}_n$ 

- Efficiently constructible: PPT  $\mathcal{S}_0, \mathcal{S}_1$
- statistically Far:  $\mathsf{SD}(X,Y) = 1 arepsilon$
- $\cdot$  computationally Indistinguishable:  $-Xpprox_c Y$





 $\mathsf{EFID}\ \mathsf{Pairs} \Longleftrightarrow \mathsf{PRG} \Longleftrightarrow \mathsf{OWF}$ 

Probability ensembles  $X = \{X_n\}_n, Y = \{Y_n\}_n$ 

- · Efficiently constructible: PPT  $S_0, S_1$
- statistically Far:  $\mathsf{SD}(X,Y) = 1 \varepsilon$
- $\cdot$  computationally Indistinguishable:  $Xpprox_{c}Y$



 $Y_n \leftarrow \mathcal{S}_1(n)$ 



Probability ensembles  $X = \{X_n\}_n, Y = \{Y_n\}_n$ 

- · Efficiently constructible: PPT  $S_0, S_1$
- · statistically Far:  $SD(X, Y) = 1 \varepsilon$
- $\cdot$  computationally Indistinguishable:  $Xpprox_{c}Y$



$$Y_n \leftarrow \mathcal{S}_1(n)$$

 $\mathsf{EFID}\ \mathsf{Pairs} \Longleftrightarrow \mathsf{PRG} \Longleftrightarrow \mathsf{OWF}$ 

Probability ensembles  $X = \{X_n\}_n, Y = \{Y_n\}_n$ 

- · Efficiently constructible: PPT  $\mathcal{S}_0, \mathcal{S}_1$
- · statistically Far:  $SD(X, Y) = 1 \varepsilon$
- $\cdot$  computationally Indistinguishable:  $X pprox_c Y$







Probability ensembles  $X = \{X_n\}_n, Y = \{Y_n\}_n$ 

- · Efficiently constructible: PPT  $\mathcal{S}_0, \mathcal{S}_1$
- · statistically Far:  $SD(X, Y) = 1 \varepsilon$
- · computationally Indistinguishable:  $X \approx_c Y$



$$Y_n \leftarrow \mathcal{S}_1(n)$$

$$\mathsf{EFID}\ \mathsf{Pairs} \Longleftrightarrow \mathsf{PRG} \Longleftrightarrow \mathsf{OWF}$$

#### Contents

Introduction

Fundamentals of Cryptography

EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

Discussion

## Computational Entanglement

#### Entanglement cost

- $\cdot$  Given  $\Phi;$  use LOCC to prepare  $\rho_{AB}$
- · How many Bell pairs do they need?

 $E_C^{\varepsilon}(\rho_{AB}) = \inf\{n \,|\, \mathcal{F}(\Gamma(\Phi^{\otimes n}), \rho_{AB}) \le 1 - \varepsilon\}$ 

#### Distillable entanglement

- $\cdot$  Given  $ho_{AB}$ ; use LOCC to distill  $\Phi$
- · How many Bell pairs can they get?

$$E_D^{\varepsilon}(\rho_{AB}) = \sup\{m \,|\, \mathcal{F}(\Gamma(\rho_{AB}), \Phi^{\otimes m}) \le 1 - \varepsilon\}$$

Restrict LOCC operations to QPT

Computational entanglement cost: Computational distillable entanglement:

## Computational Entanglement

#### Entanglement cost

- $\cdot$  Given  $\Phi;$  use LOCC to prepare  $\rho_{AB}$
- · How many Bell pairs do they need?

#### Distillable entanglement

- $\cdot\,$  Given  $\rho_{AB};$  use LOCC to distill  $\Phi$
- · How many Bell pairs can they get?

 $E_C^{\varepsilon}(\rho_{AB}) = \inf\{n \,|\, \mathcal{F}(\Gamma(\Phi^{\otimes n}), \rho_{AB}) \le 1 - \varepsilon\}$ 

$$E_D^{\varepsilon}(\rho_{AB}) = \sup\{m \,|\, \mathcal{F}(\Gamma(\rho_{AB}), \Phi^{\otimes m}) \le 1 - \varepsilon\}$$

Restrict LOCC operations to QPT

Computational entanglement cost: Computational distillable entanglement:

## Computational Entanglement

#### Entanglement cost

- $\cdot$  Given  $\Phi;$  use LOCC to prepare  $\rho_{AB}$
- · How many Bell pairs do they need?

#### Distillable entanglement

- $\cdot\,$  Given  $\rho_{AB};$  use LOCC to distill  $\Phi$
- · How many Bell pairs can they get?

 $E_C^{\varepsilon}(\rho_{AB}) = \inf\{n \,|\, \mathcal{F}(\Gamma(\Phi^{\otimes n}), \rho_{AB}) \le 1 - \varepsilon\}$ 

$$E_D^{\varepsilon}(\rho_{AB}) = \sup\{m \,|\, \mathcal{F}(\Gamma(\rho_{AB}), \Phi^{\otimes m}) \le 1 - \varepsilon\}$$

Restrict LOCC operations to QPT

Computational entanglement cost: Computational distillable entanglement:

 $\hat{E}_C^{\varepsilon}$ 

 $\hat{E}_D^{\varepsilon}$ 

#### $\psi_{AB}$ , $\phi_{AB}$ *n*-qubit mixed states

 $\cdot \,\,\psi_{AB}$  has low entanglement

$$\hat{E}_C^{\varepsilon}(\psi_{AB}) \le c(n)$$

 $\cdot \phi_{AB}$  has high entanglement

 $E_D^\varepsilon(\pmb{\phi_{AB}}) \geq d(n)$ 

· Computational ind. t = poly(n) copies



#### $\psi_{AB}$ is pseudo-entangled

- $\cdot \ \psi_{AB}$  efficient to prepare (LOCC)
- $\cdot \phi_{AB}$  must exist
- · Use  $\psi_{AB}$  instead of  $\phi_{AB}$

 $\psi_{AB}$ ,  $\phi_{AB}$  *n*-qubit mixed states

 $\cdot \hspace{0.1 cm} \psi_{AB}$  has low entanglement

$$\hat{E}_C^{\varepsilon}(\psi_{AB}) \leq c(n)$$

 $\cdot \phi_{AB}$  has high entanglement

 $E_D^\varepsilon(\pmb{\phi_{AB}}) \geq d(n)$ 

· Computational ind. t = poly(n) copies



#### $\psi_{AB}$ is pseudo-entangled

- $\cdot \psi_{AB}$  efficient to prepare (LOCC)
- $\cdot \phi_{AB}$  must exist
- · Use  $\psi_{AB}$  instead of  $\phi_{AB}$

 $\psi_{AB}$ ,  $\phi_{AB}$  *n*-qubit mixed states

 $\cdot \,\,\psi_{AB}$  has low entanglement

$$\hat{E}_C^{\varepsilon}(\psi_{AB}) \le c(n)$$

 $\cdot \phi_{AB}$  has high entanglement

 $E_D^{\varepsilon}(\phi_{AB}) \ge d(n)$ 

· Computational ind. t = poly(n) copies



 $\psi_{AB}$  is pseudo-entangled

- $\cdot \psi_{AB}$  efficient to prepare (LOCC)
- $\cdot \phi_{AB}$  must *exist*
- · Use  $\psi_{AB}$  instead of  $\phi_{AB}$

 $\psi_{AB}$ ,  $\phi_{AB}$  *n*-qubit mixed states

 $\cdot \,\,\psi_{AB}$  has low entanglement

$$\hat{E}_C^{\varepsilon}(\psi_{AB}) \le c(n)$$

 $\cdot \phi_{AB}$  has high entanglement

 $E_D^{\varepsilon}(\phi_{AB}) \ge d(n)$ 

· Computational ind. t = poly(n) copies

$$\psi_{AB}^{\otimes t} pprox_c \phi_{AB}^{\otimes t}$$

 $\psi_{AB}$  is pseudo-entangled

- $\cdot \psi_{AB}$  efficient to prepare (LOCC)
- $\cdot \phi_{AB}$  must *exist*
- · Use  $\psi_{AB}$  instead of  $\phi_{AB}$

 $\psi_{AB}$ ,  $\phi_{AB}$  *n*-qubit mixed states

 $\cdot \,\,\psi_{AB}$  has low entanglement

$$\hat{E}_C^{\varepsilon}(\psi_{AB}) \le c(n)$$

 $\cdot \phi_{AB}$  has high entanglement

 $E_D^{\varepsilon}(\phi_{AB}) \ge d(n)$ 

· Computational ind. t = poly(n) copies

$$\psi_{AB}^{\otimes t} \approx_c \phi_{AB}^{\otimes t}$$

 $\psi_{AB}$  is pseudo-entangled

- $\cdot \psi_{AB}$  efficient to prepare (LOCC)
- $\cdot \phi_{AB}$  must *exist*
- Use  $\psi_{AB}$  instead of  $\phi_{AB}$

 $W = \{W_i\}_i, Z = \{Z_i\}_i$  distr. ensembles

- $\cdot \ W$  has low entropy
- $\cdot$  Z has high entropy
- $\cdot \, W$  and Z are computational ind.

 $W = \{W_i\}_i, Z = \{Z_i\}_i$  distr. ensembles

- $\cdot W$  has low entropy
- $\cdot$  Z has high entropy
- $\cdot \, W$  and Z are computational ind.

 $W = \{W_i\}_i, Z = \{Z_i\}_i$  distr. ensembles

- $\cdot W$  has low entropy
- $\cdot$  Z has high entropy
- $\cdot \, W$  and Z are computational ind.

 $W = \{W_i\}_i, Z = \{Z_i\}_i$  distr. ensembles

- $\cdot W$  has low entropy
- $\cdot$  Z has high entropy
- $\cdot W$  and Z are computational ind.

 $W = \{W_i\}_i, Z = \{Z_i\}_i$  distr. ensembles

- $\cdot W$  has low entropy
- $\cdot$  Z has high entropy
- $\cdot \ W$  and Z are computational ind.

EFID pair  $X = \{X_n\}_n Y = \{Y_n\}_n$ 

 $\cdot B \sim \text{Bernoulli}\left(\frac{1}{2}\right)$ 

$$W_i = \begin{cases} (0,X_i) & \text{wp. } \frac{1}{2} \\ (1,Y_i) & \text{wp. } \frac{1}{2} \end{cases}$$

$$Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$$

 $W = \{W_i\}_i, Z = \{Z_i\}_i$  distr. ensembles

- $\cdot W$  has low entropy
- $\cdot$  Z has high entropy
- $\cdot W$  and Z are computational ind.

EFID pair  $X = \{X_n\}_n Y = \{Y_n\}_n$ 

 $\cdot B \sim \text{Bernoulli}\left(\frac{1}{2}\right)$ 

$$W_i = \begin{cases} (0,X_i) & \text{wp. } \frac{1}{2} \\ (1,Y_i) & \text{wp. } \frac{1}{2} \end{cases}$$

$$Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$$

 $W = \{W_i\}_i, Z = \{Z_i\}_i$  distr. ensembles

- $\cdot W$  has low entropy
- $\cdot$  Z has high entropy
- $\cdot \ W$  and Z are computational ind.

 $\begin{array}{l} \cdot B \sim \operatorname{Bernoulli}\left(\frac{1}{2}\right) \\ \cdot W_{i} = \begin{cases} (0, X_{i}) & \operatorname{wp.} \ \frac{1}{2} \\ (1, Y_{i}) & \operatorname{wp.} \ \frac{1}{2} \end{cases} \\ \cdot Z_{i} = \begin{cases} (B, X_{i}) & \operatorname{wp.} \ \frac{1}{2} \\ (B, Y_{i}) & \operatorname{wp.} \ \frac{1}{2} \end{cases} \end{array}$ 

 $\mathsf{False entropy} \Longleftrightarrow \mathsf{EFID pairs} \Longleftrightarrow \mathsf{OWF}$ 

EFID pair  $X = \{X_n\}_n$   $Y = \{Y_n\}_n$ 

 $W = \{W_i\}_i, Z = \{Z_i\}_i$  distr. ensembles

- $\cdot W$  has low entropy
- $\cdot$  Z has high entropy
- $\cdot \ W$  and Z are computational ind.

EFID pair  $X = \{X_n\}_n$   $Y = \{Y_n\}_n$  $\cdot B \sim \text{Bernoulli}\left(\frac{1}{2}\right)$  $W_{i} = \begin{cases} (0, X_{i}) & \text{wp. } \frac{1}{2} \\ (1, Y_{i}) & \text{wp. } \frac{1}{2} \end{cases}$  $\cdot Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$ 

 $W = \{W_i\}_i, Z = \{Z_i\}_i$  distr. ensembles

- $\cdot W$  has low entropy
- $\cdot$  Z has high entropy
- $\cdot \ W$  and Z are computational ind.

EFID pair  $X = \{X_n\}_n Y = \{Y_n\}_n$  $\cdot B \sim \text{Bernoulli}\left(\frac{1}{2}\right)$  $\cdot W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$  $\cdot Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$ 

$$\mathsf{False \ entropy} \Longleftrightarrow \mathsf{EFID \ pairs} \Longleftrightarrow \mathsf{OWF}$$

EFI pair  $\rho_0$ ,  $\rho_1$ 

$$\psi_{AB} = \frac{1}{4} \left( |\Phi^+\rangle\!\langle\Phi^+|_{AB} + |\Phi^-\rangle\!\langle\Phi^-|_{AB} \right) \otimes \left(\rho_{0A} + \rho_{1A}\right)$$

$$\phi_{AB} = \frac{1}{2} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} \otimes \rho_{0A} + |\Phi^-\rangle \langle \Phi^-|_{AB} \otimes \rho_{1A} \right)$$

EFI pair  $\rho_0$ ,  $\rho_1$ 

$$\psi_{AB} = \frac{1}{4} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} + |\Phi^-\rangle \langle \Phi^-|_{AB} \right) \otimes \left( \rho_{0A} + \rho_{1A} \right)$$

$$\phi_{AB} = \frac{1}{2} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} \otimes \rho_{0A} + |\Phi^-\rangle \langle \Phi^-|_{AB} \otimes \rho_{1A} \right)$$

$$\psi_{AB} = \frac{1}{4} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} + |\Phi^-\rangle \langle \Phi^-|_{AB} \right) \otimes \left( \rho_{0A} + \rho_{1A} \right)$$

 $\cdot \,\,A$  flips fair coin, prepares  $\cdot$ 

$$ho_0$$
 if  $H$   
 $ho_1$  if  $T$ 

· A flips fair coin, prepares  $\begin{cases} |0\rangle\langle 0| & \text{tells } B \text{ to prepare } |0\rangle\langle 0| & \text{if } H \\ |1\rangle\langle 1| & \text{tells } B \text{ to prepare } |1\rangle\langle 1| & \text{if } T \end{cases}$ 

$$\hat{E}_{C}^{0}\left(\psi_{AB}\right)=0$$

$$\psi_{AB} = \frac{1}{4} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} + |\Phi^-\rangle \langle \Phi^-|_{AB} \right) \otimes \left( \rho_{0A} + \rho_{1A} \right)$$

 $\cdot A$  flips fair coin, prepares  $\left\{ {}^{\prime} \right\}$ 

$$\begin{array}{cc} \rho_0 & \text{if } H \\ \rho_1 & \text{if } T \end{array}$$

$$\hat{E}_{C}^{0}\left(\psi_{AB}\right)=0$$

$$\psi_{AB} = \frac{1}{4} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} + |\Phi^-\rangle \langle \Phi^-|_{AB} \right) \otimes \left( \rho_{0A} + \rho_{1A} \right)$$

$$\begin{array}{l} \cdot \ A \ \text{flips fair coin, prepares} \begin{cases} \rho_0 & \text{if } H \\ \rho_1 & \text{if } T \end{cases} \\ \cdot \ A \ \text{flips fair coin, prepares} \begin{cases} |0\rangle\langle 0| & \text{tells } B \ \text{to prepare } |0\rangle\langle 0| & \text{if } H \\ |1\rangle\langle 1| & \text{tells } B \ \text{to prepare } |1\rangle\langle 1| & \text{if } T \end{cases}$$

$$\hat{E}_{C}^{0}\left(\psi_{AB}\right)=0$$

$$\psi_{AB} = \frac{1}{4} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} + |\Phi^-\rangle \langle \Phi^-|_{AB} \right) \otimes \left( \rho_{0A} + \rho_{1A} \right)$$

$$\begin{array}{l} \cdot \ A \ \text{flips fair coin, prepares} \begin{cases} \rho_0 & \text{if } H \\ \rho_1 & \text{if } T \end{cases} \\ \cdot \ A \ \text{flips fair coin, prepares} \begin{cases} |0\rangle\langle 0| & \text{tells } B \ \text{to prepare } |0\rangle\langle 0| & \text{if } H \\ |1\rangle\langle 1| & \text{tells } B \ \text{to prepare } |1\rangle\langle 1| & \text{if } T \end{cases}$$

$$\hat{E}_{C}^{0}\left(\psi_{AB}\right) = 0$$

#### EFI Pairs $\implies$ Pseudo-Entanglement Proof (Distillation of $\phi_{AB}$ )

$$\phi_{AB} = \frac{1}{2} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} \otimes \rho_{0A} + |\Phi^-\rangle \langle \Phi^-|_{AB} \otimes \rho_{1A} \right)$$

$$\cdot \operatorname{TD}(\rho_0, \rho_1) = 1 - \varepsilon$$

· Unbounded A distinguishes  $ho_0, 
ho_1$  and tells B

$$\cdot \begin{cases} \rho_0 & \text{then} & |\Phi^+\rangle_{AB} \\ \rho_1 & \text{then} & |\Phi^-\rangle_{AB} \end{cases}$$

$$E_D^{\varepsilon}\left(\phi_{AB}\right) = 1$$

#### EFI Pairs $\implies$ Pseudo-Entanglement Proof (Distillation of $\phi_{AB}$ )

$$\phi_{AB} = \frac{1}{2} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} \otimes \rho_{0A} + |\Phi^-\rangle \langle \Phi^-|_{AB} \otimes \rho_{1A} \right)$$

· 
$$\operatorname{TD}(\rho_0, \rho_1) = 1 - \varepsilon$$

· Unbounded A distinguishes  $ho_0, 
ho_1$  and tells B

$$\cdot \begin{cases} \rho_0 & \text{then} & |\Phi^+\rangle_{AB} \\ \rho_1 & \text{then} & |\Phi^-\rangle_{AB} \end{cases}$$

$$E_D^{\varepsilon}\left(\phi_{AB}\right) = 1$$
#### EFI Pairs $\implies$ Pseudo-Entanglement Proof (Distillation of $\phi_{AB}$ )

$$\phi_{AB} = \frac{1}{2} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} \otimes \rho_{0A} + |\Phi^-\rangle \langle \Phi^-|_{AB} \otimes \rho_{1A} \right)$$

• 
$$\operatorname{TD}(\rho_0, \rho_1) = 1 - \varepsilon$$

 $\cdot \,$  Unbounded A distinguishes  $\pmb{\rho_0}, \rho_1$  and tells B

$$\cdot \begin{cases} 
ho_0 & {\rm then} & |\Phi^+
angle_{AB} \\ 
ho_1 & {\rm then} & |\Phi^-
angle_{AB} \end{cases}$$

$$E_D^{\varepsilon}\left(\phi_{AB}\right) = 1$$

#### EFI Pairs $\implies$ Pseudo-Entanglement Proof (Distillation of $\phi_{AB}$ )

$$\phi_{AB} = \frac{1}{2} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} \otimes \rho_{0A} + |\Phi^-\rangle \langle \Phi^-|_{AB} \otimes \rho_{1A} \right)$$

• 
$$\operatorname{TD}(\rho_0, \rho_1) = 1 - \varepsilon$$

 $\cdot \,$  Unbounded A distinguishes  $\pmb{\rho_0}, \rho_1$  and tells B

$$\cdot \begin{cases} 
ho_0 & ext{then} & |\Phi^+\rangle_{AB} \\ 
ho_1 & ext{then} & |\Phi^-\rangle_{AB} \end{cases}$$

$$E_D^{\varepsilon}\left(\phi_{AB}\right) = 1$$

#### EFI Pairs $\implies$ Pseudo-Entanglement Proof (Distillation of $\phi_{AB}$ )

$$\phi_{AB} = \frac{1}{2} \left( |\Phi^+\rangle \langle \Phi^+|_{AB} \otimes \rho_{0A} + |\Phi^-\rangle \langle \Phi^-|_{AB} \otimes \rho_{1A} \right)$$

• 
$$\operatorname{TD}(\rho_0, \rho_1) = 1 - \varepsilon$$

 $\cdot \,$  Unbounded A distinguishes  $\pmb{\rho_0}, \rho_1$  and tells B

$$\cdot \begin{cases} 
ho_0 & ext{then} & |\Phi^+\rangle_{AB} \\ 
ho_1 & ext{then} & |\Phi^-\rangle_{AB} \end{cases}$$

$$E_D^{\varepsilon}\left(\phi_{AB}\right) = 1$$

$$\operatorname{Adv}_{\mathcal{D}}(\rho_{0},\rho_{1}) \leq \varepsilon \quad \Longrightarrow \quad \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB},\phi_{AB}) \leq \varepsilon'$$

$$\begin{array}{c} \cdot \\ \begin{cases} \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_1) & \longrightarrow \psi_{AB}, \phi_{AE} \\ \\ \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_0) & \longrightarrow \psi_{AB} \end{cases} \end{cases}$$

- Distinguish  $\frac{1}{2}$  the times
- $\cdot \,\, {\cal D}'$  can prepare  $\psi_{AB}$  and  $\phi_{AB}$  locally

 $\begin{aligned} \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) &\leq \frac{1}{2} \operatorname{Adv}_{\mathcal{D}}(\rho_0, \rho_1) < \varepsilon \\ \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) &\leq t \varepsilon \end{aligned}$ 

$$\operatorname{Adv}_{\mathcal{D}}(\rho_0, \rho_1) \leq \varepsilon \quad \Longrightarrow \quad \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) \leq \varepsilon'$$

$$\cdot \begin{cases} \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_1) \longrightarrow \psi_{AB}, \phi_{AB} \\ \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_0) \longrightarrow \psi_{AB} \end{cases}$$

- Distinguish  $\frac{1}{2}$  the times
- $\cdot \,\, {\cal D}'$  can prepare  $\psi_{AB}$  and  $\phi_{AB}$  locally

 $\begin{aligned} \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) &\leq \frac{1}{2} \operatorname{Adv}_{\mathcal{D}}(\rho_0, \rho_1) < \varepsilon \\ \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) &\leq t \,\varepsilon \end{aligned}$ 

$$\operatorname{Adv}_{\mathcal{D}}(\rho_0, \rho_1) \leq \varepsilon \quad \Longrightarrow \quad \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) \leq \varepsilon'$$

$$\begin{cases} \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_1) \longrightarrow \psi_{AB}, \phi_{AB} \\ \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_0) \longrightarrow \psi_{AB} \end{cases}$$

· Distinguish  $\frac{1}{2}$  the times

.

 $\cdot \,\, {\cal D}'$  can prepare  $\psi_{AB}$  and  $\phi_{AB}$  locally

 $\begin{aligned} \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) &\leq \frac{1}{2} \operatorname{Adv}_{\mathcal{D}}(\rho_0, \rho_1) < \varepsilon \\ \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) &\leq t \,\varepsilon \end{aligned}$ 

$$\operatorname{Adv}_{\mathcal{D}}(\rho_0, \rho_1) \leq \varepsilon \implies \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) \leq \varepsilon'$$

$$\begin{cases} \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_1) \longrightarrow \psi_{AB}, \phi_{AB} \\ \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_0) \longrightarrow \psi_{AB} \end{cases}$$

· Distinguish  $\frac{1}{2}$  the times

.

 $\cdot \,\, {\cal D}'$  can prepare  $\psi_{AB}$  and  $\phi_{AB}$  locally

 $\begin{aligned} \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) &\leq \frac{1}{2} \operatorname{Adv}_{\mathcal{D}}(\rho_0, \rho_1) < \varepsilon \\ \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) &\leq t \,\varepsilon \end{aligned}$ 

$$\operatorname{Adv}_{\mathcal{D}}(\rho_0, \rho_1) \leq \varepsilon \implies \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) \leq \varepsilon'$$

$$\begin{cases} \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_1) \longrightarrow \psi_{AB}, \phi_{AB} \\ \mathcal{D}'(|\Phi^+\rangle\!\langle\Phi^+|\otimes\rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\!\langle\Phi^-|\otimes\rho_0) \longrightarrow \psi_{AB} \end{cases}$$

- · Distinguish  $\frac{1}{2}$  the times
- $\cdot \,\, {\cal D}'$  can prepare  $\psi_{AB}$  and  $\phi_{AB}$  locally

 $\begin{aligned} \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) &\leq \frac{1}{2} \operatorname{Adv}_{\mathcal{D}}(\rho_{0}, \rho_{1}) < \varepsilon \\ \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) &\leq t \varepsilon \end{aligned}$ 

$$\overline{\psi}_{AB} = \bigotimes_{i=1}^{q} \psi_{AB}$$
  $\overline{\phi}_{AB} = \bigotimes_{i=1}^{q} \phi_{AB}$ 

Error:

$$\cdot \ \mathcal{F}(\rho^{\otimes q}, \, \sigma^{\otimes q}) = \mathcal{F}(\rho, \, \sigma)^q \implies (1-\varepsilon)^q \geq 1-q \, \varepsilon$$

Swap:

$$\begin{cases} \overline{\psi}_{AB}^{\otimes p} = (\bigotimes_{i=1}^{q} \psi_{AB})^{\otimes p} = \bigotimes_{i=1}^{q} (\psi_{AB}^{\otimes p}) \\ \overline{\phi}_{AB}^{\otimes p} = (\bigotimes_{i=1}^{q} \phi_{AB})^{\otimes p} = \bigotimes_{i=1}^{q} (\phi_{AB}^{\otimes p}) \end{cases}$$

 $\operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes p}, \phi_{AB}^{\otimes p}) \leq \varepsilon$  $\operatorname{Adv}_{\mathcal{D}'}(\overline{\psi}_{AB}^{\otimes p}, \overline{\phi}_{AB}^{\otimes p}) \leq q \varepsilon$ 

$$\overline{\psi}_{AB} = \bigotimes_{i=1}^{q} \psi_{AB}$$
  $\overline{\phi}_{AB} = \bigotimes_{i=1}^{q} \phi_{AB}$ 

Error:

$$\cdot \ \mathcal{F}(\rho^{\otimes q}, \, \sigma^{\otimes q}) = \mathcal{F}(\rho, \, \sigma)^q \implies (1 - \varepsilon)^q \ge 1 - q \, \varepsilon$$

Swap:

$$\begin{cases} \overline{\psi}_{AB}^{\otimes p} = (\bigotimes_{i=1}^{q} \psi_{AB})^{\otimes p} = \bigotimes_{i=1}^{q} (\psi_{AB}^{\otimes p}) \\ \overline{\phi}_{AB}^{\otimes p} = (\bigotimes_{i=1}^{q} \phi_{AB})^{\otimes p} = \bigotimes_{i=1}^{q} (\phi_{AB}^{\otimes p}) \end{cases}$$

 $\operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes p}, \phi_{AB}^{\otimes p}) \leq \varepsilon$  $\operatorname{Adv}_{\mathcal{D}'}(\overline{\psi}_{AB}^{\otimes p}, \overline{\phi}_{AB}^{\otimes p}) \leq q \varepsilon$ 

$$\overline{\psi}_{AB} = \bigotimes_{i=1}^{q} \psi_{AB} \qquad \qquad \overline{\phi}_{AB} = \bigotimes_{i=1}^{q} \phi_{AB}$$

Error:

$$\cdot \ \mathcal{F}(\rho^{\otimes q}, \, \sigma^{\otimes q}) = \mathcal{F}(\rho, \, \sigma)^q \implies (1 - \varepsilon)^q \ge 1 - q \, \varepsilon$$

Swap:

$$\cdot \begin{cases} \overline{\psi}_{AB}^{\otimes p} = (\bigotimes_{i=1}^{q} \psi_{AB})^{\otimes p} = \bigotimes_{i=1}^{q} (\psi_{AB}^{\otimes p}) \\ \overline{\phi}_{AB}^{\otimes p} = (\bigotimes_{i=1}^{q} \phi_{AB})^{\otimes p} = \bigotimes_{i=1}^{q} (\phi_{AB}^{\otimes p}) \end{cases}$$

 $\operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes p}, \phi_{AB}^{\otimes p}) \leq \varepsilon$  $\operatorname{Adv}_{\mathcal{D}'}(\overline{\psi}_{AB}^{\otimes p}, \overline{\phi}_{AB}^{\otimes p}) \leq q \varepsilon$ 

$$\overline{\psi}_{AB} = \bigotimes_{i=1}^{q} \psi_{AB} \qquad \qquad \overline{\phi}_{AB} = \bigotimes_{i=1}^{q} \phi_{AB}$$

Error:

$$\cdot \ \mathcal{F}(\rho^{\otimes q}, \, \sigma^{\otimes q}) = \mathcal{F}(\rho, \, \sigma)^q \implies (1 - \varepsilon)^q \ge 1 - q \, \varepsilon$$

Swap:

$$\begin{cases} \overline{\psi}_{AB}^{\otimes p} = (\bigotimes_{i=1}^{q} \psi_{AB})^{\otimes p} = \bigotimes_{i=1}^{q} (\psi_{AB}^{\otimes p}) \\ \overline{\phi}_{AB}^{\otimes p} = (\bigotimes_{i=1}^{q} \phi_{AB})^{\otimes p} = \bigotimes_{i=1}^{q} (\phi_{AB}^{\otimes p}) \end{cases}$$

$$\begin{aligned} \operatorname{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes p}, \phi_{AB}^{\otimes p}) &\leq \varepsilon \\ \operatorname{Adv}_{\mathcal{D}'}(\overline{\psi}_{AB}^{\otimes p}, \overline{\phi}_{AB}^{\otimes p}) &\leq q \,\varepsilon \end{aligned}$$

#### Contents

Introduction

Fundamentals of Cryptography

EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

Discussion

- · If *pseudo-entanglement* does not exist, then most cryptography is impossible.
- · New candidate for a *minimal assumption* necessary for cryptography.
- · Connect the properties of the physical world and efficient computation.
- ? Candidates for pseudo-entanglement?
- ? Applications of pseudo-entanglement?

- · If *pseudo-entanglement* does not exist, then most cryptography is impossible.
- · New candidate for a *minimal assumption* necessary for cryptography.
- · Connect the properties of the *physical world and efficient computation*.
- ? Candidates for pseudo-entanglement?
- ? Applications of pseudo-entanglement?

- · If *pseudo-entanglement* does not exist, then most cryptography is impossible.
- · New candidate for a *minimal assumption* necessary for cryptography.
- · Connect the properties of the *physical world and efficient computation*.
- ? Candidates for pseudo-entanglement?
- ? Applications of pseudo-entanglement?

- · If *pseudo-entanglement* does not exist, then most cryptography is impossible.
- · New candidate for a *minimal assumption* necessary for cryptography.
- · Connect the properties of the *physical world and efficient computation*.
- ? Candidates for pseudo-entanglement?
- ? Applications of pseudo-entanglement?

- · If *pseudo-entanglement* does not exist, then most cryptography is impossible.
- · New candidate for a *minimal assumption* necessary for cryptography.
- · Connect the properties of the *physical world and efficient computation*.
- ? Candidates for pseudo-entanglement?
- ? Applications of pseudo-entanglement?

- · If *pseudo-entanglement* does not exist, then most cryptography is impossible.
- · New candidate for a *minimal assumption* necessary for cryptography.
- · Connect the properties of the *physical world and efficient computation*.
- ? Candidates for pseudo-entanglement?
- ? Applications of pseudo-entanglement?

- · If *pseudo-entanglement* does not exist, then most cryptography is impossible.
- · New candidate for a *minimal assumption* necessary for cryptography.
- · Connect the properties of the *physical world and efficient computation*.
- ? Candidates for pseudo-entanglement?
- ? Applications of pseudo-entanglement?