



Pseudo-Entanglement is Necessary for EFI Pairs

Manuel Goulão with David Elkouss

Portugal Crypto Day — 13th of December of 2024

Overview

Introduction

Fundamentals of Cryptography

EPI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EPI Pairs

Discussion

Contents

Introduction

Fundamentals of Cryptography

EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

Discussion

Cryptography

- 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.....

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E X X W V U T S R G P O N M L K J I N G F E D C B A
N V V V U T S R G P O N M L K J I N G F E D C B A
Y X X W V U T S R G P O N M L K J I N G F E D C B A
G A C D E F G H I J K L M N O P Q R S T U V W X Y Z
X X W V U T S R G P O N M L K J I N G F E D C B A
D G U U T S R G P O N M L K J I N G F E D C B A
H A C D E F G H I J K L M N O P Q R S T U V W X Y Z
V U T S R G P O N M L K J I N G F E D C B A
F G U U T S R G P O N M L K J I N G F E D C B A
Y X X W V U T S R G P O N M L K J I N G F E D C B A
O A C D E F G H I J K L M N O P Q R S T U V W X Y Z
T R Q P O N M L K J I N G F E D C B A Z Y X W V U
H A C D E F G H I J K L M N O P Q R S T U V W X Y Z
S R Q P O N M L K J I N G F E D C B A
I A C D E F G H I J K L M N O P Q R S T U V W X Y Z
B R P O N M L K J I N G F E D C B A
J G P O N M L K J I N G F E D C B A
K A C D E F G H I J K L M N O P Q R S T U V W X Y Z
P O N M L K J I N G F E D C B A Z Y X W V U T S R Q
L A C D E F G H I J K L M N O P Q R S T U V W X Y Z
G M E K T P H G D A C B F D E G H I J K L M N O P Q R S T U V W X Y Z
A C D E F G H I J K L M N O P Q R S T U V W X Y Z
M N M L K J I N G F E D C B A Z Y X W V U T S R Q P O
W M L K J I N G F E D C B A
N A C D E F G H I J K L M N O P Q R S T U V W X Y Z
R M L K J I N G F E D C B A
O L X X J I N G F E D C B A Z Y X W V U T S R Q P O N M
P A C D E F G H I J K L M N O P Q R S T U V W X Y Z
K I N G F E D C B A Z Y X W V U T S R Q P O N M L K J I N G F E D C B A
A C D E F G H I J K L M N O P Q R S T U V W X Y Z
J I N G F E D C B A Z Y X W V U T S R Q P O N M L K J I N G F E D C B A
B A C D E F G H I J K L M N O P Q R S T U V W X Y Z
I N G F E D C B A Z Y X W V U T S R Q P O N M L K J I N G F E D C B A
H A C D E F G H I J K L M N O P Q R S T U V W X Y Z
N O F E D C B A Z Y X W V U T S R Q P O N M L K J I N G F E D C B A
T A F E D C B A Z Y X W V U T S R Q P O N M L K J I N G F E D C B A
U A C D E F G H I J K L M N O P Q R S T U V W X Y Z
F E D C B A Z Y X W V U T S R Q P O N M L K J I N G F E D C B A
V A C D E F G H I J K L M N O P Q R S T U V W X Y Z
E D C B A Z Y X W V U T S R Q P O N M L K J I N G F E D C B A
W A C D E F G H I J K L M N O P Q R S T U V W X Y Z
C S C A T X W V U T S R Q P O N M L K J I N G F E D C B A
X A C D E F G H I J K L M N O P Q R S T U V W X Y Z
G M G O N M L K J I N G F E D C B A
Y A C D E F G H I J K L M N O P Q R S T U V W X Y Z
B A E Y X W V U T S R Q P O N M L K J I N G F E D C B A
Z A C D E F G H I J K L M N O P Q R S T U V W X Y Z
A Z Y X W V U T S R Q P O N M L K J I N G F E D C B A

NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

- 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.....

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	U	T	
Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	U	
X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	
Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	
W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W
V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X
U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z
T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y
S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P
G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O
H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N
I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M
J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L
K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	L
L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J
M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I
N	M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H
O	N	M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G
P	O	N	M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R
Q	P	O	N	M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S
R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S
S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T
T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W	V	U
U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W	V
V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W
W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X
Z	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	X

NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

- 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.....

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	U	
N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	W	U	V	S	T	R	Q	P	O	
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	

NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

- 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.....

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	U	T
V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F
U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E
S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C
R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B
G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A
H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W
I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U
J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y
K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W
L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U
M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y
N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W
O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U
P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y
Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W
Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U
Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y

NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

- 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.....

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	U	T	
Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	U	
X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	
Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	
W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W
V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X
U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z
T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y
S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P
G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O
H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N
I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M
J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	K	L
K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J	L
L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I	J
M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H	I
N	M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G	H
O	N	M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R	G
P	O	N	M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S	R
Q	P	O	N	M	L	K	J	I	H	G	R	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S
R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T	S
S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W	V	U	T
T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W	V	U
U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W	V
V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X	W
W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	Z	X
Z	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	S	T	U	V	W	Z	X	Y	X

NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

- 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.....

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	X	W	V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	U	T
V	U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F
U	T	S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E
S	R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C
R	G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B
G	H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A
H	I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W
I	J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U
J	K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y
K	L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W
L	M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U
M	N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y
N	O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W
O	P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U
P	Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y
Q	Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W
Y	Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U
Z	X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y
X	W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W
W	V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U
V	R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y
R	S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W
S	T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U
T	U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y
U	F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W
F	E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U
E	D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y
D	C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W
C	B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U
B	A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y
A	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W	U	Y	W

NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Computational Cryptography

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

$$b^x = a \pmod{q}$$

Find x

Discrete logarithm problem

AES round
(Source: Wikimedia)

Used everywhere in the information-world

Computational Cryptography

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

$$b^x = a \pmod{q}$$

Find x

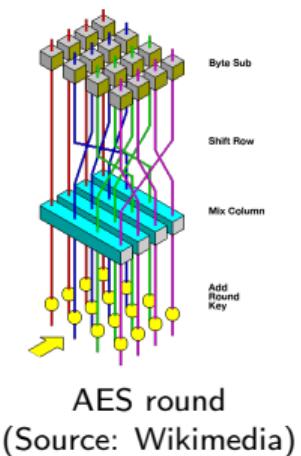
Discrete logarithm problem

AES round
(Source: Wikimedia)

Used everywhere in the information-world

Computational Cryptography

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



$$b^x = a \pmod{q}$$

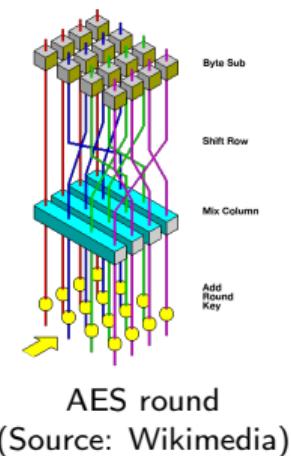
Find x

Discrete logarithm problem

Used everywhere in the information-world

Computational Cryptography

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



$$b^x = a \pmod{q}$$

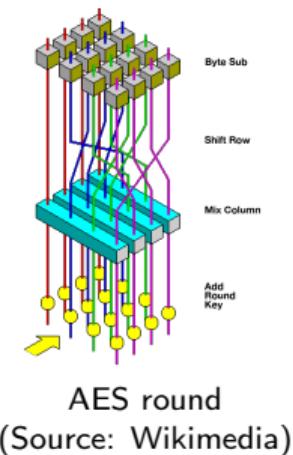
Find x

Discrete logarithm problem

Used everywhere in the information-world

Computational Cryptography

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



$$b^x = a \pmod{q}$$

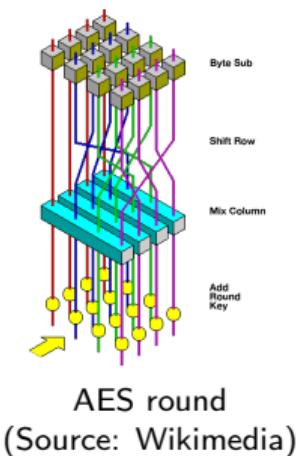
Find x

Discrete logarithm problem

Used everywhere in the information-world

Computational Cryptography

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



$$b^x = a \pmod{q}$$

Find x

Discrete logarithm problem

Used everywhere in the information-world

Contributions

- Existence of *pseudo-entanglement is necessary for EPI 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*

Contributions

- Existence of *pseudo-entanglement is necessary for EPI 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*

Contributions

- Existence of *pseudo-entanglement is necessary for EPI 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*

Contributions

- 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*

Contributions

- Existence of *pseudo-entanglement is necessary for EPI 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

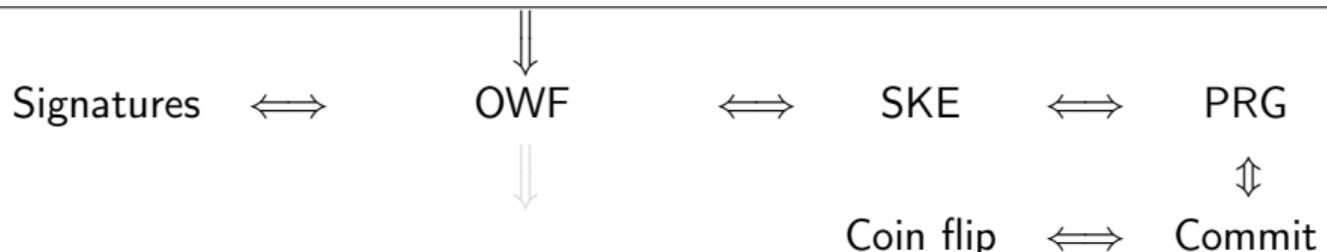
Discussion

Classical Cryptography

Cryptomania



Minicrypt



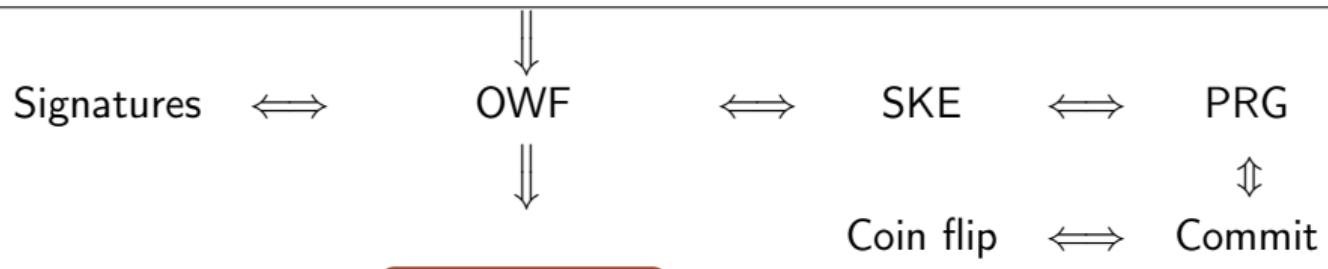
$P \neq NP$

Classical Cryptography

Cryptomania



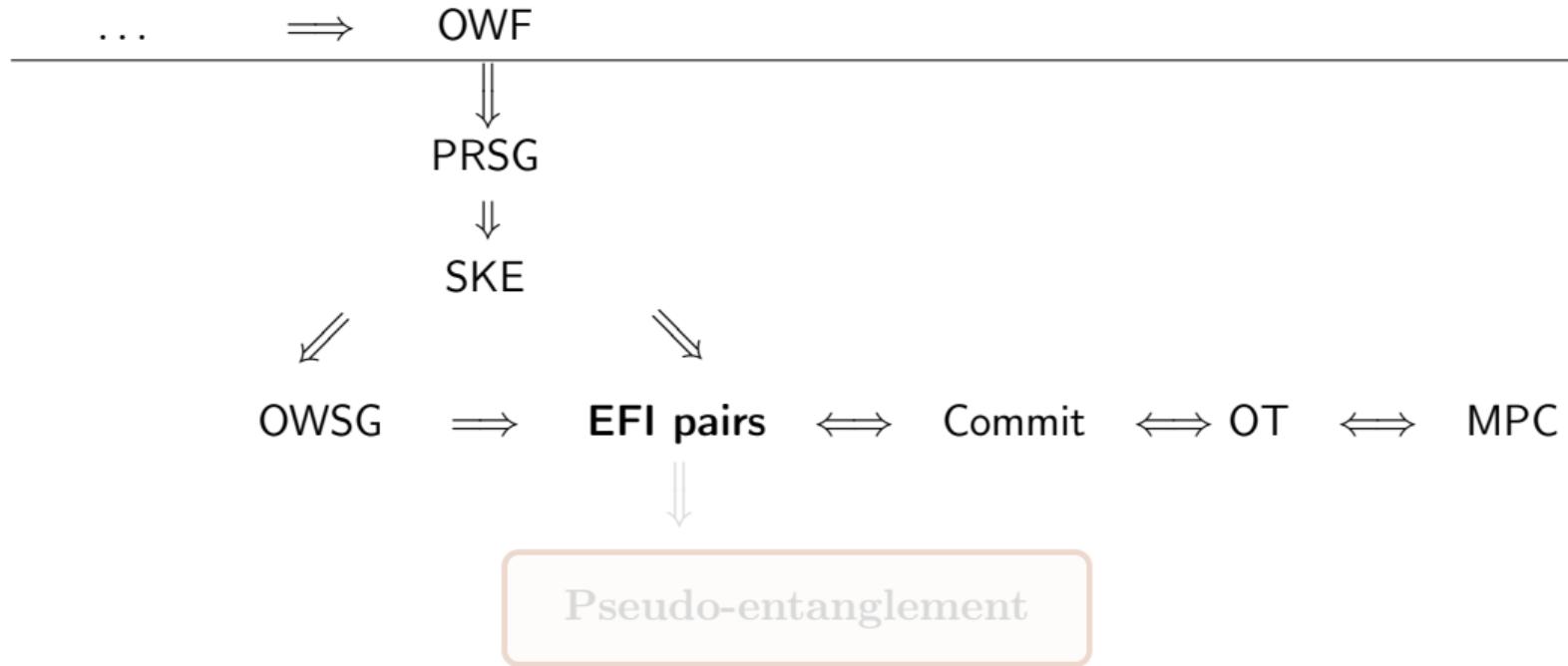
Minicrypt



$P \neq NP$

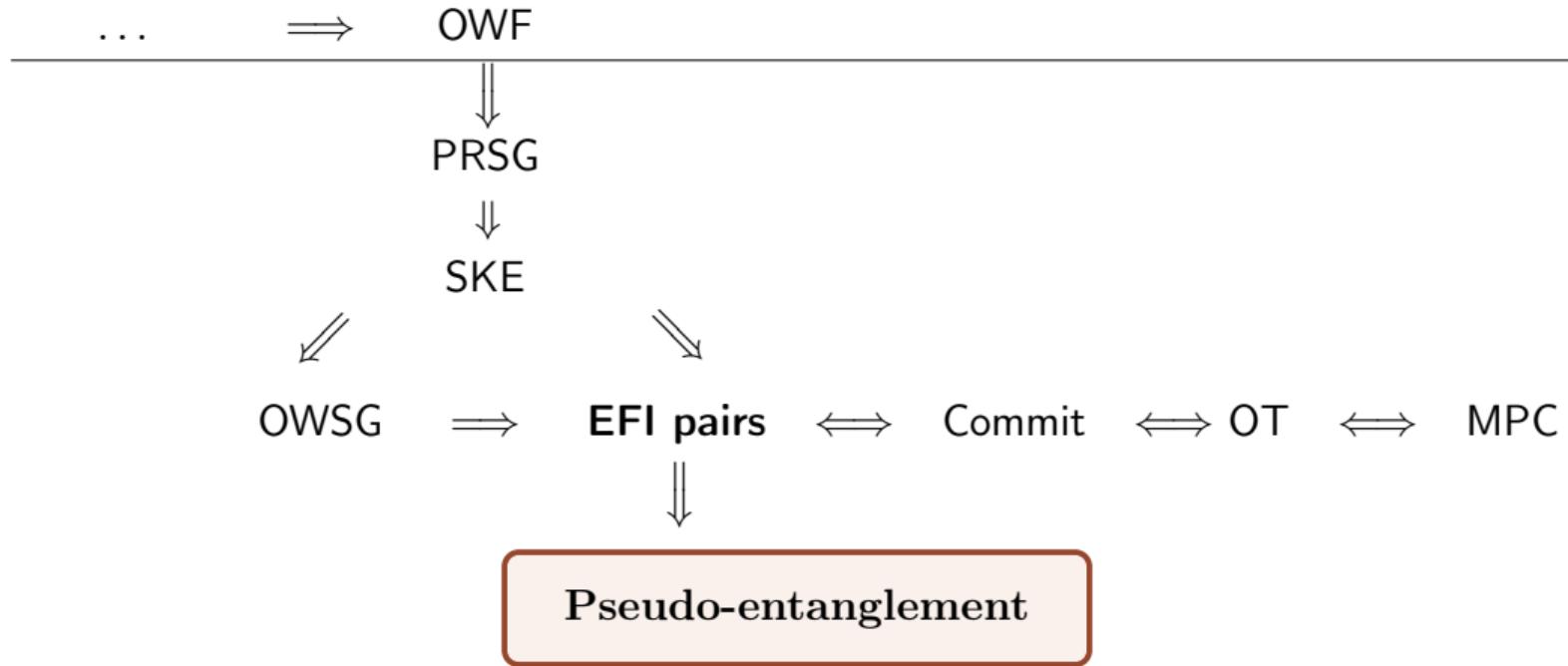
Quantum Cryptography

Minicrypt



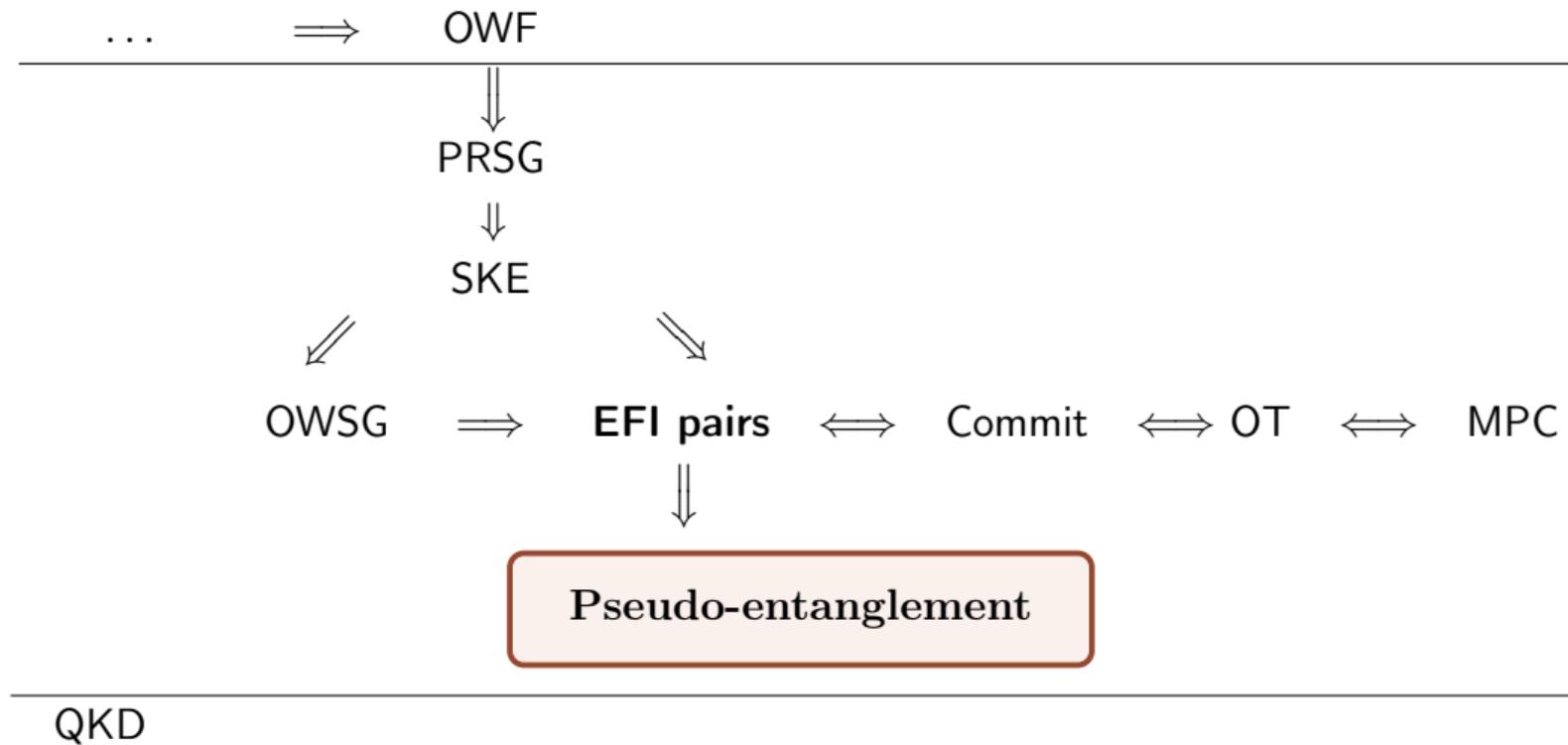
Quantum Cryptography

Minicrypt



Quantum Cryptography

Minicrypt



Classical vs. Quantum Cryptography

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

How physics and computational hardness relate through cryptography?

Classical vs. Quantum Cryptography

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

How physics and computational hardness relate through cryptography?

Classical vs. Quantum Cryptography

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

How physics and computational hardness relate through cryptography?

Classical vs. Quantum Cryptography

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

How physics and computational hardness relate through cryptography?

Classical vs. Quantum Cryptography

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

How physics and computational hardness relate through cryptography?

Classical vs. Quantum Cryptography

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

How physics and computational hardness relate through cryptography?

Contents

Introduction

Fundamentals of Cryptography

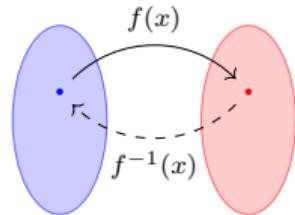
EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

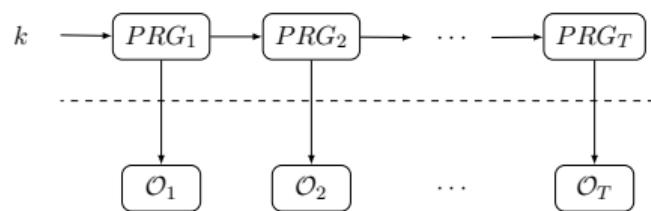
Discussion

Weaker Primitives

- One-Way Functions



- Pseudo-Random Generator



Pseudo-Random State Generator

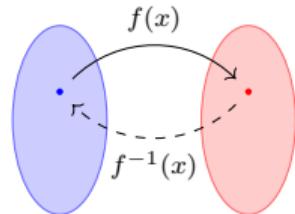
- Efficient gen. (QPT): $G_n(k) = |\psi_k\rangle$
- Pseudo-random: $G_n(k)^{\otimes p(n)} \approx_c |H\rangle^{\otimes p(n)}$

OWF \implies PRSG

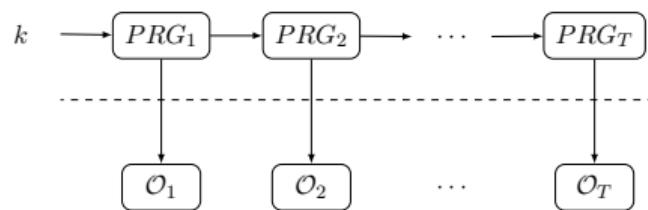
PRSG $\not\implies$ (oracle red.) OWF

Weaker Primitives

- One-Way Functions



- Pseudo-Random Generator



Pseudo-Random State Generator

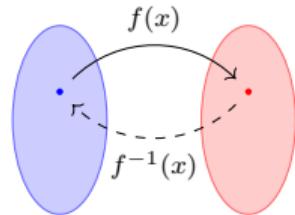
- Efficient gen. (QPT): $G_n(k) = |\psi_k\rangle$
- Pseudo-random: $G_n(k)^{\otimes p(n)} \approx_c |H\rangle^{\otimes p(n)}$

OWF \implies PRSG

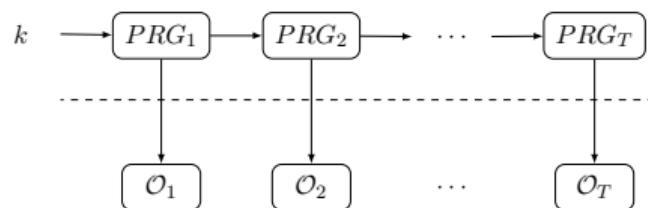
PRSG $\not\implies$ (oracle red.) OWF

Weaker Primitives

- One-Way Functions



- Pseudo-Random Generator



Pseudo-Random State Generator

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

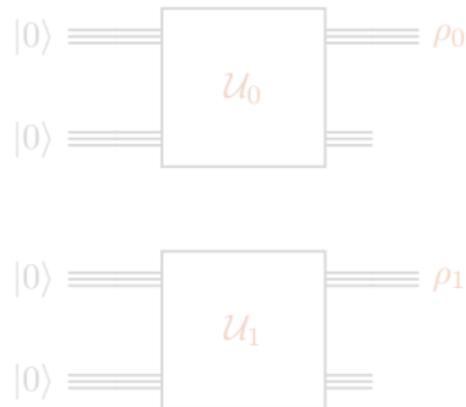
OWF \implies PRSG

PRSG $\not\implies$ (oracle red.) OWF

EFI (quantum state) Pairs

Mixed n -qubit states ρ_0, ρ_1

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

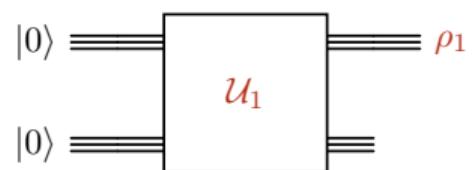


EFI Pairs \iff Commitments \iff OT \iff MPC

EFI (quantum state) Pairs

Mixed n -qubit states ρ_0, ρ_1

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

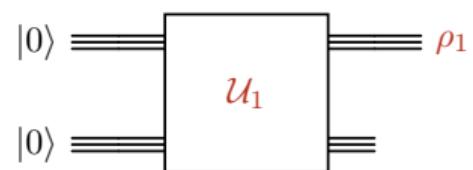
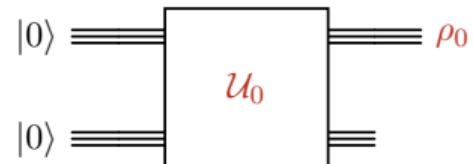


EFI Pairs \iff Commitments \iff OT \iff MPC

EFI (quantum state) Pairs

Mixed n -qubit states ρ_0, ρ_1

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

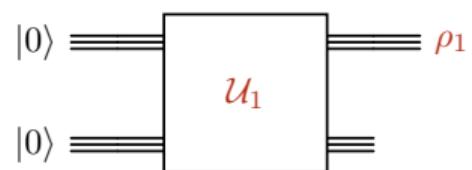
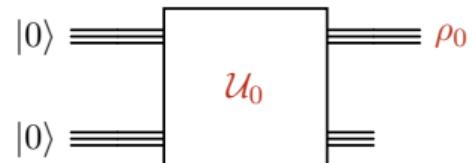


EFI Pairs \iff Commitments \iff OT \iff MPC

EFI (quantum state) Pairs

Mixed n -qubit states ρ_0, ρ_1

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

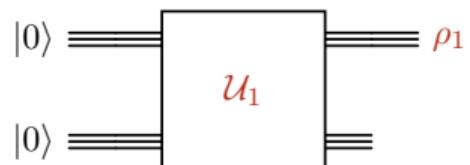
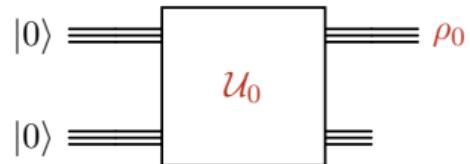


EFI Pairs \iff Commitments \iff OT \iff MPC

EFI (quantum state) Pairs

Mixed n -qubit states ρ_0, ρ_1

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



EFI Pairs \iff Commitments \iff OT \iff MPC

EFID(istribution) Pairs

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

Efficiently constructible: PPT $\mathcal{S}_0, \mathcal{S}_1$

$$X_n \leftarrow \mathcal{S}_0(n)$$

statistically Far: $\text{SD}(X, Y) = 1 - \epsilon$

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

computationally Indistinguishable: $X \approx_c Y$

EFID Pairs \iff PRG \iff OWF

EFID(istribution) Pairs

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

- Efficiently constructible: $\text{PPT } \mathcal{S}_0, \mathcal{S}_1$ $X_n \leftarrow \mathcal{S}_0(n)$
- statistically Far: $\text{SD}(X, Y) = 1 - \epsilon$ $Y_n \leftarrow \mathcal{S}_1(n)$
- computationally Indistinguishable: $X \approx_c Y$

EFID Pairs \iff PRG \iff OWF

EFID(istribution) Pairs

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

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

EFID Pairs \iff PRG \iff OWF

EFID(istribution) Pairs

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

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

EFID Pairs \iff PRG \iff OWF

EFID(istribution) Pairs

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

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

EFID Pairs \iff PRG \iff OWF

Contents

Introduction

Fundamentals of Cryptography

EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

Discussion

Computational Entanglement

Entanglement cost

- Given Φ ; use LOCC to prepare ρ_{AB}
- How many Bell pairs do they need?

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

Distillable entanglement

- Given ρ_{AB} ; use LOCC to distill Φ
- How many Bell pairs can they get?

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

Restrict LOCC operations to QPT

Computational entanglement cost:

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

Computational distillable entanglement: \hat{E}_D^ε

Computational Entanglement

Entanglement cost

- Given Φ ; use LOCC to prepare ρ_{AB}
- How many Bell pairs do they need?

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

Distillable entanglement

- Given ρ_{AB} ; use LOCC to distill Φ
- How many Bell pairs can they get?

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

Restrict LOCC operations to QPT

Computational entanglement cost:

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

Computational distillable entanglement: \hat{E}_D^ε

Computational Entanglement

Entanglement cost

- Given Φ ; use LOCC to prepare ρ_{AB}
- How many Bell pairs do they need?

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

Distillable entanglement

- Given ρ_{AB} ; use LOCC to distill Φ
- How many Bell pairs can they get?

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

Restrict LOCC operations to QPT

Computational entanglement cost:

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

Computational distillable entanglement:

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

Pseudo-Entanglement

ψ_{AB} , ϕ_{AB} n -qubit mixed states

- ψ_{AB} has low entanglement

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

- ϕ_{AB} has high entanglement

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

- Computational ind. $t = \text{poly}(n)$ copies

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

ψ_{AB} is *pseudo-entangled*

- ψ_{AB} efficient to prepare (LOCC)

- ϕ_{AB} must exist

- Use ψ_{AB} instead of ϕ_{AB}

Different definitions:
Which one for *cryptography*?

Pseudo-Entanglement

ψ_{AB} , ϕ_{AB} n -qubit mixed states

- ψ_{AB} has low entanglement

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

- ϕ_{AB} has high entanglement

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

- Computational ind. $t = \text{poly}(n)$ copies

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

ψ_{AB} is *pseudo-entangled*

- ψ_{AB} efficient to prepare (LOCC)

- ϕ_{AB} must exist

- Use ψ_{AB} instead of ϕ_{AB}

Different definitions:
Which one for *cryptography*?

Pseudo-Entanglement

ψ_{AB} , ϕ_{AB} n -qubit mixed states

- ψ_{AB} has low entanglement

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

- ϕ_{AB} has high entanglement

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

- Computational ind. $t = \text{poly}(n)$ copies

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

ψ_{AB} is *pseudo-entangled*

- ψ_{AB} efficient to prepare (LOCC)

- ϕ_{AB} must exist

- Use ψ_{AB} instead of ϕ_{AB}

Different definitions:
Which one for *cryptography*?

Pseudo-Entanglement

ψ_{AB} , ϕ_{AB} n -qubit mixed states

- ψ_{AB} has low entanglement

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

- ϕ_{AB} has high entanglement

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

- Computational ind. $t = \text{poly}(n)$ copies

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

ψ_{AB} is *pseudo-entangled*

- ψ_{AB} efficient to prepare (LOCC)

- ϕ_{AB} must exist

- Use ψ_{AB} instead of ϕ_{AB}

Different definitions:
Which one for *cryptography*?

Pseudo-Entanglement

ψ_{AB} , ϕ_{AB} n -qubit mixed states

- ψ_{AB} has low entanglement

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

- ϕ_{AB} has high entanglement

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

- Computational ind. $t = \text{poly}(n)$ copies

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

ψ_{AB} is *pseudo-entangled*

- ψ_{AB} efficient to prepare (LOCC)

- ϕ_{AB} must exist

- Use ψ_{AB} instead of ϕ_{AB}

Different definitions:
Which one for *cryptography*?

False Entropy

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

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

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

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

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

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

False entropy \iff EFID pairs \iff OWF

False Entropy

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

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

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

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

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

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

False entropy \iff EFID pairs \iff OWF

False Entropy

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

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

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

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

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

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

False entropy \iff EFID pairs \iff OWF

False Entropy

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

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

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

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

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

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

False entropy \iff EFID pairs \iff OWF

False Entropy

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

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

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

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

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

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

False entropy \iff EFID pairs \iff OWF

False Entropy

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

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

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

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

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

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

False entropy \iff EFID pairs \iff OWF

False Entropy

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

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

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

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

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

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

False entropy \iff EFID pairs \iff OWF

False Entropy

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

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

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

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

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

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

False entropy \iff EFID pairs \iff OWF

False Entropy

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

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

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

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

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

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

False entropy \iff EFID pairs \iff OWF

EFI Pairs \Rightarrow Pseudo-Entanglement

Construction

EFI pair ρ_0, ρ_1

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

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

EFI Pairs \implies Pseudo-Entanglement

Construction

EFI pair ρ_0, ρ_1

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

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

EFI Pairs \implies Pseudo-Entanglement

Proof (Cost of ψ_{AB})

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

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

$$\hat{E}_C^0(\psi_{AB}) = 0$$

EFI Pairs \implies Pseudo-Entanglement

Proof (Cost of ψ_{AB})

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

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

$$\hat{E}_C^0(\psi_{AB}) = 0$$

EFI Pairs \implies Pseudo-Entanglement

Proof (Cost of ψ_{AB})

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

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

$$\hat{E}_C^0(\psi_{AB}) = 0$$

EFI Pairs \implies Pseudo-Entanglement

Proof (Cost of ψ_{AB})

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

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

$$\hat{E}_C^0(\psi_{AB}) = 0$$

EFI Pairs \implies Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

$$\phi_{AB} = \frac{1}{2} (|\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \rho_0_A + |\Phi^-\rangle\langle\Phi^-|_{AB} \otimes \rho_1_A)$$

- $\text{TD}(\rho_0, \rho_1) = 1 - \varepsilon$
- Unbounded A distinguishes ρ_0, ρ_1 and tells B
- $\begin{cases} \rho_0 & \text{then } |\Phi^+\rangle_{AB} \\ \rho_1 & \text{then } |\Phi^-\rangle_{AB} \end{cases}$

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

EFI Pairs \implies Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

$$\phi_{AB} = \frac{1}{2} (|\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \rho_0_A + |\Phi^-\rangle\langle\Phi^-|_{AB} \otimes \rho_1_A)$$

- $\text{TD}(\rho_0, \rho_1) = 1 - \varepsilon$
- Unbounded A distinguishes ρ_0, ρ_1 and tells B

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

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

EFI Pairs \implies Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

$$\phi_{AB} = \frac{1}{2} (|\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \rho_0_A + |\Phi^-\rangle\langle\Phi^-|_{AB} \otimes \rho_1_A)$$

- $\text{TD}(\rho_0, \rho_1) = 1 - \varepsilon$
- Unbounded A distinguishes ρ_0, ρ_1 and tells B

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

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

EFI Pairs \implies Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

$$\phi_{AB} = \frac{1}{2} (|\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \rho_0_A + |\Phi^-\rangle\langle\Phi^-|_{AB} \otimes \rho_1_A)$$

- $\text{TD}(\rho_0, \rho_1) = 1 - \varepsilon$
- Unbounded A distinguishes ρ_0, ρ_1 and tells B
- $\begin{cases} \rho_0 & \text{then } |\Phi^+\rangle_{AB} \\ \rho_1 & \text{then } |\Phi^-\rangle_{AB} \end{cases}$

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

EFI Pairs \implies Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

$$\phi_{AB} = \frac{1}{2} (|\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \rho_0_A + |\Phi^-\rangle\langle\Phi^-|_{AB} \otimes \rho_1_A)$$

- $\text{TD}(\rho_0, \rho_1) = 1 - \varepsilon$
- Unbounded A distinguishes ρ_0, ρ_1 and tells B
- $\begin{cases} \rho_0 & \text{then } |\Phi^+\rangle_{AB} \\ \rho_1 & \text{then } |\Phi^-\rangle_{AB} \end{cases}$

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

EFI Pairs \implies Pseudo-Entanglement

Proof ($\psi_{AB} \approx \phi_{AB}$)

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

- . $\begin{cases} \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_1) \longrightarrow \psi_{AB}, \phi_{AB} \\ \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_0) \longrightarrow \psi_{AB} \end{cases}$
- . Distinguish $\frac{1}{2}$ the times
- . \mathcal{D}' can prepare ψ_{AB} and ϕ_{AB} locally

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) \leq \frac{1}{2} \text{Adv}_{\mathcal{D}}(\rho_0, \rho_1) < \varepsilon$$

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) \leq t\varepsilon$$

EFI Pairs \implies Pseudo-Entanglement

Proof ($\psi_{AB} \approx \phi_{AB}$)

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

- . $\begin{cases} \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_1) \longrightarrow \psi_{AB}, \phi_{AB} \\ \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_0) \longrightarrow \psi_{AB} \end{cases}$
- . Distinguish $\frac{1}{2}$ the times
- . \mathcal{D}' can prepare ψ_{AB} and ϕ_{AB} locally

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) \leq \frac{1}{2} \text{Adv}_{\mathcal{D}}(\rho_0, \rho_1) < \varepsilon$$

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) \leq t\varepsilon$$

EFI Pairs \implies Pseudo-Entanglement

Proof ($\psi_{AB} \approx \phi_{AB}$)

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

- $\begin{cases} \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_1) \longrightarrow \psi_{AB}, \phi_{AB} \\ \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_0) \longrightarrow \psi_{AB} \end{cases}$
- Distinguish $\frac{1}{2}$ the times
- \mathcal{D}' can prepare ψ_{AB} and ϕ_{AB} locally

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) \leq \frac{1}{2} \text{Adv}_{\mathcal{D}}(\rho_0, \rho_1) < \varepsilon$$

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) \leq t\varepsilon$$

EFI Pairs \implies Pseudo-Entanglement

Proof ($\psi_{AB} \approx \phi_{AB}$)

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

- . $\begin{cases} \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_1) \longrightarrow \psi_{AB}, \phi_{AB} \\ \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_0) \longrightarrow \psi_{AB} \end{cases}$
- . Distinguish $\frac{1}{2}$ the times
- . \mathcal{D}' can prepare ψ_{AB} and ϕ_{AB} locally

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) \leq \frac{1}{2} \text{Adv}_{\mathcal{D}}(\rho_0, \rho_1) < \varepsilon$$

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) \leq t\varepsilon$$

EFI Pairs \implies Pseudo-Entanglement

Proof ($\psi_{AB} \approx \phi_{AB}$)

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

- . $\begin{cases} \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_0) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_1) \longrightarrow \psi_{AB}, \phi_{AB} \\ \mathcal{D}'(|\Phi^+\rangle\langle\Phi^+| \otimes \rho_1) \text{ or } \mathcal{D}'(|\Phi^-\rangle\langle\Phi^-| \otimes \rho_0) \longrightarrow \psi_{AB} \end{cases}$
- . Distinguish $\frac{1}{2}$ the times
- . \mathcal{D}' can prepare ψ_{AB} and ϕ_{AB} locally

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}, \phi_{AB}) \leq \frac{1}{2} \text{Adv}_{\mathcal{D}}(\rho_0, \rho_1) < \varepsilon$$

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes t}, \phi_{AB}^{\otimes t}) \leq t \varepsilon$$

EFI Pairs \implies Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes p}, \phi_{AB}^{\otimes p}) \leq \varepsilon$$

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

EFI Pairs \implies Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes p}, \phi_{AB}^{\otimes p}) \leq \varepsilon$$

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

EFI Pairs \implies Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes p}, \phi_{AB}^{\otimes p}) \leq \varepsilon$$

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

EFI Pairs \implies Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

$$\text{Adv}_{\mathcal{D}'}(\psi_{AB}^{\otimes p}, \phi_{AB}^{\otimes p}) \leq \varepsilon$$

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

Contents

Introduction

Fundamentals of Cryptography

EFI Pairs are Necessary for Cryptography

Pseudo-Entanglement is Necessary for EFI Pairs

Discussion

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?

How are *computational hardness* and *physics* connected?

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?

How are *computational hardness* and *physics* connected?

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?

How are *computational hardness* and *physics* connected?

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?

How are *computational hardness* and *physics* connected?

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?

How are *computational hardness* and *physics* connected?

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?

How are *computational hardness* and *physics* connected?

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?

How are *computational hardness* and *physics* connected?