Pseudo-Entanglement is Necessary for EFI Pairs

Manuel Goulão with David Elkouss

Portugal Crypto Day — 13th of December of 2024

Overview

Contents

Cryptography

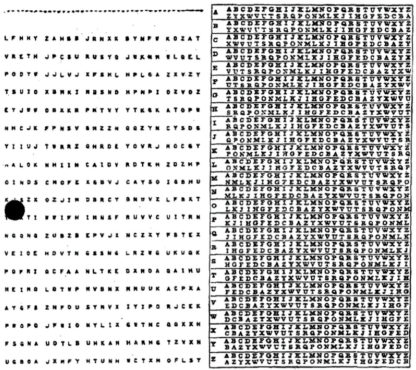
What systems may we *implement*?

Perfect encryption

All messages are valid: *Zero* information!

Key as long as the message...

Key can only be used once.....



NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

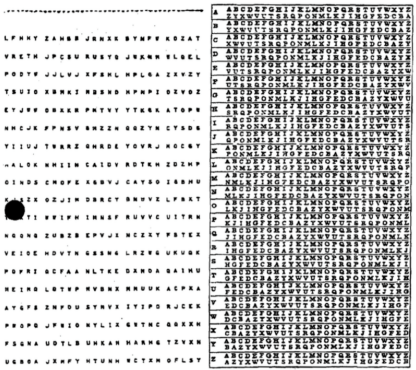
What systems may we *implement*?

Perfect encryption

All messages are valid: *Zero* information!

Key as long as the message...

Key can only be used once.....



NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

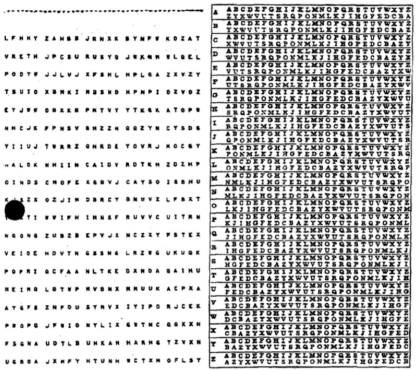
What systems may we *implement*?

Perfect encryption

All messages are valid: *Zero* information!

Key as long as the message...

Key can only be used once.....



NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

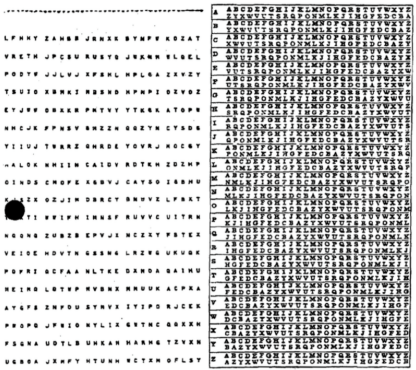
What systems may we *implement*?

Perfect encryption

All messages are valid: *Zero* information!

Key as long as the message...

Key can only be used once.....



NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

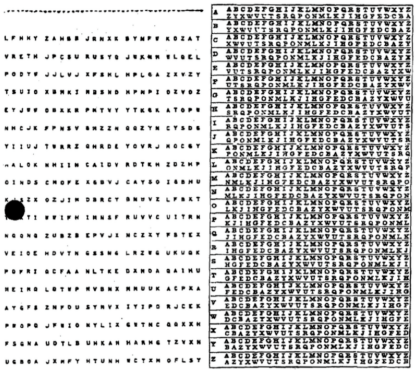
What systems may we *implement*?

Perfect encryption

All messages are valid: *Zero* information!

Key as long as the message...

Key can only be used once.....



NSA One-Time Pad (Source: Wikimedia)

How to make it practical?

Cryptography

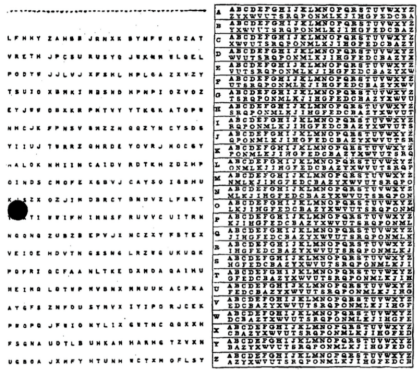
What systems may we *implement*?

Perfect encryption

All messages are valid: *Zero* information!

Key as long as the message...

Key can only be used once.....



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

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

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

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

Find x

Discrete logarithm problem

AES round
(Source: Wikimedia)

Used everywhere in the information-world

Computational Cryptography

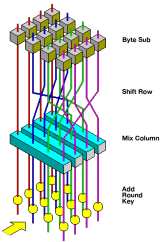
Make *computational* assumptions

Limit computational resources

1. Make problems intricate

2. Make *hardness* assumptions

Security is assumed, not proven



AES round
(Source: Wikimedia)

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

Find x

Discrete logarithm problem

Used everywhere in the information-world

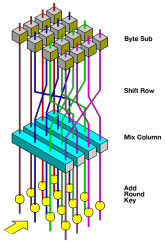
Computational Cryptography

Make *computational* assumptions

Limit computational resources

1. Make problems intricate
2. Make *hardness* assumptions

Security is assumed, not proven



AES round
(Source: Wikimedia)

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

Find x

Discrete logarithm problem

Used everywhere in the information-world

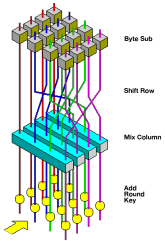
Computational Cryptography

Make *computational* assumptions

Limit computational resources

1. Make problems intricate
2. Make *hardness* assumptions

Security is assumed, not proven



AES round
(Source: Wikimedia)

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

Find x

Discrete logarithm problem

Used everywhere in the information-world

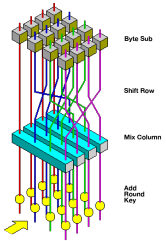
Computational Cryptography

Make *computational* assumptions

Limit computational resources

1. Make problems intricate
2. Make *hardness* assumptions

Security is assumed, not proven



AES round
(Source: Wikimedia)

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

Find x

Discrete logarithm problem

Used everywhere in the information-world

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 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 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 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 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

Classical Cryptography

Cryptomania

CCA-PKE $=)$ PKE $(=$ OT $( )$ MPC

PKE $\supset$ KE

Minicrypt

PKE $=$ OWF

Signatures $( )$ OWF $( )$ SKE $( )$ PRG

OWF $=$ PRG

SKE $( )$ Commit

Coin flip

P $\subsetneq$ NP

Classical Cryptography

Cryptomania

CCA-PKE $=)$ PKE $(=$ OT $( )$ MPC

PKE $\supsetneq$ KE

Minicrypt

PKE $=$ OWF

Signatures $( )$ OWF $( )$ SKE $( )$ PRG

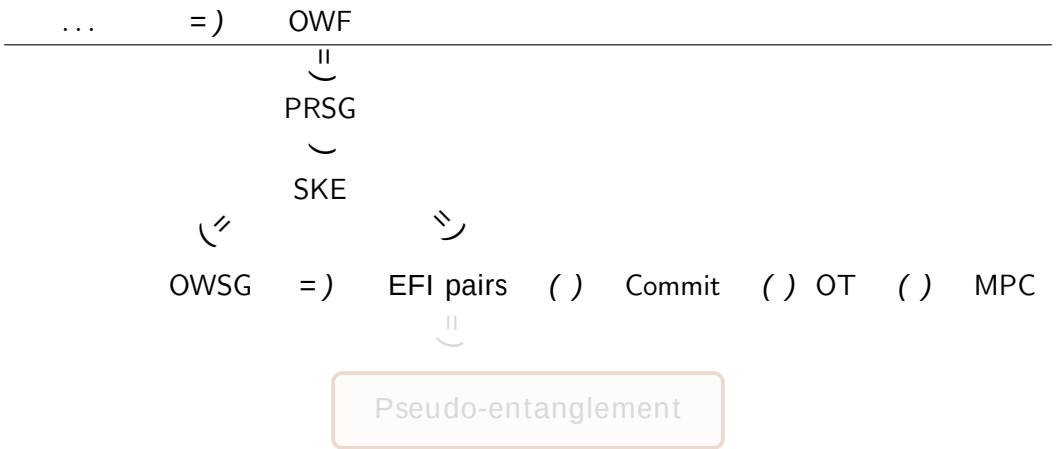
OWF $=$ PRG

Coin flip $( )$ Commit

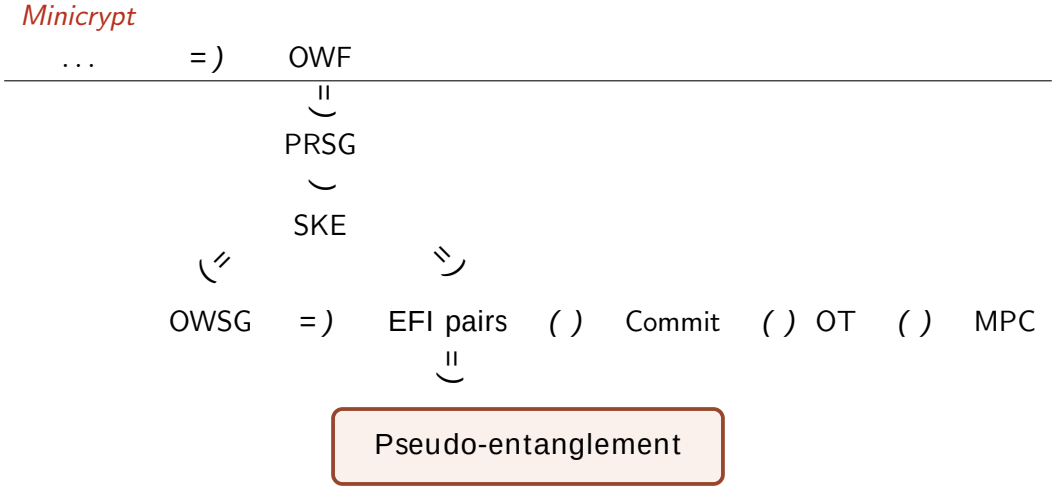
P $\subsetneq$ NP

Quantum Cryptography

Minicrypt

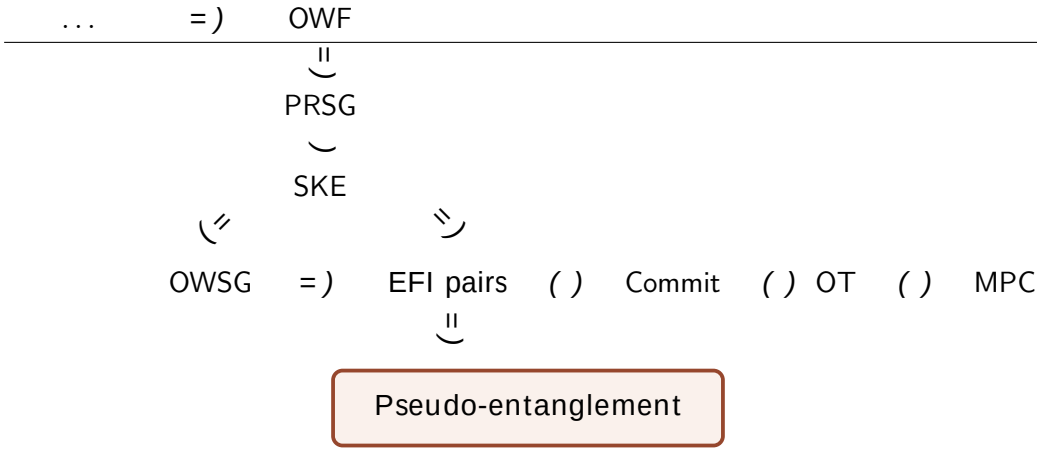


Quantum Cryptography



Quantum Cryptography

Minicrypt



QKD

Classical vs. Quantum Cryptography

Impossibility of many *Information-Theoretic* protocols

Classical (computational) cryptography $\Rightarrow$ $\mathbf{P} \neq \mathbf{NP}$

Quantum resources $\Rightarrow$ 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 $\Rightarrow$ $\mathbf{P} \neq \mathbf{NP}$

Quantum resources $\Rightarrow$ 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 $\Rightarrow$ $\mathbf{P} \neq \mathbf{NP}$

Quantum resources $\Rightarrow$ 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 $\Rightarrow$ $\mathbf{P} \neq \mathbf{NP}$

Quantum resources $\Rightarrow$ 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 $\Rightarrow$ $\mathbf{P} \neq \mathbf{NP}$

Quantum resources $\Rightarrow$ 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 $\Rightarrow$ $\mathbf{P} \neq \mathbf{NP}$

Quantum resources $\Rightarrow$ weaker Commitments, OT, QKD, ...

Assume correctness of the *Laws of Physics*

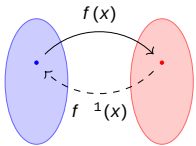
New computational world: Quantum Cryptography, but no Classical Cryptography

How physics and computational hardness relate through cryptography?

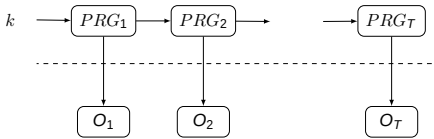
Contents

Weaker Primitives

One-Way Functions



Pseudo-Random Generator



Pseudo-Random State Generator

Efficient gen. (QPT): $G_n(k) = j\psi_k i$

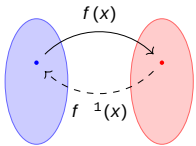
Pseudo-random: $G_n(k)^{\otimes p(n)} \approx_c jHi^{\otimes p(n)}$

OWF $\Rightarrow$ PRSG

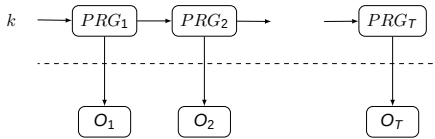
PRSG $\not\Rightarrow$ (oracle red.) OWF

Weaker Primitives

One-Way Functions



Pseudo-Random Generator



Pseudo-Random State Generator

Efficient gen. (QPT): $G_n(k) = j\psi_k i$

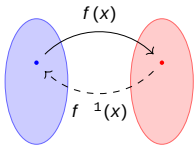
Pseudo-random: $G_n(k)$ p(n) $_c$ jHi p(n)

OWF =) PRSG

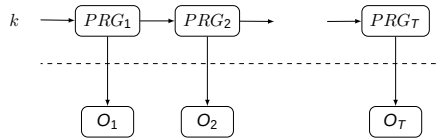
PRSG 6=) (oracle red.) OWF

Weaker Primitives

One-Way Functions



Pseudo-Random Generator



Pseudo-Random State Generator

Efficient gen. (QPT): $G_n(k) = j\psi_k i$

Pseudo-random: $G_n(k)$ p(n) $_c$ jHi p(n)

OWF =) PRSG

PRSG 6=) (oracle red.) OWF

EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

Efficiently preparable: QPT U_0, U_1

statistically Far: $\mathrm{TD}(\rho_0, \rho_1) = 1 - \varepsilon$

computationally Indistinguishable: $\rho_0 \stackrel{c}{\approx} \rho_1$

EFI Pairs ( ) Commitments ( ) OT ( ) MPC

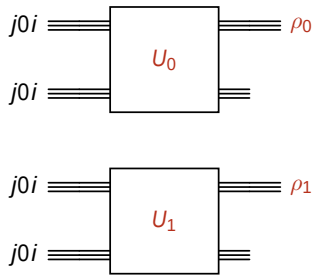
EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

Efficiently preparable: QPT U_0, U_1

statistically Far: $\mathrm{TD}(\rho_0, \rho_1) = 1 \quad \varepsilon$

computationally Indistinguishable: $\rho_0 \quad_c \rho_1$



EFI Pairs ( ) Commitments ( ) OT ( ) MPC

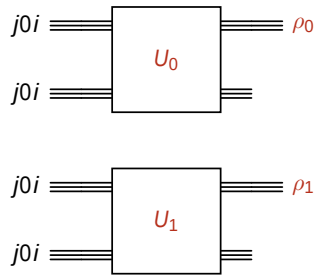
EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

Efficiently preparable: QPT U_0, U_1

statistically Far: $\mathrm{TD}(\rho_0, \rho_1) = 1 \quad \varepsilon$

computationally Indistinguishable: $\rho_0 \quad _c \; \rho_1$



EFI Pairs ( ) Commitments ( ) OT ( ) MPC

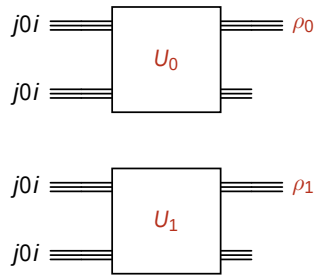
EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

Efficiently preparable: QPT U_0, U_1

statistically Far: $\mathrm{TD}(\rho_0, \rho_1) = 1 \quad \varepsilon$

computationally Indistinguishable: $\rho_0 \quad c \; \rho_1$



EFI Pairs ( ) Commitments ( ) OT ( ) MPC

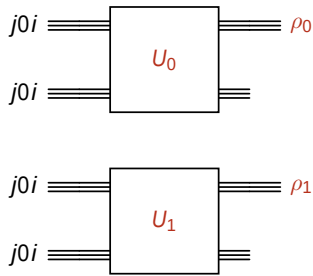
EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

Efficiently preparable: QPT U_0, U_1

statistically Far: $\mathrm{TD}(\rho_0, \rho_1) = 1 \quad \varepsilon$

computationally Indistinguishable: $\rho_0 \quad c \; \rho_1$



EFI Pairs ( ) Commitments ( ) OT ( ) MPC

EFID(istribution) Pairs

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

Efficiently constructible: PPT S_0, S_1

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

computationally Indistinguishable: $X \approx_c Y$

$X_n \quad S_0(n)$

$Y_n \quad S_1(n)$

EFID Pairs ( ) PRG ( ) OWF

EFID(istribution) Pairs

Probability ensembles $X = fX_n g_n, Y = fY_n g_n$

Efficiently constructible: PPT S_0, S_1

$X_n \quad S_0(n)$

$Y_n \quad S_1(n)$

statistically Far: $SD(X, Y) = 1 \quad \varepsilon$

computationally Indistinguishable: $X \quad _c Y$

EFID Pairs ( ) PRG ( ) OWF

EFID(istribution) Pairs

Probability ensembles $X = fX_n g_n, Y = fY_n g_n$

Efficiently constructible: PPT S_0, S_1

statistically Far: SD$(X, Y) = 1 \quad \varepsilon$

computationally Indistinguishable: $X \quad _c Y$

$X_n \quad S_0(n)$

$Y_n \quad S_1(n)$

EFID Pairs ( ) PRG ( ) OWF

EFID(istribution) Pairs

Probability ensembles $X = fX_n g_n, Y = fY_n g_n$

Efficiently constructible: PPT S_0, S_1

statistically Far: SD$(X, Y) = 1 \quad \varepsilon$

computationally Indistinguishable: $X \quad_c Y$

$X_n \quad S_0(n)$

$Y_n \quad S_1(n)$

EFID Pairs ( ) PRG ( ) OWF

EFID(istribution) Pairs

Probability ensembles $X = fX_n g_n, Y = fY_n g_n$

Efficiently constructible: PPT S_0, S_1

statistically Far: SD$(X, Y) = 1 \quad \varepsilon$

computationally Indistinguishable: $X \quad _c Y$

$X_n \quad S_0(n)$

$Y_n \quad S_1(n)$

EFID Pairs ( ) PRG ( ) OWF

Contents

Computational Entanglement

Entanglement cost

Given ; use LOCC to prepare ρ_{AB}

How many Bell pairs do they need?

$E_C^{\varepsilon}(\ _{AB}) = \inf\{n \mid F(\ (\ \ ^{n}),\ _{AB}) \quad 1 \quad "g$

Distillable entanglement

Given ρ_{AB}; use LOCC to distill

How many Bell pairs can they get?

$E_D^{\varepsilon}(\ _{AB}) = \sup\{m \mid F(\ (\ _{AB}),\ \ ^{m}) \quad 1 \quad "g$

Restrict LOCC operations to QPT

Computational entanglement cost: $\hat{E}_C^{"}$

Computational distillable entanglement: $\hat{E}_D^{"}$

Computational Entanglement

Entanglement cost

Given ; use LOCC to prepare ρ_{AB}

How many Bell pairs do they need?

$$E_C^{\varepsilon}(\ _{AB}) = \inf f n j \mathrm{F}(\ (\quad)^{n}); \ _{AB}) \quad 1 \quad "g$$

Distillable entanglement

Given ρ_{AB}; use LOCC to distill

How many Bell pairs can they get?

$$E_D^{\varepsilon}(\ _{AB}) = \sup f m j \mathrm{F}(\ (\ _{AB}); \quad ^{m}) \quad 1 \quad "g$$

Restrict LOCC operations to QPT

Computational entanglement cost: $\hat{E}_C^{"}$

Computational distillable entanglement: $\hat{E}_D^{"}$

Computational Entanglement

Entanglement cost

Given ; use LOCC to prepare ρ_{AB}

How many Bell pairs do they need?

$E_C^{\varepsilon}(\ _{AB}) = \inf\{n \mid F(\ (\ \ ^{n}); \ _{AB}) \quad 1 \quad "g$

Distillable entanglement

Given ρ_{AB}; use LOCC to distill

How many Bell pairs can they get?

$E_D^{\varepsilon}(\ _{AB}) = \sup\{m \mid F(\ (\ _{AB}); \ \ ^{m}) \quad 1 \quad "g$

Restrict LOCC operations to QPT

Computational entanglement cost: $\hat{E}_C^{"}$

Computational distillable entanglement: $\hat{E}_D^{"}$

Pseudo-Entanglement

ψ_{AB}, ϕ_{AB} n-qubit mixed states

ψ_{AB} has low entanglement

$$\hat{E}^{''}_{C}(\psi_{AB}) \quad c(n)$$

ϕ_{AB} has high entanglement

$$E^{''}_{D}(\phi_{AB}) \quad d(n)$$

Computational ind. t = poly(n) copies

$$\psi_{AB}^{\ t} \quad c\,\phi_{AB}^{\ t}$$

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

$$\hat{E}^{''}_{C}(\psi_{AB}) \quad c(n)$$

ϕ_{AB} has high entanglement

$$E^{''}_{D}(\phi_{AB}) \quad d(n)$$

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

$$\psi_{AB}{}^{t} \quad c\,\phi_{AB}{}^{t}$$

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

$$\hat{E}^{''}_{C}(\psi_{AB}) \quad c(n)$$

ϕ_{AB} has high entanglement

$$E^{''}_{D}(\phi_{AB}) \quad d(n)$$

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

$$\psi_{AB}^{\ t} \quad c\,\phi_{AB}^{\ t}$$

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

$$\hat{E}^{''}_{C}(\psi_{AB}) \quad c(n)$$

ϕ_{AB} has high entanglement

$$E^{''}_{D}(\phi_{AB}) \quad d(n)$$

Computational ind. t = poly(n) copies

$$\psi_{AB}^{\ t} \quad _c \ \phi_{AB}^{\ t}$$

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

$$\hat{E}^{''}_{C}(\psi_{AB}) \quad c(n)$$

ϕ_{AB} has high entanglement

$$E^{''}_{D}(\phi_{AB}) \quad d(n)$$

Computational ind. t = poly(n) copies

$$\psi_{AB}^{\ t} \quad _{c}\, \phi_{AB}^{\ t}$$

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

$W = fW_i g_i$, $Z = fZ_i g_i$ distr. ensembles

W has low entropy

Z has high entropy

W and Z are computational ind.

EFID pair $X = fX_n g_n$ $Y = fY_n g_n$

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

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

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

False entropy ( ) EFID pairs ( ) OWF

False Entropy

$W = fW_i g_i$, $Z = fZ_i g_i$ distr. ensembles

W has low entropy

Z has high entropy

W and Z are computational ind.

EFID pair $X = fX_n g_n$ $Y = fY_n g_n$

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

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

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

False entropy ( ) EFID pairs ( ) OWF

False Entropy

$W = fW_i g_i$, $Z = fZ_i g_i$ distr. ensembles

W has low entropy

Z has high entropy

W and Z are computational ind.

False entropy ( ) EFID pairs ( ) OWF

False Entropy

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

W has low entropy

Z has high entropy

W and Z are computational ind.

False entropy ( ) EFID pairs ( ) OWF

False Entropy

$W = fW_i g_i$, $Z = fZ_i g_i$ distr. ensembles

W has low entropy

Z has high entropy

W and Z are computational ind.

EFID pair $X = fX_n g_n$ $Y = fY_n g_n$

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

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

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

False entropy ( ) EFID pairs ( ) OWF

False Entropy

$W = fW_i g_i$, $Z = fZ_i g_i$ distr. ensembles

W has low entropy

Z has high entropy

W and Z are computational ind.

EFID pair $X = fX_n g_n$ $Y = fY_n g_n$

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

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

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

False entropy ( ) EFID pairs ( ) OWF

False Entropy

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

W has low entropy

Z has high entropy

W and Z are computational ind.

EFID pair $X = \{X_n, g_n\}$ $Y = \{Y_n, g_n\}$

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

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

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

False entropy ( ) EFID pairs ( ) OWF

False Entropy

$W = fW_i g_i$, $Z = fZ_i g_i$ distr. ensembles

W has low entropy

Z has high entropy

W and Z are computational ind.

EFID pair $X = fX_n g_n$ $Y = fY_n g_n$

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

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

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

False entropy ( ) EFID pairs ( ) OWF

False Entropy

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

W has low entropy

Z has high entropy

W and Z are computational ind.

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

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

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

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

False entropy ( ) EFID pairs ( ) OWF

EFI Pairs =) Pseudo-Entanglement

Construction

EFI pair ρ_0, ρ_1

$$\psi_{AB} = \frac{1}{4}(j \quad ^{+}\hbar \quad ^{+}j_{AB} + j \quad \hbar \quad j_{AB}) \quad (\rho_{0A} + \rho_{1A})$$

$$\phi_{AB} = \frac{1}{2}(j \quad ^{+}\hbar \quad ^{+}j_{AB} \quad \rho_{0A} + j \quad \hbar \quad j_{AB} \quad \rho_{1A})$$

EFI Pairs $\Rightarrow$ Pseudo-Entanglement

Construction

EFI pair ρ_0, ρ_1

$$\psi_{AB} = \frac{1}{4}(|+\rangle|+\rangle_{AB} + |-\rangle|-\rangle_{AB})(\rho_{0A} + \rho_{1A})$$

$$\phi_{AB} = \frac{1}{2}(|+\rangle|+\rangle_{AB}\rho_{0A} + |-\rangle|-\rangle_{AB}\rho_{1A})$$

EFI Pairs $\Rightarrow$ Pseudo-Entanglement

Proof (Cost of $_{AB}$)

$$\psi_{AB} = \frac{1}{4}(j \quad ^{+}\hbar \quad ^{+}j_{AB} + j \quad \hbar \quad j_{AB}) \quad (\rho_{0A} + \rho_{1A})$$

A flips fair coin, prepares $\begin{cases} \rho_0 & \text{if } H \\ \rho_1 & \text{if } T \end{cases}$

A flips fair coin, prepares $\begin{cases} j0\hbar 0j & \text{tells } B \text{ to prepare } j0\hbar 0j \quad \text{if } H \\ j1\hbar 1j & \text{tells } B \text{ to prepare } j1\hbar 1j \quad \text{if } T \end{cases}$

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

EFI Pairs $=)$ Pseudo-Entanglement

Proof (Cost of $_{AB}$)

$$\psi_{AB} = \frac{1}{4}(j \quad {}^{+}\!\hbar \quad {}^{+}j_{AB} + j \quad \hbar \quad j_{AB}) \quad (\rho_{0A} + \rho_{1A})$$

A flips fair coin, prepares $\begin{cases} \rho_0 & \text{if } H \\ \rho_1 & \text{if } T \end{cases}$

A flips fair coin, prepares $\begin{cases} j0\hbar 0j & \text{tells } B \text{ to prepare } j0\hbar 0j \quad \text{if } H \\ j1\hbar 1j & \text{tells } B \text{ to prepare } j1\hbar 1j \quad \text{if } T \end{cases}$

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

EFI Pairs $\Rightarrow$ Pseudo-Entanglement

Proof (Cost of $_{AB}$)

$$\psi_{AB} = \frac{1}{4}(j \quad ^{+}ih \quad ^{+}j_{AB} + j \quad ih \quad j_{AB}) \quad (\rho_{0A} + \rho_{1A})$$

A flips fair coin, prepares $\begin{cases} \rho_0 & \text{if } H \\ \rho_1 & \text{if } T \end{cases}$

A flips fair coin, prepares $\begin{cases} j0ih0j & \text{tells } B \text{ to prepare } j0ih0j & \text{if } H \\ j1ih1j & \text{tells } B \text{ to prepare } j1ih1j & \text{if } T \end{cases}$

$$\overset{\leftrightarrow}{E}{}^{0}_{C}(\psi_{AB}) = 0$$

EFI Pairs $=)$ Pseudo-Entanglement

Proof (Cost of $_{AB}$)

$$\psi_{AB} = \frac{1}{4}(j \quad {}^{+}ih \quad {}^{+}j_{AB} + j \quad ih \quad j_{AB}) \quad (\rho_{0A} + \rho_{1A})$$

A flips fair coin, prepares $\begin{cases} \rho_0 & \text{if } H \\ \rho_1 & \text{if } T \end{cases}$

A flips fair coin, prepares $\begin{cases} j0ih0j & \text{tells } B \text{ to prepare } j0ih0j & \text{if } H \\ j1ih1j & \text{tells } B \text{ to prepare } j1ih1j & \text{if } T \end{cases}$

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

EFI Pairs =) Pseudo-Entanglement

Proof (Distillation of $_{AB}$)

$$\phi_{AB} = \frac{1}{2}(j \quad ^{+}ih \quad ^{+}j_{AB} \quad \rho_{0A} + j \quad ih \quad j_{AB} \quad \rho_{1A})$$

TD$(\rho_0, \rho_1) = 1 \quad \varepsilon$

Unbounded A distinguishes ρ_0, ρ_1 and tells B

$$\begin{cases} \rho_0 \quad \text{then} \quad j \quad ^{+}i_{AB} \\ \rho_1 \quad \text{then} \quad j \quad i_{AB} \end{cases}$$

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

EFI Pairs $=)$ Pseudo-Entanglement

Proof (Distillation of $_{AB}$)

$$\phi_{AB} = \frac{1}{2}(j \quad ^{+}ih \quad ^{+}j_{AB} \quad \rho_{0A} + j \quad ih \quad j_{AB} \quad \rho_{1A})$$

$\mathrm{TD}(\rho_0, \rho_1) = 1 \quad \varepsilon$

Unbounded A distinguishes ρ_0, ρ_1 and tells B

$$\begin{cases} \rho_0 \quad \text{then} \quad j \quad ^{+}i_{AB} \\ \rho_1 \quad \text{then} \quad j \quad i_{AB} \end{cases}$$

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

EFI Pairs $=)$ Pseudo-Entanglement

Proof (Distillation of $_{AB}$)

$$\phi_{AB} = \frac{1}{2}(j \quad ^{+}ih \quad ^{+}j_{AB} \quad \rho_{0A} + j \quad ih \quad j_{AB} \quad \rho_{1A})$$

TD$(\rho_0, \rho_1) = 1 \quad \varepsilon$

Unbounded A distinguishes ρ_0, ρ_1 and tells B

$$\begin{cases} \rho_0 \quad \text{then} \quad j \quad ^{+}i_{AB} \\ \rho_1 \quad \text{then} \quad j \quad i_{AB} \end{cases}$$

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

EFI Pairs $=)$ Pseudo-Entanglement

Proof (Distillation of $_{AB}$)

$$\phi_{AB} = \frac{1}{2}(j \quad ^{+}ih \quad ^{+}j_{AB} \quad \rho_{0A} + j \quad ih \quad j_{AB} \quad \rho_{1A})$$

TD$(\rho_0, \rho_1) = 1 \quad \varepsilon$

Unbounded A distinguishes ρ_0, ρ_1 and tells B

$$\begin{cases} \rho_0 \quad \text{then} \quad j \quad ^{+}i_{AB} \\ \rho_1 \quad \text{then} \quad j \quad i_{AB} \end{cases}$$

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

EFI Pairs $=)$ Pseudo-Entanglement

Proof (Distillation of $_{AB}$)

$$\phi_{AB} = \frac{1}{2}(j \quad ^{+}ih \quad ^{+}j_{AB} \quad \rho_{0A} + j \quad ih \quad j_{AB} \quad \rho_{1A})$$

TD$(\rho_0, \rho_1) = 1 \quad \varepsilon$

Unbounded A distinguishes ρ_0, ρ_1 and tells B

$$\begin{cases} \rho_0 \quad \text{then} \quad j \quad ^{+}i_{AB} \\ \rho_1 \quad \text{then} \quad j \quad i_{AB} \end{cases}$$

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

EFI Pairs $=)$ Pseudo-Entanglement

Proof ($_{AB}$ $_{AB}$)

$$\mathrm{Adv}_D(\rho_0, \rho_1) \quad \varepsilon \quad =) \quad \mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \varepsilon^0$$

$$\begin{cases} D^0(j \ ^+\hbar \ ^+j \quad \rho_0) \text{ or } D^0(j \quad \hbar \quad j \quad \rho_1) \quad ! \quad \psi_{AB}, \phi_{AB} \\ D^0(j \ ^+\hbar \ ^+j \quad \rho_1) \text{ or } D^0(j \quad \hbar \quad j \quad \rho_0) \quad ! \quad \psi_{AB} \end{cases}$$

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

D^0 can prepare ψ_{AB} and ϕ_{AB} locally

$$\mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \frac{1}{2}\mathrm{Adv}_D(\rho_0, \rho_1) < \varepsilon$$

$$\mathrm{Adv}_{D^0}(\psi_{AB} \ ^t, \phi_{AB} \ ^t) \quad t\,\varepsilon$$

EFI Pairs =) Pseudo-Entanglement

Proof ($_{AB}$ $_{AB}$)

$$\mathrm{Adv}_D(\rho_0, \rho_1) \quad \varepsilon \quad =) \quad \mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \varepsilon^0$$

$$\begin{cases} D^0(j \ ^+ i\hbar \ ^+ j \quad \rho_0) \text{ or } D^0(j \quad i\hbar \quad j \quad \rho_1) \quad ! \quad \psi_{AB}, \phi_{AB} \\ D^0(j \ ^+ i\hbar \ ^+ j \quad \rho_1) \text{ or } D^0(j \quad i\hbar \quad j \quad \rho_0) \quad ! \quad \psi_{AB} \end{cases}$$

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

D^0 can prepare ψ_{AB} and ϕ_{AB} locally

$$\mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \frac{1}{2}\mathrm{Adv}_D(\rho_0, \rho_1) < \varepsilon$$

$$\mathrm{Adv}_{D^0}(\psi_{AB}{}^t, \phi_{AB}{}^t) \quad t\,\varepsilon$$

EFI Pairs =) Pseudo-Entanglement

Proof ($_{AB}$ $_{AB}$)

$$\mathrm{Adv}_D(\rho_0, \rho_1) \quad \varepsilon \quad =) \quad \mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \varepsilon^0$$

$$\begin{cases} D^0(j \ ^+ \hbar \ ^+ j \quad \rho_0) \text{ or } D^0(j \quad \hbar \quad j \quad \rho_1) \quad ! \quad \psi_{AB}, \phi_{AB} \\ D^0(j \ ^+ \hbar \ ^+ j \quad \rho_1) \text{ or } D^0(j \quad \hbar \quad j \quad \rho_0) \quad ! \quad \psi_{AB} \end{cases}$$

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

D^0 can prepare ψ_{AB} and ϕ_{AB} locally

$$\mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \tfrac{1}{2}\,\mathrm{Adv}_D(\rho_0, \rho_1) < \varepsilon$$

$$\mathrm{Adv}_{D^0}(\psi_{AB}{}^t, \phi_{AB}{}^t) \quad t\,\varepsilon$$

EFI Pairs =) Pseudo-Entanglement

Proof ($_{AB}$ $_{AB}$)

$$\mathrm{Adv}_D(\rho_0, \rho_1) \quad \varepsilon \quad =) \quad \mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \varepsilon^0$$

$$\begin{cases} D^0(j \ ^+ i\hbar \ ^+ j \quad \rho_0) \text{ or } D^0(j \quad i\hbar \quad j \quad \rho_1) \quad ! \quad \psi_{AB}, \phi_{AB} \\ D^0(j \ ^+ i\hbar \ ^+ j \quad \rho_1) \text{ or } D^0(j \quad i\hbar \quad j \quad \rho_0) \quad ! \quad \psi_{AB} \end{cases}$$

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

D^0 can prepare ψ_{AB} and ϕ_{AB} locally

$$\mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \tfrac{1}{2}\mathrm{Adv}_D(\rho_0, \rho_1) < \varepsilon$$

$$\mathrm{Adv}_{D^0}(\psi_{AB}{}^t, \phi_{AB}{}^t) \quad t\varepsilon$$

EFI Pairs =) Pseudo-Entanglement

Proof ($_{AB}$ $_{AB}$)

$$\mathrm{Adv}_D(\rho_0, \rho_1) \quad \varepsilon \quad =) \quad \mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \varepsilon^0$$

$$\begin{cases} D^0(j \ ^+ i\hbar \ ^+ j \quad \rho_0) \text{ or } D^0(j \quad i\hbar \quad j \quad \rho_1) \quad ! \quad \psi_{AB}, \phi_{AB} \\ D^0(j \ ^+ i\hbar \ ^+ j \quad \rho_1) \text{ or } D^0(j \quad i\hbar \quad j \quad \rho_0) \quad ! \quad \psi_{AB} \end{cases}$$

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

D^0 can prepare ψ_{AB} and ϕ_{AB} locally

$$\mathrm{Adv}_{D^0}(\psi_{AB}, \phi_{AB}) \quad \frac{1}{2}\mathrm{Adv}_D(\rho_0, \rho_1) < \varepsilon$$

$$\mathrm{Adv}_{D^0}(\psi_{AB} \ ^t, \phi_{AB} \ ^t) \quad t\varepsilon$$

EFI Pairs $\Rightarrow$ Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

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

EFI Pairs $\Rightarrow$ Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

$$\begin{aligned} \mathrm{Adv}_{D^0}(\psi_{AB}^{\otimes p}, \phi_{AB}^{\otimes p}) &\leq \varepsilon \\ \mathrm{Adv}_{D^0}(\overline{\psi}_{AB}^{\otimes p}, \overline{\phi}_{AB}^{\otimes p}) &\leq q\varepsilon \end{aligned}$$

EFI Pairs $\Rightarrow$ Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

$$\mathrm{Adv}_{D^0}(\psi_{AB}^{\,p}, \phi_{AB}^{\,p}) \leq \varepsilon$$
$$\mathrm{Adv}_{D^0}(\overline{\psi}_{AB}^{\,p}, \overline{\phi}_{AB}^{\,p}) \leq q\varepsilon$$

EFI Pairs $=)$ Pseudo-Entanglement

Proof (amplification)

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

Error:

$$\mathsf{F}(\rho^{\,q}, \sigma^{\,q}) = \mathsf{F}(\rho, \sigma)^q \;=) \; (1 \quad \varepsilon)^q \quad 1 \quad q\,\varepsilon$$

Swap:

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

$$\mathsf{Adv}_{D^0}(\psi_{AB}^{\;\;p}, \phi_{AB}^{\;\;p}) \quad \varepsilon$$
$$\mathsf{Adv}_{D^0}(\overline{\psi}_{AB}^{\;\;p}, \overline{\phi}_{AB}^{\;\;p}) \quad q\,\varepsilon$$

Contents

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?