Pseudo-Entanglement is Necessary for EFI Pairs

Manuel Goulão with David Elkouss

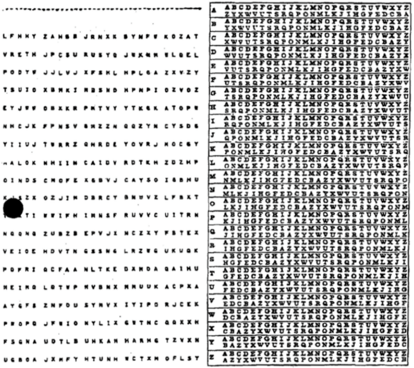
Portugal Crypto Day — 13th of December of 2024

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......

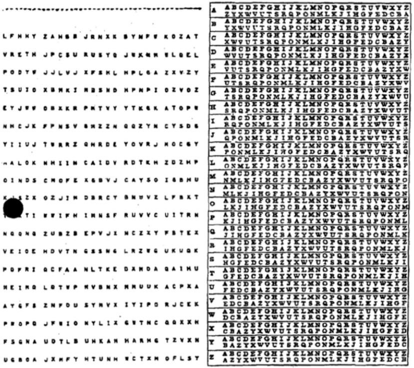


NSA One-Time Pad (Source: Wikimedia)

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. . . . . .

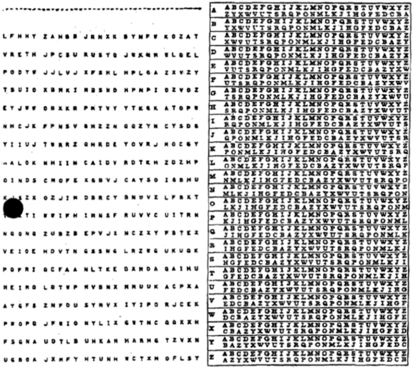


NSA One-Time Pad (Source: Wikimedia)

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. . . . . .

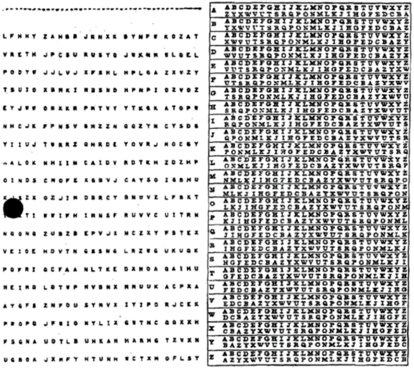


NSA One-Time Pad (Source: Wikimedia)

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......

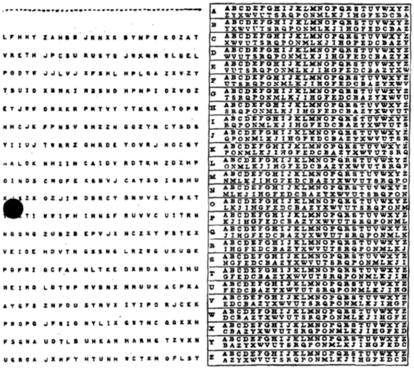


NSA One-Time Pad (Source: Wikimedia)

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......

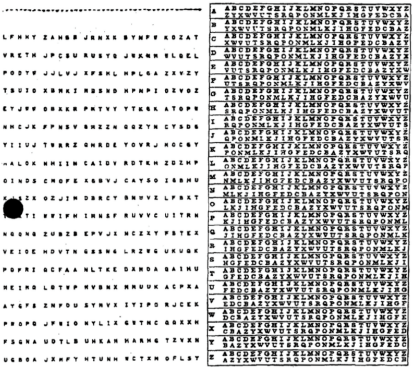


NSA One-Time Pad (Source: Wikimedia)

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

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

$$\text{Find } x$$

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

$$b^x = a \mod q$$
$$\text{Find } x$$

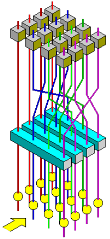
Discrete logarithm problem

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)

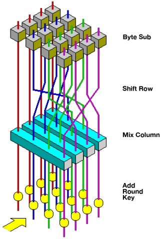
$$b^x = a \mod q$$
$$\text{Find } x$$

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)

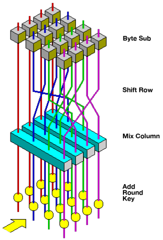
$$b^x = a \mod q$$
$$\text{Find } x$$

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)

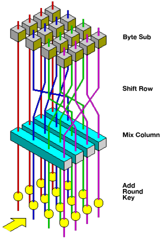
$$b^x = a \mod q$$
$$\text{Find } x$$

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)

$$b^x = a \mod q$$
$$\text{Find } x$$

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 $\Longrightarrow$ PKE $\Longleftarrow$ OT $\Longleftrightarrow$ MPC

PKE $\Downarrow$ KE

Minicrypt

KE $\Downarrow$ OWF

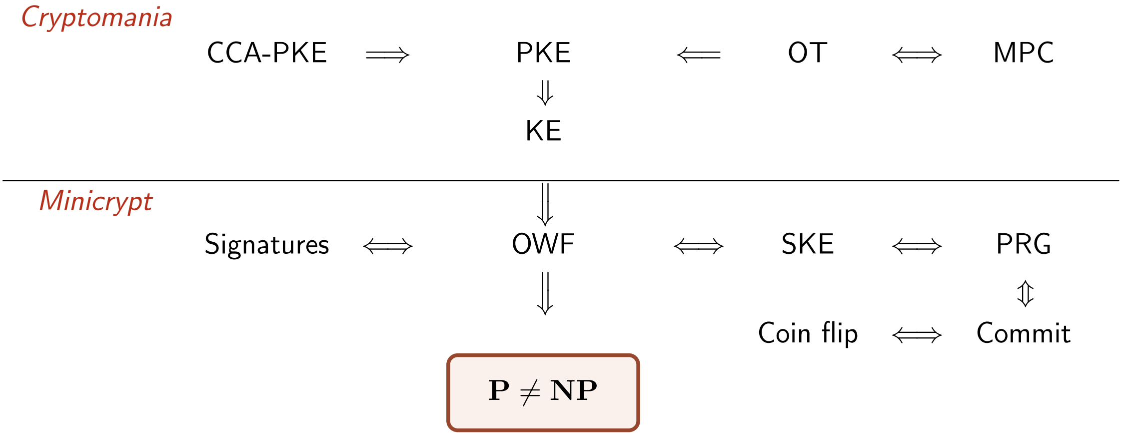
Signatures $\Longleftrightarrow$ OWF $\Longleftrightarrow$ SKE $\Longleftrightarrow$ PRG

PRG $\Updownarrow$ Commit

Coin flip $\Longleftrightarrow$ Commit

OWF $\Downarrow$ $\mathbf{P} \neq \mathbf{NP}$

Classical Cryptography



Quantum Cryptography

Minicrypt

$\ldots \implies$ OWF

$\Downarrow$

PRSG

$\Downarrow$

SKE

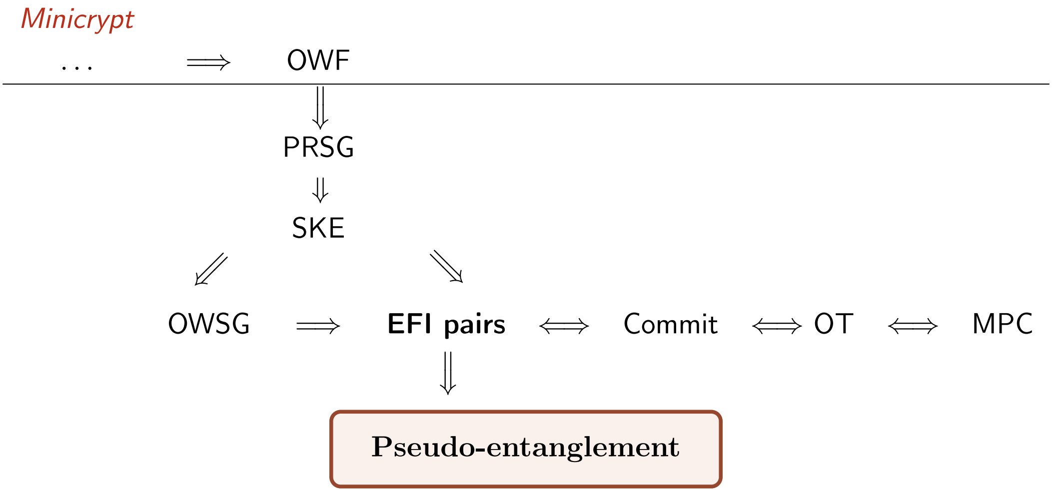
$\swarrow \quad \searrow$

OWSG $\implies$ **EFI pairs** $\iff$ Commit $\iff$ OT $\iff$ MPC

$\Downarrow$

Pseudo-entanglement

Quantum Cryptography



Quantum Cryptography

Minicrypt

. . . $\Longrightarrow$ OWF

$\Downarrow$

PRSG

$\Downarrow$

SKE

$\swarrow$ $\searrow$

OWSG $\Longrightarrow$ **EFI pairs** $\Longleftrightarrow$ Commit $\Longleftrightarrow$ OT $\Longleftrightarrow$ MPC

$\Downarrow$

Pseudo-entanglement

QKD

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* $\Longrightarrow \mathbf{P} \neq \mathbf{NP}$
- *Quantum resources* $\Longrightarrow$ 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

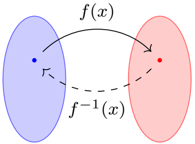
- Impossibility of many *Information-Theoretic* protocols
- *Classical (computational) cryptography* $\implies \mathbf{P} \neq \mathbf{NP}$
- *Quantum resources* $\implies$ weaker Commitments, OT, QKD, ...
- Assume correctness of the *Laws of Physics*
- *New computational world*: Quantum Cryptography,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

How physics and computational hardness relate through cryptography?

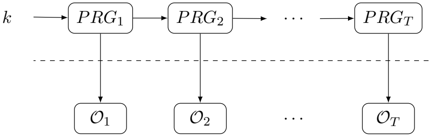
Contents

Weaker Primitives

- **One-Way Functions**



- **Pseudo-Random Generator**



Pseudo-Random State Generator

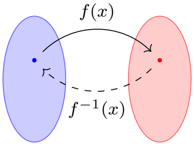
- Efficient gen. (QPT): $G_n(k) = |\psi_k\rangle$
- Pseudo-random: $G_n(k)^{\otimes \mathsf{p(n)}} \approx_c |H\rangle^{\otimes \mathsf{p(n)}}$

OWF $\implies$ PRSG

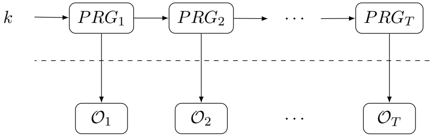
PRSG $\not\Longrightarrow$ (oracle red.) OWF

Weaker Primitives

- **One-Way Functions**



- **Pseudo-Random Generator**



Pseudo-Random State Generator

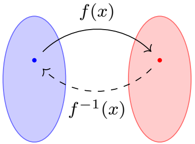
- Efficient gen. (QPT): $G_n(k) = |\psi_k\rangle$
- Pseudo-random: $G_n(k)^{\otimes \mathsf{p(n)}} \approx_c |H\rangle^{\otimes \mathsf{p(n)}}$

OWF $\implies$ PRSG

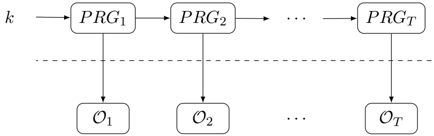
PRSG $\not\Longrightarrow$ (oracle red.) OWF

Weaker Primitives

- **One-Way Functions**



- **Pseudo-Random Generator**



Pseudo-Random State Generator

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

OWF $\Longrightarrow$ PRSG

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

EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

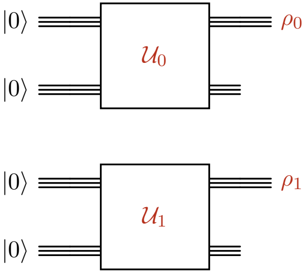
- Efficiently preparable: QPT $\mathcal{U}_0, \mathcal{U}_1$
- statistically Far: $\mathrm{TD}(\rho_0, \rho_1) = 1 - \varepsilon$
- computationally Indistinguishable: $\rho_0 \approx_c \rho_1$

EFI Pairs $\Longleftrightarrow$ Commitments $\Longleftrightarrow$ OT $\Longleftrightarrow$ MPC

EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

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

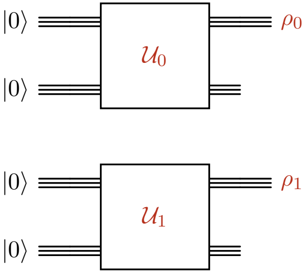


EFI Pairs $\Longleftrightarrow$ Commitments $\Longleftrightarrow$ OT $\Longleftrightarrow$ MPC

EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

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

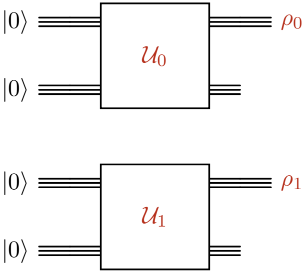


EFI Pairs $\Longleftrightarrow$ Commitments $\Longleftrightarrow$ OT $\Longleftrightarrow$ MPC

EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

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

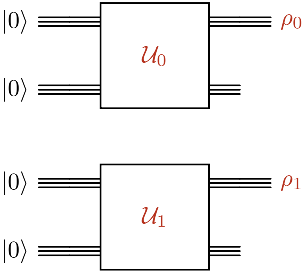


EFI Pairs $\Longleftrightarrow$ Commitments $\Longleftrightarrow$ OT $\Longleftrightarrow$ MPC

EFI (quantum state) Pairs

Mixed n-qubit states ρ_0, ρ_1

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



EFI Pairs $\Longleftrightarrow$ Commitments $\Longleftrightarrow$ OT $\Longleftrightarrow$ MPC

EFID(istribution) Pairs

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

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

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

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

EFID Pairs $\Longleftrightarrow$ PRG $\Longleftrightarrow$ OWF

EFID(istribution) Pairs

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

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

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

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

EFID Pairs $\Longleftrightarrow$ PRG $\Longleftrightarrow$ OWF

EFID(istribution) Pairs

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

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

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

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

EFID Pairs $\Longleftrightarrow$ PRG $\Longleftrightarrow$ OWF

EFID(istribution) Pairs

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

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

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

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

EFID Pairs $\Longleftrightarrow$ PRG $\Longleftrightarrow$ OWF

EFID(istribution) Pairs

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

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

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

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

EFID Pairs $\iff$ PRG $\iff$ OWF

Contents

Computational Entanglement

Entanglement cost

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

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

Distillable entanglement

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

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

Restrict LOCC operations to QPT

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

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

Computational Entanglement

Entanglement cost

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

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

Distillable entanglement

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

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

Restrict LOCC operations to QPT

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

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

Computational Entanglement

Entanglement cost

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

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

Distillable entanglement

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

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

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

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

- ϕ_{AB} has high entanglement

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

- Computational ind. $t = \mathrm{poly}(n)$ 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. $t = \mathrm{poly}(n)$ 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. $t = \mathrm{poly}(n)$ 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. $t = \mathrm{poly}(n)$ 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 $X = \{X_n\}_n$ $Y = \{Y_n\}_n$

- $B \sim \text{Bernoulli}\left(\frac{1}{2}\right)$
- $W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$
- $Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$

False entropy $\Longleftrightarrow$ EFID pairs $\Longleftrightarrow$ 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 $X = \{X_n\}_n$ $Y = \{Y_n\}_n$

- $B \sim \mathrm{Bernoulli}\left(\frac{1}{2}\right)$
- $W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$
- $Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$

False entropy $\iff$ 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 $X = \{X_n\}_n$ $Y = \{Y_n\}_n$

- $B \sim \mathrm{Bernoulli}\left(\frac{1}{2}\right)$
- $W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$
- $Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$

False entropy $\Longleftrightarrow$ EFID pairs $\Longleftrightarrow$ 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 $X = \{X_n\}_n$ $Y = \{Y_n\}_n$

- $B \sim \mathrm{Bernoulli}\left(\frac{1}{2}\right)$
- $W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$
- $Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$

False entropy $\Longleftrightarrow$ EFID pairs $\Longleftrightarrow$ 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 $X = \{X_n\}_n$ $Y = \{Y_n\}_n$

- $B \sim \mathrm{Bernoulli}\left(\frac{1}{2}\right)$
- $W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$
- $Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$

False entropy $\Longleftrightarrow$ EFID pairs $\Longleftrightarrow$ 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 $X = \{X_n\}_n$ $Y = \{Y_n\}_n$

- $B \sim \text{Bernoulli}\left(\frac{1}{2}\right)$
- $W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$
- $Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$

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

- $B \sim \text{Bernoulli}\left(\frac{1}{2}\right)$
- $W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$
- $Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$

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

- $B \sim \text{Bernoulli}\left(\frac{1}{2}\right)$
- $W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$
- $Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$

False entropy $\Longleftrightarrow$ EFID pairs $\Longleftrightarrow$ 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 $X = \{X_n\}_n$ $Y = \{Y_n\}_n$

- $B \sim \text{Bernoulli}\left(\frac{1}{2}\right)$
- $W_i = \begin{cases} (0, X_i) & \text{wp. } \frac{1}{2} \\ (1, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$
- $Z_i = \begin{cases} (B, X_i) & \text{wp. } \frac{1}{2} \\ (B, Y_i) & \text{wp. } \frac{1}{2} \end{cases}$

False entropy $\Longleftrightarrow$ EFID pairs $\Longleftrightarrow$ OWF

EFI Pairs $\implies$ Pseudo-Entanglement

Construction

EFI pair ρ_0, ρ_1

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

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

EFI Pairs $\implies$ Pseudo-Entanglement

Construction

EFI pair ρ_0, ρ_1

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

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

EFI Pairs $\implies$ Pseudo-Entanglement

Proof (Cost of ψ_{AB})

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

- 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})

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

- 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})

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

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

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

EFI Pairs $\implies$ Pseudo-Entanglement

Proof (Cost of ψ_{AB})

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

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

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

EFI Pairs $\implies$ Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

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

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

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

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

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

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

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

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

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

EFI Pairs $\implies$ Pseudo-Entanglement

Proof (Distillation of ϕ_{AB})

$$\phi_{AB} = \frac{1}{2}\left(|\Phi^+\rangle\langle\Phi^+|_{AB} \otimes {\rho_0}_A + |\Phi^-\rangle\langle\Phi^-|_{AB} \otimes {\rho_1}_A\right)$$

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

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

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

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

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

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

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

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

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

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

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

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

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

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

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

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

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

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

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

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

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

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

EFI Pairs $\implies$ Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

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

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

EFI Pairs $\implies$ Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

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

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

EFI Pairs $\Longrightarrow$ Pseudo-Entanglement

Proof (amplification)

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

Error:

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

Swap:

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

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

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?