Secure Non-Interactive Reducibility is Decidable

Kaarthik Bhusan[1] Ankit Kumar Mishra[1] Varun Narayanan [2]
Manoj Prabhakaran[1]

[1] Indian Institute of Technology Bombay, India

[2] Technion, Israel

TCC 2022

Our results

Secure Non-Interactive Reduction (SNIR) Problem

Is there a statistical SNIR for securely sampling (U, V) given (X, Y)?

i.e., $\forall \epsilon > 0$, an ϵ-SNIR for (U, V) given n_ϵ copies of (X, Y).

Our results

Secure Non-Interactive Reduction (SNIR) Problem

Is there a statistical SNIR for securely sampling (U, V) given (X, Y)?

i.e., $\forall \epsilon > 0$, an ϵ-SNIR for (U, V) given n_ϵ copies of (X, Y).

Theorem [Statistical SNIR $\implies$ Perfect SNIR]

Statistical SNIR $\implies$ Perfect SNIR for (U, V) given (X, Y).

i.e., a 0-SNIR for (U, V) given n_0 copies of (X, Y).

Our results

Secure Non-Interactive Reduction (SNIR) Problem

Is there a statistical SNIR for securely sampling (U, V) given (X, Y)?

i.e., $\forall \epsilon > 0$, an ϵ-SNIR for (U, V) given n_ϵ copies of (X, Y).

Theorem [Statistical SNIR $\implies$ Perfect SNIR]

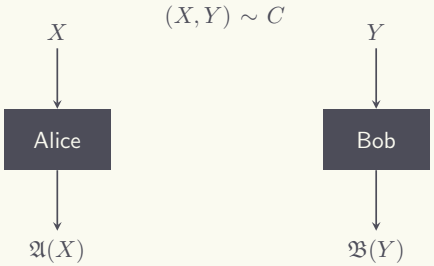
Statistical SNIR $\implies$ Perfect SNIR for (U, V) given (X, Y).

i.e., a 0-SNIR for (U, V) given n_0 copies of (X, Y).

Corollary

SNIR problem is **decidable**. Further, if there is a statistical SNIR for (U, V) given (X, Y), a perfect SNIR for the same can be computed.

Perspectives of a SNIR



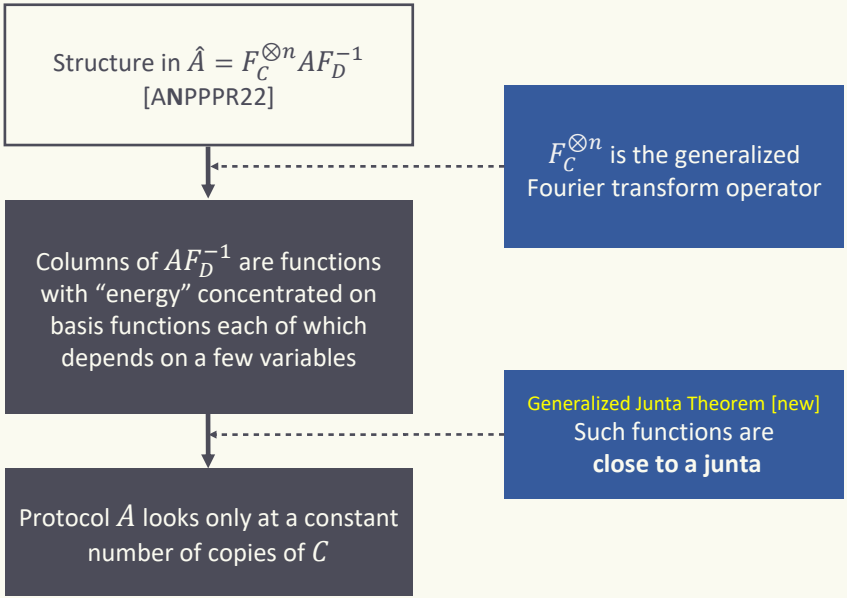
Cryptographic view: Secure protocol to sample (U, V) given many copies of (X, Y) non-interactively

Linear Algebraic view: Can be viewed as matrices: $A^\intercal C B = D$

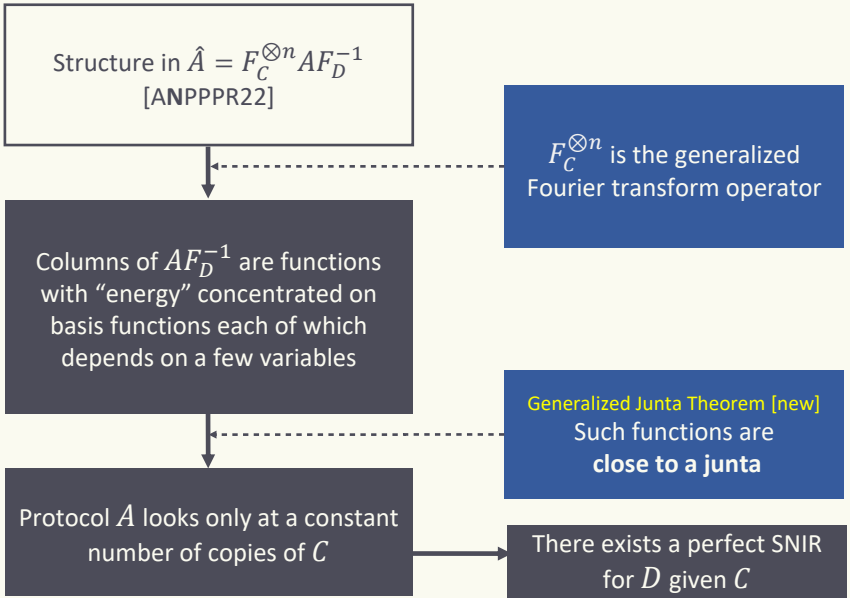
Spectral view: "Spectral protocol" obtained via singular value decomposition of C, D: $\widehat{A}^\intercal \Sigma_C \widehat{B} = \Sigma_D$

Fourier Analytic view: When C is in the form of many independent copies, analyze A, B as functions of many variables

Suppose (A, B) is an ϵ-SNIR for securely sampling a copy of D using n copies of C (i.e., $C^{\otimes n}$)



Suppose (A, B) is an ϵ-SNIR for securely sampling a copy of D using n copies of C (i.e., $C^{\otimes n}$)



Conclusion and Open Problems

- Statistical SNIR problem is decidable

Conclusion and Open Problems

- Statistical SNIR problem is decidable
- Open: *Rate* in statistical SNIR

Conclusion and Open Problems

- Statistical SNIR problem is decidable
- Open: *Rate* in statistical SNIR
- Open: Rate in secure *interactive* reductions (i.e., OT complexity)

Conclusion and Open Problems

- Statistical SNIR problem is decidable
- Open: *Rate* in statistical SNIR
- Open: Rate in secure *interactive* reductions (i.e., OT complexity)

Thank you!