Composably secure device-independent encryption with certified deletion

Srijita Kundu (CQT, Singapore)
Ernest Y.-Z. Tan (ETH Zürich, Switzerland)

03 Feb 2021

arXiv:2011.12704

Main results

- Modifications to [BI19] protocol
  - Device-independent (DI), i.e. measurements are untrusted
  - Security against eavesdropper
  - Composable security (operational)

- Existing DI proof techniques insufficient?
- Our approach: prove new parallel repetition threshold theorem
  - For games with multiple input-output rounds

“Standard” quantum cryptography setting

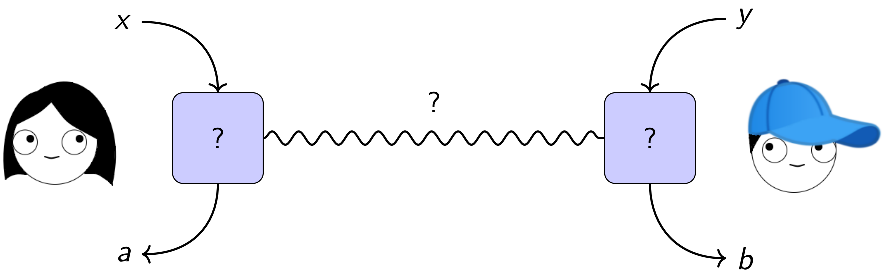
- Example: [BI19] protocol
  - Prepare-and-measure: Alice knows the states she prepares
  - Entanglement-based: Alice knows the measurements she performs

- Can we weaken assumptions? “Device-independence”

Device-independent (DI) setting

Example: Magic square game (MS)

$x, y \in \mathbb{Z}_3$ and $a, b \in \mathbb{Z}_2^3$ with $\sum_j a_j = 0$, $\sum_j b_j = 1$; win condition $a_y = b_x$

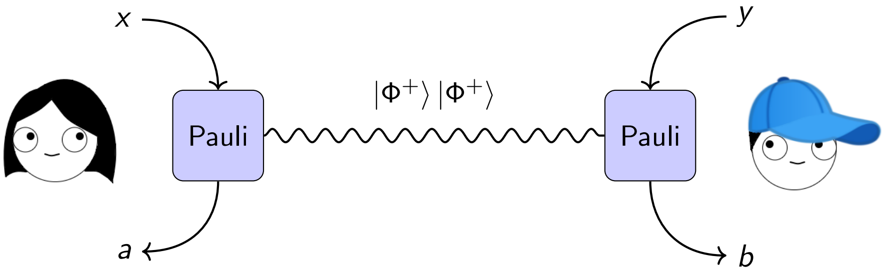


Rigidity a.k.a. self-testing

Example: Magic square game (MS)

$x, y \in \mathbb{Z}_3$ and $a, b \in \mathbb{Z}_2^3$ with $\sum_j a_j = 0$, $\sum_j b_j = 1$; win condition $a_y = b_x$

If devices win with probability $1 - \delta$, then (δ-approximately)



2-round game

- Recap: e.g. suppose Alice measures σ_Z on $|\Phi^+\rangle$
- If Bob measures σ_X, erases his information

- Consider 2-round game MSB, roughly†:
  - Round 1: Play MS game (with inputs x, y)
  - Round 2: Bob tries to guess Alice's output $a_{y'}$ (given x and $y' \neq y$)
- In honest case, Bob's measurement in Round 1 erases info about $a_{y'}$
- [FM17] prove, via rigidity:
  - Suppose Round 1 winning probability is $1 - \delta$
  - Then Round 2 winning probability is $1/2 + O(\sqrt{\delta})$
- $\implies$ MSB winning probability $< \kappa < 1$

†Actual game involves *anchoring*

Parallel repetition theorem

- Our contribution: new parallel repetition threshold theorem, for *2-round product-anchored games* (includes MSB)
- I.e. for ℓ parallel instances of MSB (denote as MSB^ℓ), probability of winning $> t$ instances (for large enough t) decreases exponentially

- Technique: for a subset C, at least one of these holds:
  - Winning probability on C is already small
  - $\exists$ instance $i \notin C$ with winning probability $< \kappa' < 1$

“Parallel security” from parallel repetition

- Idea: similar to [BI19] protocol, but use ℓ MS box pairs
- To certify deletion:
  - Alice challenges Bob to send box outputs
  - Accepts if they win MS in enough rounds

- Recap: security proof uses $H^{\varepsilon}_{\min}(\text{Alice's outputs}|\text{Bob's information})$
- (Similar to [Vid17]) Threshold theorem $\rightarrow$ min-entropy bound, roughly:
  - Suppose Alice accepts ($\sim$ Round 1 of MSB^{ℓ}) with high probability
  - $\implies$ Bob's guessing probability ($\sim$ Round 2 of MSB^{ℓ}) $\leq O(\tilde{\kappa}^{-\ell})$
  - $\implies$ $H^{\varepsilon}_{\min}(\text{Alice's outputs}|\text{Bob's information}) \geq \Omega(\ell)$

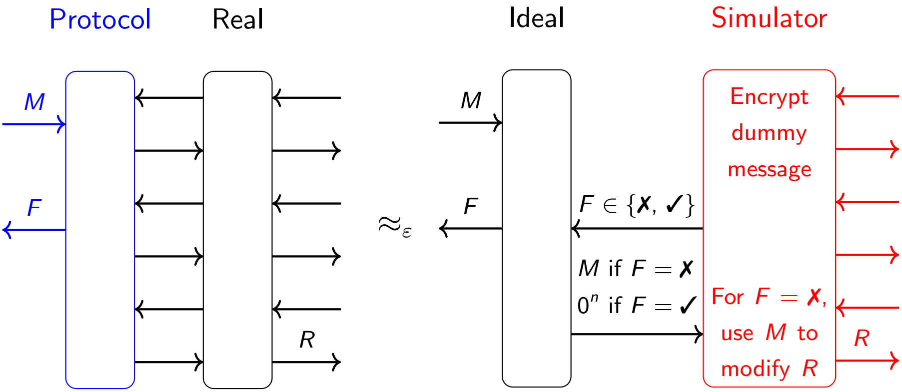
Some remarks

- "Parallel security" seems important
  - Dishonest Bob may not use his inputs sequentially
  - Unclear how to apply previous approaches, e.g. entropy accumulation theorem
- If Bob is honest, what about eavesdropper?
  - We introduce QKD-like check to detect eavesdropping
  - Proof similar to parallel-DIQKD approaches [JMS20], [Vid17]

Composable security

- *Abstract Cryptography* framework
- Define ideal functionality
- Goal: show real protocol can "safely" replace ideal functionality (operational!)
  - How? Prove real and ideal are indistinguishable (sort of)
- Does not rely on dishonest parties' "goals/incentives"
- Must describe in terms of resources
  - Instead of decryption key, define *temporarily private randomness source*
  - Supplies randomness R but publicly broadcasts it later

Simplified[‡] outline (honest Alice and dishonest Bob only)



[‡]Omits some features, e.g. security against eavesdropper

Some implications

- Minor variants follow from basically the same proof
- Suggests $|R| \geq |M|$ may be necessary
  - Indeed $|R| \geq |M|$ for [BI19] and our protocol
  - Proven necessary for tamper-evident storage [vdVCRŠ20]
- Suggests no "commitment" property is possible (if Alice dishonest)

Summary

- New parallel repetition threshold theorem
  - "Parallel security" seems important here
- Modified security arguments
  - Security against eavesdropper
  - Composable security

- Future prospects:
  - Other applications of threshold theorem
  - Combining with other protocols
  - For $|R|$, converse statements/improved efficiency