# Bit-Commitment and Coin Flipping in a Device-Independent Setting

J. Silman

Université Libre de Bruxelles

Joint work with: A. Chailloux & I. Kerenidis (LIAFA), N. Aharon (TAU), S. Pironio & S. Massar (ULB).

# Outline of Talk

- Introduction: Device-independent (DI) approach to quantum cryptography, bit-commitment (BC), the GHZ paradox.
- A DI quantum BC protocol.
- Comparison with device-dependent (DD) version of protocol.
- Implications for quantum coin flipping (CF).
- Generalization of protocols to maximally nonlocal post-quantum theories.
- Summary.
- Open questions.

# Device-Independent Approach to Quantum Cryptography

- The power of quantum cryptography is that security is guaranteed by the laws of physics irrespectively of the capabilities of an adversary, i.e. his computational power, etc.
- Still, quantum protocols call for assumptions on the capabilities of honest participants:
  - Having secure labs, source of trusted randomness, and assumptions on the inner workings of the physical setup, e.g. Hilbert space dimension of the quantum information carriers, etc.
- DI approach's aim is to base security on a minimum # of assumptions by eliminating any assumptions on the inner workings.
- Achieved by basing security on nonlocality and no-signaling (Barrett et al. 05).

- Reason no such assumptions are needed is because security is evaluated by observing nonlocal correlations between no-signaling devices. For example:
  - In DI QKD high violation of CHSH inequality implies, via monogamy of entanglement, that Eve has no information of (processed) key (Acín et al. 07).
- Contrast with the entanglement-based version of BB84 protocol, where if source dispenses qudits instead of qubits, security is utterly breached (Acín et al. 06). $\Rightarrow$ Need to know Hilbert space dimension.
- Scope of approach is so broad, it covers not only malfunctions but allows for the physical setup to have been fabricated by an adversary.

- ✦ Approach is also useful for non-cryptographic applications, e.g. RNG (Colbeck 06, Pironio et al. 10), self-testing devices (Mayers & Yao 04), and certification of genuine multi-partite entanglement (Bancal et al. 11).

- ✦ Latter work contains instructive example showing how tilting by $\theta$ one measurement axis of one device, i.e. $\sigma_y \to \cos\theta\sigma_y + \sin\theta\sigma_x$, can result in the DD genuine tri-partite entanglement witness

$$\left|\langle\psi\,|\sigma_x\otimes\sigma_x\otimes\sigma_x - \sigma_x\otimes\sigma_y\otimes\sigma_y - \sigma_y\otimes\sigma_x\otimes\sigma_y - \sigma_y\otimes\sigma_y\otimes\sigma_x|\,\psi\rangle\right| \leq 2$$

falsely classifying bi-separable states as genuinely tri-partite entangled. ⇒ Need for DI witnesses.

# Device-Independent Distrustful Cryptography

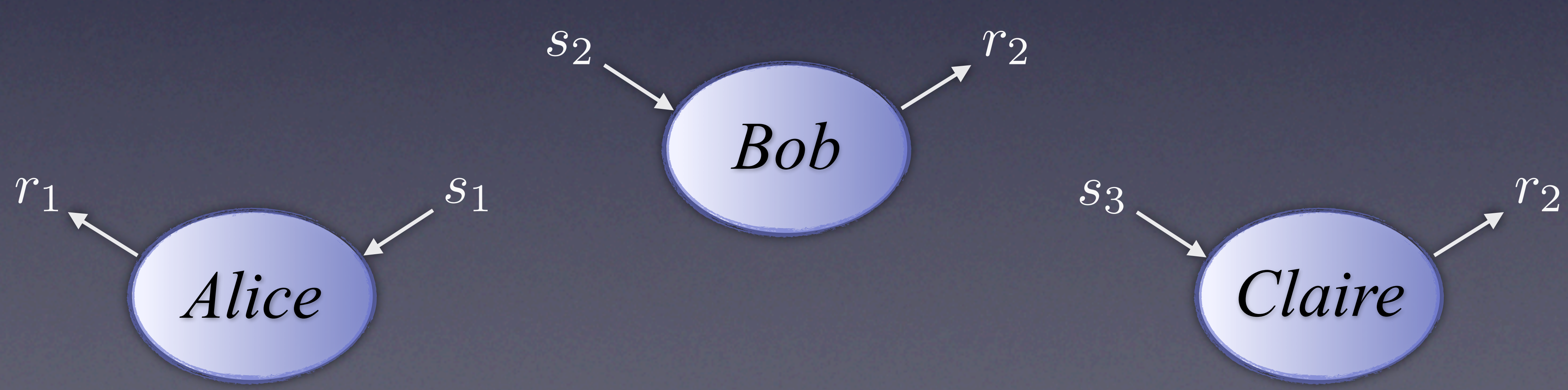
- Distrustful cryptography refers to cryptographic protocols where the participants don't trust each other.
- Example is CF where two parties wish to agree on the value of a bit but each party doesn't trust the other not to cheat, i.e. deviate from protocol.
- It isn't a priori clear if such protocols admit a DI formulation, since in contrast to DI QKD - where the parties trust each other and collaborate to (statistically) certify amount of nonlocality present and resulting level of security - honest parties can now only trust themselves.
- However, as we'll see, statistical estimation of amount of nonlocality isn't an essential building block of DI approach.
- Specifically, we'll show that BC and CF admit a DI formulation with cheating probabilities reasonably close to optimal ones of the DD setting.

# Bit-Commitment

- In BC Alice must commit a bit to Bob, such that she cannot change it once she committed, and Bob cannot learn it until she reveals it.
- BC incorporates two phases:
  - Commit phase - where Alice commits to a bit by sending Bob a token.
  - Reveal phase - where Alice reveals the bit.
- Classically, if there are no restrictions on computational power, BC is impossible, i.e. dishonest party can cheat perfectly.
- Using quantum resources, perfect BC is impossible (Mayers 96, Lo & Chau, 96), but imperfect protocols exist (Ambainis 01, Spekkens & Rudolph 01).
- Optimal quantum protocol: 0.739 cheating probability for both parties (Chailloux & Kerenidis 11).

# The GHZ paradox

- GHZ paradox is another example of nonlocality of QM. Paradox is easily explained as a three-player game:
  - Before start of game Alice, Bob and Claire may communicate and share resources, but afterwards they cannot.
  - Game starts with player $i$ receiving a binary input $s_i$. Inputs must satisfy $s_1 \oplus s_2 \oplus s_3 = 1$ with different combinations equally probable.
  - Game is won iff players' outputs satisfy $r_1 \oplus r_2 \oplus r_3 = s_1 \cdot s_2 \cdot s_3 \oplus 1$.



- Classically game cannot always be won. Easy to see by representing outputs corresponding to $s_i = 0\,,\;\; s_i = 1$ by $y_i = (-1)^{r_i},\;\; x_i = (-1)^{r_i}$, respectively. Winning conditions then read

$$y_1 \cdot y_2 \cdot x_3 = -1\,, \quad y_1 \cdot x_2 \cdot y_3 = -1\,, \quad x_1 \cdot y_2 \cdot y_3 = -1\,, \quad x_1 \cdot x_2 \cdot x_3 = 1$$

- Taking the product of all four equations we get that

$$x_1^2 \cdot y_1^2 \cdot x_2^2 \cdot y_2^2 \cdot x_3^2 \cdot y_3^2 = -1$$

- In fact, game can be won with probability 0.75 at most.

- The GHZ state $|000\rangle + |111\rangle$ has property that it's an eigenstate with eigenvalues -1 and 1, respectively, of

$$\sigma_y \otimes \sigma_y \otimes \sigma_x \,, \quad \sigma_y \otimes \sigma_x \otimes \sigma_y \,, \quad \sigma_x \otimes \sigma_y \otimes \sigma_y$$

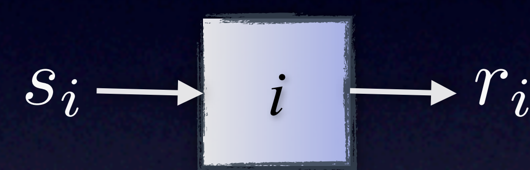
and

$$\sigma_x \otimes \sigma_x \otimes \sigma_x$$

- Strategy is then to measure $\sigma_y \,, \sigma_x$ when receiving $s_i = 0 \,, \; s_i = 1 \,,$ respectively. ⇒ Game is always won.

# The Assumptions Behind the Setup

- Each party has (‘black’) boxes with knobs to choose (classical) inputs $s_i$ and registers for (classical) outputs $r_i$. Entering an input always results in an output.




- Boxes can’t communicate with one another, implying that if $\Pi_{r_i|s_i}$ are an honest party’s POVM elements corresponding to inputting $s_i$ and outputting $r_i$, then

$$P\left(r_1, \ldots, r_n \mid s_1, \ldots, s_n\right) = \mathrm{Tr}\left(\rho \otimes_i \Pi_{r_i|s_i}\right)$$

(A dishonest party can select $\Pi_{r_i|s_i}$ and $\rho$.)

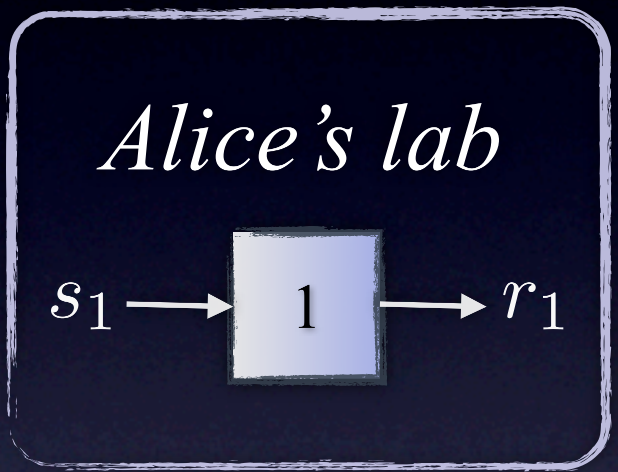
- The parties have a trusted source of randomness.

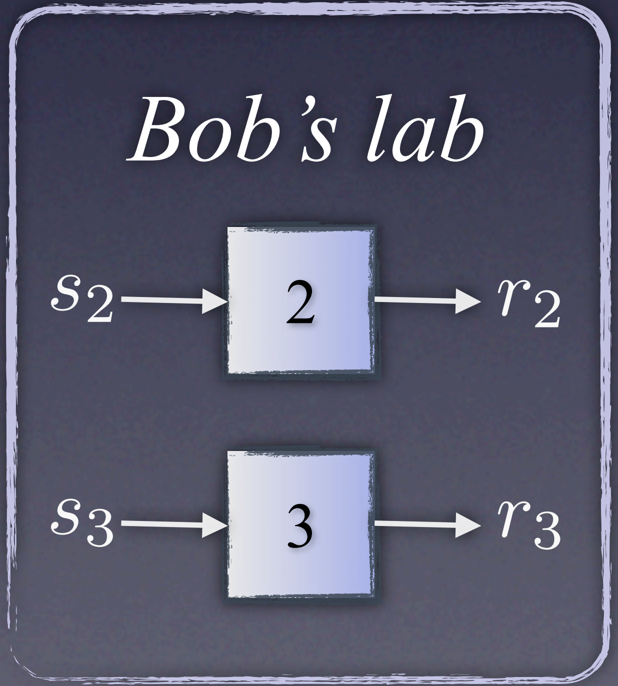
- No information leaks out of an honest party’s lab.

- The parties are restricted by QM.

# Device-Independent Bit-Commitment Protocol

- Alice has box 1 and Bob has boxes 2 and 3. The boxes are supposed to satisfy GHZ paradox.
- Commit phase:
  - Alice inputs into her box her commitment $s_1$.
  - She randomly picks a bit $a$ and sends Bob $c = r_1 \oplus (s_1 \cdot a)$.
- Reveal phase:
  - Alice sends Bob $s_1$, $r_1$. He checks if $c = r_1$ or $c = r_1 \oplus s_1$. If not, he aborts.
  - Else he randomly picks inputs $s_2$, $s_3$ satisfying $s_2 \oplus s_3 = 1 \oplus s_1$ and checks if $r_1 \oplus r_2 \oplus r_3 = s_1 s_2 s_3 \oplus 1$. If not, he aborts.



# Bob's Security: Dishonest Alice's Strategy

- Since Bob sends Alice no information WNLOG we may assume she sends $c = 0$ as her token, and accordingly prepares Bob's boxes.
- It's then straightforward to show that Alice's cheating probability is given by

  $$\frac{1}{4}\left[P\left(x_1 x_2 x_3 = 1\right) + P\left(x_1 y_2 y_3 = -1\right) + P\left(x_2 y_3 = -1\right) + P\left(y_2 x_3 = -1\right)\right]$$

  (where outputs corresponding to inputting $s_i = 0$, $s_i = 1$ are denoted by $y_i = (-1)^{r_i}$, $x_i = (-1)^{r_i}$).
- It can be shown that since Alice's side admits a single input, maximum obtains when $x_1$ is deterministic. Cheating probability then reduces to the winning probability in the CHSH game:

  $$P_A^* = \cos^2\left(\frac{\pi}{8}\right) \simeq 0.854$$

- Alice's strategy is to prepare Bob's boxes in a maximally entangled 2-qubit state and his devices such that that they maximally violate the CHSH inequality.

# Alice's Security: Dishonest Bob's Strategy

- Bob's most general strategy is to entangle Alice's box with an ancilla and after receiving $c$ (dependent on its value) measure a dichotomic operator on the ancilla, whose outcome is his guess of the bit.

- Bob's maximum cheating probability obtains by maximizing

$$\sum_{s_1,\,r_1,\,a} P(a,\,s_1)\,P(r_1 \mid s_1)\,P(g = s_1 \mid m = c = r_1 \oplus (a \cdot s_1)\,,\, r_1,\, s_1) \leq \frac{3}{4}$$

where $m$ and $g$ label Bob's input and output and to obtain the inequality we've made use of the no-signaling conditions

$$\sum_{r_{j \neq i}} P(r_1,\, r_2 \mid s_1,\, s_2) = P(r_i \mid s_i)$$

- Bound can be obtained using classical strategy:
  - Bob programs Alice's box such that $r_1 = s_1$, and guesses $c$ for the committed bit. Since Alice is honest $c = r_1$ 75% of time.

# Device-Dependent Version of Protocol

- In the DD version of protocol:
  - (Honest) Alice prepares a 3-qubit GHZ state and sends Bob two of the qubits.
  - Honest parties can trust their devices to measure $\sigma_y,\ \sigma_x$ when inputting 0, 1.
- It turns out that the DD version doesn't give rise to lower cheating probabilities than the DI version. $\Rightarrow$ DD optimal cheating strategies are also optimal in the DI case.

# Coin Flipping

- In CF remote Alice and Bob wish to agree on a bit, but they don't trust each other.
- Like BC, classically, CF is impossible.
- Using quantum resources story is different (Aharonv et al. 00, Ambainis 01, Spekkens & Rudolph 01).
- Optimal quantum protocol: 0.707 cheating probability for both parties (Kitaev 02, Chailloux & Kerenidis 10).
- Weaker version of CF, where Alice and Bob have known, opposite preferences for the outcome, allows arbitrarily small cheating probability (Mochon 07).

# Device-Indpendent Coin Flipping Protocol

- Standard way to construct CF using BC is to have Bob send Alice a random bit after commit phase. The outcome is the XOR of their bits.
- Cheating probabilities are identical to those of BC protocol.
- Imbalance in cheating probabilities can be used to construct another CF protocol with cheating probabilities evened out through repetition:
  - Protocol consists of $N$ repetitions. The outcome of the $n$th determines who commits in the $n$+1th.
  - Outcome of protocol is the outcome of the $N$th repetition.
  - Protocol aborts iff one of the BC subroutines aborts.
- Using our DI BC, we get a DI CF protocol with $P_A^*,\ P_B^* \lesssim 0.836$ .

# Device-Independent Distrustful Cryptography in Post-Quantum Theories

- It's interesting to inquire whether our protocols are secure in post-quantum theories (i.e. no-signaling theories leading to a greater violation of CHSH inequality then Tsirelson's bound).
- In the BC protocol Alice's security is based only on no-signaling but Bob's is determined by Tsirelson's bound. ⇒ Protocol is secure in all post-quantum theories except maximally nonlocal ones.
- Is DI BC possible in maximally nonlocal post-quantum theories?
  - If yes, does there exist a quantum protocol secure against maximally nonlocal post-quantum cheaters?
  - Note that perfect BC is possible under the assumption that PR boxes are available but cannot be tampered with (Buhrman et al. 06).

# Post-Quantum Device-Independent Bit-Commitment & Coin Flipping

- GHZ paradox plays a crucial role in our protocol in that it determines Bob's test for checking if Alice is a dishonest.
- Like in GHZ paradox, PR box also gives rise to psuedo-telepathic correlations:
  - PR: $r_1 \oplus r_2 = s_1 \cdot s_2$
  - GHZ: $r_1 \oplus r_2 \oplus r_3 = s_1 \cdot s_2 \cdot s_3 \oplus 1 \quad ( s_1 \oplus s_2 \oplus s_3 = 1 )$
- Similarity of correlations suggests possibility of generalizing protocols to maximally nonlocal post-quantum theories.
- Indeed, only change is that Bob now has one box instead of two.

# Security of Protocol

- Similarly to GHZ-based protocol, Alice's maximum cheating probability is now obtained by maximizing ($c = 0$):

$$\frac{1}{4}\left[P\left(y_2 = 1\right) + P\left(x_2 = 1\right) + P\left(x_1 y_2 = 1\right) + P\left(x_1 x_2 = -1\right)\right]$$

  Hence, Alice cheats with probability 0.75.

- Protocol is now balanced, since clearly Bob's cheating probability (and strategy) is unchanged.

# Summary

- At least some protocols in the distrustful cryptography class admit DI formulation.
- Above statement holds also in maximally nonlocal post-quantum theories,
- Our protocols include no statistical estimation phase. Alice's security follows from no-signaling and Bob's is determined by Tsirelson's bound.
- DD version of protocol doesn't afford more security and is therefore DI.

# Open Questions

- Is every protocol in the distrustful cryptography class which is amenable to a secure DD formulation also amenable to a DI formulation?
  - If so, can it give the same security?
    - How much more resources would that entail?
- Do there exist quantum DI BC and CF protocols secure also against post-quantum adversaries, as is the case with DI QKD (Masanes, 09)?

# Thank you.

For more information see:
Silman, Chailloux, Aharon, Kerenidis, Pironio, & Massar,
arXiv:1101.5086.