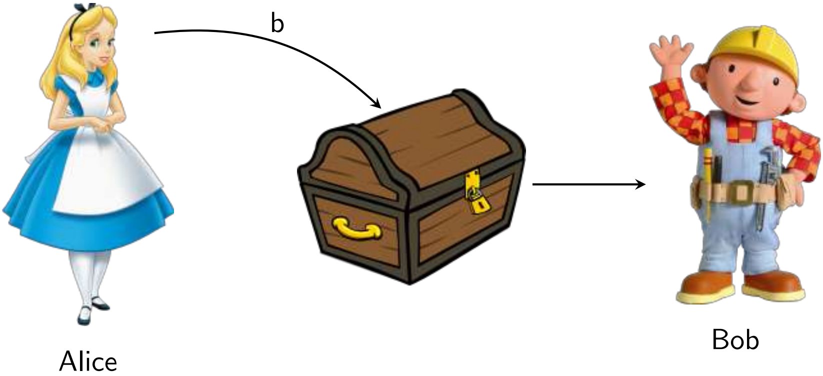
On no-signaling secure bit commitment

Jérôme Guyot[1]
Supervisor : Alex Bredariol Grilo[2]

[1] Université Paris-Saclay, ENS Paris-Saclay
[2] Sorbonne Université, CNRS, LIP6

Bit commitment : Commitment



Bob cannot see through the chest : **Hiding**

Bit commitment : Reveal

Alice

Bob

Alice cannot change the value in the chest : **Binding**

Applications

- Zero-knowledge
- Oblivious bit transfer
- Multi-party computation
- Multi-party interactive proofs

Limitations

Theorem : There is no unconditionally secure bit commitment in the classical and quantum setting [May97][1] [LC98][2].

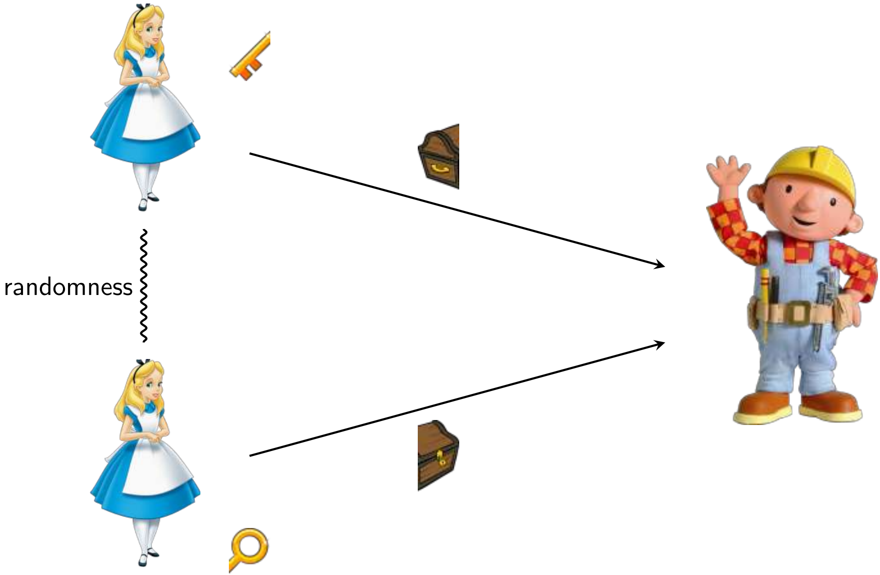
Approach : weaken Alice or Bob

- Computationally bounded Alice
- In our case : split Alice into two non-communicating provers.

[1] Dominic Mayers. *Unconditionally Secure Quantum Bit Commitment is Impossible*.

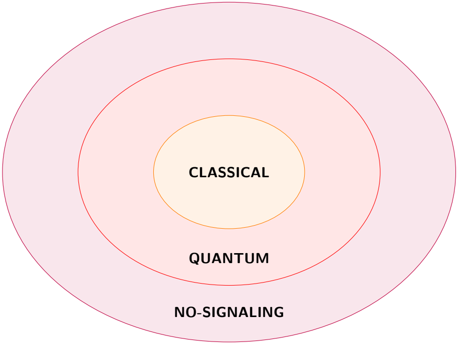
[2] Hoi-Kwong Lo and H.F. Chau. *Why quantum bit commitment and ideal quantum coin tossing are impossible*

More than one Alice [Ben+88]



Hierarchy of correlation

Theorem : [Ben+88][3] Obtains a bit commitment which is secure against adversaries with classical correlations.



[3]Ben-Or, M., Goldwasser, S., Kilian, J., Wigderson, A. (1988). *Multi-prover interactive proofs: how to remove intractability assumptions*

Previous work

Fehr and Fillinger showed in [FF15][4] that

- Schemes with only 2 Alices are not secure against no-signaling adversaries.
- There is a scheme with 3 Alices which is secure against no-signaling adversaries.

The [FF15] scheme cannot be used for zero-knowledge as it is not **selective opening**.

[4] S. Fehr and M. Fillinger. *Multi-Prover Commitments Against Non-Signaling Attacks*. Cryptology ePrint Archive, Paper 2015/501, 2015. https://eprint.iacr.org/2015/501

Goal (Informal)

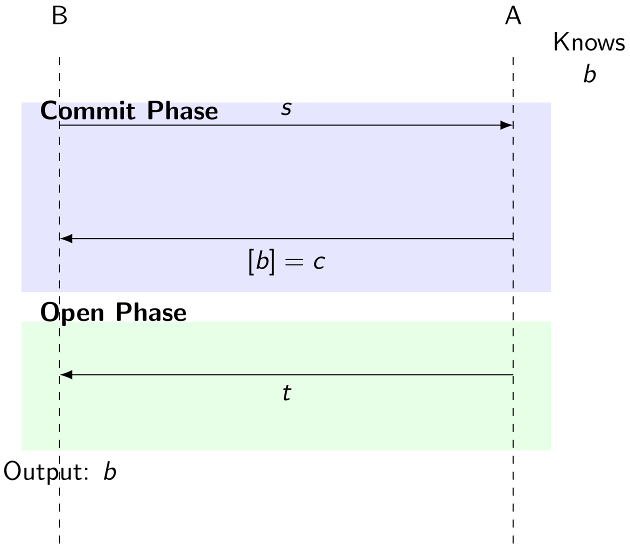
We want a bit commitment that is :

- Secure against no-signaling adversaries.
- Suited for zero-knowledge applications (selective opening) .

Is there such a bit commitment scheme ?

Background : Bit commitment

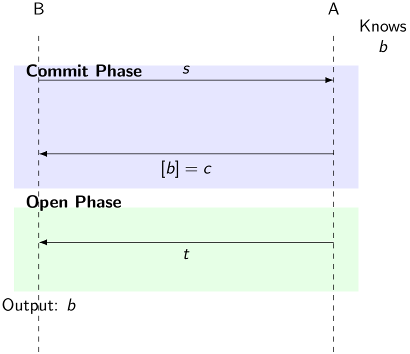
Bit commitment formally I



Bit commitment formally II

A bit commitment is defined by

- Queries of Bob : $p(s)$.
- Honest answers of Alice : $p_0(c, t|s)$ and $p_1(c, t|s)$.
- Acceptation predicate of Bob : $\mathrm{Acc}(c, t|s, b)$.



Properties of bit commitment I

Definition : ϵ-Hiding
If for all s, $\|p_0(c|s) - p_1(c|s)\| \leq \epsilon$.
$\epsilon = 0 \implies$ Perfect hiding.

Definition : ϵ-soundness
Honest answers are accepted with probability at least ϵ :

$$\sum_s p(s) \sum_{c,t} p_b(c,t|s) \text{Acc}(c,t|s,b) \geq \epsilon$$

$\epsilon = 1 \implies$ Perfect soundness.

Properties of bit commitment II

Definition : Binding game

1. B sends s.
2. A commits to c.
3. B sends b.
4. A answers t.
5. Winning condition : t opens c to b.

Definition : ϵ-Binding
If $w(G) \leq \frac{1+\epsilon}{2}$ where $w(G)$ is the value of the binding game associated to the scheme.
ϵ is negligible $\implies$ Statistical binding.

Visualization of binding game with 3 provers

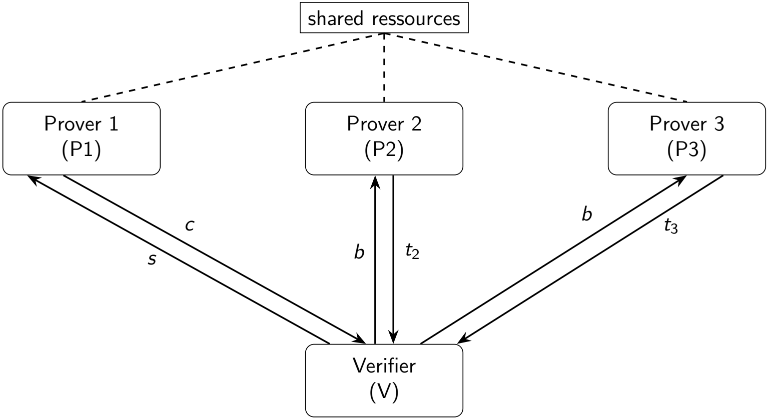


Figure: Binding game for 1 committer 2 openers bit commitment

Background : No-signaling

No-signaling

Intuition

Strategy where players $P1, P2$ cannot communicate.

Output of $P1$ contains no information about input of $P2$ and vice versa.

Definition : No-signaling

A bipartite distribution $\theta(a, b|x, y)$ is no-signaling if

$$\theta(a|x, y) = \theta(a|x) \quad \text{and} \quad \theta(b|x, y) = \theta(b|y)$$

where $\theta(a|x, y) = \sum_b \theta(a, b|x, y)$.

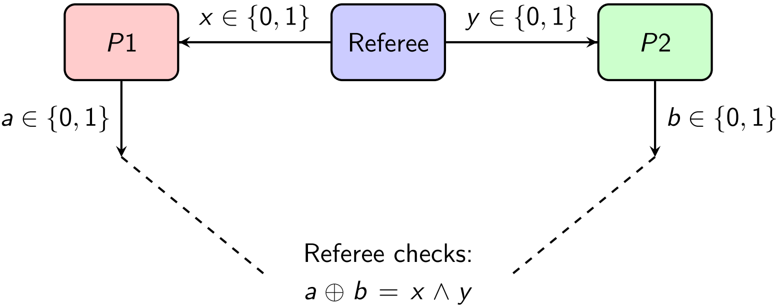
This can be extended to multipartite distributions.

Intuition

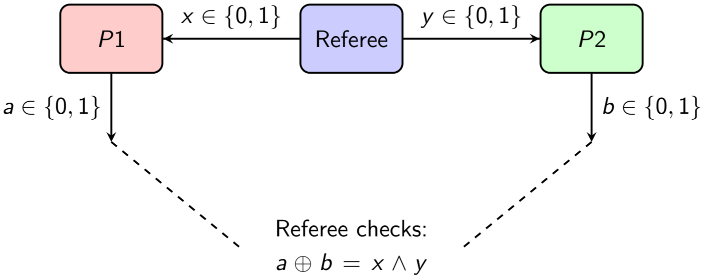
No signaling does not mean a is independent of y.

y can impact a but not its distribution.

Example : CHSH I



Example : CHSH II



- Classical value : $\frac{3}{4}$.
- Quantum value : $\cos^2(\frac{\pi}{8}) \simeq 0.85$.
- No-signaling value : 1

Example : CHSH III

Consider the strategy :

$$\theta(a, b|x, y) = \begin{cases} \frac{1}{2} & \text{if } x \wedge y = a \oplus b \\ 0 & \text{otherwise} \end{cases} .$$

It is no-signaling :

$$\theta(a|x, y) = \sum_b \theta(a, b|x, y) = \sum_{b=(x\cdot y)\oplus a} \theta(a, b|x, y) = \frac{1}{2} = \theta(a|x).$$

And similarly for $\theta(b|x, y) = \theta(b|y)$.

Goal (Formal)

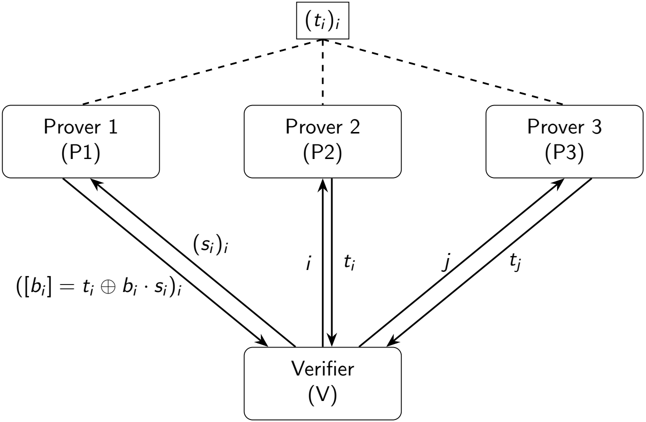
Definition : Selective opening
When more than one bit are committed, a possibly malicious Bob can open at most one bit, and can chose which bit he opens.

Is there a bit commitment scheme which is perfectly hiding, perfectly sound, selective opening and statistically binding against no-signaling adversaries ?

Selective opening bit commitment

Selective opening : Example

Consider the repeated version of the bit commitment from [FF15].



Asking $i \neq j$ reveals b_i and $b_j \implies$ not selective opening.

Impossibility theorem

Theorem : There is no simple selective opening one-round commitment scheme with 3 provers which is perfectly hiding, perfectly sound, statistically binding against no-signaling provers.

Idea of proof

For the 2 committers, 1 opener case, we can adapt the impossibility result of [FF15][5]. Let's study the other case :

[5] S. Fehr and M. Fillinger. *Multi-Prover Commitments Against Non-Signaling Attacks*. Cryptology ePrint Archive, Paper 2015/501, 2015. https://eprint.iacr.org/2015/501

Impossibility of 3 prover selective opening bit commitment

Let *Com* be perfectly hiding, perfectly sound and selective opening, with 1 committer and 2 openers.

Consider the strategy

$$q(c, t_2, t_3 | s, b_2, i, b_3, j) = p_{b_3}(c, t_2, t_3 | s, i, j)$$

It has value 1 on the binding game :

$$= \sum_{s_1, i, b} \sum_{c_1, t_2, t_3} p(s_1) q(c_1, t_2, t_3 | s_1, b, i, b, i) \mathrm{Acc}(c_1, t_2, t_3 | s, b, i)$$

$$= \sum_{s_1, i, b} \sum_{c_1, t_2, t_3} p(s_1) p_b(c_1, t_2, t_3 | s_1, i) \mathrm{Acc}(c_1, t_2, t_3 | s_1, b, i)$$

$$= 1 \quad \text{, as } Com \text{ is perfectly sound.}$$

Impossibility of 3 prover selective opening bit commitment

Let us show some of the no-signaling equalities :

$$\begin{aligned} q(c_1|s_1, b_2, i, b_3, j) &= p_{b_3}(c_1|s_1) \quad \text{, the honest strategy is no-signaling} \\ &= p_{1-b_3}(c_1|s_1) \quad \text{, as } \mathit{Com} \text{ is perfectly hiding} \\ &= q(c_1|s_1) \end{aligned}$$

Impossibility of 3 prover selective opening bit commitment

Let us show some of the no-signaling equalities :

$$\begin{aligned} q(c_1|s_1, b_2, i, b_3, j) &= p_{b_3}(c_1|s_1) \quad \text{, the honest strategy is no-signaling} \\ &= p_{1-b_3}(c_1|s_1) \quad \text{, as } Com \text{ is perfectly hiding} \\ &= q(c_1|s_1) \end{aligned}$$

$$\begin{aligned} &q(c_1, t_2|s_1, b_2, i, b_3, j) \\ &= \sum_{t_3} q(c_1, t_2, t_3|s_1, b_2, i, b_3, j) \\ &= \sum_{t_3} p_{b_3}(c_1, t_2, t_3|s_1, i, j) \\ &= p_{b_3}(c_1, t_2|s_1, i) \quad \text{, as honest provers are no-signaling} \\ &= p_{1-b_3}(c_1, t_2|s_1, i) \quad \text{, as } c_1, t_2 \text{ are perfectly hiding for all } i \\ &= q(c_1, t_2|s_1, i) \end{aligned}$$

4 and more provers schemes

Candidates

We have a few 4 and more provers candidates :

- Use $\frac{k+1}{2}, k$ secret sharing with k openers and 1 committer.

- Use $2, 2$ secret sharing, an "imitator" and 1 committer.

Linear Programming I

- No-signaling conditions are linear constraints.
- No-signaling strategies form a convex polytope.
- We can study the binding by using linear programming with an exponential number of constraints

Linear Programming II

Algorithm Check Binding of Commitment Using LP

Input: Security parameter n
Generate all bitstrings $\mathcal{S} = \{0,1\}^n$
Define decision variable $P(a_1, a_2, a_3, a_4, s, b_2, b_3, b_4, c_4) \geq 0$
Initialize constraint list $\mathcal{C} \leftarrow \emptyset$

▷ Normalization

for all $s \in \mathcal{S},\ b_2, b_3, b_4, c_4 \in \{0,1\}$ **do**
    Add constraint: $\sum_{a_1,a_2,a_3,a_4} P(\cdot|s, b_2, b_3, b_4, c_4) = 1$ to $\mathcal{C}$
end for

▷ No-signaling constraints across marginal views

for all appropriate marginals (e.g., a_1, a_2, a_3, $a_1 a_2$, $a_1 a_3$, etc.) **do**
    Add equality of marginals to $\mathcal{C}$
end for

▷ Define objective function

Initialize `objective` $\leftarrow 0$
for all $s \in \mathcal{S},\ b \in \{0,1\}$ **do**
    for all $a_1 \in \mathcal{S}$ **do**
        $t \leftarrow \mathtt{XOR}(a_1, s \cdot b)$
        for all $a_2 \in \mathcal{S}$ **do**
            $a_3 \leftarrow t \oplus a_2$
            Add $P(a_1, a_2, a_3, a_2, s, b, b, b, 0)$ to objective
            Add $P(a_1, a_2, a_3, a_3, s, b, b, b, 1)$ to objective
        end for
    end for
end for
Solve the LP: max `objective` subject to constraints $\mathcal{C}$
Output: Optimal value of LP and whether binding is broken

Conclusion & Future work

Conclusion

- Generalization of impossibility of useful no-signaling-secure bit commitment to 3 provers case.
- Experimentation and negative results on 4 provers case.

Future work

- Conjecture : Impossibility of useful no-signaling-secure bit commitment.

References I

[Ben+88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. "Multi-prover interactive proofs: how to remove intractability assumptions". In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. STOC '88. Chicago, Illinois, USA: Association for Computing Machinery, 1988, pp. 113–131. ISBN: 0897912640. DOI: 10.1145/62212.62223. URL: https://doi.org/10.1145/62212.62223.

[FF15] Serge Fehr and Max Fillinger. *Multi-Prover Commitments Against Non-Signaling Attacks*. Cryptology ePrint Archive, Paper 2015/501. 2015. URL: https://eprint.iacr.org/2015/501.

References II

[LC98] Hoi-Kwong Lo and H.F. Chau. "Why quantum bit commitment and ideal quantum coin tossing are impossible". In: *Physica D: Nonlinear Phenomena* 120.1 (1998). Proceedings of the Fourth Workshop on Physics and Consumption, pp. 177–187. ISSN: 0167-2789. DOI: https://doi.org/10.1016/S0167-2789(98)00053-0. URL: https://www.sciencedirect.com/science/article/pii/S0167278998000530.

[May97] Dominic Mayers. "Unconditionally Secure Quantum Bit Commitment is Impossible". In: *Phys. Rev. Lett.* 78 (17 Apr. 1997), pp. 3414–3417. DOI: 10.1103/PhysRevLett.78.3414. URL: https://link.aps.org/doi/10.1103/PhysRevLett.78.3414.

Selective opening formally II

Asking $i \neq j$ reveals the value of b_i and b_j.

Selective opening formally II

Asking $i \neq j$ reveals the value of b_i and b_j.

$$S_2 = \{i : p_0(c, t_2|i) \neq p_1(c, t_2|i)$$

S_2 defines the set of indices on which $P2$ leaks information (resp. S_3 for $P3$).

Proposition

Selective opening implies either ($S_2 = \emptyset$ or $S_3 = \emptyset$) or $S_2 = S_3 = \{i_0\}$.

Experimental results I

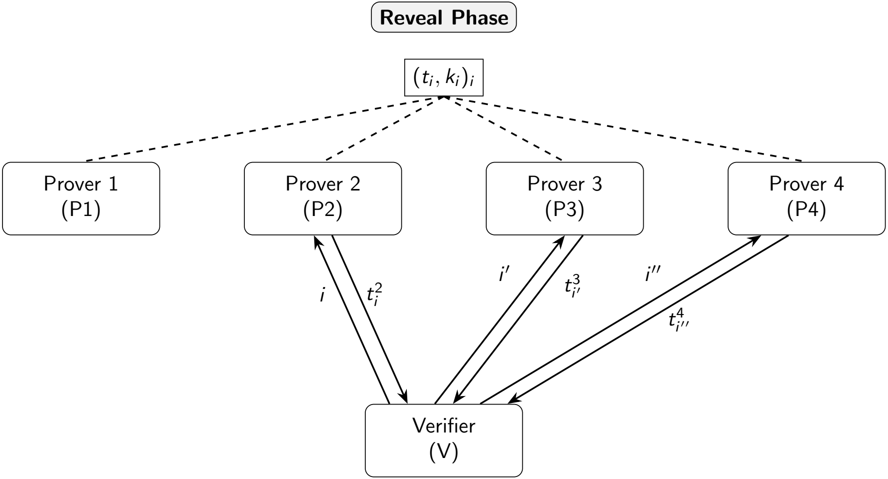


Figure: Reveal phase diagram using secret sharing

Experimental results II

- 4 or more provers schemes.
- Perfectly hiding, perfectly sound, selective opening.

All admitted a no-signaling strategy breaking binding with probability 1 !