commitments from PRSGs

pre-A

§1 Introduction

§1.1 Background

- Assume: A Sender wants to commit to sending a message m to a Receiver, at a later point.
  - The sender "encrypts" m & sends it.
  - At this later time, the sender sends a key to the receiver can open the message m.
- Properties:
  - Before the sender sends the key, the receiver shouldn't learn m. (hiding)
  - The sender shouldn't be able to change the message, once the sender commits to it. (binding)

Known: Both quantumly & classically, that both binding & hiding cannot be statistical.

Question: what is the weakest assump" needed to construct commitments?

A

Quantum Commitments & Signatures w/o One-way functions

Tomoyuki Morimae &
Takashi Yamakawa.

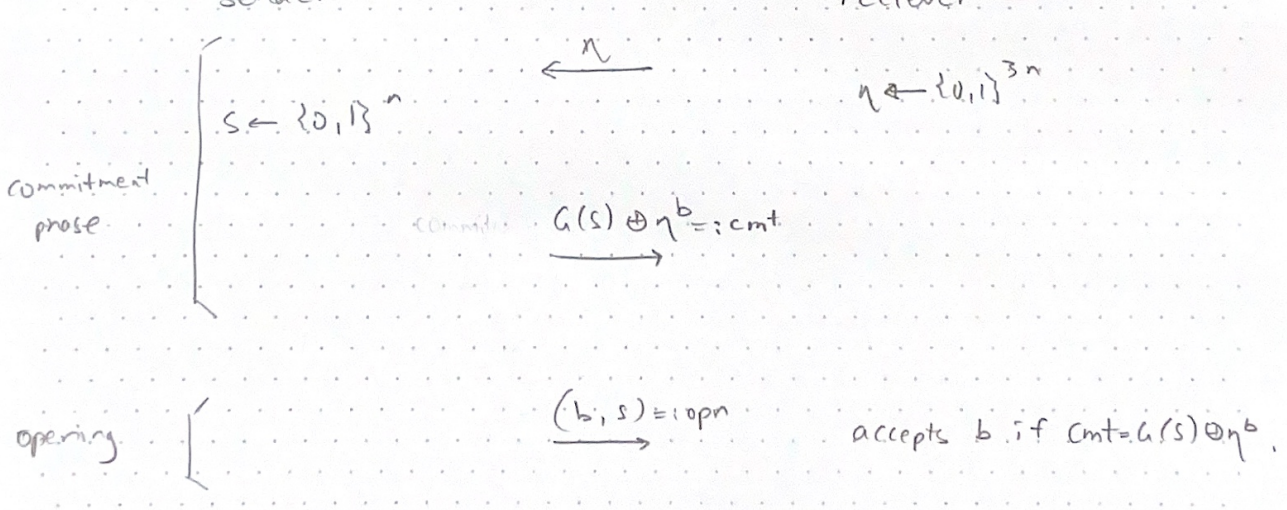
Me: Here, we only look at commitments – w/o the motivation etc.
[* See page 0 for an informal def^n of a commitment.]

§ 1.3 Technical Overview

Commitments

Story: • The basic idea is, in some sense, a quantum generalisation of the classical Naor's commitment scheme [Nao '91].

• We recall this scheme (uses $G: \{0,1\}^n \to \{0,1\}^{3n}$ a length tripling PRG)



Security Intuition:

Hiding: : The receiver doesn't know s,
(computational) the receiver cannot distinguish
$G(s)$ from $G(s) \oplus \eta$.

Binding: If both 0 & 1 can be opened,
(statistical) Then $\exists\ s_0, s_1$ s.t.
$G(s_0) \oplus G(s_1) = \eta$.
But there are at most 2^{2n} such η_{good}
(for a fixed G).
And since η is picked uniformly from $\{0,1\}^{3n}$,
the prob of such s_0, s_1 existing is
$\leq \frac{2^{2n}}{2^{3n}} = \frac{1}{2^n}$ i.e. negligible.

Idea behind their construction: (i) Replace $G(s)$ w/ a
pseudorandom state $|\phi_k\rangle$ &
(ii) replace addition of η^b w/
the quantum one-time pad.
(i.e. randomly apply X & Z).

Construction:

Sender

$|\psi_b\rangle := \frac{1}{\sqrt{2^{2m+n}}} \sum_{x,z \in \{0,1\}^m} \sum_{k \in \{0,1\}^n} |x,z,k\rangle_R \otimes P_{x,z}^b |\phi_k\rangle_C$

($|\phi_k\rangle$: pseudorandom state on m-qubits; register C →)

$P_{x,z} = \bigotimes_{j=1}^{m} X_j^{x_j} Z_j^{z_j}$

Receive

Commit phase

Me: opening ? suppose is sending register R.

NB: By the end of the "commit phase",

the receiver's state is $\rho_0 := \frac{1}{2^n} \sum_k |\phi_k\rangle\langle\phi_k|$ when $b=0$

&

$\rho_1 := \frac{1}{2^n} \frac{1}{4^m} \sum_k \sum_{x,\theta} P^b_{x,\theta} |\phi_k\rangle\langle\phi_k| P^b_{x,\theta}$

when $b=1$

Hiding: (computational) By the security of single-copy-secure PRSGs,

ρ_0 is computationally indistinguishable

from the m-qubit max. mixed state

$$\frac{\mathbb{1}^{\otimes m}}{2^m}.$$

: By the properties of the quantum one-time pad (Lemma 2.1),

$$\rho_1 = \frac{\mathbb{1}^{\otimes m}}{2^m},$$

Conclusion: Thus, ρ_0 & ρ_1 are computationally indistinguishable.

(which establishes hiding)

Statistical Sum-Binding:

Key claim: It suffices to show that the

fidelity b/w ρ_0 & ρ_1 is negligibly small

Story: To see ρ_0 & ρ_1 have negligible fidelity intuitively,

note that (i) $\rho_0 = \frac{1}{2^n} \sum_{k \in \{0,1\}^n} |\phi_k\rangle\langle\phi_k|$

has support in at most 2^n-dim space.

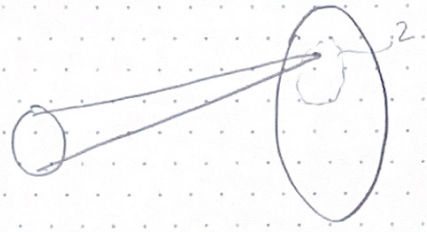
while

(ii) $\rho_1 = \frac{\mathbb{I}^{\otimes m}}{2^m}$ has support in the entire 2^n-dim space (since $m \geq cn$ with $c > 1$).

Thus, the "overlap" b/w ρ_0 & ρ_1 is small.

Rough

$\{0,1\}^n \to \{0,1\}^{3n}$



$G(s) \oplus \eta$

sent c

to convince 0,

$G(s_0) = c$

$s_1 = s$ $\quad G(s') = G(s) \oplus \eta$

$s_0 = s'$ $\quad s'$

to convince 1,

$G(s_1) = c \oplus \eta$ $\quad s_0 \neq s_1$ $\quad G(s_0) =$ ~~$G(s_0)$~~ ct

$G(s_0) \oplus G(s_1) = \eta$ $\quad s_1$ $\quad G(s_1) =$ ~~$G(s_1)$~~ $\oplus \eta$ (ct)

for