

Beacons

"Norwhal"

DRB:

n participants

random output

security properties

- unpredictable

- unbiased

- efficiency
 - few rounds
 - low bandwidth
 - low comp. costs

- no setup

Commit - reveal

Commit : p_i publish $C := \text{Commit}(r_i)$

Reveal : p_i pub. r_i

$$\Omega = \text{combine}(r_1, \dots, r_n)$$

Last-revealer can abort

Fixes

- incentives
- recovery mode (PVSS)

Optimistic Union

Commit-reveal w/ timed commit.

Commit: p_i publish $c_i = \text{Timed Commit}(r_i)$

Reveal: p_i publishes r_i
 $\Omega = \text{Combine}(r_1, \dots, r_n)$

Recover: recover $r_i = \text{Force Open}(c_i)$

$\Omega = \dots$

Naor (insecure)

One-time setup:

$G \leftarrow \text{Gen Group}()$

// trusted?

$g \leftarrow G$
 (2^t)

$h \leftarrow g$

Commit: p_i sample α_i

$C_i \leftarrow g^{\alpha_i}$

p_i publishes C_i

Reveal: p_i reveals $\tilde{\alpha}_i$

Verify $\forall i: C_i = g^{\tilde{\alpha}_i}$

$\Sigma = \prod h^{\tilde{\alpha}_i}$

Naor (insecure)

One-time setup:

$$G \leftarrow \text{Gen Group}()$$

// trusted?

$$g \xleftarrow{\$} G$$

$$h \leftarrow g^{(2^t)}$$

Commit: p_i sample α_i

$$c_i \leftarrow g^{\alpha_i}$$

p_i publishes c_i

Recover: $\Sigma = (\prod c_i)^{(2^t)}$

Attack

pre-compute $\Sigma_* = (w_*)^{(2^t)}$

$$\text{set } c_n = w_*^{-1} \left(\prod_{i < n} c_i \right)$$

Fixes

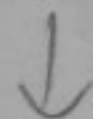
1) Narwhal - ZK

publish ZK PoK

for

$DL(c_i, g)$

BBF19



2) Narwhal - PC

Add precommitment round

$$d_i = H(c_i)$$

(3) Norwhal - RX

Reveal:

$$d = H(c_1 \parallel \dots \parallel c_n)$$

$$\Omega = \prod h^{\tilde{a}_i \cdot \#(c_i \parallel d)}$$

Norwalk-RX game (0)

c
Setup()

$G, g, h \rightarrow$

Adv

A_0

$\text{poly}(t, \lambda)$

$\downarrow$ advice

$c_1 \xleftarrow{\$} G$

$c_1 \rightarrow$

A_1

$c_2, \dots, c_n$

$\downarrow$ advice

$\text{RunTime}(A_1 + A_2) < t$

$b \xleftarrow{\$} \{0, 1\}$
 $H(A_1)$
 πc_i

$b = 0$

$b = 1$

$\tilde{\Omega} = \{ \xleftarrow{\$} G$

$\tilde{\Omega} \rightarrow$

A_2

$\downarrow$
 b'

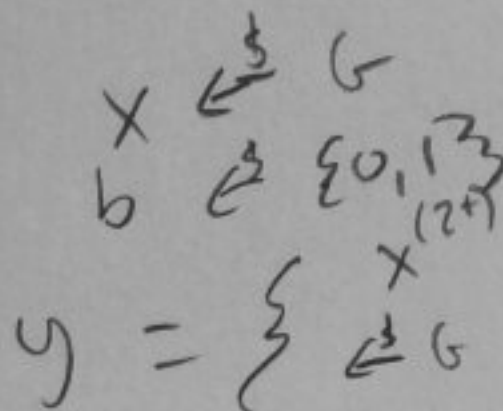
DRSW game



A_0

$\text{poly}(\lambda, t)$

advise



$b=0$

$b=1$



A_1

$< t$

b'

C DRSW

$$\underline{G} \rightarrow$$

Reduction

$$g \in G$$

$$h = g^{z^*}$$

A Normal

A₀

$$\underline{G, g, h} \rightarrow$$

GenElenc()

$$\underline{z_i = g^{r_i}}$$

$$\underline{C_i = X}$$

A₁

GenElenc

$$\underline{z_i = g^{r_i}}$$

$$C_i = \prod_j q_{i,j}$$

$$d = H(c_1 || \dots || c_n)$$

Simulate Ω computation
using $\tilde{y} = (c_1)$

A₂