Beacons "Narwhal"

DRB:

n participants

Ω random output

security properties

- unpredictable
- unbiasable
- efficiency
  - few rounds
  - low bandwidth
  - low comp. costs
- no setup

SWISSQUOTE

Commit - reveal

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

Reveal: p_i pub. r_i

$$\Omega = \mathrm{Combine}(r_1, \ldots r_n)$$

Last-revealer can abort

Fixes
- incentives
- recovery mode (PVSS)

Optimistic Unicorn

Commit-reveal w/ timed commitm.

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

Reveal: p_i publishes r_i

$\Omega = \text{Combine}(r_1, \ldots r_n)$

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

$\Omega = \ldots$

SWISSQUOTE

Narwhal (insecure)

One-time setup:

$G \leftarrow \mathrm{GenGroup}()$ // 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

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

Verify $\forall_i$ $c_i = g^{\tilde{\alpha}_i}$

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

Narwhal (insecure)

One-time setup:

$G \leftarrow \text{GenGroup}()$ // 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: $\Omega = (\prod c_i)^{(2^t)}$

Attack pre-compute $\Omega_* = (\omega_*)^{(2^t)}$

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

<u>Fixes</u>

BBF19

1) Narwhal - ZK

publish ZK PoK for $DL(c_i, g)$

2) Narwhal - PC

Add precomittment round

$$d_i = H(c_i)$$

(3) Narwhal -RX

Reveal:

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

$$\Omega = \prod h^{\hat{a}_i \cdot H(c_i \,||\, d)}$$

Narwhal-RX game (D)

C | Adv

$\text{Setup}() \xrightarrow{G,\, g,\, h} A_0$ $\quad$ poly(t, λ)

$A_0 \xrightarrow{\text{advice}} A_1$

$C_1 \xleftarrow{\$} G \xrightarrow{C_1} A_1$

$A_1 \xrightarrow{C_2, \ldots, C_n} C$

$A_1 \xrightarrow{\text{advice}} A_2$ $\quad$ Runtime$(A_1 + A_2) < t$

$b \xleftarrow{\$} \{0,1\}$

$$\tilde{\Omega} = \begin{cases} \prod C_i^{H(A|c_i)[2n]} & b = 0 \\ \xleftarrow{\$} G & b = 1 \end{cases} \xrightarrow{\tilde{\Omega}} A_2 \rightarrow b'$$

DRSW game

$C \xrightarrow{G} A_0$ $\quad$ $\text{poly}(\lambda, t)$

$A_0 \xrightarrow{\text{advice}} A_1$

$x \xleftarrow{\$} G$

$b \xleftarrow{\$} \{0,1\}$

$$y = \begin{cases} x^{(2^t)} & b=0 \\ \xleftarrow{\$} G & b=1 \end{cases} \xrightarrow{x,y} A_1 \quad < t$$

$A_1 \rightarrow b'$

C_{DRSW} | Reduction | A_{Normal}

$C_{DRSW} \xrightarrow{G}$ Reduction: $g \xleftarrow{\$} G$, $h = g^{z^*}$

Reduction $\xrightarrow{G,\, g,\, h}$ A_0

$\xleftarrow{\text{GenElem()}}$

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

$C_{DRSW} \xrightarrow{x,\, \tilde{y}}$ Reduction

Reduction $\xrightarrow{c_1 = x}$ A_1

$\xleftarrow{\text{GenElem}}$

$\xrightarrow{q_i = g^{r_i}}$

$e_{i,j}$

$\xleftarrow{c_i = \prod_j q_i}$

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

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

A_2