Ring Signature [RST01] @ Asiacrypt'01.

- KeyGen(1^n, n); Each member executes RSA.KeyGen(1^n).

  output $P_i = (n_i, e_i)$ and $S_i = (p_i, q_i, d_i)$.

- Sign(m, $\{P_i\}$, S_s); compute $k := H(m)$.

  choose $v \xleftarrow{\$} \{0,1\}^b$. and $x_i \xleftarrow{\$} \{0,1\}^b$ for $1 \le i \le r$, $i \neq s$.

  compute $y_i := g(x_i) = x_i^{e_i} \bmod n_i$.

  solve the equation $C_{k,v}(y_1, \cdots, y_s, \cdots, y_r) = v$ for y_s.

  compute $x_s := g_s^{-1}(y_s) = y_s^{d_s} \bmod n_s$.

  output $\sigma := (v, x_1, x_2, \cdots, x_r)$.

- Verify(m, σ, $\{P_i\}$); compute $y_i := g_i(x_i)$ for all i.

  $k := H(m)$

  compute $v' = C_{k,v}(y_1, \cdots, y_r)$.

  If $v' = v$, then output 1.

  otherwise, output 0.