其中一种：只需两方即可合谋恢复（半诚实）　　复原秘密？

① 让 $x = x_1 + x_2 + x_3$

A (x_1, x_2)

B (x_2, x_3) } 预先产生一随机数 r

C (x_3, x_1)

A与C本地计算 $x_1' = \frac{x_1}{2^d}$，则A与C都有 x_1'

B本地计算 $x_2' = \frac{x_2 + x_3}{2^d} - r$，并且将 x_2' 发给A

A (x_1', x_2')　B x_2'　C x_1'

B与C再本地计算 $x_3' = r$

A (x_1', x_2')　B (x_2', x_3')　C (x_1', x_3')

则 $x_1' + x_2' + x_3' = \frac{1}{2^d}(x_1 + x_2 + x_3)$

② 共享 $[r]$ 与 $[r'] = [\frac{r}{2^d}]$ ？

计算 $x' = [\frac{x}{2^d}]$

向所有人公开 $[x - r] = [x] - [r]$

每人都可获得 $x - r$ ⇒ 计算 $\frac{x-r}{2^d}$

再计算：$[x'] = [r'] + \frac{x-r}{2^d} = [\frac{r}{2^d}] + \frac{x-r}{2^d}$

截断流程：

A、B、C三方产生k位随机数r，每个参与者拿到r的share

记为 $[r]^B$，上标的B是r是按比特分享，令 $[r']$ 是 $[r]$ 从高位往低位数的前 $k-d$ 位 $r' = \frac{r}{2^d}$

又产生k位随机数 $[r_2]^B$、$[r_3]^B$ 与 $k-d$ 位随机数 $[r_2']^B$、$[r_3']^B$

r_2 与 $r_2' \longrightarrow A、B$

r_3 与 $r_3' \longrightarrow C、B$

用减法电路，每个参与者计算 $[r]^B = [r]^B - [r_2]^B - [r_3]^B$

$[r_1']^B = [r']^B - [r_2']^B - [r_3']^B$