安全多方计算--利用牛顿迭代法进行除法计算

牛顿迭代法迭代公式推演：

假设x，y的值分别为M与N，需要计算 x / y

$$x = N, y = M;$$

将除法形式变成相乘

$$\frac{x}{y} = x * \frac{1}{y} = N * \frac{1}{M}$$

如何得到1/M，当如下方程为0的时候解：

$$f(x) = \frac{1}{x} - M \quad (EQ.1)$$

在可导情况下有

$$f(x_1) = f(x_0) + f'(x_0)(x_1 - x_0)$$

令

$$f(x_1) = 0$$

则有

$$0 = f(x_0) + f'(x_0)(x_1 - x_0)$$

得到牛顿迭代公式：

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)} \quad (EQ.2)$$

将EQ.1代入到EQ.2得到迭代公式：

$$x_1 = x_0 - \frac{\frac{1}{x_0} - M}{(\frac{1}{x_0} - M)'}$$

$$x_1 = x_0 - \frac{\frac{1}{x_0} - M}{-\frac{1}{x_0^2}}$$

$$x_1 = x_0 + x_0 * (1 - M * x_0)$$

$$x_1 = x_0 * (2 - M * x_0)$$

使用牛顿迭代法计算除法

将M变成D*2^e (1 <= D < 2), 就是标准的浮点数表示。

$$M' := M/2^{e+1}$$

$$N' := N/2^{e+1}$$

$$x_0 = 48/17 - 32/17 * M'$$

迭代公式：

$$x_1 = x_0 * (2 - M * x_0)$$

计算:

$$\frac{N}{M} = N' * x$$

接口定义:

```
//计算a/b；p为精度可取2，4，8，16
share* newtonMethodDiv(share *s_a, share *s_b, uint8_t P, BooleanCircuit *bc){

}
```