安全多方计算--高精度指数函数计算

协议介绍：

在安全计算电路中计算e^x

在二进制下利用指数基底精确表示指数函数，基于布尔共享进行高效指数计算。

协议内容：

1. 初始化二进制基底

$$B_0 = e^{2^0}, B_1 = e^{2^1}, B_2 = e^{2^2}, B_3 = e^{2^3}, B_4 = e^{2^4}, \ldots, B_i = e^{2^i}$$

2. 把x换算成二进制：

$$x = a_0 * 2^0 + a_1 * 2^1 + a_2 * 2^2 + \ldots + a_n * 2^n$$

3. 计算：

$$e^x = B_0^{a_0} B_1^{a_1} \ldots B_n^{a_n}$$

e.g.

$$23 = 1 + 1 * 2 + 1 * 2^2 + 0 * 2^3 + 1 * 2^4 \quad 23 = (10111)_B$$
$$\text{则}：e^{23} = B_0^1 B_1^1 B_2^1 B_3^0 B_4^1$$

接口定义：

```
share* binaryExponentCircuit(share *s_x1, uint32_t bitlen, BooleanCircuit *bc){

}
```