No.

Date. / /

E7.1

已知消息攻击的存在性伪造：

若敌手向 Alice 发送两条消息 x_1，x_2 让其签名

则可得到 $y_1 = x_1^{2a} \pmod n$，$y_2 = x_2^{2a} \pmod n$

∴ 敌手可算出 $x = x_1 \cdot x_2$ 的签名 $y = y_1 \cdot y_2 = (x_1 \cdot x_2)^{2a} \pmod n$