**Завдання 3: зламати ECDSA**

Вам наданий документ, що підписаний вразливою бібліотекою підпису ECDSA на основі кривих Едвардса: <https://github.com/juja256/EdwardsCurves>

Вам потрібно проаналізувати бібліотеку, знайти вразливість та за допомогою неї відновити закритий ключ, який використовувався для підпису цього документу. Геш-значення sha3-256 від документу наступне:

h=0x5433A582070AF8FBAFDF65B5310CA99164F4F3DE016194163B239412F778A16B

Документ був підписаний публічним ключем:

Qx=0x2B2833FB68299DF82A4342B46FAB03600DD3B3C657F02FAA48B7499609EE387E Qy=0x0089F9E049AB4F819950243F70F640071015CB8C819CBA43BFF4A517F8D75D26

Отриманий підпис σ = (r,s) наступний:

r=0x03ED92681510AC291C473A58ECEEE7AD4C181CEB781BF8FAEADEE47FDE4C5E48 s=0x048BCD9074A0BEA08A601089017700219A2C577E6ABF32364FEBE3A6CEEA6EC8