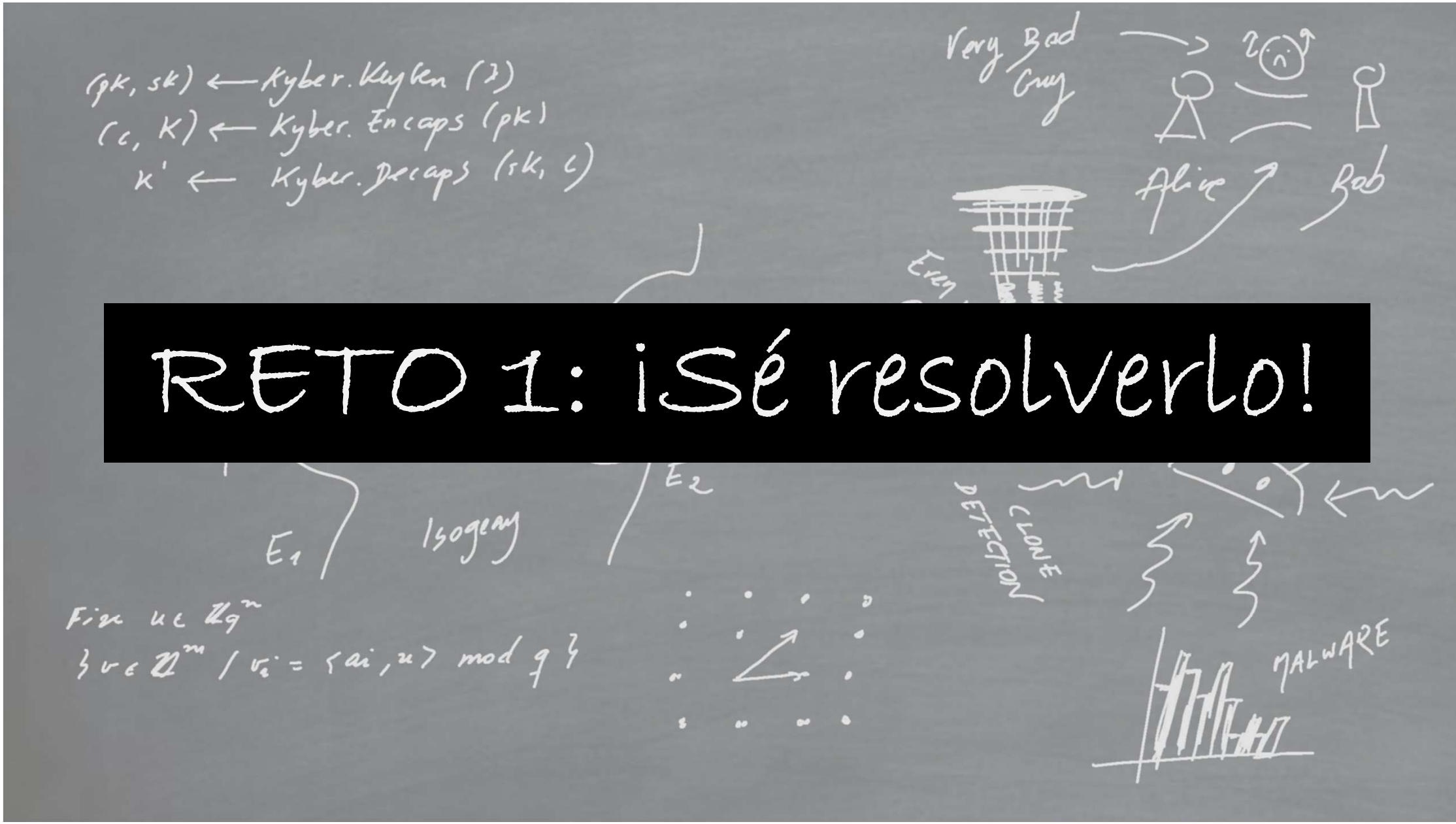

(pk, sk) ← Kyber.KeyGen ()
(c, K) ← Kyber.Encaps (pk)
K' ← Kyber.Decaps (sk, c)
Very Bad Guy
Alice
Bob
RETO 1: ¡Sé resolverlo!
E1
Isogeny
E2
CLONE DETECTION
MALWARE

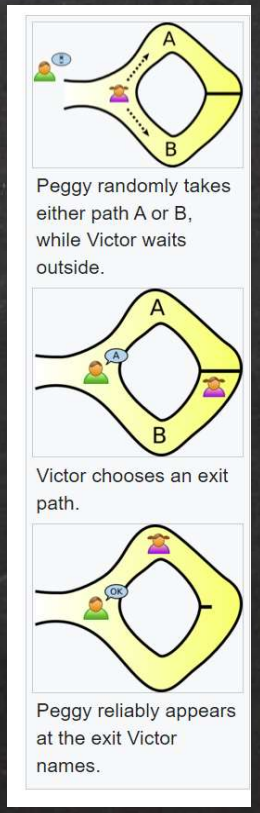
RETO 1: ¡Sé resolverlo!

NOCIÓN DE CONOCIMIENTO CERO (ZERO KNOWLEDGE)

- Una entidad (Prover) convence a otra (verifier) de la veracidad de un postulado P, sin revelar más que el hecho de que P es TRUE.
- Una ZKP puede ser interactiva o no interactiva
- Sus propiedades deseables son tres:
  - **Completeness**: si P es verdad, el Prover puede convencer al Verifier
  - **Soundness**: si P no es verdad, el Prover solo convence al verifier con probabilidad muy pequeña
  - **Zero-knowledge**: lo único que aprende el Verifier es el valor de verdad de P

La cueva de Alí Babá

[Quisquater, Jean-Jacques; Guillou, Louis C.; Berson, Thomas A. (1990). "How to Explain Zero-Knowledge Protocols to Your Children". Advances in Cryptology — CRYPTO' 89 Proceedings doi:10.1007/0-387-34805-0_60. ISBN 978-0-387-97317-3].



[Imagen e historia completa en Wikipedia]

El Reto:

Existen varias propuestas para demostrar en ZK que se conoce la solución a un juego o acertijo (¡busca referencias en nuestra web!)

¿Se te ocurre alguna idea para demostrar en conocimiento cero que conoces la solución a un problema o acertijo diferente? Puede ser un tipo concreto de crucigrama, un tablero de ajedrez para el que se persigue una solución con un número fijo de movimientos o incluso una sopa de letras...

Enviar ideas y propuestas a mariaisabel.gonzalez@uc3m.es con el asunto "CryptoClub - RETO 1"