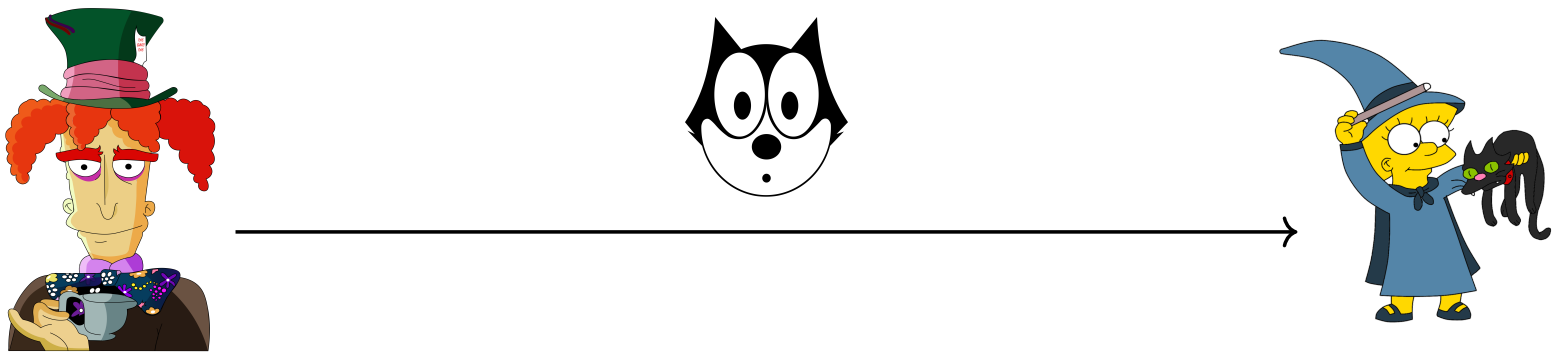
My thesis topic explained in 10 slides?

Jesús-Javier Chi-Domínguez [1]

[1]Computer Science Department, Cinvestav - IPN, Mexico City, Mexico

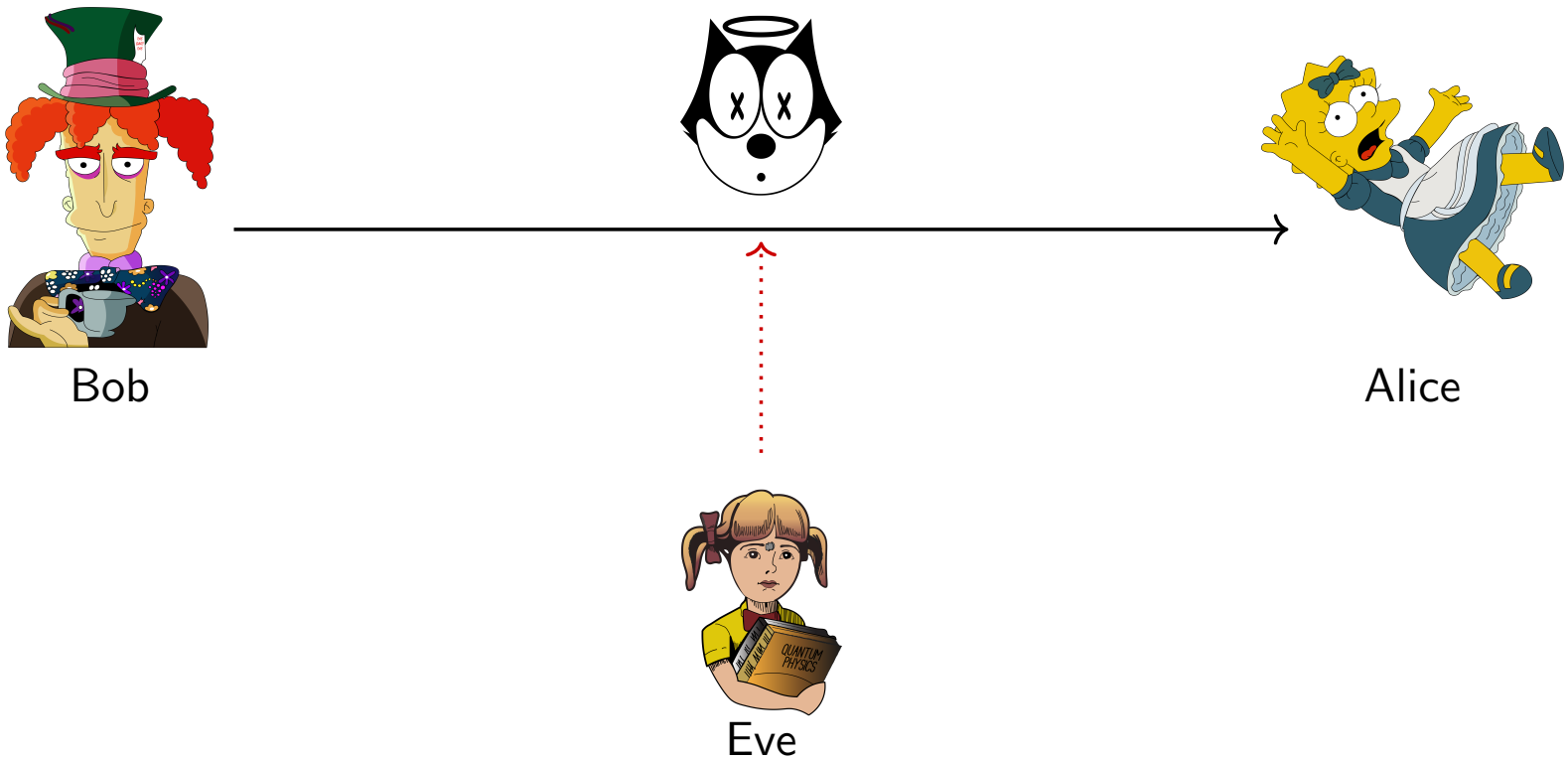
November 13, 2019

Basic communication scheme



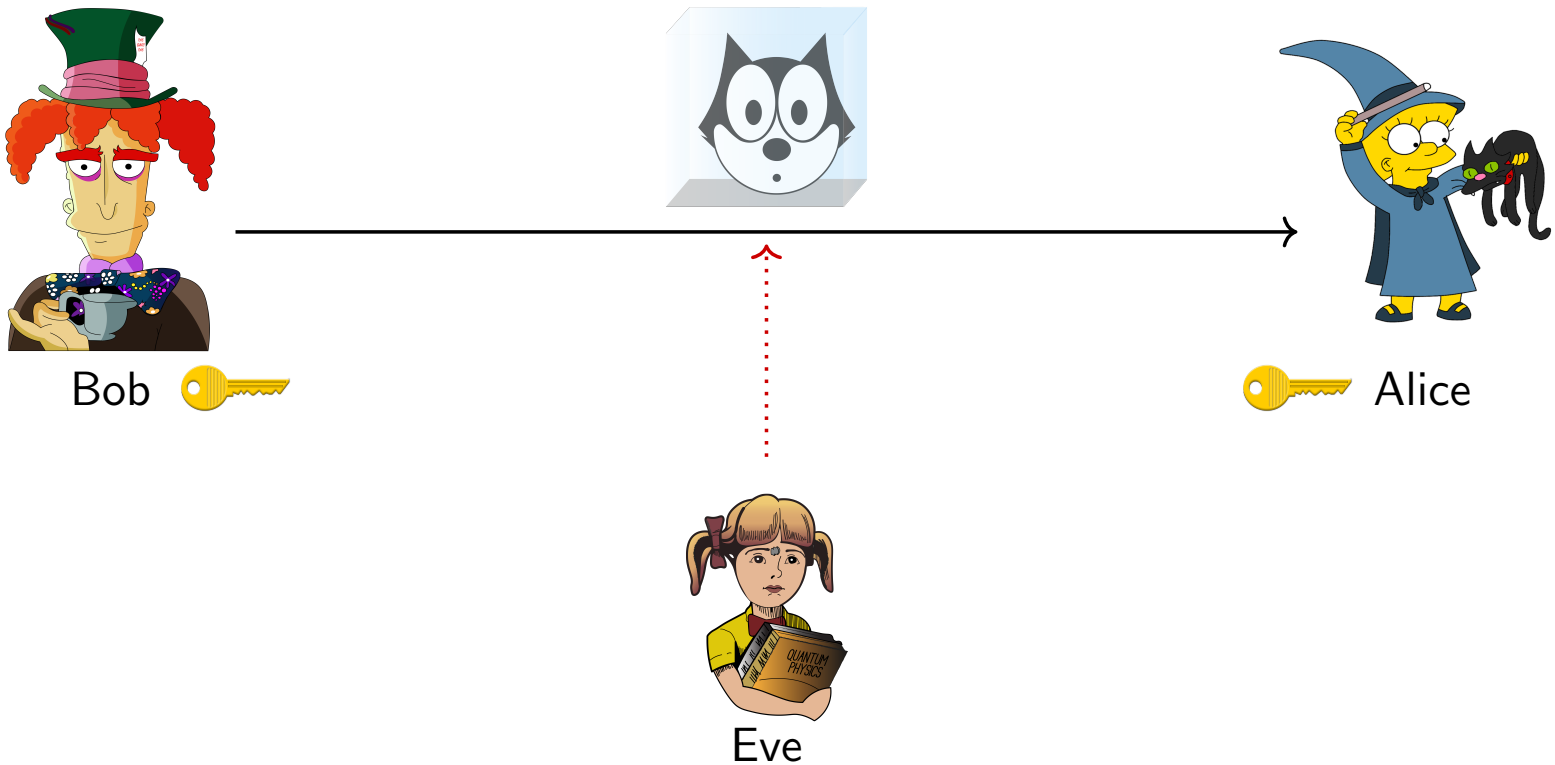
Basic communication scheme

There are not secure channels.



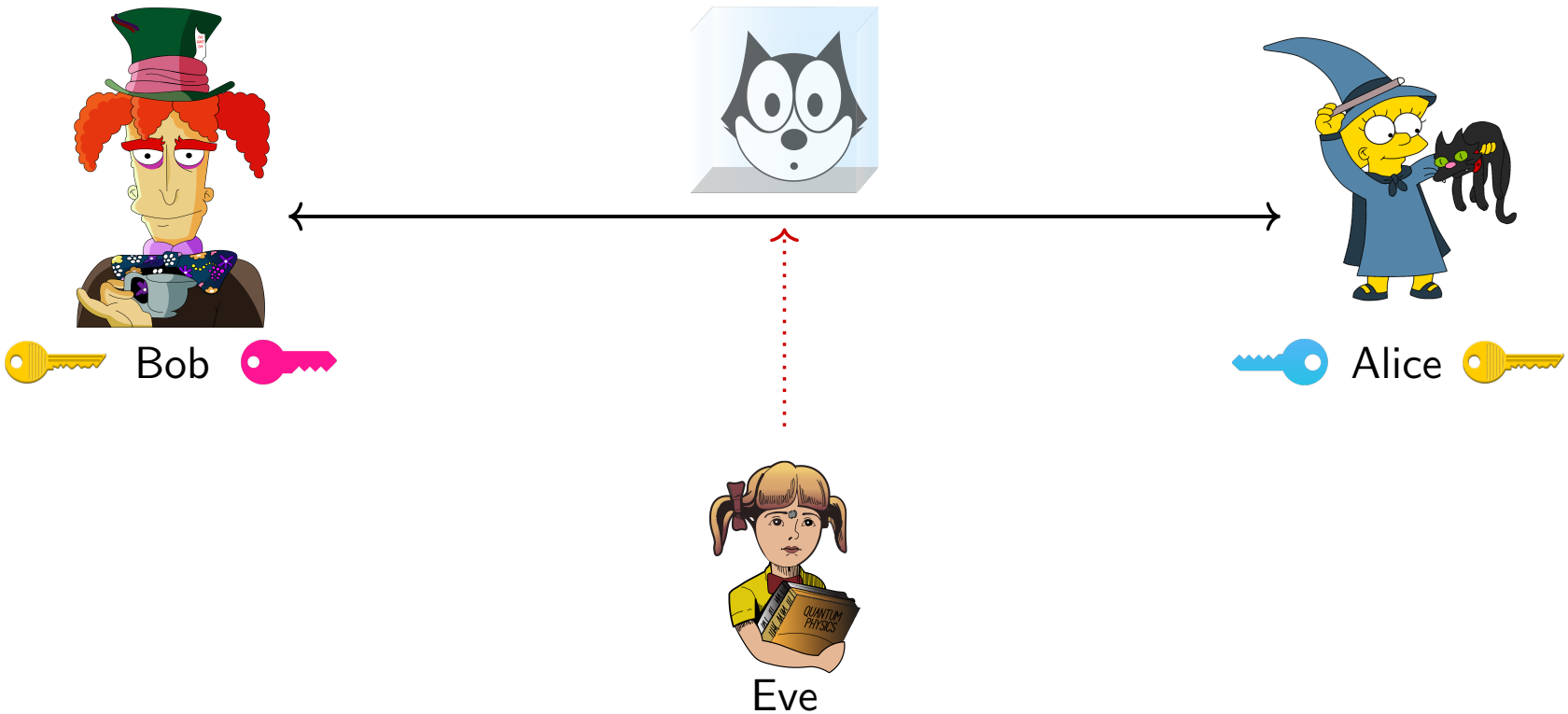
Basic communication scheme

There are not secure channels. Thereby the need of using Cryptography (i.e., to encrypt messages).



Current public-key cryptography

Security based on hard computational problems like *Integer Factorization (IFP)* and *Discrete Logarithm (DLP)*



Quantum computing risks current crypto!

Figure 1: *... y'know, eight-year-old white girl, middle of the ghetto, bunch of monsters, this time of night with quantum physics books? ... those books are WAY too advanced for her. If you ask me, I'd say she's up to something...* - James Edwards from MIB film (1997).

Quantum computing risks current crypto?

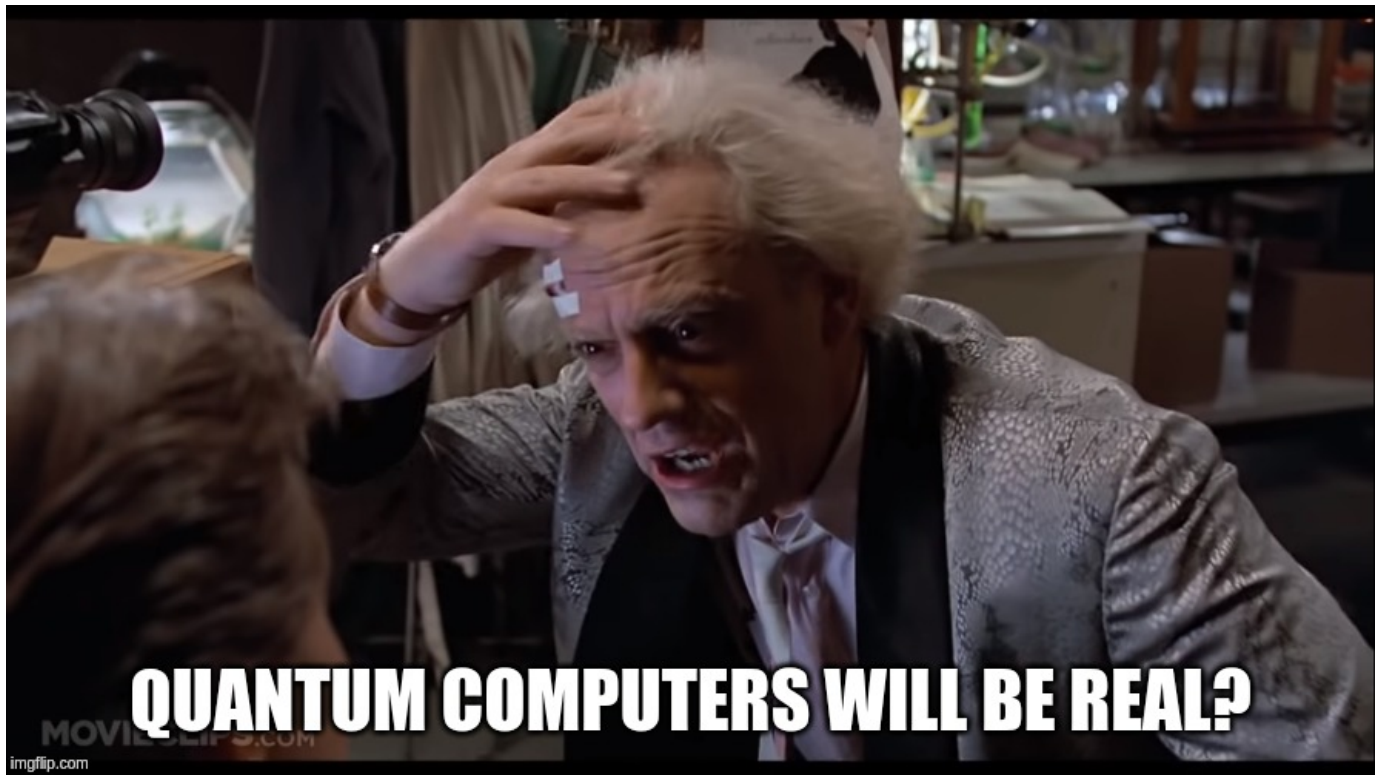
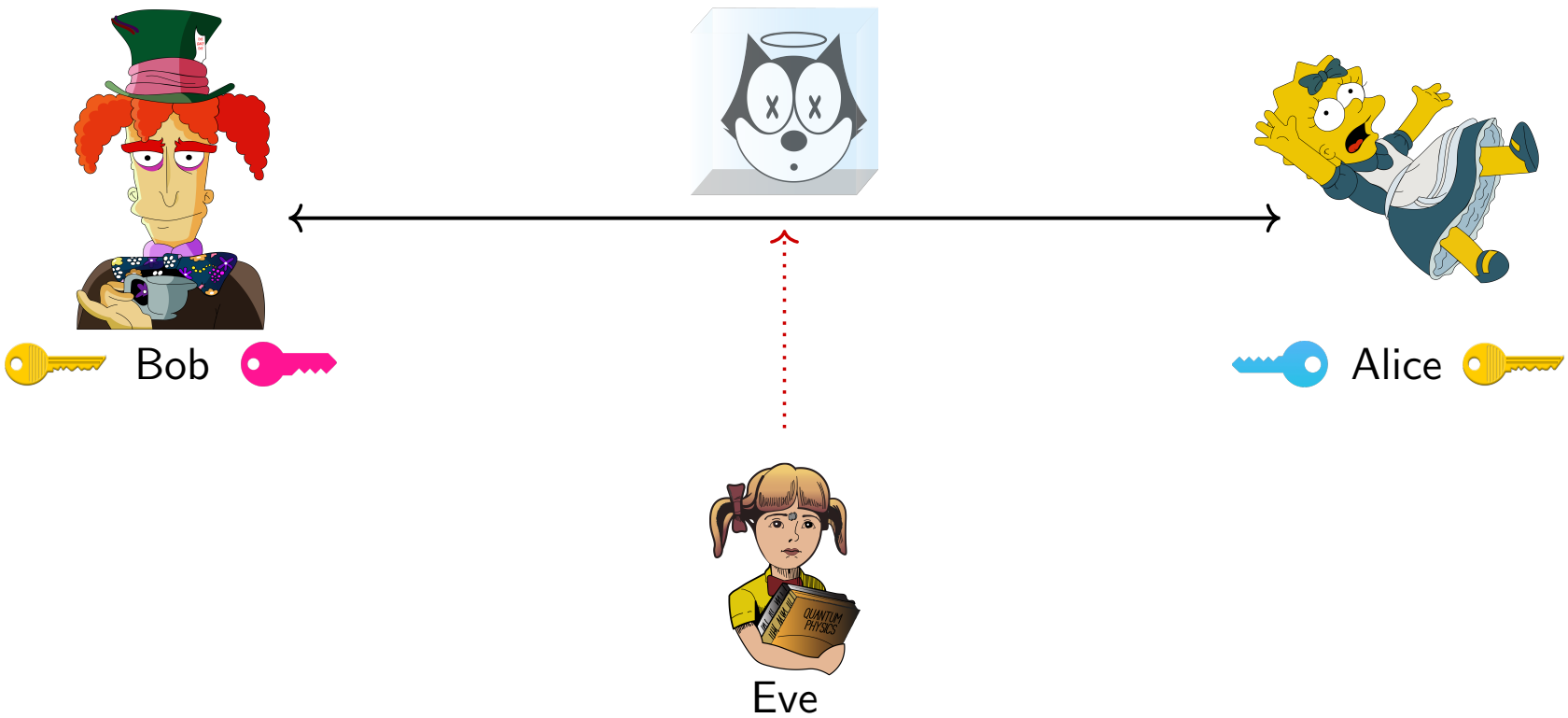


Figure 2: Original picture was taken from Back to the future film (1985).

Quantum computing risks current crypto!

The Shor's quantum algorithm allows to solve the IFP and DLP with a polynomial running-time complexity, and the global giants such as Intel, Google, IBM, Rigetti, and Microsoft are investing heavily in the development of quantum computers.

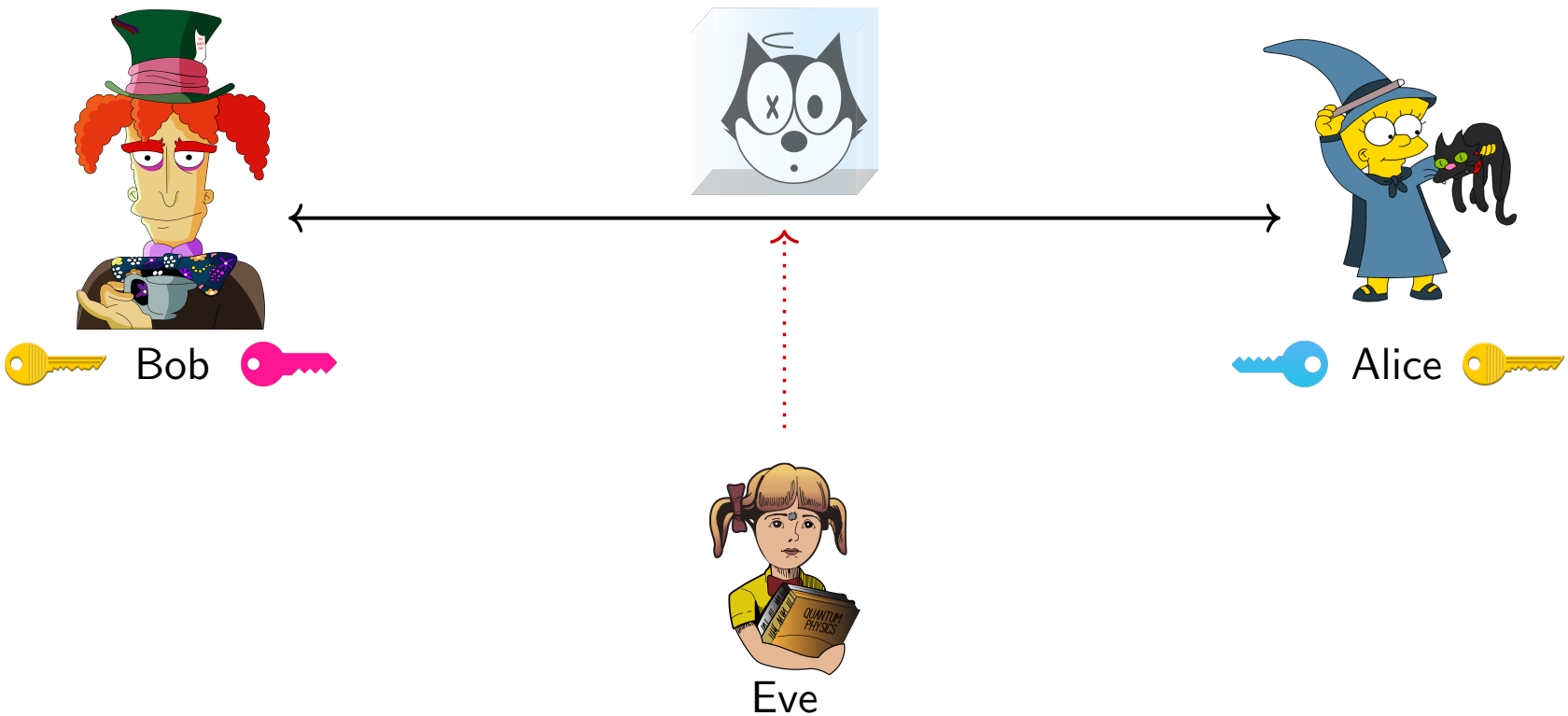


Quantum computing risks current crypto?

Figure 3: Original pictures were taken from White chicks film (2004).

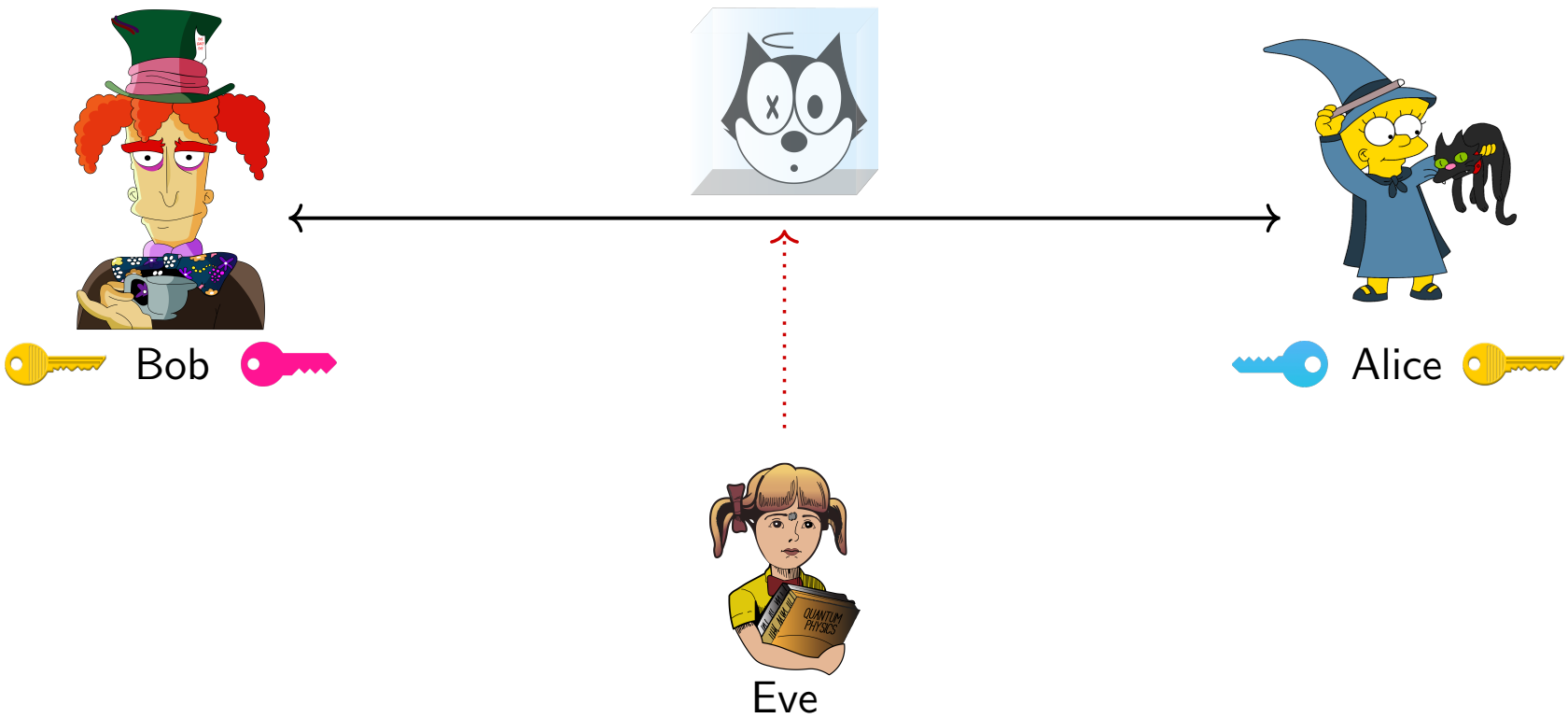
Quantum-safe cryptography

The U.S. government's National Institute of Standards and Technology (NIST) is asking for inclusion in a forthcoming standard for quantum-safe cryptography, which are based on codes, lattices, multivariate-quadratic, hash, and isogenies .



Quantum-safe cryptography

The U.S. government's National Institute of Standards and Technology (NIST) is asking for inclusion in a forthcoming standard for quantum-safe cryptography, which are based on codes, lattices, multivariate-quadratic, hash, and isogenies... wait! elliptic curves?.



Quantum-safe cryptography

Figure 4: Original pictures were taken from White chicks film (2004).

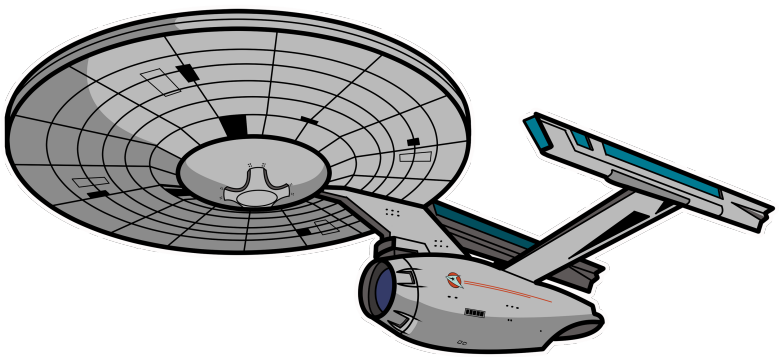
Elliptic curves and isogenies: *metaphoric idea*

Elliptic-curve based crypto: moving from cities to cities.

Isogeny-based crypto: moving from planets to planets

Intuitively, isogeny-based crypto is much slower and costly than elliptic-curve based crypto but it is quantum-resistance.

Elliptic curves and isogenies: *metaphoric idea*



Enterprise ship from *Star Trek* series (1966).

Isogeny-based crypto: moving from planets to planets

We are focusing on improvements for isogeny-based crypto.

Thank you for your attention

Figure 5: Original picture was taken from Back to the future film (1985).

I look forward to your comments and questions.

e-mail: jjchi@computacion.cs.cinvestav.mx