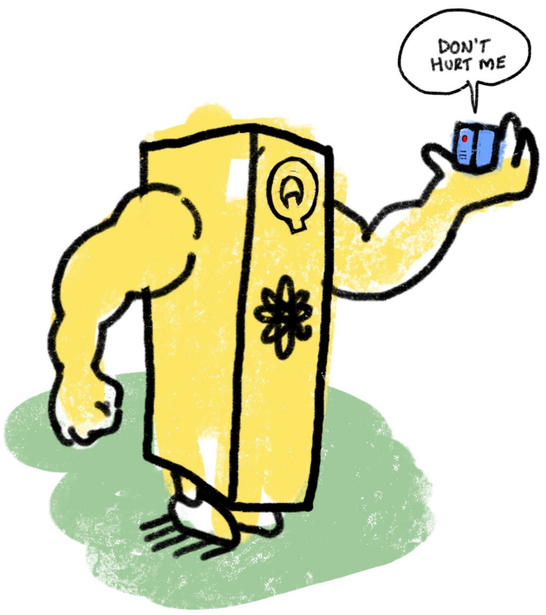
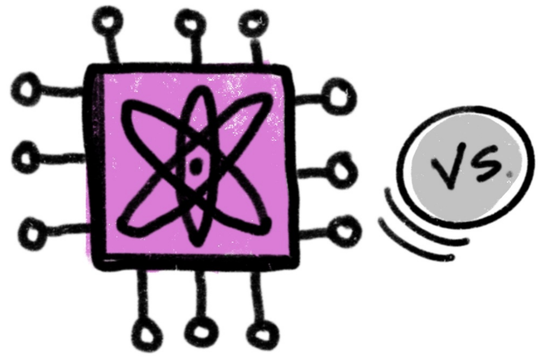
# IMPLEMENTING QUANTUM-RESISTANT CRYPTOGRAPHY IN INDUSTRY

SAMUEL SABOGAL PARDO




"HARVEST NOW, DECRYT LATER" IS A SERIOUS ATTACK.

INFORMATION CAN HAVE VALUE FOR DECADES!

OBFUSCATION CAN BE REVERSED

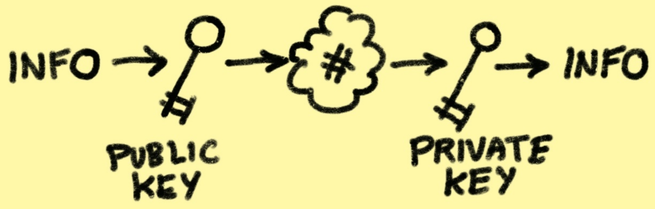
SHOULD WE BE OPTOMISTC OR PESSIMISTIC ABOUT THE POSSIBILITIES OF QUANTUM COMPUTING

QUANTUM TECH IS GETTING NEAR THE POINT WHERE RSA-2048 CAN BE BROKEN (372 Q-Bits)

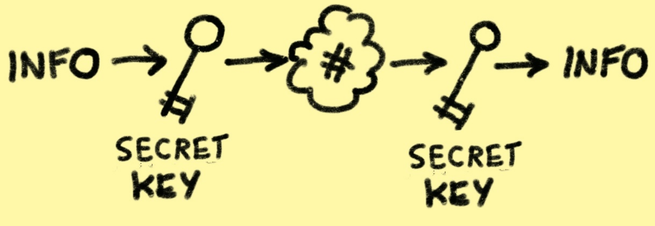
"IN CYBERSECURITY WE ARE NOT OPTIMISTIC OR PESSIMISTIC, WE ARE ALL PARANOID!"

CURRENT ENCRYPTION TECHNIQUES CAN BE ENHANCED BY WRAPPING OLD WEAK ENCRYPTION CONTENT

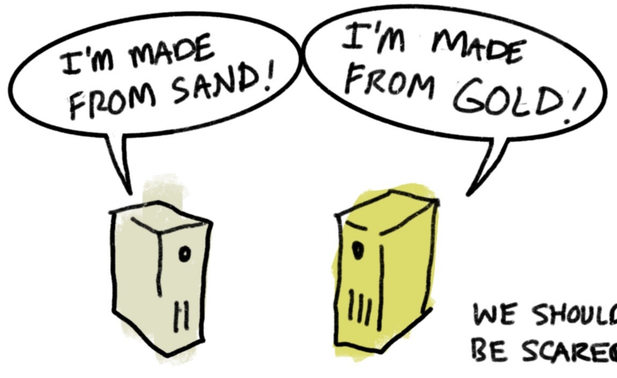

## ASYMMETRIC CRYPTO




## SYMMETRIC CRYPTO




DIFFERENT PHYSICAL PROPERTIES ALLOW QUANTUM COMPUTERS TO HAVE DIFFERENT KINDS OF ALGORITHMS




WE SHOULD BE SCARED.

QUANTUM ALGORITHM