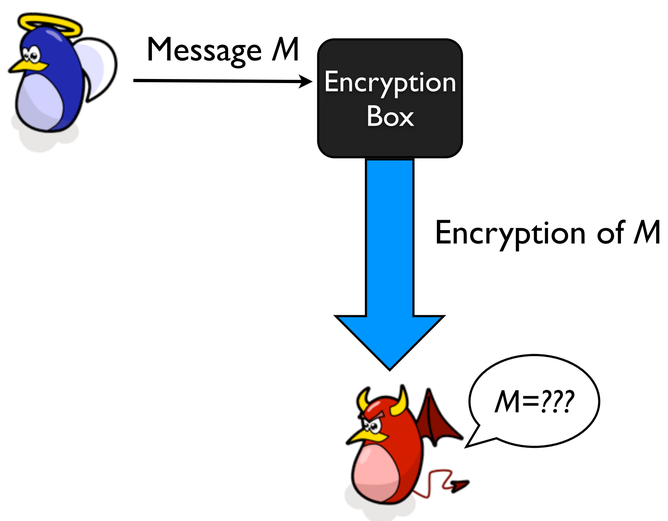
Side-Channel Resilient Cryptography

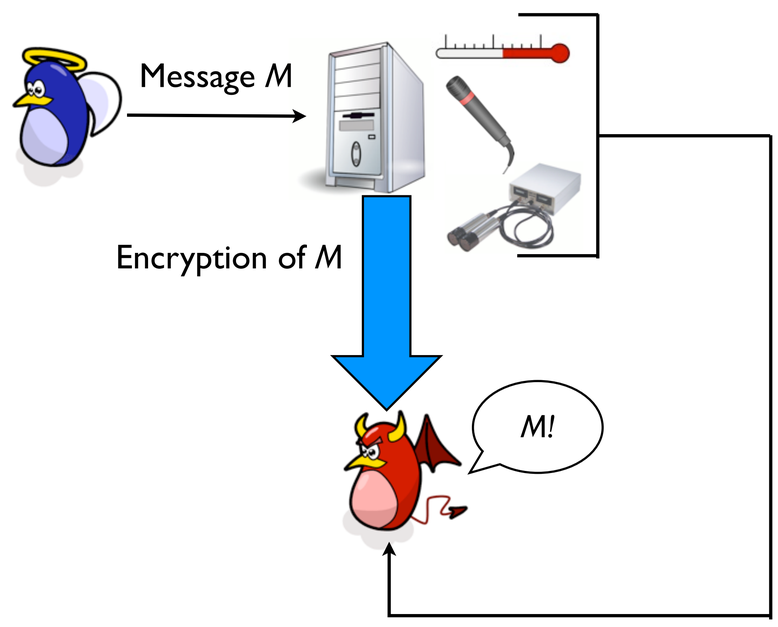
Side-channel attacks

Information about the internal state of a physical device can be gained by making various measurements, such as temperature, sound, power consumption, and radiation.

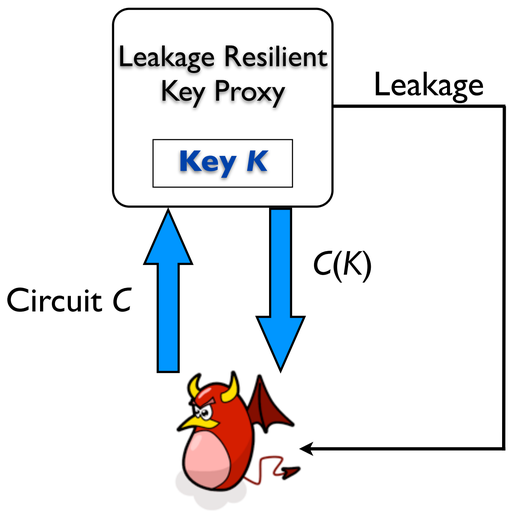
Crypto in theory



Crypto in reality

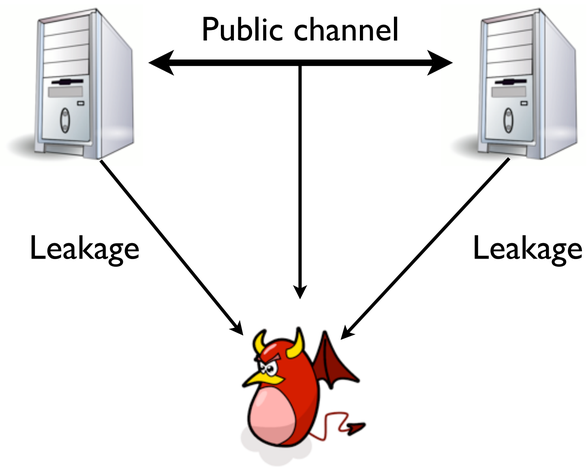


Our new primitive



The adversary gains no useful information about key K through information obtained by side-channel attacks. We refer to information obtained this way as "leakage".

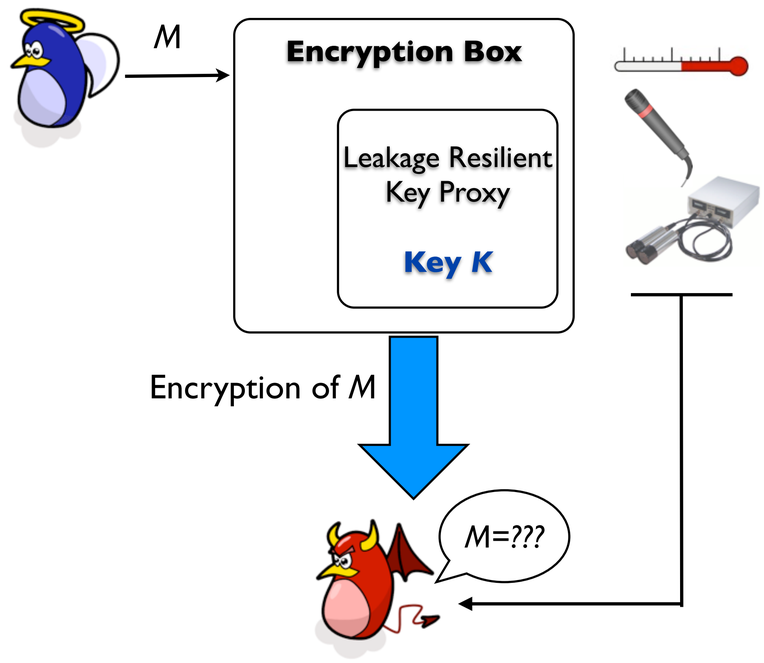
The hardware model



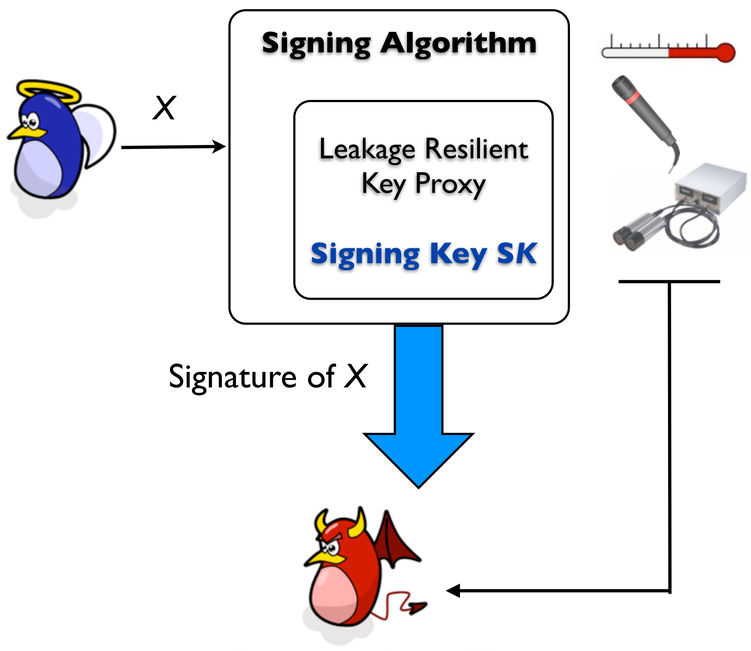
The model consists of two computers connected by a public channel (like the internet). The adversary is allowed to obtain leakage from both computers, which leak independently.

Applications

Private Key Encryption



Digital Signatures

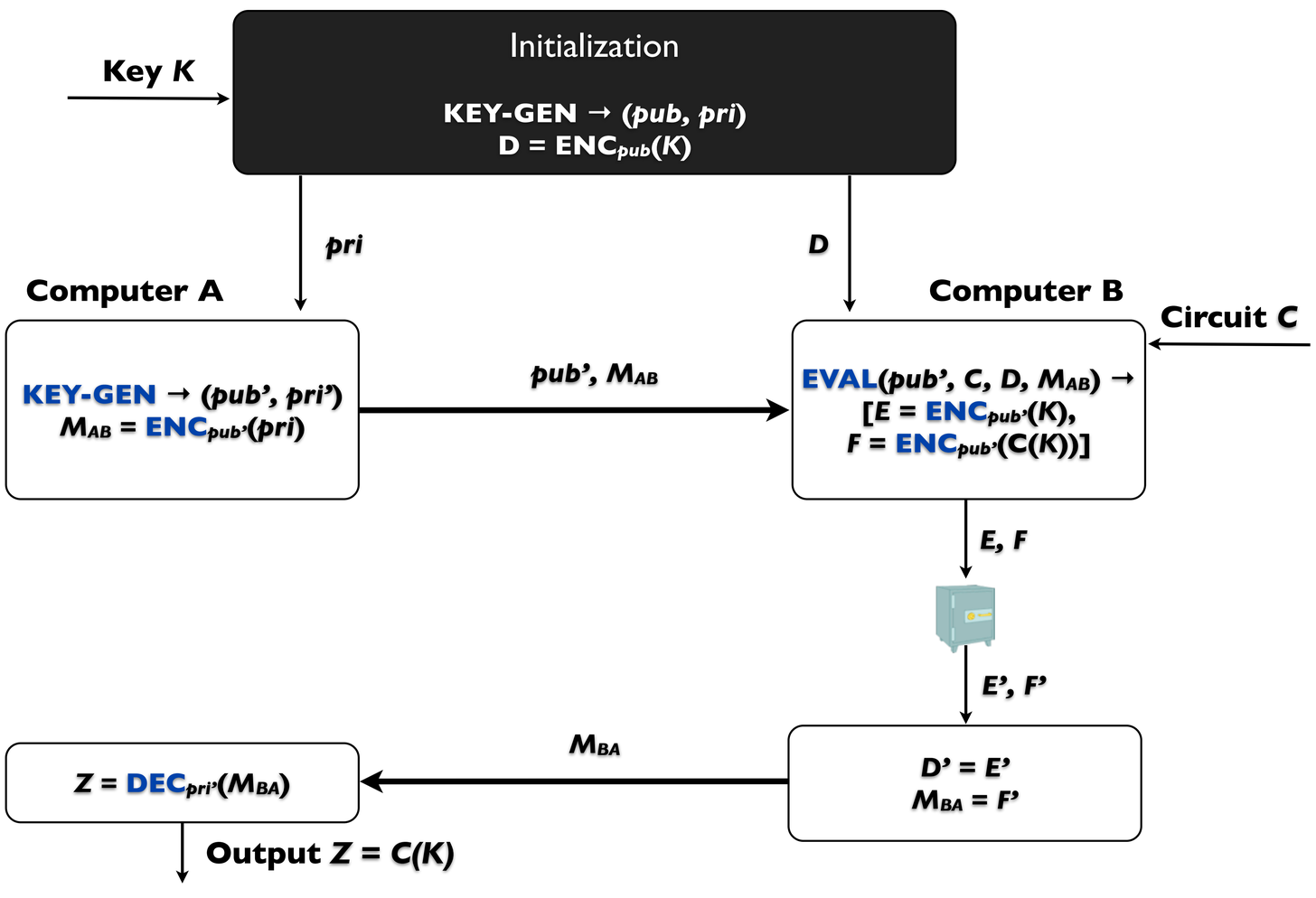


And More...

Our construction

Tools:

- Fully homomorphic public-key encryption scheme: KEY-GEN, ENC, DEC, EVAL
- Leakage-free re-randomizer



by Ali Juma and Yevgeniy Vahlis