ECCS-2029323: Exploiting Co-Existence for Verifiable Everlasting Security in Wireless Communications

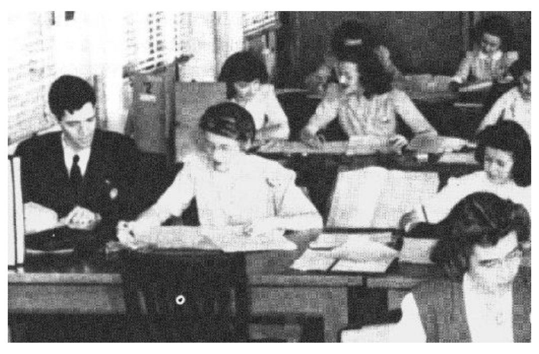
PI: Dennis Goeckel, Co-PI: Robert Jackson, PhD student: James Doty

University of Massachusetts Amherst

Motivation: Post-Quantum Secrecy

Everlasting secrecy

- We are interested in keeping something secret forever.
- A challenge of cryptography (e.g. the VENONA project) is that recorded messages can be deciphered later



How cryptography can be broken?

- If the cryptographic system is broken.
- If significant computational advances are made.
- If the eavesdropper somehow obtains the key.

The recorded message can be deciphered later

I. IT secrecy and its limitations

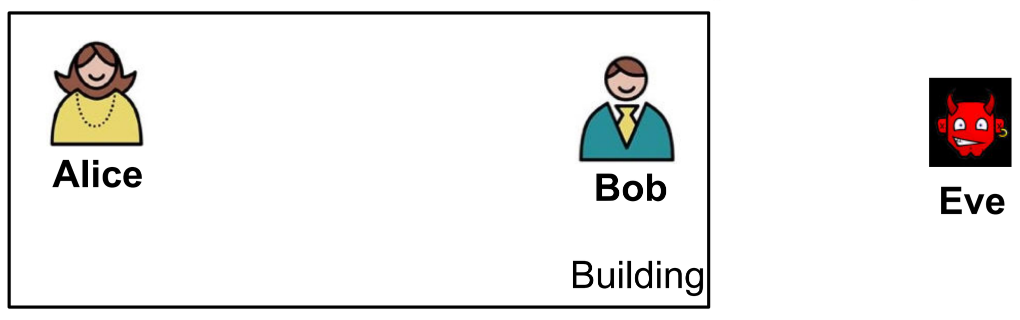
The Wiretap Channel [Wyner, 1975]

R_{AB}: Capacity of channel from Alice to Bob

R_{AE}: Capacity of channel from Alice to Eve

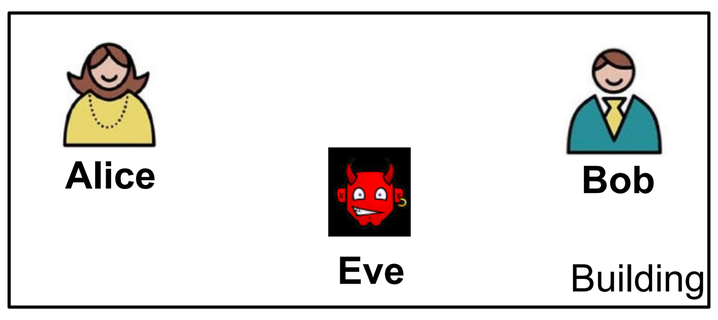
If $R_{AB} > R_{AE}$

Positive rate "if Bob's channel is better", and Eve gets <u>nothing</u>.



Gaussian channels: $$R = \log_2(1 + SNR_{AB}) - \log_2(1 + SNR_{AE})$$

<u>Important Challenge</u>: the "near Eve" problem…



Many would argue that we have traded a long-term computational risk (cryptography) for a short-term scenario (information-theoretic secrecy) risk…no, thank you!

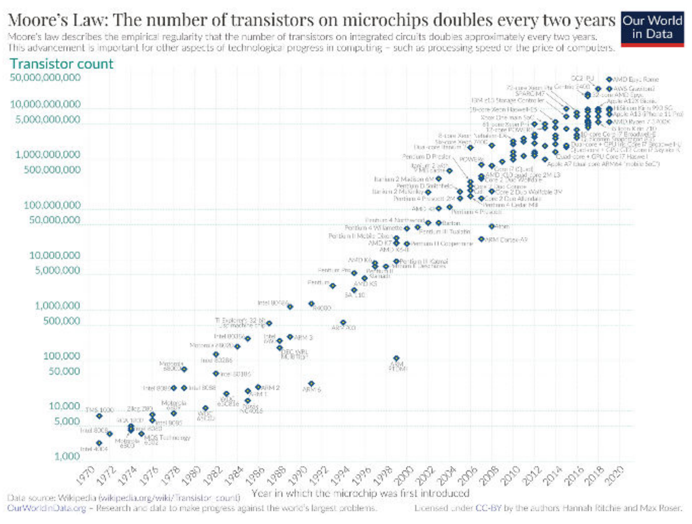
II. Attacking the hardware

Recall Goal: Keep Eve from *<u>recording</u>* a signal from which she can later extract the information.

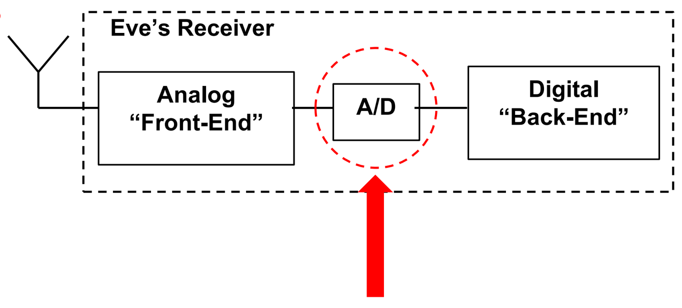
Bounded Memory Model [Cachin and Maurer, 1997]:

- Eve with memory<M cannot store enough to eventually break the cipher.
- However, it is hard to pick a memory size that Eve cannot use beyond.

1. The density of memories grows quickly (Moore's Law).
2. Memories can be stacked arbitrarily subject only to (very large) space limitations.

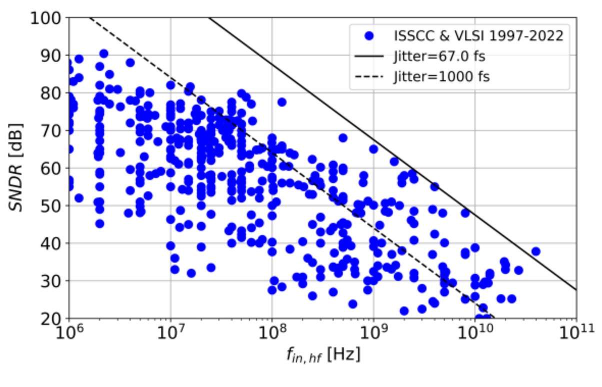


Perhaps Cachin and Maurer attacked the wrong part of the receiver.



Bounded Conversion Model

A/D aperture jitter has marginally improved since 2005

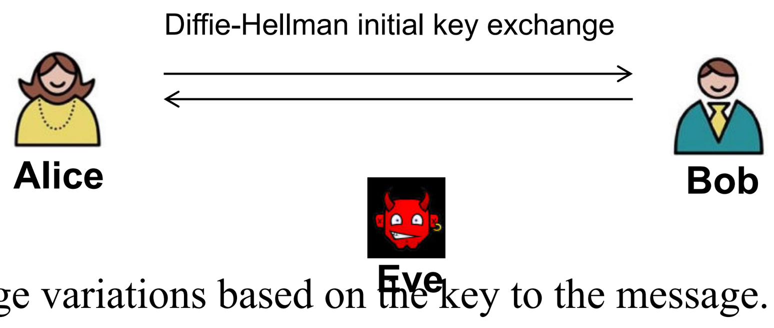


[From B. Murmann, "ADC performance survey 1997-2022"]

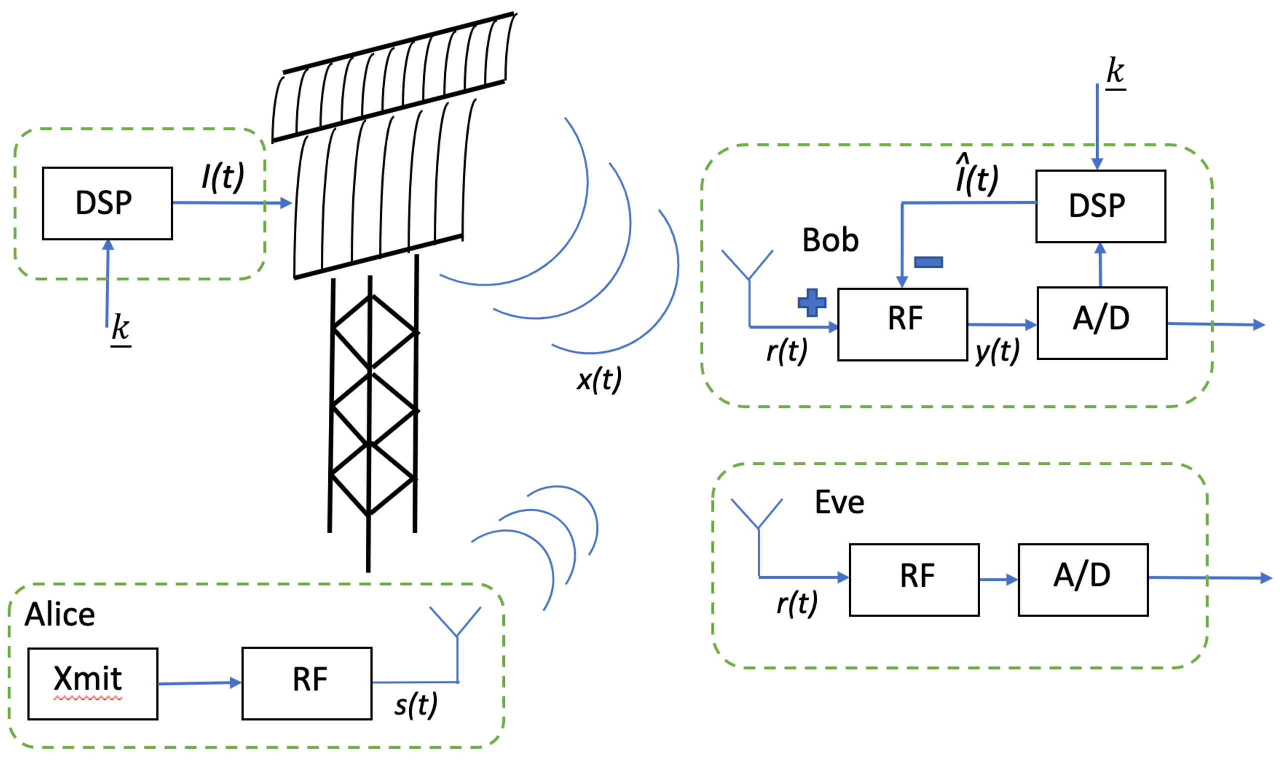
1. **In the combative sender-eavesdropper game, front-end dynamic range is a critical aspect of the receiver.**
2. A/D Technology progresses very slowly.
3. High-end A/D's are already stacked to the limit of the jitter.

III. Random jamming for secrecy

- Alice and Bob share a short "ephemeral" cryptographic key.
- By employing a cryptographic stream-cipher generation method, this initial key is used to obtain a long key sequence.



- Radar emits a random jamming signal with large variations based on the key to the message.
- Bob uses key to cancel the effect of jamming before A/D conversion.
- Eve has to wait to obtain the key after completion of transmission.



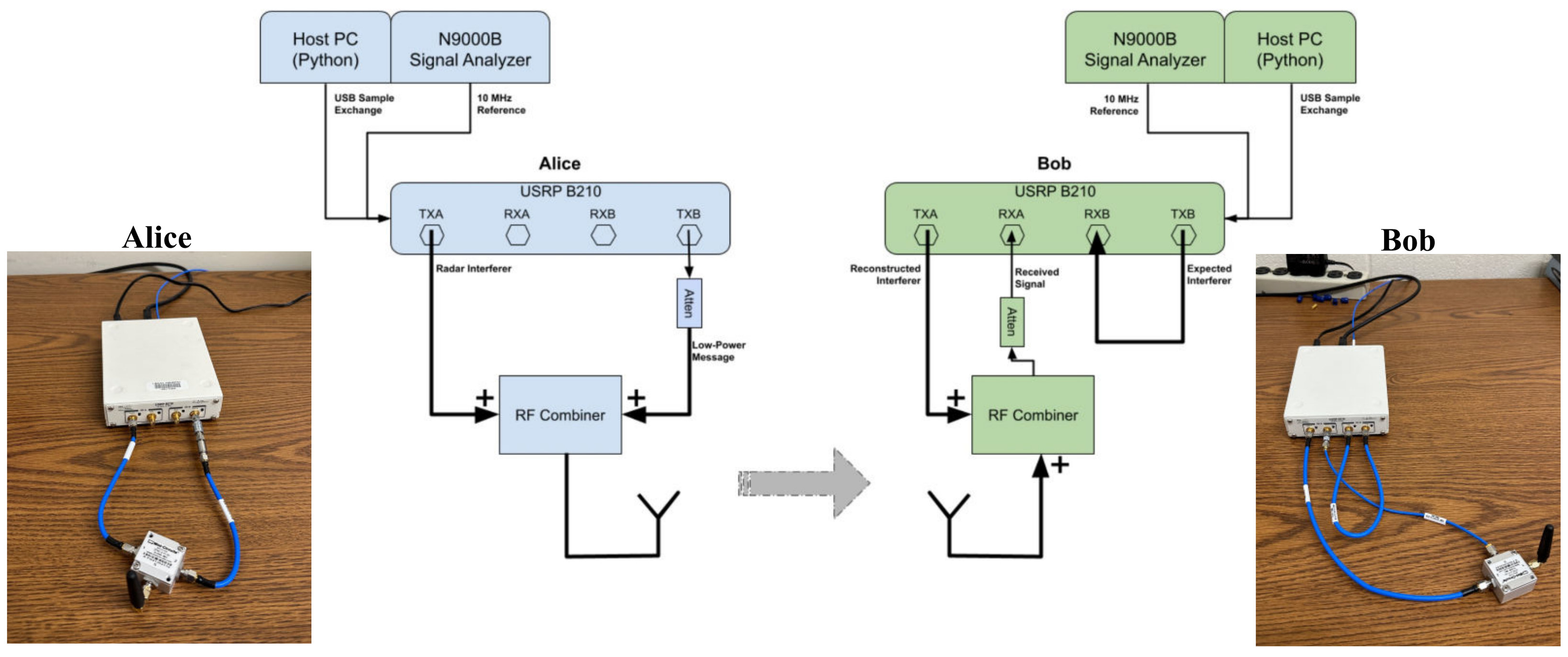
Eve's strategy:

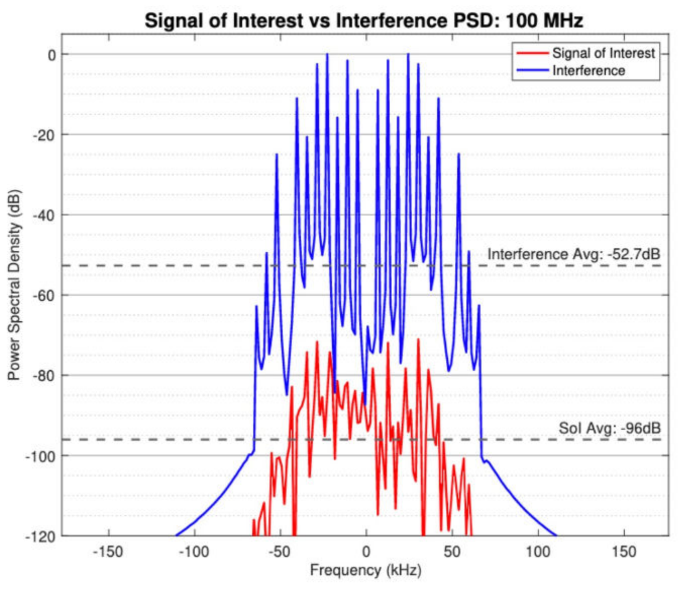
- Do not change span of her A/D → A/D overflows
- Enlarge span of A/D to prevent overflows → degrade resolution

Information loss

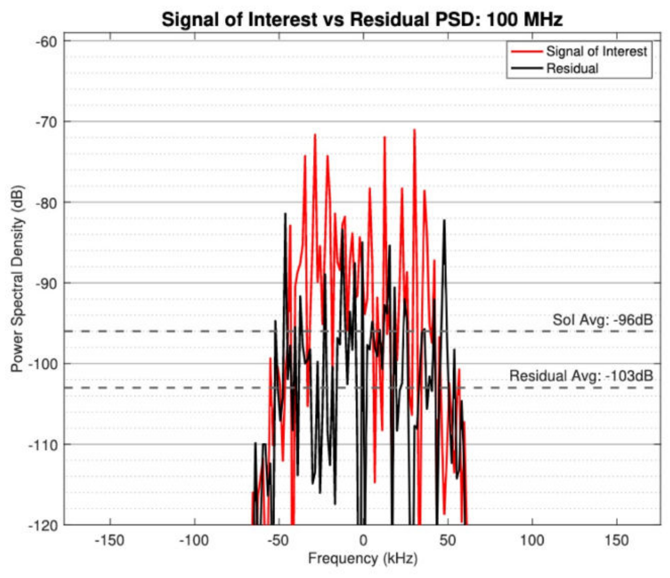
IV. Key Challenge: *Analog* Interference Cancellation at Bob

Bob knows the interfering signal – when it leaves the radar. But it comes across a time-varying wireless channel. Analog cancellation is a (stiff) challenge that must be solved.





Eve's (Tough) Challenge



Bob's (Easier) Challenge

6. Conclusion and future work

- We have proposed a technique to convert ephemeral "cheap" cryptographic key bits to "expensive" information-theoretically secure bits to achieve everlasting security.
- A jamming signal (known in advance by Bob, afterward by Eve) from a radar is employed. Eve, in order to prevent overflows of her A/D converter, needs to enlarge her A/D span and thus degrade the resolution of her A/D, thus resulting in information loss.
- **A critical challenge is the analog cancellation of a remote known interference: 40+ dB cancellation can be maintained with inexpensive SDRs despite synch challenges; secrecy rates estimated at 2.3 bits/symbol (100 MHz) or 2.0 bits/symbol (1 GHz).**
- Ongoing work:
  - enhanced system design (e.g., multiplicative jamming) and analysis, cryptographic design and analysis [with Paul Staat, Christof Paar (Ruhr) and Meik Dorpinghaus, Gerhard Fettweis (TU-Dresden)]
  - analyzing potential degradations in secrecy versus multiple A/D's, with independent jitter (thanks to Wayne Start (UMich) for this idea).

Acknowledgements: This project has been funded by the National Science Foundation under grant ECCS-2029323.