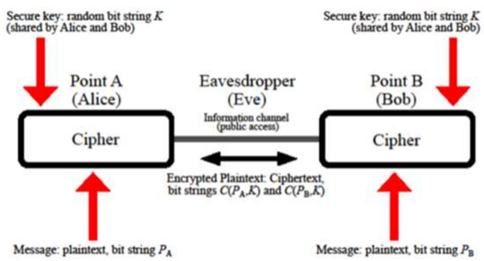
Statistical RNG Attack against the KLJN Secure Key Exchange Protocol

Christiana Chamon, Shahriar Ferdous, Laszlo B. Kish

Texas A&M University, Department of Electrical and Computer Engineering, College Station, TX

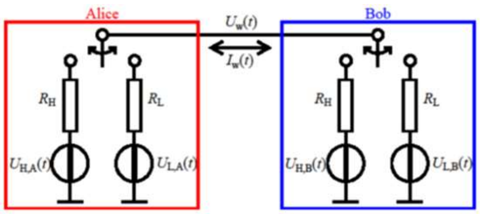
Secure Key Exchange



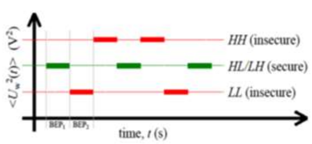
- Conversion of plaintext into a cipher
- For decryption, conversion of cipher back into plaintext
- Eve knows every detail the system except for the key.
- The key is assumed to be generated from truly random numbers.

The KLJN Scheme

- A statistical physical scheme based on the thermal noise of resistors
- Classical (statistical) physical alternative of Quantum Key Distribution (QKD)



- They have identical pairs of resistors, RA and RB.
- The statistically independent thermal noise voltages represent the noise voltages of RH and RL (RH > RL) of Alice and Bob, respectively, which are generated from RNGs
- At the beginning of each BEP, Alice and Bob randomly choose one of their resistors to connect to the wire.
- Alice and Bob (as well as Eve) use the mean-square voltage of the wire to assess the bit status, given by the Johnson formula
- Four possible resistance situations can be formed by Alice and Bob: HH, LL, LH, and HL.



- The HH and LL cases represent insecure situations
- The HL and LH cases represent secure bit exchange because Eve cannot distinguish between the corresponding two resistance situations

Selected References

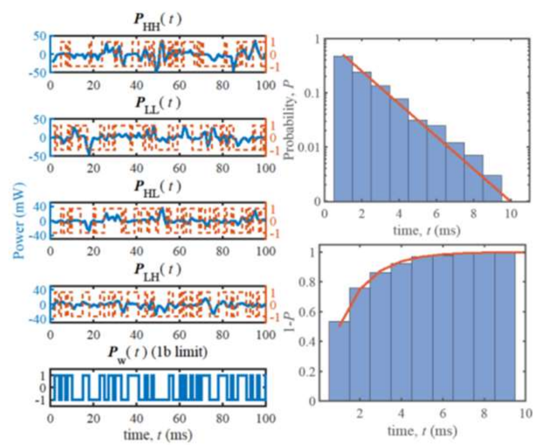
- L. B. Kish and C. G. Granqvist, “On the security of the Kirchhofflaw–Johnson-noise (KLJN) communicator”, Quantum Information Processing, 13 (2014) (10), 2213-2219.
- L. B. Kish, “Totally secure classical communication utilizing Johnson (-like) noise and Kirchhoff’s law”, Physics Letters A, 352 (2006) 178-182.
- J. Kelsey, B. Schneier, D. Wagner, and C. Hall. “Cryptanalytic Attacks on Pseudorandom Number Generators". Fast Software Encryption, Fifth International Workshop Proceedings. Springer-Verlag. (1998) pp. 168–188.

Random Number Generators

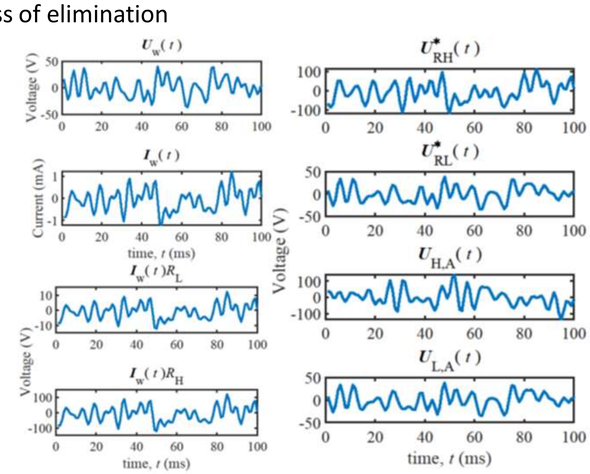
- Computational vs. true RNGs
- Computational RNGs collect randomness from various low-entropy input streams and try to generate outputs indistinguishable from truly random streams
- The randomness of an RNG relies on the uncertainty of the random seed and a long sequence with uniform distribution
- The moment an adversary learns the seed, the outputs are known, and the RNG is compromised.

Demonstration

- Bilateral parameter knowledge: Eve measures the power along the channel and only needs a single bit to do so



- Unilateral parameter knowledge: Eve uses Ohm’s Law and a process of elimination



Conclusion

- If Eve knows the seed of both Alice’s and Bob’s RNGs, she can crack the bit exchange with one bit of resolution
- If Eve knows the seed of only Alice’s RNG, she can crack the secure bit using the whole bit exchange period
- Future work would involve the noises not being accurately known but only noise with a nonzero correlation