Shared secret key generation at the Physical layer in EchoRing

Introduction:
Wireless medium being broadcast in nature is prone to passive attacks (eavesdropping) and active attacks (false identity claims) by adversaries. Henceforth, it is of great interest to design, implement and test novel (physical-layer) schemes (e.g., shared secret key generation, device authentication etc.) which ensure secure communication between the legitimate parties while simultaneously keeping the adversaries almost oblivious about it.
EchoRing is a novel token-passing wireless protocol which provides ultra-high reliabilities coupled with very low end-to-end latencies [1]; and therefore, finds its application in many machine-to-machine applications, e.g., industrial automation etc. However, like all other wireless protocols, EchoRing is prone to attacks by adversaries which, if not taken care of, can cause massive damage to the industrial equipment. To this end, there have been some recent efforts where cryptographic mechanisms were employed for device authentication in the EchoRing. Having said this, the goal of this thesis is to incorporate additional physical-layer mechanism of shared secret key generation so as to enhance the current security-level of the EchoRing.

Thesis outline:
This work considers a setting where two legitimate nodes (Alice and Bob) communicate with each other in the presence of a passive eavesdropper (Eve). The mutual goal of Alice and Bob is the following: extract common secrecy out of some shared physical layer attribute (e.g., wireless channel, frequency offset etc.), generate shared secret keys, and subsequently use them to encrypt their later transmissions [2]. To this end, the student will design a protocol for shared secret key generation (tailored for EchoRing), implement it on WARP software-defined radios, and evaluate the core performance metrics, e.g., secret key generation rate etc. Then, the implementation will be integrated into already existing prototype of EchoRing. Depending upon the student's progress, a far-end extension is also possible where the student will extend the same protocol to the scenario with multiple legitimate nodes and multiple adversaries.

Requirements:
Candidate is expected to have reasonable (or, at least, basic) knowledge of security mechanisms employed by existing and upcoming wireless LAN/PAN standards (e.g., 802.11x, Zigbee, Bluetooth etc.). At the same time, some past exposure to FPGA programming is a plus; and therefore, is highly encouraged.

Contact:
james.gross@ee.kth.se
mahboob.rahman@ee.kth.se

References:
[1] Dombrowski, C., & Gross, J. (2015). EchoRing: A Low-Latency, Reliable Token-passing MAC Protocol for Wireless Industrial Networks. In European Wireless Conference 2015 (EW 2015).
[2] Chunxuan Ye; Mathur, S.; Reznik, A.; Shah, Y.; Trappe, W.; Mandayam, Narayan B., "Information-Theoretically Secret Key Generation for Fading Wireless Channels," Information Forensics and Security, IEEE Transactions on , vol.5, no.2, pp.240,254, June 2010.