Highly Efficient Privacy-Preserving Key Agreement for Wireless Body Area Networks

Wireless Body Area Networks (WBANs) consist of miniaturized computing devices which can be fitted inside or around the human body. Through use of short range communication technologies, these devices talk to a designated centralized node (Hub) which further communicates with external networks via a Gateway. Mindful of the peculiarities of communicating in and around the human body, the IEEE published IEEE Std 802.15.6 for WBAN communications in 2012. In addition to conventional security guarantees, privacy is of utmost importance for typical target application areas such as healthcare and the military. The security of traffic in IEEE Std 802.15.6 is protected using authenticated encryption, which requires the establishment of symmetric session keys. The procedure for agreeing these keys is thus critical to the overall security and privacy of a WBAN.

The session key agreement methods of IEEE Std 802.15.6 have been shown to have security weaknesses, but also do not provide the privacy features that should be expected of a WBAN. To date, no key agreement protocol has been proposed which fulfills all the requisite security and privacy objectives for deployment in a resource constrained WBAN environment. In this talk, based upon symmetric cryptographic primitives only, two key agreement protocols would be discussed which, in addition to good performance also offer the desirable privacy attributes of *node anonymity* and *session unlinkability.* The protocols are also suitable for post-quantum deployment scenarios as they are independent of any public key based operations. We focus on two privacy aspects:

Node Anonymity. An adversary, who is observing all communications, should not be able to learn the identity of any node N who is participating in the key agreement protocol with the Hub node.

Session Unlinkability. An adversary, who is observing communications, should not be able to link one successfully executed key agreement session of node a N to another successfully completed session of the same node.

The first protocol addresses the privacy flaws found in previous works. The second protocol, additionally provides forward security and KCI resilience (in case of compromise of the long term secret of node N). Given recent successes towards achieving practical universal quantum computers, it is imperative that proposals for any standard should also cater for this soon to be realized threat. Our PPKA protocols avoid any public key cryptography and thus are well suited for post quantum deployment scenarios. The proposed protocols emerge as attractive alternates for the current key exchange methods described in the IEEE 802.15.6 standard, which are based upon legacy public key based primitives and do not offer any privacy features.