Lightweight extensions of secret sharing schemes

Prof. Keith Martin

Royal Holloway, University of London, UK

(Joint work with Thalia Laing)

Secret sharing schemes have become increasingly important cryptographic primitives with the rise of networking environments which lack single points of trust. Such networks are particularly prominent in settings such as so-called *Internet-of-things* applications, where devices may be highly constrained. We revisit the basic idea of a secret sharing scheme in several settings where the application environment places restrictions on computational operations. We discuss the problems that arise and potential solutions.

Information Security Group, Royal Holloway, University of London
Egham Hill, Egham, Surrey TW20 0EX, UK
keith.martin@rhul.ac.uk