Identity-Based Encryption Gone Wild
By Gregory Neven (IBM)

In an identity-based encryption (IBE) scheme, any arbitrary string can be used as a user's public key, for example the user's identity or email address. The concept of IBE was proposed as early as in 1984, but the proposal of the first truly efficient schemes in 2001 based on bilinear maps, also known as pairings, sparked a renewed interest from the research community. This talk will discuss a number of variations and extensions of the basic IBE functionality, including performing keyword searches on encrypted data, adding wildcard functionality to users’ identities, and building traitor tracing schemes. Each of these are joint research results between various ECRYPT partners, and were the direct outcome of a number of ECRYPT-supported research retreats around Europe.