Modifying the One-Time Pad Cryptosystem for Practical Use

Rees, Gavin

A primary goal of cryptographic research is to develop more secure cryptosystems to ensure secrecy in the information-centric era we live in. Only the one-time pad cryptosystem achieves the theoretical maximum of security – the random key is the same size as the data to be encrypted. However, this large size of the random key makes the cryptosystem inefficient. The approach described in this paper begins with this theoretical maximum but develops an efficient alternative that retains very high security. This is achieved by using hashes as the source of a pseudorandom bitstream. By using an initial random key that is slightly altered then hashed each block of data that is encrypted, the hashes generated are random if regarded separately. Though the inputs to the hash function do share a common relationship and the cryptosystem does not retain perfect secrecy as a result. However, upon testing, sample bitstreams were indistinguishable from random by a battery of statistical tests and were significantly more random than bitstreams generated by other well-known cryptosystems. Furthermore, by pseudo randomly modifying the bitstream with an algorithm that depends on the previously encrypted data, the cryptosystem ensures message integrity: if the encrypted plaintext is modified in transit then the entire decryption will result in garbage data. This dependency also enlarges the amount of possible bitstreams exponentially without a larger key, makes attempts to brute force keys less effective, and protects against known plaintext attacks.

Awards Won:

Fourth Award of $500