

PUBLIC KEY ENCRYPTION OF STREAM CIPHERS

D. D. Buckley* and M. Beale.
Department of Electrical Engineering,
University of Manchester,
Manchester. M13 9PL U.K.

COPY COPY

*Also with Plessey Crypto,
Wavertree Technology Park,
Liverpool. L7 9PE. U.K.

The ever increasing requirement for the secure transmission of data, with corresponding key management problems, has resulted in Public Key Cryptosystems receiving much attention. However, developments in Public Key Cryptography have concentrated on block rather than stream ciphers, and the computation required to implement these cryptosystems results in slow encryption/decryption speeds. In addition, since each bit in a ciphertext block depends on every other bit in that block, a one-bit error in transmission results in erroneous deciphering of the entire block. Although this property is desirable in some applications, there are others in which such error propagation is a distinct disadvantage.

In this paper, we present a technique for implementing the RSA Public Key Algorithm for use with stream ciphers in such a way that high speed encryption/decryption may be performed. After an initial configuration prior to transmission, speeds in excess of one tenth of those associated with a conventional one-time pad cipher may be achieved. These transmission speeds are dependant on the error rates present in the channel, and we illustrate how the encrypted plaintext may be successfully decrypted even under severe error conditions. Another feature of the scheme is its resistance to "known plaintext" attacks.

Results of a simulation of the technique are included which give quantitative indications of the speed improvement over a conventional RSA system, and the performance in the presence of errors.

[1] R.L.Rivest, A.Shamir and L.Adleman, "A Method for obtaining Digital Signatures and Public Key Cryptosystems", Vol. 21 pp.121-126, February 1978.