of 15 μs. This suggests therefore that the system could safely be used in most geographical locations of interest. In mountainous regions with very long echo delays, some gain would still be achieved by setting τ to $T/2$ without significantly degrading the receiver equalisation capability.

The technique has also been validated through testing with more complex Rayleigh fading channel models specified by GSM[5] which are typical of particular geographical locations. For example, a gain of over 6 dB at a bit error rate of 10^{-2} has been found for the 'rural area' model[5] with $\tau = T$.

Diversity system configuration: This diversity scheme may be implemented both at the BS (base station) and at the MS (mobile station), using different configurations which are briefly reviewed below.

(*a*) *Receiver diversity:* This is a direct realisation of the system illustrated in Fig. 1, which could be implemented at either the BS or the MS. For the MS, only a small spacing between the two antennas is required to achieve good fading decorrelation.[2] To comply with the GSM equaliser specification, MS manufacturers might consider several possible configurations, e.g. (i) a small fixed delay of $T/2$ giving reduced diversity gain but enabling compliance, or (ii) provision of a more complex equaliser designed to cope with up to 20 μm dispersion (i.e., the specified 16 μs plus one bit period). A more sophisticated approach would consist of allowing the delay τ itself to be set adaptively after sensing the channel dispersion. Thus τ could be reduced and eventually nulled (no diversity) under extreme dispersive conditions.

(*b*) *Transmitter diversity:* Assuming reciprocity, it follows that diversity in the BS to MS direction could be generated by the BS itself using the arrangement of Fig. 1 for transmission, effectively providing two transmission paths with a relative time delay large enough for the equaliser to separate them at the MS. The resulting gain should be identical to that found for receiver diversity. The main advantage of this mode of operation lies in the fact that the MS would only require one antenna and no extra processing. However, a handset designed according to the GSM specifications might not operate correctly in areas exhibiting large delay spreads, and the BS would therefore need to adapt the delay τ to ensure that excessive dispersion was not generated, or alternatively implement only a small fixed delay $T/2$ as discussed above for receiver diversity.

Conclusions: A combined space/time diversity technique has been described which does not require any special switching or combining arrangements as well as avoiding the complexity of frequency hopping based schemes. This technique is particularly suited to narrowband TDMA links where the receiver processing is likely to include equalisation, which may be directly used to resolve and combine the diversity paths.

L. B. LOPES *19th May 1989*

Department of Electrical & Electronic Engineering
University of Leeds
Leeds LS2 9JT, United Kingdom

References

1 PROAKIS, J. G.: 'Digital Communications' (McGraw-Hill, New York, 1983), ch. 7
2 TAPANI, N.: 'Experimental results on diversity in digital mobile radio'. Proceedings of the second Nordic Seminar on Digital Land Mobile Radio Communication, Stockholm, 1986, pp. 74–79
3 HAUG, T.: 'Overview of the GSM Project'. Proceedings of the Eighth European Conference on Electrotechnics (Area Communication), Stockholm, 1988, pp. 455–457
4 LOPES, L. B.: 'Performance of Viterbi equalisers for the GSM system'. Proceedings of the second IEE National Conference on Telecommunications, York, 1989, pp. 61–66
5 'Transmission and reception'. CEPT/GSM Recommendation 05/05

NEW SCHEME FOR DIGITAL MULTISIGNATURES

Indexing terms: Codes, Information theory

When two individual users wish to carry on a secure conversation, they can use the well-known RSA public key cryptosystem in doing so. This cryptosystem provides to these users both data secrecy and digital signature in a very efficient manner. However, in many applications, multiple users need to sign a document. In this letter, we propose a modified scheme, based on the RSA scheme, which will allow any number of users to sign a document and send it secretly to the receiver. The length of ciphertext remains constant, no matter how great the number of signatories. The trade-off is that the processing times required for generating the multisignature, and for verifying multisignatures, depend on the number of signatories.

Introduction: In 1976, Diffie and Hellman[1] invented the concept of the public-key distribution cryptosystem. Since then, several public-key systems[2–4] have been proposed. Among them, the RSA scheme[3] has received the widest attention. For this RSA scheme, the difficulty of breaking the system is based on the difficulty of factoring a large integer into its two large prime factors. This scheme provides both data encryption and digital signature for one-to-one communication with bit ratios of 1 : 1.

However, for some applications, there are multiple users involved in signing a document. This problem is the so-called 'multisignature' problem. Itakura and Nakamura[5] have developed a solution based on an extended RSA scheme. In their method, any user must first join a system by registering with a key generating centre, which centre distributes to that user a set of public keys and a set of secret keys. In addition, a public key which reflects the user's position in the system must also be generated by the centre at registration time. There are two major drawbacks in their proposed scheme, which make it inappropriate outside its intended realm of application, i.e. within certain types of organisations. First, the key generation process is centralised. For most current networks, where there are millions of users involved, this arrangement is obviously impractical. Second, for most networks, a hierarchical relationship among users either cannot be predetermined or does not exist, rendering this method unsuitable.

Boyd[6] proposed a double signature scheme. He states that this method, however, cannot be extended to apply to the case of more than two signatories, without requiring that all signatories other than the first and last ones be willing to sign a document that they cannot see, i.e. be 'blind signatories'.

In this letter we propose a modified RSA scheme which can allow any number of users to sign a document and send it secretly to the receiver. The length of ciphertext remains constant no matter the number of signatories. One major feature in our method is the following: since the signatories need to sign the document consecutively, it becomes necessary to apply a succession of transformations on intermediate signatures using different moduli, which moduli must therefore be ordered; hence, we incorporate the ideas proposed by Rivest *et al.*[3] and Kohnfelder[7] to provide this ordering of moduli, thus eliminating any need to reblock intermediate signatures. In other words, if the RSA scheme is already implemented on the system, then our scheme allows network users to use that scheme for the additional task of providing multisignatures when needed.

Our proposed method for providing data secrecy and multisignature:

Public/secret keys: Each user has to select randomly two sets of two large primes as his/her secret key, (p_{A_1}, q_{A_1}) and (p_{A_2}, q_{A_2}), and then to evaluate the corresponding public keys as $n_{A_1} = p_{A_1}q_{A_1}$ and $n_{A_2} = p_{A_2}q_{A_2}$, where $n_{A_1} < h < n_{A_2}$, and h is a special system threshold value which is publicly known. Two other sets of keys also need to be calculated. The first set,

(E_{A_1}, D_{A_1}), is used for providing signatures, and the second set, (E_{A_2}, D_{A_2}), is used for providing secrecy. These keys must satisfy the following conditions:

$$E_{A_1} D_{A_1} \bmod \Phi(n_{A_1}) = 1$$

$$E_{A_2} D_{A_2} \bmod \Phi(n_{A_2}) = 1$$

where Φ is the Euler totient function. Finally $(n_{A_1}, E_{A_1}, E_{A_2})$ needs to be made publicly known and $(p_{A_1}, q_{A_1}, p_{A_2}, q_{A_2}, D_{A_1}, D_{A_2})$ needs to be kept as a personal secret.

Encryption for multisignature: We think that it is reasonable that any document which needs to be signed by multiple users be prepared by one of those users whom we call the 'initiator'. The initiator needs to determine all the signatories and to access their public keys. Then the signing order is determined according to their public key values. The signing order for signatories U_i and U_j is that U_i precedes U_j whenever $n_{U_{i,1}} < n_{U_{j,1}}$.

Multisignature generation: Without loss of generality, we will assume that there are t users $U_1, U_2, \ldots, U_t$ who need to sign some document, and that their public key values satisfy the inequality $n_{U_{1,1}} < n_{U_{2,1}} < \ldots < n_{U_{t,1}}$. Note that only their first public key elements, $n_{U_{i,1}}$, the ones used for providing signatures, are involved.

Step 1: The initiator needs to send this signing order information, and the document, to the first signatory on the list. Therefore, the initiator needs to compute $C_1 = E_{U_{1,1}}(M)$ and send $(\{U_1, U_2, \ldots, U_t\}, C_1)$ to U_1. Note that we use the expression $E_{U_{1,1}}(M)$ to indicate the computation $(M)^{E_{U,1,1}} \bmod n_{U_{1,1}}$.

Step 2: U_1 first deciphers the encrypted message C_1 as $M = D_{U_{1,1}}(C_1)$. Then if U_1 agrees to sign the message, he/she will put the signature on this message as $S_1 = D_{U_{1,1}}(M)$, and send this signature secretly to the second signatory on the list. Therefore, U_1 needs to compute $C_2 = E_{U_{2,1}}(S_1)$ and send $(\{U_1, U_2, \ldots, U_t\}, C_2)$ to U_2.

Step 3: U_2 first will decipher the encrypted message C_2 by computing $S_1 = D_{U_{2,1}}(C_2)$ and storing S_1. Then he/she will decipher S_1 again to see the plaintext message M as $M = E_{U_{1,1}}(S_1)$. Since $n_{U_{2,1}} > n_{U_{1,1}}$, the original message, M will be recovered. Then if U_2 agrees to sign the message he/she will put his/her signature on the S_1 value stored previously, as $S_2 = D_{U_{2,1}}(S_1)$ and send this double signature which involves both U_1 and U_2 to the third signatory on the list. Therefore, U_2 needs to compute $C_3 = E_{U_{3,1}}(S_2)$ and send $(\{U_1, U_2, \ldots, U_t\}, C_3)$ to U_3.

Step (i + 1) ($3 \le i \le t - 1$): U_i first will decipher the encrypted message C_i by computing $S_{i-1} = D_{U_{i,1}}(C_i)$ and storing S_{i-1}. Then he/she will decipher S_{i-1} again to see the plaintext message M as $M = (E_{U_{1,1}}(E_{U_{2,1}}, \ldots, (E_{U_{(i-1),1}}(S_{i-1})) \ldots))$. Since $n_{U_{(i-1),1}} > \ldots > n_{U_{2,1}} > n_{U_{1,1}}$, the original message M will be recovered. Then if U_i agrees to sign the message, he/she will put his/her signature on S_{i-1} as $S_i = D_{U_{i,1}}(S_{i-1})$ and send this multisignature S_i which involves $U_1, U_2, \ldots, U_i$ to the $(i + 1)$th signatory on the list. Therefore, U_i needs to compute $C_{i+1} = E_{U_{(i+1),1}}(S_i)$ and send $(\{U_1, U_2, \ldots, U_t\}, C_{i+1})$ to U_{i+1}.

Step (t + 1): U_t first will decipher the encrypted message C_t by computing $S_{t-1} = D_{U_{t,1}}(C_t)$ and storing S_{t-1}. Then he/she will decipher S_{t-1} again to see the plaintext message M as $M = (E_{U_{1,1}}, \ldots, (E_{U_{(t-1),1}}(S_{t-1})), \ldots,)$. Then if U_t agrees to sign the message, he/she will put his/her signature on S_{t-1} as $S_t = D_{U_{t,1}}(S_{t-1})$ and send this multisignature, which involves all t signatories, to the legitimate receiver R. Therefore, U_t needs to compute $C_{t+1} = E_{R_2}(S_t)$ and send $(\{U_1, U_2, \ldots, U_t\}, C_{t+1})$ to R where E_{R_2} is the public key for data enciphering purposes of receiver R. Note that we use here the second public key of the receiver, since it functions for secrecy, not digital signature. It is to be noted also that $n_{R_2} > n_{U_{t,1}} > n_{U_{(t-1),1}} > \ldots > n_{U_{1,1}}$.

Multisignature verification and message decryption: User R will decipher the multisignature as $S_t = D_{R_2}(C_{t+1})$ and store S_t, which involves the secret keys of $U_1, U_2, \ldots, U_t$, as a proof of their multisignature of the message to be revealed. Then the corresponding signed message can be derived from S_t by computing $M = (E_{U_{1,1}}(E_{U_{2,1}}(\ldots, (E_{U_{t,1}}(S_t)), \ldots,)))$.

Conclusion: In this letter we have proposed a cryptographic algorithm which can provide both data secrecy and multisignatures based on the well known RSA cryptosystem. Without requiring any extra investment, our scheme provides this additional ability to network users on any network system which already provides for the use of the RSA cryptosystem.

L. HARN
T. KIESLER

Computer Science & Telecommunications Program
University of Missouri
5100 Rockhill Road, Kansas City, MO 64110-2499, USA

4th April 1989

References

1 DIFFIE, W., and HELLMAN, M. E.: 'New Directions in Cryptography', *IEEE Trans. Inf. Theory*, 1976, **IT-22**, pp. 644–654
2 MERKLE, R. C., and HELLMAN, M. E.: 'Hiding Information and Signatures in Trapdoor Knapsack', *IEEE Trans. Inf. Theory*, 1978, **IT-24**, pp. 525–530
3 RIVEST, R. L., SHAMIR, A., and ADELMAN, L.: 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystem', *Commun. of ACM*, 1978, **21**, (2), pp. 120–126
4 ELGAMEL, T.: 'A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms', *IEEE Trans. Inf. Theory*, 1985, **IT-31**, pp. 469–472
5 ITAKURA, K., and NAKAMURA, K.: 'A Public-Key Cryptosystem Suitable for Digital Multisignatures', *NEC Research and Develop.*, 1983, **71**, pp. 1–8
6 BOYD. C.: 'Some Applications of Multiple Key Ciphers'. Lecture Notes in Computer Science: Advances in Cryptology – EUROCRYPT '88, 1988, pp. 455–467
7 KOHNFELDER, L. M.: 'On the Signature Reblocking Problem in Public-Key Cryptoststems', *Comm. ACM*, 1978, **21**, (2), p. 179

3 GHz OPTICAL SOLITON PROPAGATION USING ALL LASER DIODES

Indexing terms: Optics, Optical communications, Nonlinear optics, Optical fibres

Optical soliton propagation at a 3 GHz repetition rate is demonstrated using optical pulses from a gain-switched 1·55 μm distributed feedback laser diode. An Er^{3+}-doped fibre amplifier and a Raman amplifier, both pumped by 1·47 μm Fabry-Perot laser diodes, are employed for achieving high-peak-power optical pulses and fibre-loss compensation, respectively.

Introduction: Recent successful demonstrations of optical soliton transmissions over more than 6000 km[1,2] have shown their potential for future ultra-high-speed, long-distance optical communication systems. To generate optical solitons at a high repetition rate, laser diodes (LDs) must be promising light sources for these systems because of their advantages concerning high-speed modulation and small size.[3] We have reported experimental results of optical soliton propagation using gain-switched optical pulses at a 2·6 GHz repetition rate from a 1·3 μm distributed feedback laser diode (DFB-LD).[4] However, in our previous experiments, a mode-locked YAG laser was employed as the pump source for Raman amplification to obtain intense optical pulses.

In this letter we report the first demonstration of optical soliton propagation through a 20 km-long, dispersion-shifted, single-mode optical fibre by all laser diodes. Optical pulses at a 3 GHz repetition rate are generated by a 1·55 μm DFB-LD. Fabry-Perot LDs (FP-LDs) are used for both amplifying the optical pulses and reducing the transmission fibre-loss.

Experiments: Fig. 1 shows the experimental set-up of optical soliton propagation by all laser diodes. The gain-switched