not shown in the Figure, the dominant-mode wavelength of the short laser also shifted one mode spacing towards longer wavelengths relative to the spontaneous emission peak under DC operation just below threshold, probably owing to an increase in junction temperature.[4] Note that the build-up time of the dominant mode is significantly faster in the short-cavity and the type-B ridge-waveguide lasers than in the type-A device.

The time-dependent output of these lasers, at discrete wavelengths and in real time, is shown in Fig. 2, where for clarity the evolution of four individual shots are shown (clean traces) in comparison with several thousand pulses (smeared traces).

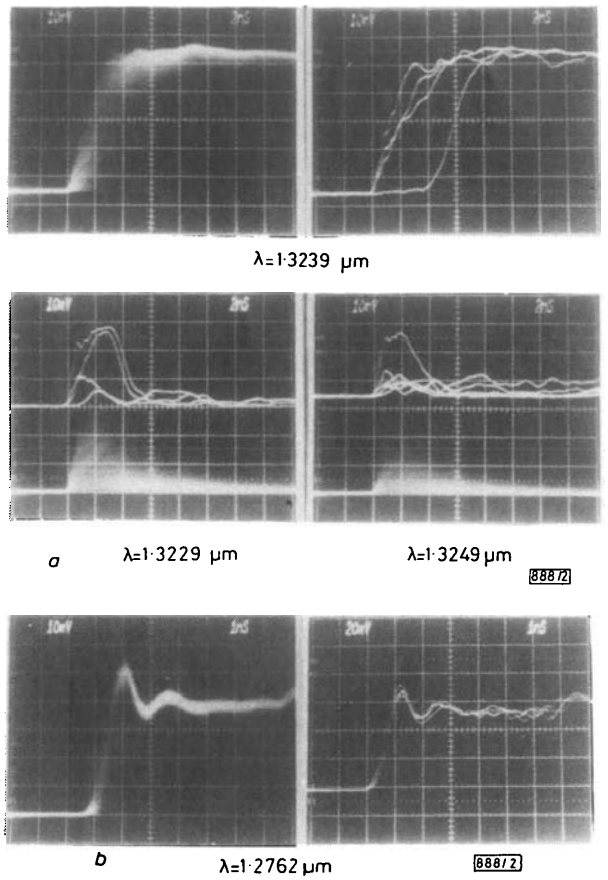

Fig. 2 *Transient response of (a) type-A standard-length ridge-waveguide laser and (b) short-cavity laser*

Both traces of a few thousand scans and four individual scans are shown. The wavelength indicates the spectrometer setting at which the traces were recorded. Type-B ridge-waveguide laser behaved similarly to the short-cavity laser

Note that, for the type-A ridge-waveguide laser, Fig. 2*a*, the individual pulse of any one mode can start at different times and go through different evolution paths.[5,6] The secondary modes decay while the dominant mode increases to its steady-state value in about 6 ns. A similar display of the output of the dominant mode of the type-B or the short-cavity laser is reproduced in Fig. 2*b*, which shows far less pulse-to-pulse variation.

We conclude that any laser with genuinely stable single-mode output, whether achieved by design or by accident (as, for example, by a buried periodic ripple providing wavelength-selective feedback), leads to transient behaviour compatible with modulation at high bit rates.

The origin of the intensity fluctuations is the spontaneous emission.[3,7-9] Even when biased slightly below threshold, the number of spontaneous photons at each longitudinal mode wavelength is significant,[3] and the instantaneous spectrum just before application of the current step has large fluctuations. Subsequent to the arrival of the current step, each mode builds up at different rates from these fluctuations until the stimulated emission of the dominant mode finally takes over. It has been pointed out that, if the side mode initially contains significant power, it takes several nanoseconds for it to decay. In a short-cavity laser, however, the decay of the side modes is faster, allowing faster build-up of the dominant mode.

We note again that the jitter in the equipment was less than 50 ps. Thus the displayed random fluctuations (partition of the optical energy among longitudinal modes as a function of time) represent a direct observation of the mode partition noise in real time.

We are indebted to J. A. Copeland, E. A. J. Marcatili and S. E. Miller for unpublished information, and to N. K. Cheung and A. Tomita for the use of equipment.

PAO-LO LIU
Bell Laboratories
Holmdel, New Jersey 07733, USA

T. P. LEE
C. A. BURRUS
I. P. KAMINOW
J.-S. KO
Bell Laboratories
Crawford Hill Laboratory
Holmdel, New Jersey 07733, USA

31st August 1982

References

1 KAMINOW, I. P., NAHORY, R. E., STULTZ, L. W., and DEWINTER, J. C.: 'Performance of an improved InGaAsP ridge waveguide laser at 1·3 μm', *Electron. Lett.*, 1981, **17**, pp. 318–320
2 BURRUS, C. A., LEE, T. P., and DENTAI, A. G.: 'Short-cavity single-mode 1·3 μm InGaAsP lasers with evaporated high-reflectivity mirrors', *ibid.*, 1981, **17**, pp. 954–956
3 LEE, T. P., BURRUS, C. A., COPELAND, T. A., DENTAI, A. G., and MARCUSE, D.: 'Short-cavity InGaAsP injection lasers: Dependence of mode spectra and single-longitudinal power on cavity length', *IEEE J. Quantum Electron.*, 1982, **QE-18**, pp. 1101–1113
4 NAGANO, M., and KASAHARA, K.: 'Dynamic properties of transverse junction stripe lasers', *ibid.*, 1977, **QE-13**, pp. 632–637
5 MACHIDA, S., TSUCHIYA, H., and ITO, T.: 'Single-mode optical fiber cable transmission experiment at 0·85 μm wavelength', *Rev. Electr. Commun. Lab.*, 1979, **27**, pp. 599–610
6 HENNING, I.: 'Technique for measuring true time-resolved spectra of a semiconductor laser', *Electron. Lett.*, 1982, **18**, pp. 368–369
7 MCCUMBER, D. E.: 'Intensity fluctuations in the output of cw laser oscillators I', *Phys. Rev.*, 1966, **141**, pp. 306–322
8 JÄCKEL, H., and GUEKOS, G.: 'High frequency intensity noise spectra of axial groups in the radiation from cw GaAlAs diode lasers', *Opt. & Quantum Electron.*, 1977, **9**, pp. 233–239
9 ITO, T., MACHIDA, S., NAWATA, K., and IKEGAMI, T.: 'Intensity fluctuations in each longitudinal mode of a multimode AlGaAs laser', *IEEE J. Quantum Electron.*, 1977, **QE-13**, pp. 574–579

0013-5194/82/210904-02$1.50/0

FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM

Indexing terms: Codes, Cryptography, Public-key cryptosystem, RSA

A fast algorithm is presented for deciphering cryptograms involved in the public-key cryptosystem proposed by Rivest, Shamir and Adleman. The deciphering method is based on the Chinese remainder theorem and on improved modular multiplication algorithms.

Introduction: Among the published public-key cryptosystems, the scheme proposed by Rivest, Shamir and Adleman[1] (usually referred to as the RSA or MIT cryptosystem) seems to be the most attractive for many applications. Its security is based on the fact that any known successful cryptanalytic attack has the same complexity as the factorisation of a large composite number:[2,3] at this time, no very efficient method of factoring is known. However, a frequently quoted disadvantage of the RSA cryptosystem is the relative time complexity

of its operations (discrete exponentiation modulo a large integer) as compared to conventional systems such as the DES.[4,5]

In this letter a fast algorithm is presented for deciphering cryptograms in the RSA system, which is about 4–8 times faster than the classical algorithm for computing a modular exponentiation.[2] This algorithm is based on the Chinese remainder theorem and on improved modular multiplications.

RSA scheme: Let an RSA box be a small electronic device[2] the memory of which contains two large prime numbers p and q. These numbers have been generated by the RSA box itself and are accessible to nobody. The product $r = pq$ has been computed and a random integer e which is relatively prime with both $p - 1$ and $q - 1$ has been generated too. The RSA box has also precomputed the only integer $d < r$ such that

$$ed \equiv 1 (\text{mod } (p-1)(q-1))$$

The enciphering key consists of the pair (e, r), possibly listed in a directory. The deciphering key is the pair (d, r) and is kept secret in the RSA box.

If a user wants to send a private message M to the owner of this RSA box, he proceeds as follows:

(i) He retrieves the (public) enciphering key (e, r).

(ii) He breaks the message M into a sequence of blocks $(m_1, \ldots, m_i, \ldots, m_k)$, where each block is represented as an integer m_i between 0 and $r - 1$.

(iii) He transmits the cryptograms $(c_1, \ldots, c_i, \ldots, c_k)$, where $c_i = E(m_i) = m_i^e \pmod r$.

The RSA box can decipher the cryptograms c_i by computing $D(c_i) = c_i^d \pmod r = m_i$. Hence the message M is recovered by the owner of the RSA box when the whole sequence $(c_1, \ldots, c_k)$ is deciphered.

Fast deciphering algorithm: Classically, as the quantities m, r, e and d would be about 500 or 600 bits long,[4,6,7] the enciphering and the deciphering processes require up to several hundred multiplications of integers of this length. The enciphering key can be as short as 2 bits,[2,4] but, for avoiding attacks by enumerative techniques, the deciphering key requires the maximum length. However, the deciphering process can be expedited. Before describing the fast deciphering algorithm, some notations[2,8] must be introduced.

Let us consider the following residues of the quantities m, c and d:

$$c_1 = c(\text{mod } p) \qquad c_2 = c(\text{mod } q)$$

$$d_1 = d(\text{mod } p-1) \qquad d_2 = d(\text{mod } q-1)$$

$$m_1 = m(\text{mod } p) = c_1^{d_1} (\text{mod } p)$$

$$m_2 = m(\text{mod } q) = c_2^{d_2} (\text{mod } q)$$

since the message m and the cryptogram c are related by $m = c^d \pmod r$.

Given p and q, $p < q$, let A be a constant integer such that $0 < A < q - 1$ and $A_p \equiv 1 \pmod q$. This constant is obtained by applying Euclid's algorithm[2] for computing gcd (p, q). By using the Chinese remainder theorem it is easily observed that m satisfies

$$m = [((m_2 + q - m_1)A) (\text{mod } q)]p + m_1 \qquad (1)$$

Hence, to decipher the cryptogram c, the algorithm first computes $m_1 = c_1^{d_1} \pmod p$ and $m_2 = c_2^{d_2} \pmod q$ rather than computing $m = c^d \pmod r$ classically. The quantities p, q, c_1, c_2, d_1 and d_2 are now only about 300 bits long. This permits one to reduce the time complexity to about a quarter. Moreover the two computations may be done in parallel. To recover the message m, it remains to compute expr. 1.

Let us remark that the exponents d_1 and d_2 may be chosen to be greater than $p - 1$ and $q - 1$; that does not affect the result. But if the (binary) weight of the exponent is smaller, then the modular exponentiation becomes possibly faster.

Even so, the most time-consuming part of the deciphering scheme remains the modular exponentiations. A modular exponentiation algorithm for computing $P = c^d \pmod p$ is described in the Appendix. This algorithm is distinguished from the classical ones. Many simplifications are made due to the context in which it is implemented. For example, the modular multiplications by c are reduced to a sequence of table look-ups and accumulations.[9] Also the number P is mostly required to be at most $n = \lceil \log_2 p \rceil$ bits long[10] and not necessarily smaller than p. This explains that only the most significant bit of P, and not the integer P itself, is tested before a possible reduction of P. So the reductions modulo p are made as few as possible. These reductions are also very simplified by the precomputations of the integers Q and R. Finally, let us remark that this algorithm does away with the integer division.

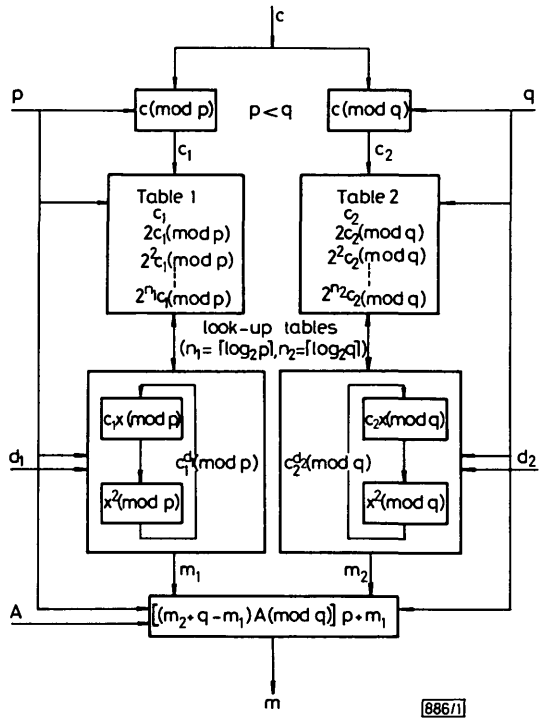

Fig. 1

Fig. 1 is a functional diagram of the deciphering process of the RSA cryptosystem, using this improved modular exponentiation algorithm and computing $m_1 = c_1^{d_1} (\text{mod } p)$ and $m_2 = c_2^{d_2} (\text{mod } q)$ in parallel.

If the lengths of p and q are about 256 bits, then Tables 1 and 2 use $2 \times (256)^2$ bits $\simeq$ 128 kbits: this value is within the range of current technology. Faster implementation is still possible with additional memory of the expressions $(2^{i-1} + 2^i)c (\text{mod } p)$ in both Tables.

We would like to mention that Krishnamurthy and Ramachandran[11] have independently proposed to use the Chinese remainder theorem for computing modular exponentiations in their conventional cryptosystems.

Acknowledgments: We would like to thank J.-M. Goethals for helpful comments.

Appendix: Let p be an integer, > 1, with exactly n bits, i.e. $n = \lceil \log_2 p \rceil$. An n-bit number d is represented as $[d_{n-1} \ldots d_1 d_0]$. The following algorithm computes the modular exponentiation.

Procedure MODULAR EXPONENTIATION (c, d, p): given the integers c, d and p, where $0 \leq c < p$, $0 \leq d < p - 1$, the procedure computes the integer $P = c^d \pmod p$, $0 \leq P < p$.

Initialisation: $Q \leftarrow 2^n - p$; $P \leftarrow 1$;

Step 1: for $i = n - 1, n - 2, \ldots, 1$

1.1 if $P_{n-1} = 1$ **then** $P \leftarrow$ REDUCTION(P)
1.2 $P \leftarrow$ MODMUL(P, P, p, P)
1.3 if $d_i = 1$ **then** $P \leftarrow$ MODMULCO$(P, p,$ table, $P)$;

Step 2: if $P_{n-1} = 1$ **then** $P \leftarrow$ REDUCTION(P);

Return P

The procedures used in the above algorithm can be described as follows.

Procedure REDUCTION (P): given the n-bit integer P, $0 \leq P < 2^n$, and the precomputed (global variable) integer $Q = 2^n - p$, this procedure returns the value $P \pmod p$, between 0 and $p - 1$.

Initialisation: $R \leftarrow P + Q$;

if $R_n = 1$ **then** $P \leftarrow [R_{n-1} \ldots R_0]$;

Return P

Procedure MODMUL (x, y, p, P): given the integers x, y and p, $0 \leq x < p$, $0 \leq y < 2^n$, this procedure computes the integer $P = x \,.\, y \pmod p$. The integer P is a $(n+1)$-bit number $[P_n P_{n-1} \ldots P_1 P_0]$ but as output, P verifies $0 \leq P < 2^n$.

Initialisation: $R \leftarrow Q + x$; $P \leftarrow 0$;

for $i = n - 1, n - 2, \ldots, 1$

1. $P \leftarrow$ one left shift of P
2. **if** $y_i = 1$ **then**
   if $P_n = 1$ **then** $P \leftarrow [P_{n-1} \ldots P_0] + R$ **else** $P \leftarrow P + x$
3. **if** $P_n = 1$ **then** $P \leftarrow [P_{n-1} \ldots P_0] + Q$
4. **if** $P_n = 1$ **then** $P \leftarrow [P_{n-1} \ldots P_0] + Q$;

Return P

Procedure LOOK-UP TABLE (c, n, p, table): given the integers c, n and p, $0 \leq c < p$, this procedure computes the sequence $c, 2c, 2^2c, \ldots, 2^{n-1}c$, each value being stored modulo p in a table. This table is used by MODMULCO.

Initialisation: $P \leftarrow c$; table(0) $\leftarrow c$;

for $i = 1, 2, \ldots, n - 1$

1. $P \leftarrow$ one left shift of P
2. **if** $P_n = 1$ **then** $P \leftarrow [P_{n-1} \ldots P_0] + Q$
3. **if** $P_{n-1} = 1$ **then** $P \leftarrow$ REDUCTION(P)
4. table(i) $\leftarrow P$;

Return

Procedure MODMULCO (x, p, table, P): given x, $0 \leq x < 2^n$, p and the table generated by LOOK-UP TABLE for the integer c, this procedure returns the value $P = c \,.\, x \pmod p$, $0 \leq P < 2^n$.

Initialisation: $P \leftarrow 0$;

for $i = 0, 1, 2, \ldots, n - 1$

if $x_i = 1$ **then**

1. $P \leftarrow P +$ table(i)
2. **if** $P_n = 1$ **then** $P \leftarrow [P_{n-1} \ldots P_0] + Q$;

Return P

J.-J. QUISQUATER
C. COUVREUR

Philips Research Laboratory
Av. Van Becelaere 2, Box 8
B-1170 Brussels, Belgium

27th August 1982

References

1 RIVEST, R. L., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signatures and public-key cryptosystems', *Commun. ACM*, 1978, **21**, pp. 120–126
2 KNUTH, D. E.: 'The art of computer programming, Vol. 2: seminumerical algorithms' (Addison-Wesley, Reading, Mass., 2nd edn., 1981)
3 WILLIAMS, H. C.: 'A modification of the RSA public-key encryption procedure', *IEEE Trans.*, 1980, **IT-26**, pp. 726–729
4 MICHELMAN, E. H.: 'The design and operation of public-key cryptosystems', *NCC*, 1979, pp. 305–311
5 SCHANNING, B. P.: 'Data encryption with public-key distribution'. Proc. Eascon 1979, IEEE, pp. 653–660
6 DAVIES, D. W., PRICE, W. L., and PARKIN, G. I.: 'An evaluation of public-key cryptosystems'. NPL report, CTU1 (revised), April 1980
7 RIVEST, R. L.: 'A description of a single-chip implementation of the RSA cipher', *Lambda*, 4th quarter 1980, pp. 14–18
8 SZABÓ, N. S., and TANAKA, R. I.: 'Residue arithmetic and its applications to computer technology' (McGraw-Hill, New York, 1967)
9 HENRY, P. S.: 'Fast decryption algorithm for the knapsack cryptographic system', *Bell Syst. Tech. J.*, 1981, **60**, pp. 767–773
10 BLAKLEY, G. R.: 'A computer algorithm for calculating the product AB modulo M'. Research report, Department of Mathematics, Texas A & M University, Texas, USA
11 KRISHNAMURTHY, E. V., and RAMACHANDRAN, V.: 'A cryptographic system based on finite field transforms', *Proc. Ind. Acad. Sci. (Math. Sci.)*, 1980, **89**, pp. 75–93
12 AHO, A. V., HOPCROFT, J. E., and ULLMAN, J. D.: 'The design and analysis of computer algorithms' (Addison-Wesley, Reading, Mass., 1974)
13 WILLONER, R., and I-NGO CHEN: 'An algorithm for modular exponentiation'. Proc. 5th symp. on computer arithmetic, IEEE Computer society, 1981, pp. 135–138

0013-5194/82/210905-03$1.50/0

MEASUREMENT OF POLARISATION MODE DISPERSION IN ELLIPTICAL-CORE SINGLE-MODE FIBRES AT 1·3 μm

Indexing terms: Optical fibres, Polarisation, Dispersion

Polarisation mode delay differences in three single-mode fibres were measured interferometrically at 1·3 μm with a resolution below 25 fs. Polarisation mode dispersion increases strongly with core ellipticity.

Introduction: Polarisation mode dispersion may be a limiting factor in high-capacity single-mode optical-fibre transmission systems[1,2] that will be operated most likely at about 1·3 μm wavelength, where the material dispersion is minimum. We report here on polarisation mode dispersion measurements carried out interferometrically at 1·3 μm. This is to complement some related recently published results[3,4] that concentrated on the shorter wavelengths around 0·85 μm. The results illustrate the strong dependence of the polarisation mode dispersion on the fibre core ellipticity. Some special features of our measurement method and set-up resulted in an improved resolution of below ± 25 fs delay time difference.

Measurement set-up: For our measurements we used the interferometric method described by Mochizuki *et al.* (see Fig. 1 in their paper[3]). A temperature stabilised quaternary semiconductor laser, model HLD 5400 (Hitachi), emitting at 1·300 μm was used as optical source. Its spectral profile is shown in Fig. 1.

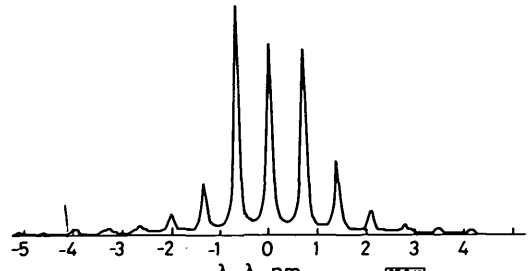

Fig. 1 *Spectral profile of laser diode used (HLD 5400)*
Operating conditions: 28·8 mA, 298 K; centre wavelength: λ_0 = 1300·0 nm