It can be proven, moreover, that if breaking the RSA scheme is hard, deriving S from (I, X, V, Y) in our scheme is difficult, and vice versa. Assume that deriving S from (I, X, V, Y) is easy. For a ciphertext $C = M^e \bmod n$, where M represents a plaintext of C, generate a random number r and put $I = C^V \bmod n$, $X = r^e/C \bmod n$ and $Y = r^V \bmod n$, then (I, X, V, Y) satisfy eqns. 1, 2 and 3, where $S = M^V \bmod n$ and $R = r/M \bmod n$. By the assumption, we get $S = M^V \bmod n$ and obtain M from $C = M^e \bmod n$ and $S = M^V \bmod n$. This contradicts the assumption that breaking the RSA scheme is hard. The proof that our schemes are secure from any attack is, however, an unsolved problem.

If an adversary guesses the correct V, he can cheat a verifier as follows. Since V is coprime to e, he can find (a, b) such that $ae - bV = 1$. He generates a random number r and calculates $\tilde{X} = r^e I^b \bmod n$ and $\tilde{Y} = r^V I^a \bmod n$, then $\tilde{X}$ and $\tilde{Y}$ satisfy eqn. 4. Therefore, when we choose e as a prime number, the probability of this forgery is $\{(1 - 1/e)\tilde{V}\}^{-1}$. Besides, if the value of $a = (bV + 1)/e$ is an integer where b is used to generate $\tilde{X} = I^b \bmod n$ and V is sent by a verifier, an adversary can cheat a verifier calculating $\tilde{Y} = I^a \bmod n$. Therefore, the probability of this forgery is $1/e$. Consequently the probability of either forgery being successful is $\{(1 - 1/e)\tilde{V}\}^{-1} + 1/e \approx 2^{-v} + 2^{-w}$, where $v = \log_2 \tilde{V}$ and $w = \log_2 e$.

Transmission efficiency: A prover and a verifier transmit $(2 \log_2 n + \log_2 \tilde{V} + \log_2 I)$ bits in the proposed identification scheme, while $(2t \log_2 n + kt + \log_2 I)$ bits are transmitted in the Fiat–Shamir scheme. In our signature scheme, a prover transmits $(2 \log_2 n + \log_2 I + \log_2 M)$ bits, while $(t \log_2 n + kt + \log_2 I + \log_2 M)$ bits are transmitted in the Fiat–Shamir scheme. The proposed schemes are, therefore, more efficient than the Fiat–Shamir schemes from the standpoint of transmitted message length, when $t \geq 2$. Note that when we use $t = 1$, we must choose a large k.

Secret memory size: Each smart card stores $\log_2 n$ bits of secret information S in our schemes, while the Fiat–Shamir schemes require $k \log_2 n$ bits of secret information. The proposed schemes are, therefore, more efficient than the Fiat–Shamir schemes from the standpoint of secret information size stored in a smart card, when $k \geq 2$.

Processing amount: We compare the amount of processing needed for our scheme versus the RSA and Fiat–Shamir schemes using the average number of modular multiplications required to generate or verify a proof of identity and authenticity.

The RSA scheme requires $(3 \log_2 n)/2$ steps, the Fiat–Shamir scheme requires $t(k + 2)/2$ steps, and our scheme requires $\{3(v + w)/2 + 1\}$ steps. To attain the same level of security (i.e. $tk = v - 1 = w - 1$), our scheme requires about six times more steps than the Fiat–Shamir scheme. For example $tk = v - 1 = w - 1 = 20$, our scheme requires 64 steps, while the Fiat–Shamir and the RSA schemes require 14 and 768 steps, respectively, where $\log_2 n = 512$, $t = 4$ and $k = 5$.

Acknowledgment: I would like to thank K. Koyama and T. Okamoto of NTT Corporation for valuable discussions.

K. OHTA

NTT Communications & Information Processing Laboratories
1-2356, Take
Yokosuka-shi, Kanagawa 238-03, Japan

11th November 1987

References

1. FIAT, A., and SHAMIR, A.: 'How to prove yourself: Practical solution to identification and signature problems'. Proceedings of Crypto-86, Santa Barbara, Aug. 1986, pp. 18-1–18-7
2. SHAMIR, A.: 'Identity-based cryptosystems and signature schemes'. Proceedings of Crypto-84, Santa Barbara, Aug. 1984, pp. 47–53
3. RIVEST, R. L., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signatures and public-key cryptosystems'. *Commun. ACM*, 1977, **21**, pp. 120–126
4. SIMMONS, G. J.: 'A "weak" privacy protocol using the RSA crypto-algorithm'. *Cryptologia*, 1983, **7**, pp. 180–182

LINEWIDTH OF SATURATED SEMICONDUCTOR LASER DIODES

Indexing terms: Lasers and laser applications, Semiconductor lasers, Diodes, Integrated optics

A theory is given for the frequency noise of saturated laser diodes having arbitrary geometry. The frequency noise is expressed in terms of integrals of the unperturbed resonating field. The formula simplifies considerably when the shot noise contribution, in addition to the spontaneous emission contribution, is taken into account. The validity of the perturbation formula used is verified by comparison with a direct exact calculation for a two-active-element electrical circuit.

A general three-dimensional formula for the product $\Delta\nu P$ of a laser diode in the unsaturated, or linear, regime, where $\Delta\nu$ denotes the full width half-power linewidth and P the total dissipated (or generated) power, has been given in Reference 1. This theory involves a longitudinal K-factor, which has been evaluated in Reference 2 for DFB lasers. In the linear regime the carrier density is independent of time, and the optical power fluctuates according to a Rayleigh distribution.

In reality, single-mode lasers exhibit above threshold very little power fluctuation. This is because the diode is current-driven and/or the series resistance in the confining layers is large. The carrier density can then react to counteract the perturbing effects of spontaneous emission.

An expression for the $\Delta\nu P$ product in the saturated regime is given in this letter. The frequency noise can be expressed in terms of integrals of the unperturbed resonating field, for any geometry and any spatial dependence of the injected current, of the gain and of Henry's α-factor,[3] for any baseband frequency. However, for the sake of brevity we consider here explicitly only the low-frequency limit when $\alpha = 0$, and when spontaneous carrier recombination can be neglected.

Frequency noise originates from spontaneous emission and from shot noise in the injected electrons and holes. In a single-active-element device,[4,5] the laser frequency is insensitive to first-order changes of the injected current, and the shot noise contribution can therefore be neglected. However, this is not the case in a multielement device, even when $\alpha = 0$ everywhere. Remarkably, the frequency noise formula that we find simplifies considerably when the shot noise contribution is taken into account.

A multielement laser theory has been proposed by Lang and Yariv.[6] This theory rests on the concept of stored energy in the various elements. While this concept is valid for high-Q coupled oscillators, we believe that it should not be used in the general case. There is therefore a basic conceptual difference between our theory and previous theories. In addition, the perturbation formula given in Reference 1, but not used earlier to our knowledge, considerably simplifies the final expressions.

For clarity, we consider electrical circuits. Generalisation to continuous media is straightforward. Let the electrical circuit consists of capacitances C_k in parallel with conductances G_k, and inductances L_k in series with resistances R_k, connected in arbitrary manner. We set $G \equiv G_p - G_a$ and $R \equiv R_p - R_a$, where G_p and R_p refer to constant passive parts that depend on the number of electrons in the element considered. Full population inversion is assumed. The subscripts k are omitted when no confusion may arise.

The isolated circuit oscillates in the steady unperturbed state at some real frequency ν_0. The voltage across C_k is denoted by V_k and the current through L_k is denoted by I_k. Since the phase reference of the oscillation is arbitrary, it may be set such that

$$\sum_k C_k V_k^2 - L_k I_k^2 \equiv A \tag{1}$$

is a real positive number.

Now let G_k and R_k be incremented by y_k and z_k, respectively. The complex change of resonant frequency $\delta\nu$ is given by the perturbation formula[1]

$$2\pi i \, \delta\nu = A^{-1} \sum_k y_k V_k^2 - z_k I_k^2 \tag{2}$$

Because the two terms in the sum of eqn. 2 are analogous, only the first will be discussed in detail.

The small admittance y consists of two parts: the Nyquist noise current $j_n \equiv c + is$, divided by $|V|$, and the conductance g expressing the reaction of the medium:

$$y = (c + is)/|V| + g \tag{3}$$

Let us now write down the carrier rate equation for each active element. Neglecting spontaneous recombination and at small frequencies, the number J/e of electrons injected per unit time in the element must equal the number of photons generated per unit time, $G_a|V|^2/2h\nu_0$. If j denotes a small increment of J and ρ the relative change of $|V|^2$, we have

$$j/J = \rho + [c/|V| + g]/G_a \tag{4}$$

where ρ is proportional to the time integral of the imaginary part of the frequency deviation; it should be considered as independent of the specific element considered.

At small frequencies, the imaginary part of the frequency deviation $\delta\nu$ must be zero; otherwise ρ would be unbounded. Thus, the real part of the sum in eqn. 2 vanishes. Inserting g from eqn. 4 into eqn. 3 and then into eqn. 2, one obtains the following expression for ρ:

$$\rho = \sum [j \cos\phi - (e|V|/2h\nu_0)s \sin\phi]/\sum J \cos\phi \tag{5}$$

where ϕ denotes either the phase of V^2, or the phase of I^2 plus π. By substituting ρ from eqn. 5 into eqn. 4 each g_k is obtained. Inserting further these g_k values into the imaginary part of the right-hand side of eqn. 2, the real frequency deviation is found to be

$$\begin{aligned} 2\pi\,\delta\nu_r = A^{-1} \sum (\cos\phi + a \sin\phi) \\ \times (s \cos\phi - c \sin\phi)|V| \\ + (2h\nu_0/e)j(a\cos\phi - \sin\phi) \end{aligned} \tag{6a}$$

$$a \equiv \sum J \sin\phi/\sum J\cos\phi \tag{6b}$$

The spectral density S of $\delta\nu_r$ follows from eqns. 6 and the spectral densities $8h\nu_0 G_a$, $8h\nu_0 G_a$ and $4eJ$ (accounting for both electrons and holes), respectively, of the uncorrelated processes $c(t)$, $s(t)$ and $j(t)$. Eqn. 6 then leads to an extremely simple result:

$$S = (2h\nu_0/\pi A)^2(I/e)(1 + a^2) \tag{7}$$

where I is the total current, and the constants A and a are expressed in terms of the unperturbed resonating fields by eqns. 1 and 6b, respectively. This formula is the same as that given in Reference 1 for unsaturated laser diodes, except for the factor $(1 + a^2)/2$, and the fact that the fields (or voltages) are the saturated fields. In a laser diode we may assume that J = constant along the diode length (z co-ordinate). It thus remains to evaluate the z-average of sin ϕ and cos ϕ, where ϕ is twice the phase of the voltage (or field) along the diode length. The latter depends on the steady-state saturation condition. The variation of the field intensity under these conditions has been reported by a number of authors, but more work is required to obtain the phase, particularly if spatial hole burning needs to be considered.

Eqns. 6 give the frequency modulation of the laser diode by setting $c = s = 0$. The result has been verified by comparison with a direct exact calculation for a two-active-element electrical circuit (one element, labelled by 1, being in parallel with the capacitance and the other, labelled by 2, in series with the inductance of an LC circuit). The approximations $j_1 \ll J_1$ and $j_2 \ll J_2$ are made only in the final result.

If the α-factors are nonzero, remarkable simplification also occurs when the shot noise contribution is added. In this letter we have mostly emphasised the concepts. The complete theory and the application to specific laser diodes requires additional algebra, but no new concepts.

J. ARNAUD

Equipe de Microoptoèlectronique de Montpellier
Unité associée au CNRS 392, USTL
Place E. Bataillon, 34060 Montpellier Cédex, France

10th November 1987

References

1 ARNAUD, J.: 'Natural linewidth of semiconductor lasers', *IEE Proc. J, Optoelectron.*, 1987, **134**, pp. 2–6
2 WANG, J., SCHUNK, N., and PETERMANN, K.: 'Linewidth enhancement for DFB lasers due to longitudinal field dependence in the laser cavity', *Electron. Lett.*, 1987, **23**, pp. 715–717
3 WESTBROOK, L. D., and ADAMS, M. J.: 'Simple expressions for the linewidth enhancement factor in direct-gap semiconductors', *IEE Proc. J, Optoelectron.*, 1987, **134**, pp. 209–214
4 LAX, M.: 'Classical noise V. Noise in self-sustained oscillators', *Phys. Rev.*, 1967, **160**, pp. 290–307
5 ARNAUD, J.: 'Role of Petermann's K-factor in semiconductor laser oscillators—a further note', *Electron. Lett.*, 1987, **23**, pp. 450–451
6 LANG, R., and YARIV, A.: 'Semiclassical theory of noise in multi-element semiconductor lasers', *IEEE J. Quantum Electron.*, 1986, **QE-22**, pp. 436–448

HIGH-SPEED 1·55 μm GaInAsP/InP DFB LASER WITH SIMPLE MESA STRUCTURE

Indexing terms: Lasers and laser applications, Semiconductor lasers, Ion beams, Etching

A new mesa structure has been developed for high-speed 1·55 μm GaInAsP/InP DFB lasers. This structure was easily fabricated using Ar ion beam etching on broad-area-contacted BH wafers. Laser parasitics were reduced by making the carrier concentration of the n-InP burying layer as low as $5 \times 10^{16}\,cm^{-3}$. A 3 dB bandwidth of 7 GHz was achieved.

Introduction: 1·55 μm distributed feedback (DFB) lasers are required to operate in a single longitudinal mode when modulated at several Gbit/s in large-capacity optical communication systems. However, there have been few reports of high-speed 1·55 μm DFB lasers,[1] even though there have been many concerned with 1·3 μm lasers.[2,3]

To achieve such high performance lasers, the following techniques are indispensable:

(i) reduction of laser parasitics

(ii) enhancement of the relaxation oscillation frequency

Technique (ii), which involves the properties of the active region itself, only becomes effective after the laser parasitics have been reduced. Conventionally, the parasitics have been reduced by using constricted mesa structures with SiO_2 stripe contacts. Such structures require quite complicated fabrication procedures and there may also be problems with adhesion of metals to the oxide films. We have developed a new, simple mesa structure, which does not require an oxide film, to reduce the laser parasitics. This was achieved by optimising the carrier concentrations of the burying layers. This letter describes high-speed 1·55 μm DFB lasers fabricated with this new structure and their DC and modulation characteristics.

Fabrication: The structure of the new mesa geometry BH (buried-heterostructure)-DFB laser is illustrated schematically in Fig. 1. An SEM view of part of this laser is also given in Fig. 2. A conventional BH structure was fabricated using liquid phase epitaxial (LPE) growth techniques.[4] A key point to realising this structure is the well controlled carrier concentration of the burying layers. We used a 1·5 μm thick p-InP blocking layer doped to $5 \times 10^{17}\,cm^{-3}$, and a 2 μm thick undoped n-InP blocking layer ($5 \times 10^{16}\,cm^{-3}$). The undoped n-InP layer, in particular, contributes greatly to reducing the junction capacitance.

The p-side electrode (AuZn/Ti/Pt/Au) is formed directly on the top layer (p^+-GaInAsP) without an oxide film. To reduce the parasitic capacitance even more, the undoped n-InP blocking layer and the p-electrode were removed simultaneously, except for a 20 μm wide stripe region which contained the active layer, connected to a 100 μm diameter circu-