pressure increases to 7 torr at 14·5 mA. At this pressure, the operating laser lines and their output powers are measured as a function of the discharge current. When the current is higher than 17 mA, the laser produces CO_2 laser radiation only. The maximum power is 0·8 W at 20 mA. When the current is lower than 15 mA, the laser produces N_2O laser radiation only. The maximum power is 0·2 W at 14·9 mA. Between these two conditions, the laser produces CO_2 and N_2O laser radiation simultaneously. The output powers are shown in Fig. 1*a* as a function of the discharge current.

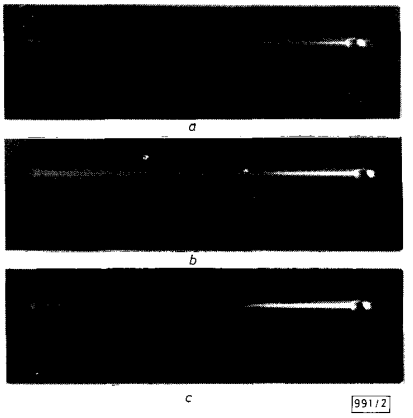

Fig. 2 *Discharge photographs according to operating lasers*
a N_2O laser only
b CO_2 and N_2O laser together
c CO_2 laser only

In another gas mixture, $CO_2 : N_2O : N_2 : He = 1 : 1·1 : 1 : 4$ at a total pressure of 4 torr, similar behaviour is obtained as shown in Fig. 1*b*. With this gas mixture, when the input current is higher than 23 mA, the laser produces CO_2 laser radiation only. When the current is lower than 19 mA, the laser produces N_2O laser radiation only. Between these two conditions the laser produces N_2O and CO_2 laser radiation simultaneously.

We attribute the cessation of N_2O laser emission output at high current to the dissociation of N_2O by collision with electrons because of its low dissociation energy: the dissociation energy of N_2O is 1·74 eV, while that of CO_2 is 5·54 eV.[2] To observe the dissociation of N_2O, we have taken photographs of the laser discharge and measured the total gas pressure in the tube at different discharge currents by fixing the gas ratio $CO_2 : N_2O : N_2 : He = 1 : 1·1 : 1 : 4$ at a initial gas pressure of 4 torr. The photographs in Fig. 2 were taken using an orange colour filter to detect oxygen, since a laser tube with oxygen radiates orange.[2] Fig. 2*a* shows the discharge when only N_2O laser radiation is produced at a current of 19 mA, Fig. 2*b* shows when CO_2 and N_2O laser radiation is produced simultaneously at 22·5 mA, and Fig. 2*c* shows when the laser produced CO_2 laser radiation only at 24 mA. The length of the bright region on the right-hand side (where the gas inlet is positioned) increases as the discharge current increases. We attribute the bright region to the dissociation of N_2O, since, at 19 mA, the total gas pressure of the laser tube is 4·5 torr, and at 26 mA the pressure is increased to 5·5 torr, although we cannot measure the fraction of dissociation of N_2O and CO_2 directly. The same phenomena have been observed with other gas mixtures.

Fig. 3 shows the CO_2 and N_2O laser output powers as a function of the He fraction ratio. Other gases are fixed at $CO_2 : N_2O : N_2 = 1 : 1 : 1$ at a total gas pressure of 4 torr. The Figure shows a decrease in the N_2O laser output as the He gas ratio increases. We have interpreted the phenomenon in the same way as above. By increasing the He pressure, the percentage of N_2O decreases more rapidly in comparison with CO_2 because of the lower dissociation energy of N_2O than of CO_2. Thus, the N_2O laser output is reduced.

Since the laser is not tuned, frequent jumps between CO_2 and N_2O laser lines occur. Thus the laser oscillates on CO_2 laser lines at 10·6 μm from P-16 to P-26 and on N_2O laser lines at 10·8 μm from P-16 to P-26. The data are an average of the power measured over 10 min.

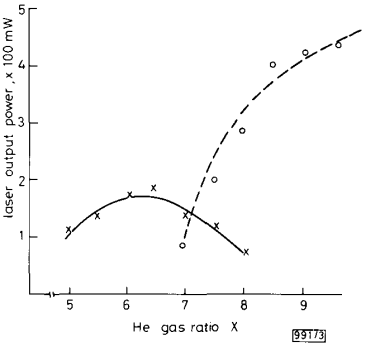

Fig. 3 *Output powers of each laser as function of He fraction at 4 torr cavity pressure, at 9·7 kV applied voltage and 15 mA discharge current*
Gas mixture is $CO_2 : N_2O : N_2 : He = 1 : 1 : 1 : X$
—— N_2O – – – CO_2

In conclusion, we have studied the conditions for the simultaneous operation of CO_2 and N_2O laser lines. The operating conditions are determined by the dissociation of the N_2O gas because of its low dissociation energy. Although this laser has not been tuned, the broad gain spectrum of this laser will make it useful for spectroscopic studies. These results will also be helpful in the study of other duolaser systems.

This study was supported by the Basic Science Research Institute Program of the Korean Ministry of Education, 1988, C. M. Kim is partially supported by the Korean Science & Engineering Foundation. We gratefully acknowledge the help of Y.-H. Min and H. l'Yee in the experiments.

C.-M. KIM
Department of Physics
Pai Chai University
439-6 Domadong, Seogu, Daejeon 302-162, Korea

S. HAN
J.-K. JI
Y. KIM
Department of Physics
Sogang University
CPO Box 1142, Seoul, Korea

2nd October 1989

References

1 NISHIHARA, H., and KRONAST, B.: 'A TE duolaser providing simultaneous lasing on CO_2 and N_2O transitions', *IEEE J. Quantum Electron.*, 1968, **QE-4**, p. 783
2 WEAST, R. C.: 'CRC handbook of chemistry and physics' (CRC Press, FL, 69th edn., 1986)

INFORMATION RATE OF McELIECE's PUBLIC-KEY CRYPTOSYSTEM

Indexing terms: Information theory, Codes and coding, Encoding

We encode messages into the error vectors in McElieces's public-key cryptosystem so that its information rate can be significantly increased, and yet do not reduce its security.

Introduction: McEliece[1] has introduced a public-key cryptosystem which is based on the technique of known error-correcting codes. So far, this cryptosystem has been

considered as secure.[2] However, this system has the drawback of low information rate, since much redundancy is needed in the required error-correcting code to remove the intentionally added error vectors. We note that the added error vectors can be designed to carry information. By introducing a low-complexity algorithm which can easily encode and decode the error vectors, we can significantly increase the information rate of the cryptosystem.

McEliece's system: Let C be a t-error-correcting (n, k) Goppa code with an easily solvable generator matrix G which is a $k \times n$ matrix. Let S be a $k \times k$ invertible scrambling matrix and P an $n \times n$ permutation matrix. We can obtain a matrix $G' = SGP$. The $k \times n$ matrix G' is the generator matrix of a linear code C', which is equivalent to C in the sense that C and C' have the same weight distribution. In McEliece's public-key cryptosystem, the matrix G' is published as the encryption key, while S, G and P are kept as the private key. The sender encrypts a k-bit message vector $\boldsymbol{u}$ into an n-bit ciphertext vector $\boldsymbol{c}$ using

$$\boldsymbol{c} = \boldsymbol{u}G' \oplus \boldsymbol{e} \tag{1}$$

where $\boldsymbol{e}$ is an arbitrary n-bit error vector of weight t chosen by the sender. The receiver computes

$$\boldsymbol{c}P^{-1} = (\boldsymbol{u}G' \oplus \boldsymbol{e})P^{-1} = [(\boldsymbol{u}S)G] \oplus [\boldsymbol{e}P^{-1}] \tag{2}$$

and uses the decoding algorithm of C to remove the vector $\boldsymbol{e}P^{-1}$ and recover the vector $\boldsymbol{u}S$. The message $\boldsymbol{u}$ is then recovered by $\boldsymbol{u} = (\boldsymbol{u}S)S^{-1}$. The security of the system is based on the selection of S and P such that it is difficult for a cryptanalyst to remove $\boldsymbol{e}P$ from $\boldsymbol{c}$ using the decoding algorithm of C'.

It is proposed that $n = 1024$ and $t = 50$[1] or $t = 37$[2] be used in the cryptosystem. For $t = 50$ and 37, the information rates are about 524/1024 and 654/1024, respectively, which are pretty low. However, we note that the $\binom{n}{t}$ distinct weighted-t error vectors can be used to carry information. It is seen that $\binom{1024}{37} > 2^{225}$ and $\binom{1024}{50} > 2^{284}$. If we can design an easily implemented encoding and decoding algorithm for the messages and the error vectors, the information rate can be around 80% or more.

Coding for constant-weight N-tuples: Suppose that we divide the set of all the $\binom{n}{t}$ weight-t n-tuples S into 2^m disjoint subsets $Y_0, Y_1, \ldots, Y_{2^m-1}$ such that $S = Y_0 \cup Y_1, \ldots, \cup Y_{2^m-1}$ and $|Y_i| - |Y_j| \leq 1$ for any i and j, where $|Y_i|$ is the cardinal number of Y_i. Let

$$2^r \leq \binom{n}{t} < 2^{r+1} \tag{3}$$

where r is an integer. If $m \leq r$, then we can encode the sth message into a randomly chosen n-tuple in Y_s for $0 \leq s < 2^m$. Then, the error vectors in McEliece's cryptosystem can be used to carry all the distinct m-bit messages.

In our algorithm, we first number the n-tuples in S as $\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{|S|-1}$ and then we assign Y_s as the set of $\boldsymbol{v}_j$, where $s = j \bmod 2^m$. Thus, we convert our problem of encoding a message into an error vector and decoding an error vector into a message to the problem of finding $\boldsymbol{v}_j$ for a given number j and finding the subscript j for a given weight-t n-tuple $\boldsymbol{v}_j$. Denote each n-tuple $\boldsymbol{v}$ by $\boldsymbol{v} = (a_0, \ldots, a_{n-1})$. We divide S into the disjoint union of two subsets $S(0)$ and $S(1)$, where $S(0)$ and $S(1)$ are the sets of n-tuples in S for which $a_0 = 0$ and $a_0 = 1$, respectively. Let $S(0) = \{\boldsymbol{v}_j\colon \boldsymbol{v}_j \in S \text{ and } 0 \leq j < \binom{n-1}{t}\}$ and $S(1) = \{\boldsymbol{v}_j\colon \boldsymbol{v}_j \in S \text{ and } \binom{n-1}{t} \leq j < \binom{n}{t}\}$. We then further divide $S(a_0)$ into the disjoint union of subsets $S(a_0, 0)$ and $S(a_1, 1)$, where $S(a_0, 0)$ and $S(a_0, 1)$ are the sets of n-tuples in $S(a_0)$ with $a_1 = 0$ and $a_1 = 1$, respectively. Let $S(0, 0) = \{\boldsymbol{v}_j\colon \boldsymbol{v}_j \in S \text{ and } 0 \leq j < \binom{n-2}{t}\}$, $S(0, 1) = \{\boldsymbol{v}_j\colon \boldsymbol{v}_j \in S \text{ and } \binom{n-2}{t} \leq j < \binom{n-1}{t}\}$, $S(1, 0) = \{\boldsymbol{v}_j\colon \boldsymbol{v}_j \in S \text{ and } \binom{n-1}{t} \leq j < \binom{n-1}{t} + \binom{n-2}{t-1}\}$ and $S(1, 1) = \{\boldsymbol{v}_j\colon \boldsymbol{v}_j \in S \text{ and } \binom{n-1}{t} + \binom{n-2}{t-1} \leq j < \binom{n}{t}\}$. Then, we continue this process of checking $a_2, a_3, \ldots$, etc. Note that $|S(a_0, \ldots, a_l)| = \binom{n-l-1}{t-w}$, where w is the number of ones in $(a_0, \ldots, a_l)$. In the case that $S(a_0, \ldots, a_l) = \{\boldsymbol{v}_j\colon \boldsymbol{v}_j \in S \text{ and } p \leq j < q\}$, we have $S(a_0, \ldots, a_l, 0) = \{\boldsymbol{v}_j\colon \boldsymbol{v}_j \in S \text{ and } p \leq j < p + \binom{n-l-2}{t-w}\}$ and $S(a_0, \ldots, a_l, 1) = \{\boldsymbol{v}_j\colon \boldsymbol{v}_j \in S \text{ and } p + \binom{n-l-2}{t-w} \leq j < q\}$. The process stops if each final subset $S(a_0, \ldots, a_f)$ contains only one n-tuple. It is clear that either $w = t - (n - f - 1)$ or $w = t$. For $l = f + 1, f + 2, \ldots, n - 1$ we assign $a_l = 1$ if $w = t - (n - f - 1)$ and assign $a_l = 0$ if $w = t$. In this way, we have a one-to-one correspondence between $(a_0, \ldots, a_{n-1})$ and the number j, where the number of ones in (a_0, a_{n-1}) equals t and $0 \leq j < n$.

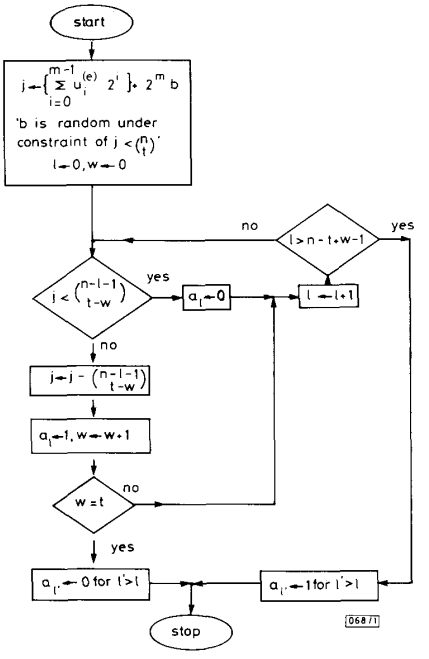

Fig. 1 *Encoding m-bit message into weight-t n-tuple*

For McEliece's cryptosystem, we write each $(k + m)$-bit message $\boldsymbol{u}$ as $\boldsymbol{u} = (\boldsymbol{u}^{(c)}, \boldsymbol{u}^{(e)})$, where $\boldsymbol{u}^{(c)}$ and $\boldsymbol{u}^{(e)}$ are k-tuple and m-tuple, respectively. Let $\boldsymbol{u}^{(e)} = (u_0^{(e)}, \ldots, u_{m-1}^{(e)})$. The ciphertext is then

$$\boldsymbol{c} = \boldsymbol{u}^{(c)}G' \oplus \boldsymbol{e} \tag{4}$$

where $\boldsymbol{e}$ is an n-tuple arbitrarily chosen from Y_s, and

$$s = \sum_{i=0}^{m-1} u_i^{(e)} 2^i \tag{5}$$

The algorithm for encoding $\boldsymbol{u}^{(e)}$ into $\boldsymbol{e}$ is shown in Fig. 1. The receiver recovers $\boldsymbol{u}^{(c)}$ and $\boldsymbol{e}$ from $\boldsymbol{c}$ as described at the beginning of this letter. The algorithm for decoding $\boldsymbol{e}$ into $\boldsymbol{u}^{(e)}$ is simply the reverse process of Fig. 1, and is omitted here. In this way, we can increase the number of information bits in McEliece's cryptosystem from k to $k + m$ without sacrificing security.

M.-C. LIN
T.-C. CHANG

Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan, Republic of China

H.-L. FU

Department of Applied Mathematics
National Chiao Tung University
Hsinchu, Taiwan, Republic of China

16th October 1989

References

1 MCELIECE, R. J.: 'A public-key cryptosystem based on algebraic coding theory'. DSN Progress Rep., Jet Propulsion Laboratory, Calif. Inst. Technol., Pasadena CA, Jan.–Feb. 1978, pp. 42–44

2 ADAMS, C. M., and MEIJER, H.: 'Security-related comments regarding McEliece's public-key cryptosystem', *IEEE Trans.*, 1989, **IT-35**, pp. 454–455

SURFACE-EMITTING LASER DIODE WITH DISTRIBUTED BRAGG REFLECTOR AND BURIED HETEROSTRUCTURE

Indexing terms: Semiconductor lasers, LEDs, Optoelectronics, Semiconductor growth

A surface-emitting laser diode (SELD) with distributed Bragg reflector (DBR) and buried heterostructure (BH) is fabricated by the metalorganic chemical vapour deposition (MOCVD), reactive ion beam etching (RIBE) and liquid phase epitaxial (LPE) regrowth techniques. An $Al_{0.1}Ga_{0.9}As/Al_{0.7}Ga_{0.3}As$ multilayer is employed for the lower reflector. The active region is embedded with $Al_{0.4}Ga_{0.6}As$ current blocking layers. The threshold current is 28 mA, and the spectral width is 2·5 Å. A 2 × 2 array is also demonstrated.

An SELD has the advantage of optoelectronic integration such as wafer-to-wafer communication and two-dimensional laser diode array structures. The use of semiconductive multilayers realises the monolithic formation of highly reflective mirrors, cladding and active layers in a single epitaxial step and reduces the fabrication processes significantly.[1,2] As the area of the active region decreases, to enclose the entire boundary of the active region by high energy bandgap cladding layers become important to ensure effective carrier confinement and subsequent low threshold current density.[3] At the same time, carrier injection should be concentrated at the centre of the optical cavity, where the optical electric field is maximum, to suppress the spontaneous emission. In this letter we realised a DBR-SELD with a BH which confines injected carriers firmly inside the active region.

Fig. 1 shows a schematic drawing and cross-sectional photograph of the SELD taken by a scanning electron microscope (SEM). The *n*-type multilayer reflector (Se-doped) and double heterostructure (DH) are grown successively on a (100)-oriented Si-doped GaAs substrate by the MOCVD technique. The *n*-type multilayer reflector comprises 30 pairs of $Al_{0.1}Ga_{0.9}As$ and $Al_{0.7}Ga_{0.3}As$ with thicknesses of 62 and 68 nm, respectively, which corresponds to a quarter optical wavelength in the materials. The maximum reflectivity of the multilayer is calculated to be 99%. The DH comprises an *n*-type $Al_{0.4}Ga_{0.6}As$ cladding layer (Se-doped, 2·1 μm), *p*-type GaAs active layer (Zn-doped, 1·45 μm), *p*-type $Al_{0.4}Ga_{0.6}As$ cladding layer (Zn-doped, 2·6 μm) and *p*-type $Al_{0.1}Ga_{0.9}As$ cap layer (Zn-doped, 0·25 μm). A silicon nitride film of thickness 100 nm is formed as the mask for the selective LPE regrowth in the next step. A cylindrical optical cavity with a diameter of 7 μm is formed by the RIBE technique.[4] Pure chlorine gas is employed for the reactive ion source. The RIBE technique realises a nearly perpendicular sidewall of the optical cavity. The etched depth is 12 μm. For the LPE regrowth it is necessary to expose the GaAs surface. This cylindrical optical cavity is embedded by *p*-type $Al_{0.4}Ga_{0.6}As$ (Ge-doped, 2–5 μm) and *n*-type $Al_{0.4}Ga_{0.6}As$ (Te-doped, 1–3 μm) current blocking layers, *p*-type $Al_{0.4}Ga_{0.6}As$ embedding layer (Ge-doped, 2–7 μm) and *p*-type GaAs cap layer (Ge-doped, 0·1–3 μm) to form the *pnp* type current blocking structure. The *n*-type AlGaAs current blocking layer, which is seen as darker in the SEM picture, is placed at the side of the active layer. The indented sidewall of the active and multilayer region is the artefact of the meltback, which is intentionally strength-

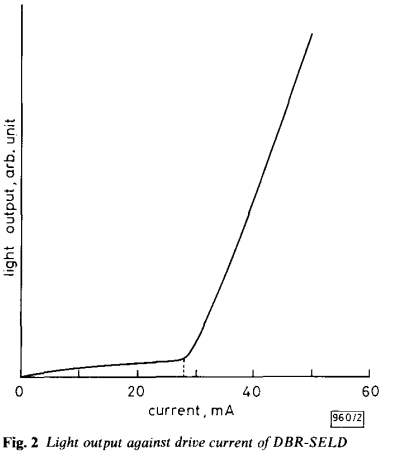

Fig. 2 *Light output against drive current of DBR-SELD*
27°C, pulsed, I_{th} = 28 mA

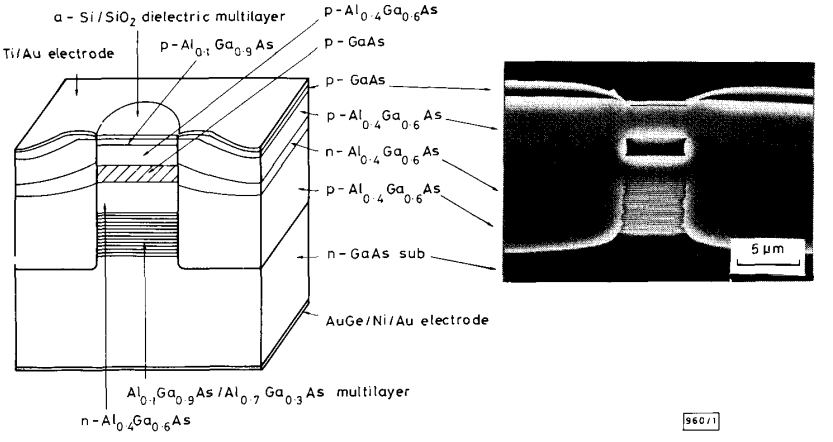

Fig. 1 *Schematic diagram of DFB-SELD with BH and cross-sectional SEM picture, after selective etching of GaAs layers by 50 : 1 (H_2O_2 : NH_4OH) for 15 s*
White parts of stripes are AlGaAs