Defect-free (denuded) zones are formed at the top layers. The removal of impurities and defects from the surface region results in an increase of surface Hall mobility. So, the mobility grains are gettered by grain boundaries. Furthermore, we assume that phosphorus atoms in grain boundaries do not act as electrically active atoms. During growth of CZ silicon, phosphorus was doped into silicon to control the resistivity of the polycrystalline layer in the annealed sample B is nearly one order of magnitude higher than that in the annealed sample A. To explain the results, we suggest a model in which substitutional phosphorus atoms in grains are gettered by grain boundaries during annealing. For a long period is effective for increasing resistivity in the polycrystalline layer and a good SOPL substrate is formed by using three-step annealing.

In this study, high-resistivity polycrystalline layers were buried beneath the surface top layers and the surface Hall mobility increased by about 25% compared with the original mobility. The high-resistivity layer beneath the top layer results in low parasitic capacitance of devices fabricated on the surface layer of the poly silicon single crystal. Parasitic capacitance and carrier mobility are the two most important material properties which affect the speed of ICs. The two material properties have been improved by using SOPL substrate for a long period is effective for increasing resistivity in the polycrystalline layer and a good SOPL substrate is formed by using three-step annealing.

In this letter we present a new probabilistic encryption algorithm which is very similar to that of Jingmin and Kaicheng. However, this new algorithm chains the cipher texts obtained by recursively encrypting two message bits at a time, with message bit expansion the same as theirs, while providing encryption and decryption operations that are twice as fast.

**2-BIT, CHAINED PROBABILISTIC ENCRYPTION SCHEME**

In this letter we present a new probabilistic encryption algorithm based on the scheme proposed by Jingmin and Kaicheng in 1988. This algorithm utilizes the public key concept and recursively encrypts two-bit at a time. The message bit expansion is very low and is the same as in their scheme. At the same time, this new scheme is twice as fast.

**Introduction:** Diffie and Hellman introduced the concept of public key cryptographic systems in their classic paper of 1976.\(^1\) Schemes to implement it quickly followed: the RSA knapsack trapdoor scheme of Rivest, Shamir, and Adelman in 1978,\(^2\) the knapsack trapdoor scheme of Merkle and Hellman in 1978,\(^3\) the knapsack trapdoor scheme of Rivest, Shamir, and Adelman in 1978,\(^4\) and finally the knapsack trapdoor scheme of Rivest, Shamir, and Adelman in 1978.\(^5\) In 1982, Goldwasser and Micali\(^6\) pointed out some basic problems with all the schemes thus far presented, and proposed a new approach called probabilistic encryption as an alternative approach which assures what they termed polynomial security. Probabilistic encryption algorithms provide that corresponding to every message there are many possible encrypted forms, not just one. The first probabilistic encryption algorithm proposed by Goldwasser and Micali\(^6\) was impractical, in that it required the encryption of every bit of message independently, thus utilising a message bit expansion of \(1/K\), where \(K\) is called the security parameter and constitutes the length of ciphertext used to represent the single bit being transmitted. Blum and Goldwasser\(^7\) proposed a more efficient probabilistic encryption scheme in which every message bit sequence was encrypted with a pseudorandom number generator. More recently Jingmin and Kaicheng\(^8\) proposed an elegant way to chain into a single cipher text a sequence of encryptions of the individual message bits of a long message string of \(L\) bits, with a low message bit expansion of \((L + (K - 1))/K\), where \(K\) is the security parameter (length of cipher text).

**2-BIT, CHAINED PROBABILISTIC ENCRYPTION SCHEME**

In this letter we present a new probabilistic encryption algorithm which is very similar to that of Jingmin and Kaicheng. However, this new algorithm chains the cipher texts obtained by recursively encrypting two message bits at a time, with message bit expansion the same as theirs, while providing encryption and decryption operations that are twice as fast.

**References**


**Theorem:** For any integer \(n = p_1 p_2\), with \(p_1\) and \(p_2\) primes of the form \(4k + 3\), and an integer \(a \in \mathbb{Q}_n\), the four square roots of \(a\) are distinguishable among four different cases as specified in any of the following ways:

- **Case (a):** root \(a \in \mathbb{Q}_n^\ast\) is a QR, and root is even
- **Case (b):** root \(a \in \mathbb{Q}_n^\ast\) is a QR, and root is odd
- **Case (c):** root \(a \in \mathbb{Q}_n^\ast\) is a QR, and root is even
- **Case (d):** root \(a \in \mathbb{Q}_n^\ast\) is a QR, and root is odd

**1432 ELECTRONICS LETTERS 12th October 1989 Vol. 25 No. 21**
primes
2-bit, chained, probabilistic encryption algorithm:

Secret key: Every user i needs to select two large distinct primes \( p_i \) and \( n_i \), with \( p_i \) and \( n_i \), of the form \( 4n + 3 \), and calculate their product \( n = p_i p_j \). \( (p_i, p_j) \) becomes user i’s secret key.

Public key: Every user i will select one parameter \( y_i \) from the region \([1, n_i - 1] \) and \( y_i \in QNR_{p_i} \cap QNR_{p_j} \). User i’s public key is then \((n, y)\).

Probabilistic encryption: Any user who wants to send binary message string \( m = m_1 m_2 \ldots m_l \) to user i, secretly, needs to access user i’s public key \((n, y)\) and randomly select a binary string \( x \) within the region \([1, n_i - 1] \) such that \((x, n_i) = 1\):

Set \( C_0 = x \)

For \( j = 1 \) to \( l \) do:

\[
C_j = C_{j-1} \mod n_i \quad \text{if} \quad m_j = 1
\]

\[
C_j = C_{j-1} \mod n_i \quad \text{if} \quad m_j = 0
\]

End

Probabilistic Decryption: Once user i receives the cipher text, he/she will start to decipher the message \( m \) in backward fashion (recursively):

Calculate \( C_l \) from \( S \) using \( d_l \):

For \( j = l \) to \( 1 \) by \(-1\) do:

\[
C_j = \begin{cases} 
S_j \pmod{n_i} & \text{if } 0 < C_{j+1} < n_i/2 \\
0 & \text{otherwise}
\end{cases}
\]

End

Security discussion: The secrecy of this algorithm is based on the difficulty of finding square roots of a quadratic residue modulo an integer which is a product of two large primes. Although by each two bits \((m_j, n_i)\) of a message, we transmit in plain text, a bit pair \((b_j, d_j)\), where \( b_j \) specifies whether a subtraction operation was applied to \( C_j \) and \( d_j \) specifies uniquely \( C_j \) as square root of \( C_{j+1} \), knowledge of \( (b_j, d_j) \) by an outsider does not reveal any information about the encrypted message bits \((m_{j+1}, n_i)\). This is due to the fact that each square root has probability \(1/2\) of being in either the first half or second half of the region \((0, n_i)\), or of being an even number or odd number. Further, these two Boolean properties are uncorrelated. It also needs to be pointed out that, given cipher text \( C_i \), any user could check the region of \( C_i \) without knowing \( p_i \) and \( p_j \) and determine the last bit \( m_l \). It is for this reason that we transmit \( S \) instead.

We need to point out here that even should a sender encrypt the same message string \( m \) repeatedly, since the sender randomly selects \( x \) as the starting binary string each time the message is sent, then the corresponding cipher text will be different each time. The bit expansion is \((K + L)/L\), where \( K \) is the security parameter and \( L \) is the length of the message.

The difference between our scheme and that of Jingmin and Kaichung is that we do not need to require that each \( C_j \) lie in the interval \((0, n_i/2)\). Being able to use the entire interval, we can encrypt two bits in the same time that it takes them to encrypt one bit. Thus, for the same message string, our encryption and decryption schemes are twice as fast as theirs.

L. HARN
T. KIESLER

Computer Science Telecommunications Program
University of Missouri
Kansas City, MO 64110, USA

References

4 RABIN, M. O.: ‘Digitalized signatures and public key functions as intractable as factorization’. MIT/LCS/TR-212, January 1979

PLASMA-HYDROGENATED LOW-THRESHOLD WIDE-BAND 1.3μm BURIED RIDGE STRUCTURE LASER

Indexing terms: Semiconductor lasers, Plasma, Semiconductor growth

The plasma hydrogenation of p-type InP has been applied to the fabrication of buried ridge structure (BRS) lasers. The threshold current, output power and modulation bandwidth of the obtained devices compare favourably with those of more conventional ones fabricated by proton implantation on the same wafer.

Introduction: The use of plasma hydrogenation for decreasing the conductivity of p-type InP by several orders of magnitude has been the object of recent reports. The physical phenomenon involved is the neutralisation of electrically active acceptors by the in-diffused hydrogen species, with the formation of hydrogen acceptor pairs. An obvious application of this effect is the realisation of electrical isolation in InP-based devices. The BRS laser technology makes use of proton implantation to enhance the output efficiency by reducing the current leaks across the InP/InP homojunction. Although proton implantation provides adequate electrical insulation, it is also likely to introduce defects which can act as non-radiative centres. In this letter we report for the first time the realisation and preliminary characterisation of high performance lasers by plasma hydrogenation instead of proton implantation.

Experimental: Fig. 1 shows the main fabrication steps of the plasma hydrogenated 1.3 μm wavelength BRS laser. This