favourable cases, namely when the line width is of the order of half the window dimensions, the accuracy of line segment orientation is within 0.4°, significantly better than that obtainable for edge segments by use of the Sobel operator. Although a full theoretical analysis is difficult, this Letter has shown that the situation is well understood, and simulations provide useful demonstrations of the properties of this type of operator.

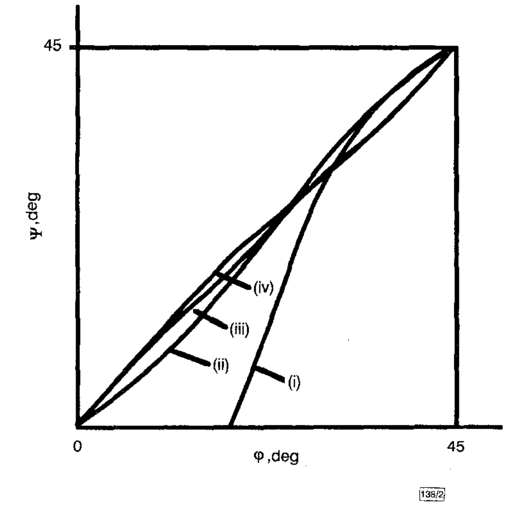

**Fig. 2** *Graphs of estimated against actual orientation*

(i) $w = 0$, $\rho = 1.0$
(ii) $w = 1.0$, $w = 1.2$
(iii) $w = 1.4$, $\rho = 0.86$
(iv) $w = 2.0$, $\rho = 0.6$
(Minimised) maximum error for w in range $1 \leq w \leq 2$ is 2.4°, and occurs for graph (ii)
Curve (iii) is accurate everywhere to within 0.4°

This work is expected to be useful in applications ranging from fingerprint analysis to document interpretation (where thin lines have to be tracked), and in many industrial inspection applications including crack, scratch and fiducial line detection Indeed, we have already applied the approach successfully to a real inspection application where much larger masks are required, and will report on this work when we have extended the theory to optimise the greatly increased numbers of mask coefficients that then occur.

*19 June 1997*
*Electronics Letters Online No: 19971219*

E.R. Davies (*Machine Vision Group, Department of Physics, Royal Holloway, University of London, Egham Hill, Egham, Surrey, TW20 0EX, United Kingdom*)

## References

1 DAVIES, E.R.: 'Machine vision: Theory, algorithms, practicalities' (Academic Press, London, 1996), 2nd edn.

2 HARALICK, R.M.: 'Edge and region analysis for digital image data', *Comput. Graph. Image Process.*, 1980, **12**, pp. 60–73

3 DAVIES, E.R.: 'Circularity – a new principle underlying the design of accurate edge orientation operators', *Image Vision Comput.*, 1984, **2**, pp. 134–142

# Cryptanalysis of 'key agreement scheme based on generalised inverses of matrices'

A.M. Youssef and S.E. Tavares

*Indexing terms: Matrix algebra, Cryptography*

The authors show that breaking the key agreement scheme proposed by Dawson and Wu is equivalent to solving a set of linear equations, hence it is insecure.

*Introduction:* Dawson and Wu [2] proposed a new key agreement scheme based on generalised inverses of matrices [1]. They suggested that for a key length of $kn$, using binary matrices of size $k \times m$, $k < m$, and $m \times n$, the security parameter is at least $2^{(m-k)n}$. In this Letter, we show that this scheme is insecure. In particular, we show that breaking this scheme is equivalent to solving a set of $m \times n$ consistent linear equations with $m^2$ binary variables.

*Definition*: Any matrix $A$ has a generalised inverse $A^-$ if and only if

$$AA^-A = A \tag{1}$$

$A^-$ is given by

$$A^- = C^{-1} \begin{bmatrix} I_r & U \\ V & W \end{bmatrix} R^{-1} \tag{2}$$

where $r$ is the rank of $A$, $I_r$ is the identity matrix of order $r$, $R$ and $C$ are such that

$$A = R \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} C \tag{3}$$

$U$, $V$ and $W$ are arbitrary matrices of the proper order. A generalised inverse which satisfies $AA^-A = A$ and $A{-}AA^- = A^-$ is called a reflexive generalised inverse of $A$. In this case, we must have $W = VU$. Note that a generalised inverse, defined by eqn. 1, always exists.

Throughout the rest of this Letter, our discussion will be on the binary field $F_2 = \{0, 1\}$. The key agreement scheme proposed in [2] is described by the authors as follows: assume that a user, Alice, wants to establish a common secret key with Bob via a public channel. They can follow the steps below:
(i) Alice randomly chooses a binary $k \times m$ matrix $A$ and an arbitrary generalised inverse $A^-$ of $A$.
(ii) Alice sends Bob $A^- A$; Alice keeps $A$ and $A^-$ secret.
(iii) Bob randomly chooses a binary $m \times n$ matrix $B$ and an arbitrary generalised inverse $B^-$ of $B$.
(iv) Bob sends Alice the matrices $A^- AB$ and $A^- ABB^-$; Bob keeps $B$ and $B^-$ secret.
(v) Alice sends Bob the matrix $AA^- ABB^- = ABB^-$.
(vi) Alice and Bob are then able to formulate the key $K = AB$, which is a $k \times n$ matrix, by computing $AA^- AB = AB$ and $ABB^- B = AB$, respectively.

Pinch [3] proposed two attacks on the above scheme. The first attack reduces the security parameter to $2^{k2}$ and the second attack, which applies to ~ 28% of the cases, reduces the security parameter to $2^{(m-k)m}m^3$. Here we show that breaking this scheme (i.e. obtaining $AB$ from public information) is equivalent to solving a set of consistent $m \times n$ linear equations with $m^2$ binary variables.

The following Lemma will be used in the attack.

*Lemma 1:* There exists at least one matrix $Y$ that satisfies the equation:

$$XBB^-YXB = XB \tag{4}$$

Proof: Take $Y = B(XB)^-$, then

$$\begin{aligned} XBB^-YXB &= X(BB^-B)(XB)^-XB \\ &= (XB)(XB)^-(XB) = XB \end{aligned} \tag{5}$$

The security argument given in [2] was based on the difficulty of solving for $A$ and $B$ given the public information $A^- A$, $A^- AB$, $A^- ABB^-$ and $ABB^-$. Here, we show that we can determine the product $AB$ without solving separately for $A$ or $B$.

*Proposed attack:* Let $X = A^- A$, then solve the linear equation:

$$(XBB^-)Y(XB) = (XB) \tag{6}$$

for the $m \times m$ matrix $Y$. By lemma 1, this equation has at least one valid solution. Note that we need to solve this equation (i.e. we cannot directly use the solution given in lemma 1 because $B$ is not known.)

Multiplying both sides of eqn. 6 by $A$ (and by noting that $AX = AA^- A = A$), we obtain

$$(ABB^-)Y(XB) = AB \tag{7}$$

Both $ABB^-$ and $XB = A^- AB$ are sent over the public channel. Hence, we can determine the secret key.

For $(k, m, n) = (7, 12, 15)$, the security parameter suggested in [2] is $2^{75}$. The attack described in this Letter obtains the key by solving a set of consistent 180 linear equations with 144 binary variables.

*Example:* Take $(k, m, n) = (3, 4, 5)$. Let

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad A^- = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \tag{8}$$

and

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \quad B^- = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{9}$$

Then, we have

$$XB = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad XBB^- = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$ABB^- = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{10}$$

Solving eqn. 6 for $Y$, we obtain 4096 distinct valid solutions. Here we give just two of them:

$$Y = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ or } Y = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{11}$$

It can be verified that

$$(ABB^-)Y(XB) = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} = AB \tag{12}$$

*Conclusion:* The key agreement scheme proposed by Dawson and Wu is insecure.

*11 August 1997*
*Electronics Letters Online No: 19971192*

A.M. Youssef and S.E. Tavares (*Department of Electrical and Computer Engineering, Queen's University, Kingston, Ontario, K7L 3N6, Canada*)

E-mail: tavares@ee.queensu.ca

## References

1 BEN-ISRAEL, A., and GREVILLE, T.N.E.: 'Generalised inverses: Theory and applications' (John Wiley and Sons, New York, 1974)

2 DAWSON, E., and WU, C.-K.: 'Key agreement scheme based on generalised inverses of matrices', *Electron. Lett.*, 1997, **33**, (14), pp. 1210–1211

3 PINCH, R.G.E.: Comments on 'Key agreement scheme based on generalised inverses of matrices', 1997 (Preprint)

# Integration of CMOS-VLSI and light emitting sources by capacitive coupling

M. Kuijk and R. Vounckx

*Indexing terms: Flip-chip devices, CMOS integrated circuits, VLSI, Light emitting devices*

A novel principle is proposed for integration of III-V light sources with CMOS VLSI circuits. The flipped III-V chip is connected to the CMOS chip by capacitive coupling instead of by a conductive connection method. Energy is transmitted through a dielectric connection layer using a high frequency carrier signal. The proposed system requires no post-processing of the CMOS circuits and offers potentially high reworkability and good coupling efficiency.

The hybridisation of CMOS VLSI with III-V components or circuits is mostly obtained by some kind of flip-chip solder bonding. This requires post-processing of CMOS chips or wafers, including a sequence of plating steps. The flip-chip soldering requires heating of both chips and is irreversible for high-density, fine-pitch connections. When connecting two substrates with different expansion coefficients (e.g. III-V and Si), difficulties arise due to shear stress. One solution to this is to remove the substrate after flipchip solder bumping leaving separate islands of detectors, light sources or modulators [1].

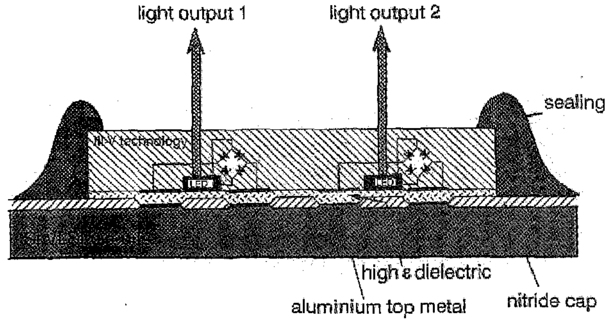

**Fig. 1** *Schematic cross-section of flipped III-V chip on Si using capacitive coupling*

Pads on both chips connect capacitively through dielectric layer

In this Letter, we propose not to separate the light sources by substrate removal, but to connect the chips using capacitive coupling, thereby allowing the chips to move laterally such that shear stress cannot build-up. Use of capacitive coupling in general was originally proposed in [2]. The capacitive coupling is intended to occur between opposing pads on the III-V chip and on the CMOS chip (Fig. 1). This is at the cost of additional processing efforts at the side of the light sources. The mechanical advantages and disadvantages of this coupling method are not yet fully explored. Although problems associated with the galvanic connection and solder are avoided, other problems may arise. Nevertheless, when using a liquid-film as the dielectric material, it is expected that the chips can glide laterally, and shear stress is avoided. The technique also bears the capacity to connect a high number of light emitters per unit area, probably in a detachable way. An alternative for the liquid as a filling material is the use of a slurry with particles of a high dielectric constant ceramic material. Finally, the system should be sealed to keep the filling material in place and to protect the assembly.

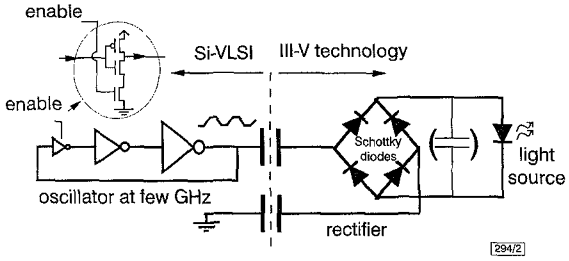

**Fig. 2** *Ring oscillator at CMOS side and rectifier (constructed with Schottky diodes) at light source side are required*

By turning oscillator on and off, current through light sources is modulated

At the CMOS side we propose to use a three stage ring-oscillator (Fig. 2) which can be turned ON and OFF, by an enable input. Analogue values at the enable input allow us to operate the oscillator as a VCO. At the reception side an oscillating current is rectified by a Schottky diode bridge (Schottky for low diffusion capacitance). These diodes need to be integrated by modification of the light source technology. For every light source, we foresee one return capacitor (connected to GND). When driving multiple light sources, one large return capacitance can be shared. The current through the light source pulsates at the oscillation frequency. The light source diffusion capacitance (in the case of driving an LED) averages this current. When driving lasers, it is beneficial