In the following, we will discuss the general form of the above signature equation to satisfy security considerations.

(i) Since x and k are two secret numbers and the verifier does not know these two values, x and k should be treated as in different terms in the above equation. Otherwise, if we combine these two secret parameters together (i.e. for example, if $xk = r+s \bmod \varnothing(p)$, then $y^k = \alpha^{r+s} \bmod p$ or $r^x = \alpha^{r+s} \bmod p$), the verifier cannot verify the signature.

(ii) To claim that s is a signature for the random public key r, the random public key r should be included in the signature equation and can be included in any parameter of (a, b, c).

(iii) To provide a digital signature, s should also be included in any parameter of (a, b, c). Thus, there are four parameters, (x, k, r, s), in the equation.

(iv) For security reasons, c cannot be zero. For example, if $rx = sk \bmod \varnothing(p)$, it is easy to forge a signature for a random public key to satisfy the verification $y^r = r^s \bmod p$. This can be shown by randomly selecting a $u \in [1, p-2]$ and computing $r' = y^u \bmod p$. The forged signature for the random r' is $s' = y^u u^{-1} \bmod p-1$.

(v) For security reasons, r cannot be combined with s. For example, if $x = k + rs \bmod \varnothing(p)$, it is easy to forge a signature for a random public key to satisfy the verification $y = r\alpha^{rs} \bmod p$. This can be shown by randomly selecting an $r' \in [1, p-2]$ and computing $r'' = y\alpha^{-r'} \bmod p$. The forged signature for the random r'' is $s'' = r'r''^{-1} \bmod p-1$.

(vi) The signature equation contains four parameters. Two parameters, (r, s), are public information. But, x is the fixed secret key of the signer and k is a random secret value for each random public key. Since the number of secret parameters is always one larger than the number of linear equations available to the attacker, the signature scheme is secure based on the discussion in the original ElGamal paper. We list all possible signature variations in Table 1.

Table 1: All possible signature variations

	Signature	
	Equation	Verification
(i)	$rx = k+s \bmod \varnothing(p)$	$y^r = r\alpha^s \bmod p$
(ii)	$sx = k+r \bmod \varnothing(p)$	$y^s = r\alpha^r \bmod p$
(iii)	$x = rk+s \bmod \varnothing(p)$	$y = r^r\alpha^s \bmod p$
(iv)	$x = sk+r \bmod \varnothing(p)$	$y = r^s\alpha^r \bmod p$

Discussion:

(i) Among all signature schemes we have listed in Table 1, the signature generation only requires us to solve a linear equation. The signature verification requires two modular exponentiations. In schemes (i) and (iii), the signature s can be solved without computing the inverse. More important than the efficiency is that these signature schemes are not relied on any one-way hash function.

(ii) The techniques used in the DSA [7] and the Schnorr scheme [8] can also be applied to all schemes in the table to shorten the signature and to speed up computation.

Conclusion: We have proposed signature schemes which are especially suitable for signing the Diffie-Hellman public keys. Using these schemes to sign Diffie-Hellman public keys, they do not require any one-way hash function and are very efficient in signature generation and signature verification.

© IEE 1997 *8 October 1996*
Electronics Letters Online No: 19970071

L. Harn (*Department of Computer Networking, University of Missouri, Kansas City, MO 64110, USA*)

References

1 BOYD, C.: 'Comment: New digital signature scheme based on discrete logarithm', *Electron. Lett.*, 1994, **30**, (6), pp. 480–481

2 NYBERG, K.: 'Comment: New digital signature scheme based on discrete logarithm', *Electron. Lett.*, 1994, **30**, (6), pp. 481

3 DOBBERTIN, H.: 'The status of MD5 after a recent attack', *CryptoBytes*, 1996, **2**, (2), pp. 1–6

4 DIFFIE, W., and HELLMAN, M.E.: 'New directions in cryptography', *IEE Trans.*, 1976, **IT-22**, (6), pp. 644–654

5 ARAZI, A.: 'Integrating a key cryptosystem into the digital signature standard', *Electron. Lett.*, 1993, **29**, (11), pp. 966–967

6 NYBERG, K., and RUEPPEL, R.A.: 'Message recovery for signature schemes based on the discrete logarithm problem'. Proc. Eurocrypt '94, May 1994, pp. 175–190

7 'The digital signature standard', *Comm. ACM*, 1992, **35**, (7), pp. 36–40

8 SCHNORR, C.P.: 'Efficient identification and signatures for smart cards'. Advance in Cryptology - CRYPTO'89, Santa Barbara, 20–24 Aug. 1989, (Springer-Verlag), pp. 239–252

Optimum source-to-channel assignment

A.K. Khandani

Indexing terms: Channel coding, Source coding

The problem of the optimum assignment of a set of source symbols to a set of channel symbols is expressed in terms of a quadratic assignment problem (QAP). Numerical examples are presented for the assignment of a scalar quantiser to a binary channel.

Consider a communication system aimed at transmitting a source **S** through a channel **C**. The source **S** has T symbols, $\mathbf{s}_i$, $i = 0, ..., T-1$, where $\mathbf{s}_i$ occurs with probability $P_s(i)$. The distortion between $\mathbf{s}_i$, $\mathbf{s}_j \in \mathbf{S}$ is equal to $D_s(i,j)$. The channel **C** has T symbols $\mathbf{c}_i$, $i = 0, ..., T-1$. The probability of receiving a channel symbol j conditioned on transmitting a channel symbol i is equal to: $P_c(j|i)$. The objective is to select a one-to-one mapping ξ between the set of the source symbols and the set of the channel symbols to minimise the end-to-end average distortion, namely

$$D_{ave} = \sum_{i=0}^{T-1}\sum_{j=0}^{T-1} P_s(i)P_c[j|\xi(i)]D_s[i,\xi^{-1}(j)]$$

We assign a T dimensional binary vector to each symbol of the source at the channel input. The vector corresponding to the ith symbol is composed of the elements: $[x_{ij}, j = 0, ..., T-1]$. If the ith source symbol is assigned to the lth channel symbol, we set $x_{ij} = 1$ for $j = l$ and $x_{ij} = 0$ for $j \neq l$. Using these notations, the assignmemt problem is formulated as

$$\begin{aligned} \text{minimise} \; & \sum_{i=0}^{T-1}\sum_{j=0}^{T-1}\sum_{k=0}^{T-1}\sum_{l=0}^{T-1} P_s(i)P_c(l|j)D_s(i,j)x_{ij}x_{kl} \\ \text{subject to:} \; & x_{ij} \in \{0,1\} \quad i,j = 0,...,T-1 \qquad (1) \\ & \sum_{j=0}^{T-1} x_{ij} = 1 \quad i = 0,...,T-1 \\ & \sum_{i=0}^{T-1} x_{ij} = 1 \quad j = 0,...,T-1 \end{aligned}$$

The optimisation scheme in eqn. 1 is equivalent to a standard problem of discrete optimisation known as a quadratic assignment problem (QAP) [3, 4]. This problem arises in discrete locational problems with mutual interaction between facilities. QAPs are known to be NP-hard and are generally very difficult to solve. The exact solution methods are mainly based on either finding an integer programming formulation for the problem or using the method of the branch and bound. There are also numerous works discussing different heuristic approaches to approximate the optimum solution [3, 4].

Tables 1 and 2 contain numerical results for the optimum assignment of the levels of a scalar Max quantiser [5] to the symbols of a binary channel. The distortion measure is the mean square distance. The corresponding QAP is solved using the branch and bound algorithm. A supplementary technique (known as reduction) is used which allows us to decompose the objective function of the QAP as the sum of a linear term and a quadratic term. The main strategy in computing lower bounds for a QAP (as required in the branch and bound method) is based on minimising the linear term and replacing the quadratic term by a lower bound

Table 1: Optimum and worst index assignment for 3 bit Max quantisation of source with uniform, Laplacian and Gaussian distributions

Uniform	Optimum	000	001	010	011	100	101	110	111
	Worst	000	011	101	110	111	100	010	001
Laplacian	Optimum	000	001	010	011	111	110	101	100
	Worst	000	011	111	100	010	001	101	110
Gaussian	Optimum	000	001	010	011	111	110	101	100
	Worst	000	011	101	110	100	010	001	111

Table 2: Degradation in D_{ave} (denoted as Loss) for different sub-optimum assignment rules (with respect to optimum rule) for 3 bit Max quantisation of sources with uniform, Laplacian and Gaussian distributions, P_b indicates probability of bit error

Uniform			Laplacian			Gaussian		
P_b	Mapping	Loss [dB]	P_b	Mapping	Loss [dB]	P_b	Mapping	Loss [dB]
10^{-3}	natural	0.0	10^{-3}	natural	2.25	10^{-3}	natural	0.81
10^{-3}	grey	1.09	10^{-3}	grey	0.93	10^{-3}	grey	0.27
10^{-3}	worst	4.41	10^{-3}	worst	4.53	10^{-3}	worst	4.00
10^{-2}	natural	0.0	10^{-2}	natural	2.21	10^{-2}	natural	0.80
10^{-2}	grey	1.07	10^{-2}	grey	0.91	10^{-2}	grey	0.26
10^{-2}	worst	4.33	10^{-2}	worst	4.45	10^{-2}	worst	3.91
10^{-1}	natural	0.0	10^{-1}	natural	1.84	10^{-1}	natural	0.66
10^{-1}	grey	0.87	10^{-1}	grey	0.72	10^{-1}	grey	0.20
10^{-1}	worst	3.60	10^{-1}	worst	3.70	10^{-1}	worst	3.24

thereof. To increase the efficiency, the reduction rule is selected to enhance the relative effect of the linear term with respect to the quadratic term. The minimisation of the linear term reduces to a linear assignment problem (LAP) which can be easily solved using the method explained in [6].

Acknowledgment: This work was supported by Natural Sciences and Engineering Research Council of Canada (NSERC).

© IEE 1997 *8 October 1996*
Electronics Letters Online No: 19970072

A.K. Khandani (*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada*)

References

1 DE MARCA, J.R.B., and JAYANT, N.S.: 'An algorithm for assigning binary indices to the code-vectors of a multi-dimensional quantizer'. Proc. IEEE Int. Commun. Conf., Seattle, WA, June 1987, pp. 1128–1132

2 FARVARDIN, N.: 'A study of vector quantization for noisy channels', *IEEE Trans. Inform. Theory*, 1990, **36**, pp. 799–809

3 FINKE, G., BURKARD, R.E., and RENDL, F.: 'Quadratic assignment problems', *Ann. Discrete Math.*, 1987, **31**, pp. 61–82

4 BURKARD, R.E.: 'Locations with spatial interactions: The quadratic assignment problem', *in* MIRCHANDANI, P.B., and FRANCIS, R.L. (Eds.): 'Discrete location theory' (John Wiley, 1991)

5 MAX, J.: 'Quantizing for minimum distortion', *IEEE Trans. Inform. Theory*, 1960, pp. 7–12

6 KERKÓ, B.: 'Linear programming' (Pitman & Sons Ltd., 1968)

Harmonic distortion due to output conductance in SI cells

J. Martins and V. Dias

Indexing terms: Integrated circuits, Switched current circuits, Harmonic distortion

A closed-form equation for the effect of the output conductance on the harmonic distortion in switched-current basic memory cells is presented here. The authors show that in memory cells with short channel transistors, the variation of the output conductance can generate high levels of harmonic distortion (–51dB for L = 2μm using a 1.2μm CMOS technology); however a suitable relation of transistor lengths can lead to very low distortion levels. The results are confirmed both by simulation and measurements on an IC prototype.

Introduction: The need for analogue techniques suitable for single poly technologies (usually referred to as digital technologies), together with the need for lower supply voltages and higher speed has led to the development of the switched-current (SI) technique [1].

In SI circuits, harmonic distortion is a major source of concern, and several authors refer to it as the main cause of the mismatch between the threshold voltages in the current mirrors [2], clock feedthrough [2], and nonlinear settling [3]. We have found that an important cause of distortion that has been overlooked is the variation of the output conductance with signal level.

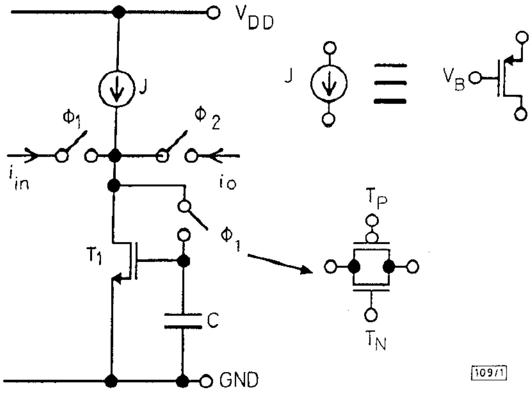

Fig. 1 *Second generation SI memory cell*

Theoretical study: The basic second generation SI memory cell [4] is represented in Fig. 1 (the results to be obtained also apply to the first generation memory cell [1]). A transistor in saturation has $i_D = K(v_{GS}-V_t)^2(1+\lambda v_{DS})$ and can be represented by an equivalent circuit consisting of an 'ideal' transistor with $\lambda = 0$ with a conductance G_o connected between drain and source, which is a function of the signal (and not only of the bias current):

$$G_o(t) \simeq \lambda i_D(t) \tag{1}$$

We represent a variable x at the end of the acquisition phase ϕ_1, as $x(\phi_1)$ and in the hold phase ϕ_2, as $x(\phi_2)$; if the difference between $x(\phi_1)$ and $x(\phi_2)$ is only of second order, the phase is not indicated. The current error is defined as

$$i_\varepsilon(\phi_2) = i_o(\phi_2) - i_{in}(\phi_1) \tag{2}$$

It is possible to show that it can be written as

$$i_\varepsilon = [G_{oJ} + G_{o1} + g_{m1}\theta][v_{DS1}(\phi_2) - v_{DS1}(\phi_1)] \tag{3}$$

where

$$\theta = C_{dg1}/(C_{dg1} + C_{gs1} + C) \tag{4}$$

is related to the feedback from v_{DS1} to v_{GS1} via the parasitic capacitances C_{dg1} of T_1. We note that $G_{oJ} \simeq \lambda_J J$, $G_{o1} \simeq (J+i_{in}(\phi_1))$, $g_{m1} \simeq 2\sqrt{\{K_1(J+i_{in}(\phi_1))\}}$ and $V_{DS1}(\phi_1) = v_{GS1}(\phi_1) \simeq \sqrt{\{(J+i_{in}(\phi_1))/K_1\}} + V_t$. Assume that during ϕ_2, the cell is connected to a similar cell in the acquisition mode with transistor T_2, $V_{DS1}(\phi_2) = v_{DS2}(\phi_2) = v_{GS2}(\phi_2) \simeq \sqrt{\{(J-i_{in}(\phi_1))/K_2\}} + V_t$.

Although i_ε is a discrete-time variable, it is convenient to consider that it is the sampled version of a continuos-time variable $i_\varepsilon(t)$. If $K_1 = K_2 = K$, $m_i = i_{in}(\phi_1))/J$, and $\Delta V = \sqrt{\{J/K\}}$ is the overdrive voltage, we can write eqn. 3 as

$$i_\varepsilon(t) \simeq \left[\lambda_1 J(1+m_i) + \lambda_J J + 2\theta\sqrt{KJ}\sqrt{1+m_1}\right] \times \Delta V\left(\sqrt{1-m_i} - \sqrt{1+m_i}\right) \tag{5}$$

If we consider that $\sqrt{\{1+m_i(t)\}} \simeq 1+m_i(t)/2-m_i^2(t)/8$, and assume that $m_i = M_{im}\cos\omega t$, the amplitude of the second harmonic relative to the amplitude of the input signal is

$$\varepsilon_{2\omega} \simeq \frac{3\lambda_1 \Delta V M_{im}}{8} - \frac{\lambda_J \Delta V M_{im}}{8} + \frac{\theta M_{im}}{4} \tag{6}$$

Since $\varepsilon_{2\omega}$ has both positive and negative terms, it is possible to have no harmonic distortion if the lengths of T_1 and T_J are related: for instance, if L_J = 2μm, ΔV = 0.7V, and M_{im} = 0.5, we find that for L_1 = 8μm, there is almost no harmonic distortion (–81 dB). However, if short length transistors are used, distortion levels as high as –51 dB can be obtained.