sponding OTA-C circuits and join them together with the cross-cascade interconnection. Fig. 3*b* shows the same completed circuit, suitable for any transfer function, and it employs only seven identical OTAs and grounded capacitances. The required numbers of OTAs in Fig. 3*b* are less than those in previous works [2–5], and a comparison of the numbers of OTAs and capacitors used in our work and other works is shown in Table 1. Fig. 3*b* is experimentally verified by using the bipolar OTAs LM13600 [6] along with discrete capacitors. Here, we use the R-C pole-zero compensation, also shown in Fig. 3*b*, to reduce the high quality factor Q of the complex pole at node A [7]. Its amplitude response is shown in Fig. 4. The deviations between the theoretical and experimental curves are specified by the input and output impedances of the LM13600.

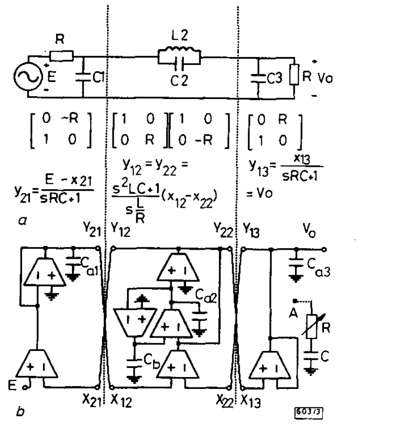

Fig. 3 *Third-order LC filter prototype and its transformation matrices and design equations, and corresponding OTA-C filter derived from proposed design tables*

a Third order LC filter
b Corresponding OTA-C filter

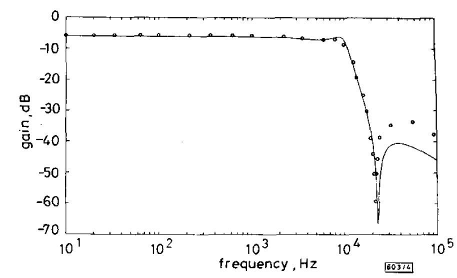

Fig. 4 *Amplitude response of Fig. 3b*

Conclusions: Systematic and effective design tables for simulating high-order LT OTA-C filters are presented. According to these design tables, we can realise filters with minimum numbers of OTAs and grounded capacitors. It is a powerful method for realising high-order filters.

9 September 1994
Electronics Letters Online No: 19941318

Y.-S. Hwang, S.-I. Liu, D.-S. Wu and Y.-P. Wu (*Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 10664, Republic of China*)

References

1 DIMOPOULOS, H.G., and CONSTANTINIDES, A.G.: 'Linear transformation active filters', *IEEE Trans.*, 1978, **CAS-25**, (10), pp. 845–852

2 DE QUEIROZ, A.C.M., CALOBA, L.P., and SANCHEZ-SINENCIO, E.: 'Signal flow graph OTA-C integrated filters'. Proc. IEEE ISCAS, 1988, pp. 2165–2168

3 CALOBA, L.P., and DE QUEIROZ, A.C.M.: 'OTA-C simulation of passive filters via embedding'. Proc. IEEE ISCAS, 1989, pp. 1083–1086

4 CALOBA, L.P., DE QUEIROZ, A.C.M., and SANCHEZ-SINENCIO, E.: 'Signal flow graph OTA-C band-pass and band-reject integrated filters'. Proc. IEEE ISCAS, 1989, pp. 1624–1627

5 ANADA MOHAN, P.V.: 'Novel OTA-C filter structures using grounded capacitors'. Proc. IEEE ISCAS, 1991, pp. 1347–1350

6 National Semiconductor Corporation, 'Linear data book', 1982

7 DE QUEIROZ, A.C.M., and CALOBA, L.P.: 'Some practical problems in OTA-C filters related with parasitic capacitances'. Proc. IEEE ISCAS, 1990, pp. 2279–2282

Voltage-mode notch, lowpass and bandpass filter using current-feedback amplifiers

C.-M. Chang, C.-S. Hwang and S.-H. Tu

Indexing terms: Active filters, Current-mode circuits

A voltage-mode filter employing three current-feedback amplifiers, two grounded capacitors and three floating resistors is presented. The proposed circuit offers the following advantages: realisation of notch, lowpass and bandpass signals from the same configuration, no requirements for component matching conditions, orthogonal control of ω_o and Q, and the use of two grounded capacitors ideal for IC implementation, and low active and passive sensitivities and cascadability.

Introduction: The applications and advantages in the realisation of various active filter transfer functions using current conveyors have received a considerable amount of attention [1]. A current-feedback amplifier (CFA) which is now available in integrated circuit form is equivalent to a plus-type second-generation current conveyor with a voltage buffer [2]. Recently, some filtering amplifiers with high performance, such as essentially extended bandwidths and high values for the slew rates, were proposed by using current-feedback amplifier(s) [3–5]. First, in 1992, Fabre proposed a voltage-mode highpass and bandpass filter using two CFAs, one grounded capacitor and one floating capacitor [3]. Then, in 1993, Fabre proposed a voltage-mode bandpass and highpass/lowpass filter using one single CFA, one grounded capacitor and one floating capacitor in which highpass and lowpass signals cannot be directly connected to the next stage because the output impedance of these two signals does not approach zero [4]. Liu and Hwang proposed a voltage-mode lowpass/bandpass filter using one single CFA, one grounded capacitor and one floating capacitor [5]. In this Letter, the author proposes a voltage-mode notch, lowpass and bandpass filter employing three CFAs and two grounded capacitors. Critical component matching conditions/cancellation constraints are not required in the design. The employment of grounded capacitors makes the proposed circuit suitable for integrated-circuit implementation [6, 7]. The output impedance of the proposed circuit is very small, so the proposed circuit is cascadable.

Circuit description: The proposed network, based on and employing the current-feedback amplifier (CFA), is shown in Fig. 1. Using standard notation, the port relations of a CFA can be characterised by [5] $v_x = v_y$, $v_o = v_z$, $i_z = i_x$ and $i_y = 0$. In Fig. 1, two grounded capacitors are employed in the design. The use of grounded capacitors is particularly attractive for integrated-circuit implementation [6, 7]. Because the output impedance of terminal V_o approaches zero, the three output terminals, V_{o1}, V_{o2} and V_{o3}, can be directly connected to the next stage, respectively. The voltage transfer functions for the network of [1] are given by the following equations:

$$\frac{V_{o1}}{V_{in}} = \frac{s^2C_1C_2G_1 + G_1G_2G_3}{s^2C_1C_2G_1 + sC_2G_2G_3 + G_1G_2G_3} \qquad (1)$$

$$\frac{V_{o2}}{V_{in}} = \frac{G_1G_2G_3}{s^2C_1C_2G_1 + sC_2G_2G_3 + G_1G_2G_3} \quad (2)$$

and

$$\frac{V_{o3}}{V_{in}} = \frac{-sC_2G_1G_2}{s^2C_1C_2G_1 + sC_2G_2G_3 + G_1G_2G_3} \quad (3)$$

Thus, the circuit realises a noninverting notch signal at V_{o1}, a noninverting lowpass signal at V_{o2} and an inverting bandpass signal at V_{o3}. Component matching conditions are not required in the design.

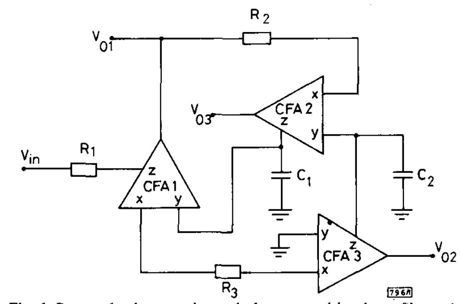

Fig. 1 *Proposed voltage-mode notch, lowpass and bandpass filter using three current-feedback amplifiers*

Taking into account the nonidealities of a CFA, namely, $i_z = \alpha i_x$, $v_x = \beta v_y$ and $v_o = \gamma v_z$ where $\alpha = 1-e_i$ and $e_i(>1)$ denotes the current tracking error, $\beta = 1-e_v$ and $e_v(>1)$ denotes the input voltage tracking error and $\gamma = 1-e'_v$ and $e_v(>1)$ denotes the output voltage tracking error. The resonance angular frequency ω_o and quality factor Q are given by

$$\omega_o = (G_2G_3/C_1C_2)^{1/2}(\alpha_2\alpha_3\beta_1\beta_2)^{1/2} \quad (4)$$

and

$$Q = G_1(C_1/C_2G_2G_3)^{1/2}(1/\alpha_1\gamma_1)(\alpha_3\beta_2/\alpha_2\beta_1)^{1/2} \quad (5)$$

Note that ω_o and Q are orthogonally adjustable. The sensitivities of ω_o and Q to active and passive components are

$$S^{\omega_o}_{\alpha_2,\alpha_3,\beta_1,\beta_2} = 1/2 = S^Q_{\alpha_3,\beta_2} = -S^Q_{\alpha_2,\beta_1} \qquad S^Q_{\alpha_1,\gamma_1} = -1$$
$$S^{\omega_o}_{G_2,G_3} = -S^{\omega_o}_{C_1,C_2} = 1/2 \quad S^Q_{C_2,G_2,G_3} = -S^Q_{C_1} = -1/2$$
$$\text{and} \quad S^Q_{G_1} = 1$$

all of which are small.

Finally, to verify the theoretical prediction of the proposed network, a lowpass filter prototype has been realised with discrete components. The experimental network in Fig. 1 was built with $R_1 = R_2 = R_3 = 10\text{k}\Omega$, and $C_1 = C_2 = 1\text{nF}$. Three commercial CFAs (AD844s) were used. The measured frequency response of the lowpass filter shown in Fig. 2 agrees well with theory.

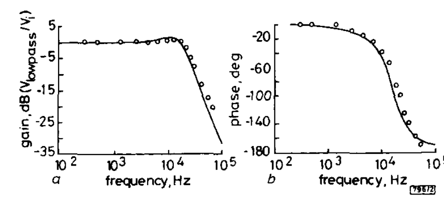

Fig. 2 *Amplitude-frequency response and phase-frequency response*

a Amplitude-frequency
b Phase-frequency

——— ideal response
O measured response

Conclusions: In this Letter, three current-feedback amplifiers, two grounded capacitors and three floating resistors are employed to construct a voltage-mode notch, lowpass and bandpass filter in which the CFA-based notch filter is proposed for the first time. The new filter offers the following advantageous features:

(i) realisation of notch, lowpass and bandpass signals from the same configuration

(ii) no requirements for critical component matching conditions

(iii) orthogonal adjustment of ω_o and Q

(iv) use of only two grounded capacitors which makes the circuit suitable for integrated-circuit implementation

(v) small active and passive sensitivities

(vi) very low output impedance which makes the voltage-mode circuit cascadable.

28 September 1994
Electronics Letters Online No: 19941416

C.-M. Chang, C.-S. Hwang and S.-H. Tu (*Dept. of Electrical Engineering, Chung Yuan Christian University, Chung-Li, Taiwan 32023, Republic of China*)

References

1 WILSON, B.: 'Recent developments in current conveyors and current-mode circuits', *IEE Proc. G*, 1990, **137**, (2), pp. 63–77
2 SVOBODA, J.A., MCGORY, L., and WEBB, S.: 'Applications of a commercially available current conveyor', *Int. J. Electron.*, 1991, **70**, (1), pp. 159–164
3 FABRE, A.: 'Gyrator implementation from commercially available transimpedance operational amplifiers', *Electron. Lett.*, 1992, **28**, (3), pp. 263–264
4 FABRE, A.: 'Insensitive voltage-mode and current-mode filters from commercially available transimpedance opamps', *IEE Proc. G*, 1993, **140**, (5), pp. 319–321
5 LIU, S.J., and HWANG, Y.S.: 'Realisation of R-L and C-D impedances using a current feedback amplifier and its applications', *Electron. Lett.*, 1994, **30**, (5), pp. 380–381
6 BHUSAN, M., and NEWCOMB, R.W.: 'Grounding of capacitors in integrated circuits', *Electron. Lett.*, 1967, **3**, pp. 148–149
7 PAL, K., and SINGH, R.: 'Inductorless current conveyor allpass filter using grounded capacitors', *Electron. Lett.*, 1982, **18**, pp. 47

Construction of dynamic threshold schemes

H.-M. Sun and S.-P. Shieh

Indexing term: Cryptography

An (m, n) threshold scheme is to decompose a shared secret into n shares in such a way that the shared secret cannot be reclaimed unless any m shares are collected. A new dynamic threshold scheme that allows the shared secret to be updated without changing the shares is proposed.

Introduction: In 1979, Blakley and Shamir [1, 2] introduced the concept of threshold schemes which are mainly used to protect the master key of a secure system from being lost, destroyed and modified. The main idea underlying an (m, n) threshold scheme is to divide the shared secret (master key) K into n shares S_is $(1 \le i \le n)$ in such a way that the shared secret K cannot be reclaimed unless m shares are collected. The security of a threshold scheme is classified into two levels: information theoretic security (perfect security) and computational security [3]. A threshold scheme is perfectly secure if any $m-1$ or less shares provide no information about the shared secret K [4], and it is computationally secure if for any $m-1$ or less shares it is computationally infeasible to determine the shared secret K in polynomial time [5].

In conventional threshold schemes, the corresponding shares must be updated accordingly when the shared secret is renewed. It is time-consuming and inconvenient if the shares need be changed frequently, especially when the number n of the shares is large. In