Conclusions: The insight gained from our limit theorem is that if any n phase Barker sequences of length L exists with $L > 31$, it is very likely that there are infinite number of them. This is a desirable result, which seems to have added some extra significance to the most challenging problem: 'Does a uniform Barker sequence exist for every length?'. There is currently no evidence against a positive answer.

Friese and Zottmann's discovery of Barker sequences of length 31 provided a counter-example to the conjecture of Zhang and Golomb that Barker sequences do not exist for $L > 30$. More importantly, their search experiences give hope for the existence of even longer Barker sequences.

From [3], it can be observed that the minimum alphabet size for which a Barker sequence exists grows rapidly with the sequence length. This is clearly why those exhaustive or partial searches, (e.g. see [3]) which started with a fixed alphabet size, failed to discover any result. On the other hand, the approach of stochastic optimisation algorithms attempts to obtain a solution in the continuous-space so that an infinite alphabet size is implicitly assumed. Thus there is a better chance of obtaining a result in spite of the rapid growth of the minimum alphabet size. Nonetheless, the multimodal nature of this search problem will eventually make this approach impractical. It is thus clear that the analytical approach is the only way out.

Acknowledgment: The author wishes to acknowledge the financial support of the Humboldt Foundation Fellowship 1996.

9 May 1996
Electronics Letters Online No: 19960944

W.H. Mow (*Lehrstuhl für Nachrichtentechnik, Technische Universität München, Arcisstrasse 21, D-80290 München, Germany*)

References

1 ZHANG, N., and GOLOMB, S.W.: 'A limit theorem for n-phase Barker sequences', *IEEE Trans. Info. Theory,* 1990, **IT-36**, pp. 863–866
2 GOLOMB, S.W., and SCHOLTZ, R.A.: 'Generalised Barker sequences', *IEEE Trans. Info. Theory,* 1965, **IT-11**, pp. 533–537
3 ZHANG, N., and GOLOMB, S.W.: 'Sixty-phase generalised Barker sequences', *IEEE Trans. Info.. Theory,* 1989, **IT-35**, pp. 911–912
4 ZHANG, N., and GOLOMB, S.W.: 'Uniqueness of the generalised Barker sequences of length 6', *IEEE Trans. Info.. Theory,* 1990, **IT-36**, pp. 1167–1170
5 ZHANG, N., and GOLOMB, S.W.: 'Polyphase sequence with low autocorrelations', *IEEE Trans. Info.. Theory,* 1993, **IT-39**, pp. 1085–1088
6 BÖMER, L., and ANTWEILER, M.: 'Polyphase Barker sequences', *Electron. Lett.,* 1989, **25**, (23), pp. 1577–1579
7 FRIESE, M., and ZOTTMANN, H.: 'Polyphase Barker sequences up to length 31', *Electron. Lett.,* 1994, **30**, (23), pp. 1930–1931

Parallel computation of the generating keys for RSA cryptosystems

C.-C. Chang and M.-S. Hwang

Indexing terms: Public key cryptography, Number theory

The authors present a parallel implementation for generating RSA keys without using the Euclidean algorithm. Their method is based on a unique factorisation theorem, which combines with Derôme's method and allows the generation of RSA keys without using the Euclidean algorithm.

Introduction: The RSA system [1] is one of the most popular asymmetric cryptosystems and offers high security and easy implementation. In the RSA cryptosystem, the plaintext M is encrypted by the following formula:

$$C = M^e \bmod N \tag{1}$$

where e denotes a public key (or enciphering key), $N = pq$, p and q are large strong primes. In turn the ciphertext C can be decrypted by the following formula:

$$M = C^d \bmod N \tag{2}$$

where d denotes a secret key (or deciphering key). Note that, in order to satisfy eqn. 2:

$$ed \bmod s = 1 \tag{3}$$

where s denotes a Euler totient function of N. We now seek a pair of keys (e, d) that satisfy eqn. 3. One of the solutions can be obtained using the extended Euclidean algorithm [2]. The other solution is obtained as follows: choose an e such that $gcd(e, s) = 1$, and then compute the inverse of e using the following equation:

$$d = e^{-1} \bmod s \tag{4}$$

$$= e^{\phi(s)-1} \bmod s \tag{5}$$

Obviously, it is very time consuming to compute the above equation because the value of s is usually very large.

Recently, Derôme proposed an efficient method which does not involve the Euclidean algorithm. We extend Derôme's method to implement a parallel computation of the generating keys for an RSA cryptosystem.

Review of Derômes method: Since our method is inspired by Derôme's method, we first review his method in brief. Eqn. 3 implies that an integer $j > 0$ exists such that

$$de - js = 1 \tag{6}$$

From Derôme's method, the secret key can he generated without the Euclidean algorithm as follows:

$$d = 1 + j\left\lfloor \frac{s}{e} \right\rfloor + [j(s \bmod e)] \bmod (e-1) \tag{7}$$

and

$$j = (-s^{\phi(e)-1}) \bmod e \tag{8}$$

It is easy to prove that the secret key d in eqn. 7 satisfies eqn. 3. Note that whenever the public key e is given, the dual key d can be simply computed by using eqn. 7. Thus the Euclidean algorithm can be avoided.

Our method: We present a parallel implementation for generating RSA keys without the Euclidean algorithm in the following steps:

(i) Decompose the public key e into $e = e_1^{a_1}, e_2^{a_2} \ldots e_n^{a_n}$ using the unique factorisation theorem where $e_1, e_2, \ldots, e_n$ are n primes, and $a_1, a_2, \ldots, a_n$ are n positive integers.
(ii) Compute $d_1, d_2, \ldots, d_n$ by Derôme's method (shown in eqn. 7), where d_i is the dual key of e_i.
(iii) Compute the secret key d by multiplying all $d_i^{a_i}$, i.e. $d = \Pi_{i=1}^{n} d_i^{a_i} \bmod s$.

The correctness of our method can be shown as follows. By Derôme's method, we know that

$$\begin{cases} e_1 d_1 \equiv 1 \pmod s \\ e_2 d_2 \equiv 1 \pmod s \\ \quad \vdots \\ e_n d_n \equiv 1 \pmod s \end{cases} \tag{9}$$

Multiplying all of the equations in eqn. 9 together, we obtain

$$(e_1 e_2 \cdots e_n)(d_1 d_2 \cdots d_n) \equiv 1 \pmod s \tag{10}$$

Thus

$$ed \equiv 1 \pmod s \tag{11}$$

So eqn. 3 holds. Since e has been decomposed to n separate e_is eqn. 9 can be implemented by parallel processing.

Advantages: There are some important advantages to our method.

(i) The computational size is small. Since $e_i d_i \bmod s = 1$, it follows that $d_i e_i - j_i s = 1$. Using Derôme's method, $d_i = 1 + j_i\lfloor s/e_i \rfloor + [j_i(s \bmod e_i)] \bmod (e_i - 1)$, where $j = (-s^{\phi(e_i)-1}) \bmod e_i, i = 1,2, \ldots, n$. Since

$$\phi(e) = \phi(e_1)\phi(e_2)\cdots\phi(e_n) \tag{12}$$

$$= (e_1 - 1)(e_2 - 1)\cdots(e_n - 1) \tag{13}$$

Therefore $\phi(e_i) \ll \phi(e)$. Thus the computational size in our method is small.

(ii) Our method provides an efficient approach to assist an end user to choose a public key e. Since $gcd(e_i, s) = 1$, $i = 1, 2, ..., n$, $gcd(e, s) = 1$ is also true, where $e = \Pi_{i=1}^{n} e_i$. The user can thus select a set of small primes e_i and then multiply these primes together to produce a larger prime e. Our parallel implementation can then be used to generate the dual key d.

(iii) Our method can be implemented by parallel processing. If there are n processors in the system the secret key d can be generated by one computation of d_i and (logn) computations of $d_i \times d_j$, where $i \neq j$.

3 May 1996
Electronics Letters Online No: 19960886

C.-C. Chang (*Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan 621, Republic of China*)

M.-S. Hwang (*Department of Information Management, Chao-Yang Institiute of Technology, PO Box 55-67, Taichung, Taiwan 404, Republic of China*)

References

1 RIVEST, R.L., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signatures and public key cryptosystems', *Comm. ACM*, 1978, **21**, (2), pp. 120–126

2 KNUTH, D.E.: 'The art of computer programming, Vol. 2., Seminumberical algorithms' (Addison Wesley, 1981) 2nd edn. pp. 317–330

3 DERÔME, M.F.A.: 'Generating RSA keys without the Euclid algorithm', *Electron. Lett.*, 1993, **29**, (1), pp. 19–21

Super-low gain bandwidth and small area amplifier

J. Wulleman

Indexing terms: Amplifiers, Compensation, Silicon-on-insulator, BICMOS integrated circuits

A low-powered super-low gain bandwidth (SL-GBW) amplifier with a small area is discussed. The circuit has a transition frequency f_T of 38kHz (including gain stage, A), a power consumption of 150nW, a phase margin $PM \simeq 70°$, a total area of 300×36μm² and a minimum current per transistor of 7nA which is far above the leakage current after irradiation. The circuit was implemented in the radiation hard SOI BiCMOS technology of DMILL.

Introduction: The super-low gain bandwidth (SL-GBW) amplifier presented in [1] has been used as a compensation amplifier. Since the core amplifier in [1] has a high gain, the compensation amplifiers had to have an extremely low GBW in order to avoid any instability. The whole system is intended to be used in an irradiative environment with a level of irradiation up to 10Mrad. One of the consequences of the irradiation is an increased leakage current between the source and drain of the MOS devices. To avoid any influence of the leakage current on the performance of the compensation amplifier, a minimum current of 5nA per transistor was put forward. On the other hand, this current should not be too high, so that the power consumption can be minimised. The final constraint was the total area that is normally dominated by the area of the compensation capacitor C_C. At the expense of a large area, the use of a very large C_C is a possibility for obtaining a very low GBW. Through use of a gyrator, a small area C_C can be used to emulate a very large C_C, but at the expense of power consumption. The final goal was to develop an SL-GBW compensation amplifier with minimum area and power consumption, but with a current high enough so as not to cause problems with leakage current after irradiation. Fig. 1*a* represents the circuit that meets these constraints and specifications.

Amplifier: Fig. 2 represents the simplified equivalent circuit of Fig. 1*a*. MP_2, MP_3, MN_2 and MN_3 make up g_{m1} and MP_1, MP_4, MN_1 and MN_4 make up g_{m2}. G_1 and g_2 represent the output conductances of nodes V_1 and V_2. Fig. 1*b* shows the V-V buffer, with M_{s3} being part of the core amplifier [1], with the gain A given as:

$$A = \frac{V_{out,l,r}}{V_2} = \frac{gm_{Mb}}{sC_0 + g_{out}} \quad (1)$$

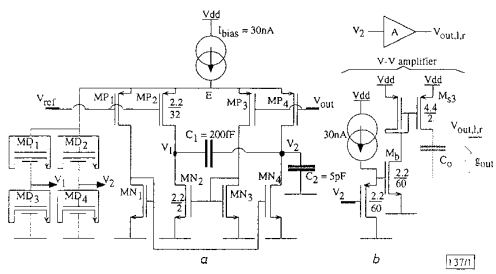

Fig. 1 *SL-GBW amplifier and V-V amplifier that is part of circuit in [1]*

a SL-GBW
b V-V amplifier

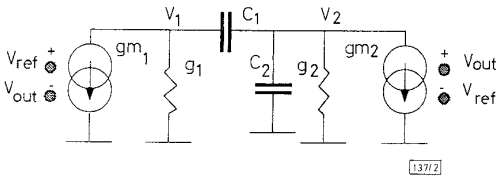

Fig. 2 *Simplified small signal model of Fig. 1 with V_{ref}–V_{out} as differential input signal*

When the V-V amplifiers are taken into account, $V_{out} = AV_2$

Consider now V_{ref}–$V_{out} = \Delta V_{in}$ as the input, V_2 as the output, $C_2 = 0$ and $g_{m1} = g_{m2} = g_m$; the transfer function of Fig. 2 is

$$T = \frac{V_2}{\Delta V_{in}} = \frac{gm\, g_1}{sC_1(g_1 + g_2) + g_1 g_2} \quad (2)$$

If we consider $g_1 = g_2$, the *GBW* becomes

$$GBW = \frac{gm}{2(2\pi C_1)} \quad (3)$$

We see that the GBW is a factor of 2 smaller then in the case of a classical Miller compensated OTA. To reach the same GBW with the new circuit topology, we can reduce C_1, and so its area, by a factor of 2. When the gain stage A is taken into account the output $V_{out,l,r}$ has to be connected to V_{out}, the input of $MP_{3,4}$, as it is implemented in [1]. In principle when we study the PM and GBW of the SL-GBW amplifier, we have to open the connection $V_{out,l,r}$–V_{out} and consider V_{out} as the input and $V_{out,l,r}$ as the output of the system. This is equivalent to leaving open the connection $V_{out,l,r}$–V_{out}, considering $V_{out,l,r}$ as the output and V_{ref} as the input but with opposite sign. For the discussion of the transfer function we will consider the connection closed and V_{ref} as the input because we cannot uncouple the core amplifier from the compensation amplifier without changing the characteristics of the V-V amplifier part drastically. This way we will not observe any DC gain in the simulations but this is only of minor importance. Only the PM is important in the region of the GBW and the f_T when studying the stability. With $C_2 = 0$, $g_{m1} = g_{m2} = g_m$, and taking into account the gain stage A, we have

$$T = \frac{V_{out,l,r}}{V_{ref}} = \frac{gm\, g_1 A}{sC_1(g_1 + g_2) + g_1(g_2 + Agm)} \quad (4)$$

When calculating the *GBW*, only the (calculated) DC gain and the dominant pole are important. This implies only the low frequency region is important and for reasons of simplicity we will neglect the term sC_0 in eqn. 1, resulting in $A \simeq gm_{Mb}/g_{out}$. This is in contrast with the transfer function of the core amplifier, where C_0 is indeed very important [1]. For the *GBW* we have

$$GBW = \frac{gm\, g_1 A}{2\pi C_1(g_1 + g_2)} \quad (5)$$

Problems: In Fig. 1 we see that node V_2 is DC controlled (feedback through the gain stage A) whereas V_1 is not. If the two