..., N}. The simplest case where q_k consists of a block of contiguous carriers (i.e., $q_k = \{j + (k-1)N/V \mid j = 1, ..., N/V \in \})$, which is especially suitable for differential detection systems [1]. Blocks may contain non-contiguous carriers for better PF reduction capability at the cost of extra complexity [3]. Let ϕ_k, $k = 1, ..., V$, be a set of phases with $\phi_1 = 0$. The modified symbols $\tilde{c}_j = c_j e^{i\phi_k}$ for $j \in q_k$ and $\underline{\tilde{c}} = [\tilde{c}_1, \tilde{c}_2, ..., \tilde{c}_n]$. For a given information vector $\underline{c}$, the reported optimisation criterion is [1]

$$\left[\hat{\phi}_2, \hat{\phi}_3, ..., \hat{\phi}_V\right] = \underset{[\phi_2, \phi_3, \dots, \phi_V]}{\operatorname{argmin}} \|A\underline{\tilde{c}}\|_\infty \tag{4}$$

Then, the actual transmitted sequence is given by eqn. 3 with this set of block phase factors ($\underline{c}$ replaced by $\underline{\tilde{c}}$), which may have to be transmitted by some means (e.g. on extra carriers). To reduce the search complexity, each ϕ_k is discrete and takes a value from the set $\phi_k \in \{0, \pi/2, \pi, 3\pi/2\}$.

Fig. 1 shows the distribution of the PF for the uncoded case (i.e. there is no attempt to reduce the peak factor) and for a PTS with four blocks. Several observations can be made:

(i) For the uncoded case, the LPF follows the Rayleigh distribution. However, the TPF is ~0.5dB worse than that predicted by the Rayleigh distribution.

(ii) The use of the TPF results in an estimated PF reduction of only 1dB for the PTS scheme.

(iii) The use of the LPF results in an estimated PF reduction of 4dB for the PTS scheme.

Therefore, at least in this case, the PTS gains reported [1] appear to be optimistic. Note that the difference between the TPF and the LPF is ~3dB (Fig. 1). The reason seems to be the following: since eqn. 4 is equivalent to suppressing $|s(kT)|$ for $k = 0, ..., N-1$ while keeping the area under $|s(t)|^2$ constant, this very fact *causes* the true peak of $|s(t)|$ to move away from the sampling points.

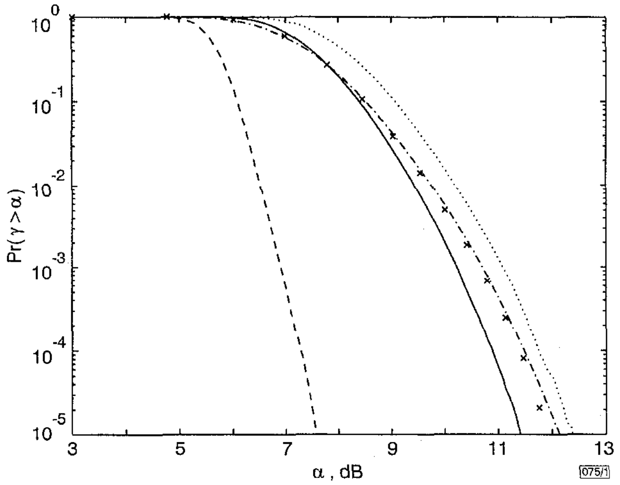

Fig. 1 *Probability that peak factor γ exceeds α for 128 QPSK-modulated carriers*

TPF: true peak factor LPF: lower peak factor UNC: uncoded
Optimisation criterion eqn. 4, 10^6 simulation points
——— TPF for PTS
· – · – · Rayleigh
– – – – LPF for PTS
· · · · · · TPF for UNC
××× LPF for UNC

In fact, eqn. 4 is not the only possible optimisation criterion. A recent Letter [4] shows that a bound on the PF can obtained by the sum of the autocorrelation (aperiodic) sidelobe magnitudes of the modulation symbol sequence. This suggests another optimisation criterion. Let $\rho(k)$ be the aperiodic autocorrelation of $\underline{\tilde{c}}$. Then, for a given information vector $\underline{c}$, the new optimisation criterion is

$$\left[\hat{\phi}_2, \hat{\phi}_3, ..., \hat{\phi}_V\right] = \underset{[\phi_2, \phi_3, \dots, \phi_V]}{\operatorname{argmin}} \sum_{k=1}^{N-1} |\rho(k)| \tag{5}$$

Fig. 2 shows the PF distribution with the use of eqn. 5. A PF reduction of ~2.5dB can be achieved at $\Pr(\gamma > \alpha) = 10^{-5}$. Note that the difference between the TPF and the LPF is 0.5dB in this case (Fig. 2). Since the sum in eqn. 5 determines a bound on the true peak, its minimisation leads to a flatter $|s(t)|$ for $0 \leq t < \tau$, not just on the sampling points. In a practical system, implementing eqn. 5 can be too complicated. For QPSK, the real and imaginary part of each $\rho(k)$ can be obtained without any multiplications (the number of integer additions is in the order of N^2). So the total complexity varies as $O(4^{V-1}N^2)$.

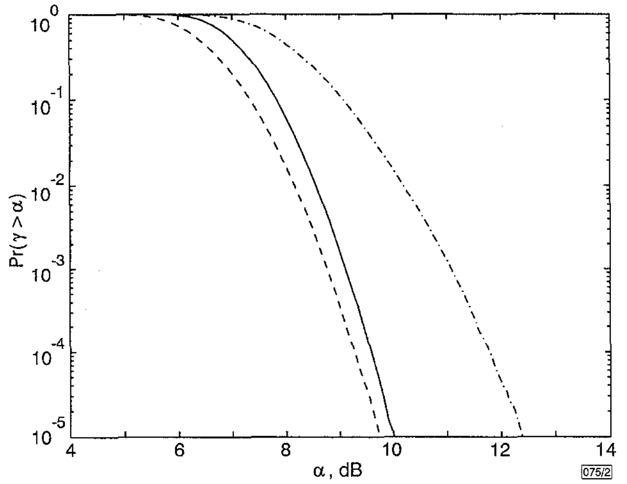

Fig. 2 *Probability that peak factor γ exceeds α for 128 QPSK-modulated carriers*

Optimisation criterion eqn. 5, 10^6 simulation points
——— TPF for PTS
– – – – LPF for PTS
· – · – · TPF for UNC

Conclusions: The PTS approach requires that we determine several block phase factors, for which a new optimisation criterion has been presented. Assuming an ideal anti-aliasing filter, the output signal closely resembles the multicarrier signal (eqn. 1). Therefore, it is not sufficient to find the PF on the basis of N samples. The reported gains of PTS with eqn. 4 appear to be optimistic, however, it may be that the use of a raised-cosine filter alleviates this problem.

© IEE 1998 *21 october 1997*
Electronics Letters Online No: 19980163

C. Tellambura (*Department of Digital Systems, Monash University, Wellington Road, Clayton, Victoria 3168, Australia*)

E-mail: chintha@dgs.monash.edu.au

References

1 MÜLLER, S.H., and HUBER, J.B.: 'OFDM with reduced peak-to-average power ratio by optimum combination of partial transmit sequences', *Electron. Lett.*, 1997, **33**, pp. 368–369

2 MÜLLER, S.H., BÄUML, R.W., FISCHER, R.F.H., and HUBER, J.B.: 'OFDM with reduced peak-to-average power ratio by multiple signal representation', *Annals of Telecommun.*, 1997, **52**, pp. 58–67

3 MÜLLER, S.H., and HUBER, J.B.: 'A novel peak power reduction scheme for OFDM'. 1997 Int. Sym. on Personal, Indoor and Mobile radio comms. Proc., 1997, (IEEE), pp. 1090–1094

4 TELLAMBURA, C.: 'Upper bound on the peak factor of N-multiple carriers', *Electron. Lett.*, 1997, **33**, pp. 1608–1609

Security of the Cao-Li public key cryptosystem

Lim Lek Heng

The author shows that the Cao-Li cryptosystem proposed in [1] is not secure. Its private key can be reconstructed from its public key using elementary means such as LU-decomposition and the Euclidean algorithm.

Description of cryptosystem: The Cao-Li public key cryptosystem was first proposed in [1]. It encrypts messages using a bilinear form that is chosen to permit easy decryption by the Chinese remainder theorem. Public key cryptosystems that are designed along this line are not uncommon in the Chinese cryptographic literature. However, as most of the original papers were published in Chinese, they remained relatively obscure until a few of them were described in [2] (in English) recently. Our description below is based on the latter reference.

Let $p_1, ..., p_n$ be n distinct primes where $p_i \equiv 3 \bmod 4$. For $i = 1, ..., n$, define

$$m_i := \frac{1}{p_i}\left(\prod_{j=1}^{n} p_j\right)$$

Compute for each m_i, an integer m'_i that satisfies $m'_i m_i \equiv 1 \bmod p_i$ and $0 < m'_i < p_i$. We define positive integers

$$\lambda_i := m'_i m_i$$

for $i = 1, ..., n$ and the diagonal matrix

$$\Lambda := \text{diag}[\lambda_1, ..., \lambda_n]$$

Note that

$$\lambda_i \equiv \delta_{ij} \bmod p_j \qquad (1)$$

where δ_{ij} is 1 if $i = j$ and 0 otherwise.

We choose another two invertible $n \times n$ lower-triangular matrices P_1 and P_2 with non-negative integer entries that are bounded by

$$\beta := \min_{1 \leq i \leq n} \sqrt{\frac{p_i}{i(i+1)d}} \qquad (2)$$

where $d \geq 1$ is a chosen positive integer.

The secret key comprises the two matrices P_1, P_2 and the primes p_i, $i = 1, ..., n$. The public key is the $n \times n$ symmetric matrix B given by

$$B := P_2^T P_1^T \Lambda P_1 P_2$$

Let the message block be $\mathbf{x} = (x_1, ..., x_n)$ where $0 \leq x_i \leq d$. The ciphertext y is computed as

$$y = \mathbf{x} B \mathbf{x}^T$$

If we let $\mathbf{z} := \mathbf{x} P_2^T P_1^T$, then

$$y = \mathbf{z}\Lambda\mathbf{z}^T = \lambda_1 z_1^2 + \cdots + \lambda_n z_n^2$$

From eqn. 1, we have

$$z_k^2 \equiv y \bmod p_k \qquad (3)$$

Keeping in mind that P_1^T and P_2^T are upper-triangular and their entries are non-negative and bounded by β, we have, from eqn. 2 and $0 \leq x_i \leq d$, that

$$0 \leq z_k \leq \sum_{i=1}^{k}\sum_{j=i}^{k} d\beta^2 = d\beta^2 \frac{k(k+1)}{2} < \frac{p_k}{2} \qquad (4)$$

We can carry out decryption as follows. For each $k = 1, ..., n$, compute the unique z_k satisfying eqns 3 and 4. The message can then be recovered by

$$\mathbf{x} = \mathbf{z}(P_2^T P_1^T)^{-1} \qquad (5)$$

Note that since $p_k \equiv 3 \bmod 4$, effective algorithms for computing square roots mod p_k exist (see [3]).

Key recovery: We will first recover Λ from B. Let $P_1 P_2 =: P = (p_{ij})_{1 \leq i,j \leq n}$. Then P is an invertible lower-triangular matrix with non-negative integral entries by the same properties of P_1 and P_2. Since P is invertible and has non-negative integral entries, we have det $P = 1$. Moreover, we also have det $P = p_{11} \times ... \times p_{nn}$ since P is triangular. As all the P_{ii} values are non-negative, it then follows that $p_{ii} = 1$ for $i = 1, ..., n$.

Λ and P can be recovered from B using an algorithm that is very similar to the algorithm for LU-decomposition of a matrix (the difference being that row reduction is done starting from the bottom rows). Denote the ith row of B by $\mathbf{b}_i = (b_{i1}, ..., b_{in})$, $i = 1, ..., n$. We know immediately that $b_{nn} = \lambda_n$. Table 1 shows algorithm A.

The following shows that algorithm A indeed yields the required output. Let the ith row of P be $\mathbf{p}_i$, $i = 1, ..., n$. Since $p_{ji} = 0$ if $j < i$ and $p_{ii} = 1$, we may write $\mathbf{b}_i = \lambda_i \mathbf{p}_i + \Sigma_{j=i+1}^{n} \lambda_j p_{ji} \mathbf{p}_j$. For each $i = n - 1, n - 2, ..., 1$, the inner loop of step 1 effectively carries out the following:

$$\mathbf{b}_i \leftarrow \mathbf{b}_i - \sum_{j=i+1}^{n} \frac{b_{ji}}{b_{jj}} \mathbf{b}_j$$

Table 1: Algorithm A

```
Algorithm A
Input    $B = (\mathbf{b}_1, ..., \mathbf{b}_n)^T = (b_{ij})_{1 \leq i,j \leq n}$
Output   $\lambda_1, ..., \lambda_n, P$
Step 1   for $i = n-1, n-2, ..., 1$ do
             for $j = n, n-1, ..., i+1$ do
                 $\mathbf{b}_i \leftarrow \mathbf{b}_i - \frac{b_{ji}}{b_{jj}} \mathbf{b}_j$;
             end;
         end;
Step 2   for $i = 1, ..., n$ do
             $\lambda_i \leftarrow b_{ii}$;
             $\mathbf{b}_i \leftarrow \mathbf{b}_i / \lambda_i$;
         end;
         $P \leftarrow B$
```

We shall show inductively that $\mathbf{b}_i$ is reduced to $\lambda_i \mathbf{p}_i$ at stage i: clearly $\mathbf{b}_n = \lambda_n \mathbf{p}_n$; suppose $\mathbf{b}_i$ is reduced to $\lambda_i \mathbf{p}_i$ at stage $i = n - 1, ..., n - k$, then at stage $n - k - 1$:

$$\begin{aligned} \mathbf{b}_{n-k-1} &\leftarrow \mathbf{b}_{n-k-1} - \sum_{j=n-k}^{n} \frac{b_{ji}}{b_{jj}} \mathbf{b}_j \\ &= \mathbf{b}_{n-k-1} - \sum_{j=n-k}^{n} \lambda_j p_{ji} \mathbf{p}_j \\ &= \lambda_{n-k-1} \mathbf{p}_{n-k-1} \end{aligned}$$

Hence, step 1 reduces $B = (\mathbf{b}_1, ..., \mathbf{b}_n)^T$ to $(\lambda_n \mathbf{p}_n, ..., \lambda_n \mathbf{p}_n)^T = \Lambda P$. Since the diagonal entries of P are all ones, the diagonal entries of ΛP are the required λ_i values. Consequently, P can be recovered by dividing each row by its corresponding diagonal entry.

We can now recover the moduli $p_1, ..., p_n$ from $\lambda_1, ..., \lambda_n$. From eqn. 1, we see that, for a fixed i, $p_i | \lambda_j$ for all $j \neq i$ and $p_i | \lambda_i - 1$. Hence

$$p_i | d_i := \gcd(\lambda_1, ..., \lambda_{i-1}, \lambda_i - 1, \lambda_{i+1}, ..., \lambda_n)$$

It could of course happen that $d_i \neq p_i$ for some i. Hence, this process only partially recovers the p_i values. However, our computer simulations (using C++ with LiDIA) show that instances where $d_i \neq p_i$, are rare. We shall give some heuristics to substantiate this claim. For $d_i = p_i$, it is sufficient that $\gcd(m'_1, ..., m'_{i-1}, m'_{i+1}, ..., m'_n) = 1$. From [4], we have

$$\#\{(a_1, ..., a_k) \in \mathbb{N}^k | \gcd(a_1, ..., a_k) = 1, \text{ all } a_i \leq N\}$$
$$= \begin{cases} N^k/\zeta(k) + O(N^{k-1}) & \text{if } k > 2 \\ 6N^2/\pi^2 + O(N \log N) & \text{if } k = 2 \end{cases}$$

where $\zeta(s) = \Sigma_{i=1}^{\infty} i^{-s}$ the Riemann zeta function. Assuming that each m'_i is randomly distributed in $\{1, ..., N\}$ where $N := \max\{p_1, ..., p_n\}$, the probability that $\gcd(m'_1, ..., m'_{i-1}, m'_{i+1}, ..., m'_n) = 1$ is then at least $\zeta(n - 1) \geq 6/\pi^2 \simeq 0.60$ when N is large enough. So we can expect to recover more than half of the p_i values. In fact, our simulations show that we almost always have $d_i = p_i$ and many of the rare exceptions are of the form $d_i = 2\,p_i$, where p_i can also be recovered easily.

Conclusion: Note that algorithm A is essentially LU-decomposition and the d_i values can be computed using the Euclidean algorithm. Since these two methods can be carried out efficiently, we can easily recover P and most of the p_i values. It then follows that the Cao-Li cryptosystem is insecure and thus should not be used.

© IEE 1998 2 September 1997
Electronics Letters Online No: 19980195

Lim Lek Heng (*DSO National Laboratories, 25th Storey, Tower A, Defence Technology Towers, Depot Road, Singapore 109679, Singapore*)

E-mail: llekheng@dso.org.sg

References

1 CAO, Z.F., and LI, Y.C.: 'A matrix-covering public-key cryptosystem'. Research Report of the Harbin University of Industry, pp. 1–37, 1991 (in Chinese)

2 DING, C., PEI, D., and SALOMAA, A.: 'Chinese remainder theorem: Applications in computing, coding, cryptography' (World Scientific, Singapore, 1996)

3 COHEN, H.: 'A course in computational algebraic number theory' (Springer-Verlag, Berlin Heidelberg, 1993)

4 HLAWKA, E., SCHOIßENGEIER, J., and TASCHNER, R.: 'Geometric and analytic number theory' (Springer-Verlag, Berlin Heidelberg, 1991)

Asynchronous analogue-to-digital converter for single-electron circuits

Su Jin Ahn and Dae Mann Kim

An analogue-to-digital conversion scheme based on the *e*-periodic transfer characteristics of an SET inverter is proposed. The authors demonstrate the 4 bit analogue-to-digital converter performance using Monte-Carlo simulation in which an SET inverter implements a binary quantiser and encoder for one significant bit. This scheme can be easily extended to higher order bits.

Introduction: The rapid progress in nanofabrication technologies have led to the discovery of a novel, single-electron tunnelling device. Since operation of a single-electron device is based on the Coulomb blockade phenomenon [1] emphasised in nanoscale-devices, single-electron transistors (SETs) have their own distinct features such as their inherent stochastic [3] and *e*-periodic output transfer characteristics. We propose an analogue-to-digital converter (ADC) architecture using the SET inverter's periodic output nature instead of directly imitating the method used in VLSI circuits by replacing FETs by SETs. In the proposed circuit, composed of a switch and voltage ramps supplied from the conventional VLSI circuitry and SET inverters, the analogue input signal is represented by modulated digital pulses coded by pulsewidth modulation (PWM), i.e. the magnitude of the analogue signal is represented by the duration of the pulse, and the digital output signal has a voltage of either 0V or V_{dd}, depending on its logical state '0' or '1', respectively. In this Letter, we have demonstrated a 4 bit ADC using numerical simulation and have also examined the possibility of extending an *N* bit ADC.

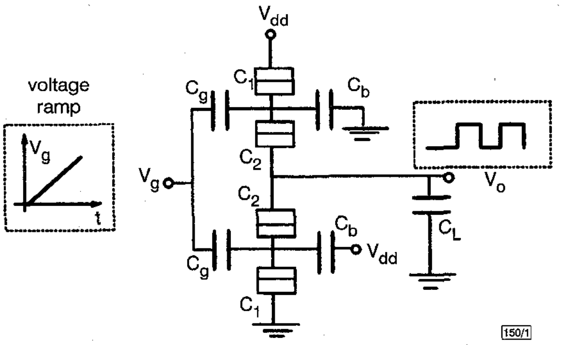

Fig. 1 *Proposed SET inverter circuit*

Principle of operation: The principle part of an asynchronous ADC circuit is an SET inverter modified from that by Tucker in [2], as shown in Fig. 1. The set of capacitance parameters used in Fig. 1 is

$$C_1 = C_2 = 1aF \qquad C_g = 2aF \qquad C_b = 7aF$$
$$C_L = 24aF = \frac{e}{V_{dd}} \qquad V_{dd} = 0.007V \tag{1}$$

Fig. 2 shows the inverter's transfer characteristics based on the stability diagram for both *n* and *p* SETs with extended gate voltage range over V_{dd}.

Since each *n* and *p* SET has a periodic output nature of gate voltage periodicity, $\Delta V_g = e/C_g$, the inverter's output follows trace A in Fig. 2 repeatedly, with the same periodicity ΔV_g as for an upward gate voltage sweep. We can expect almost 50% duty-cycle square wave-like signals as an output when we apply a voltage ramp $V_r(t)$ to the gate of the inverter quasistatically. It is noted that our inverter resulted in almost 50% duty-cycle square wave-like signals for both rising and falling gate voltage ramps, while Tucker's resulted in < 50% and > 50% duty-cycle square wave-like signals for rising and falling gate voltage ramps, respectively. When the voltage ramp signal is applied to the inverter, the net charge at the load capacitor C_L oscillates from 0 to *e* and the net charge of the centre island of *n* and *p* SET is added up by $-e$ per gate voltage increment of ΔV_g. To eliminate the nonlinearity occurring from the input offset voltage V_{offset} shown in Fig. 2, voltage ramp signals start not from 0V, but from V_{offset}. In addition, by varying the slopes of the voltage ramps, we can obtain several square wavelike outputs with various frequencies $S_i/\Delta V_g$ to the time-axis, where S_i is the slope of a voltage ramp.

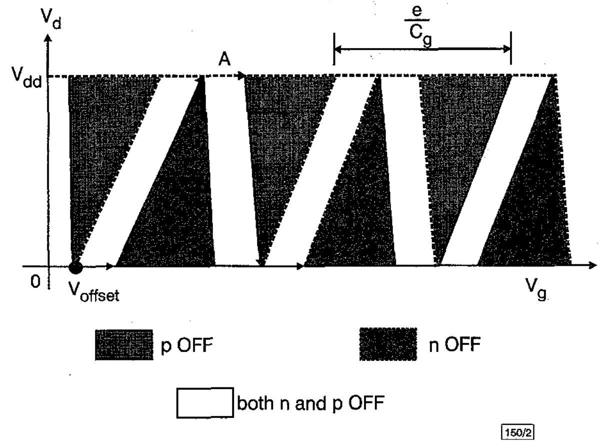

Fig. 2 *Output stability diagram of inverter consists of n and p SET stability diagram*

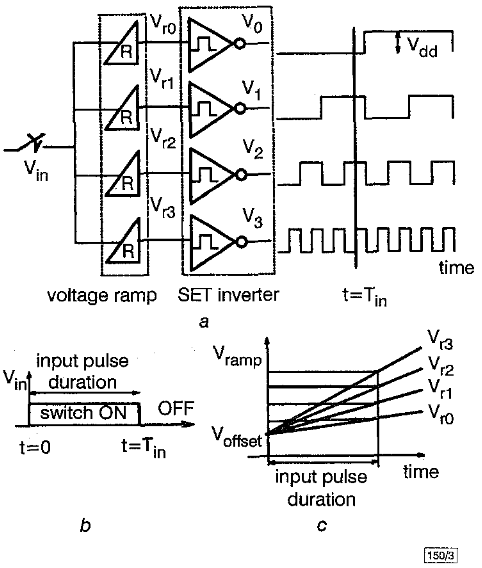

Fig. 3 *Schematic view of proposed ADC circuit with input signal representation and applied voltage ramp characteristics*

a Proposed circuit
b Input signal
c Voltage ramp characteristics

Fig. 3 shows the schematic view of the resulting 4 bit ADC architecture in which a single stage consists of a voltage ramp and a SET inverter.

As an analogue input signal coded by PWM is applied to the switch, voltage ramps start to rise from V_{offset} during the duration of pulse (switch ON time) with various speeds of their own, and then the output of each bit, either 0 V or V_{dd}, is measured at time T_{in}. The ramping slope of LSB is determined by $S_0 = \Delta V_g/2t_{unit}$, according to the input signal resolution of t_{unit}. The slope of *i*th bit voltage ramp S_i is automatically determined to one 2^ith of S_0.

Simulation results: We simulated the proposed circuit using a Monte-Carlo simulator called SIMON [4]. The gate voltage periodicity can be calculated to 0.08V. The slope of the voltage ramp S_0 is selected to be 0.08/20ns and thus the resolution of the input signal is 10ns. Fig. 4 shows the simulation results of the proposed 4 bit ADC under the assumption of zero temperature and co-tunnelling probability for simplicity. The bits deviate from an ideal