(i) Using 10^6 parallel processors to search over the key space (containing 2^{56} keys), we will need at most 1h and 1Mb units of memory.

(ii) To make the scheme more practical, we let $t = l = N^{7/16}$ and $m = N^{1/8}$. Then 100 parallel processors and 3 months will be required.

Making a comparison with the results of Hellman, the advantages of our proposed scheme are clear because of the time and cost savings evident.

© IEE 2000 *30 November 1999*
Electronics Letters Online No: 20000377
DOI: 10.1049/el:20000377

Song Qingwen and Zhou Yuanhua (*Department of Electronic Engineering, Shanghai JiaoTong University, 200030 Shanghai, People's Republic of China*)

E-mail: qwsong@email.com.cn

References

1 HELLMAN, M.E.: 'A cryptanalytic time-memory trade-off', *IEEE Trans.*, 1980, **IT-26**, pp. 401–406

2 DIFFIE, W., and HELLMAN, M.E.: 'Exhaustive cryptanalysis of the NBS data encryption standard', *Computer*, 1977, **10**, pp. 74–84

3 SONG, QINGWEN, and QIN, ZHONGPING: 'Approach to resolve one-way function with TMP trade-off', *J. Huazhong Univ. Sci. & Tech.*, 1998, **26**, (12), pp. 94–97

4 AMIRAZIZI, H.R., and HELLMAN, M.E.: 'Time-memory-processor trade-offs', *IEEE Trans.*, 1988, **IT-34**, (3), pp. 505–512

5 DIFFIE, W., and HELLMAN, M.E.: 'New directions in cryptography', *IEEE Trans.*, 1976, **IT-22**, pp. 644–654

Complementary neu-GaAs structure

P. Celinski, J.F. López, S. Al-Sarawi and D. Abbott

A neu-MOS like transistor structure using complementary GaAs HIGFET transistors, neu-GaAs, which uses capacitively coupled inputs onto a floating gate is presented. The design and simulation results of a neu-GaAs ripple carry adder are presented, demonstrating the potential for a very significant reduction in transistor count and area for equal power dissipation, through the use of neu-GaAs in VLSI design. A neu-GaAs design is presented which does not require floating gate initialisation due to the presence of a small gate leakage current in the HIGFET structure.

Introduction: Complementary GaAs has a number of highly desirable properties for low-power, high-speed digital and mixed RF/digital applications. These include low voltage operation (0.9–1.5V), very low static power dissipation using CMOS-like designs and significantly higher operating speeds than CMOS.

The neuron-MOS transistor (neu-MOS or νMOS for short) was originally developed by Shibata and Ohmi in 1991 [1]. The structure of a neu-MOS transistor is identical to that of an ordinary MOS transistor, but with a number of additional inputs capacitively coupled onto a floating gate. The floating gate potential is a weighted sum of the inputs, the weightings being determined by coupling capacitor ratios.

The use of neu-MOS transistors provides additional functionality which allows, for example, the design of a full adder cell with only eight transistors as compared to 28 in CMOS and an area of 55% of the CMOS design [2].

The aim of this Letter is to extend the neu-MOS paradigm to the complementary GaAs technology. In particular, we demonstrate the suitability of 0.5μm HIGFET transistors for application to neu-GaAs [3], present a basic neu-GaAs circuit structure and the simulation results of a neu-GaAs 4 bit ripple carry adder, for the first time.

Neu-GaAs inverter structure: The basic neu-GaAs transistor structure, analysis and symbolism are given in [3]. A variable threshold neu-GaAs inverter structure is shown in Fig. 1. MOSFET style transistor symbols have been used to emphasise the semi-insulating nature of the HIGFET transistor gate. This neu-GaAs inverter is a fundamental building block in digital neu-GaAs design and is similar to an ordinary CMOS-like ratioless inverter consisting of a *p*-channel GaAs pull-up and an *n*-channel pull-down transistor. The gates of the two transistors are connected and two inputs which are capacitively coupled to this floating gate are added. When the floating gate potential exceeds the inverter threshold, the inverter output goes low and *vice versa*. By using two inputs, one which is to be inverted, V_{in}, and the other a threshold control, V_{ref}, the effective neu-GaAs inverter threshold can be made variable. The simulation results for three values of V_{ref} are shown in Fig. 1.

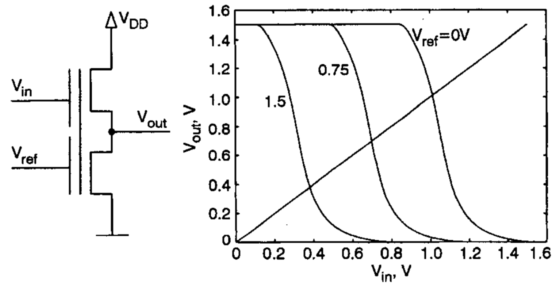

Fig. 1 *Basic neu-GaAs inverter structure*

Choice of GaAs technology: The realisation of neu-GaAs circuits requires that the floating gate voltage remain stable for periods of time depending on the clock frequency being used. This means that a low gate leakage current is needed. The HIGFET uses a semi-insulating AlGaAs layer to reduce gate leakage currents (to ~2nA/μm² of the gate area) and it appears, at least in the short term, as the most viable option for complementary neu-GaAs applications.

The simulations were based on a realistic composite SPICE parameter set derived from a number of complementary GaAs processes, including Honeywell, Sandia, Univ. Lille, Motorola and MIT [3].

4 bit neu-GaAs ripple carry adder (RCA): A 4bit RCA was chosen as a simple circuit to demonstrate the feasibility of circuit design using neu-GaAs. Ripple carry adders have a relatively low power dissipation, but the delay for computing the final carry depends on the number of bits to be added, because the carry propagates successively from the first stage to the last. The basic neu-GaAs full-adder (FA) was implemented based on the following expressions obtained from the truth table for addition:

$$c_i = 1 \Longleftrightarrow a_i + b_i + c_{i-1} \geq 2 \qquad (1)$$

$$s_i = 1 \Longleftrightarrow a_i + b_i + c_{i-1} - 2c_i \geq 1 \qquad (2)$$

where a_i and b_i are the two bits at the *i*th position and c_i is the carry generated at the *i*th position. In the inequalities (eqns. 1 and 2) a_i, b_i, c_i and c_{i-1} take values of 0 or 1 corresponding to 0V and V_{DD}, respectively, and + denotes algebraic addition. As there are no negative voltages in the circuit (there is only a 1.5V supply), $-2c_{i+1}$ must be converted into $2(\overline{c_{i+1}})$ and hence

$$c_1 = 1 \Longleftrightarrow a_i + b_i + c_{i-1} \geq 2 \qquad (3)$$

$$s_i = 1 \Longleftrightarrow a_i + b_i + c_{i-1} + 2\overline{c_i} \geq 3 \qquad (4)$$

It should be noted that in order to compute s_i, $\overline{c_i}$ has to be precomputed. The neu-GaAs realisation of the two inequality expressions for c_i and s_i is shown on the right hand side of Fig. 2. All coupling capacitor magnitudes in Fig. 2 are equal (30fF) with the exception of $\overline{c_i}$ which is 60fF. Fig. 2 also shows a comparison of the full adder cell design in both conventional complementary GaAs and neu-GaAs and shows a significant transistor count reduction in the neu-GaAs design. The conventional design consists of 28 transistors whereas the neu-GaAs design has only 8.

Simulation results for neu-GaAs RCA: HSPICE simulation results for a single neu-GaAs full adder, where c_{in} was switched, were carried out. From these results it was found that there is no degradation of the c_{out} output even when c_{in} is maintained high for an extended period of time (25ns).

The technique used to simulate the RCA structure using HSPICE is as follows. The two input words were set to (a_3 a_2 a_1 a_0) = (0 0 0 0) and (b_3 b_2 b_1 b_0) = (1 1 1 1). The c_{in} was switched from 0 to 1.5V at a frequency of 200MHz. This causes the output carry c_3 to switch when the input carry c_{in} propagates through the four bit slices.

The propagation delay and power dissipation of the carry signal through the 4 bit ripple carry adder operating at 200MHz were then measured as functions of the supply voltage, as plotted in Fig. 3. The carry and sum outputs were loaded by conventional complementary minimum sized inverters. For a typical supply voltage of 1.5V, it was found that the power dissipation and delay are approximately equal for both the 4bit neu-GaAs and conventional adders based on the designs shown in Fig. 2.

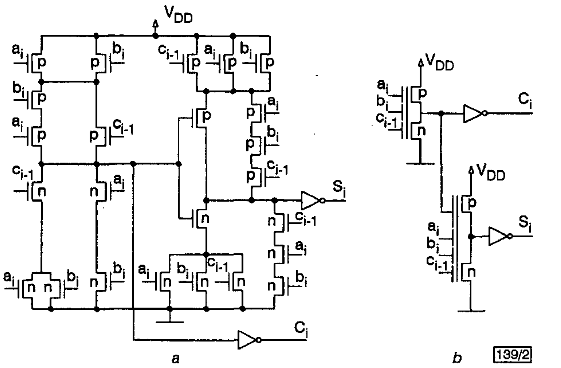

Fig. 2 *Conventional GaAs and neu-GaAs full adder designs*
a CHFET
b neu-GaAs

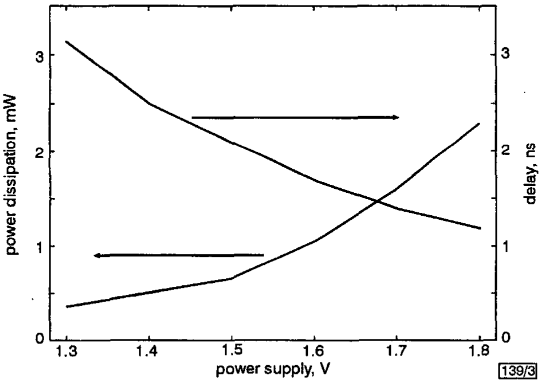

Fig. 3 *Carry delay and power dissipation against supply voltage for 4 bit neu-GaAs RCA*

Conclusions: A complementary neu-GaAs structure has been proposed and a 4bit ripple carry adder based on this structure has been simulated. It has been shown that by using neu-GaAs, a very significant reduction in the number of transistors is attainable over conventional complementary GaAs designs despite the presence of a small gate leakage current. Moreover it is anticipated that the gate leakage eliminates the need for the UV erasure of residual floating gate charge as is required in CMOS designs. The use of neu-GaAs techniques in HIGFET transistor designs promises to give VLSI designers more freedom in designs where area, delay and power dissipation are critical and hence provides a step forward towards boosting the effective integration level.

Acknowledgments: This research has been partially funded by the DSIPS project from the Comisión Interministerial de Ciencia y Tecnología (CICYT), Spain. The support of the Australian Research Council (ARC) and the Sir Ross and Sir Keith Smith Fund is also gratefully acknowledged.

© IEE 2000 *16 December 1999*
Electronics Letters Online No: 20000384
DOI: 10.1049/el:20000384

P. Celinski, D. Abbott and S. Al-Sarawi (*Centre for High Performance Integrated Technology and Systems (CHiPTec) and Centre for Biomedical Engineering (CBME), The Department of Electrical and Electronic Engineering, The University of Adelaide, Adelaide, SA 5005, Australia*)

E-mail: celinski@eleceng.adelaide.edu.au

J.F. López (*Research Institute for Applied Microelectronics, University of Las Palmas de Gran Canaria, 35017 Las Palmas de Gran Canaria, Spain*)

References

1 SHIBATA, T., and OHMI, T.: 'An intelligent MOS transistor featuring gate-level weighted sum and threshold operations'. Int. Electron Devices Meeting, Tech. Dig., Dec. 1991, (IEEE, New York, NY, USA)

2 HIROSE, K., and YASUURA, H.: 'A comparison of parallel multipliers with neuron MOS and CMOS technologies'. Proc. IEEE Asia Pacific Conf. Circuits and Systems 96, November 1996, (IEEE), pp. 488–491

3 ABBOTT, D., AL-SARAWI, S.F., GONZALEZ, B., LOPEZ, J.F., AUSTIN-CROWE, J., and ESHRAGHIAN, K.: 'Neu-MOS (MOS) circuits for smart sensors and an extension to a novel neu-GaAs (GaAs) paradigm'. IEEE ICECS98, Lisbon, September 1998, Vol. 3, pp. 379–404

Physically-based RF model for metal-oxide-metal capacitors

Chunqi Geng, Kok Wai Chew, Kiat Seng Yeo, Manh Anh Do, Jianguo Ma, Chee Tee Chua and Kai Shao

A new metal-oxide-metal (MOM) capacitor model is presented for RF (radio frequency) applications. Parasitics resulting from the geometry and physical topology of the model are taken into account. The model fits very well with the measured data in the frequency range 1–10GHz. The results show that the proposed model provides more accurate results than the conventional model, while retaining the physical properties of every element in the model.

Introduction: Capacitors are one of the most crucial elements in mixed-signal integrated circuits and are used extensively in many radio frequency integrated circuit (RF IC) applications such as data converters, sample and holds, switched-capacitor circuits, RF oscillators and mixers [1, 2]. Metal-oxide-metal (MOM) capacitors, due to their linearity, high-quality Q factor, and very small temperature variations, are very important passive components used in RF circuits [3]. An accurate MOM capacitor model is therefore urgently needed for RF circuit design and characterisation [4, 5].

The weakness of the conventional MOM capacitor model when used in RF applications is that the series resistance (i.e. the real part of the impedance) is constant for all frequency ranges [6]. Since a change in the series resistance will affect the Q factor of the overall circuit, its effect must be taken into account.

In this Letter, a new RF MOM capacitor model is derived based on the physical topology of the device, and the parasitics resulting from the geometry and physical topology are taken into account.

Device fabrication and description: The MOM capacitor is fabricated by adding additional process steps into the conventional CMOS backend process. This begins with the insertion of additional metal wiring between the third layer metal (M3) and the last thick layer metal (M4). After M3 is deposited, a silicon dioxide (SiO_2) dielectric layer is deposited to a thickness of ~100 nm by plasma-enhanced chemical vapour deposition (PECVD). Subsequently, the capacitor top plate is deposited, lithographically defined and etched. The bottom plate is then patterned to define both the MOM bottom plate and the local wiring. An intermetal dielectric is then deposited, into which vias are etched and filled,