mode locked fibre lasers. We anticipate that, by inserting a proper saturable absorber, the stability of periodically amplified long distance soliton transmission systems may also be substantially improved.

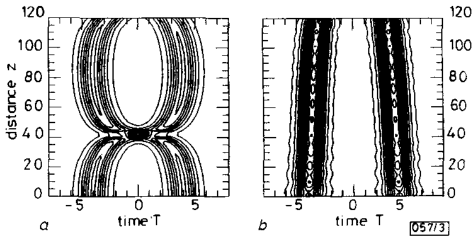

Fig. 3 *Pulse collision without and with bandwidth limited amplification and nonlinear gain*

a Without
b With

Acknowledgments: The work of Y. Kodama was partially supported by the NSF grant DMS-9109041. The work of M. Romagnoli and S. Wabnitz was carried out in the framework of the agreement between the Fondazione Ugo Bordoni and the Istituto Superiore Poste e Telecomunicazioni.

14th August 1992

Y. Kodama (*Department of Mathematics, Ohio State University, Columbus, Ohio 43210, USA*)

M. Romagnoli and S. Wabnitz (*Fondazione Ugo Bordoni, Via B. Castiglione 59, 00142 Rome, Italy*)

References

1 ĎULING, I. N. III,: 'Subpicosecond all-fibre erbium laser', *Electron. Lett.*, 1991, **27**, 544–545.
2 HOFER, M., FERMANN, M. E., HABERL, F., OBER, M. H., and SCHMIDT, A. J.: 'Mode-locking with cross-phase and self-phase modulation', *Opt. Lett.*', 1991, **16**, pp. 502–504
3 CHEN, C. J., WAI, P. K., and MENYUK, C. R.: 'Soliton fibre ring laser', *Opt. Lett.*, 1992, **17**, pp. 417–419
4 HASEGAWA, A., and KODAMA, Y.: 'Guiding center soliton', *Phys. Rev. Lett.*, 1991, **66**, pp. 161–164
5 KELLEY, S. M., SMITH, K., BLOW, K. J., and DORAN, N. J.: 'Average soliton dynamics of a high gain erbium fibre laser', *Opt. Lett.*, 1991, **16**, pp. 1337–39
6 KODAMA, Y., and HASEGAWA, A.: 'Generation of asymptotically stable optical solitons and suppression of the Gordon-Haus effect', *Opt. Lett.*, 1992, **17**, pp. 31–33
7 KODAMA, Y.: 'Optical solitons in a monomode fiber', *J. Stat. Phys.*, 1985, **39**, p. 597
8 KODAMA, Y., and WABNITZ, S.: 'Reduction of soliton interaction forces by bandwidth limited amplification', *Electron. Lett.*, 1991, **27**, pp. 1931–1933

DELAYED-TURN-ON PHENOMENON IN ACCUMULATION-TYPE SOI pMOS DEVICE OPERATING AT LIQUID NITROGEN TEMPERATURE

J. B. Kuo and J. H. Sim

Indexing terms: Metal-oxide-semiconductor structures and devices, Modelling

A unique delayed-turn-on phenomenon in an accumulation-type SOI *p*MOS device operating at 77 K based on the low-temperature PISCES simulation is reported. As compared with the 300 K case, in the delayed-turn-on region, the accumulation-type SOI *p*MOS device at 77 K may not provide a larger transconductance as a result of the carrier freezeout effects in the thin film.

Introduction: SOI MOS devices have been attracting much attention owing to their high speed and reduced second-order effects [2]. Cryogenic temperature performance of SOI MOS devices has also been reported [3, 4]. However, most of these devices are inversion-type SOI MOS devices. For ultrathin SOI structures, enhancement-type *p*MOS devices may be difficult to build using an *n*-type ultrathin film with $N+$ polysilicon gate. Recently, an accumulation-type SOI *p*MOS device using a *p*-type ultrathin film and an $N+$ polysilicon gate was introduced to produce an enhancement-type *p*MOS device [5]. However, low temperature performance of the accumulation-type SOI *p*MOS device has not been reported. In this Letter, analysis of the liquid nitrogen temperature performance of an accumulation-type SOI *p*MOS device is reported. It will be shown that, at 77 K, the accumulation-type *p*MOS device has a unique delayed-turn-on phenomenon.

Delayed-turn-on phenomenon: Fig. 1 shows the cross-section of the accumulation-type ultrathin SOI *p*MOS device structure [5] under study. The accumulation-type SOI *p*MOS device using an $N+$ polysilicon gate has a front gate oxide of 200 Å, a *p*-type thin silicon film of 1000 Å (t_{si}) with a doping density of $4 \times 10^{16}\,cm^{-3}$, and an insulator of 3500 Å (t_{ox2}). A *p*-type substrate with a doping density of $10^{15}\,cm^{-3}$ has been used in the study. The interface charge densities at the front and back oxide interface are $5 \times 10^{10}\,cm^{-3}$ and $10^{11}\,cm^{-3}$, respectively [5]. Low-temperature PISCES [1] simulation has been used to obtain the results.

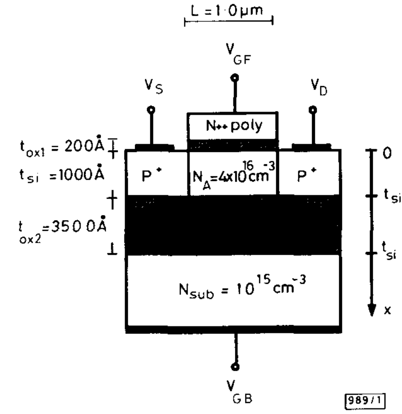

Fig. 1 *Accumulation-type SOI pMOS device structure under study*

Fig. 2 shows the drain current (I_D) against front gate voltage (V_{GF}) characteristics of the accumulation-type SOI *p*MOS device operating at 77 and 300 K biased at a back gate voltage $V_{GB} = +1, 0, -1$, and -2 V, a drain voltage of $V_D =$

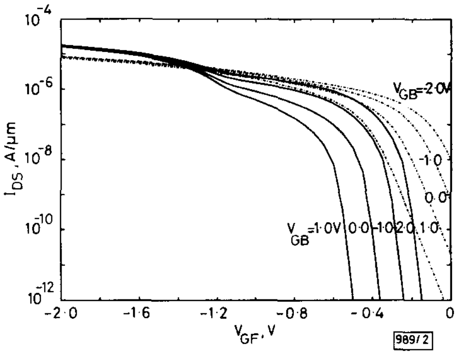

Fig. 2 *Drain current I_D against front gate voltage V_{GF} characteristics of accumulation-type SOI pMOS device operating at 77 and 300 K biased at back gate voltage $V_{GB} = +1, 0, -1$, and -2 V, drain voltage of $V_D = -0{\cdot}1$ V and source voltage $V_S = 0$ V*

Currents are on log scale
——— 77 K
–·–·–· 300 K

$-0{\cdot}1$ V and a source voltage of $V_S = 0$ V. At 300 K, the I_D against V_{GF} characteristics can be divided into a subthreshold region and a strong inversion region. Consider $V_{GB} = 0$ V. At 77 K, for V_{GF} smaller than $-1{\cdot}2$ V, the *p*MOS device is working in the fully-turned-on region. For a V_{GF} greater than $-0{\cdot}4$ V, the *p*MOS device is biased in the subthreshold region. Between the fully-turned-on region and the subthreshold region, a unique 'delayed-turn-on' region can be identified. As the back gate voltage is negative, a wider delayed-turn-on region can be observed. On the other hand, a positive back gate voltage leads to a narrower delayed-turn-on region.

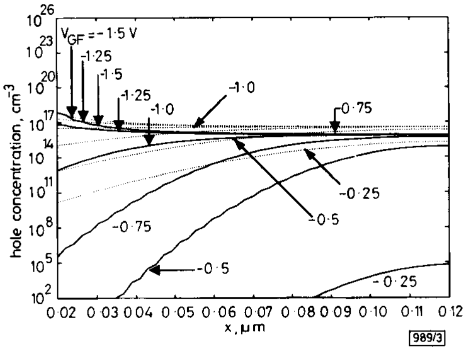

Fig. 3 *Hole density in substrate direction in centre of thin film of accumulation-type SOI pMOS device operating at 77 K biased at $V_{GB} = 0$ V and $V_{GF} = -0{\cdot}25, -0{\cdot}5, -0{\cdot}75, -1, -1{\cdot}25$, and $-1{\cdot}5$ V*

——— 77 K
········ 300 K

In fact, this delayed-turn-on region is similar to the delayed-turn-off phenomenon in the buried-channel *p*MOS device [6]. Fig. 3 shows the hole density in the substrate direction in the centre of the thin film of the accumulation-type SOI *p*MOS device operating at 77 K biased at $V_{GB} = 0$ V and V_{GF} varying from $-0{\cdot}25$ V to $-1{\cdot}5$ V. As shown by the solid lines, at 77 K, and $V_{GF} = -0{\cdot}25$ V, the whole thin film is fully depleted. At $V_{GF} = -0{\cdot}5$, $-0{\cdot}75$ V, holes are gathering at the bottom but the thin film is still depleted at the top. At $V_{GF} = -1{\cdot}25$, $-1{\cdot}5$ V, accumulation of holes exists at the top interface. As for the 300 K operation, its hole distributions are shown by dashed lines. Compared to the 300 K case, the 77 K case shows many fewer holes existing in the thin film as a result of the freezeout effect. In the subthreshold region, current conduction is mainly by diffusion current via the bottom portion of the thin film. In the delayed-turn-on region, holes in the thin film are forming and a substantial hole gradient can be identified in the lateral direction at the top oxide interface. At this time, the conduction current mainly consists of the drift current in the thin film close to bottom. As the device is fully turned on, the whole thin film is full of holes and an accumulation of holes exists at the top oxide interface. At full turn-on, the conduction current is dominated by the drift current coming from accumulated holes at the top interface. As for the 300 K operation, in the subthreshold region, current conduction is mainly due to the diffusion current at the bottom. At 300 K, in the fully-turned-on region, current conduction is by the drift current in the thin film or/and in the top accumulation layer.

Discussion: The delayed-turn-on behaviour can be viewed from another angle: In the delayed-turn-on region, hole accumulation at the top interface does not yet exist. Current conduction mainly consists of the current via the thin film. At delayed-turn-on, the advantage of the higher mobility has been offset by the lower hole density due to freezeout, as compared to the 300 K case. As hole accumulation at the top occurs, this situation ceases because the accumulated holes at the top are not susceptible to freezeout effects. As a result, the low-temperature case indicates a ×3·6 advantage in transconductance owing to a higher mobility.

7th August 1992

J. B. Kuo and J. H. Sim (*Rm. 526, Dept. of Electrical Eng., National Taiwan University, Roosevelt Rd., Sec. 4, #1, Taipei 106-17, Taiwan*)

References

1 KUO, J. B., *et al.*: 'Two-dimensional analysis of a BiNMOS transistor operating at 77 K', *IEEE Trans. Electron Devices*, February 1992, **ED-39**

2 HOSACK, H. H., *et al.*: 'SIMOX silicon-on-insulator: materials and devices', *Solid State Technol.*, December 1990, pp. 61–66

3 AOKI, H., OKABAYASHI, H., and MOGAMI, T.: 'Device simulation of 0·1 μm gate-length, 77 K operated, ultra-thin film SOI-MOSFETs'. Proc. IEEE SOS/SOI Technol. Conf., October 1989, pp. 141–142

4 KUO, J. B., LEE, W. C., and SIM, J. H.: 'Back gate bias effect on the subthreshold behavior and the switching performance in an ultra-thin SOI CMOS inverter operating at 77 K and 300 K', to be published in *IEEE Trans. Electron Devices*

5 COLINGE, J. P.: 'Conduction mechanisms in thin-film accumulation-mode SOI p-channel MOSFETs', *IEEE Trans. Electron Devices*, **ED-37**, March 1990, pp. 718–723

6 SIM, J. H., and KUO, J. B.: 'Analytical delayed-turn-off model for buried-channel PMOS devices operating at 77 K', *IEEE Trans. Electron Devices*, April 1992, **ED-39**

LOW COMPLEXITY ARCHITECTURE FOR EXPONENTIATION IN GF(2^m)

M. A. Hasan and V. K. Bhargava

Indexing terms: Cryptography, Digital arithmetic, Number theory

A pipeline bit-serial multiplier architecture for the Galois field GF(2^m) is presented. A structure for finite field exponentiation is developed based on the multiplier. The structure is regular, area efficient and suitable for VLSI implementation for large fields.

Introduction: Many practical applications require secure communications over a nonsecure channel. With the recent trend in personal communications systems, where a wireless channel is easily accessible to a cryptanalyst, the inclusion of some form of cryptosystem with mobile terminals has been emphasised in the literature [1]. Many of these terminals must be quite small in size. For such compact terminals the cryptosystem, when implemented in VLSI, should require minimal silicon area and may need to coexist with other signal processing circuitry in a single chip. Thus it is important to develop area efficient cryptosystems.

For the public-key cryptosystem, the Diffie-Hellman scheme is a well known key-exchange protocol based on finite field exponentiation [2]. Several architectures have been proposed for exponentiation in the finite field GF(2^m) [3–5]. The main components of these architectures are finite field multipliers. The complexity of the exponentiator mainly depends on the multiplier used.

This Letter extends the work of Reference 6 by presenting a multiplier for a sequence of elements of GF(2^m). This sequential multiplier is then used to develop an area efficient exponentiation structure over GF(2^m).

Finite field sequential multiplier: Let $g(x) = \sum_{i=0}^{m} g_i x^i$ be an irreducible monic polynomial of degree m over GF(2). Let $\alpha \in$ GF(2^m) satisfy $f(\alpha) = 0$. Then the set of m elements $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ forms a basis over GF(2) and can be used to represent all elements of GF(2^m) [7]. Specifically, if $a \in$ GF(2^m), then there exists $a_i \in$ GF(2) such that $a = \sum_{i=0}^{m-1} a_i \alpha^i$.

Consider a sequence $\{\xi_0, \xi_1, \ldots, \xi_{n-1}\}$ of n elements of GF(2^m), i.e. $\xi_i = \sum_{j=0}^{m-1} \xi_{i,j} \alpha^j$ where $\xi_{i,j} \in$ GF(2). Let $p_m \in$ GF(2^m) be the product of these elements, i.e.

$$p_n = \prod_{i=0}^{n-1} \xi_i \tag{1}$$

One approach to the realisation of this sequence multiplication is to use a finite field bit-serial multiplier [7] in conjunction with an m bit buffer to store the most recent partial