$(\gamma)_i = c'(\gamma)_{i-1} + s'(\gamma)$. Let m-dimensional vector $\vec{t} = [h_{m-k}, h_{m-k+1}, \ldots, h_{m-1}, 0, \ldots, 0]^T$, then the output $E^i = \gamma^T(E^{i-1} \downarrow k + R^T \vec{t})$.

To give its complexities in terms of gate counts and time delay owing to gates, we let r_j, $0 \leq j \leq k-2$, be the jth column of the reduction matrix R, i.e., $R = [r_0, r_1, \ldots, r_{m-1}]$ and $H(r_j)$ be the Hamming weight (i.e. the number of 1s) of r_j. We denote θ as the maximum Hamming weight of a column of R, i.e.

$$\theta = \max\{H(r_j) : 0 \leq j \leq m-1\} \tag{2}$$

and $H(R)$ as the Hamming weight of R, i.e.

$$H(R) = \sum_{0}^{m-1} H(r_j) \tag{3}$$

Now, consider each PM module except the first and last ones of the multiplier in Fig. 1. For computing $c'(\gamma)_i$, it needs mk AND gates and $(k-1)(m-1) + H(R) + k$ XOR gates. For the E^i, using (3), one can determine the maximum number of XOR gates needed as $H(R)$. As the inputs of the first PM module do not include $c'(\gamma)_{i-1}$ and the last one does not need to compute E^i, the multiplier has a total of m^2 AND gates and $q((k-1)(m-1) + 2H(R) + k) - k - H(R) = m^2 - qm + (2q-1)H(R) + q - k$ XOR gates.

Table 1: Comparison of different types of multipliers using trinomials

Algorithm	XOR gates	AND gates	Delay
Koç-Sunar [7]	$m^2 - 1$	m^2	$T_A + (2 + \lceil \log_2(m-1) \rceil)T_X$
Lee [8]	$m^2 + m - 1$	m^2	$T_A + (2 + \lceil \log_2(m-1) \rceil)T_X$
Wu [9]	$(m-1)^2$	m^2	$T_A + (\lceil \log_2(m) \rceil)T_X$
Sunar-Koç [10]	$m^2 - 1$	m^2	$T_A + (\lfloor (m-2)/(m-n) \rfloor + 1 + \lceil \log_2(m-1) \rceil)T_X$
Katti-Brennan [11]	$m^2 - 1$	m^2	$T_A + (\lfloor (m-2)/(m-n) \rfloor + 1 + \lceil \log_2 m \rceil)T_X$
Elia *et al.*[12] (m even)	$(3m^2)/4 + (5m)/2 + n - 4$	$3m^2/4$	$T_A + (3 + \lceil \log_2(m-1) \rceil)T_X$
Elia *et al.* [12] (m odd)	$(3m^2)/4 + 4m + n - 23/4$	$(3m^2 + 2m - 1)/4$	$(2m-1)(T_A + T_X)$
C.W. Chiou, L.C. Lin, F.H. Chou and S.F. Shu [13]	$m+1$	m	$m(T_A + T_X)$
Proposed design	$m^2 + (3 - q - 2/q)m - q$	m^2	$T_A + (2 + \lceil \log_2 m - \log_2 q \rceil)T_X$

To determine the time complexity of this architecture, for a single PM module computing E^i and $(c'(\gamma)_i$ at the same time, we need to consider the larger time delays owing to gates of computing E^i as well as $(c'(\gamma)_i$. Let T_A and T_X denote the AND gate delay and the XOR gate delay. Using (2), the maximum gate delay of computing E^i is $\lceil \log_2(H(\theta) - 1) \rceil T_X$, and the maximum gate delay of computing $(c'(\gamma)_i$ is $T_A + (\lceil \log_2 k \rceil + \lceil \log_2(1 + H(\theta)) \rceil)T_X$. Thus, an upper bound for the time delay of the entire multiplier structure is $T_C \leq T_A + (\lceil \log_2 k \rceil + \lceil \log_2(1 + H(\theta)) \rceil)T_X$.

Compared with [7–13], the space and time complexities of different types of multipliers are given in Table 1, where the irreducible polynomial is $x^m + x^n + 1$ (the case of $t = 1$) and $m - n \geq m/q - 1$.

Conclusions: By considering the advantages of bit-serial and bit-parallel multipliers for GF(2^m), a new design of multipliers has been presented, which can adapt to different requirements by selecting the parameter q based on the actual situations. By combining the bit-serial and bit-parallel schemes together and using pipeline architecture, the new design improves the efficiency of multipliers for GF(2^m).

Acknowledgments: This work was assisted by Project supported by the National High Technology Research and Development Program of China, under grant 2008AA01Z218.

5 February 2010
doi: 10.1049/el.2010.0246

Z. Mao, G. Shou, Y. Hu and Z. Guo (*School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China*)

E-mail: maozx486@163.com

References

1 Vanstone, S.A., and Oorschot, P.C.: 'An introduction to error correcting codes with applications' (Kluwer, 1989)
2 Mastrovito, E.D.: ''VLSI designs for multiplication over finite field, GF(2^m)' in Mora, T. (Ed.): 'Applied algebra, algebraic algorithms, and error-correcting codes'. Proc. Sixth Int'l Conf., (AAECC-6), Rome, Italy, July 1988, pp. 297–309
3 Lidl, R., and Niederreiter, H.: 'Introduction to finite fields and their applications' (Cambridge University Press, New York, USA, 1994)
4 Reyhani-Masoleh, A., and Hasan, A.: 'Low complexity bit parallel architecture for polynomial basis multiplication over GF (2^m)', *IEEE Trans. Comput.*, 2004, **53**, (8), pp. 945–959
5 Meher, P.K.: 'Systolic and non-systolic scalable modular designs of finite field multipliers for Reed-solomon codec', *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, 2009, **17**, (6), pp. 747–757
6 Meher, P.K.: 'Systolic and super-systolic multipliers for finite field. GF(2^m) based on irreducible trinomials', *IEEE Trans. Circuits Syst.*, 2008, **55**, (4), pp. 1031–1040
7 Koç, Ç.K., and Sunar, B.: 'Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields', *IEEE Trans. Comput.*, 1998, **47**, (3), pp. 353–356
8 Lee, C.Y.: 'Low complexity bit-parallel systolic multiplier over GF(2m) using irreducible trinomials', *IEEE Proc., Comput. Digit. Tech.*, 2003, **150**, (1), pp. 39–42
9 Wu, H.: 'Bit-parallel finite field multiplier and square using polynomial basis', *IEEE Trans. Comput.*, 2002, **51**, (7), pp. 750–758
10 Sunar, B., and Koç, Ç.K:: 'Mastrovito multiplier for all trinomials', *IEEE Trans. Comput.*, 1999, **48**, (5), pp. 522–527
11 Katti, R., and Brennan, J.: 'Low complexity multiplication in a finite field using ring representation', *IEEE Trans. Comput.*, 2003, **52**, (4), pp. 418–427
12 Elia, M., Leone, M., and Visentin, C.: 'Low complexity bit-parallel multipliers for GF(2^m) with generator polynomial $x^m + x^k + 1$', *Electron. Lett.*, 1999, **35**, (7), pp. 551–552
13 Chiou, C.W., Lin, L.C., Chou, F.H., and Shu, S.F.: 'Low-complexity finite field multiplier using irreducible trinomials', *Electron. Lett.*, 2003, **39**, (24), pp. 1709–1711

10 GHz cryocooled sapphire oscillator with extremely low phase noise

S. Grop, P.-Y. Bourgeois, R. Boudot, Y. Kersalé, E. Rubiola and V. Giordano

The phase noise characterisation of two 10 GHz cryogenic sapphire oscillators exhibiting frequency stability higher than 3×10^{-15} is reported. One of these oscillators developed for the deep space navigation ground stations of the European Space Agency, incorporates a closed cycle cryocooler as cold source. Near the carrier, the measured phase noise is limited by a flicker frequency noise: $S_\varphi(f) = -30\log(f) - 98$ dBrad^2/Hz.

Introduction: Cryogenic sapphire oscillators (CSO) based on whispering gallery mode sapphire resonator are known to present unbeatable frequency stability at short integration time. A few prototypes have demonstrated short-term frequency stability ranging from 1×10^{-14} to 4 to 5×10^{-16} [1–3] offering unprecedented resolution to probe atomic resonance in fountain atomic clocks [4] or to search for possible variation of fundamental constants [5] including light velocity (test of the Lorentz local invariance [6]).

These microwave frequency references are generally validated by measuring the Allan deviation $\sigma_y(\tau)$. Only in a few cases have phase noise characterisations been presented with a limited range of Fourier frequencies, making difficult the link between time domain and frequency domain measurements [7, 8]. The difficulty of phase noise characterisation results mainly from the impossibility to design two CSOs at very near frequencies. Indeed, a high resolution phase noise measurement setup requires that the two CSOs be phase locked. Mechanical tolerances of the sapphire resonator geometry limit the frequency accuracy to 1×10^{-5}. Thus two resonators machined from the same high purity crystal typically differ by 100 kHz–1 MHz. As the sapphire resonator bandwidth is of the order of 10 Hz, a direct phase lock of one CSO to the other is not possible.

We are developping a 10 GHz CSO for the European Space Agency (ESA) Deep Space Network (DSN). The sapphire resonator is cooled by a closed cycle cryocooler to ensure the long autonomy needed by the

DSN ground station. Low-frequency mechanical vibrations and temperature fluctuations owing to the gas flow inside the cryocooler are filtered by a special design [9]. Nevertheless, since the filter is not perfect, residual modulation should be detected in the phase noise spectrum. We then conducted the phase noise characterisation by comparing the cryocooled CSO with a second CSO in a liquid helium bath. The second CSO is free from mechanical vibrations and temperature modulation.

CSO design and frequency stability: The two CSOs are based on quasi-identical 54.2 mm diameter and 30 mm high sapphire resonators [9] inserted in the centre of a cylindrical copper cavity. The first resonator is placed on the second stage of a specially designed cryocooler. The second one is cooled in a large liquid-helium dewar. They operate on the whispering gallery mode $WGH_{15,0,0}$ at 9.99 GHz. At the temperature of $\simeq$6K, the two CSOs' frequencies differ by 745 kHz. The CSOs use a Pound frequency stabilisation and a power servo [1]. Time-domain frequency stability measurements have demonstrated an Allan deviation better than 3×10^{-15} between 1 and 1000 s integration time (frequency flicker). Assuming that the two CSOs are equivalent, each one shows a frequency stability of 2×10^{-15}.

Phase noise: Fig. 1 shows the setup we implemented to measure the CSOs' phase noise. The two CSO signals are mixed to get a beatnote frequency of 745 kHz. After amplification the beatnote is compared to the signal obtained from the frequency division of a 95 MHz signal coming from a low-noise RF synthesiser (HP 8662A). The latter is eventually phase locked on the beatnote signal. To provide the best measurement noise floor, we did not use the synthesiser in FM modulation mode. The PLL acts on the varactor of a 10 MHz VCO used as reference for the RF synthesiser. The obtained phase noise is shown in Fig. 2. The measurement noise floor was determined by replacing the CSO beatnote by a signal generated by another equivalent frequency divided HP8662A synthesiser. The measured phase noise is dominated at low Fourier frequencies by a flicker frequency noise ($1/f^3$ slope). Assuming that the random frequency fluctuations of the two CSOs are equivalent, the phase noise for one oscillator is simply obtained by substracting 3 dB in Fig. 2. For one CSO, we get $S_\varphi(1\text{ Hz}) = -98$ dBrad2/Hz, which is fully consistent with the flicker floor of the Allan deviation. Indeed, for a flicker frequency noise characterised by $S_\varphi(f) = b_{-3}/f^3$, the Allan variance does not depend on the integration time and is equal to $\sigma_y^2 = 2\ln 2\, b_{-3}/\nu_0^2$ [10]. The frequency stability of one CSO deduced from the phase noise spectrum is then $\sigma_y \simeq 1.5 \times 10^{-15}$.

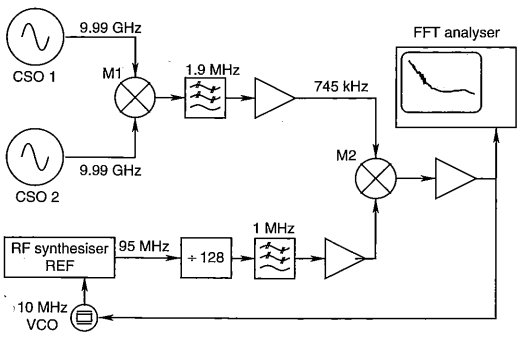

Fig. 1 *Phase noise measurement setup*

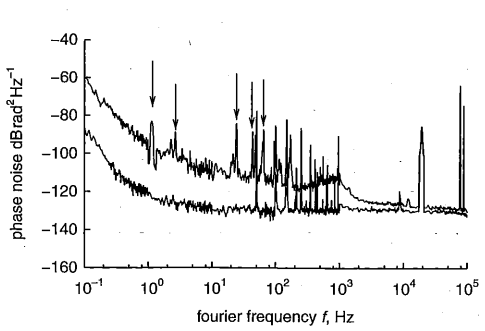

Fig. 2 *Power spectral density of phase fluctuations measured with setup of Fig. 1 (upper curve) compared to measurement noise floor (lower curve)*

Few sharp lines show up between 1 and 100 Hz, the highest of which are highlighted by black arrows in Fig. 2. Conversely to the random part of the spectrum, we do not have to take away the 3 dB for these lines because they result from the mechanical vibration affecting only the resonator inside the cryocooler. Taking into account the FFT analyser resolution bandwidth, i.e. 25 mHz, the rms phase modulation corresponding to the first spurious at $f_m = 1.1$ Hz is $\varphi_{rms} = 12.6$ μrad. Assuming the vertical acceleration is the main contribution, the rms fractionnal frequency variation can be written as:

$$\left[\frac{\Delta\nu}{\nu_0}\right] = \frac{f_m}{\nu_{0rms}}\,\varphi_{rms} = 4\pi^2 f_m^2 k_z z_{rms} \tag{1}$$

where z_{rms} is the rms vertical resonator displacement at the modulation frequency $f_m = 1.1$ Hz and k_z the resonator sensitivity to a vertical acceleration: $k_z \simeq 3.2 \times 10^{-11}$ m^{-1} s^2 [11]. Equation (1) leads to $z_{rms} < 1$ μm. The bump around 1 kHz corresponds to the bandwidth of the Pound servo, the gain of which can be optimised in a next step. The two bright lines near 100 kHz come from the phase modulations intentionally injected into the sustaining circuit of both CSOs and needed for the Pound servos. The other spurii come from the measurement setup itself.

Conclusion: We have measured for the first time the phase noise of a state-of-the-art cryocooled sapphire oscillator. We demonstrate that a mechanical filtering of the cryocooler low frequency vibration can be made sufficiently efficient to enable a relative frequency stability better than 3×10^{-15}.

Acknowledgments: This work has been supported by the European Space Agency (ESA). We gratefully acknowledge J. de Vicente (ESA), our colleagues from the National Physical Laboratory (UK) and from TimeTech GmbH (D) for their contribution to this project.

27 January 2010
doi: 10.1049/el.2010.0263
One or more of the Figures in this Letter are available in colour online.

S. Grop, P.-Y. Bourgeois, R. Boudot, Y. Kersalé, E. Rubiola and V. Giordano (*Institut FEMTO-ST, UMR 6174 CNRS, Université de Franche-Comté, 32 Avenue de l'Observatoire, Besançon 25044, France*)

E-mail: giordanofemto-st.fr

References

1 Locke, C.R., Ivanov, E.N., Hartnett, J.G., Stanwix, P.L., and Tobar, M.E.: 'Invited article: design techniques and noise properties of ultrastable cryogenically cooled sapphiredielectric resonator oscillators', *Rev. Sci. Instrum.*, 2008, **79**, p. 051301–1–12

2 Watabe, K., Hartnett, J., Locke, C.R., Santarelli, G., Yanagimachi, S., Ikegami, T., and Ohshimal, S.: 'Progress in the development of cryogenic sapphire resonator oscillator at NMIJ/AIST'. Proc. 20th European Frequency and Time Forum, Braunschweig, Germany, March 2006, pp. 92–95

3 Bourgeois, P.Y., Kersalé, Y., Bazin, N., Chaubet, M., and Giordano, V.: 'A cryogenic open-cavity sapphire reference oscillator with low spurious mode density', *IEEE Trans. Ultrason. Ferroelectr. Freq. Control*, 2004, **51**, (10), pp. 1232–1239

4 Bize, S., Laurent, P., Abgrall, M., Marion, H., Maksimovic, I., Cacciapuoti, L., Grunert, J., Vian, C., dos Santos, F.P., Rosenbusch, P., Lemonde, P., Santarelli, G., Wolf, P., Clairon, A., Luiten, A., Tobar, M., and Salomon, C.: 'Advances in atomic fountains', *C.R. Physique*, 2004, **5**, pp. 829–843

5 Tobar, M.E., and Hartnett, J.G.: 'Proposal for a new test of the time independence of the fine structure constant α using orthogonally polarized whispering gallery modes in a single sapphire resonator', *Phys. Rev. D*, 2003, **67**, (6), 062001

6 Stanwix, P.L., Tobar, M.E., Wolf, P., Susli, M., Locke, C.R., Ivanov, E.N., Winterflood, J., and Kann, F.van: 'Test of Lorentz invariance in electrodynamics using rotating cryogenic sapphire microwave oscillators', *Phys. Rev. Lett.*, 2005, **95**, 040404

7 Marra, G., Henderson, D., and Oxborrow, M.: 'Frequency stability and phase noise of a pair of x-band cryogenic sapphire oscillators', *Meas. Sci. Technol.*, 2007, **18**, pp. 1224–1228

8 Watabe, K., Inaba, H., Okumura, K., Hong, F.-L., Hartnett, J., Locke, C., Santarelli, G., Yanagimachi, S., Minoshima, K., Ikegami, T., Onae, A., Ohshima, S., and Matsumoto, H.: 'Optical frequency

synthesis from a cryogenic sapphire oscillator using a fiber-based frequency comb', *IEEE Trans. Instrum. Meas.*, 2007, **56**, (2), pp. 632–636
9 Grop, S., Bourgeois, P.-Y., Bazin, N., Kersalé, Y., Rubiola, E., Langham, C., Oxborrow, M., Clapton, D., Walker, S., Vicente, J.D., and Giordano, V.: 'A crycooled 10 GHz oscillator with 10^{-15} frequency stability', *Rev. Sci. Instrum.*, 2010, **81**, 025102, see http://arxiv.org/abs/0909.3971 accessed February 2010
10 Rubiola, E.: 'Phase noise and frequency stability in oscilltors', (Cambridge University Press, 2008)
11 Oxborrow, M., Benmessäi, K., Grop, S., Bazin, N., Bourgeois, P., Kersalé, Y., and Giordano, V.: 'g-sensitivity of a cryogenic sapphire resonator'. Proc. 22th European Frequency and Time Forum (EFTF 2008), Toulouse, France, April 2008, FPE-062

480 GHz oscillator with an InP Gunn device

H. Eisele

An InP Gunn device with a graded doping profile was evaluated for third-harmonic power extraction around 480 GHz. The oscillator used the configuration of a WR-6 waveguide cavity for the InP Gunn device, two back-to-back waveguide transitions, WR-3 → 1.5 and WR-1.7 → 3, to block fundamental and second-harmonic frequencies, and WR-6 waveguide spacers to optimise the location of the reactive termination at the fundamental frequency. With 350 μm-thick spacers, the oscillator yielded an RF output power of more than 85 μW at 479.01 GHz.

Introduction: Third-harmonic power extraction from GaAs tunnel injection transit-time (TUNNETT) diodes and InP Gunn devices was demonstrated recently with output powers exceeding 140 μW at 355 GHz [1] and 280 μW at 412 GHz [2]. For the experiments with InP Gunn devices, a WR-1.7 → 3 waveguide transition was used to provide the Gunn device with virtually reactive terminations as close to it as possible, at the fundamental and second-harmonic frequencies. This waveguide transition sufficiently blocks all signals at frequencies below approximately 305 GHz [2]. Therefore, the evaluation of Gunn devices that had shown state-of-the-art performance in a second-harmonic mode was limited to frequencies below approximately 460 GHz. For example, the InP Gunn device with a second-harmonic output power of 1.6 mW at 329 GHz [3] could not be tested correctly as some fraction of this second-harmonic power leaked through to the power meter. A WR-1.5 → 3 waveguide transition blocks all signals at frequencies below 340 GHz, but its reduced aperture area compared to a WR-1.7 → 3 transition prevented sufficient coupling of the third-harmonic electric field into the WR-1.5 waveguide and the performance was poor. This role of efficient coupling into the waveguide aperture was also verified with an InP Gunn device at 412 GHz [2] where a WR-1.9 → 3 waveguide transition increased the measured output power from 283 to 330 μW. As a consequence of these findings, a different waveguide configuration was explored for third-harmonic power extraction around 480 GHz.

Experimental procedure: The device, with an output power of 1.6 mW at 329 GHz, had a graded doping profile, which was designed for efficient second-harmonic power extraction at 240 GHz and above [3]. The device's exact diameter was not recorded before packaging, but it is estimated to be in the range 25–35 μm. The device was mounted on a diamond heatsink for efficient heat management [3]. Fig. 1 shows the configuration for third-harmonic power extraction. It uses the same WR-6 waveguide cavity and tunable back short as for second-harmonic power extraction [3]. The aperture at the WR-3 side of the WR-3 → 1.5 transition is much wider and allows for efficient coupling into the waveguide, but the signal at the fundamental frequency is still blocked, which provides the virtually reactive termination as close as possible to the Gunn device. The signal at the second-harmonic frequency is also blocked, but further down this transition. The subsequent WR-1.7 → 3 (or WR-1.9 → 3) waveguide transition connects the oscillator either to the WR-3 → 10 waveguide transition of the waveguide-based broadband power meter (PM3, Erickson Instruments, USA) [4] or the WR-3 waveguide of the *J*-band (220–325 GHz) harmonic mixer (M03HWD, OML, USA) [2]. A slightly larger waveguide size was chosen for the second transition to reduce negative effects from any misalignment that may occur during assembly.

The distance between the locations of the Gunn device and the reactive termination at the fundamental frequency was varied by inserting one or two WR-6 waveguide spacers with total thicknesses of 100–400 μm between the oscillator and the WR-3 flange of the waveguide transition [2]. The readings of the power meter PM3 were corrected by 1.6 dB to account for the losses in the two WR-1.7 → 3 → 10 waveguide transitions to the PM3 and in the waveguide section inside the PM3 sensor (correction setting 0%) [2]. The WR-3 → 1.5 waveguide transition was regarded as an integral part of the oscillator and its attenuation of the third-harmonic output signal was therefore not corrected.

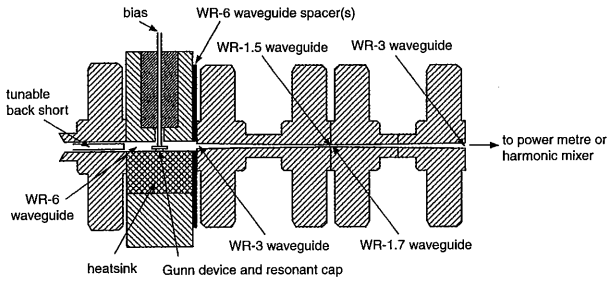

Fig. 1 *Schematic of WR-6 waveguide cavity and two waveguide transitions for third-harmonic power extraction*

A series resistor of 1 Ω and a large parallel capacitor (>50 mF) were used to filter out any unwanted noise signals from the DC power supply. Such noise signals (of less than 1 mV) caused appreciable frequency modulation of the Gunn oscillator in the experiments of [2], and prevented the use of small resolution bandwidths with the spectrum analyser for a reduction of the noise floor.

Results and discussion: An output power of 18 μW was first measured without a waveguide spacer. This output power was too low to determine the oscillation frequency with the spectrum analyser (FSU46, Rohde & Schwarz, Germany) connected to the aforementioned *J*-band harmonic mixer. Contrary to the findings of [2], the use of one or two WR-6 waveguide spacers significantly affected the third-harmonic output power from the oscillator. Table 1 summarises the results obtained without a spacer and with total spacer thicknesses of 100–400 μm. The highest output power of 86 μW was obtained at 479.01 GHz with 350 μm-thick spacers. Fig. 2 shows the very clean spectrum of the oscillator in this configuration.

Table 1: RF output power and third-harmonic oscillation frequency for different WR-6 waveguide spacer thicknesses

Spacer thicknesses [μm]	0	100	250	250 + 100	250 + 150
RF output power [μW]	18	32	54	86	68
Oscillation frequency [GHz]	n/a	483.052	480.446	479.014	n/a
'Stability' (see text)	−−	−	++	++	++

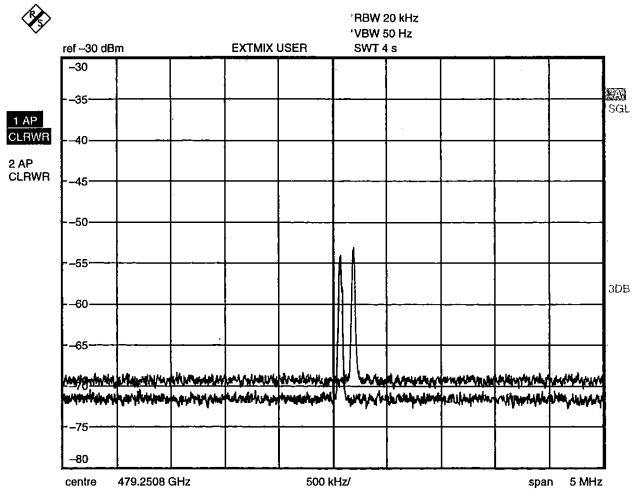

Fig. 2 *Spectrum of free-running InP Gunn device oscillator in third-harmonic mode (total spacer thickness 350 μm)*

RF output power: 0.077 mW; centre frequency: 479.25 GHz; vertical scale: 5 dB/div; horizontal scale: 500 kHz/div; resolution bandwidth: 20 kHz; video bandwidth: 50 Hz; reference level not calibrated