RESEARCH   **Open Access**

Chaos-based true random number generators

Luis L Bonilla*, Mariano Alvaro and Manuel Carretero

*Correspondence:
bonilla@ing.uc3m.es
Gregorio Millán Institute for Fluid
Dynamics, Nanoscience and
Industrial Mathematics, Universidad
Carlos III de Madrid, Avenida de la
Universidad 30, Leganés, 28911,
Spain

Abstract

Random number (bit) generators are crucial to secure communications, data transfer and storage, and electronic transactions, to carry out stochastic simulations and to many other applications. As software generated random sequences are not truly random, fast entropy sources such as quantum systems or classically chaotic systems can be viable alternatives provided they generate high-quality random sequences sufficiently fast. The discovery of spontaneous chaos in semiconductor superlattices at room temperature has produced a valuable nanotechnology option. Here we explain a mathematical model to describe spontaneous chaos in semiconductor superlattices at room temperature, solve it numerically to reveal the origin and characteristics of chaotic oscillations, and discuss the limitations of the model in view of known experiments. We also explain how to extract verified random bits from the analog chaotic signal produced by the superlattice.

Keywords: random bit generator; semiconductor superlattice; deterministic and stochastic chaos

1 Background

Generation of random numbers at high speed is at the core of many activities of economic importance. Online gambling, finance, computer telecommunications, online commerce and data encryption systems, [1–3], stochastic modeling [4], and Monte Carlo simulations [5] among many others, rely on fast random number generators (RNGs). We also talk about random bit generators (RBGs) when emphasizing that binary numbers are produced. Usually, these generators are based on numerical algorithms that produce seemingly unpredictable number sequences. The generator is a function whose input is a short random seed, and whose output is a long stream which is indistinguishable from truly random bits. Such numerical strings yield the keys for secure storage and transmission of data. This conventional approach is cheap and fast, as it is limited only by the processor speed. However, the number sequences thus produced are only pseudorandom, as two identical programs that begin at the same state will produce the same sequence. Then vulnerability in the pseudorandom number generator (PRNG) may follow, as it famously was the case for Microsoft Windows operating system secure encryption several years ago [6].
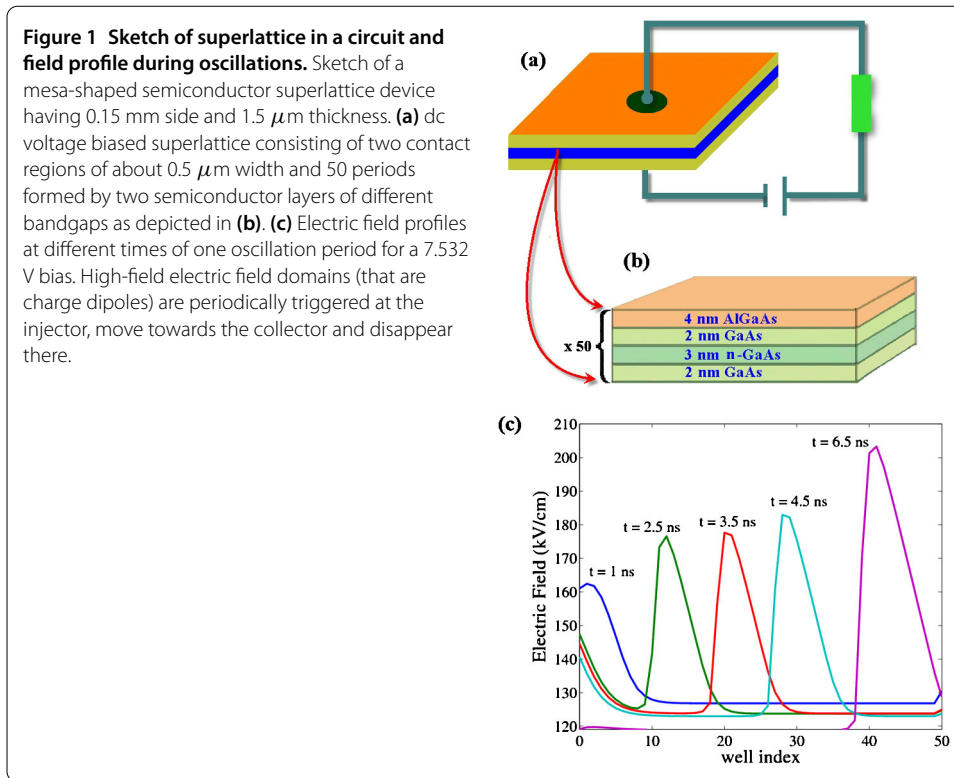
To get cryptographically secure PRNGs, it is convenient to have generated truly random numbers that may be obtained ideally from inherently random or unpredictable processes. Deterministic processes that are difficult to predict have been used in gambling

since antiquity. For instance, the mechanics of coin tossing shows that small uncertainties in the initial condition ensure equal probability of heads and tails provided some parameter (e.g., initial velocity) is large enough [7, 8]. Similar analyses apply to the case of rolling dice, card shuffling or spinning a roulette wheel. An obvious drawback of these mechanical methods is that they are too slow for practical use. Other physical sources of entropy are too sensitive to external influences and lack robustness, for example, thermal noise or electrical noise in diodes and resistors. These physical processes yield a low analog signal and are easily affected by disturbances including temperature fluctuations. More robust systems are based on quantum mechanical uncertainty, e.g., on whether a photon is detected, but they are limited to relatively low rates of number generation (tens of Mb/s) [9, 10]. Recently, fast generation of truly random numbers (tens or hundreds of Gb/s) has been achieved using chaotic semiconductor lasers [11–14] and superlattices [15]. In both cases, quantum fluctuations are amplified by chaotic dynamics to a macroscopic fluctuating signal. This signal can be detected by using conventional electronics that is much faster than optical photon counting detectors. While semiconductor lasers require a mixture of optical and electronic components, semiconductor superlattices are all electronic submicron devices that can be integrated in more complex circuits. As of now, these two types of devices have been shown to reliably produce truly random sequences of numbers at fast rates in laboratory experiments. If they show to be scalable, these devices could be vastly useful, as the performance and reliability of our digital networked society relies on the ability to generate fast and cheaply large quantities of random numbers.

In this paper, we comment the possible use of spontaneously chaotic semiconductor superlattices (SLs) as true random number generators. In Section 2, we discuss the mathematical model for a single SL under voltage bias. The model consists of a number of coupled stochastic differential equations together with algebraic boundary and voltage bias conditions. In Section 3.1, numerical solutions of the model equations show that the thermal and shot noises existing in the SL enhance stable spontaneous chaos in voltage intervals where the corresponding deterministic model exhibits chaos. The noises also induce chaos in nearby voltage intervals where the deterministic system had periodic oscillations. We also discuss the relation of our results to experiments and which features of the model need to be revised in order to optimize the chaotic oscillations. In Section 3.2 and following Ref. [15], we explain how to obtain a high-speed true random bit generator by processing the chaotic current oscillations provided by the device. Section 4 summarizes our findings and perspectives for fast random bit generators based on semiconductor superlattices. Two Appendices provide details on the derivation of the model equations.

2 Mathematical model and methods for a single superlattice

SLs are artificial crystals whose periods comprise two very wide layers of different semiconductors having similar lattice constants. For example, one period may consist of a few monolayers of gallium arsenide (GaAs) and a few monolayers of aluminum gallium arsenide (AlGaAs), as in Figures 1(a) and (b). Since the two semiconductors have different bandgaps, an electron moving in the SL growth direction at zero applied electric field sees the potential energy profile of each period, of length l, as a well, of width d_W, followed by a barrier, of width d_B. $l = d_W + d_B$. Solving the Schrödinger equation for a one-dimensional periodic potential with rectangular barriers and wells produces a continuum spectrum formed by a succession of minibands and minigaps. The miniband width depends on the electron wavenumber times the barrier width: as this product increases, the

Figure 1 Sketch of superlattice in a circuit and field profile during oscillations. Sketch of a mesa-shaped semiconductor superlattice device having 0.15 mm side and 1.5 μm thickness. **(a)** dc voltage biased superlattice consisting of two contact regions of about 0.5 μm width and 50 periods formed by two semiconductor layers of different bandgaps as depicted in **(b)**. **(c)** Electric field profiles at different times of one oscillation period for a 7.532 V bias. High-field electric field domains (that are charge dipoles) are periodically triggered at the injector, move towards the collector and disappear there.

miniband width strongly decreases [16]. In the limit of infinite wavenumber times width, the miniband widths vanish and the spectrum corresponds to that of an isolated quantum well (QW). Superlattices with wide (narrow) minibands are said to be strongly (weakly) coupled [17]. Superlattice layered materials are now routinely grown by molecular beam epitaxy as wafers that are then processed into a number of cylindrical mesas of very large circular or square section (50 to 100 microns are the typical radii or sides). Contact regions are attached to the ends of the SL that are then integrated in a circuit, as sketched in Figure 1(a).

SLs were proposed in 1970 by Esaki and Tsu to develop a device that exhibits Bloch oscillations [18]. Although such oscillations were observed in experiments years later [19], no practical device using them has been so far developed. Instead, SLs have been used to build gigahertz oscillators for communications purposes, detectors for terahertz signals or infrared radiation and quantum-cascade lasers commercially used for a variety of purposes, such as environmental sensing and pollution controlling, industrial processes control (e.g., combustion control, converter diagnosis, collision avoiding radar in automotive industry), medical applications (breath analysis, early detection of ulcers), etc. [17]. In 2012, experiments demonstrated the existence of spontaneously chaotic oscillations of the current through a SL at room temperature under voltage bias, as in the sketch of Figures 1(a) and (b) [20]. This paved the way to using SLs as true random number generators [15].

Modeling electron transport in a SL is a bit more complicated than modeling mass transport in a fluid. One first thought could be following the route from Boltzmann equation to Navier-Stokes equations, as done in the kinetic theory of gases [21], and advocated in the mathematical literature on semiconductors [22, 23]. This has achieved some success in

the case of strongly coupled SLs [24, 25], but none so far for weakly coupled SLs, as those displaying spontaneous chaos in experiments [15, 20]. The main reason for this failure is that Boltzmann-type equations for SLs are based on electrons populating minibands at zero electric field, and such a picture is far from reality in the presence of electric fields that are sufficiently strong: $eFl > \Delta$, where $-e < 0$ is the electron charge, $-F$ the electric field, l the SL period and Δ is the miniband width [17].

2.1 Model

For chaotic phenomena in weakly coupled SLs, $\Delta \ll eFl$, and different modeling is called for. One key observation is that the miniband widths are small compared with the broadening of the energy levels due to scattering, $\hbar/\tau_{sc}$, and to the typical values of the electrostatic energy per SL period, eFl. Thus, the escape time from a QW $\tau_{esc} \sim l/\nu_M \sim \hbar/\Delta$ (ν_M and F_M are typical electron velocities and electric fields during oscillations) is much larger than the scattering time, τ_{sc}. This implies that the electron distribution in the wells is in local equilibrium [26]. Moreover, the dielectric relaxation time $\tau_{di} \sim Nl_{di}/\nu_M \sim N\varepsilon F_M\tau_{esc}/(eN_D)$ (ε is the SL dielectric constant, N_D is the two-dimensional (2D) doping density, and N is of the order of the number of SL periods), in which the current density across the SL reacts to sudden changes in the electric field profile, is typically larger than the escape time. Therefore, we can assume that the tunnelling current density between quantum wells is stationary on the longer time scale of the dielectric relaxation time [26]. A minimal theory of charge transport in weakly coupled SLs should therefore specify (i) which slowly varying magnitudes characterize the local equilibrium distribution function in the wells (at least the electric field and the electrochemical potential or the electron density), (ii) the equations relating these magnitudes (e.g. the charge continuity and the Poisson equation) and (iii) how to close these equations by calculating the necessary relations between magnitudes (e.g. the stationary tunnelling current between adjacent wells). In our simulations, we have added intrinsic noise to the usual sequential tunneling model of electron transport in a weakly coupled n-doped SL [17, 27, 28]

$$\varepsilon dF_i + J_{i\to i+1}\,dt + \sqrt{\xi_i}\,dW_i = J(t)\,dt, \tag{1}$$

$$J_{i\to i+1} = \frac{en_i}{l}\nu^{(f)}(F_i) - J^-_{i\to i+1}(F_i, n_{i+1}, T), \tag{2}$$

$$n_i = N_D + \frac{\varepsilon}{e}(F_i - F_{i-1}). \tag{3}$$

Here $i = 1, \ldots, N$ ($N = 50$ is the number of SL periods [20]) and the Ito stochastic differential equations (1) are current balance (Ampère) equations. Together with the Poisson equation (3), they ensure charge continuity, as time differentiation of (3) and use of (1) yield

$$edn_i = [J_{i-1\to i}\,dt + \sqrt{\xi_{i-1}}\,dW_{i-1}] - [J_{i\to i+1}\,dt + \sqrt{\xi_i}\,dW_i]. \tag{4}$$

The 2D electron density n_i is given by the Poisson equation (3), in which the equivalent 2D doping density due to the doping of the central part of the QW is $N_D = 6 \times 10^{10}$ cm^{-2}. $J_{i\to i+1}$, $\sqrt{\xi_i}\,dW_i/dt$, $J(t)$ are the tunneling current density from well i to well $i + 1$, the corresponding zero-mean fluctuating current density, and the total current density, respectively. The tunneling current density in Eq. (2) from well i to $i + 1$ depends on the electric field F_i in

well i and the 2D electron densities in the corresponding wells, n_i and n_{i+1}, according to the formulas [27, 28]

$$J^-_{i \to i+1}(F_i, n_{i+1}, T) = \frac{em^* k_B T}{\pi \hbar^2 l} \nu^{(f)}(F_i) \ln\left[1 + e^{-\frac{eF_i l}{k_B T}}\left(e^{\frac{\pi \hbar^2 n_{i+1}}{m^* k_B T}} - 1\right)\right], \tag{5}$$

$$\nu^{(f)}(F_i) = \sum_{j=1}^{n} \frac{\frac{\hbar^3 l(\gamma_{C1} + \gamma_{Cj})}{2m^{*2}} \mathcal{T}_i(\epsilon_{C1})}{(\epsilon_{C1} - \epsilon_{Cj} + eF_i l)^2 + (\gamma_{C1} + \gamma_{Cj})^2}, \tag{6}$$

$$\mathcal{T}_i(\epsilon) = \frac{16 k_i^2 k_{i+1}^2 \alpha_i^2 (k_i^2 + \alpha_i^2)^{-1}(k_{i+1}^2 + \alpha_i^2)^{-1}}{(d_W + \alpha_{i-1}^{-1} + \alpha_i^{-1})(d_W + \alpha_{i+1}^{-1} + \alpha_i^{-1}) e^{2\alpha_i d_B}}, \tag{7}$$

$$\hbar k_i = \sqrt{2m^* \epsilon}, \qquad \hbar k_{i+1} = \sqrt{2m^*(\epsilon + elF_i)}, \tag{8}$$

$$\hbar \alpha_{i-1} = \sqrt{2m^*\left[eV_B + e\left(d_B + \frac{d_W}{2}\right)F_i - \epsilon\right]}, \tag{9}$$

$$\hbar \alpha_i = \sqrt{2m^*\left[eV_B - \frac{ed_W F_i}{2} - \epsilon\right]}, \tag{10}$$

$$\hbar \alpha_{i+1} = \sqrt{2m^*\left[eV_B - e\left(d_B + \frac{3d_W}{2}\right)F_i - \epsilon\right]}. \tag{11}$$

These formulas are obtained by writing the electron Hamiltonian as a sum of eigenstates of the electron in each QW plus a small term that expresses the possible motion from one QW to its adjacent wells by tunneling across the barrier separating them; see Appendix 1 and Ref. [29]. Then the tunneling current density is obtained by first-order perturbation theory in the tunneling term and use of the transfer Hamiltonian method [17, 29]. The integrals appearing in the tunneling current are further approximated by asymptotic methods as explained in Appendix A of Ref. [30]. The forward velocity $\nu^{(f)}(F_i)$ is a function given in [17, 28, 30] with peaks corresponding to three energy levels $\mathcal{E}_{Cj}$ at 53, 207, and 440 meV calculated by solving a Kronig-Penney model for the SL configuration of References [15, 20, 31]. The level broadenings due to scattering, γ_{Cj}, are 2.5, 8 and 24 meV, respectively, for the three energy levels [28]. The energy barrier in the absence of potential drops, eV_B, depends on the fraction x of Al in the barriers, $x = 0.45$ for the SLs of Refs. [15, 20, 31]. In this paper, we have used $eV_B = 600$ meV. Also $m^* = (0.063 + 0.083x)m_e = 0.1m_e$ (for $x = 0.45$), m_e, $d_B = 4$ nm, $d_W = 7$ nm, $l = d_B + d_W$, $\varepsilon = l/[\frac{d_W}{\varepsilon_W} + \frac{d_B}{\varepsilon_B}]$, $\varepsilon_B = 10.9\epsilon_0$, $\varepsilon_W = 12.9\epsilon_0$, ϵ_0, k_B, and T, are the effective electron mass, the electron mass in vacuum, the (Al, Ga)As barrier thickness, the GaAs well thickness, the SL period, the SL permittivity, the barrier permittivity, the well permittivity, the dielectric constant of the vacuum, the Boltzmann constant, and the lattice temperature, respectively.

The coefficients of the independent identically distributed Brownian motions dW_i in (1) represent the correlations of internal noise due to shot and thermal noise [32]. Shot noise in SLs has been considered in Ref. [33] for a somewhat simpler discrete transport model and in Ref. [34] for the discrete transport model we solve in this paper. We also consider current fluctuations associated to dissipation due to electron diffusion and model them by Landau-Lifshitz fluctuating hydrodynamics [35, 36] adapted to SLs; see Appendix 2. The

resulting formula is:

$$
\xi_i = \frac{e}{A} \Bigg[\frac{e v^{(f)}(F_i)}{l} n_i + J^{-}_{i \to i+1}(F_i, n_{i+1}, T)
$$

$$
+ \frac{2 e m^* k_B T}{\pi \hbar^2 l} v^{(f)}(F_i) \frac{e^{-\frac{eF_i l}{k_B T}} (e^{\frac{\pi \hbar^2 n_i}{m^* k_B T}} - 1)}{1 + e^{-\frac{eF_i l}{k_B T}} (e^{\frac{\pi \hbar^2 n_i}{m^* k_B T}} - 1)} \Bigg], \tag{12}
$$

in which $A = s^2$ is the SL cross section of a square mesa with side $s = 120\ \mu$m. The current density at the contacts and the voltage bias condition are

$$
J_{0 \to 1} = \sigma_0 F_0, \qquad J_{N \to N+1} = \sigma_0 \frac{n_N}{N_c} F_N, \tag{13}
$$

$$
\sum_{i=1}^{N} F_i = \frac{V + \eta(t)}{l}. \tag{14}
$$

Here V is the dc voltage, $\eta(t)$ is a fluctuation due to the voltage source and σ_0 and N_c are the contact conductivity, and the equivalent 2D doping density of the anode region, respectively [27].

The mathematical model we use has some limitations that may have to be overcome in more precise future studies. It corresponds to an idealized SL in which all periods have identical values of d_W, d_B, N_D, and V_B. The effective mass m^* and permittivity ε are the same irrespective on whether they correspond to a barrier or a well. In addition, the model does not include 2D effects due to imperfect growth: barrier and well widths may vary in the SL cross section perpendicular to the growth direction. Some of these effects were addressed in [37].
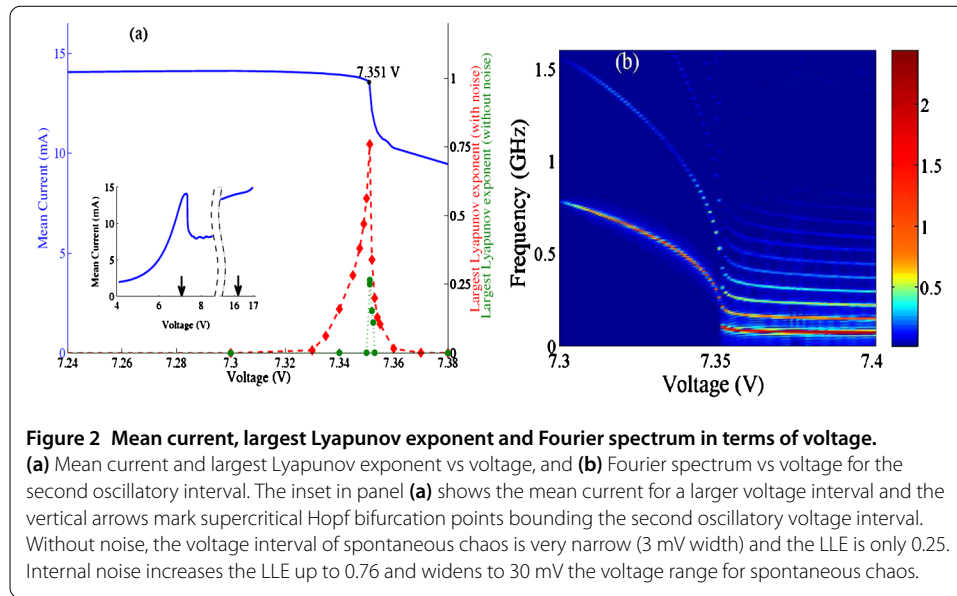
2.2 Methods

We have solved the stochastic model given by Eqs. (1)-(14) with $\eta(t) = 0$ (internal noise only) for the SL of Refs. [15, 20, 31] at 300 K using a standard stochastic Euler-Maruyama method (explicit Euler method corresponding to Ito integration) [38]. Coding of the numerical method follows the indications in Ref. [39]. To calculate the largest Lyapunov exponent (LLE), we have simultaneously integrated all perturbed and unperturbed trajectories during 10,000 ns and used the Benettin *et al.* algorithm [40] with a renormalization period of 1 ns. LLE calculations with the Gao *et al.* algorithm [41] give similar results.

3 Results and discussion

3.1 Spontaneous chaotic oscillations

Spontaneous chaos at room temperature has been observed in quite recent experiments with voltage biased, doped, weakly coupled SLs [15, 20]. Before the 2012 experiments, spontaneous chaos was observed only at very low temperatures (from 4 to 77 K) [42]. The new key modification that allows observing oscillations of the current at room temperature is adding 55% of gallium in the barriers. The technical reasons are discussed in [20] and references cited therein. Early theoretical explanations of spontaneous chaotic oscillations at low temperature are based on complex dynamics of wave front solutions [43] when applied to discrete model equations such as those of Section 2; see Ref. [44]. At
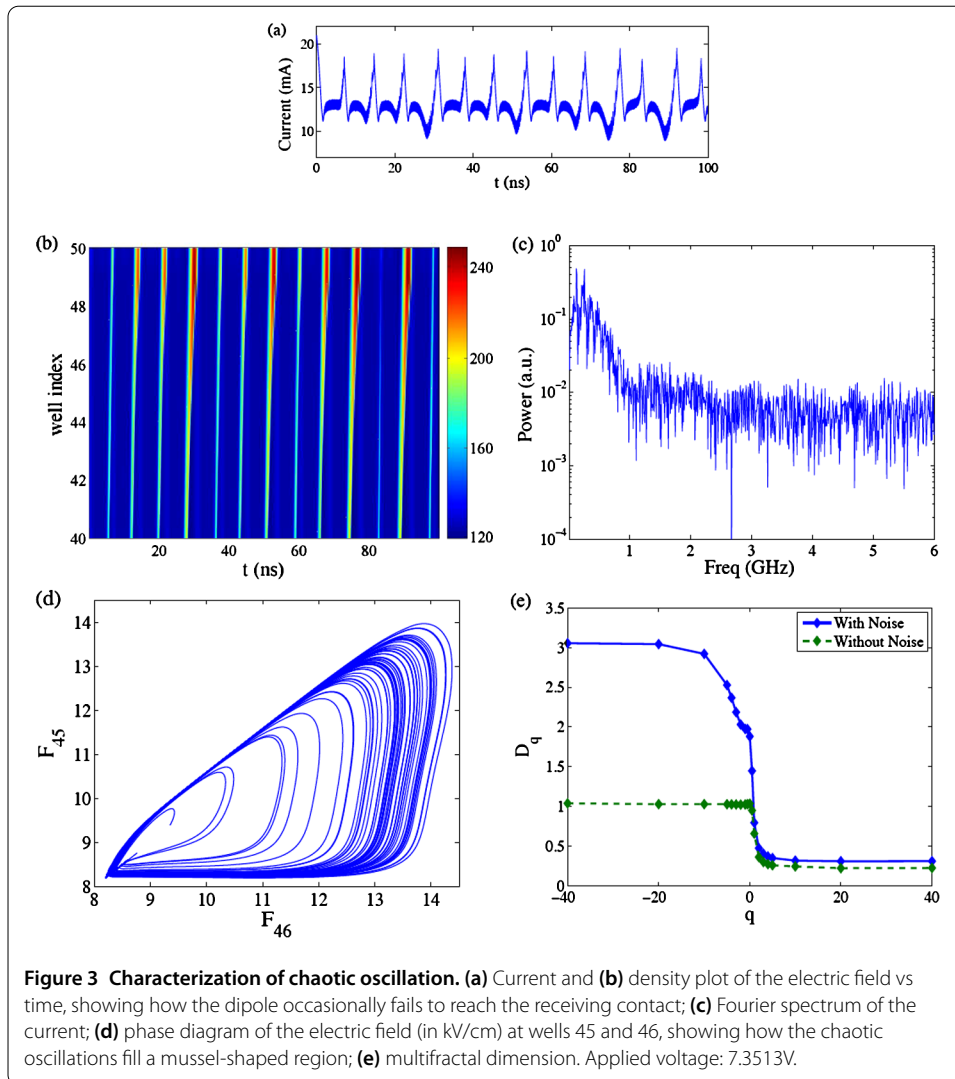
Figure 2 Mean current, largest Lyapunov exponent and Fourier spectrum in terms of voltage.
(a) Mean current and largest Lyapunov exponent vs voltage, and **(b)** Fourier spectrum vs voltage for the second oscillatory interval. The inset in panel **(a)** shows the mean current for a larger voltage interval and the vertical arrows mark supercritical Hopf bifurcation points bounding the second oscillatory voltage interval. Without noise, the voltage interval of spontaneous chaos is very narrow (3 mV width) and the LLE is only 0.25. Internal noise increases the LLE up to 0.76 and widens to 30 mV the voltage range for spontaneous chaos.

room temperature, wave fronts are not sharp, and spontaneous chaos arises due to other reasons, as explained in Ref. [27] and in what follows.

3.1.1 Internal noise induces and enhances chaos

We have found self-sustained oscillations in two voltage intervals that appear as plateaus in the SL current-voltage characteristics, for $V < (\mathcal{E}_{C2} - \mathcal{E}_{C1})/e$ and for $V > (\mathcal{E}_{C2} - \mathcal{E}_{C1})/e$. At the left end of both intervals, small-amplitude current oscillations appear as supercritical Hopf bifurcations from the stationary state. They are caused by the repeated creation of field pulses that dissolve before arriving at the collector. The range of voltages for which this behavior is observed is much narrower on the first voltage interval than on the second one. On both voltage intervals, oscillations die via supercritical Hopf bifurcations. The reverse tunneling current $J^-_{i \to i+1}$ given by (5) is much larger for the smaller fields at the first voltage plateau than for the larger fields at the second plateau. The internal noise is correspondingly larger compared with the mean current at the first plateau. Spontaneous chaotic oscillations in the first voltage interval were discussed in Ref. [27]. Here we shall present similar results obtained for voltages on the second plateau.

In the second voltage interval, small-amplitude current oscillations appear as a supercritical Hopf bifurcation from the stationary state. These oscillations correspond to the periodic creation of field pulses (charge dipoles) that die before arriving at the collector. An abrupt drop of the mean current in Figure 2(a) and a transition to an oscillation of richer harmonic content in the spectrum of Figure 2(b) mark the voltage beyond which the field pulses move throughout the whole SL as in Figure 1(c), and produce a large-amplitude current oscillation. The extra frequency appearing at the transition in Figure 2(b) suggests that the first oscillation becomes unstable because two complex conjugate Floquet multipliers thereof leave the unit circle, which would suggest a scenario of a direct route from a two-frequency quasiperiodic attractor to chaos [45]. That two oscillatory modes are present in the observed spontaneous chaotic oscillations is commented in Ref. [31], whose authors identify them as the dipole motion mode and the well-to-well hopping mode. In our simulations, they should correspond to the fully developed dipole motion

Figure 3 Characterization of chaotic oscillation. (a) Current and **(b)** density plot of the electric field vs time, showing how the dipole occasionally fails to reach the receiving contact; **(c)** Fourier spectrum of the current; **(d)** phase diagram of the electric field (in kV/cm) at wells 45 and 46, showing how the chaotic oscillations fill a mussel-shaped region; **(e)** multifractal dimension. Applied voltage: 7.3513V.

of Figure 1(c) and to the confined dipole motion, respectively. Just after the mean current peak in Figure 2(a), there is a voltage interval of positive LLE that indicates sensitivity to initial conditions characteristic of a chaotic attractor.

Figure 2(a) shows that the LLE is positive in a narrow voltage interval of the deterministic system. Internal noise both widens this interval and increases the LLE. At voltage values for which the LLE is positive for the stochastic system but not for the deterministic system, noise induces chaos. At voltages for which the deterministic system has a positive LLE, noise enhances chaos, something already demonstrated for simple dynamical systems [41, 46]. This picture is confirmed by examining the chaotic attractor. At the voltage marked in Figure 2(a) corresponding to the maximum value of the LLE, the fluctuations create a mussel-shaped *multifractal* chaotic attractor out of the above mentioned small and large amplitude oscillatory modes, as shown in Figure 3(d). The current trace shows several irregularly separated large spikes whereas many small spikes occur between two large ones. The large spikes indicate nucleation of a new dipole at the injector whereas small current spikes (between two large ones) mark the well-to-well advance of the charge accumulation layer at the back of a dipole. Then the number of small spikes in Figure 3(a)

and the density plot in Figure 3(b) show that shorter time separations between two large spikes correspond to the formation of a dipole that dissolves before reaching the collector. Longer separations between consecutive large spikes correspond to a dipole that reaches the collector, as in Figure 1(c). Thus, two different oscillation modes are observable in the chaotic attractor: injector-to-collector dipole motion and dipole motion from injector to premature annihilation inside the SL. The latter corresponds to the well-to-well hopping mode postulated in Ref. [31]. The inter-spike intervals are similar but never repeat themselves and tend to produce a mussel-shaped attractor in the phase plane of the field at two adjacent wells as depicted in Figure 3(d). Noise increases the multifractal dimension D_q of the deterministic attractor as shown in Figure 3(e). In Figure 3(a), the mean oscillation amplitude (understood as difference between the peak and the valley currents) is $\sim$8 mA, the mean interspike interval is $\sim$7.5 ns, and there are 13 large peaks in a 100 ns time interval. Our values are quite close to those observed in the experiments, $\sim$8 mA mean oscillation amplitude and $\sim$6.5 ns mean interspike interval, with 15 large spikes in a 100 ns interval [15]. What is the role of fluctuations in the creation of spontaneous chaos? Without noise, the LLE reaches a maximum value of 0.25 in a narrow voltage interval, whereas the fluctuations widen this interval and enhance the LLE up to 0.76. The internal noise due to fluctuations of the current enhances spontaneous chaos, increases its fractal dimension and induces chaos in voltage regions adjacent to those of purely deterministic chaos. Voltage fluctuations widen the voltage interval of spontaneous chaos.
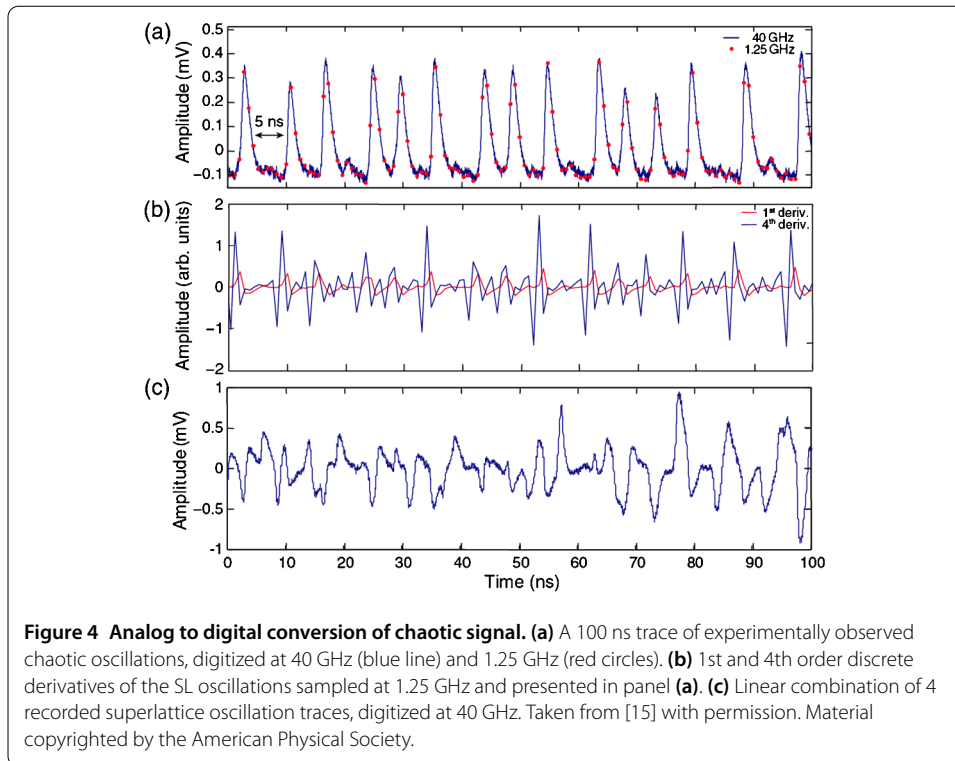
3.1.2 Comparison with experiments

Experiments [15, 20, 31] show that oscillations appear for voltages on the first plateau and that they have frequencies about 7.5 times larger than those predicted by simulations of our mathematical model [27]. The current spikes observed in experiments are more irregular than those appearing in simulations. These features of oscillations observed in experiments point to the presence of imperfections not taken into account in the model. In earlier work on the role of imperfections [37], numerical simulations of a related discrete model showed that a 3% fluctuation in doping density could increment by a factor of 5 the oscillation frequency. Obvious imperfections that should be taken into account in our model include: (i) fluctuations of the doping density, (ii) fluctuations in d_B and d_W, (iii) fluctuations in V_B. Once imperfections are included in the mathematical model, we can pose the objective of *optimizing chaos*, i.e., introducing intentional imperfections so as to widen the voltage intervals for which there are chaotic oscillations, and increase the LLE and the complexity of attractors. These features would increase the usefulness of the device as a true random number generator.

3.2 Random Bit Generation from chaotic oscillations

There are a number of ways to obtain a RBG out of a chaotic signal. In this section, we will explain the methods used by Li *et al.* [15], using one of the figures they extracted from experimental measurements.

Figure 4(a) shows a 100 ns trace of experimentally observed chaotic oscillations, digitized (with an 8-bit resolution) at 40 GHz (blue line) and 1.25 GHz (red circles). As in Figure 3(a), the signal has large peaks, corresponding to pulse generation, and smaller spikes that mark the advance of a pulse toward the collector and may be quite influenced by random noise. At 1.25 GHz sampling rate, a significant number of the sampling measurements occur between large peaks, resulting in degraded randomness of the generated

Figure 4 Analog to digital conversion of chaotic signal. (a) A 100 ns trace of experimentally observed chaotic oscillations, digitized at 40 GHz (blue line) and 1.25 GHz (red circles). **(b)** 1st and 4th order discrete derivatives of the SL oscillations sampled at 1.25 GHz and presented in panel **(a)**. **(c)** Linear combination of 4 recorded superlattice oscillation traces, digitized at 40 GHz. Taken from [15] with permission. Material copyrighted by the American Physical Society.

bit sequence. To overcome this limitation, we may calculate a high order derivative to mix data sampled in a window between large peaks with nearby random spikes. For the case of a 1.25 GHz sampling rate, the 4th discrete derivative mixes data from 5 consecutive measurements which are separated by $\Delta = 0.8$ ns, at times t, $t - \Delta$, $t - 2\Delta$, $t - 3\Delta$, and $t - 4\Delta$. Hence, each derived data point used for the generation of the random bit sequence mixes 4 ns of information, which is close to the average period of the oscillation (5 ns), as indicated in Figure 4(a). Thus this time window includes, with a high probability, combined data taken from a chaotic current peak and the interval between large peaks. Figure 4(b) shows the 1st and 4th derivatives of the signal in Figure 4(a), sampled at 1.25 GHz. Whereas for the 1st derivative many points have values near zero, the 4th derivative values fluctuate at all time scales and it has a number of peaks comparable to the number of large peaks in Figure 4(a).

The generation of the random bit stream from the chaotic consists of the following two steps. First, we calculate the nth derivative using $n + 1$ successive values of the recorded signal. Second, we append the m least significant bits (LSBs) of the results of the nth derivative to the bit sequence. Recall that the LSBs are the most sensitive to small fluctuations. Using $n = 4$ and retaining $m = 5$ LSBs out of 8 bits, truly random bits are generated at 6.25 Gbit/s using a sampling rate of 1.25 GHz [15]. For higher sampling rates, larger values of n are needed to achieve verified randomness using the NIST statistical test suite [47]. Then a more efficient method is to use a linear combination of chaotic signals to fill the time interval between large peaks. These signals may come from different SLs or from far segments of the recorded chaotic signal of a single SL, as in [15]. In the latter case, the chaotic nature of the signal ensures lack of correlation between the segments thereof. To minimize the possible emergence of bias in the combined analog signals, each pair of signals is combined by subtraction [4]. Figure 4(c) shows a linear combination SL1 + SL3 −

SL2 – SL4 of four uncorrelated traces of the chaotic signal, digitized at 40 GHz. Li *et al.* obtained a 40 Gbit/s RBG with verified randomness using such a linear combination, a 10 GHz sampling rate and 4 LSBs. They obtained a faster rate verified RBG by combining 6 signals and a faster sampling rate. See [15] for details.

4 Conclusions

The discovery of fast spontaneous chaotic oscillations of the current through semiconductor superlattices at room temperature brings to light their possible applications as true random bit generators [15]. Fast true random bit generators coming from tiny submicron all-electronic devices could be invaluable in secure communications and data storage. In this paper, we have discussed a mathematical model to describe spontaneous chaos in *idealized* superlattices with identical wells and barriers. Our numerical simulations show that spontaneous chaos possibly may appear directly from a two-frequency quasiperiodic attractor. We have also shown that the unavoidable shot and thermal noises existing in the nanostructure both enhance existing deterministic chaos (increasing its fractal dimension and largest Lyapunov exponent) and induce chaos in nearby voltage intervals. We have discussed that the differences between numerical and experimental results may be due to imperfections in the doping density, the gallium content in the barriers, and the size thereof. A better model needs to be developed to discuss the imperfections and their effect in the chaotic oscillations: ideally we could tune chaos via the introduction of controlled imperfections. We also explain how to extract verified random bit generators from a chaotic signal by digitalization and extraction of least significant bits from high order numerical derivatives, or by combining several chaotic signals coming either several superlattices or from far apart segments of the same long chaotic signal.

Appendix 1: Derivation of deterministic tunneling currents

We use the methods of Ref. [29]. The tunneling Hamiltonian is

$$H_{\text{total}} = H + H_T = \sum_{i=0}^{N+1} H_i + \sum_{j=0}^{N} H_{T_j}, \tag{A.1}$$

$$H_i = \sum_{\mathbf{k}_i} E_{i\mathbf{k}_i} c_{i\mathbf{k}_i}^\dagger c_{i\mathbf{k}_i}, \qquad H_{T_j} = \sum_{\mathbf{k}_j \mathbf{k}_{j+1}} \left(T_{\mathbf{k}_j \mathbf{k}_{j+1}} c_{j+1\mathbf{k}_{j+1}}^\dagger c_{j\mathbf{k}_j} + H.c. \right). \tag{A.2}$$

Here the Hamiltonian H is a sum of individual Hamiltonians for each QW or contact and assumes that they are uncoupled from one another. H.c. stands for the Hermitian conjugate of the preceding term. The unperturbed single-electron states have absolute energies denoted by $E_{i\mathbf{k}_i}$ measured from the conduction band edge in the emitter contact. The operators $c_{i\mathbf{k}_i}^\dagger$ and $c_{i\mathbf{k}_i}$ denote creation and annihilation operators for electrons in the ith well or contact with three-dimensional wave vector $\mathbf{k}_i$ and satisfy standard fermionic commutation rules: $\{c_{i\mathbf{k}_i}, c_{j\mathbf{k}_j}\} = c_{i\mathbf{k}_i} c_{j\mathbf{k}_j} + c_{j\mathbf{k}_j} c_{i\mathbf{k}_i} = 0$, $\{c_{i\mathbf{k}_i}^\dagger, c_{j\mathbf{k}_j}^\dagger\} = 0$, $\{c_{i\mathbf{k}_i}, c_{j\mathbf{k}_j}^\dagger\} = \delta_{ij} \delta_{\mathbf{k}_i \mathbf{k}_j}$. Each QW contains a set of n subbands and its Fermi energy measured from the conduction band edge in the emitter contact is ϵ_{w_i}. H_T is a small perturbation of H representing the tunneling coupling between adjacent wells. When an electron tunnels into a QW, it relaxes instantly (in the long dielectric relaxation time scale) to the first subband of that QW.

The change of the electron operator number at the ith well, $N_i = \sum_{\mathbf{k}_i} c_{i\mathbf{k}_i}^\dagger c_{i\mathbf{k}_i}$, is related to the tunneling current operator $\hat{J}_{i \to i+1}$ by

$$e\dot{N}_i = \frac{i}{\hbar}[H_{\text{total}}, eN_i] = \frac{i}{\hbar}[H_{T_{i-1}}, eN_i] - \frac{i}{\hbar}[H_{T_i}, eN_i] = \hat{J}_{i-1 \to i} - \hat{J}_{i \to i+1}. \tag{A.3}$$

In the interaction representation, we have $H_T(t) = e^{iHt/\hbar} H_T e^{-iHt/\hbar}$ and $\hat{J}_{i \to i+1}(t) = e^{iHt/\hbar} \times \hat{J}_{i \to i+1} e^{-iHt/\hbar}$ and the average tunneling current density satisfies the Kubo formula [48]

$$J_{i \to i+1}(t) = \frac{1}{\hbar} \int_{-\infty}^{t} \langle [\hat{J}_{i \to i+1}(t), H_T(t')] \rangle \, dt'. \tag{A.4}$$

Here the average is over the thermodynamic local equilibria at the QWs i and $i + 1$. A straightforward lengthy evaluation yields

$$J_{i \to i+1}(t) = \frac{4\pi e}{\hbar} \sum_{\mathbf{k}_j \mathbf{k}_{j+1}} |T_{\mathbf{k}_j \mathbf{k}_{j+1}}|^2 \delta(E_{j+1\mathbf{k}_{j+1}} - E_{j\mathbf{k}_j})$$

$$\times \left[n_F(E_{j+1\mathbf{k}_{j+1}} - \epsilon_{w_{j+1}}) - n_F(E_{j\mathbf{k}_j} - \epsilon_{w_j}) \right], \tag{A.5}$$

where $n_F(x) = 1/(1 + e^{x/k_B T})$ is the Fermi distribution function. Here the overall energy at the jth QW is $E_{j\mathbf{k}_j} = \epsilon + E_\perp$, $E_\perp = \hbar^2 \mathbf{k}_\perp^2/(2m^*)$, in which ϵ is the energy at the well, and $\mathbf{k}_\perp$ comprises the components of the wave vector that are orthogonal to the SL growth direction. The matrix element:

$$T_{\mathbf{k}_j \mathbf{k}_{j+1}} = \frac{\hbar^2}{2m^*} \int_A \left(\psi_j \nabla \psi_{j+1}^* - \psi_{j+1}^* \nabla \psi_j \right) \cdot d\mathbf{A}, \tag{A.6}$$

is calculated by using Bardeen's Transfer Hamiltonian method [49, 50]. The wave functions of two adjacent square QWs, ψ_j and ψ_{j+1}, are approximated by those of free particles in two isolated wells separated by an infinitely thick barrier. Then continuity of wave functions and their derivatives are used to find out the coefficients of the wave function expressions in different space intervals and the resulting wave functions produce the matrix element (A.6) [50]. The result is [29]

$$|T_{\mathbf{k}_i \mathbf{k}_{i+1}}|^2 = \frac{\pi \hbar^4}{2m^{*2}} B_{i-1,i} B_{i,i+1} T_i \delta_{\mathbf{k}_\perp \mathbf{k}_\perp'}, \qquad B_{i,i+1} = \frac{k_{i+1}}{d_W + \alpha_i^{-1} + \alpha_{i+1}^{-1}}, \tag{A.7}$$

where the transmission coefficient through a thick barrier is

$$T_i(\epsilon) = \frac{16 k_i^2 k_{i+1}^2 \alpha_i^2}{(k_i^2 + \alpha_i^2)(k_{i+1}^2 + \alpha_i^2)} e^{-2\alpha_i d_B}. \tag{A.8}$$

In (A.7) and (A.8), we have used the definitions

$$\hbar k_i = \sqrt{2m^*(\epsilon + e\mathcal{W}_i)}, \tag{A.9}$$

$$\hbar \alpha_i = \sqrt{2m^* e \left[V_B - \mathcal{W}_i - \frac{V_{w_i}}{2} - \frac{\epsilon}{e} \right]}, \tag{A.10}$$

$$\mathcal{W}_i = \frac{\Delta_1}{e} + V_0 + \sum_{j=1}^{i-1}(V_j + V_{w_j}) + \frac{V_{w_i}}{2}. \tag{A.11}$$

We now transform the sums in (A.5) to integrals over the energies $E_{j\mathbf{k}_j} = \epsilon + E_\perp$ using a broadened spectral density to account for scattering. If the latter depends only on ϵ, we obtain

$$J_{i\to i+1} = \frac{e\hbar}{2m^*} \sum_{j=1}^n \int d\epsilon\, A_{C1}^i(\epsilon) A_{Cj}^{i+1}(\epsilon) B_{i-1,i}(\epsilon) B_{i,i+1}(\epsilon) T_i(\epsilon)$$

$$\times \int dE_\perp \left[\frac{1}{1 + e^{(\epsilon+E_\perp-\epsilon_{w_i})/k_B T}} + \frac{1}{1 + e^{(\epsilon+E_\perp-\epsilon_{w_{i+1}})/k_B T}} \right]. \tag{A.12}$$

Here the broadened spectral function is

$$A_{Cv}^i(\epsilon) = \frac{\gamma_{Cv}}{\pi} \frac{1}{(\epsilon - \epsilon_{Cv}^i)^2 + \gamma_{Cv}^2}, \tag{A.13}$$

where $\gamma_v = \hbar/\tau_{\mathrm{sc}}$, with τ_{sc} being the lifetime associated to the dominant scattering processes (interface roughness, impurity scattering, phonon scattering, etc.). The relation between the local Fermi energy and the electron density at the ith well is obtained from

$$n_i = \frac{m^* k_B T}{\pi^2 \hbar^2} \int A_{C1}^i(\epsilon) \ln\left[1 + e^{\frac{\epsilon_{w_i}-\epsilon}{k_B T}} \right] d\epsilon. \tag{A.14}$$

Integrating now (A.12) over $E_\perp$, we obtain

$$J_{i\to i+1} = \frac{e\hbar k_B T}{2\pi^2 m^*} \sum_{j=1}^n \int A_{C1}^i(\epsilon) A_{Cj}^{i+1}(\epsilon) B_{i-1,i}(\epsilon) B_{i,i+1}(\epsilon) T_i(\epsilon)$$

$$\times \ln\left[\frac{1 + e^{(\epsilon_{w_i}-\epsilon)/k_B T}}{1 + e^{(\epsilon_{w_{i+1}}-\epsilon)/k_B T}} \right] d\epsilon. \tag{A.15}$$

In (A.15) all energies are measured from the conduction band edge in the emitter contact. Notice that the complicated dependence of the wave vectors k_i and α_i with the potential, $\mathcal{W}_i$, may be transferred to the Fermi energies by changing variables in the integrals of the system (A.15) so that the lower limit of integration (the bottom of the ith well) is zero: $\epsilon' = \epsilon + e\mathcal{W}_i$. Then the resulting expressions have the same forms as Eqs. (A.15) and (A.14) if ϵ_{C1}^i, ϵ_{Cj}^{i+1}, and ϵ_{w_i} in them are replaced by

$$\epsilon_{C1} = \epsilon_{C1}^i + e\mathcal{W}_i, \tag{A.16}$$

$$\mu_i \equiv \epsilon_{w_i} + e\mathcal{W}_i, \tag{A.17}$$

respectively. $\mathcal{W}_i$ is given by (A.11). The integrations now go from $\epsilon' = 0$ to infinity. Notice that ϵ_{Cj} is independent of the well index i provided we assume that the energy level drops half the potential drop for the whole well eV_{w_i} with respect to its position in the absence of bias. Equation (A.14) becomes

$$n_i(\mu_i) = \frac{m^* k_B T}{\pi^2 \hbar^2} \int_0^\infty A_{C1}(\epsilon) \ln\left[1 + e^{\frac{\mu_i-\epsilon}{k_B T}} \right] d\epsilon. \tag{A.18}$$

Here $A_{C1}(\epsilon)$ is obtained by substituting ϵ_{C1} (the energy of the first subband measured from the bottom of a given well, therefore independent of electrostatics) instead of ϵ_{C1}^i in (A.13). Notice that (A.18) defines a one-to-one relation between n_i and μ_i which is independent of the index i or the potential drops. The inverse function $\mu_i = \mu(n_i, T)$ gives the chemical potential or free energy per electron. This is the *entropic* part of the electrochemical potential (Fermi energy)

$$\epsilon_{w_i} = \mu(n_i, T) - \Delta_1 - eV_0 - e\sum_{j=1}^{i-1}(V_j + V_{w_j}) - \frac{eV_{w_i}}{2}. \tag{A.19}$$

According to (A.19), the Fermi energy, ϵ_{w_i} (electrochemical potential), is the sum of the electrostatic energy at the ith well, $-\Delta_1 - eV_0 - e\sum_{j=1}^{i-1}(V_j + V_{wj}) - eV_{wi}/2$, and the chemical potential, $\mu_i = \mu(n_i, T)$. After the change of variable in the integrals, the wave vectors in (A.15) become:

$$\hbar k_i = \sqrt{2m^*\epsilon},$$

$$\hbar\alpha_i = \sqrt{2m^*\left(eV_B - \frac{eV_{w_i}}{2} - \epsilon\right)},$$

$$\hbar k_{i+1} = \sqrt{2m^*\left(\epsilon + eV_i + e\frac{V_{w_i} + V_{w_{i+1}}}{2}\right)}, \tag{A.20}$$

$$\hbar\alpha_{i-1} = \sqrt{2m^*\left(eV_B + \frac{eV_{w_i}}{2} + eV_{i-1} - \epsilon\right)},$$

$$\hbar\alpha_{i+1} = \sqrt{2m^*\left(eV_B - \frac{eV_{w_i}}{2} - eV_i - eV_{w_{i+1}} - \epsilon\right)},$$

where now $\epsilon = 0$ at the bottom of the ith well. This shows that the tunneling current density, $J_{i,i+1}$, in (A.15) is a function of: the temperature, μ_i and μ_{i+1} (therefore of n_i and n_{i+1}), the potential drops V_i, V_{i+1}, V_{w_i}, and $V_{w_{i+1}}$. The potential drops are related to the electron density through the discrete Poisson equations

$$\varepsilon\frac{V_{w_i}}{d_W} = \varepsilon\frac{V_{i-1}}{d_B} + \frac{e(n_i - N_D)}{2}, \tag{A.21}$$

$$\varepsilon\frac{V_i}{d_B} = \varepsilon\frac{V_{i-1}}{d_B} + e(n_i - N_D), \tag{A.22}$$

from which

$$V_{w_i} = d_W\frac{V_i + V_{i-1}}{2d_B}. \tag{A.23}$$

To obtain simpler expressions for the tunneling current density, we assume that V_i/d_B and $V_{i\pm1}/d_B$ are approximately equal to an average field F_i. Then $V_{w_i} = d_W F_i$ according to (A.23). This assumption departs from the previous approximations and yields a new model. The point of contact with our previous results is that $A_{C1}(\epsilon)A_{Cj}(\epsilon + eV_i + e[V_{w_i} + V_{w_{i+1}}]/2)$ is the controlling factor in the expressions for $\nu^{(f)}$ and $J^-_{i\to i+1}$ (the transmission coefficient contains an exponential factor, $e^{-2\alpha_i d_B}$, which is almost constant at the energies

contributing most to the integral). This controlling factor is uniquely determined by the potential drop $V_i + (V_{w_i} + V_{w_{i+1}})/2 \approx (d_W + d_B)F_i = F_i l$. Then the wave vectors k_i, α_i, etc. become the expressions in (5)-(11). If the Lorentzian functions (A.13) are sharp enough ($\gamma_{Cv} \to 0$),

$$n_i = \frac{m^* k_B T}{\pi^2 \hbar^2} \ln\left[1 + e^{\frac{\mu_i - \epsilon_{C1}}{k_B T}}\right], \tag{A.24}$$

in (A.18) and we may keep only the product of two Lorentzian functions inside the integral (A.15), and approximate all other functions by their values at $\epsilon' = \epsilon_{C1}$ ($\epsilon = \epsilon_{C1}^i$). Then (2) and (5) are obtained; see also Appendix A of [30].

Appendix 2: Stochastic current

The stochastic currents have two components: shot (partition) noise of Poisson type and thermal noise. The shot noise appears because it is really single electrons that tunnel through barriers and there is a large *integer* number of electrons, whereas the tunneling current deals with real-valued electron densities, not with integer multiples of electron charge divided by surface area. The difference constitutes shot noise. For the large values of the barrier cross section area, Poissonian statistics of the shot noise is appropriate [32], and thus its correlation is proportional to the terms of the tunneling current (2). This produces the first two terms in (12) according to [32, 34]. To derive the correlation due to thermal noise, we first write (2) as

$$J_{i \to i+1} = \frac{e n_i}{l} v^{(f)}(F_i) - J_{i \to i+1}^-(F_i, n_i, T)$$
$$- \left[J_{i \to i+1}^-(F_i, n_{i+1}, T) - J_{i \to i+1}^-(F_i, n_i, T)\right]. \tag{B.1}$$

The two last terms in (B.1) form a discrete diffusive term,

$$J_{i \to i+1}^{\text{diff}} = \left[J_{i \to i+1}^-(F_i, \mu_{i+1}, T) - J_{i \to i+1}^-(F_i, \mu_i, T)\right] = D_\mu^+\left[J_{i \to i+1}^-(F_i, \mu_i, T)\right], \tag{B.2}$$

in which, using (A.24), we have written that the tunneling current depends on the chemical potential instead of the electron density. Then

$$J_{i \to i+1}^-(F_i, \mu_{i+1}, T) = \frac{e m^* k_B T}{\pi \hbar^2 l} v^{(f)}(F_i) \ln\left(1 + e^{\frac{\mu_{i+1} - eF_i l - \epsilon_{C1}}{k_B T}}\right). \tag{B.3}$$

After linearization, the discrete diffusive current (B.2) becomes

$$\delta\left(D_\mu^+ J_{i \to i+1}^-(F_i, \mu_i, T)\right) = \frac{\partial J_{i \to i+1}^-}{\partial \mu_i} D_\mu^+(\delta\mu_i). \tag{B.4}$$

According to fluctuating hydrodynamics, there is a zero mean white noise $\eta_i(t)$ corresponding to the diffusive current whose correlation is [35, 36]:

$$\langle \eta_i(t)\eta_j(t')\rangle = 2e k_B T \frac{\partial J_{i \to i+1}^-}{\partial \mu_i} \frac{\delta_{ij}}{A} \delta(t - t')$$

$$= \frac{2e^2 m^* k_B T}{\pi \hbar^2 A l} \frac{v^{(f)}(F_i) e^{\frac{\mu_i - \epsilon_{C1} - eF_i l}{k_B T}}}{1 + e^{\frac{\mu_i - \epsilon_{C1} - eF_i l}{k_B T}}} \delta_{ij}\delta(t - t'). \tag{B.5}$$

This contributes the last term to (12) after we replace n_i instead of μ_i by means of (A.24).

It turns out that the numerical simulations of the stochastic model are not that sensitive to the particular expressions derived in this Appendix. Terms of the same order of magnitude produce very similar results.

Abbreviations
RNG, RBG, PRNG, SL, QW, LLE, LSB

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
LLB wrote the paper, proposed the model and directed the investigation. MA and MC solved numerically the model equations. All authors discussed the results and their interpretation in equal share.

Authors' information
LLB is a Professor of Applied Mathematics and director of the Institute. He has done research work on modeling, analysis, interpretation and validation of nonlinear charge transport in semiconductor superlattices and other nanostructures since 1994. He co-proposed discrete models widely used in this field, wrote review articles and one related book. MC is Associate Professor of Applied Mathematics and MA is a Lecturer and both are members of the Institute. They have been working in this field since the 2000s, with particular expertise in the numerical solutions of ordinary, partial and stochastic differential equations. The authors collaborate regularly with experimental physicists working on these topics.

References
1. Stinson DR. Cryptography: theory and practice. 3rd ed. Boca Raton: CRC Press; 2006.
2. Gallager RG. Principles of digital communication. Cambridge: Cambridge University Press; 2008.
3. Nielsen MA, Chuang IL. Quantum computation and quantum information. Cambridge: Cambridge University Press; 2000.
4. Asmussen S, Glynn PW. Stochastic simulation: algorithms and analysis. New York: Springer; 2007.
5. Binder K, Heermann DW. Monte Carlo simulation in statistical physics. An introduction. 4th ed. Berlin: Springer; 2002.
6. Dorrendorf L, Gutterman Z, Pinkas B. Cryptanalysis of the random number generator of the windows operating system. ACM Trans Inf Syst Secur 2009;13(1):10. doi:10.1145/1609956.1609966.
7. Keller JB. The probability of heads. Am Math Mon. 1986;93:191-7.
8. Diaconis P, Holmes S, Montgomery R. Dynamical bias in the coin toss. SIAM Rev. 2007;49(2):211-35.
9. Dynes FJ, Yuan ZL, Sharpe AW, Shields AJ. A high speed, postprocessing free, quantum random number generator. Appl Phys Lett. 2008;93:031109.
10. Comandar LC, Fröhlich B, Lucamarini M, Patel KA, Sharpe AW, Dynes JF, Yuan ZL, Penty RV, Shields AJ. Room temperature single-photon detectors for high bit rate quantum key distribution. Appl Phys Lett. 2014;104:021101.
11. Uchida A, Amano K, Inoue M, Hirano K, Naito S, Someya H, Oowada I, Kurashige T, Shiki M, Yoshimori S, Yoshimura K, Davis P. Fast physical random bit generation with chaotic semiconductor lasers. Nat Photonics. 2008;2:728-32.
12. Murphy TE, Roy R. The world's fastest dice. Nat Photonics. 2008;2:714-5.
13. Reidler I, Aviad Y, Rosenbluh M, Kanter I. Ultrahigh-speed random number generation based on a chaotic semiconductor laser. Phys Rev Lett. 2009;103:024102.
14. Kanter I, Aviad Y, Reidler I, Cohen E, Rosenbluth M. An optical ultrafast random bit generator. Nat Photonics. 2010;4:58-61.
15. Li W, Reidler I, Aviad Y, Huang Y, Song H, Zhang Y, Rosenbluth M, Kanter I. Fast physical random-number generation based on room-temperature chaotic oscillations in weakly coupled superlattices. Phys Rev Lett. 2013;111:044102.
16. Bastard G. Wave mechanics applied to semiconductor heterostructures. New York: Halsted Press; 1988.
17. Bonilla LL, Grahn HT. Nonlinear dynamics of semiconductor superlattices. Rep Prog Phys. 2005;68:577-683.
18. Esaki L, Tsu R. Superlattice and negative differential conductivity in semiconductors. IBM J Res Dev. 1970;14:61-5.
19. Feldmann J, Leo K, Shah J, Miller DAB, Cunningham JE, Meier T, von Plessen G, Schulze A, Thomas P, Schmitt-Rink S. Optical investigation of Bloch oscillations in a semiconductor superlattice. Phys Rev B. 1992;46:7252-5.
20. Huang YY, Li W, Ma WQ, Qin H, Zhang YH. Experimental observation of spontaneous chaotic current oscillations in GaAs/Al$_{0.45}$Ga$_{0.55}$As superlattices at room temperature. Chin Sci Bull. 2012;57:2070-2.
21. Cercignani C. Mathematical methods in kinetic theory. New York: Plenum Press; 1969.
22. Markowich PA, Schmeiser CA, Ringhofer C. Semiconductor equations. Vienna: Springer; 1990.
23. Jüngel A. Transport equations for semiconductors. Lecture notes in physics. vol. 773. Berlin: Springer; 2009.
24. Bonilla LL, Escobedo R, Perales A. Generalized drift-diffusion model for miniband superlattices. Phys Rev B. 2003;68:241304.
25. Bonilla LL, Álvaro M, Carretero M. Theory of spatially inhomogeneous Bloch oscillations in semiconductor superlattices. Phys Rev B. 2011;84:155316.

26. Bonilla LL, Galán J, Cuesta JA, Martínez FC, Molera JM. Dynamics of electric field domains and oscillations of the photocurrent in a simple superlattice model. Phys Rev B. 1994;50:8644-57.
27. Alvaro M, Carretero M, Bonilla LL. Noise enhanced spontaneous chaos in semiconductor superlattices at room temperature. Europhys Lett. 2014;107:37002.
28. Bonilla LL, Escobedo R, Dell'Acqua G. Voltage switching and domain relocation in semiconductor superlattices. Phys Rev B. 2006;73:115341.
29. Xu H, Teitsworth SW. Dependence of electric field domain relocation dynamics on contact conductivity in semiconductor superlattices. Phys Rev B. 2007;76:235302.
30. Bonilla LL. Theory of nonlinear charge transport, wave propagation and self-oscillations in semiconductor superlattices. J Phys Condens Matter. 2002;14:R341-81.
31. Huang YY, Li W, Ma WQ, Qin H, Grahn HT, Zhang YH. Spontaneous quasi-periodic current self-oscillations in a weakly coupled GaAs/(Al, Ga)As superlattice at room temperature. Appl Phys Lett. 2013;102:242107.
32. Blanter YM, Büttiker M. Shot noise in mesoscopic conductors. Phys Rep. 2000;336:1-166.
33. Bonilla LL, Sánchez O, Soler JS. Nonlinear stochastic discrete drift-diffusion theory of charge fluctuations and domain relocation times in semiconductor superlattices. Phys Rev B. 2002;65:195308.
34. Bonilla LL. Theory of charge fluctuations and domain relocation times in semiconductor superlattices. Physica D. 2004;199:105-14.
35. Landau LD, Lifshitz EM. Fluid mechanics. New York: Pergamon Press; 1959.
36. Keizer J. Statistical thermodynamics of nonequilibrium processes. New York: Springer; 1987.
37. Schwarz G, Wacker A, Prengel F, Schöll E, Kastrup J, Grahn HT, Ploog K. The influence of imperfections and weak disorder on domain formation in superlattices. Semicond Sci Technol. 1996;11:475-82.
38. Kloeden PE, Platen E. Numerical solution of stochastic differential equations. Berlin: Springer; 1992.
39. Higham DJ. An algorithmic introduction to numerical simulation of stochastic differential equations. SIAM Rev. 2001;43:525-46.
40. Benettin G, Casartelli M, Galgani L, Giorgilli A, Strelcyn JM. On the reliability of numerical studies of stochasticity. Nuovo Cimento B. 1978;44:183-95.
41. Gao JB, Hwang SK, Liu JM. When can noise induce chaos? Phys Rev Lett. 1999;82:1132-5.
42. Zhang Y, Kastrup J, Klann R, Ploog KH, Grahn HT. Synchronization and chaos induced by resonant tunneling in GaAs/AlAs superlattices. Phys Rev Lett. 1996;77:3001-4.
43. Cantalapiedra IR, Bergmann MJ, Bonilla LL, Teitsworth SW. Chaotic motion of space charge waves in semiconductors under time-independent voltage bias. Phys Rev E. 2001;63:056216.
44. Amann A, Schlesner J, Wacker A, Schöll E. Chaotic front dynamics in semiconductor superlattices. Phys Rev B. 2002;65:193313.
45. Moon H-T. Two-frequency motion to chaos with fractal dimension $d > 3$. Phys Rev Lett. 1997;79:403-6.
46. Crutchfield JP, Farmer D, Huberman BA. Fluctuations and simple chaotic dynamics. Phys Rep. 1982;92:45-82.
47. NIST Statistical Test Suite. http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html
48. Zwanzig R. Nonequilibrium statistical mechanics. New York: Oxford University Press; 2001.
49. Bardeen J. Tunneling from a many-particle point of view. Phys Rev Lett. 1961;6:57-9.
50. Payne MC. Transfer Hamiltonian description of resonant tunneling. J Phys C, Solid State Phys. 1986;19:1145-55.