Fast Physical Random-Number Generation Based on Room-Temperature Chaotic Oscillations in Weakly Coupled Superlattices

Wen Li,[1] Igor Reidler,[2] Yaara Aviad,[2] Yuyang Huang,[1] Helong Song,[1]
Yaohui Zhang,[1] Michael Rosenbluh,[2] and Ido Kanter[2,*]

[1]*Suzhou Institute of Nano-tech and Nano-bionics, Chinese Academy of Sciences, Suzhou 215125, China*
[2]*Department of Physics, Bar-Ilan University, Ramat-Gan, 52900, Israel*

(Received 29 March 2013; revised manuscript received 28 May 2013; published 25 July 2013)

An all-electronic physical random number generator at rates up to 80 Gbit/s is presented, based on weakly coupled GaAs/$Ga_{0.55}Al_{0.45}$As superlattices operated at room temperature. It is based on large-amplitude, chaotic current oscillations characterized by a bandwidth of several hundred MHz and do not require external feedback or conversion to an electronic signal prior to digitization. The method is robust and insensitive to external perturbations and its fully electronic implementation suggests scalability and minimal postprocessing in comparison to existing optical implementations.

DOI: 10.1103/PhysRevLett.111.044102 PACS numbers: 05.45.−a, 05.40.−a, 73.21.Cd

Semiconductor superlattices (SLs) have been characterized as a one-dimensional nonlinear system exhibiting the formation of electric field domains [1–5]. The nonlinearity originates from negative differential conductance induced by well-to-well sequential resonant tunneling [6,7]. There are a diversity of spatiotemporal patterns observed in dc biased SLs including static high-field domains, self-sustained periodic current, and quasiperiodic current oscillations [1,2,8]. The *I-V* characteristic of these devices clearly shows multistability [9], which is a typical property of a nonlinear system. In particular, spontaneous chaotic oscillations were observed in GaAs/AlAs SLs operated below liquid-nitrogen temperature range, with the frequency spectrum of the chaotic oscillations ranging from dc to several GHz [10].

Spontaneous chaotic and periodic current oscillations were previously observed by tuning of the dc bias in a doped superlattice below liquid nitrogen temperatures [6]. Very recently, however, spontaneous chaotic oscillations have also been observed in GaAs/$Al_{0.45}Ga_{0.55}$As superlattices at room temperature [11], where the mole fraction of aluminum in the barrier layers was chosen to be 0.45 to suppress the thermal leakage current through the *X* valley [4,12,13]. The theoretical understanding of the observed chaotic oscillations is currently not well understood. Previously published models predict low dimensional chaos in a homogenous semiconductor with negative differential resistance by considering the dynamics of the charge carrier drift along with the creation of free carriers via impurity impact ionization and the destruction of free carriers via impurity trapping sites [14]. A model predicting chaotic behavior for an undoped SL under photoexcitation has also been reported [15], but in this model electron-hole recombination plays a significant role, and this phenomena is absent in our voltage driven SL with only electron charge carriers. Theoretical progress in understanding the behavior in the SL of our experiments may lead to optimization of the bandwidth and parameter window for chaotic oscillations in such devices. The discovery of room temperature chaotic oscillations in weakly coupled SLs paves the way for the use of semiconductor SLs as a practical physical source for random bit generators (RBG).

The generation of random bit sequences is crucial in several key digital technologies [16–19] and is either built on physical entropy sources, or uses a deterministic algorithm based on a random seed known as pseudorandom bit generators. Various physical processes, such as electronic or photonic noise on the classical and the quantum levels have been suggested as sources for random bit generation. Until recently, however, the physical RBG bit rate was much slower than the bit rate provided by pseudorandom bit generators and did not meet the requirements of modern data rates. Recently, a number of photonic implementations based on chaotic semiconductor lasers were demonstrated. Semiconductor lasers subject to delayed optical feedback can produce strongly diverging chaotic trajectories consisting of irregular sub-nanosecond spikes. The RBG is made by digitally representing the chaotic optical signal, followed by a postprocessing procedure to remove remaining correlations in the digitized sequence [20–23].

Here, we demonstrate an all-electronic physical RBG with rates up to 80 Gbit/s, based on the digitization of the electric signal of weakly coupled SLs at room temperature. The randomness is verified using NIST statistical test suite [24] and statistical test batteries implemented in TestU01 suite [25]. Unlike optical RBG schemes, the proposed method does not require external optical feedback, detection schemes or the conversion of an optical signal to an analog electronic signal prior to digitization. In addition, the proposed method suggests a scalable design involving minimal postprocessing compared to existing optical implementations.

The structure of the investigated samples is schematically shown in Fig. 1(a) and consists of a 50-period, weakly coupled GaAs/$Al_{0.45}Ga_{0.55}As$ superlattice with GaAs wells and $Al_{0.45}Ga_{0.55}As$ barriers. Each GaAs quantum well was Si doped. A spacing of GaAs, 2 nm thick, was introduced between the GaAs/$Al_{0.45}Ga_{0.55}As$ interface to avoid diffusion of Si atoms into the $Al_{0.45}Ga_{0.55}As$ barriers. The superlattice was sandwiched within two 300 nm Si doped GaAs contacting layers to form a $n^+ - n - n^+$ diode structure. The detailed superlattice structure is described in [11].

Sustained chaotic current oscillations were observed at room temperature for several ranges of the dc bias voltage, between 4–4.3 V and 6.20–6.80 V as shown in Fig. 1(b). The oscillation amplitude, exceeded 8 mA (0.4 V into a 50 Ω load resistor) with a bandwidth of several hundred MHz as shown in Fig. 1(c). A 100 ns long recording, digitized at 40 GHz is shown in the inset of Fig. 1(c). For detailed superlattice and recording methods, see [11].

Two methods were used to generate a random bit sequence from the recorded oscillations as schematically shown in Fig. 2. The first method is similar to our demonstrated optical RBG scheme, where the generation of the random bit sequence consists of the following two steps [21]. In the first step a dynamical buffer of the last $n + 1$ successively digitized electrical current values of the SL is used to calculate the nth discrete derivative as exemplified for $n = 3$ in Fig. 2(b). In the second step, the m least significant bits (LSBs) of the resulting nth derivative are appended to the random bit sequence as shown in Fig. 2(a).

The bit rate of this type of RBG is limited to a few Gbit/s which is consistent with the bandwidth of the chaotic oscillations and the postprocessing method used. We were able to achieve a speed of 6.25 Gbit/s using a sampling rate of 1.25 GHz, 4th derivative and retention of 5 LSBs out of 8 bits. In our current implementation the postprocessing, derivative and LSB retention was performed in an offline procedure. The relatively limited speed can also be understood from the interspike intervals (ISIs) which have an average ∼5 ns time lag between two consecutive spikes (with a spike width of ∼1.5 ns) as shown in Fig. 3(a). The noise amplitude between the spikes is at least 1 order of magnitude lower than the spike heights

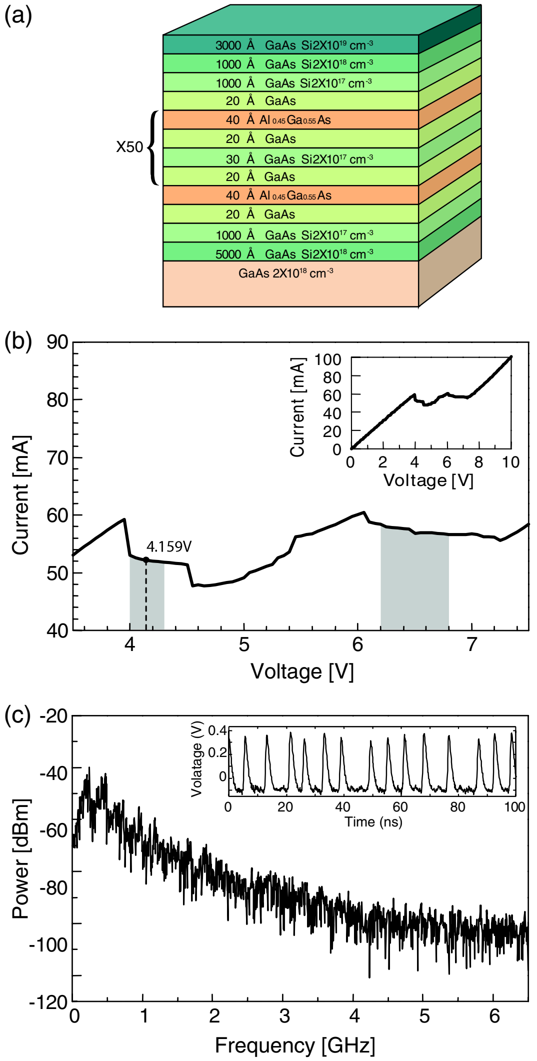

FIG. 1 (color online). (a) Schematic representation of the superlattice (SL) device. (b) A plateau region of the I-V curve of the SL consisting of two voltage segments (gray regions) characterized by chaotic current oscillations. Most of the presented measurements were carried out at 4.159 V (dashed vertical line). The inset represents the entire I-V range. (c) Spectrum of the chaotic oscillations [11]. Inset: A 100 ns trace of SL current oscillations.

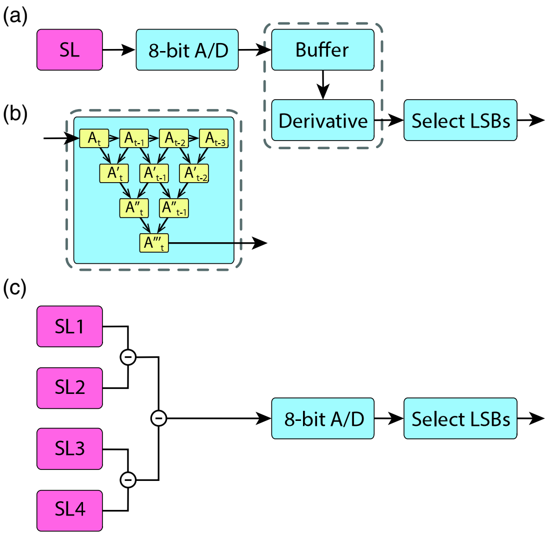

FIG. 2 (color online). (a) Schematic diagram of the RBG method based on discrete time derivative of the digitized current signal and retention of only a number of least significant bits. (b) An example of the 3rd discrete derivative implementation of the method described in (a), where A_t stands for of the digitized signal. (c) Schematic diagram of the parallel combination RBG method where a minus sign stands for the subtraction, i.e., signal of SL1 minus the signal of SL2.

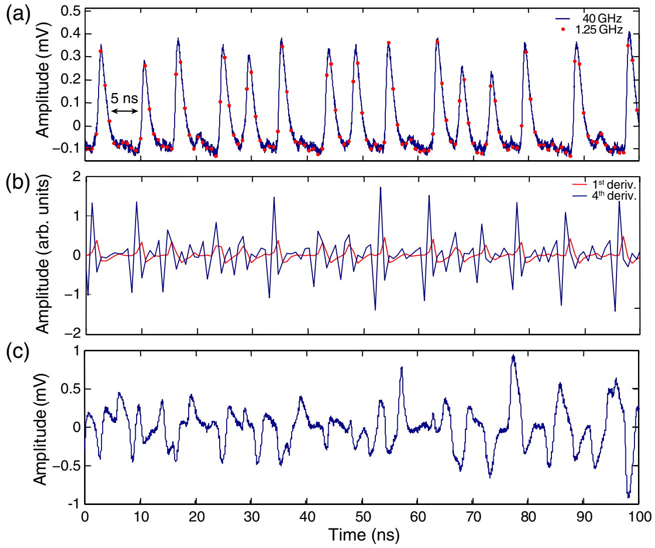

FIG. 3 (color online). (a) A 100 ns trace of SL oscillations, digitized at 40 GHz (blue line) and 1.25 GHz (red circles). (b) 1st and 4th order discrete derivatives of the SL oscillations sampled at 1.25 GHz and presented in panel (a). (c) Linear combination of 4 recorded superlattice oscillation traces, digitized at 40 GHz.

of the SL device and is a combination of instrumental noise and intrinsic noise originating in the SL from thermal and electronic shot noise sources. The chaotic spikes, which might be seeded by this random noise as reported in [26], are present only a fraction of the time. Thus, at a 1.25 GHz sampling rate, for instance, a significant number of the sampling measurements occur in the ISIs, resulting in degraded randomness of the generated bit sequence. To overcome this limitation a high order derivative can be used to mix data sampled in an ISI window with nearby chaotic current 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. Thus this time window includes, with a high probability, combined data taken from a chaotic current spike and the ISI. Figure 3(b) shows the 1st and the 4th derivatives of the signal presented in Fig. 3(a). Whereas for the first derivate there are many time points with near zero value, the fourth derivate values fluctuate at all-time scales. Retaining only the LSBs is still required to guarantee the generation of random sequences with verified randomness using the NIST statistical test suite (Table I) [24]. Higher sampling rates than the 1.25 GHz used here, with the retention of 5 LSBs, require much higher orders of derivative; for example, a sampling rate of 5 GHz requires the 10th discrete derivative so as to pass the NIST statistical test (not shown). The implementation of higher derivatives requires a longer buffer t and does not result in much improved bit rate generation.

The second method for implementing an SL based RBG overcomes these difficulties. Since the spike timings of independent SL devices are uncorrelated, one can linearly combine several such signals and ‘‘fill’’ the ISIs as shown in Fig. 3(c). A schematic implementation of this method is presented in Fig. 2(c), where the buffer and the discrete higher order derivative are replaced by a linear combination of the analog chaotic current oscillations of several uncorrelated SLs. Because of the unavailability of several such SL devices in our experiment, we test this RBG method by combining far segments of the

TABLE I. NIST results for a random bit sequence generated using 4th derivative of a signal sampled at 1.25 GHz, retaining 5 LSBs (Derivative), and parallel linear combining of 6 independent SL signals sampled at 20 GHz and retaining 4 LSBs (Combine).

	P value		Proportion		
Statistical test	Derivative	Combine	Derivative	Combine	Result
Frequency	0.911 413	0.626 709	0.9900	0.9870	Success
Block frequency	0.480 771	0.413 628	0.9930	0.9860	Success
Cumulative sum	0.643 366	0.607 993	0.9920	0.9880	Success
Runs	0.474 986	0.821 937	0.9830	0.9910	Success
Longest run	0.544 254	0.170 922	0.9880	0.9850	Success
Rank	0.329 850	0.431 754	0.9930	0.9940	Success
Spectral	0.953 089	0.969 588	0.9890	0.9830	Success
Nonoverlapping	0.011 223	0.031 637	0.9860	0.9890	Success
Overlapping	0.126 658	0.709 558	0.9960	0.9840	Success
Universal	0.326 749	0.424 453	0.9890	0.9890	Success
Approximate entropy	0.467 322	0.616 305	0.9890	0.9880	Success
Random excursions	0.030 939	0.138 761	0.9903	0.9922	Success
Random excursions variant	0.129 379	0.011 209	0.9839	0.9938	Success
Serial	0.288 249	0.307 077	0.9930	0.9950	Success
Linear complexity	0.743 915	0.798 139	0.9900	0.9950	Success

TABLE II. For a given number of combined independent signals the RBG rate is fixed by the sampling rate and the number of retained LSBs. The minimum order of derivative necessary for verified randomness is minimized to zero for 4 or more combined signals.

Number of combined SL devices	1	2	4	6
Derivative	4	3	...	...
Max sampling rate (GHz)	1.25	5	10	20
Retained LSBs	5	4	4	4
RBG rate (Gbit/s)	6.25	20	40	80

recorded current oscillations of a single device. The chaotic nature of the device ensures lack of correlation between the segments.

This method, as illustrated in Fig. 2(c), requires only a single analog to digital converter regardless of the number of combined SL devices. To minimize the possible emergence of bias in the combined analog signals, each pair of signals is combined by subtraction [19]. In Fig. 2(b), for instance, the combined signal consists of SL1 + SL3 − SL2 − SL4. A 40 Gbit/s RBG with verified randomness was obtained using a linear combination of 4 signals, a 10 GHz sampling rate, and 4 LSBs [19]. At a sampling rate of 20 GHz, the statistical NIST tests for randomness of this combination failed; however, a combination of 6 signals passed the statistical tests, as indicated in Table I, resulting in 80 Gbit/s RBG with verified randomness.

Table II shows several key points of the tested parameter space for the order of the derivatives and the number of combined independent SL signals, with the retention of 5 or 4 LSBs. For a single SL sampled at 1.25 GHz and 5 LSBs retained, at least the 4th order derivative is required to generate a verified random sequence resulting in a 6.25 Gbit/s RBG rate. Increasing the sampling rate to 5 GHz necessitates higher derivatives even for fewer than 5 LSBs. Alternatively, a combination of both methods may be used at 5 GHz sampling rate with 2 SLs, a 3rd order derivative, and retention of 4 LSBs for a generation rate of 20 Gbit/s [19]. The previously mentioned parallel combination of 4 and 6 SLs with retention of 4 LSBs makes it possible to further increase the sampling rate, resulting in 40 and 80 Gbit/s RBG rates, respectively, without the use of derivatives. The results present the interplay between the sampling rate, order of the derivative and the number of combined SL signals. For a given number of retained LSBs the rate of the RBG can be enhanced either by increasing the number of combined SL signals or by increasing the order of the derivative.

Randomness of the four different configurations shown in Table II was also verified using the statistical test batteries of the TestU01 suite in addition to the NIST suite. Detailed results of Alphabit and SmallCrush test batteries, which require sequence lengths of more than 1 Gbit, are presented in [27].

In conclusion, a high speed all-electronic RBG based on chaotic current oscillations of SL devices at room temperature is proposed and demonstrated experimentally. The randomness of the generated sequences is verified using the NIST and TestU01 statistical test suites [24,25]. The all electronic method uses the parallel combination of multiple, independent SL signals, as well as a single SL with high order derivatives, or a combination of these methods, demonstrating a large degree of scalability and customization options, depending on RBG rate requirements and complexity restrictions of the setup. Further developments of the proposed RBG methods may lead to a miniaturized, on-chip, high speed physical random bit generator with verified randomness.

This work is supported by the Department of Science and Technology, Jiangsu Province (BK2010005, BY20111179), Natural Science Foundation of China (61204093), and Artificial structure and quantum control laboratory of Shanghai Jiao Tong University (2013). The research I. K. and M. R. is supported by the Ministry of Science and Technology, Israel. Computational assistance by Zav Shotan is acknowledged.

*ido.kanter@biu.ac.il

[1] L. Bonilla and H. Grahn, Rep. Prog. Phys. **68**, 577 (2005).

[2] A. Wacker, Phys. Rep. **357**, 1 (2002).

[3] L. Esaki and L. L. Chang, Phys. Rev. Lett. **33**, 495 (1974).

[4] Y. Zhang, X. Yang, W. Liu, P. Zhang, and D. Jiang, Appl. Phys. Lett. **65**, 1148 (1994).

[5] B. J. Keay, S. Allen, J. Galán, J. Kaminski, K. Campman, A. Gossard, U. Bhattacharya, and M. Rodwell, Phys. Rev. Lett. **75**, 4098 (1995).

[6] Y. Zhang, J. Kastrup, R. Klann, K. Ploog, and H. Grahn, Phys. Rev. Lett. **77**, 3001 (1996).

[7] G. Jona-Lasinio, C. Presilla, and F. Capasso, Phys. Rev. Lett. **68**, 2269 (1992).

[8] H. Grahn, J. Kastrup, K. Ploog, L. Bonilla, J. Galán, M. Kindelan, and M. Moscoso, Jpn. J. Appl. Phys. **34**, 4526 (1995).

[9] J. Kastrup, H. T. Grahn, K. Ploog, F. Prengel, A. Wacker, and E. Scholl, Appl. Phys. Lett. **65**, 1808 (1994).

[10] Y. Zhang, R. Klann, H. T. Grahn, and K. H. Ploog, Superlattices Microstruct. **21**, 565 (1997).

[11] Y. Y. Huang, W. Li, W. Ma, H. Qin, and Y. Zhang, Chin. Sci. Bull. **57**, 2070 (2012).

[12] M. H. Meynadier, R. Nahory, J. Worlock, M. Tamargo, J. de Miguel, and M. Sturge, Phys. Rev. Lett. **60**, 1338 (1988).

[13] J.-B. Xia, Phys. Rev. B **41**, 3117 (1990).

[14] I. R. Cantalapiedra, M. Bergmann, L. Bonilla, and S. Teitsworth, Phys. Rev. E **63**, 056216 (2001).

[15] J. I. Arana, L. L. Bonilla, and H. T. Grahn, Phys. Rev. B **81**, 035322 (2010).

[16] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[17] D. R. Stinson, *Cryptography: Theory and Practice* (CRC Press, Boca Raton, 1995), The CRC Press series on discrete mathematics and its applications.

[18] R. G. Gallager, *Principles of Digital Communication* (Cambridge University Press, Cambridge, England, 2008).

[19] S. Asmussen and P. W. Glynn, *Stochastic Simulation: Algorithms and Analysis* (Springer-Verlag, New York, 2007).

[20] A. Uchida *et al.*, Nat. Photonics **2**, 728 (2008).

[21] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nat. Photonics **4**, 58 (2009).

[22] T. E. Murphy and R. Roy, Nat. Photonics **2**, 714 (2008).

[23] C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Opt. Express **18**, 23584 (2010).

[24] NIST Statistical Test Suite http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html.

[25] P. L'Ecuyer and R. Simard, ACM Trans. Math. Softw. **33**, 22 (2007).

[26] Y. Bomze *et al.*, Phys. Rev. Lett. **109**, 026801 (2012).

[27] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.111.044102 for statistical analysis and methods.