Gambling with Superconducting Fluctuations

Marek Foltyn and Maciej Zgirski

Phys. Rev. Applied **4**, 024002 — Published 4 August 2015

DOI: 10.1103/PhysRevApplied.4.024002

Gambling with superconducting fluctuations

Marek Foltyn and Maciej Zgirski
Institute of Physics, Polish Academy of Sciences,
al. Lotników 32/46, PL 02-668 Warszawa, Poland

Josephson junctions and superconducting nanowires, when biased close to superconducting critical current, can switch to a non-zero voltage state by thermal or quantum fluctuations. The process is understood as an escape of a Brownian particle from a metastable state. Since this effect is fully stochastic, we propose to use it for generating random numbers. We present protocol for obtaining random numbers and test the experimentally harvested data for their fidelity. Our work is prerequisite for using Josephson junction as a tool for stochastic (probabilistic) determination of physical parameters such as magnetic flux, temperature and current.

I. INTRODUCTION

In microworld particles are subject to random interaction with environment and undergo a perpetual random walk. Usually these temperature stimulated movements, random and uncorrelated at a single particle level, seem to be not visible in everyday live and in fact were first identified only in 1827, by botanist Robert Brown. Subsequently Johnson and Nyquist proved that thermal motions are also responsible for noise in electrical circuits that competes with a desired signal [1, 2]. However they may manifest themselves in a more sophisticated manner e.g. rubber band holds a stack of paper because smaller molecules "kick" the long ones, thus not allowing them to elongate [3]. Quite recently Brownian motions have been utilized in a modern *Maxwell's demon* experiment to transfer hot electrons from colder to hotter electrode across a tunnel junction leading to refrigeration of the former [4].

In superconductivity electrons are strongly correlated which allows to describe them with a single macroscopic wave function. The phase of the wave function across a Josephson junction (JJ), interacting randomly with environment, fluctuates just like a position of a single particle. This time, however, we deal with a macroscopic Brownian particle, since for any fluctuation to happen, many electrons must be involved. It has been shown that JJs provide a convenient tool for studies of superconducting fluctuations [5, 6]. In the current work we propose to use the Brownian behavior of a superconducting wave function of a JJ or a superconducting nanowire to generate a sequence of random numbers.

Random numbers are ubiquitous: in cryptography we use them to encode information, in computer simulations – to predict the behavior of various statistical systems, in gambling – to earn and lose money. Software random number generators are actually only pseudo-random due to their dependence on a seed and generating algorithm. Hardware random number generators, if properly designed, can approach the true random number generation. Existing fast hardware random number generators (RNGs) are based on the processing of natural noise or stochastic physical phenomena. One of such devices is based on the radioactive nucleus decay [7]. Electric pulses, generated by detected particles, are counted and processed resulting in random stream of 10 kb/s. Ultra fast RNGs derive their randomness from a quantum optical physics, by detecting single photons received from attenuated and split beam of light, incident on two detectors [8, 9]. Each photon detection is converted into a random bit. Such devices can generate even 2 Gb/s [10]. Commercial devices are primarily taking advantage of other physical observable, such as Johnson-Nyquist noise of resistors. Generally, amplified resistor noise is converted by comparator into a train of random-length pulses, which afterwards can be processed in many different ways in order to obtain random bits streams [11, 12]. The other examples of techniques and phenomena used for generating random bits are based on subharmonic oscillators [13], spontaneously initiated stimulated Raman scattering [14], turbulent electroconvection [15]. Since fluctuations are more pronounced in small physical systems it is reasonable to develop random number generators based on nanoobjects. It has been recently demonstrated that thermal oscillations of the magnetic moment in magnetic tunnel junctions [16] may be harnessed for such generation.

Our generator, upon optimization, is capable of delivering similar speeds as state-of-the-art RNGs, being inherently limited only by the frequency of superliquid oscillation on the junction (so called plasma frequency, with response in ps range), but there are also other features that make it unique on the market of RNGs: (i) it is to the best of our knowledge the smallest solid state – based RNG (decaying atom is smaller but it can generate only one bit while our generator can work perpetually), (ii) it is very simple – just piece of a nanowire interrupting a thicker wire, (iii) its operation is conceptually transparent: it behaves like *a coin with tunable probability*. After probing with current pulse it can be found in two easily distinguishable states, normal (*the head*, with probability P) or superconducting (*the tail*, with probability $1 - P$), with no arbitrary criterion separating the two.

In the next section we describe the roots of randomness in JJs and superconducting wires. We then present a protocol allowing to obtain a random sequence of bits. This is followed by a few statistical tests on the exper-

imentally obtained sequences of data. Next, in discussions, possible improvements and extensions of our RNG are presented. Subsequently, prior to summary, we go beyond random number generation and briefly mark potential of JJ probed with pulses to measure magnetization, temperature and current noise.

II. JOSEPHSON JUNCTION AND SUPERCONDUCTING NANOWIRES AS RANDOM SWITCHES

Tunneling weak links or Dayem nanobridges are examples of Josephson junctions (JJs). The former consist of two superconducting leads having a weak contact through a thin insulating layer, the latter are simply narrow short constrictions (bridges) in otherwise continuous superconducting material. Supercurrent carrying state of a JJ or a superconducting nanowire is conveniently described within tilted washboard potential arising from the Resistively and Capacitively Shounted Junction model (RCSJ) [5] (Fig. 1). Within the model, state of the superconducting wavefunction is mapped into a position of a particle moving in the one-dimensional potential. The particle exhibits Brownian fluctuations due to interaction with constant temperature bath [6]. They correspond to random changes in the superconducting phase across the JJ around a mean value, meaning, by virtue of DC Josephson effect, average DC supercurrent flowing in the JJ. The height of the potential barrier separating two local minima is controlled by biasing current. For supercurrents much below critical current, the height of a potential barrier is much larger than accessible thermal energy k_BT and the particle cannot escape through the barrier. However, increasing the biasing current, one can reduce the barrier height to an extent that thermal or quantum fluctuations are sufficient to drive the particle over the barrier [17–19]. If such a so-called phase slip happens [20, 21], the particle acquires sufficient inertia to jump over lower barriers (it is true for an underdamped junction). Superconducting wave function accumulates the phase and this, by virtue of AC Josephson effect, creates voltage across the JJ giving an experimentalist a mean to test the escape. We call such an event *switching*. In case of superconducting wires and Dayem nanobridges, the voltage appears due to phase-slip followed by overheating and transition to normal state [20, 22, 23].

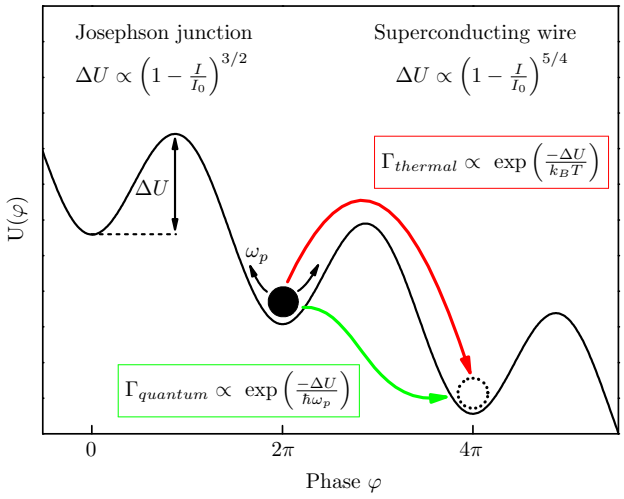


FIG. 1. Brownian particle undergoing random oscillations in tilted washboard potential can jump over or tunnel through barrier (switching), or may stay trapped in the well (no switching). Γs denote rates for both processes. The fluctuations of the particle are visualized in Video 1 and 2.

The Brownian behavior of superconducting wavefunction suggests that JJs and superconducting wires can be used as random number generators. By applying a rectangular current pulse we give the particle a chance to jump over the barrier. If lifetime in local minimum is τ then a probability for the particle to escape in short time dt is dt/τ. It follows that $1-dt/\tau$ is the probability that the particle does not escape in time dt. For current pulse of length T the probability for the particle NOT to escape is $(1-dt/\tau)^{T/dt} = exp(ln(1-dt/\tau)^{T/dt})$. After expanding logarithm around 1 ($ln(x) = 1-x$) we get $exp(-T/\tau)$. Finally, the probability for the particle to escape is $P = 1-exp(-T/\tau)$. In experiment, since the escape rate $\Gamma = 1/\tau$ is both current and temperature dependent, escape probability can be tuned by using the feedback on current pulses e.g. by applying bisection algorithm. The formula for probability has general validity, both for wires and Josephson Junctions. For the case of JJs the switching rate is $\Gamma = (\omega_p/2\pi)\exp(-\Delta U/k_BT_{esc})$, where ω_p is natural frequency of the particle oscillations at the bottom of the potential, T_{esc} is an effective temperature of the escape [5], ΔU is the height of the potential barrier roughly equal to $\Phi_0 I_c$ (Φ_0 - flux quantum, I_c - critical current) at zero current and can be lowered with bias current $\Delta U(i) = \Delta U(0)(1-i/i_0)^{3/2}$. For 1D superconducting wires the formula is the same, but ΔU at zero current corresponds to the condensation energy of the smallest possible volume of the superconducting wire which can be driven to normal state i.e. $\Omega = \xi S$ [21] (ξ - superconducting coherence length, S - wire cross-section) and exponent has the value of 5/4 instead of 3/2 [22]. For thicker wires we can think of similar formula, but the exact energy landscape and switching scenario is more disputable (e.g. one could assume that energy fluctuation necessary to drive wire normal is related to the condensation energy of the piece of the wire of length ξ). Since it is not the primary goal of our paper we will not discuss it here, but only notice that the exact nature of switching in thick superconducting wires is not essential for generating random bits.

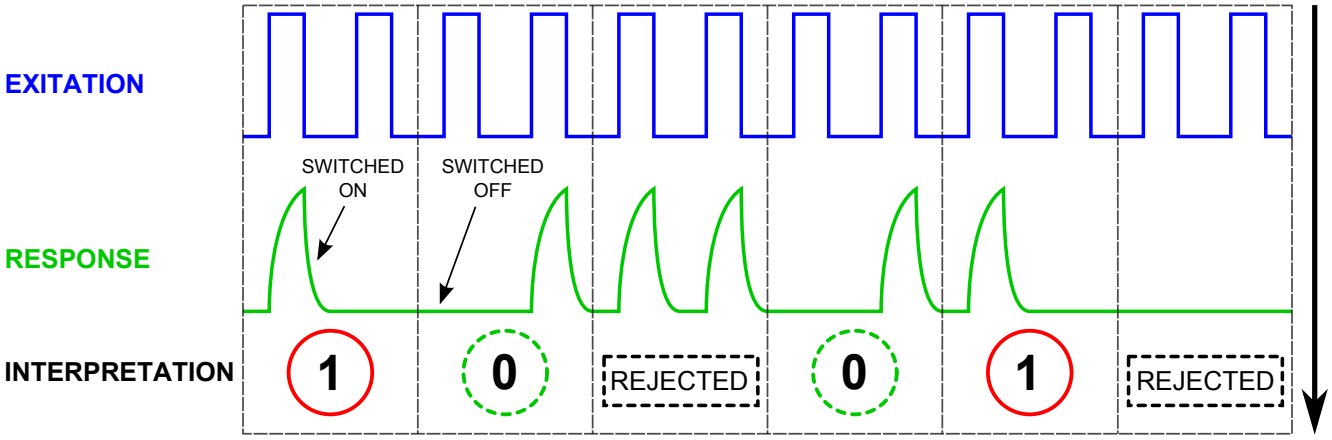


FIG. 2. JJ tested with pulse train (EXCITATION). For each testing pulse the JJ switches or remains silent (RESPONSE). Response as recorded on oscilloscope is rounded, for it is measured with twisted pairs serving as low-pass filters. For analysis we split testing pulses in groups of 2. If within the group for the first pulse the JJ switches and for the second pulse it does not, it encodes logical one (solid red circle). In the opposite case, logical zero is encoded (dashed green circle). Other results (dotted black box) are discarded (INTERPRETATION).

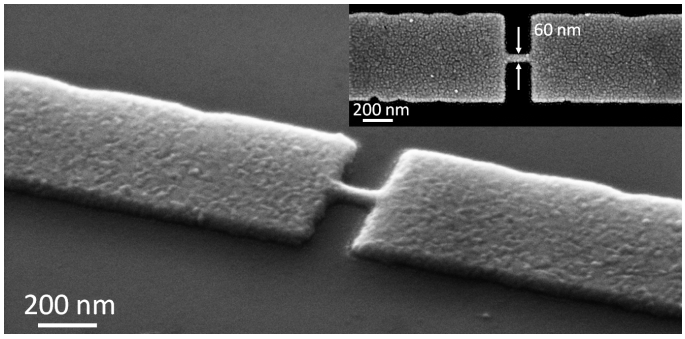


FIG. 3. Scanning electron micrograph of the Dayem nanobridge. Inset shows the nanobridge dimensions.

III. PROTOCOL TO GENERATE RANDOM BITS

Suppose we have a coin which is not fair in the sense that probability P to get the head differs from 0.5. Moreover the probability varies very slowly with time. Obviously a game played with such a coin is not fair. However we can make it fair introducing following assumption: we flip the coin twice one flip after another. If in the first flip we get the head and in the second the tail, player A wins (logical *one*). If in the first flip we get the tail and in the second the head, player B wins (logical *zero*). If two successive trials give the same result, the drawing is discarded. Since we assumed probability for flipping the head to vary slowly with time such a game can be considered fair, for it gives the same probability $P(1-P)$ for both players to win after coin has been flipped twice. The procedure outlined above was first proposed by von Neuman [24] and is considered as a one of the most straightforward ways to unbias the random sequence i.e. to convert random sequence of zero and ones with unequal probabilities for both into random sequence for which probability to get bit 0 is the same as for bit 1, and equal 0.5. JJ is such an unfair coin. It is difficult to set switching probability exactly equal to 0.5. But whatever this probability is, the response to 2 successive testing pulses encodes logical zero or one, provided JJ switched for one testing pulse and did not switch for another. The idea of generating 4-bit random number is explained in Fig. 2.

IV. EXPERIMENTAL

We fabricated Dayem nanobridge by standard e-beam lithography followed by thermal evaporation of 30 nm thick Aluminum (Fig. 3). The circuit employing the bridge as a random number generator is schematically drawn in Fig. 4a. Details of the circuit are described in Methods [25]. The principle of operation is the following. We record IV of the JJ by applying a triangular voltage sweep (Fig. 4b) and find current pulse amplitude for which JJ switches with probability of 0.5. It is easily accomplished by collecting a so-called S-curve (Fig. 4c and Fig. 4d). The train of N_0 current pulses is sent down the JJ and number of switchings n is recorded. It gives switching probability $P = n/N_0$ for a given current amplitude. Then current pulse amplitude is increased and the procedure is repeated. Having found the current amplitude I_A (cf. Fig. 4c) for which JJ switches with probability $P \approx 0.5$ we have sent to JJ train of $N_0 = 4 \times 10^6$. We have recorded response of JJ with digitizer, collecting a point each 500ns. We can use such a low acquisition rate because the sustaining part of the pulse holds the

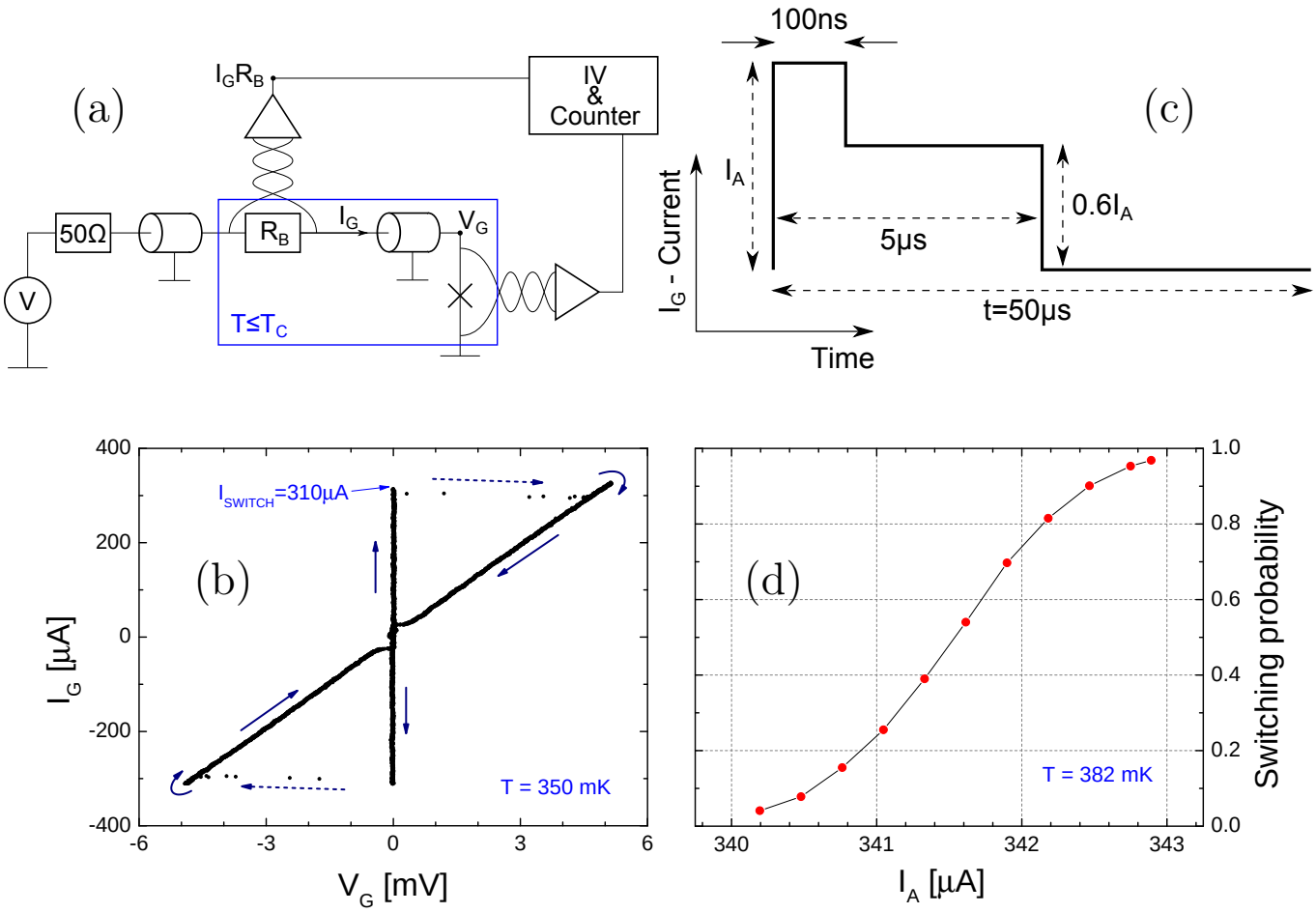


FIG. 4. (a) The circuit employing a JJ for random number generation. (b) The Dayem nanobridge current-voltage characteristic revealing switching behavior at a threshold current. (c) Complex pulse used for JJ testing. Its amplitude I_A defines probability for JJ to switch and lower plateau (sustaining part) allows for read-out with low-pass twisted pairs. Timing, amplitude and repetition rate are controlled by arbitrary waveform generator. (d) Experimentally obtained S-curve. Each point is the estimator for switching probability at given current amplitude I_A measured with train of N_0=10 000 pulses. The line is a guide for the eye.

memory of switching event over $5\mu s$. We have performed post-processing of the data in the spirit of idea explained in the Fig. 2. On converting the data into sequence of zeros and ones we are ready to check its randomness.

V. ARE GENERATED BITS RANDOM?

We have generated a stream of $N = 10^6$ bits [26]. For non-biased sequence we expect to obtain $NP = 0.5 \cdot 10^6$ ones with standard deviation of $\sqrt{NP(1-P)} = 500$. We have obtained 500 142 ones. It allows us to proceed with more involved tests. There are many statistical tests for random sequences, but none quarantees 100% certainty for lack of clear criteria of randomness and finite number of samples [27]. Nevertheless we present a few statistical tests which seem to confirm the randomness of our stream. First test starts with division of the sequence of $N = n \cdot m$ samples (zeros and ones) into m bins, each consisting of n samples. Probability to obtain k times one in a single bin of a length n is given with binomial distribution:

$$p_k = \binom{n}{k} P^k (1-P)^{n-k} \overset{P=0.5}{=} \binom{n}{k} \frac{1}{2^n} \qquad (1)$$

Its mean value is $< k >= n \cdot P$ and standard deviation is $\sigma = \sqrt{(1-P)P \cdot n}$. Similarly probability to obtain q_k bins within m each with k ones is:

$$p(q_k) = \binom{m}{q_k} p_k^{q_k} (1-p_k)^{m-q_k} \qquad (2)$$

The expected number of bins with k ones is $< q_k >= p_k \cdot m$. We expect the experimentally determined number of bins with k ones, $q_k^{\exp}$ to deviate on average from q_k by

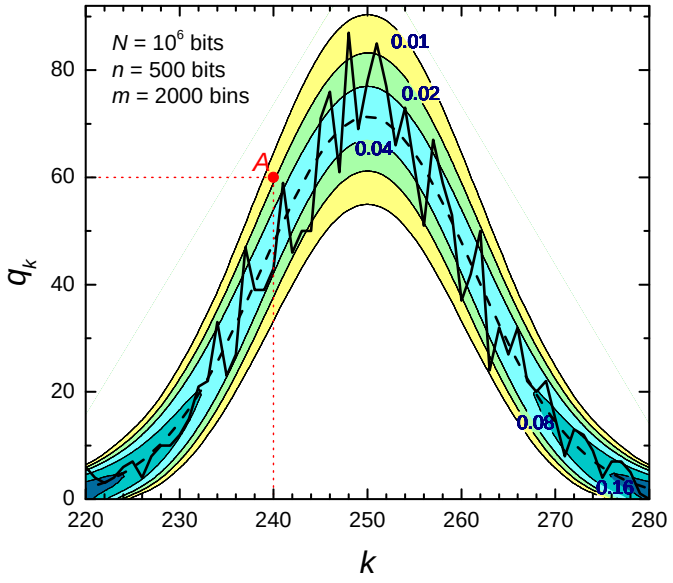


FIG. 5. Probability map for getting q_k bins with k ones with imposed experimentally determined distribution $q_k^{\exp}$ – solid line. Dashed line represents $< q_k >$ distribution. The interpretation of the probability map is explained for point A. It tells that probability for obtaining 60 bins in the total number of 2 000 bins, each with 240 ones is 0.02. We notice that experimentally determined distribution falls within the expected range of probabilities.

standard deviation $\Delta q_k = \sqrt{p_k(1-p_k)m}$. In Fig. 5 we plot theoretical $p(q_k)$ distribution subject to statistical broadening expected for the finite number of m bins. In the same Figure experimentally determined distribution $q_k^{\exp}$ is plotted. We conclude that the test does not negate the randomness of the sequence, for $q_k^{\exp}$ has probability significantly different from zero for all k–values and fluctuates around the mean value $< q_k >$.

The second test utilizes the concept of random walk. We divide the stream of N bits into m bins. Each bin defines one random walk with bit 1 meaning one step forward and bit 0 meaning one step backward. Such a walk, if really random, should obey Einstein-Smoluchowski law: $< l^2 >= i$, where l is a distance traveled from the origin after i steps. The movement corresponds to 1D diffusion of a particle. The distance traveled by the particle after i steps is described with Gaussian distribution with mean value 0 and variance $< l^2 >$. We present trajectories of numerous walks in Fig. 6a. On imposing all walks on each other (Fig. 6b) we obtain a distribution of final positions of the particle after 1, 2, ..., i, ..., n steps. In Fig. 6c we compare average deflection for walks $< l^2 >$ after i steps against Einstein-Smoluchowski law. We conclude that the walks are indeed random.

In the third test stream of random bits $\{\theta_1, \theta_2, ..., \theta_i, ..., \theta_{i+j}, ..., \theta_N\}$ is analyzed for temporal correlations. We define discrete autocorrelation function in the form:

$$ac(j) = \frac{1}{n}\sum_{i=1}^{n} \theta(i) \cdot \theta(i+j) \qquad (3)$$

The product in the sum should give for true random number sequence either 1 (with probability P=1/4) or 0 (with probability P=3/4). The expected value of the autocorrelation function is $< ac >= 1/4$. Autocorrelation with mean value fluctuating around 0.25 calculated for n=730 000 pairs is presented in Fig. 7. It shows no obvious evidence of frequency components. Randomness of our data is also confirmed by NIST Test Suite [25].

VI. DISCUSSION AND POSSIBLE IMPROVEMENTS

We have conducted analogous experiment on superconducting Aluminum nanowire (30 nm thickness, 600 nm cross-section). Sequences obtained for the nanowire also pass tests for randomness. However, since switching current for our nanowire is higher than for Dayem nanobridge, it takes longer time for the nanowire to recover after switching to dissipative state. Switching produces a number of quasiparticles [18]. It accounts for rising the temperature and increases the switching probability in the next trial. It is possible to tackle this problem by using a tunnel JJ that switches to a finite voltage with almost zero current (multiple Andreev reflections [28] produce negligible transmission for tunnel JJ), and consequently a small power dissipated in the JJ. Another approach is to use prepulse, preceding actual measuring pulse. Due to larger amplitude (say 1.3 of that of the measuring pulse) it makes the JJ switch (so called forced switching) and nulls a memory of the JJ. One can say that on average after forced switching the JJ is left with the same number of quasiparticles. The forced switching removes a possible correlation between two successive trials – the obligatory requirement for a good random number generator.

Switching probability is extremely sensitive to the biasing current. It changes according to current noise fed to the junction [29]. It follows junction can be used as a digitizer of the noise with Nyquist frequency limited by the probing period. The frequency components of the noise may be revealed in the time correlation of the switching events. The unbiasing protocol applied to our bits removes correlations due to the random spacing between not rejected pairs of the initial bit stream (Fig.7) (although correlations performed on initial stream may show the 50Hz parasitic current component from power supplies).

One can envisage generation of random bits with magnetic clusters. Magnetization reversal in ferromagnetic nanoclusters, if thermally excited, is described with the Neel-Brown model [30]. The picture of magnetization reversal in the model remains in the complete analogy to

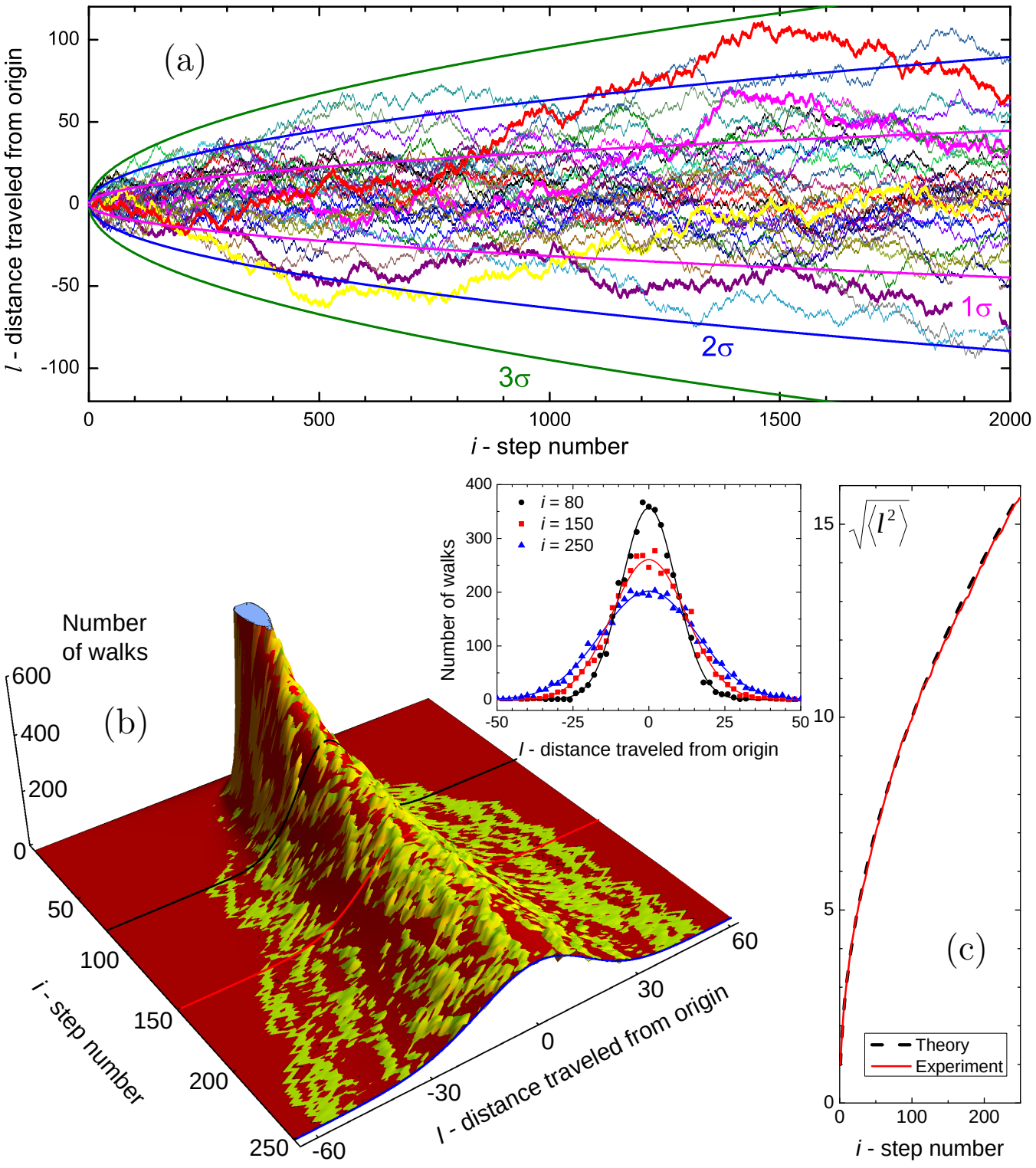


FIG. 6. (a) Representative random walks with theoretical standard deviation imposed ($\sigma, 2\sigma, 3\sigma$ curves). (b) Evolution of random walks distribution with step number i. Smooth red surface is theory - Gaussian distributions with $\sqrt{< l^2 >}$ standard deviations. Yellow rough surface corresponds to experimental distribution established on summing of m=4 000 walks. Three sections, along solid lines, are chosen for clarity and presented in the separate plot. (c) Einstein-Smoluchowski law (dashed black line) compared with experimental data (solid red line).

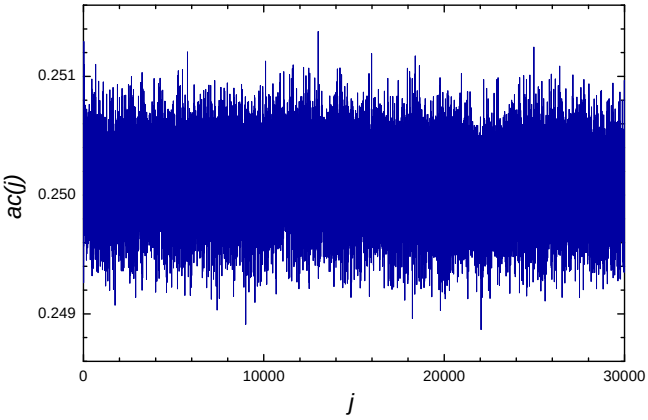


FIG. 7. Autocorrelation of bits vs. distance between them.

the JJ escape out of the metastable state. It follows one can test stochastic character of magnetization reversal by the same measuring protocol we have presented, but rather than pulses of current, magnetic field pulses should be used to give the magnetization a chance to reverse.

VII. OUTLOOK

One straightforward application of our RNG is to use it as an on-chip source of random bits in superconducting circuits. However, there are other fields where our study may be used, involving magnetic flux measurements [31], noise measurements (as briefly pointed out in the Discussion) and mesoscopic thermometry [32]. Switching probability of JJ is very sensitive to biasing current, temperature and magnetic field (if two JJs are connected in parallel to form a SQUID). Conventional measuring protocol for SQUID magnetometry requires use of non-hysteretic SQUIDs [33], although reducing sizes of studied objects towards single spin detection may make hysteretic SQUIDs an interesting alternative for experiments [34, 35]. For such SQUIDs a small change in the switching probability to normal state can be a signature of a spin flip. It is important to stress here that small magnetization change can slightly alter the switching probability, and hence be detectable, in contrast to a threshold detection when magnetization reversal drives the SQUID (initialized in superconducting state with bias just below switching threshold) to the normal state. Of course, the first method requires to launch the same experiment many times (for probability to be measured) and the second is a single shot detection, though if one can afford many repetitions, the enhancement in the sensitivity in the former case is obvious. Our study provides an interesting background for a new type of mesoscopic thermometry and calorimetry [18, 36]. Relaxation of switching probability of JJ initially driven to normal state has allowed us to study heat transport in superconducting nanowires, particularly get access to temporal dynamics of temperature in mesoscopic wires with resolution approaching 10ns. In future we will study thermal properties of mesoscopic islands coupled to JJ.

VIII. CONCLUSIONS

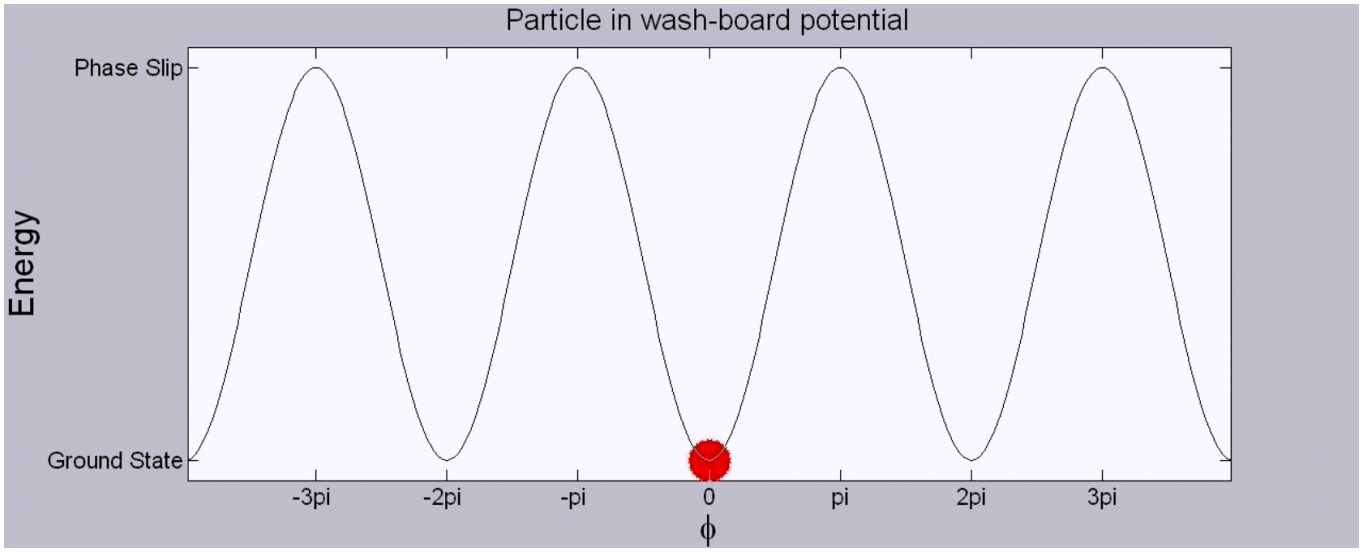
We have demonstrated the operation of the new true nanoscale RNG exploiting inherent randomness of the switching from a superconducting to a non-zero voltage state in Josephson junctions and superconducting nanowires. Our experiments have shown that Cooper pairs in these systems exhibit collective response to a random external stimulus, which allows to treat them as a single archetypal Brownian particle. We have achieved random number generation rates of 10-100 kb/s. However, owing to very fast intrinsic dynamics of JJ (ps response), we anticipate the rate could significantly exceed a few Gb/s in the optimized device. Successful operation of the presented generator has direct implications for applied science. It creates a necessary background for using JJ as a tool in stochastic measurements of physical parameters such as current, magnetic flux and temperature.

ACKNOWLEDGMENTS

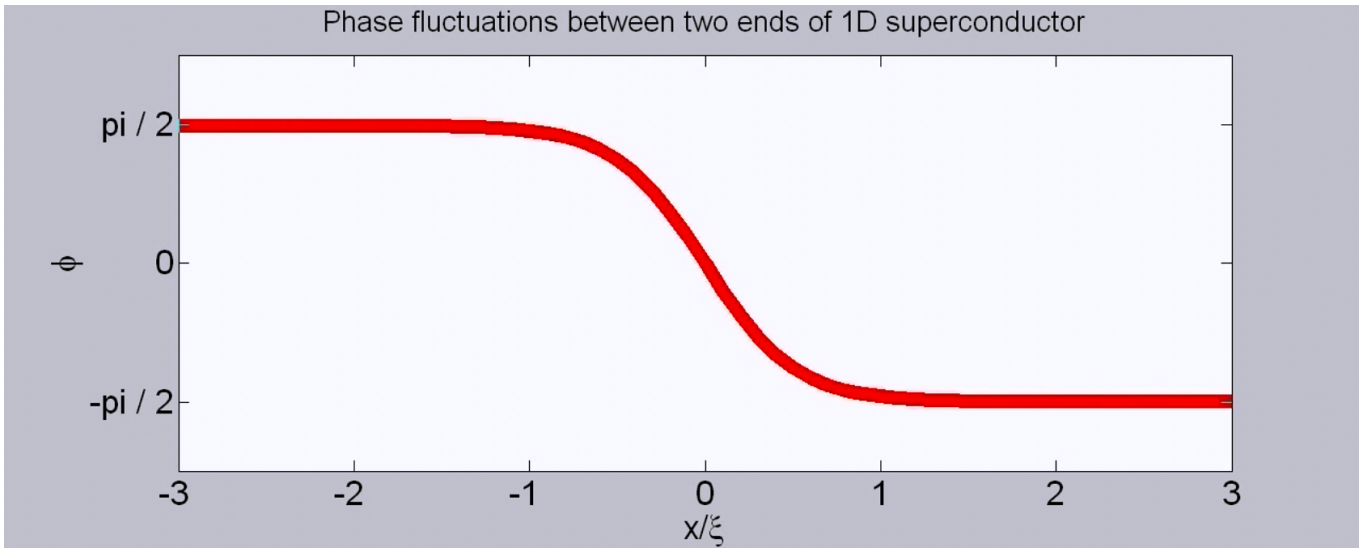
The authors thank Tomasz Dietl for his helpful advice, Łukasz Cywiński for discussions, Olli-Pentti Saira for valuable comments, Cezary Śliwa and Grzegorz Mazur for a technical support. We are very grateful to the Foundation for Polish Science for funding this work through the HOMING PLUS program. We also thank National Science Center, grant MAESTRO (2011/02/A/ST3/00125), and the EAgLE Project. We acknowledge the National Institute of Standards and Technology for access to Test Suite Software.

[1] J. B. Johnson, "Thermal agitation of electricity in conductors," Phys. Rev. **32**, 97–109 (1928).
[2] H. Nyquist, "Thermal agitation of electric charge in conductors," Phys. Rev. **32**, 110–113 (1928).
[3] BBC TV series 'Fun to Imagine' (1983), http://www.bbc.co.uk/archive/feynman/.
[4] J. T. Peltonen, M. Helle, A. V. Timofeev, P. Solinas, F. W. J. Hekking, and J. P. Pekola, "Brownian refrigeration by hybrid tunnel junctions," Phys. Rev. B **84**, 144505 (2011).
[5] John Clarke, Andrew N. Cleland, Michel H. Devoret, Daniel Esteve, and John M. Martinis, "Quantum mechanics of a macroscopic variable: The phase difference

of a josephson junction," Science **239**, 992–997 (1988).
[6] Michel H. Devoret, Daniel Esteve, John M. Martinis, Andrew Cleland, and John Clarke, "Resonant activation of a brownian particle out of a potential well: Microwave-enhanced escape from the zero-voltage state of a josephson junction," Phys. Rev. B **36**, 58–73 (1987).
[7] M. Isida and Y. Ikeda, Ann. Inst. Stat. Math. **8**, 119–126 (1956).
[8] Andre Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden, "Optical quantum random number generator," Journal of Modern Optics **47**, 595–598 (2000).
[9] Ma Hai-Qiang, Wang Su-Mei, Zhang Da, Chang Jun-Tao, Ji Ling-Ling, Hou Yan-Xue, and Wu Ling-An, "A random number generator based on quantum entangled photon pairs," Chinese Physics Letters **21**, 1961 (2004).
[10] T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," Applied Physics Letters **98**, 231103 (2011).
[11] W.T. Holman, J.Alvin Connelly, and A.B. Dowlatabadi, "An integrated analog/digital random noise source," Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on **44**, 521–528 (1997).
[12] M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, and M. Varanonuovo, "A high-speed ic random-number source for smartcard microcontrollers," Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on **50**, 1373–1380 (2003).
[13] Fred Sterzer, "Random number generator using subharmonic oscillators," Review of Scientific Instruments **30**, 241–243 (1959).
[14] D. G. England, P. J. Bustard, D. J. Moffatt, J. Nunn, R. Lausten, and B. J. Sussman, "Efficient raman generation in a waveguide: A route to ultrafast quantum random number generation," Applied Physics Letters **104**, 051117 (2014).
[15] J. T. Gleeson, "Truly random number generator based on turbulent electroconvection," Applied Physics Letters **81**, 1949–1951 (2002).
[16] K. Lee, T. Kim, X. Zhu, D.M. Jacobson, R.S. Madala, W. Wu, J.P. Kim, and S.H. Kang, (2014), Magnetic tunnel junction based random number generator, US Patent App. 13/651,954.
[17] Mitrabhanu Sahu, Myung-Ho Bae, Andrey Rogachev, David Pekker, Tzu-Chieh Wei, Nayana Shah, Paul M. Goldbart, and Alexey Bezryadin, "Individual topological tunnelling events of a quantum field probed through their macroscopic consequences," Nat Phys **5**, 503–508 (2009).
[18] M. Zgirski, L. Bretheau, Q. Le Masne, H. Pothier, D. Esteve, and C. Urbina, "Evidence for long-lived quasiparticles trapped in superconducting point contacts," Phys. Rev. Lett. **106**, 257003 (2011).
[19] T. A. Fulton and L. N. Dunkleberger, "Lifetime of the zero-voltage state in josephson tunnel junctions," Phys. Rev. B **9**, 4760–4768 (1974).
[20] William A. Little, "Decay of persistent currents in small superconductors," Phys. Rev. **156**, 396–403 (1967).
[21] J. S. Langer and Vinay Ambegaokar, "Intrinsic resistive transition in narrow superconducting channels," Phys. Rev. **164**, 498–510 (1967).
[22] M. Tinkham, J. U. Free, C. N. Lau, and N. Markovic, "Hysteretic i-v curves of superconducting nanowires," Phys. Rev. B **68**, 134515 (2003).
[23] H. Courtois, M. Meschke, J. T. Peltonen, and J. P. Pekola, "Origin of hysteresis in a proximity josephson junction," Phys. Rev. Lett. **101**, 067002 (2008).
[24] David K. Gifford, *Natural Random Numbers*, Tech. Rep. (1988).
[25] See Supplemental Material at [URL will be inserted by publisher] for Methods, movies visualising phase fluctuations across nanobridge and NIST Test Suite.
[26] See Randombits.txt at [URL will be inserted by publisher] for a representative stream of generated random bits.
[27] A. Drake, *Fundamentals of Applied Probability Theory* (McGraw Hill, New York, 1967).
[28] E. Scheer, P. Joyez, D. Esteve, C. Urbina, and M. H. Devoret, "Conduction channel transmissions of atomic-size aluminum contacts," Phys. Rev. Lett. **78**, 3535–3538 (1997).
[29] Q. Le Masne, H. Pothier, Norman O. Birge, C. Urbina, and D. Esteve, "Asymmetric noise probed with a josephson junction," Phys. Rev. Lett. **102**, 067002 (2009).
[30] W. Wernsdorfer, E. Bonet Orozco, K. Hasselbach, A. Benoit, B. Barbara, N. Demoncy, A. Loiseau, H. Pascard, and D. Mailly, "Experimental evidence of the néel-brown model of magnetization reversal," Phys. Rev. Lett. **78**, 1791–1794 (1997).
[31] C. P. Foley and H. Hilgenkamp, "Why nanosquids are important: an introduction to the focus issue," Superconductor Science and Technology **22**, 064001 (2009).
[32] S. Gasparinetti, K. L. Viisanen, O. P. Saira, T. Faivre, M. Arzeo, M. Meschke, and J. P. Pekola, "Fast electron thermometry for ultrasensitive calorimetric detection," Phys. Rev. Applied **3**, 014007 (2015).
[33] J. Clarke and A.I. Braginski, *The SQUID Handbook* (WILEY-VCH, Weinheim, 2004).
[34] W Wernsdorfer, "From micro to nano-squids: applications to nanomagnetism," Superconductor Science and Technology **22**, 064013 (2009).
[35] John Gallop, "Squids: some limits to measurement," Superconductor Science and Technology **16**, 1575 (2003).
[36] Foltyn, M. and Zgirski, M., "Heat Transfer in superconducting nanowires investigated with Josephson junctions," (2015), (unpublished).



Video 1. Fluctuations of the particle (phase) in the tilted washboard potential leading occasionally to phase slip.



Video 2. Fluctuating phase across nanobridge.