Experimental quantum randomness generation invulnerable to the detection loophole

Gustavo Cañas1,2,3, Jaime Carirne2,4, Esteban S. Gómez1,2,3, Johanna Figueroa1,2,3, Adán Cabello5, Guilherme B. Xavier2,3,4, Gustavo Lima1,2,3 & Marcin Pawłowski6
1Departamento de Física, Universidad de Concepción, 160-C Concepción, Chile.
2Center for Optics and Photonics, Universidad de Concepción, 160-C Concepción, Chile.
3MSI-Nucles for Advanced Optics, Universidad de Concepción, 160-C Concepción, Chile.
4Departamento de Ingeniería Eléctrica, Universidad de Concepción, 160-C Concepción, Chile.
5Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain.
6Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, PL-80-952 Gdańsk, Poland.

Random numbers are essential for multiple applications, including cryptography, financial security, digital rights management and scientific simulations. However, producing random numbers from a finite state machine, such as a classical computer, is impossible. One option is to use conventional quantum random number generators (QRNGs) based on the intrinsic uncertainty of quantum measurement outcomes. The problem in this case is that private randomness relies on assumptions on the internal functioning of the measurement device. “Device-independent” QRNGs not relying on devices inner workings assumptions can be built but are impractical. They require a detection efficiency that, so far, has only been achieved with trapped ions and with photons detected with transition-edge superconducting sensors. Here we introduce a novel protocol for quantum private randomness generation that makes no assumption on the functioning of the devices and works even with very low detection efficiency. We implement the protocol using weak coherent states and standard single-photon detectors. Our results pave the way towards a second generation of more secure practical QRNGs.

The protocol based on the semi-device-independent (SDI) approach to randomness generation introduced by Pawłowski and Brunner. The SDI approach works in a prepare-and-measure scenario in which no assumption is made on the internal functioning of the preparation and measurement devices, except that the dimension of the quantum system accessed by the measurement device is bounded. Remarkably, unlike device-independent QRNGs, our protocol is able to certify randomness even with very low detection efficiency, thus proving right the conjecture that SDI protocols could be robust against detection loophole attacks. We demonstrate this protocol by experimentally generating certified private random bits with weak coherent states and standard single-photon detectors providing an overall detection efficiency of 6%.

The protocol works in the scenario and under the assumptions described in Fig. Each round of the experiment produces an event \( (b|x,y,z) \). The user follows the steps below:

Step 1. The user estimates the probabilities \( p(b|x,y \lambda,z) \) and also the probabilities \( p'(b|x,y \lambda,z) \) obtained after removing all events in which \( b = \emptyset \).

Step 2. The goal of step 2 is to allow the user to check whether or not there is shared randomness between \( x \) and \( z \) that may compromise the randomness and privacy of the final string. For that, the user estimates the probability \( p_{av} = \frac{1}{2} \sum_{x,z} p'(0|x,y > \lambda,z) \) and the observed overall detection efficiency \( \eta = \frac{1}{2} \sum_{x,z} \sum_{b \in \{0,1\}} p(b|x,y > \lambda,z)/\sum_{x,z} \sum_{b \in \{0,1\}} p(b|x,y > \lambda,z) \). If \( p_{av} \) is above a certain threshold that depends on \( \lambda \) and \( \eta \), then the user can conclude that there is no shared randomness and moves on to the step 3 (see Methods). If it is below this threshold, then the user aborts.

Step 3. The user defines a bit string \( S \) as follows: \( b \) if \( y > \lambda \) and \( b \in \{0,1\} \), 0 if \( y > \lambda \) and \( b = 0 \). Hereafter we will denote these events as \( (b|x,z) \). The goal of step 3 is to estimate the randomness in \( S \). The method for this is as follows.

The Lemma in Methods shows that the best strategy for an adversary without shared randomness is the following: For each \( x \), the adversary’s agent in \( P \) prepares a pure qubit state \( |\tilde{x} \rangle \) in the equatorial plane of the Bloch sphere. For a given \( z \), the adversary’s agent in \( M \): (I) With frequency \( p_z \), performs a measurement that projects the qubit into \( |m_z = 0 \rangle \) or \( |m_z = 1 \rangle \) and outputs \( b = 0 \) or \( b = 1 \), respectively. (II) With frequency \( q_z \), makes no measurement on the qubit and outputs \( b = 0 \). (III) With frequency \( q_z \), makes no measurement on the qubit and outputs \( b = 1 \). Since in those cases in which no measurement is performed, the choice of output \( b = 0 \) or \( b = 1 \) can be done using a pseudo random number generator (PRNG), we will assume that there is no randomness with frequency \( q_z + q_z = 1 \). By the normalization condition for probabilities, \( p_z + q_z = 1 \). The amount of randomness in the events \( (b|x,z) \), measured by the min-entropy, is

\[
H_{av}(b|x,z) = -p_z \log_2 \left| \langle m_z = b|x \rangle \right|^2,
\]

where \( \left| \langle m_z = b|x \rangle \right|^2 \) is the probability of projecting into \( |m_z = b \rangle \) when the state prepared is \( |x \rangle \). Since \( P \) and \( M \) are black boxes, the user does not know \( p_z \), \( |x \rangle \) and \( |m_z = b \rangle \). The user only has access to the probabilities \( p(b|x,z) \) that can be estimated from the experiment. The relation between them is

\[
p(b|x,z) = q_z + p_z|\langle m_z = b|x \rangle|^2.
\]

The randomness indicator used in the protocol is a list \( \tilde{P} \) of the 8 probabilities \( p(0|x,z) \). After the experiment is complete, the user has each \( p(0|x,z) \) with a confidence

\[
p(0|x,z)_{min} \leq p(0|x,z) \leq p(0|x,z)_{max}.
\]

Then, a numerical minimization of the min-entropies of the 8 events \( (0|x,z) \) under the constraints is performed to obtain the amount of randomness.

What is remarkable in our protocol is that \( \tilde{P} \) allows the user to certify more randomness than with any indicator used in previous works, e.g., the average success probability, \( p_{av} = \frac{1}{2} \sum_{x,z} p(0|x,z) \), or the worst case probability, \( \min_{x,z} p(0|x,z) \), the benefit of using \( \tilde{P} \) over \( p_{av} \) or \( \min_{x,z} p(0|x,z) \) is illustrated in Fig. 2. This clear advantage contrasts with the marginal increase in the amount of certified randomness found in Bell-inequality scenarios when using the whole probability distribution instead of a single number.
certification follows from the analysis of the conditional probability distributions \( p \) being generated and measured through the control of the grey.

One has full control of the real and imaginary parts of the states onto the next one. The qubit state preparation in \( P \) sets of lenses are employed to project the image of one SLM through a sequence of four spatial light modulators (SLMs) 20. The optical pulses are then sent through a sequence of four spatial light modulators (SLMs) 20. Each QRNG supplies a continuous string of bits. The field programmable gate array (FPGA) in \( P \) produces an electrical synchronization signal and attenuated optical pulses (weak coherent quantum states). The optical pulses are then sent through a sequence of four spatial light modulators (SLMs) 20. The repetition rate of the attenuated optical pulses is set to 30 Hz, which is the limit of the employed SLMs. The SLMs are controlled by their corresponding FPGA units. The modulation applied in each SLM is triggered by the sync signal. An internal delay in respect to the AOM in the FPGAs is used to ensure that the SLMs in \( P \) and \( M \) are properly set by the time each coherent state is sent. Each QRNG produces approximately 4 million bits/s, which means that for every sync signal there are always fresh random numbers available to randomly prepare and measure. Each round, pre-determined phase and amplitude masks are applied to the SLMs based on the new numbers produced by the QRNGs. These masks are built such that the states are the dimensional quantum states to study more complex scenarios for quantum randomness generation.

The purpose of the protocol is to generate certified random private bits from apparently random bits. The final string of certified random private bits is obtained after post-processing the events \( b|x,y,z \). This certification follows from the analysis of the conditional probability distributions \( p(b|x,y,z) \) estimated by the user.

**Figure 1: Scenario and assumptions of our SDI randomness generation protocol.** In each round of the experiment, the preparation device \( P \) receives an input \( x \) and emits a system that goes into a measurement device \( M \) that receives an input \( z \) and produces an outcome \( b \). There is a blocker \( B \) that may or may not block the system depending on input \( y \). The assumptions made in our protocol are: (i) \( P \) and \( M \) are black boxes built by the adversary, their internal functioning is unknown and inaccessible to the user. Each device may contain an agent of the adversary. (ii) \( P \) and \( M \) are shielded in the sense that \( P \) only receives input \( x \in \{00,01,10,11\} \) and only outputs a qubit state \( \rho \), and \( M \) only receives a qubit (or nothing, i.e., \( \emptyset \)) and \( z \in \{0,1\} \) as inputs, and only outputs \( b \in \{0,1,\emptyset\} \). The outcome \( b = \emptyset \) corresponds to the case in which no result is obtained either because the blocker \( B \) was acting or because the detection efficiency is not perfect. (iii) \( B \) only receives \( y \in [0,1] \) as input and blocks (absorbs) the qubit if and only if \( y \leq \lambda \) (where \( \lambda \) is characteristic of \( B \)). (iv) \( x, y, z \) are apparently random. A string is apparently random when it has passed some standard tests of randomness, but may fail to pass other tests. (v) The laboratory containing \( P, B, M \) and the generators of \( x, y \) and \( z \) is shielded in the sense that nothing can enter or exit. The purpose of the protocol is to generate certified random private bits from apparently random bits. The final string of certified random private bits is obtained after post-processing the events \( b|x,y,z \). This certification follows from the analysis of the conditional probability distributions \( p(b|x,y,z) \) estimated by the user.

Step 4. The user extracts the final private random bit string by applying standard post-processing techniques on \( \mathcal{S} \) (e.g., ref. 13).

Our experimental implementation of the protocol is shown schematically in Fig. 1. As the sources of \( x, y \) and \( z \) we use three commercial QRNGs QUANTIS. They satisfy the definition of apparent randomness because they have passed standard tests of randomness. Each QRNG supplies a continuous string of bits. The field programmable gate array (FPGA) in \( P \) produces an electrical synchronization signal and attenuated optical pulses (weak coherent quantum states). The optical pulses are then sent through a sequence of four spatial light modulators (SLMs). Sets of lenses are employed to project the image of one SLM onto the next one. The qubit state preparation in \( P \) (the projections in \( M \)) is implemented using SLM 1 and SLM 2 (SLM 3 and SLM 4) working with amplitude-only and phase-only modulation, respectively. We use the linear transverse momentum of the single photons transmitted by the SLMs as the degree of freedom for codifying qubit states. This is done by making only two paths available for the photon transmission through the SLM. One has full control of the real and imaginary parts of the states being generated and measured through the control of the grey level of the SLMs pixels. The advantage of this setup (with respect to other encoding approaches, such as polarization or time-bin) is that it can be easily adapted to codify higher dimensional quantum states to study more complex scenarios for quantum randomness generation.
Figure 3: **Experimental setup.** Attenuated optical pulses are produced with a continuous wave laser, an acousto-optic modulator (AOM), and adjustable optical attenuators. The SLMs are controlled by their corresponding FPGA electronics, which prepare the qubit state and perform the appropriate projection based on the supplied random numbers from their corresponding QRNG. The three QRNGs provide the random numbers required for our SDI quantum randomness generation protocol. In order to detect shared randomness between the preparation and measurement stages, a random blocker is placed in the path between them (see Methods). A computer (PC) receives the blocking and the random settings information to estimate the min-entropy of the generated random bit string.

With the rest of the setup. For each round of the experiment, the blocker’s FPGA unit randomly decides whether it will block the pulse or not, with an user-adjustable blocking probability. If a pulse is blocked, this information is sent to a computer (PC).

For our experimental implementation, with $\eta = 0.06$, a blocking rate of 99% was employed to guarantee that there is no shared randomness. The threshold for privacy as a function of the blocking rate and $\eta$ is presented in Fig. 4. Clearly, one can see that our generated bit string is certifiably private.

Remarkably, Fig. 4 also shows that, for $\eta > 0$, there is always a blocking rate smaller than 1 such that observing $p_{av} > 0.5$ allows the user to guarantee with a 99% confidence that there is no shared randomness.

The optical quality of the experiment is indicated by the fact that the experimental probabilities $p'(0|x, y > \lambda, z)$ show a very good agreement with the predictions of quantum mechanics, as illustrated in Fig. 5. In each round of the experiment 0.0093 true random bits are certified, yielding a random bit generation rate of 0.28 Hz. The effectiveness of our randomness indicator $\bar{P}$ is demonstrated by the fact that no random bits would have been certified using $p_{wc}$ or $p_{av}$. The final certified bit string $\mathcal{S}$ generated in our experiment is $10^5$ bits long. We emphasize that our rate could be increased to the Mbit/s range with current technology of SLMs based on integrated silicon photonics. Even without modern SLMs, the private random bit generation rate of our experiment can be increased by a factor of 20 by decreasing the blocking rate to 0.8. Therefore, our scheme is capable of outperforming the rate produced by recent experiments based on Bell inequalities with photons detected with superconducting transition-edge sensors (0.4 Hz with overall detection efficiency of 75%).

In conclusion, we have experimentally demonstrated a new protocol for generating private random numbers which is more secure than conventional QRNGs and is, at the same time, practical for real-life applications. It is more secure because: (i) it does not require the assumptions on the internal functioning of the devices needed in current QRNGs and (ii) it does not need the assumption that the preparation and measurement devices have no initial shared randomness. It is practical because it does not require high detection efficiency. It is the first protocol for randomness generation invulnerable to the detection loophole. Therefore, in this work we have demonstrated a novel approach that can rise up to the challenge of real-life applications requiring private, secure and high-rate random number generation certified by quantum mechanics.

**Methods**

**Blocking to counteract shared randomness**

In order to understand why the use of $B$ is sufficient to counteract any shared randomness, imagine an adversary who sells the user $P$ and $M$ devices equipped with identical PRNGs fed with the same seed. There are three ways in which the same seed can be fed: (i) The devices may have the seed stored inside them since they were built by the adversary. Option (i) is problematic for the adversary, since the user can employ several $P$ and $M$ devices paired randomly. If all of them share the same
random string, correlations will be seen in success probabilities if all devices get the same inputs. (ii) The seed may be sent to P and M when they are operating. Option (ii) is not possible in our scenario with P and M inside a shielded laboratory. (iii) The seed may be communicated somehow from the adversary’s agent in P to the adversary’s agent in M using the qubit during the protocol. In this case, randomly blocking some rounds of the experiment helps the user against the communication of the agent’s seed. Even if the agents in P and M manage to establish a common seed, they would still need a way of synchronizing their strategies. That is, even if they know the value of the random variable for every round of the protocol, the agents need to agree on which round of protocol they are currently in. If we assume the most favourable condition for the adversary, which is that the synchronization uses only one round of the protocol, then in this round the success probability will be $\frac{1}{2}$.

It is also important to notice that B also helps the user in case the adversary’s agents in P and M share quantum correlations. Even if the agents have entangled pairs of particles, this is useless to them since the agents do not know whether or not their particles belong to the same pair.

Figure 2: Comparison among randomness indicators. Large diagram: Randomness, measured by the min-entropy, certified using $\hat{P}$ (green curve), $p_{wc}$ (red curve) and $p_{av}$ (blue curve). It is assumed that $p(0|x,z)^{\text{min}} = \alpha - \frac{\delta}{2}$ and $p(0|x,z)^{\text{max}} = \alpha + \frac{\delta}{2}$, with $\delta = 10^{-8}$. The results for $p_{av}$ are taken from Mironowicz et al. The threshold probability for certifying randomness when using $\hat{P}$ is 0.5, while it is 0.75 for $p_{wc}$ and 0.829 for $p_{av}$. Small diagram: Randomness certified using $\hat{P}$ for small $\alpha$ and $\delta = 10^{-8}$. $p_{wc}$ and $p_{av}$ cannot certify randomness in this case.

Figure 4: Threshold value for $p_{av}'$ to guarantee that there is no shared randomness with a confidence of 0.99 and taking the most favourable conditions for the adversary, as a function of the blocking rate and for different values of $\eta$. The invulnerability against the detection loophole follows from the fact that, for $\eta > 0$, there is always a blocking rate smaller than 1 such that observing $p_{av}' > 0.5$ allows the user to guarantee that there is no shared randomness. The dot with error bars indicates the $p_{av}'$ observed in our experiment in which the blocking rate is 0.99 and $\eta = 0.06$. The error bars are calculated using Poissonian statistics. The blocking rate was chosen to show that we can discard shared randomness even with a very low detection efficiency ($\eta = 0.001$).

Most general attack with no shared randomness
Assuming no shared randomness, the most general attack that the adversary can follow is always equivalent to performing some positive-operator valued measure (POVM) in M. However, this attack is difficult to parameterize. The Lemma below enables us to use classical preprocessing and projective measurements to describe the most general attack that the adversary can perform.

Lemma: In a prepare-and-measure scenario without shared randomness, if the communicated system is a qubit and the output is $b \in \{0, 1\}$, any conditional probability distribution $p(b|x,z)$ can be achieved by choosing outcome $b = 0$ with probability $q_0$, outcome $b = 1$ with probability $q_1$, and performing a projective measurement with probability $p_\text{z} = 1 - q_0^2 - q_1^2$. The error bars are calculated using Poissonian statistics. The blocking rate was chosen to show that we can discard shared randomness even with a very low detection efficiency ($\eta = 0.001$).

Proof: For each $z$ let us consider the most general two-outcome POVM. Let $E_z$ be the POVM element corresponding to the outcome $b$. Let $E_z^0 = \begin{pmatrix} c_z & 0 \\ 0 & c_z^* \end{pmatrix}$ and the basis in which $E_z^1$ is diagonal be $\{|m_0 = 0\}, \{|m_1 = 1\}\}$. For any state $|x\rangle = c_x^0 |0\rangle_z + c_x^1 |1\rangle_z$, the probability to observe outcome $b = 0$ is $p(0|x,z) = c_x^0 d_x^0 c_z^* + c_x^1 d_x^1 c_z^*$. Without loss of generality, we may assume that $c_x^0 \geq c_x^1$. If we set $q_0 = c_x^0$ and $q_1 = 1 - c_x^0$ and choose the projective measurement to be in the basis $\{|m_x = 0\}, \{|m_x = 1\}\}$, then the prescription given in the Lemma exactly reproduces the probability distribution of the outcomes of the measurement $E_z^0$.

To certify randomness the user estimates $p(0|x,z)$ from the experimental data and then uses the Lemma to numerically optimize over $q_0, q_1, |x\rangle, \{|m_0 = 0\}, \{|m_1 = 1\}$ minimizing the min-entropy for $x,z$.

Acknowledgements: This work was supported by the grants
Figure 5: Theoretical and experimental probabilities. Observed conditional probabilities $p/(0|x, y > \lambda, z)$ compared with the theoretical predictions. The error bars are calculated using Poissonian statistics for single photon detection.

References

[1] Rarity, J. G., Owens, P. C. M., & Tapster, P. R. Quantum random-number generation and key sharing. J. Mod. Opt. 41 2435 (1994).

[2] Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L., & Zbinden, H. Optical quantum random number generator. J. Mod. Opt. 47, 595 (2000).

[3] Uchida, A., Amano, K., Inoue, M., Hirano, K., Naito, S., Someya, H., Owada, I., Kurashige, T., Shiki, M., Yoshimori, S., Yoshimura, K., & Davis, P. Fast physical random bit generation with chaotic semiconductor lasers. Nature Photon. 2, 728 (2008).

[4] Gabriel, C., Wittmann, C., Sych, D., Dong, R., Mauerer, W., Andersen, U., Marquardt, C., & Leuchs, G. A generator for unique quantum random numbers based on vacuum states. Nature Photon. 4, 711 (2010).

[5] Ren, M., Wu, E., Liang, Y., Jian, Y., Guang, W., & Zeng H. Quantum random-number generator based on a photon-number-resolving detector. Phys. Rev. A 83, 023820 (2011).

[6] Colbeck, R. Quantum and Relativistic Protocols for Secure Multi-Party Computation, Ph.D. Thesis, Cambridge University (2007).

[7] Pironio, S., Acín, A., Massar, S., Boyer de la Giroday, A., Matsukevich, D. N., Maunz, P., Olimschek, S., Hayes, D., Luo, L., Manning, T. A. & Monroe, C. Random numbers certified by Bell’s theorem. Nature 464, 1021 (2010).

[8] Giustina, M., Mech, A., Ramelow, S., Wittmann, B., Kofler, J., Beyer, J., Lita, A., Calkins, B., Gerrits, T., Nam, S. W., Ursin, R., & Zeilinger, A. Bell violation using entangled photons without the fair-sampling assumption. Nature 497, 227 (2013).

[9] Christensen, B. G., McCusker, K. T., Altepeter, J. B., Calkins, B., Gerrits, T., Lita, A. E., Miller, A., Shalm, L. K., Zhang, Y., Nam, S. W., Brunner, N., Lim, C. C. W., Gisin, N. & Kwiat, P. G. Detection-loophole-free test of quantum nonlocality, and applications. Phys. Rev. Lett. 111, 130406 (2013).

[10] Pawlowski, M. & Brunner, N. Semi-device-independent security of one-way quantum key distribution. Phys. Rev. A 84, 010302(R) (2011).

[11] Dall’Arno, M., Passaro, E., Gallego, R., Pawlowski, M. & Acín, A. Attacks on semi-device independent quantum protocols. Quant. Inf. Comp. 15, 0037 (2015).

[12] Bowles, J., Quintino, M. T. & Brunner, N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. Phys. Rev. Lett. 112, 140407 (2014).

[13] Li, H.-W., Yin, Z.-Q., Wu, Y.-C., Zou, X.-B., Wang, S., Chen, W., Guo, G.-C. & Han, Z.-F. Semi-device-independent random-number expansion without entanglement. Phys. Rev. A 84, 034301 (2011).

[14] Ambainis, A., Nayak, A., Ta-Shma, A. & Vazirani, U. Dense quantum coding and quantum finite automata. J. ACM 49, 496 (2002).

[15] Nieto-Silleras, O., Pironio, S. & Silman, J. Using complete measurement statistics for optimal device-independent randomness evaluation. New J. Phys. 16, 013035 (2014).

[16] Bancal, J.-D., Sheridan, L. & Scarani, V. More randomness from the same data. New J. Phys. 16, 033011 (2014).

[17] Mironowicz, P., Li, H.-W. & Pawłowski, M. Properties of dimension witnesses and their semi-definite programming relaxations. Phys. Rev. A 90, 022322 (2014).

[18] von Neumann, J. Various techniques used in connection with random digits. National Bureau of Standards Applied Math Series 12, 36 (1951).

[19] http://www.idquantique.com/random-number-generators/products.html

[20] Grier, D. G. A revolution in optical manipulation. Nature 424, 810 (2003).

[21] Lima, G., Vargas, A., Neves, L., Guzmán, R. & Saavedra, C. Manipulating spatial qudit states with programmable optical devices. Opt. Express 17, 10688 (2009).

[22] Lima, G., Neves, L., Guzmán, R., Gómez, E. S., Nogueira, W. A. T., Delgado, A., Vargas, A. & Saavedra, C. Experimental quantum tomography of photonic qudits via mutually unbiased basis. Opt. Express 19, 3542 (2011).

[23] Etcheverry, S., Cañas, G., Gómez, E. S., Nogueira, W. A. T., Saavedra, C., Xavier, G. B. & Lima, G. Quantum key distribution session with 16-dimensional photonic states. Sci. Rep. 3, 2316 (2013).
[24] Cañas, G., Etcheverry, S., Gómez, E. S., Saavedra, C., Xavier, G. B., Lima, G. & Cabello, A. Experimental implementation of an eight-dimensional Kochen-Specker set and observation of its connection with the Greenberger-Horne-Zeilinger theorem. *Phys. Rev. A* **90**, 012119 (2014).

[25] Cañas, G., Arias, M., Etcheverry, S., Gómez, E. S., Cabello, A., Xavier, G. B. & Lima, G. Applying the simplest Kochen-Specker set for quantum information processing *Phys. Rev. Lett.* **113**, 090404 (2014).

[26] Qiu, C., Chen, J., Xia, Y. & Xu, Q. Active dielectric antenna on chip for spatial light modulation. *Sci. Rep.* **2**, 855 (2012).

**Author contributions:** M.P. conceived the protocol. G.C., J.C., E.S.G. & J.F. carried out the experiment and analyzed the data. A.C., G.B.X., G.L. & M.P. supervised the project and wrote the manuscript. All authors discussed the results and agreed on the conclusions.

**Additional information:** Correspondence and requests for materials should be addressed to G.L. & M.P. The authors declare no competing financial interests.