SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:
QUANTUM INFORMATION
QUBITS
INFORMATION THEORY AND COMPUTATION
QUANTUM OPTICS

Received
23 April 2013

Accepted
29 July 2013

Published
16 August 2013

Correspondence and requests for materials should be addressed to X.F.M. (xma@tsinghua.edu.cn)

Decoy-state quantum key distribution with biased basis choice

Zhengchao Wei[1,2], Weilong Wang[1,2], Zhen Zhang[1], Ming Gao[2], Zhi Ma[2] & Xiongfeng Ma[1]

[1]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, P. R. China, [2]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, China.

We propose a quantum key distribution scheme that combines a biased basis choice with the decoy-state method. In this scheme, Alice sends *all* signal states in the *Z* basis and decoy states in the *X* and *Z* basis with certain probabilities, and Bob measures received pulses with optimal basis choice. This scheme simplifies the system and reduces the random number consumption. From the simulation result taking into account of statistical fluctuations, we find that in a typical experimental setup, the proposed scheme can increase the key rate by at least 45% comparing to the standard decoy-state scheme. In the postprocessing, we also apply a rigorous method to upper bound the phase error rate of the single-photon components of signal states.

Quantum key distribution (QKD)[1,2] is one of the most realistic applications in quantum information. It aims at extending a secret key between two distant parties, commonly noted as Alice and Bob. The unconditional security has been proven even when an eavesdropper, Eve, has unlimited computation power permitted by quantum mechanics[3–6].

The best known protocol of QKD is the BB84 protocol[1] presented by Bennett and Brassard in 1984. In BB84, Alice encodes the key information randomly into the *X* and *Z* bases and sends quantum pulses to Bob. Bob measures the received pulses in two bases randomly. After that, they compare the basis through an authenticated classical channel. The key can only be extracted from the pulses where they use the same basis and this results in that on average half of the raw data is discarded. That is, the basis-sift factor is 1/2 in the original BB84 protocol. This factor can be improved by the efficient BB84 scheme proposed by Lo et al.[7]. In the efficient scheme, Alice and Bob put a bias in the probabilities of choosing the *Z* basis and *X* basis, which can make the basis sift-factor close to 100% in the infinitely long key limit. The efficient BB84 scheme is experimentally demonstrated in 2009[8].

In practical QKD systems, a highly attenuated laser or a weak coherent state source is widely used to substitute for a perfect single-photon source which is beyond state-of-the-art technology. A weak coherent state source contains multi-photon components (details shown in Methods). When multi-photon states are used for QKD, Eve can launch attacks, like the photon-number-splitting (PNS) attack[9,10], to break the security. Since Eve could have a full control of the quantum channel, she can make the transmittance of multi-photon states to be 100% in the PNS attack. In a conventional security analysis[11], Alice and Bob have to assume all the losses and errors come from the single-photon components in the worst scenario case. As a result, the performance of QKD is very poor. To improve the performance of the weak coherent state QKD, Hwang proposed the decoy-state method[12]. Instead of sending one coherent state, Alice sends pulses with different intensities, so that she can obtain more information to monitor the quantum channel. To maintain the detection statistics of coherent states with different intensities, Eve is not able to change the transmittances of single-photon and multi-photon state freely without being noticed by Alice and Bob. The security of the decoy-state method is proven[13], along with various practical schemes[14,15]. Follow-up experimental demonstrations show that the decoy-state method is a very effective way to improve QKD performance[16–20].

Naturally, we can improve the decoy-state method by applying the biased-basis idea of the efficient BB84 protocol. There are a few observations. First, Alice does not need to choose basis when she chooses the vacuum decoy state. Second, if Alice and Bob mainly choose one basis, say *Z* basis, for key generation, they effectively treat *X* basis as for quantum channel testing. In this sense, the functionality of *X* basis is similar to the decoy states. Intuitively, one may expect to combine decoy states and *X* basis together.

Here, we propose a new decoy-state method with biased basis choice, following the widely used decoy-state scheme, vacuum + weak decoy-state method[15] (a quick review is shown in Methods), where Alice sends out

pulses with three different intensities, vacuum (with an intensity of 0), weak decoy (with an intensity of v) and signal (with an intensity of μ) states.

1. Alice prepares *all* the signal pulses (μ) in the Z basis, where the final secure key is extracted from.
2. She prepares weak decoy pulses (v) in the X and Z with certain probabilities.
3. If she chooses the vacuum decoy state, she does not need to set any basis.
4. Bob measures the received pulses in the X basis and Z basis with probabilities p_x and p_z, respectively.

The scheme is summarized in Table 1. In the new scheme, only 4 sets of preparations are used by Alice. Compared to the original vacuum + weak decoy-state method, where 6 sets are used, the proposed scheme can simplify the system and reduce the cost of random numbers. Later in the simulation, we will show that this scheme can also improve the QKD performance.

Following the GLLP security analysis[11], the key generation rate[13,21] is given by

$$\begin{aligned} R &\geq q\{-I_{ec}+Q_1^z[1-H(e_1^{pz})]+Q_0\},\\ I_{ec} &= fQ_\mu H(E_\mu),\\ q &= \frac{N_\mu p_z}{N_{total}}, \end{aligned} \tag{1}$$

where q is the raw data sift factor, including basis-sift factor and signal-state ratio; I_{ec} is the cost of error correction and the rest terms in the bracket is the rate of privacy amplification; f is the error correction inefficiency; Q_μ and E_μ are the overall gain and quantum bit error rate (QBER); Q_1^z is the gain of the single-photon components and e_1^{pz} is its corresponding phase error rate; Q_0 is the background gain; $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. Note that in our scheme, the final key is extracted from Z-basis measurement results, so all the variables in equation (1) should be measured in the Z basis. The phase error rate e_1^{pz} cannot be measured directly, which, instead, can be inferred from the error rate in the X basis[22].

The gain and QBER, Q_μ and E_μ, can be measured from the experiment directly. Alice and Bob need to estimate Q_1^z and e_1^{pz} for privacy amplification. According to the model reviewed in Methods, we have $Q_1^z = Y_1^z\mu e^{-\mu}$ and $Q_0 = Y_0 e^{-\mu}$, where Y_1^z and Y_0 are the yield of single-photon components measured in the Z basis and background rate, respectively. In order to lower bound the key rate equation (1), one can lower bound Y_1^z, Y_0 and upper bound e_1^{pz}.

Since that both the vacuum state and the single-photon state are basis independent, the yields of vacuum states and single-photon states in different bases are equal

$$\begin{aligned} Y_0^x &= Y_0^z,\\ Y_1^x &= Y_1^z. \end{aligned} \tag{2}$$

While a multi-photon state is basis dependent, whose basis information may be revealed to Eve by, for example, PNS attack[9], so for any i-photon state ($i \geq 2$), in general,

$$Y_i^x \neq Y_i^z. \tag{3}$$

That is, depending on the basis information, Eve may set the yield of i-photon state different for the X and Z bases. As for the error rates, the phase error probability in the Z basis equals to the bit error probability in the X basis

$$e_1^{pz} = e_1^{bx}. \tag{4}$$

Then, in the finite-key-size situation where statistical fluctuations should be taken into account[22,23], we have

Table 1 | List of Alice and Bob's operations. Alice prepares and sends N_{total} pulses, with $N_{total} = N_\mu + N_v^z + N_v^x + N_0$. Bob measures the received pulses with certain probabilities, $p_z + p_x = 1$

Alice prepares and sends	Bob measures
N_μ signal pulses in the Z basis	with probability p_z in the Z basis
N_v^z decoy pulses in the Z basis	
N_v^x decoy pulses in the X basis	with probability p_x in the X basis
N_0 vacuum pulses	

$$e_1^{pz} \approx e_1^{bx}. \tag{5}$$

Given e_1^{bx}, we can upper bound e_1^{pz} by the random sampling argument (details shown in Methods). We need to point out that even though the single-photon state is basis independent, the error rates in two basis may not be the same

$$e_1^x \neq e_1^z. \tag{6}$$

This can be easily seen by considering a simple intercept-and-resend attack where Eve measures all the pulses in the Z basis, and then she will not introduce any additional error in the Z basis $e_1^z = 0$, but $e_1^x = 1/2$.

Results

In our simulation, the parameters of the experimental setup are listed in Table 2. Statistical fluctuations are taken into account in the simulation (details shown in Methods). We compare the key generation rate in our scheme with that in the standard BB84 protocol with the vacuum + weak decoy-state scheme. The result is shown in Fig. 1.

As one can see from Fig. 1, the key rate of the proposed biased scheme is larger than that of the standard BB84 with vacuum + weak decoy states by at least 45%. When the transmission loss is 0, the key rate improvement can go up to 80%. As the transmission loss increases, the improvement of the biased scheme decreases. This is because at a larger transmission loss, more pulses for decoy states are needed and Bob also needs a larger p_x to estimate the privacy amplification part in Eq. (1). The improvement comes from the fact that p_x is less than 1/2. As p_x approaches to 1/2, the biased scheme becomes similar to the original scheme, where $p_x = p_z = 1/2$. It is an interesting prospective question how to apply our scheme to QKD systems with high channel losses[24].

For a practical QKD system, one needs to optimize the bias p_x for the key rate. The dependence of the optimal bias on the transmission loss is shown in Fig. 2, from which we can see that the optimal p_z is about 0.95 when the transmission loss is below 3 dB and decreases as the transmission loss increases. The minimal optimal p_z is about 0.6, which is close to 1/2. That is why our scheme approaches the standard BB84 with the vacuum + weak decoy-state scheme as the transmission loss increases.

Discussion

In conclusion, we combine the decoy-state QKD with a biased basis choice to enhance the system performance. The key point of our scheme is increasing the raw data sift factor by setting all signal states in one (Z) basis. We take statistical fluctuations into account and use a rigorous method to upper bound the phase error rate of the single-photon components of the signal state. Comparing the result with that in the standard decoy-state BB84 protocol, we find an improvement in

Table 2 | List of experimental parameters for simulation

N_{total}	f	e_d	Y_0
6×10^9	1.16	3.3%	1.7×10^{-6}

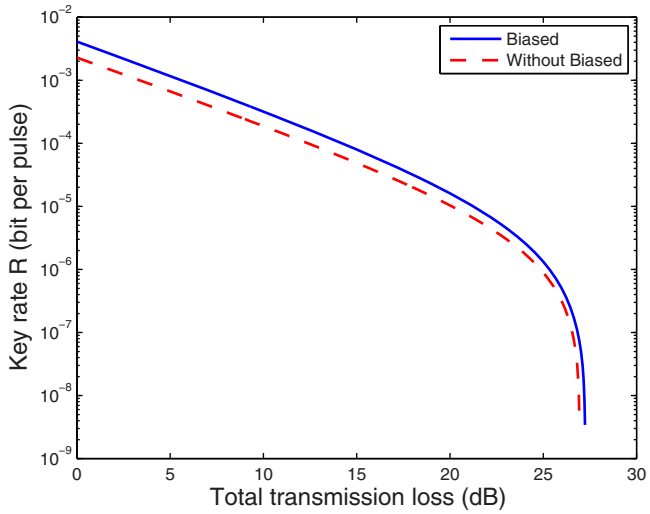

Figure 1 | Plot of key rate versus total transmittance. The solid line shows the result of our scheme and the red line shows the result of the standard BB84 with the vacuum + weak decoy-state method. The simulation parameters are shown in Table 2. The confidence interval for statistical fluctuation is 5 standard deviations (i.e., 1–5.73 × 10^{-7}). The expected photon number of signal state μ is 0.479. For each transmission loss, we optimize all the parameters, v, N_μ, N_v^z, N_v^x, N_0, p_z, and p_x.

the key generation rate. Meanwhile, we reduce the complexity of the QKD system by assigning all signal states in the Z basis.

Methods

Model. The weak coherent state source is equivalent to a photon-number channel model and its photon number follows a Poisson distribution[15]:

$$P(n)=\frac{\mu^n}{n!}e^{-\mu}. \tag{7}$$

Define Y_i as the yield of an i-photon state; η as the transmittance of the channel measured in dB; Y_0 as the background count rate. Then, in a normal channel when there is no Eve's intervention, Y_i is given by:

$$Y_i=1-(1-Y_0)(1-\eta)^i. \tag{8}$$

The gain of i-photon states Q_i is given by:

$$Q_i=Y_i\frac{\mu^i}{i!}e^{-\mu}. \tag{9}$$

The overall gain which means the probability for Bob to obtain a detection event in one pulse with intensity μ is:

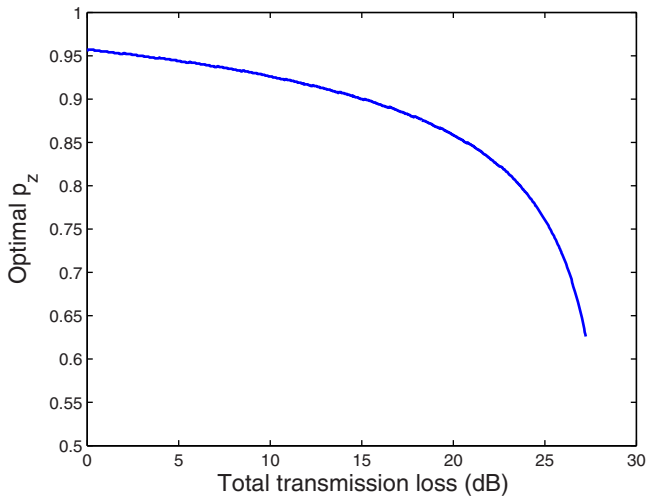

Figure 2 | Plot of optimal p_z versus transmission loss.

$$Q_\mu=\sum_{i=0}^{\infty}Q_i=\sum_{i=0}^{\infty}Y_i\frac{\mu^i}{i!}e^{-\mu}. \tag{10}$$

The error rate of i-photon states e_i is given by

$$e_iY_i=e_0Y_0+e_d\left[1-(1-\eta)^i\right](1-Y_0), \tag{11}$$

where e_d is the probability that a photon hits the erroneous detector and e_0 = 1/2. The overall QBER is given by

$$E_\mu Q_\mu=\sum_{i=0}^{\infty}e_iY_i\frac{\mu^i}{i!}e^{-\mu}. \tag{12}$$

Without Eve changing Y_i and e_i, the gain and QBER are given by

$$\begin{aligned}Q_\mu&=1-e^{-\eta\mu}(1-Y_0),\\ E_\mu Q_\mu&=e_0Y_0+e_d(1-e^{-\eta\mu})(1-Y_0)\end{aligned} \tag{13}$$

Upper bound of e_1^{pz}. Here, we review the random sampling argument[23]: using the bit error rate measured in the X basis, e_1^{bx}, to estimate the phase error rate in the Z basis, e_1^{pz}, for privacy amplification.

If the key size is infinite, we know that $e_1^{bx}=e_1^{pz}$. Otherwise, given e_1^{bx}, n_x (the number of decoy states that Alice sends and Bob measures in the X basis), and n_z (the number of signal states that Alice sends and Bob measures in the Z basis), we can give a probabilistic upper bound of e_1^{pz} such that it is lower than e_1^{pz} with a small probability $P_{\theta x}$

$$P_{\theta x}\equiv Pr\left\{e_{pz}\geq e_{bx}+\theta_x\right\}, \tag{14}$$

where θ_x is the deviation of the phase error rate from the tested value. Here, $P_{\theta x}$ is a controllable variable and is equal to 10^{-7} in the simulation. We have

$$P_{\theta x}<\frac{\sqrt{n_x+n_z}}{\sqrt{e_{bx}(1-e_{bx})n_xn_z}}2^{-(n_x+n_z)\xi_x(\theta_x)}, \tag{15}$$

where the function $\xi_x(\theta_x)$ is given by

$$\xi_x(\theta_x)\equiv H(e_{bx}+\theta_x-q_x\theta_x)-q_xH(e_{bx})-(1-q_x)H(e_{bx}+\theta_x), \tag{16}$$

and $q_x = n_x/(n_x + n_z)$. Given $P_{\theta x}$, we compute the value of ξ_x and find the value θ_x which is the root of equation (16). We get the probabilistic upper bound

$$e_1^{pzU}=e_{bx}+\theta_x. \tag{17}$$

Vacuum + weak decoy state. In this protocol, Alice and Bob use two decoy states to estimate the low bound of Y_1 and the upper bound of e_1. First, they implement a vacuum decoy state to estimate the background counts in signal states

$$\begin{aligned}Q_{vacuum}&=Y_0,\\ E_{vacuum}&=e_0=\frac{1}{2}.\end{aligned} \tag{18}$$

Secondly, they perform a weak decoy state where Alice uses a weaker intensity v ($v<\mu$) for the decoy state to estimate Y_1 and e_1. We have:

$$Y_1\geq Y_1^L=\frac{\mu}{\mu v-v^2}\left(Q_ve^v-Q_\mu e^\mu\frac{v^2}{\mu^2}-\frac{\mu^2-v^2}{\mu^2}Y_0\right), \tag{19}$$

and

$$e_1\leq e_1^U=\frac{E_vQ_ve^v-e_0Y_0}{Y_1^Lv}. \tag{20}$$

Note that in our scheme all the parameters for estimating Y_1^L are measured in the Z basis and the parameters for estimating e_1^U are measured in the X basis. And we must lower bound Y_0 to obtain the lower bound of the key rate[15]. The e_1^U we get here will substitute e_{bx} in equation (14).

Statistical fluctuation. Here, we consider statistical fluctuations for the decoy-sate method[15]. We need to modify the estimation of Y_1, equation (19), and e_1, equation (20).

The total number of pulses sent by Alice is composed of four cases

$$N_{total}=N_\mu+N_v^z+N_v^x+N_0. \tag{21}$$

Since that Alice sends all signal states in the Z basis and the final key is only extracted from the data measured in the Z basis, the parameter q in equation (1) is given by

$$q=\frac{N_\mu p_z}{N_{total}}. \tag{22}$$

We follow the statistical fluctuation analysis proposed by Ma *et al.*[25].

$$
\begin{aligned}
Q_{\mu}^{U} &= \hat{Q}_{\mu}\left(1+\frac{u_{\alpha}}{\sqrt{N_{\mu}p_{z}Q_{\mu}}}\right),\\
Q_{v}^{L} &= \hat{Q}_{v}\left(1-\frac{u_{\alpha}}{\sqrt{N_{v}^{z}p_{z}Q_{v}}}\right),\\
Y_{0}^{L} &= \hat{Y}_{0}\left(1-\frac{u_{\alpha}}{\sqrt{N_{0}Y_{0}}}\right),\\
Q_{0}^{L} &= Y_{0}^{L}e^{-\mu}\left(1-\frac{u_{\alpha}}{\sqrt{N_{0}Q_{0}}}\right),
\end{aligned}
\tag{23}
$$

where $\hat{Q}_{\mu}$, $\hat{Q}_{v}$ and $\hat{Y}_{0}$ are measurement outcomes which means that they are rates instead of probabilities. If we follow the standard error analysis assumption, u_{α} is the number of standard deviations one chooses for the statistical fluctuation analysis. Note that Q_{μ}^{U} and Q_{v}^{L} are used to estimate Y_{1}^{L}, so they should be measured in the Z basis. Here we use equation (14) to estimate the upper bound of e_{1}^{pz} with

$$
\begin{aligned}
n_{z} &= N_{\mu}p_{z}Y_{1}^{L}\mu e^{-\mu},\\
n_{x} &= N_{v}^{x}p_{x}Y_{1}^{L}ve^{-v}.
\end{aligned}
\tag{24}
$$

1. Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing,* 175–179 (IEEE Press, New York, 1984).
2. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
3. Mayers, D. Unconditional security in quantum cryptography. *Journal of the ACM (JACM)* **48**, 351–406 (2001).
4. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050 (1999).
5. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
6. Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72**, 012332 (2005).
7. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology* **18**, 133–165 (2005).
8. Erven, C., Ma, X., Laflamme, R. & Weihs, G. Entangled quantum key distribution with a biased basis choice. *New Journal of Physics* **11**, 045025 (2009)
9. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330–1333 (2000).
10. Lütkenhaus, N. & Jahma, M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics* **4**, 44.1–44.9 (2002).
11. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4**, 325 (2004).
12. Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
13. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
14. Wang, X.-B. Beating the *pns* attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
15. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
16. Zhao, Y., Qi, B., Ma, X., Lo, H.-K. & Qian, L. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.* **96**, 070502 (2006).
17. Zhao, Y., Qi, B., Ma, X., Lo, H.-K. & Qian, L. Simulation and implementation of decoy state quantum key distribution over 60 km telecom fiber. In *Proc. of IEEE ISIT,* 2094 (IEEE, 2006).
18. Rosenberg, D. *et al.* Long-distance decoy-state quantum key distribution in optical fiber. *Phys. Rev. Lett.* **98**, 010503 (2007).
19. Schmitt-Manderbach, T. *et al.* Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **98**, 010504 (2007).
20. Peng, C.-Z. *et al.* Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett.* **98**, 010505 (2007).
21. Lo, H.-K. Getting something out of nothing. *Quantum Inf. Comput.* **5**, 413–418 (2005).
22. Ma, X., Fung, C.-H. F., Boileau, J.-C. & Chau, H. Universally composable and customizable post-processing for practical quantum key distribution. *Computers & Security* **30**, 172–177 (2011).
23. Fung, C.-H. F., Ma, X. & Chau, H. F. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **81**, 012318 (2010).
24. Meyer-Scott, E. *et al.* How to implement decoy-state quantum key distribution for a satellite uplink with 50-db channel loss. *Phys. Rev. A* **84**, 062326 (2011).
25. Ma, X., Fung, C.-H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).

Acknowledgments

This work is supported by National Basic Research Program of China Grants No. 2011CBA00300 and No. 2011CBA00301, National Natural Science Foundation of China Grants No. 61073174, No. 61033001, No. 61061130540 and No. U1204602, the 1000 Youth Fellowship program in China, and National High-Tech Program of China Grant No. 2011AA010803.

Author contributions

Z.W., W.W., Z.Z., M.G., Z.M. and X.M. all contributed equally to this paper.

Additional information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Wei, Z.C. *et al.* Decoy-state quantum key distribution with biased basis choice. *Sci. Rep.* **3**, 2453; DOI:10.1038/srep02453 (2013).

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported license. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/3.0