7. R. A. Friedel, R. B. Anderson, *J. Am. Chem. Soc.* **72**, 1212–1215 (1950).
8. I. Puskas, R. S. Hurlbut, *Catal. Today* **84**, 99–109 (2003).
9. Supplementary materials are available on *Science* Online.
10. G. Yang, N. Tsubaki, J. Shamoto, Y. Yoneyama, Y. Zhang, *J. Am. Chem. Soc.* **132**, 8129–8136 (2010).
11. K. Fujimoto, H. Saima, H. O. Tominaga, *J. Catal.* **94**, 16–23 (1985).
12. Q. Ge, X. Li, H. Kaneko, K. Fujimoto, *J. Mol. Catal. Chem.* **278**, 215–219 (2007).
13. Y. Yu *et al.*, *React. Kinet. Mech. Catal.* **112**, 489–497 (2014).
14. J. Ereña, J. M. Arandes, J. Bilbao, A. T. Aguayo, H. I. de Lasa *Ind. Eng. Chem. Res.* **37**, 1211–1219 (1998).
15. P. Mohanty, K. K. Pant, J. Parikh, D. K. Sharma, *Fuel Process. Technol.* **92**, 600–608 (2011).
16. Y. Tamaura, M. Tahata, *Nature* **346**, 255–256 (1990).
17. G. Melaet *et al.*, *J. Am. Chem. Soc.* **136**, 2260–2263 (2014).
18. J. Xiao, T. Frauenheim, *J. Phys. Chem. Lett.* **3**, 2638–2642 (2012).
19. C. Jia *et al.*, *Phys. Chem. Chem. Phys.* **16**, 7538–7547 (2014).
20. F. Qi, *Proc. Combust. Inst.* **34**, 33–63 (2013).
21. J. D. Savee *et al.*, *Science* **347**, 643–646 (2015).
22. NIST Chemistry WebBook, http://webbook.nist.gov/chemistry/mw-ser.html.
23. T. A. Cool *et al.*, *J. Chem. Phys.* **119**, 8356–8365 (2003).
24. B. Yang *et al.*, *Int. J. Mass Spectrom.* **309**, 118–128 (2012).
25. D. Chen, K. Moljord, A. Holmen, *Micro. Meso.Mater.* **164**, 239–250 (2012).
26. J. Chanmugam, M. Burton, *J. Am. Chem. Soc.* **78**, 509–519 (1956).
27. Z. H. Zhang, Y. Zhang, J. B. Wang, *ACS Catal.* **1**, 1621–1630 (2011).
28. J. W. Williams, C. D. Hurd, *J. Org. Chem.* **5**, 122–125 (1940).



## ACKNOWLEDGMENTS

This work was financially supported by the National Natural Science Foundation of China (grant nos. 21425312, 21321002, and 91545204), the Ministry of Science and Technology of China (no. 2013CB933100), the "Strategic Priority Research Program" of the Chinese Academy of Sciences (grant XDA09030101), and Dalian Institute of Chemical Physics Fundamental Research Program for Clean Energy (DICP M201308). The Advanced Light Source is supported by the Director, Office of Science, Office of Basic Energy Sciences, of the U.S. Department of Energy under contract no. DE-AC02-05CH11231. A Chinese patent and an international patent application under the Patent Cooperation Treaty are pending.


## SUPPLEMENTARY MATERIALS

www.sciencemag.org/content/351/6277/1065/suppl/DC1
Materials and Methods
Figs. S1 to S18
Tables S1 to S4
References (*29*, *30*)

3 January 2016; accepted 22 January 2016
10.1126/science.aaf1835

QUANTUM COMPUTING

# Realization of a scalable Shor algorithm

**Thomas Monz,[1]* Daniel Nigg,[1] Esteban A. Martinez,[1] Matthias F. Brandl,[1] Philipp Schindler,[1] Richard Rines,[2] Shannon X. Wang,[2] Isaac L. Chuang,[2] Rainer Blatt[1,3]**

**Certain algorithms for quantum computers are able to outperform their classical counterparts. In 1994, Peter Shor came up with a quantum algorithm that calculates the prime factors of a large number vastly more efficiently than a classical computer. For general scalability of such algorithms, hardware, quantum error correction, and the algorithmic realization itself need to be extensible. Here we present the realization of a scalable Shor algorithm, as proposed by Kitaev. We factor the number 15 by effectively employing and controlling seven qubits and four "cache qubits" and by implementing generalized arithmetic operations, known as modular multipliers. This algorithm has been realized scalably within an ion-trap quantum computer and returns the correct factors with a confidence level exceeding 99%.**

Shor's algorithm for factoring integers (*1*) is one example in which a quantum computer (QC) outperforms the most efficient known classical algorithms. Experimentally, its implementation is highly demanding (*2*–*7*) because it requires both a sufficiently large quantum register and high-fidelity control. Such challenging requirements raise the question of whether optimizations and experimental shortcuts are possible. Optimizations, especially system-specific or architectural optimizations, are certainly possible, but for a demonstration of Shor's algorithm in a scalable manner, special care must be taken to not oversimplify the implementation—for instance, by employing knowledge about the solution before the actual experimental application (*8*).

How does Shor's algorithm work? First, we consider a classical factoring recipe, assuming that the number we want to factor is $N = 15$. We pick a random number $a \in [2, N-1]$ (the base)—say, $a = 7$. We evaluate whether the greatest common divisor $\gcd(a, N) = 1$; if not, a factor is already determined. This is the case for $a = \{3, 5, 6, 9, 10, 12\}$. Next, we calculate the modular exponentiation $a^x \bmod N$ for $x = 0, 1, 2\ldots$ and find its period $r$: the first value of $x > 0$ such that $a^x \bmod N = 1$. Given $r$, finding the factors of $N$ requires calculating the greatest common divisors of $a^{r/2} \pm 1$ and $N$, which is efficiently possible with a classical approach—for instance, using Euclid's algorithm. For our example ($N = 15$, $a = 7$), the modular exponentiation yields 1, 7, 4, 13, 1,..., which has a period of 4. The greatest common divisors of $a^{r/2} \pm 1 = 7^{4/2} \pm 1 = \{48, 50\}$ and $N = 15$ are $\{3, 5\}$, the nontrivial factors of $N$. In this example, the cases $a = \{4, 11, 14\}$ have period $r = 2$ and require a single multiplication step ($a^2 \bmod N = 1$), which is considered an "easy" case (*8*). Note that the periodicity for a chosen $a$ cannot be predicted.

How can this recipe be implemented in a QC? A QC also has to calculate $a^x \bmod N$ in a computational register for $x = 0, 1, 2\ldots$ and then extract $r$. Using the quantum Fourier transform (QFT) applied to the period register, the period of $a^x \bmod N$ can be extracted from a number of measurements not increasing with the size of the number to be factored.

What are the requirements and challenges of implementing Shor's algorithm? We first focus on the period register and subsequently address modular exponentiation in the computational register. Factoring $N$, an $n = \lceil \log_2(N) \rceil$-bit number (with the quantity in brackets rounded up to next integer number), requires a minimum of $n$ qubits in the computational register (to store the results of $a^x \bmod N$) and generally about $2n$ qubits in the period register (*9*, *10*). Thus, even a seemingly simple example, such as factoring 15 (an $n = 4$-bit number), requires $3n = 12$ qubits. These qubits then have to be manipulated with high-fidelity gate operations. Given the current state-of-the-art control over quantum systems (*11*), such an approach would probably yield an unsatisfactory performance. However, a full quantum implementation of this part of the algorithm is not necessary. As noted by Kitaev (*12*), if only the classical information of the QFT (such as the period $r$) is of interest, $2n$ qubits subject to a QFT can be replaced by a single qubit. Still, this approach requires qubit recycling (specifically, in-sequence single-qubit readout and state reinitialization) paired with feed-forward behavior to compensate for the reduced system size.

In the following, Kitaev's QFT will be referred to as $\mathrm{KQFT}^{(M)}$. It replaces a QFT acting on $M$ qubits with a semiclassical QFT acting repeatedly on a single qubit. Similar applications of Kitaev's approach to a semiclassical QFT in quantum algorithms have been investigated (*13*–*15*). For the implementation of Shor's algorithm, Kitaev's approach provides a reduction from the previous $n$ computational qubits and $2n$ QFT qubits (in total, $3n$ qubits) to only $n$ computational qubits and 1 $\mathrm{KQFT}^{(2n)}$ qubit (in total, $n + 1$ qubits).

The second key ingredient of Shor's algorithm—and a notably more challenging aspect than the QFT—is modular exponentiation, which admits the following general simplifications.

1) Considering Kitaev's approach (Fig. 1), the input state $|1\rangle$ (in decimal representation) is subject to a conditional multiplication based on the most significant bit $k$ of the period register. At most, there will be two results after this first step.

[1]Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria. [2]Center for Ultracold Atoms, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA. [3]Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Otto-Hittmair-Platz 1, A-6020 Innsbruck, Austria.
*Corresponding author. E-mail: thomas.monz@uibk.ac.at

It follows that, for the very first step, it is sufficient to implement an optimized operation that conditionally maps $|1\rangle \rightarrow |a^{2^k} \bmod N\rangle$. Considering the importance of a high-fidelity multiplication (with its performance being fed forward to all subsequent qubits), this efficient simplification improves the overall performance of experimental realizations.

2) Subsequent multipliers can similarly be replaced with maps by considering only possible outputs of the previous multiplications. However, using such maps will become intractable, as the number of input and output states to be considered grows exponentially with the number of steps: After $n$ steps, $2^n > N$ possible outcomes need to be considered, a numerical task as challenging as factoring $N$ by classical means. Thus, controlled full modular multipliers should be implemented. Figure 2 shows the experimentally obtained truth table for the modular multiplier 2 mod 15 [see also (*16*) for modular multipliers with bases {7, 8, 11, 13}]. These quantum circuits can be efficiently derived from classical procedures by using a variety of standard techniques for reversible quantum arithmetic and local logic optimization (*17*, *18*).

3) The very last multiplier allows one more simplification: Considering that the results of the modular exponentiation are not required for Shor's algorithm (as only the period encoded in the period register is of interest), the last multiplier only has to create the correct number of correlations between the period register and the computation register. Local operations after the conditional (entangling) operations may be discarded to facilitate the final multiplication without affecting the results of the implementation.

4) In rare cases, certain qubits are not subject to operations in the computation. Thus, these qubits can be removed from the algorithm entirely.

For large-scale quantum computation, optimization steps 1, 3, and 4 will only marginally affect the performance of the implementation. These steps represent merely a small subset of the entire computation, which mainly consists of the full modular multipliers. Thus, the realization of these modular multipliers is a core requirement for the implementations of a scalable Shor algorithm.

Furthermore, Kitaev's approach requires insequence measurements, qubit recycling to reset the measured qubit, feed-forward behavior of gate settings on the basis of previous measurement results, and controlled quantum operations—tasks that have not been realized in a combined experiment to date.

We demonstrate these techniques in our realization of Shor's algorithm in an ion-trap QC, with five $^{40}Ca^{+}$ ions in a linear Paul trap. The qubit is encoded in the ground state $S_{1/2}(m = -1/2) = |1\rangle$ and the metastable state $D_{5/2}(m = -1/2) = |0\rangle$ (where $m$ denotes the Zeeman sublevel) [for more details, see (*16*, *19*)]. Unitary operations, illustrated in Fig. 1, are decomposed into primitive components, such as two-target controlled-NOT (C-NOT) and C-SWAP gates (or gates with global symmetries, such as the four-target C-NOT gate employed

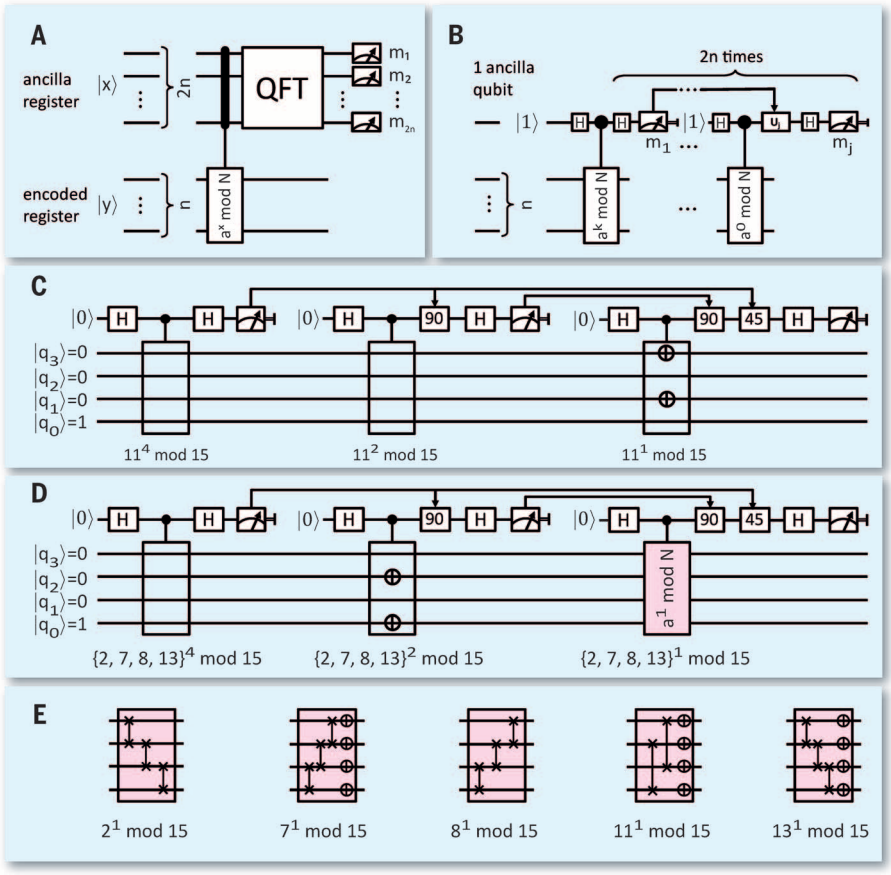


**Fig. 1. Quantum circuits.** Diagrams of Shor's algorithm for factoring $N = 15$, using a generic textbook approach (**A**) compared with Kitaev's approach (**B**) for a generic base $a$. (**C**) The actual implementation for factoring 15 to base 11, optimized for the corresponding single-input state. Here $q_i$ corresponds to the respective qubit in the computational register. (**D**) Kitaev's approach to Shor's algorithm for the bases {2, 7, 8, 13}. Here, the optimized map of the first multiplier is identical in all four cases, and the last multiplier is implemented with full modular multipliers, as depicted in (E). In all cases, the single QFT qubit is used three times, which, together with the four qubits in the computation register, totals seven effective qubits. (**E**) Circuit diagrams of the modular multipliers of the form $a$ mod $N$ for bases $a$ = {2, 7, 8, 11, 13}.

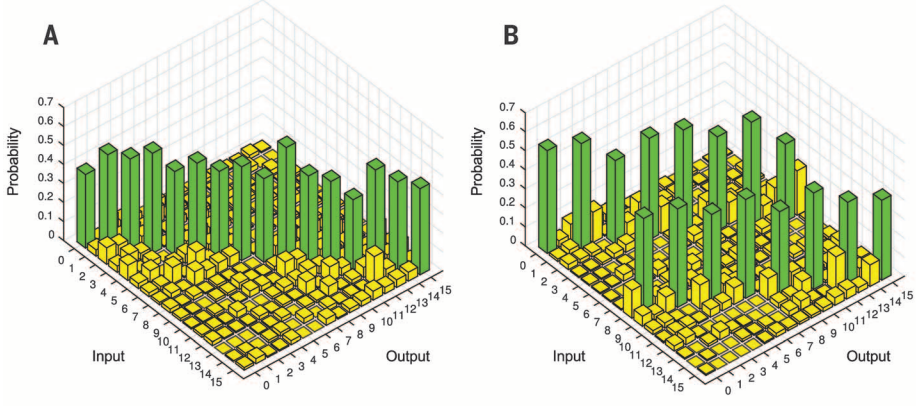


**Fig. 2. Truth table.** Experimentally obtained truth table of the controlled 2 mod 15 multiplier. (**A**) With the control-qubit being in state 0, the truth table corresponds to the identity operation. (**B**) When the control qubit triggers the multiplication, the truth table illustrates the multiplication of the input state with 2 mod 15. The mean fidelity with respect to the expected output state is 48(5)%.

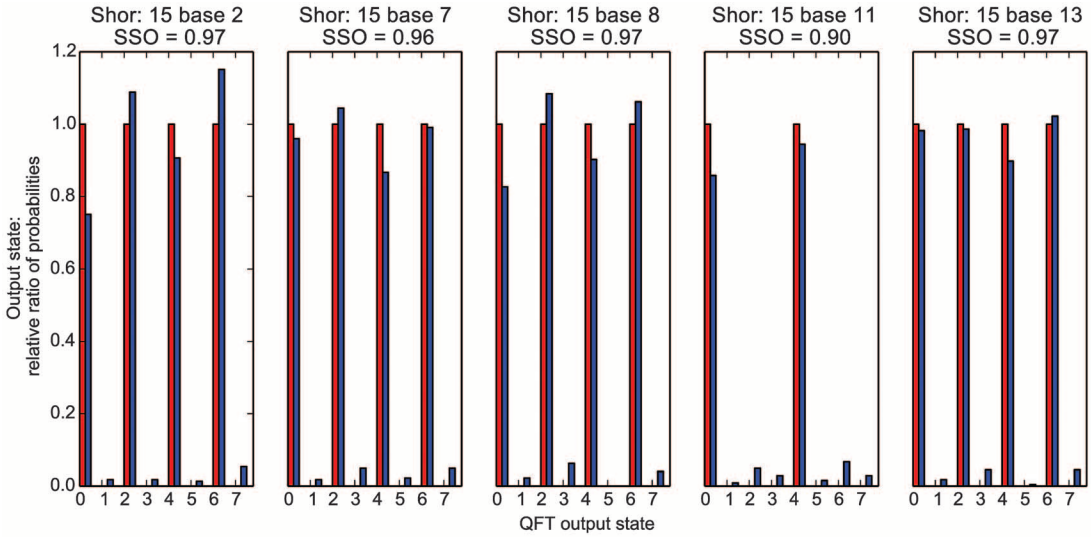


**Fig. 3. Experimental findings.** Results and correct order-assign probability for the different implementations to factor $N = 15$. Three-digit results (in decimal representation) of Shor's algorithm for the different bases. The ideal data (red) for period {2, 4} are shown adjacent to the raw data (blue). The squared statistical overlap is larger than 90% for all cases.

here), from which an adaptation of the gradient-ascent pulse engineering algorithm (*20*) can efficiently derive an equivalent sequence of laser pulses acting on only the relevant qubits. The problem with this approach is that the resulting sequence generally includes operations acting on all qubits. Implementing the optimized three-qubit operations for a five-ion string therefore requires decoupling the remaining qubits from the computation space. We spectroscopically decouple qubits by transferring any information from $|S\rangle$ to $|D'\rangle = D_{5/2}(m = -5/2)$ and from $|D\rangle$ to $|S'\rangle = S_{1/2}(m = 1/2)$. Here, the subspace $\{|S'\rangle, |D'\rangle\}$ serves as a readily available "quantum cache" to store and retrieve quantum information for the purpose of facilitating quantum computations.

Finally, to complete the toolbox necessary for Kitaev's approach to Shor's algorithm, we also implement (i) single-qubit readout, by encoding all other qubits in the $\{|D\rangle, |D'\rangle\}$ subspace and subsequent electron shelving (*21*) on the $S_{1/2} \leftrightarrow P_{1/2}$ transition; (ii) feed-forward behavior, by storing counts detected during the single-qubit readout (*22*) in a classical register and subsequent conditional laser pulses; and (iii) state reinitialization, using optical pumping for the ion, and Raman cooling (*23*, *24*) for the motional state of the ion string. The pulse sequences and additional information on the implementation of the modular multipliers are available in (*16*).

The measurement results for base $a = \{2, 7, 8, 11, 13\}$ with period $r = \{4, 4, 4, 2, 4\}$ are shown in Fig. 3. To quantify the performance of the implementation, previous realizations focused mainly on the squared statistical overlap (SSO) (*25*), the classical equivalent to the Uhlmann fidelity (*10*). Although we achieved an SSO of {0.968(1), 0.964(1), 0.966(1), 0.901(1), 0.972(1)} for the case of $a = \{2, 7, 8, 11, 13\}$, we argue that this does not answer the question "What is the period?" Shor's algorithm allows one to deduce the period with high probability from a single-shot measurement, as the output of the QFT ($x$) is, in the exact case, a ratio of integers, where the denominator gives the desired period. This period is extracted by using a continued fraction expansion applied to $x/2^k$, a good approximation of the ideal case when $k$, the number of qubits, is sufficiently large. In our realizations with bases $a = \{2, 7, 8, 11, 13\}$, the probabilities (and their error estimates in parentheses) to obtain output states that allow the derivation of the correct period are {56(2), 51(2), 54(2), 47(2), 50(2)}%. Thus, to obtain a confidence level of >99% for the periodicity, the experiment has to run about eight times.

We have presented the realization of Kitaev's vision of Shor's algorithm based on scalable building blocks with three-digit resolution to factor $N = 15$, using bases {2, 7, 8, 11, 13}. To do this, we successfully employed a semiclassical QFT combined with single-qubit readout, feed-forward behavior, and qubit recycling. Compared with the traditional algorithm, our realization of Shor's algorithm reduces the required number of qubits by nearly a factor of 3. Furthermore, the entire quantum register has been subject to the computation in a "black-box" fashion. Employing the equivalent of a quantum cache by spectroscopic decoupling facilitated the derivation of the necessary pulse sequences to achieve high-fidelity results. We envision that our scalable algorithm implementation will be combined with a scalable trap architecture (*26*) and quantum error correction to enable arbitrary long quantum computation.

## REFERENCES AND NOTES


1. P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, 1994), pp. 124–134.
2. A. Politi, J. C. F. Matthews, J. L. O'Brien, *Science* **325**, 1221 (2009).
3. E. Martín-López *et al.*, *Nat. Photonics* **6**, 773–776 (2012).
4. E. Lucero *et al.*, *Nat. Phys.* **8**, 719–723 (2012).
5. C. Y. Lu, D. E. Browne, T. Yang, J. W. Pan, *Phys. Rev. Lett.* **99**, 250504 (2007).
6. B. P. Lanyon *et al.*, *Phys. Rev. Lett.* **99**, 250505 (2007).
7. L. M. K. Vandersypen *et al.*, *Nature* **414**, 883–887 (2001).
8. J. A. Smolin, G. Smith, A. Vargo, *Nature* **499**, 163–165 (2013).
9. E. G. Rieffel, W. H. Polak, *Quantum Computing: A Gentle Introduction (Scientific and Engineering Computation)* (The MIT Press, ed. 1, 2011).
10. M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Series on Information and the Natural Sciences, Cambridge Univ. Press, ed. 1, 2004).
11. J. Stajic, *Science* **339**, 1163 (2013).
12. A. Y. Kitaev, http://arxiv.org/abs/quant-ph/9511026 (1995).
13. R. B. Griffiths, C. S. Niu, *Phys. Rev. Lett.* **76**, 3228–3231 (1996).
14. S. Parker, M. B. Plenio, *Phys. Rev. Lett.* **85**, 3049–3052 (2000).
15. M. Mosca, A. Ekert, in *Quantum Computing and Quantum Communications*, vol. 1509 of *Lecture Notes in Computer Science*, C. P. Williams, Ed. (Springer, 1999), pp. 174–188.
16. Supplementary materials are available on *Science* Online.
17. V. Vedral, A. Barenco, A. Ekert, *Phys. Rev. A* **54**, 147–153 (1996).
18. R. Van Meter, K. M. Itoh, *Phys. Rev. A* **71**, 052320 (2005).
19. P. Schindler *et al.*, *New J. Phys.* **15**, 123012 (2013).
20. V. Nebendahl, H. Häffner, C. F. Roos, *Phys. Rev. A* **79**, 012312 (2009).
21. H. Dehmelt, *Bull. Am. Phys. Soc.* **20**, 60 (1975).
22. M. Riebe *et al.*, *Nature* **429**, 734–737 (2004).
23. D. J. Wineland *et al.*, *J. Res. Natl. Inst. Stand. Technol.* **103**, 259 (1998).
24. I. Marzoli, J. I. Cirac, R. Blatt, P. Zoller, *Phys. Rev. A* **49**, 2771–2779 (1994).
25. J. Chiaverini *et al.*, *Science* **308**, 997–1000 (2005).
26. D. Kielpinski, C. Monroe, D. J. Wineland, *Nature* **417**, 709–711 (2002).


## ACKNOWLEDGMENTS


We acknowledge support from the Austrian Science Fund (FWF), through the SFB FoQus (FWF project no. F4002-N16); the European Commission (AQUTE), the NSF Interdisciplinary Quantum Information Science and Engineering (iQuISE) Integrative Graduate Education and Research Traineeship (IGERT); and the Institut für Quantenoptik und Quanteninformation. E.A.M. is a recipient of a DOC Fellowship of the Austrian Academy of Sciences. This research was funded by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), through Army Research Office grant W911NF-10-1-0284. All statements of fact, opinion, or conclusions contained herein are those of the authors and should not be construed as representing the official views or policies of IARPA, the ODNI, or the U.S. government. T.M., D.N., and P.S. developed the research, on the basis of theoretical ideas derived with R.R., S.X.W., and I.L.C; T.M., D.N., E.A.M., M.F.B., P.S., and S.X.W. performed the experiments; T.M. and D.N. analyzed the data; T.M., D.N., E.A.M., P.S., M.F.B., and R.B. contributed to the experiment; T.M., D.N., R.R., M.F.B., I.L.C., and R.B. wrote the manuscript; and all authors contributed to discussions about the results and the manuscript. We declare no competing financial interests.


## SUPPLEMENTARY MATERIALS

www.sciencemag.org/content/351/6277/1068/suppl/DC1
Supplementary Text
Figs. S1 and S2
Tables S1 and S2
References (*27*, *28*)


25 November 2015; accepted 1 February 2016
10.1126/science.aad9480

Science

# Realization of a scalable Shor algorithm

Thomas Monz, Daniel Nigg, Esteban A. Martinez, Matthias F. Brandl, Philipp Schindler, Richard Rines, Shannon X. Wang, Isaac L. Chuang and Rainer Blatt

*Science* **351** (6277), 1068-1070.
DOI: 10.1126/science.aad9480

**Reducing quantum overhead**

A quantum computer is expected to outperform its classical counterpart in certain tasks. One such task is the factorization of large integers, the technology that underpins the security of bank cards and online privacy. Using a small-scale quantum computer comprising five trapped calcium ions, Monz *et al.* implement a scalable version of Shor's factorization algorithm. With the function of ions being recycled and the architecture scalable, the process is more efficient than previous implementations. The approach thus provides the potential for designing a powerful quantum computer, but with fewer resources.

*Science*, this issue p. 1068