Best of both worlds

Citation for published version:
Diamanti, E & Kashefi, E 2017, 'Best of both worlds' Nature Physics, vol. 13, no. 3-4, pp. 3-4. DOI:
10.1038/nphys3972

Digital Object Identifier (DOI):
10.1038/nphys3972

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Nature Physics

Best of both worlds

Eleni Diamanti and Elham Kashefi

Secure communication is emerging as a significant challenge for our hyper-connected data-dependent society. The answer may lie in a clever combination of quantum and classical cryptographic techniques.

Edward Snowden's revelations on the mass surveillance practices in the US and UK brought to the forefront the issues of privacy and security of data and communications. In an increasingly connected world, the words 'big data' and 'cloud technologies' have left the vocabulary of technology experts to reach mainstream culture and become the very centre of the emerging digital transformation of services and applications. Ensuring privacy and security is now an imperative. At the same time, it poses a formidable challenge — one that may be best served by a hybrid quantum and classical approach.

Indeed, addressing this challenge in the coming years will undoubtedly require pushing the boundaries of current cryptographic techniques, which typically rely on the difficulty of certain mathematical operations, to include techniques enabled by the fundamental laws of quantum physics. Well-established quantum algorithms and protocols allow, for example, for exponentially faster factorization, or the distribution of secret keys with unconditional security — impossible tasks using only classical resources.

The far-reaching potential of quantum technologies has led the NSA and NIST to initiate a transition to quantum-resistant cryptographic algorithms. Google and Microsoft have launched dedicated laboratories for studying applications of quantum computing to machine learning and other fields. And IBM has made the use of its quantum platform freely accessible in a cloud network setting. Major efforts are also underway in the EU with a continent-scale investment, and in China with the development of a 2,000 km quantum network — the common vision being to accelerate innovation and technology transfer. But what do these rapid developments mean for new cryptography functionalities that use the best of the classical and quantum worlds?

Classical progress

Let's start on the classical side. With ever-increasing numbers of miniature computing mobile devices and powerful central servers, the traditional view of cryptography as the art of passing secret messages from point to point has evolved to secure outsourced data processing. Can we compute with encrypted data without decrypting them first? This is the key concept behind modern cryptography protocols leading to functionalities such as multiparty secure computation, delegated computing, verification of outsourced data manipulation and differential privacy in emerging platforms such as cloud services.

© TOMASZ ZAJDA / ALAMY STOCK PHOTO

The stack of protocols for basic functionalities, such as public and symmetric encryption, message passing and authentication, are already running as the building blocks of the Internet. However, these new functionalities are still under development. And although the race is on between all the information and communication technology stakeholders, and progress is being made with significant speed, practical solutions compatible with fast, day-to-day processing of big data still remain a challenge.

Moreover, should advances in quantum technologies succeed in building powerful devices capable of breaking the computational assumptions behind these classical protocols, both traditional and modern protocols would be under the threat of a security breach. For example, Shor's quantum factoring algorithm would compromise the widely used RSA scheme[1]. In response to this threat, the field of post-quantum cryptography has emerged in recent years. The aim is to develop cryptographic primitives that remain secure even against quantum computers, by exploiting properties of error-correcting codes or lattice-based hard problems[2]. This line of research has put forward a new trade-off between the desired level of security and the required efficiency for practical purposes currently explored by Google's New Hope scheme in Chrome. But while cryptographers search for new computational assumptions that provide resistance to quantum attacks, crypto-analysts are busy finding new quantum trickery to break them down[3]. This in turn leads to the need for more complex protocols and hence to even more challenges for practical solutions.

Quantum developments

Quantum key distribution (QKD) — the quantum cryptographic scheme that enables unconditionally secure message exchange — is arguably a milestone in the quantum information field. QKD promises future-proof security: it is resilient against future technological developments that may threaten the integrity of the secret information, including powerful quantum devices, and has seen tremendous developments in recent years. The quantum cryptography toolbox, however, is much broader[4]. It includes protocols in various security models and settings with respect to user trust, device complexity and power, for which a rigorous quantum advantage can be shown in practice.

In parallel, although a universal quantum computer may still be some decades in the future, it is now possible to prepare, manipulate and precisely control systems involving a few quantum information bits (qubits) encoded in systems such as superconducting circuits, cold atoms, ions, photons, and nitrogen–vacancy centres in diamond. The first elements of universal quantum computations and quantum error correction have been demonstrated in these systems, as well as the nonlocal character of quantum mechanics, which opens the door to so-called device-independent implementations — free from security threats due to practical imperfections.

The main challenge now is to move towards large-scale systems and networks, where the true disruptive potential of quantum technologies can be shown. This requires the development of practical, scalable resources as building blocks and of adapted multiparty communication and distributed computation protocols performed between (potentially malicious) clients and servers. As an example, blind quantum computing opens the way to the verification of a complex computation performed by an assumed quantum, all powerful, untrusted server by clients equipped with only limited resources[5,6].

With the current rate of progress in quantum technologies, we can clearly foresee the first 50-qubit systems appearing within the next decade. However, despite this progress, the concrete applications of quantum cryptography still occupy a niche in practical information and communication technologies, and the demonstration of the full extent of the quantum superiority in a large-scale system or network is extremely challenging due to the high cost of the associated error correction schemes. While recent breakthroughs in the design of new codes[7,8] are a promising route to overcome this apparent bottleneck, we could, in the meantime, explore the noisy qubits directly to enhance classical schemes.

Going hybrid

In order to do so, we believe in adopting a vision that combines the advantages of classical and quantum algorithms and technologies. The first step is to realize that we need both: the classical world offers solid mathematical foundations and easiness of implementation based on widely deployed infrastructures. The quantum world provides the means to enhance the security and efficiency of cryptographic techniques to render them unbreakable by future technologies. At this point, we are able to verify, certify and program today's small quantum devices so that we can effectively exploit tomorrow's scalable machines.

A concrete platform illustrating how this can be put into place is the evolution towards a hybrid quantum-safe infrastructure. And we are already seeing various threads of such developments in the field. One straightforward hybrid approach involves employing a quantum cryptography protocol such as QKD as a subroutine within classical infrastructures, as was demonstrated in the Swiss elections in 2007. In doing so, the eventual success is dictated by a detailed performance analysis, taking into account the realistic cost of the required quantum hardware versus the obtained added value. This issue of the price of trust is even more critical when the added quantum primitives do not necessarily provide unconditional security, but only better than classical, as is the case for quantum bit commitment[9], coin flipping[10,11] and digital signatures[12,13].

Recently the opposite direction has also been proposed, in which classical primitives such as one-time memory, secure multiparty computing, or fully homomorphic encryption are put in use to obtain new quantum functionalities[14–16]. These new protocols will be needed in a not-too-distant future where quantum servers will provide computing services along with classical devices in a distributed network with potentially malicious parties in place. More broadly, the development of quantum functionalities such as multiparty quantum computation and secret sharing[17,18] is desirable.

A less conventional hybrid scheme has been also explored in recent years, which combines elements of classical computing (such as linear functions) with minimal quantum effects (like contextuality) to derive a new computing platform[19] that may also provide better-than-classical security in specific scenarios[20,21].

Exploring a framework where the aforementioned quantum and classical primitives can be securely combined is one of the key challenges upon which researchers from both classical and quantum domains have recently embarked[22,23]. Taking into account realistic implementation constrains such as bounded or noisy storage[24,25] and relativistic constrains[26,27] is another promising route towards obtaining practical solutions implementable with currently available quantum technology.

The roadmap to obtaining a realistic hybrid quantum–classical secure computing and communication platform is clear. First, we need to develop classical protocols for multiparty computing, verification and delegation that are secure against quantum attacks. In doing so, we need to establish the efficiency and security bottlenecks associated with these novel post-quantum functionalities. The next challenge is to design quantum subroutine protocols for these bottlenecks within the classical schemes. And finally, we need to develop purpose-built devices implementing these quantum protocols and taking into account low-cost and flexibility criteria amenable to an ultimate industrial exploitation. Stay tuned for configurable quantum USB keys. ❐

Eleni Diamanti and Elham Kashefi are at CNRS, Université Pierre et Marie Curie, 75005 Paris, France. E.K. is also at the University of Edinburgh, Edinburgh EH8 9AB, UK.
e-mail: eleni.diamanti@upmc.fr; ekashefi@inf.ed.ac.uk

References

1. Rivest, R., Shamir, A. & Adleman, L. *Commun. ACM* **21,** 120–126 (1978).
2. Chen, L. *et al. Report on Post-Quantum Cryptography* (NIST, US Department of Commerce, 2016); http://go.nature.com/2gY56xB
3. Kaplan, M., Leurent, G., Leverrier, A. & Naya-Plasencia, M. In *Advances in Cryptology – CRYPTO 2016* 207–237 (Springer, 2016).
4. Broadbent, A. & Schaffner, C. *Design. Code. Cryptogr.* **78,** 351–382 (2016).
5. Broadbent A., Fitzsimons, J. & Kashefi, E. In *Proc. 50th Annual IEEE Symp. on Foundations of Computer Science*, 517–526 (IEEE, 2009).
6. Barz, S., Fitzsimons, J. F., Kashefi, E. & Walther, P. *Nat. Phys.* **9,** 727–731 (2013).
7. Gottesman, D. *Quant. Inf. Comp.* **14,** 1338–1371 (2014).
8. Leverrier, A., Tillich, J.-P. & Zémor, G. In *Proc. 56th Annual IEEE Symp. on Foundations of Computer Science* 810–824 (IEEE, 2015).
9. Konig, R., Wehner, S., & Wullschleger, J. *IEEE Trans. Inf. Theory* **58,** 1962–1984 (2012).
10. Berlín, G. *et al. Nat. Commun.* **2,** 561 (2011).
11. Pappa, A. *et al. Nat. Commun.* **5,** 3717 (2014).
12. Gottesman, D. & Chuang, I. Preprint at https://arxiv.org/abs/quant-ph/0105032 (2001).
13. Donaldson, R. J. *et al. Phys. Rev. A* **93,** 012329 (2016).
14. Broadbent, A., Gutoski, G. & Stebila, D. In *Advances in Cryptology – CRYPTO 2013* 344–360 (Springer, 2013).
15. Dupuis, F., Nielsen, J. B. & Salvail, L. In *Advances in Cryptology – CRYPTO 2012* 794–811 (Springer, 2012).
16. Dulek, Y., Schaffner, C. & Speelman, F. In *Advances in Cryptology – CRYPTO 2016* 3–32 (Springer, 2016).
17. Ben-Or, M., Crépeau, C., Gottesman, D., Hassidim, A. & Smith, A. In *Proc. 47th Annual IEEE Symp. on Foundations of Computer Science* 249–260 (2006).
18. Bell, B. A. *et al. Nat. Commun.* **5,** 5480 (2014).
19. Anders, J. & Browne, D. E. *Phys. Rev. Lett.* **102,** 050502 (2009).
20. Dunjko, V., Kapourniotis, T. & Kashefi, E. *Quant. Inf. Comput.* **16,** 61–86 (2016).
21. Loukopoulos, K. & Browne, D. E. *Phys. Rev. A* **81,** 062336 (2010).
22. Hallgren, S., Smith, A. & Song, F. In *Advances in Cryptology – CRYPTO 2011* 411–428 (Springer, 2011).
23. Unruh, D. In *Advances in Cryptology – CRYPTO 2013* 380–397 (2013).
24. Damgård, I. B., Fehr, S., Salvail, L. & Schaffner, C. *SIAM J. Comput.* **37,** 1865–1890 (2008).
25. Wehner, S., Schaffner, C. & Terhal, B. M. *Phys. Rev. Lett.* **100,** 220502 (2008).
26. Kent, A. *Phys. Rev. Lett.* **83,** 1447–1450 (1999).
27. Chakraborty, K., Chailloux, A. & Leverrier, A. *Phys. Rev. Lett.* **115,** 205501 (2015).