Futures 72 (2015) 17–26

Contents lists available at ScienceDirect

Futures

journal homepage: www.elsevier.com/locate/futures

Global catastrophic risk and security implications of quantum computers

Andy Majot *, Roman Yampolskiy

Computer Engineering and Computer Science, University of Louisville, Louisville, KY, USA

ARTICLE INFO

Article history:
Received 7 August 2014
Received in revised form 22 February 2015
Accepted 25 February 2015
Available online 13 April 2015

Keywords:
Quantum computing
Cryptography
Global catastrophic risk
Post-quantum
RSA
ECC

ABSTRACT

With advancements in quantum computing happening almost weekly it is time to examine the effects this new technology will have on society and current computational systems. Specifically, cryptographic systems need to be carefully analyzed since the introduction of quantum computational resources would render discrete logarithm and factoring based cryptographic systems like those based on Rivest, Shamir, Adleman (RSA) and Elliptic Curve Cryptography (ECC) algorithms woefully obsolete. These algorithms are widely used in the form of digital certificates, message encryption, and even physical authentication devices like Radio Frequency Identification (RFID) badges. With this technology compromised by quantum computing, governments and other organizations would be able to eavesdrop on private citizens with relative ease. This has the potential to cause a slew of rights violations and atrocities leading to catastrophe. With compromised digital certificates 3rd parties could masquerade as trusted organizations. This would call many types of digital transactions like into question, including those related to stock exchanges, personal banking, and software verification. By eroding this previously solid foundation of trust global scale economic catastrophes are not out of the question. This paper introduces quantum computing to the study of catastrophic threats since the use of quantum technology while existing vulnerable encryption schemes are still in place raises severe safety issues. These issues are addressed here along with a proposed two-fold solution involving the development and maturation of post-quantum cryptographic algorithms coupled with government and international regulation. This regulation would promote the containment and responsible use of quantum computers in order to help alleviate some of the security issues posed by outdated cryptographic systems in a post-quantum environment.

1. Introduction

The world is inching toward the day when full-fledged quantum computing becomes a reality, changing the way society thinks about computational problems and their solutions. Researchers in labs across the world are spinning and entangling electrons in experiments that bring us closer to all of the incredible benefits of quantum computing. These benefits include an advanced computing platform capable of implementing an inherently secure cryptographic communication scheme and making possible more advanced artificial intelligence (Miakisz, Piotrowski, & Sładkowski, 2006). The current state of the

* Corresponding author at: 316 Helbig St., Sellersburg, IN 47172, USA. Tel.: +1 502 930 9742.
E-mail addresses: ammajo01@louisville.edu, amajot@gmail.com (A. Majot), roman.yampolskiy@louisville.edu (R. Yampolskiy).

http://dx.doi.org/10.1016/j.futures.2015.02.006
0016-3287/

quantum computing field is briefly examined in this paper and, as the reader will see, current estimates show useful quantum computing is still several years away.

It does not take a large imagination to realize that the introduction of this quantum technology into the world will revolutionize many aspects of technology and society. One facet of modern technology, that of cryptographic systems, will be particularly affected by the start of the quantum computing era. The public key based cryptographic algorithms and Elliptic Curve Cryptography (ECC) certificate protocols behind many currently used cryptographic schemes can be broken using quantum computations. These schemes are heavily entrenched in everyday use, from online certificates to encrypted email and Virtual Private Network (VPN) connections (Bernstein, Buchmann, & Dahmén, 2009).

Without heavy restructuring of critical cryptographic infrastructure in advance of the quantum computing era, there may be severe safety dilemmas that arise from the use of quantum computers by those who have access to them in opposition of those who do not. This duality has the potential to cause an extreme imbalance of power and tip the scales more in the direction of a global catastrophe. Quantum computing could make wide spread surveillance systems like the US's National Security Administration (NSA) PRISM program look like an afterthought due to the ability of 3rd parties to intercept encrypted communications much faster and incredibly more efficiently than would otherwise be possible. Depending on who or what the 3rd party is, this could lead to a plethora of rights violations, suppression of dissent, sabotage, and targeted arrests or killings. Security certificates, the backbone of trust for most digital transactions would also be rendered meaningless by this technology. Attackers could masquerade as legitimate companies or banking institutions by using these compromised certificates, causing massive fraud and disruption in the global markets. Entire economies could end up in the dust bin after consumers and governments lose trust in previously reliable pillars of the global economy. By spoofing software certificates it would also be possible for attackers to install spyware on computers by slipping it in during software and operating system updates. This would give an open tap of information for any organization to use if they were looking to suppress dissent or direct sabotage.

These catastrophic threats need to be examined and avoided at all costs, which is why the authors have brought the previously absent subject of quantum computing into the discussion of global catastrophic threats. We raise some important questions, and pose potential solutions in advance of the oncoming quantum-based computing paradigm shift that could lead us to a global catastrophe.

2. Current state of quantum computing

How far away is the world from a functional and useful quantum computer? According to the claims of one Canadian company, the era of limited quantum computing is already here. D-Wave Systems announced the D-Wave One in May of 2011, which was touted as the first commercially available quantum computer and had 128 qubits of quantum processing power (Simonite, 2012; Anthony, 2011). Not long after the announcement of this quantum computer a major US defense contracting firm named Lockheed Martin signed a deal with D-Wave to purchase one of these machines (Systems, 2014a). Two years later in 2013 D-Wave began selling the next production ready quantum computer, the D-Wave Two, which featured a 512 qubit processor (Systems, 2014b). In the first half of 2015 they are scheduled to ship the next generation machine, which will feature 2048 qbits (Rose, 2014).

Several big names bought into the D-Wave Two including Google, NASA, and again, Lockheed Martin (Systems, 2014a). There has been some criticism of D-Wave in the past, and doubts as to whether or not they were truly selling a quantum computer (Aaronson & Desultory, 2008; Guizzo, 2010). These doubts have mostly been answered with the release of the D-Wave Two system, but there are still those who would like to see much better performance out of a quantum computing system before making up their minds. It should be noted that D-Wave machines are not general-purpose, and that ordinary computers will still be able to outperform them at many tasks (Guizzo, 2010). For the ideal version of a general purpose quantum computer, scientists estimate that they are still at least 10 years away from a workable quantum processor (Quantum, 2012; Heger, 2009). This 10 year figure is important because of the amount of time it takes to rework global IT infrastructure to meet new paradigms. One example is the conversion from IP V4 to IP V6, which is still ongoing and has been in progress for years due to its difficulty (Czyz et al., 2013).

Other than D-Wave, who else is looking at the quantum computer problem? Unsurprisingly, this technology seems to have sparked the interest of the intelligence branches of the US government. As revealed in the documents leaked by Edward Snowden about NSA surveillance, the US government is actively looking at acquiring a quantum computer for the purposes of intelligence gathering (Berghel, 2013; Rich & Gellman, 2014). Given what the NSA managed to accomplish with only traditional computers, it does not take much thinking to imagine what they would be able to accomplish with a full-fledged quantum computer.

The problem of Artificial Intelligence (AI) is also actively being investigated with quantum computers. Google and NASA partnered up to purchase a D-Wave Two computer, which passed all of the benchmarks and requirements they gave it. This success lead Google to announce that it will invest its resources to create a quantum computer of its own (Simonite, 2014a). Not to be outdone, Microsoft is also looking at quantum computing using a different type of processor than D-Wave and Google (Simonite, 2014b).

3. Technologies and concerns

While there are many examples of cryptographic technologies that are seemingly unaffected by quantum algorithms, the ones that are compromised by them are in widespread use and currently entrenched in various communications schemes