ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 2, Issue 10, October 2013

Quantum Secure Digital Signature, Cryptography and Post Quantum Certificates

A. K. Agarwal

Department of Physics, Government College, Nasirabad, India

ABSTRACT: Quantum digital signature (QDS) is based on the laws of quantum physics, and can provide unconditional security for signing messages between remote multi-party users. To date, different QDS protocols have been proposed and corresponding security analysis has been done. Just most security analyses are directed against signing single-bit messages, and the security cannot be ensured when signing multi-bit messages if one simply puts blocks together. Recently, T.Y. Wang et al. analyzed the security under this situation and gave a solution for eliminating potential eavesdropping attacks. However, its efficiency is relatively low since they need to consume more than 2n-bit signatures to sign a classical n-bit message. In this paper, we propose a high efficient approach for signing multi-bit messages. As a result, the efficiency can be improved with 36.92% when signing a 128-bit message.

Like many modern systems, the security of electronic passports and other electronic travel documents relies on public key cryptography. Whilst there are a number of very well-accepted and widely used public key schemes, the advent of large-scale, general-purpose, quantum computing will radically change the situation. Quantum computers are built upon quantum mechanical phenomena, and can solve mathematical problems that classical computers cannot. Over the past few years, much effort has been devoted to building such a device, although experts in the field suggest that it will be one or two decades before large scale quantum computers are a reality. In the post-quantum era, the currently used asymmetric cryptographic techniques, i.e. integer factorization based schemes and discrete logarithm-based schemes will be susceptible to being broken .This threatens the security of a wide range of systems, including the authenticity of electronic travel documents (the main focus of this paper). The recent effort has been devoted to developing post-quantum cryptographic schemes, i.e. schemes secure against attack using both quantum and classical computers. In parallel with this research effort, a number of major standardisation bodies have inaugurated projects to develop standards for post-quantum algorithms. Perhaps the most important of these is the competition led by the National Institute of Standards and Technology (NIST) . So far, from an initial 82 submissions, after Round 2 of this competition only 26 schemes remain in the running for adoption . Besides providing a portofolio of cryptographic algorithms resilient to quantum computers, this process of standardisation also aims to ensure that they are practical and can interoperate with current applications and protocols based on asymmetric cryptography. For example, post-quantum X.509 certificates are viable for TLS-like communication protocols for use in a "post-quantum Internet". X.509 certificates are also commonly used to protect the authenticity and integrity of data inside electronic travel documents, namely the owner's data.

KEYWORDS: quantum, post quantum, digital, secret, signature, certificates, documents

I. INTRODUCTION

One of the main goals of cryptography is to allow an authorized party, typically holding a secret key, to perform an action which an unauthorized party (without the key) cannot. For example, in a digital signature scheme, the authorized party, Alice, holds a secret key that allows her to create digital signatures that will be accepted by a public verification algorithm. Anyone without Alice's key cannot forge her signature. Classically, Bob either knows the secret key or doesn't, and there is no way to control how many times the key is used. But with quantum mechanics, the situation is different: the no cloning theorem [1] allows us to create secrets that cannot be copied. Consequently, we propose the design of cryptographic schemes with two levels of secrets: one classical "master" secret, which is used only to generate any number of unclonable quantum "tokens", each of which can be used to perform one action, and is consumed in the process due to destructive effects of quantum measurements. If Alice holds the secret key, she can delegate authorization to Bob by granting him a limited number of quantum tokens.[2]

Digital signature is a cryptographic primitive which is arguably second in importance only to encryption. A digital signature scheme [2] consists of three Probabilistic Polynomial Time (PPT) algorithms: key-gen, sign, and verify. The first algorithm outputs a secret key sk and a public key pk. The signer can use sk to sign a document α by calling sign (sk, α). This produces a signature sig, which can be verified by anyone holding the public key by calling verify (pk, α, sig). We will denote the keys as subscripts, so these calls are sign $sk(\alpha)$ and verify $pk(\alpha, sig)$. The verify algorithm

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 2, Issue 10, October 2013

returns either “accept” or “reject”. A valid signature should be accepted, so verify pk(α,signsk(α)) should accept for all α. Informally, a digital signature scheme is secure if an adversary which can ask for signed documents, cannot efficiently forge any new signed document.[3]

Here are two motivating examples.

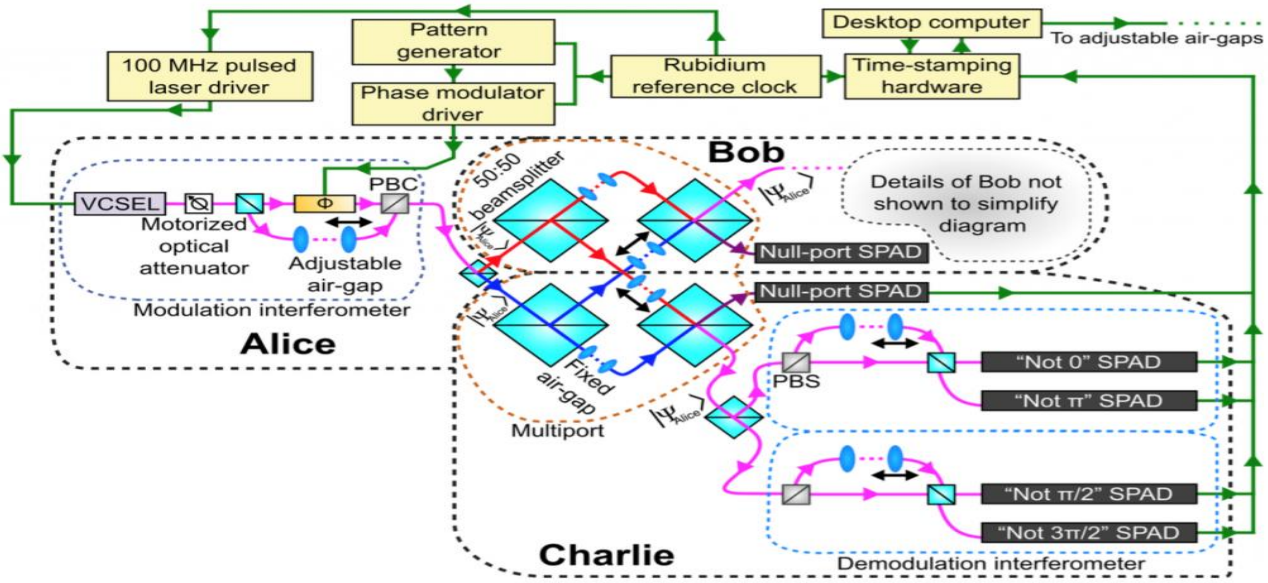
(i) A manager wants to hedge the embezzlement risks that an accountant introduces. This can be achieved by agreeing with the bank that any signed wire is limited to $1000. Then, the manager can grant the accountant a number of tokens according to the level of her trust in the accountant.

(ii) Online computers are more prone to hacks than offline computers. A system administrator can hold the secret keys on an offline computer, and generate signing tokens to be used on the online computer. The hacker who steals n signing tokens can sign at most n documents, whereas a stolen secret key can be used to sign any number of documents. Tokenized signatures have several other useful properties. A Tokenized signature scheme can be used as a digital signature scheme. Every tokenized digital scheme is also revocable: the signer can destroy a token in a publicly-verifiable way. Our construction has an even stronger notion of revocability, testability, which allows testing the signing token without consuming it.[4]

One of the functions of money is store of value. From an engineering perspective, this makes quantum money (which our construction is based on) a challenging task, as it requires a long term quantum memory to store the quantum money. Signing tokens do not necessarily need to be stored for long periods (perhaps, only the signed documents are), and therefore some applications may require relatively short term memory, and will thus be easier to implement in practice. Furthermore, signing requires a very simple (depth 1) quantum circuit, and verification is done on a classical computer. Our tokens can be generated using Clifford circuits, which do not require a universal quantum computer, and therefore may be easier to implement. The only task which requires a universal quantum computer is verify-token. The security of the weak scheme is exponential in the number of qubits; this means, among other things, that the depth of token-gen in all our schemes is only super-logarithmic (in the security parameter)[5]

II. OBSERVATIONS

Digital signatures attempt to guarantee the validity of internet transactions. Their security rests on the mathematical difficulty of factorising large numbers into primes. This difficulty cannot be proved, so there is a possible flaw in all current schemes. Quantum digital signatures have security guaranteed by the laws of physics. We have developed test systems that run digital signature protocols in laboratory situations [6] and are exploring moving these towards trials in fibre networks. The diagram shows a digital signature system based on unambiguous quantum state elimination.



We show that a testable tokenized signature scheme can be used as quantum money[5, 6, 7, 8, 9, 3, 10, 11, 12]. Interestingly, the quantum money scheme we get this way has a combination of desirable properties that no previous scheme had, not even the Aaronson-Christiano scheme on which our construction is based. To get a quantum money scheme from a testable tokenized signature scheme, simply use the signing tokens as money. An interesting property of this scheme is that the money can be converted into a verifiable signature for a document. This can be used to send the money over a classical channel (vis-`a-vis “standard” quantum money, which can only be sent via a quantum channel).

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 2, Issue 10, October 2013

In particular, suppose Alice wants to send money to Bob, but she is stranded and cannot get quantum internet reception on her quantum cellphone. With our scheme, Alice can use her money as a signing token to sign the document "I'm sending this money, with the serial number 03217, to Bob". Bob can then take the signed document and present it to his bank. The bank knows that Alice must have burned her money to produce the signed document, and so it can safely issue Bob a new money state. In essence, Alice can convert a quantum coin into a classical check. We discuss other advantages of this schemes related to fraud and other attack vectors. [7]

III. DISCUSSION

Today no quantum computer can run quantum algorithms, but once it does, a multitude of public key-based protocols including TLS / SSL, IPSEC, SSH, Internet of Things (IoT), digital signing and code signing will become vulnerable to eavesdropping and public disclosure as they are not strong enough to resist a quantum attack. No one has a concrete date as to when we will hit the post-quantum era, but there are strong indicators that it will start somewhere between 2023 and 2030. [8] If these dates are in fact true, then in some cases, it might already be too late. For example:

- Root Certificate Authorities (CAs) – are valid from 2028 to 2038 which is well beyond when quantum computing will arrive
- Data Retention Requirements – an enterprise that stores and keeps data safe for a determined period of time for compliance or business reasons must take into account the post-quantum era as it may only be 4 years away
- Code Signing Certificates - most will expire in 2021, but any data you transferred over TLS will be potentially decryptable with perfect forward secrecy
- Document Signing Solutions – anything signed now will not have integrity in the post-quantum era [9]

IV. CONCLUSION

Post-quantum X.509 certificates can be used in current applications such as that on which we focused: electronic travel documents. We used the cryptographic qTESLA family as an example for our proof-of-concept, and showed that, the performance for key generation and digital signature are better than some classical cryptographic asymmetric techniques (namely RSA and Brainpool). At the same time, whilst the memory requirements increase, the change is not sufficiently large to make the algorithms impractical.[10] Of course, eMRTDs produced with a post-quantum algorithm such as qTESLA would not be compliant with ICAO Doc 9303 which defines the algorithms to can be used. ICAO will have to update their specifications for the post-quantum era in order to ensure the security of the electronic travel documents. For this feasibility test of postquantum PKI for electronic travel documents, we decided to use Open SSL to have freedom and ease of use, but this tool is not optimized or even designed for such a specific PKI [11].

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information (Cambridge University Press, Cambridge, UK, 2000).
[2] R. Rivest, in Handbook of Theoretical Computer Science (Elsevier, Amsterdam, The Netherlands, 1990), Vol. 1, pp. 717–755.
[3] R. L. Rivest, A. Shamir, and L. Adleman, Comm. Assoc. Comput. Mach. 21, 120 (1978).
[4] P. W. Shor, SIAM J. Comp. 26, 1484 (1997).
[5] J. Rompel, Proc. 22th Ann. ACM Symp. on Theory of Computing (STOC '90) 387 (1990).
[6] L. Lamport, Technical Report CSL-98, SRI International (1979).
[7] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, arXive e-print quant-ph/0102001 (2001). [8] A. S. Holevo, Rep. Math. Phys. 12(2), 273 (1977).
[9] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. 78, 3410 (1997).
[10] D. Mayers, Phys. Rev. Lett. 78, 3414 (1997).
[11] D. Chaum and S. Roijakkers, Lecture Notes in Computer Science 537, 206 (1991).