Quantum Communications and Cryptography

Henry McNeil  
 College of IS&T  
 University of Nebraska at Omaha  
 Omaha, NE, US  
 hcmcneil@unomaha.edu

Bryan Tomey  
 College of IS&T  
 University of Nebraska at Omaha  
 Omaha, NE, US  
 btomey@unomaha.edu

Casey Schmitz  
 College of IS&T  
 University of Nebraska at Omaha  
 Omaha, NE, US  
 caseyschmitz@unomaha.edu

Zexi Xing  
 College of IS&T  
 University of Nebraska at Omaha  
 Omaha, NE, US  
 zxing@unomaha.edu

ABSTRACT

Quantum computers provide many new opportunities for cryptography, such as key distribution, confidentiality, integrity, and non-repudiation. Because of the destructive and probabilistic nature of quantum measurements and the no-cloning theorem which prevents the duplication of quantum states, quantum cryptographic protocols are dramatically different from classical cryptography. A large number of these protocols have been proposed, but little comparative work has been done. We perform a survey of existing protocols, with a focus on practical applications, in order to provide an overview of the current state of the field. We also present an implementation of a practical quantum cryptographic algorithm capable of providing confidentiality, integrity, and non-repudiation. In addition, we generalize our implementation process in order to provide a template for the translation of algorithms from a research paper into a quantum programming framework.

∗Article Title Footnote needs to be captured as Title Note

†Author Footnote to be captured as Author Note

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

*WOODSTOCK’18, June, 2018, El Paso, Texas USA*

© 2018 Copyright held by the owner/author(s). 978-1-4503-0000-0/18/06...$15.00

https://doi.org/10.1145/1234567890

CCS CONCEPTS

• Insert CCS text here • Insert CCS text here   • Insert CCS text here

KEYWORDS

Quantum Communication, Quantum bit, Qiskit, Quantum Key Distribution, BB84, Twin-field QKD, MID-QKD, Photon, Quantum Cryptographic.

ACM Reference format:

FirstName Surname, FirstName Surname and FirstName Surname. 2018. Insert Your Title Here: Insert Subtitle Here. In *Proceedings of ACM Woodstock conference (WOODSTOCK’18). ACM, New York, NY, USA, 2 pages.* https://doi.org/10.1145/1234567890

1 Introduction

Quantum computers have the world on the brink of a second computing revolution. By using the unique properties of subatomic particles, they will be able to solve complex problems in minutes which would take a classical computer thousands of years. Foremost among these problems are many which are foundational to modern cryptography, such as the prime factorization problem at the core of internet security. While current quantum computers do not have the level of sophistication necessary to break today's encryption systems, it is only a matter of time before they gain that capability. We are undertaking this project to explore the implications of quantum computing on cryptography in order to stay ahead of this anticipated threat and preserve the security of sensitive communications as used for everything from internet browsing to military instructions.

In highly critical communications systems, such as those used to initiate a military action, messages must have guaranteed delivery, must not be tampered with, and must be authenticated and correct. These systems must not allow for false messages, as these could lead to widespread loss of life in the worst case, so non-repudiation is a primary concern. Our goal in this project is to identify the best ways for a critical system to send confidential messages with a guarantee of integrity and non-repudiation in a world where quantum computers are prevalent and capable. These cryptographic mechanisms may include quantum key distribution, quantum digital signatures, and quantum-resistant encryption algorithms performed on a classical computer.

The updated template, user manuals, samples, and required fonts, all are available at the URL <https://www.acm.org/publications/proceedings-template>. It contains said information for all three versions of MS Word (Windows and 2 versions of Mac). There are also separate links to the user guide, which can be referred to by the user. This URL also contains some useful video links, which describe how to add the template, structure the paper, and generate the layout, in different clips. **Display Formula with Number**

 (1)

**Continuation part of Paragraph Text** The user must style this paragraph in **ParaContinue** style, which follows immediately after the **DisplayFormula** (numbered equation). The **DisplayFormula** style is applied only in case of a numbered equation. A numbered equation always has a number to its right. Insert paragraph text here. **Display Formula without Number**



The **DisplayFormulaUnnum** style is applied only in case of an unnumbered equation. An unnumbered display equation never contains an equation number to its right, and this unique property distinguishes it from a numbered equation.



Figure 1: Figure Caption and Image above the caption [In draft mode, Image will not appear on the screen]

**Theorem/Proof/Lemma.** Insert text here for the enunciation or Math statement. Insert text here for the enunciation or Math statement. Insert text here for the enunciation or Math statement. Insert text here for the enunciation or Math statement. Insert text here for the enunciation or Math statement.

....Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract, Insert text here for the Quotation or Extract.

1.1 Heading Level 2

In the below paragraph, it is explained how alt-txt value is placed in **MS Word 2010**. To add alternative text to a picture in Word 2010, follow these steps:

1. In a Word 2010 document, insert a picture.
2. Right click on the inserted picture and select the **Format Picture** option.
3. Select the **Alt Txt** option from the left-side panel options.
4. In the "Title:" and "Description:" text boxes, type the text you want to represent the picture, and then click "Close".

Below are steps to place alt-txt value in **MS Word 2013/2016**. To add alternative text to a picture in Word 2013/2016, follow these steps:

1. In a Word 2013/2016 document, insert a picture.
2. Right click on the inserted picture and select the **Format Picture** option.
3. In the settings at the right side of the window, click on the "Layout & Properties" icon (3rd option).
4. Expand **Alt Txt** option.
5. In the "Title:" and "Description:" text boxes, type the text you want to represent the picture, and then click "Close".

*1.1.1 Heading Level 3.* Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here.

*1.1.1.1 Heading Level 4.*Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here.

ACKNOWLEDGMENTS

Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here.

REFERENCES

[1] Patricia S. Abril and Robert Plant, 2007. The patent holder's dilemma: Buy, sell, or troll? *Commun. ACM* 50, 1 (Jan, 2007), 36-44. DOI: <https://doi.org/>10.1145/1188913.1188915.

[2] Sten Andler. 1979. Predicate path expressions. In *Proceedings of the 6th. ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL '79)*. ACM Press, New York, NY, 226-236. DOI:https://doi.org/10.1145/567752.567774

[3] Ian Editor (Ed.). 2007. *The title of book one* (1st. ed.). The name of the series one, Vol. 9. University of Chicago Press, Chicago. DOI:https://doi.org/10.1007/3-540-09237-4.

[4] David Kosiur. 2001. *Understanding Policy-Based Networking* (2nd. ed.). Wiley, New York, NY..

Conference Name:ACM Woodstock conference

Conference Short Name:WOODSTOCK’18

Conference Location:El Paso, Texas USA

ISBN:978-1-4503-0000-0/18/06

Year:2018

Date:June

Copyright Year:2018

Copyright Statement:rightsretained

DOI:10.1145/1234567890

RRH: F. Surname et al.

Price:$15.00