MD.Sarwar Pasha *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 3, March- 2014, pg. 102-116 **ISSN: 2321-8363**

Key Pre Distribution Using Quantum Key Channel

MD.Sarwar Pasha[1], A. Bala Ram[2]

[1]M.Tech. Student, CSE Dept., CMR Institute of Technology, Hyderabad, A.P
Email-id: pashamohd42@gmail.com
[2]Associate Professor, CSE Dept., CMR Institute of Technology, Hyderabad, A.P
Email-id: balaram.balaram@gmail.com

Abstract

Modern optical networking techniques have the potential to greatly extend the applicability of quantum communications by moving beyond simple point-to-point optical links, and by leveraging existing fibre infrastructures. We experimentally demonstrate many of the fundamental capabilities that are required. These include optical-layer multiplexing, switching, and routing of quantum signals; quantum key distribution (QKD) in a dynamically reconfigured optical network; and coexistence of quantum signals with strong conventional telecom traffic on the same fibre. We successfully operate QKD at 1310 nm over a fibre shared with four optically amplified data channels near 1550 nm. We identify the dominant impairment as spontaneous anti- Stokes Raman scattering of the strong signals, quantify its impact, and measure and model its propagation through fibre. We describe a quantum networking architecture which can provide the flexibility and scalability likely to be critical for supporting widespread deployment of quantum applications.

Index Terms- Quantum key distribution, multiple access, cryptography

1. Introduction

The ultimate usefulness of most communications services depends strongly on the ability to network, i.e., to efficiently connect many end users with each other or with shared resources. Much of the experimental research on Quantum Key Distribution (QKD) has focused on improving transmission performance over a fixed end-to-end connection between

a single pair of quantum endpoints, Alice and Bob. However, this type of connectivity does not scale well, because the level of resources that are required increases very rapidly with the number of end users. Efficient networking solutions are clearly needed to move QKD and other types of quantum communications beyond the realm of niche deployments.

Many of the technologies, components and techniques needed to address these problems have been developed over the past quarter century for use in conventional optical fibre networks.

Early fibre networks utilized optics solely for point-to-point (PTP) transmission between opaque nodes, in which all networking functions were implemented electronically. In contrast, modern fibre networks increasingly take advantage of optical transparency, in which a subset of critical networking functions such as switching, routing and multiplexing are preferentially performed in the optical layer [1]. This enables the establishment of multiple optically transparent lightpaths through a network domain, and highly dynamic re-routing or reconfiguration of these lightpaths.

Applied to QKD, optical networking offers the prospect of flexible and scalable on-demand connectivity for a large number of Alice-Bob pairs. End-to-end key establishment over an untrusted network is feasible for lightpaths compatible with the maximum attenuation allowed 5 Current address: DARPA/DSO, 3701 North Fairfax Dr., Arlington VA 22203; work performed while affiliated with Telcordia by the QKD system. Communications over longer end-to-end paths, or between endpoints with incompatible QKD systems, can be routed on demand via a shared set of ‘trusted relay’ nodes in secured locations [2-8]. The network can also provide endpoints with optically transparent access to other shared resources, such as ‘centralized’ entangled-photon sources for QKD. Finally, optical networking offers the prospect of leveraging costly infrastructure already deployed for telecom and enterprise networks, via wavelength-division multiplexing (WDM) of quantum and conventional data signals onto the same fibres. A central question for the future of QKD is to what extent it can attain wide applicability by taking advantage of these major advances in conventional optical networking.

Achieving this vision requires developing new capabilities, and validating them in realistic network environments. In this paper, we experimentally demonstrate a number of fundamental capabilities of optical networking as applied to QKD. These include optical routing, automated restoration after network path reconfiguration, and multiplexing and transmission of QKD with strong conventional WDM channels on the same fibre. We also examine practical considerations for applying optical networking architectures and technologies to QKD, and resulting impacts on the quantum signals in these environments. Although the experiments and analyses reported in this paper focus entirely on QKD, many of the results are likely to also carry implications for a broader range of quantum communications services which rely on the transport of photonic qubits over fibre networks.

The earliest QKD optical networking experiments were reported by Townsend's group [9-10], which measured quantum bit error rates (QBER) for QKD signals transmitted through a 1:3 passive optical splitter to facilitate distribution of QKD signals to three different receivers. Following this work, several additional groups proposed passive fibre distribution networks to transmit key to multiple nodes [11-13]. Our group reported the first demonstrations of QKD through optical switches, including key establishment through several types of switch fabrics, and optical protection switching between two fibre paths connecting Alice and Bob [14]. Honjo et al. used a planar lightwave circuit (PLC) switch to connect Alice with either of two Bobs, demonstrating low QBER in the presence of crosstalk from a much stronger channel on a different path through the switch [15]. Optical switching has also been used in a portion of the DARPA quantum network [8], and investigated in a three-node QKD configuration at NIST [16].

The first experiment using WDM to combine QKD with an uncorrelated data channel on the same fibre was reported by Townsend [17]. WDM is often employed for carrying 'bright' synchronization pulses along with the quantum signals, and has occasionally been used to support one or a small number of data channels. However, few experiments have reflected the environments encountered in routing quantum signals through a modern telecom or enterprise network, in which very strong (~1 mW) data channels create substantial

impairments which must be understood and mitigated. Early work with multi-channel WDM can be found in [18, 19] and [20], for QKD signals near 1310 nm or 1550 nm, respectively.

Our approach differs from, but is complementary with, the 'trusted relay' backbone architecture demonstrated by the SECOQC collaboration [2-4], and related approaches [5] which build on concepts developed for the DARPA quantum network [6-8]. For example, the SECOQC network is constructed from a collection of fixed PTP QKD links, with a variety of QKD technologies, connecting opaque quantum nodes in secured locations. Networking functions are performed entirely in the electronic domain, in a trusted network dedicated to QKD.

The following section provides a brief overview of the role of optical networking in quantum communications. Section 3 presents experimental results on the operation of QKD in dynamically reconfigurable networks, while Section 4 reports results on combining QKD with strong data channels in shared network environments. Section 5 provides a summary and conclusions.

RESULTS AND DISCUSSIONS

Testing

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produces valid outputs. All decision

branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Integration testing is of three types:

- Bottom up Integration
- Top down Integration
- Sandwich Integration

Bottom up integration testing consists of unit testing followed by system testing. Unit testing has the goal of testing individual modules in the system. Subsystem testing is concerned with verifying the operation of the interfaces between modules in the sub systems. Top down integration testing starts with the main routine and one or two immediately subordinate routines in the system structure. Top down integration requires the use of program stubs to simulate the effect of lower level routines that are called by those being tested.

Top down method has the following advantages:

- System integration is distributed through the implementation phase. Modules are integrated as they are developed.
- Top level interfaces are tested first and most often.
- The top level routine provides a natural test harness for lower level routines.
- Errors are localized to the new modules and interfaces that are being added.

Functional test

Functional tests provide a systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation , and user manuals. Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.
Invalid Input : identified classes of invalid input must be rejected.
Functions : identified functions must be exercised.
Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

Test Cases

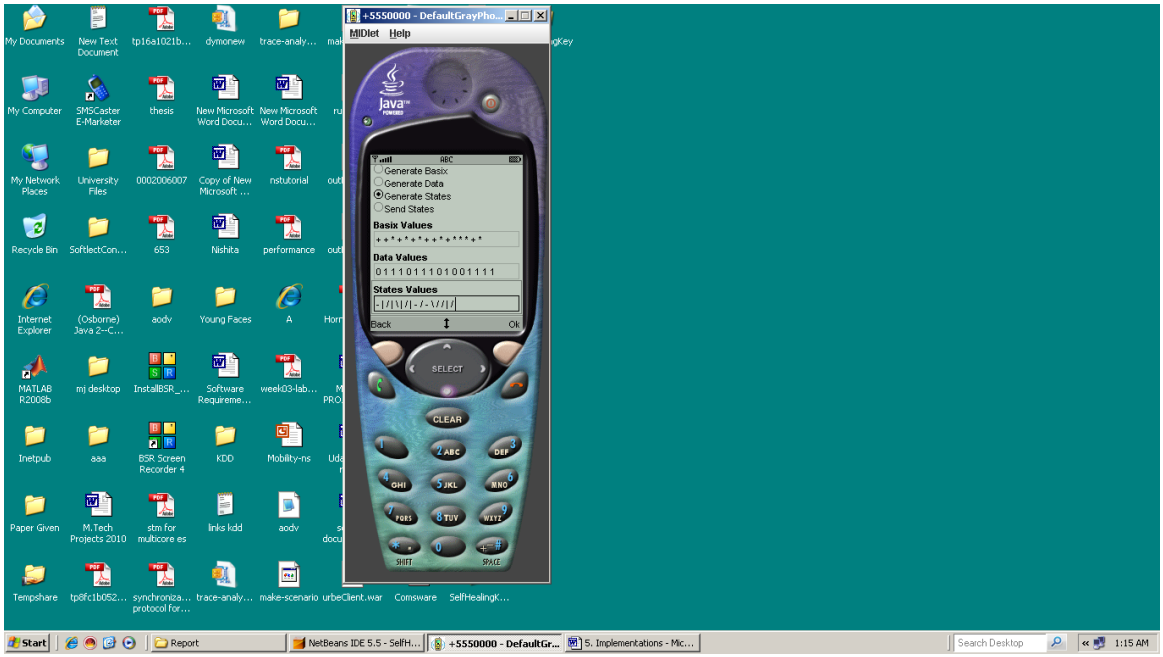
Test Case ID:	1
Test Case Name:	Required Software Testing
Purpose:	To check weather the required Software is installed on the systems
Input:	Enter Javac –version, and Java –version
Expected Result:	Should Display the version number for both the java compiler and Java virtual Machine
Actual Result:	Displays java version "1.6.0_01" and Javac "1.6.0_01"
Failure	If the java environment is not installed then the Deployment fails

Test Case ID:	2
Test Case Name:	Programs Integration Testing
Purpose:	To ensure that all the modules works together
Input:	All the Mobile user interfaces must be accessed
Expected Result:	All the Mobile user interface should run in the common Midlet
Actual Result:	All the Mobile user interface runs in the common Midlet
Failure	If the Communication is not started then the Mobile interface will not work

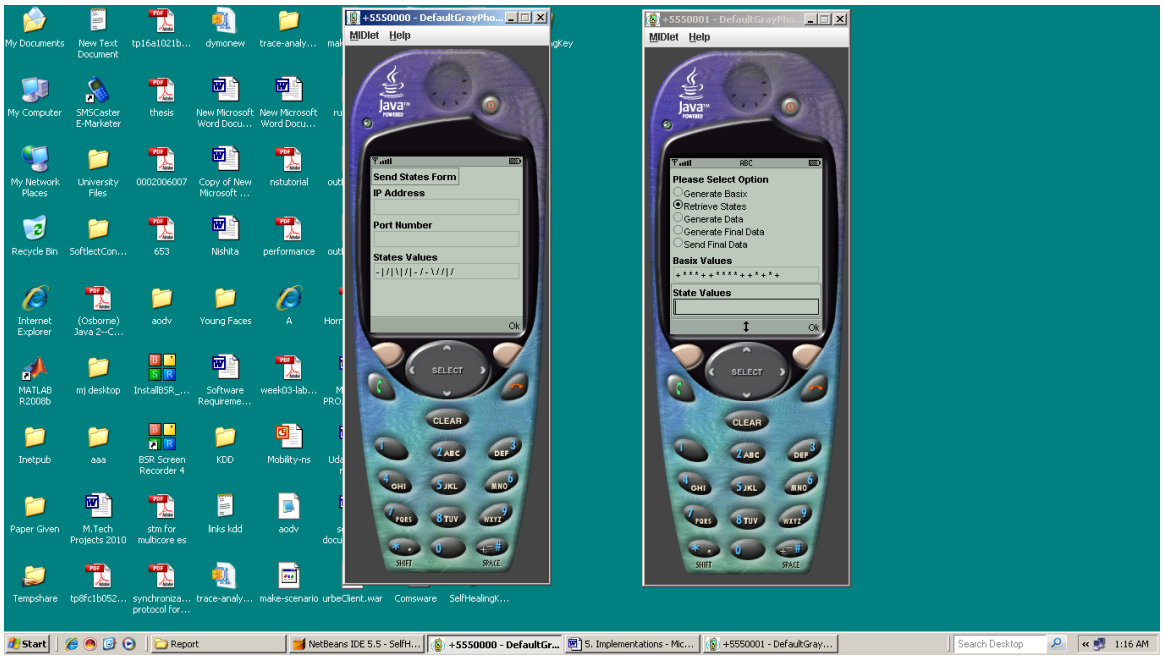
Results

Generating Base Values

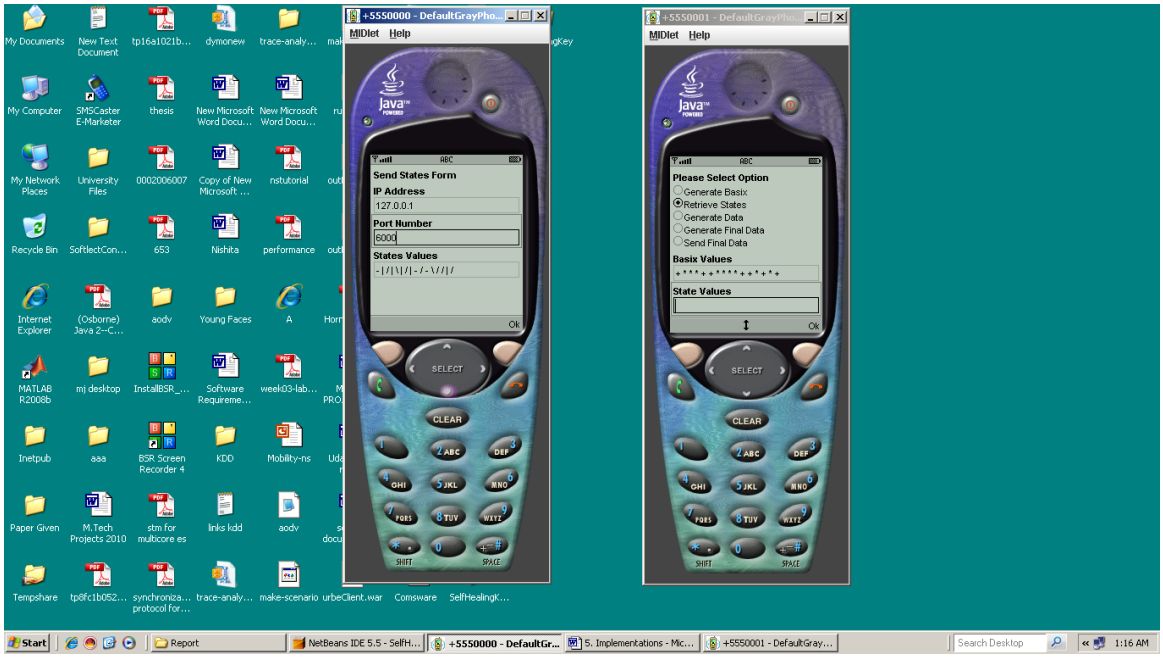
Generating Data Values



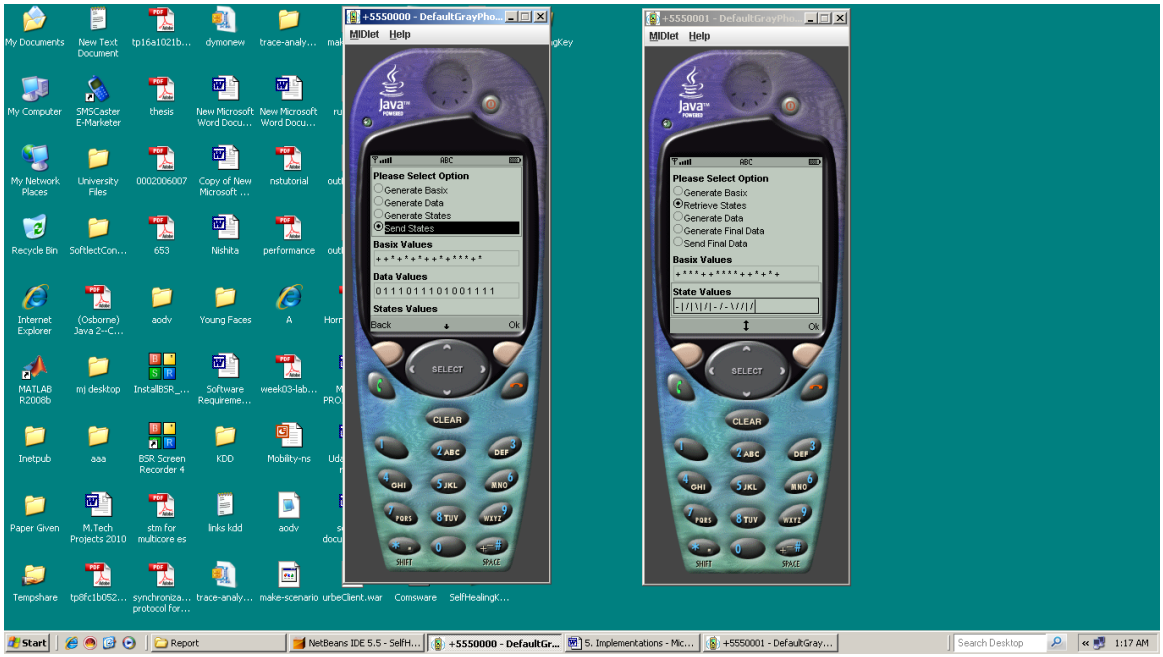
Generating State Values



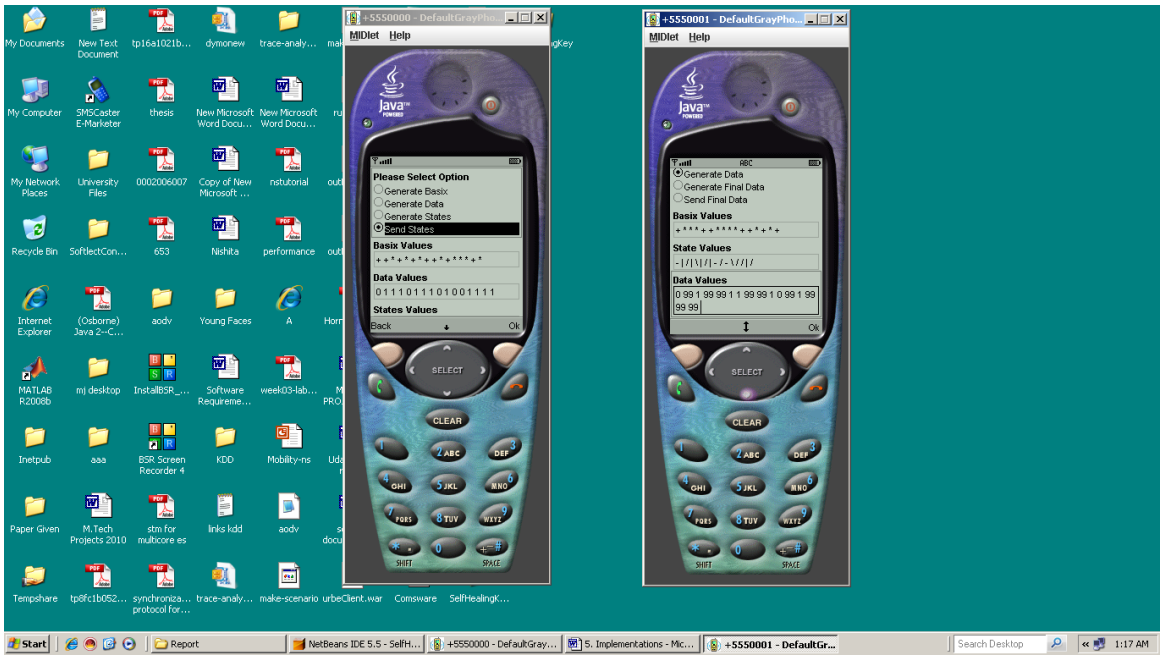
Sending State Form



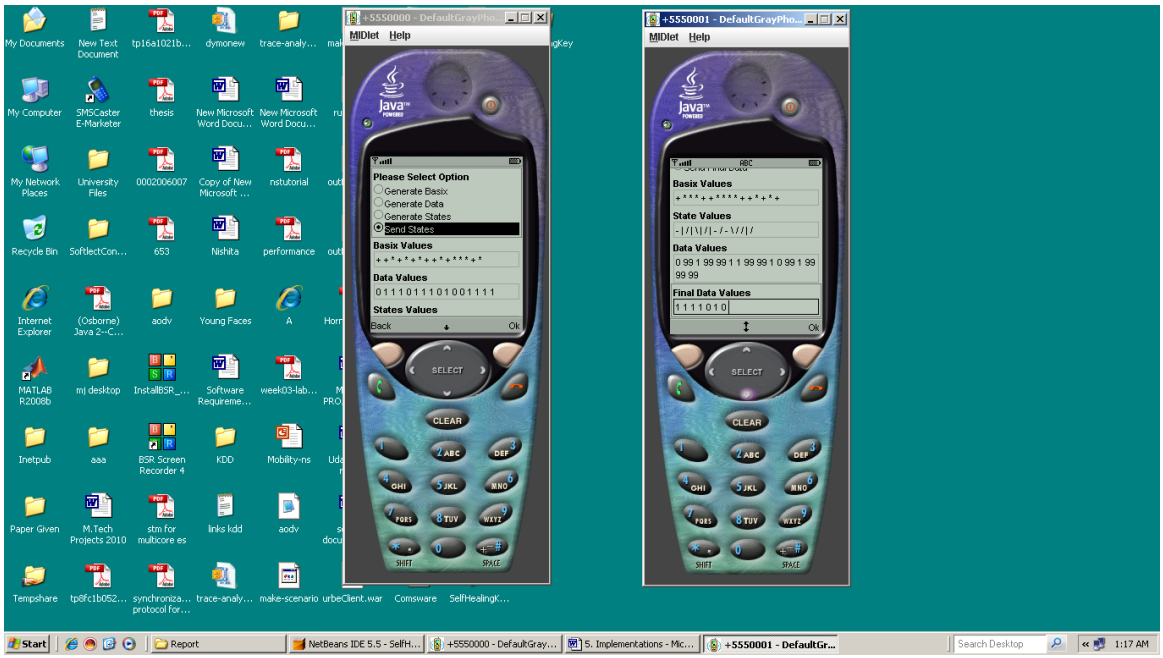
Sending State Values



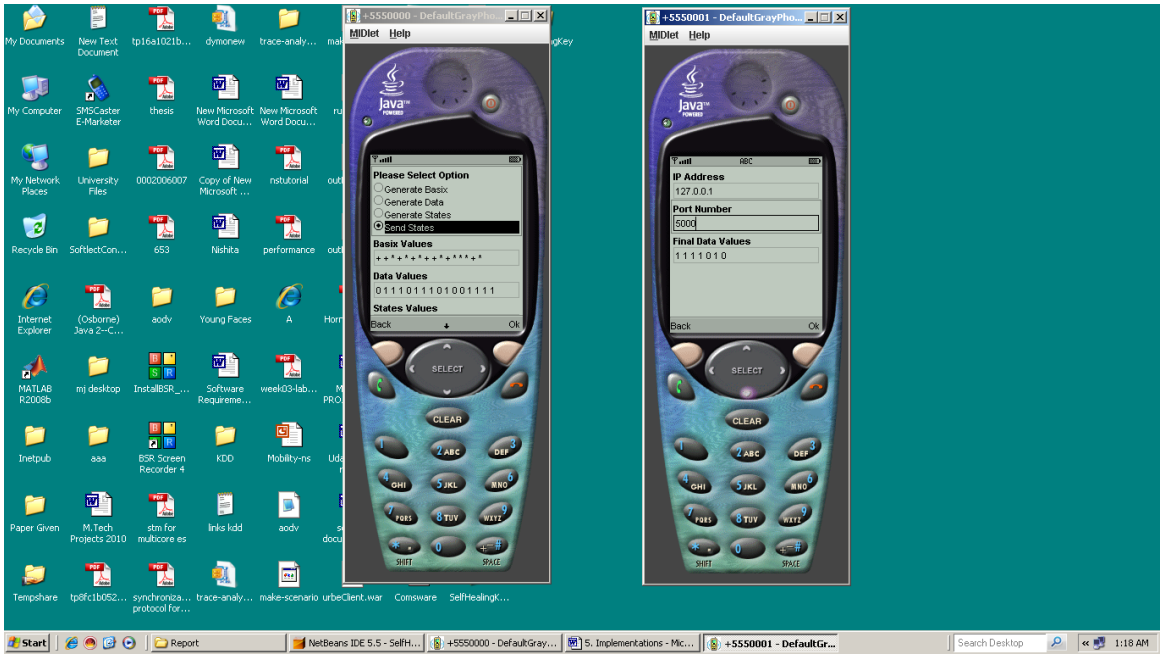
Retrieving State Values



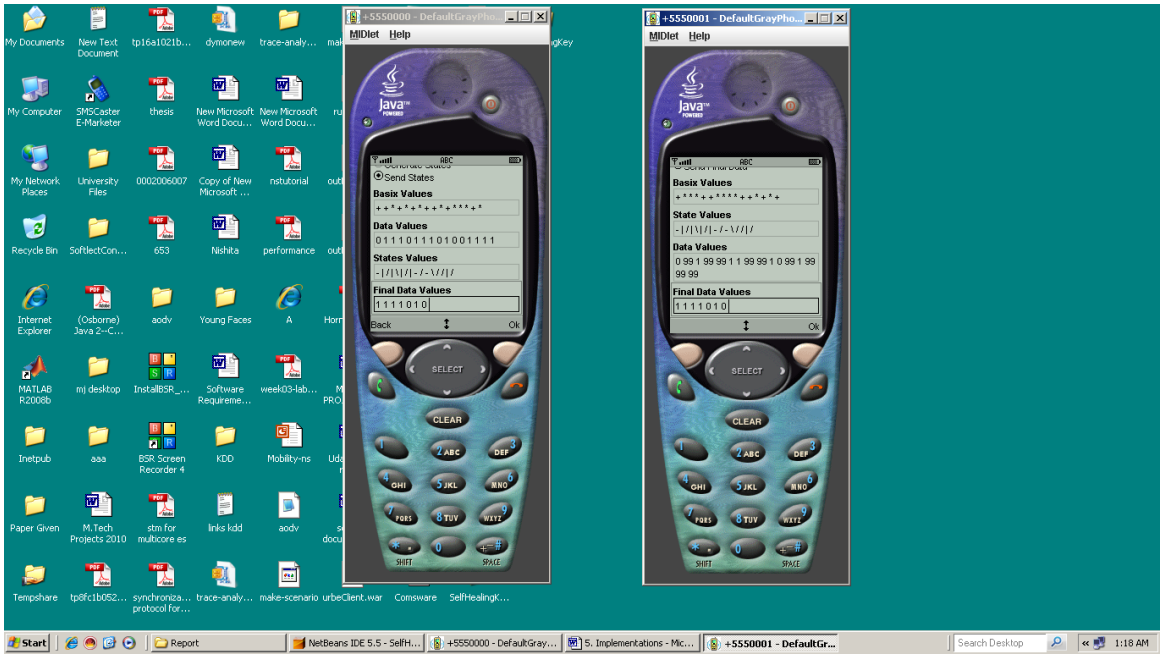
Generating Data



Generating Final Data Values



Sending Final Data



Checking the Final Data

Conclusion

In this paper, well-known techniques in classical multiple access optical communications were applied to quantum cryptography applications. That enabled multiple users to exchange secret keys, via an optical network, without trusting any other nodes. The proposed setups offered key features that would facilitate their deployment in practice. In all of them, classical communications services were integrated with that of quantum on a shared platform, which would substantially reduce the cost for public and private users. More generally, by sharing network resources among many users, the total cost per user would shrink, making the deployment of such systems more feasible. Another cost-saving feature in our setups was their relying on only one QKD detection module per user. The setups considered were inspired by existing optical access networks as well as future all-optical networks. A passive starcoupler network was first studied when multiple QKD users could pair up and simultaneously exchange secret keys via the network. Each user could independently use classical communications as well. Different users could be distinguished in time, using a TDMA scheme, or in the code space using OOC CDMA. It turned out that, whereas TDMA QKD could offer an interference free, or, effectively, a point-to-point QKD service, CDMA QKD should deal with the interference effect. It was shown that the optimal performance for a CDMA QKD system could be achieved if codes with weight one were used, for which interference probability would be minimum. In this case, the encoded CDMA signal was somehow similar to the TDMA one, except that no time coordination was needed between all network users. To enjoy the benefits of both TDMA and CDMA systems, a listen-before-send protocol was proposed, whose performance could approach the TDMA QKD once the number of listening periods was sufficiently large. To support a larger number of users, hybrid WDMTDMA CDMA architectures, potentially compatible to future all-optical networks and PON access systems, were proposed and their performance in terms of secret key generation rates and numbers of users was studied.

References

[1] Mohsen Razavi, " Multiple-Access. Quantum Key Distribution Networks", vol. 60, ISSN :0090-6778, July 2012.

[2] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Exp.*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[3] M. Razavi, M. Piani, and N. L¨utkenhaus, "Quantum repeaters with imperfect memories: cost and scalability," *Phys. Rev. A*, vol. 80, p. 032301, Sept. 2009.

[4] N. A. Peters *et al.*, "Dense wavelength multiplexing of 1550nm QKD with strong classical channels in reconfigurable networking environments," *New J. Phys.*, vol. 11, p. 045012, Apr. 2009.

[5] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, p. 010504, 2007.

[6] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, pp. 3762–3764, 2004.

[7] T. J. Xia, D. Z. Chen, G. A. Wellbrock, A. Zavriyev, A. C. Beal, and K. M. Lee, "In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels," in *Opt. Fiber Commun.,Technical Digest*. Optical Society of America, 2006, paper OTuJ7.

[8] W. Chen *et al.*, "Field experiment on a star type metropolitan quantum key distribution network," *IEEE Photon. Technol. Lett.*, vol. 21, no. 9, pp. 575–577, May 2009.

[9] T. E. Chapuran *et al.*, "Optical networking for quantum key distribution and quantum comunications," *New J. Phys.*, vol. 11, p. 105001, Oct. 2009.

[10] M. Razavi and J. H. Shapiro, "Long-distance quantum communication with neutral atoms," *Phys. Rev. A*, vol. 73, p. 042303, Apr. 2006.

Authors' Biography

Md Sarwar Pasha had B.Tech from Syed Hashim College of Science and Technology, Pregnapur, Medak District. He is an M.Tech. student in CSE Department of CMR Institute of Technology, Hyderabad. He is currently doing his M.Tech.project work under the guidance of **Mr.A.Bala Ram.**

Mr. A. Bala Ram, He is currently working as Associate Professor in CSE Department of CMR Institute of Technology, Hyderabad. His areas of interest are Net work security, cloud computing, image processing.

