氏　　名	玉木　潔
学位（専攻分野）	博士(理学)
学位記番号	総研大甲第790号
学位授与の日付	平成１６年３月２４日
学位授与の要件	先導科学研究科　光科学専攻 学位規則第４条第１項該当
学位論文題目	Security analysis of the Bennett 1992 quantum key-distribution protocol over a realistic channel
論文審査委員	主　査　教授　井元　信之 教授　石黒　真木夫 助教授　小芦　雅斗 助教授　平野　琢也（学習院大学）

博士論文の要旨

Security analysis of the Bennett 1992 quantum key-distribution protocol over a realistic channel

In this thesis, we analyze the security of the Bennett 1992 quantum key-distribution protocol (B92 protocol) over a realistic channel assuming that bit values are encoded in single photon polarization states.

First, we study the security of the B92 protocol against individual attack. In the individual attack, eavesdropper (Eve) interacts a qubit emitted by the sender (Alice) with her probe system followed by a measurement on each probe. To make our analysis simple, we propose a modified B92 protocol. Using this protocol, Alice and the receiver (Bob) can estimate Eve's information gain as a function of a few parameters that reflect the imperfections of devices or Eve's disturbance. We find a counter-intuitive behavior of Eve's maximum information gain, i.e., it decreases as the amount of disturbances increases. We also estimate the secret key gain that is the net growth of the secret key per one pulse. We show the region where the modified B92 protocol over a realistic channel is secure against individual attack.

Next, we study the unconditional security of the B92 protocol, which is the security against any attack. To prove the security, we first propose a protocol that is unconditionally secure and can be reduced to the B92 protocol. This protocol employs the entanglement distillation protocol (EDP) based on a filtering operation and the Calderbank-Shor-Steane (CSS) quantum error correcting codes. The bit errors and the phase errors, which have to be estimated for the EDP based on the CSS codes, are correlated after the filtering operation, and we can bound the amount of phase errors from the observed bit errors by an estimation method involving nonorthogonal measurements. The angle between the two states shows a trade-off between accuracy of the estimation and robustness to noises. We show a way to run the unconditionally secure B92.

論文の審査結果の要旨

申請者は、量子暗号の安全性について、現実的通信路を仮定して研究を進め、理論上の困難さを取り除く工夫をいくつか行った結果、世界で初めてB92(Bennett 1992)量子暗号の安全性の証明に成功した。よって本論文は博士論文として十分なオリジナリティを有するものと判定した。試験としては口頭発表に続き、随時審査委員からの質疑に対する応答で進められた。口頭発表は要点を押さえ、要領よくまとめられていた。審査委員からの質疑に対してもわかりやすく本質を突いた受け答えがなされた。また論文の骨格となる英語論文が筆頭著者として3編国際誌に掲載されており、申請者の国際学会での発表も（招待1件を含め）5件あることから、英語能力も十分であると判断した。これらから審査員全員一致して玉木潔氏は、博士の学位授与に足る学識と研究能力を持つものと判定した。