where $q = \log 1/c$ is the quality factor and

$$x = \frac{(1-5\delta)(1-\delta)\eta(1-\eta)}{(\delta+(1-2\delta)\eta)(1-\delta)-(1-5\delta)\eta)},$$

where $\eta = (2\alpha\beta)^2$ and $\delta = 2/3p, (0 < p < 1)$, where p describes the amount of noise in the channel. The error rate conditioned on acceptance is given by $\varepsilon = \delta/(1-2\delta)\eta + 2\delta$, $\alpha \in (0, \frac{1}{\sqrt{2}})$ and $\beta = \sqrt{1-\alpha^2}$ are complex vectors [18]. By substitution of Equation (22) into Equation (21), we find that the secret key rate r, varies with the number of signals N, as shown in Figure 1. Again, if we combine Equation (22) with the proposed bound on the achievable key length in Equation (21) and also by using the Quantum Leftover Hash Lemma [19] we have

$$\triangle \leq \bar{\varepsilon} + \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\bar{\varepsilon}}}(X|E')} \leq 2\bar{\varepsilon} + \varepsilon_{PA}, \tag{23}$$

where E' summarizes all information Eve learned about $\mathbf{X}$ during the protocol including the classical communication sent by Alice and Bob over the authenticated channel. This equation shows that one can extract a $\triangle$-secret key of length ℓ from X. This completes the proof for security bound for the B92 protocol.

4. Conclusion

We have demonstrated how one can use results of the uncertainty relations and smooth Rényi entropies to derive security bounds for the B92 QKD protocol when a finite number of signals are used. The results show that a minimum number of approximately $10^4 - 10^6$ signals are required in order to extract a reasonable length of secret key in QKD protocols under realistic scenarios. This minimum number has also been discussed in [6, 8, 9]. Therefore, the uncertainty relations and the smooth Rényi entropies prove to be a powerful technique for the derivation of the security bounds in QKD protocols in the finite size-key regime.

Acknowledgments

This work is based on research supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

References

[1] Bennett C and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* vol 175 (Bangalore, India)
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–195
[3] Ekert A 1991 *Physical Review Letters* **67** 661–663
[4] Bennett C 1992 *Physical Review Letters* **68** 3121–3124
[5] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[6] Scarani V and Renner R 2008 *Physical Review Letters* **100** 200501
[7] Renner R 2008 *International Journal of Quantum Information* **6** 1–127
[8] Cai R and Scarani V 2009 *New Journal of Physics* **11** 045024
[9] Sheridan L, Le T and Scarani V 2010 *New Journal of Physics* **12** 123019
[10] Sheridan L and Scarani V 2010 *Phys. Rev. A* **82**(3) 030301
[11] Tan Y and Cai Q 2010 *The European Physical Journal D* **56** 449–455
[12] Abruzzo S, Kampermann H, Mertz M and Bruß D 2011 *Physical Review A* **84** 032321
[13] Tomamichel M and Renner R 2011 *Physical Review Letters* **106** 110506
[14] Rényi A 1961 *Fourth Berkeley Symposium on Mathematical Statistics and Probability* pp 547–561
[15] Kraus B, Gisin N and Renner R 2005 *Physical Review Letters* **95** 80501
[16] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nature communications* **3** 634
[17] Phuc Thinh L, Sheridan L and Scarani V 2011
[18] Christandl M, Renner R and Ekert A 2004 *arXiv:0402131v2*
[19] Tomamichel M, Schaffner C, Smith A and Renner R 2011 *IEEE Transactions on Information Theory* **57** 5524 –5535 ISSN 0018-9448