# A general framework for Quantum Secret Sharing protocols with ditter measurements

Zoé AMBLARD
XLIM Laboratory
University of Limoges

François ARNAULT
XLIM Laboratory
University of Limoges

April 29, 2016

In Quantum Cryptography, entanglement-based protocols exploit a specific property of Quantum Physics known as entanglement to establish a secret key between all authorized participants. This property also provides an interesting feature absent in classical cryptography : detection of a perturbation in the protocol by checking the violation value of a Bell inequality.

In this work, we consider entanglement-based schemes using quantum systems in dimension $d$. One way to measure a $d$-dimensional quantum system is to use a device called *multiport beamsplitter*, or ditter. A mathematical description of such devices is given in [1]. Some have already been experimentally tested such as tritters in [2] when $d = 3$.

We also perform security checks by computing the violation value of specific Bell inequalities belonging to the family called *homogeneous Bell inequalities* and introduced by François Arnault in [3]. As these inequalities use products of observables which do not commute, we demonstrated in a previous work [4] how to measure such product with a combination of a ditter and slightly modified detectors, enabling experimental checks of homogeneous Bell inequalities.

If only two participants are involved, one usually refers to these schemes as Quantum Key Distribution (QKD) protocols. When the interest is to share a common secret between $n$ participants in such a way that all participants must cooperate to retrieve the secret, these schemes are called Quantum Secret Sharing (QSS) protocols.

First QSS entanglement-based protocols for 2-dimensional systems and up to four participants, commonly referred to as HBB and KKI respectively, were introduced by Hillery, Bužek, Berthiaume in [5] and by Karlsson, Koashi, Imoto in [6]. Yu, Lin and Huang extended the HBB-type protocols for $n$ participants and $d$-dimensional systems in [7].

We present here a general framework for Quantum Secret Sharing protocols for $d$-dimensional systems and $n$ participants using ditter measurements, inspired from the protocols described by Yu *et al.* in [7]. In order to derive this framework, we first describe two new notions of *matching* and *almost matching* measurements which allow us to derive usable conditions on each participant's measurements in order to maximize the retrieval of key dits in Quantum Secret Sharing entanglement-based protocols with $d$-dimensional systems.

In the light of this new framework, we show how the protocol described by Yu, Lin and Huang in [7] can be seen as a special case of our work and we construct two new entanglement-based QSS schemes for $d = 3$ and $n = 2, 3$ using well-chosen tritter measurements.

A detailed version of this work can be found in attachment below.

## References


[1] M. Ẑukowski, A. Zeilinger, and M.A. Horne. Realizable higher-dimensional two-particle entanglements via multiport beam splitters. *Physical Review A*, 55:2564, 1997.

[2] K. Mattle, M. Michler, H. Weinfurter, A. Zeilinger, and M. Ẑukowski. Non-classical statistics at multiport beam splitters. *Applied Physics B*, 60:S111, 1995.

[3] F. Arnault. A complete set of multidimensional Bell inequalities. *Journal of Physics A*, 45:255304, 2012.

[4] F. Arnault and Z. Amblard. A quantum key distribution protocol for qudits with better noise resistance. arXiv e-print:1504.08161, 2015.

[5] M. Hillary, V. Bu̇zek, and A. Berthiaume. Quantum secret sharing. *Physical Review A*, 59:1829, 1999.

[6] A. Karlsson, M. Koashi, and N. Imoto. Quantum entanglement for secret sharing and secret splitting. *Physical Review A*, 59:162, 1999.

[7] I-C Yu, F-L Lin, and C-Y Huang. Quantum secret sharing with multi-level mutually (un-)biased bases. *Physical Review A*, 78:012344, 2008.