Quick comparison table about the practical aspects of Quantum Communicators and the Kirchoff-loop-Johnson-like-noise (KLJN) Communicators. **Table 4** in: L.B. Kish and P. Mingesz, "Totally secure classical networks with multipoint telecloning (teleportation) of classical bits through loops with Johnson-like noise", *Fluct. Noise Lett.* **6** (2006) C9-C21.

	Quantum Comm.	**KLJN Comm.**
Physics behind the security	Quantum (Fragile information bit)	Classical statistical (Robust information bit)
Max. number of eavesdropped bits before 99% probability of eavesdropper detection	Few thousand	0-4
Vulnerability against the man-in-the-middle attack	Usually yes	No
Information leak below the eavesdropper detection radar (eavesdropper hiding in noise)	>1%	0.01% or less is easily reachable
Ultimate speed-cut-off versus range	Exponential cut-off	1/range cut-off
Network key distribution	No. Only point-to-point	Yes. Whole-network key distribution within two clock periods
Telecloning	Yes, with fidelity < 71%	Yes, with 100% fidelity
Network telecloning in one step. Number of units N.	Only if all Units are *directly connected to each other* which needs $(N^2-N)/2$ connections. Acceptable fidelity (>50%) only for $N \approx 30$, or less.	Yes, even if the Units connected as an arbitrarily large ($N \to \infty$) *chain network* (needs only $N-1$ connections), within two clock periods.
Vibration resistant	No	Yes
Shock resistance	Poor	Excellent
Dust resistant	No	Yes
Microelectronic integrated parallel multi-line (>100) driver chip	No	Yes
Low-power consumption	No	Yes
Communicator as a computer card	No	Yes
Price	High	Low