Proposal to delete the Kish cypher page

Dear All,

This is Laszlo B. Kish, the originator of the Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange system with the popular but incorrect name "Kish cypher". I have been informed that there is a proposal to delete the "Kish cypher" page.

I want to express that I fully and strongly support this proposal. Already, in March 2012, I asked Wikipedia Editor Jake Ocaasi to delete that page because my name has been used in fights where the supporters of both the quantum-informatics and the KLJN systems have been often wrong and fighters at both sides often misrepresented our results.

I am somewhat sympathizing with their failure because I myself also went through such a learning phase after publishing the first KLJN paper, where I used the word "totally" instead of the proper "perfectly", etc. However, for me, it has always perfectly clear that what we are discussing here is measurement information in a system of thermal equilibrium, which most debate participants seem to miss. They also miss elementary terms such as information theoretic security (=unconditional security); perfect security; imperfects security, etc, etc.

Anyway, to cut it short, public debates about scientific matters should be done by professionals at conferences and in peer-reviewed journals, and not by enthusiastic supporters on Wikipedia. While I am not wiki expert, my understanding is that Wikipedia should represent the peer-reviewed scientific literature in a balanced fashion, not the personal opinions of enthusiastic supporters of the Pro and Con sides. The history of the "Kish cypher" page has proven that these rules cannot be enforced therefore I strongly support the termination of this page, which is related to my name and is misrepresenting the research results of our team.

Note, while I fully support deletion, I must express that I disagree with the personal opinion of Skyppido that the KLJN system is "almost totally ignored by the cryptographic community" and is " fringe research by cryptographic/security standards, and totally dead in terms of citations/potential research". I encourage Skyppido to take a look at the history of the first 10 years of quantum key distribution, and see how many papers they published, how large team they were, how many citations they received that time, and at which type of journals (often only at conferences) they succeeded to publish because they were turned down elsewhere. If you do that comparison, KLJN is actually much better off already during its first 8 years. Future will show how these will further evolve.

For those, who are interested in deeper debates than wiki I recommend to read quantum-cryptography-founder Charles Bennet's recent manuscript about KLJN, where he and his coworker (coauthor Jess Riedel) are attempting to "debunk" the KLJN claim, see the manuscript at http://arxiv.org/abs/1303.7435 . While we disagree with almost all the claims in that manuscript, we are very happy about it because this is the way a scientific debate should be. We encourage interested people to read also our detailed response, which will soon be available. All the debate materials will be available at the KLJN page http://www.ece.tamu.edu/~noise/research_files/research_secure.htm at Texas A&M University.

Finally, for those who are interested in a *scientific* debate about the question if quantum key distribution is really secure or not, I recommend the forthcoming meeting *Hot Topics of Physical Informatics* http://www.ece.tamu.edu/%7Enoise/HotPI_2013/HotPI_2013.html and its conference proceedings, where the major challengers of quantum security will be present and debate with the representatives of quantum security in a *public debate session* that will also be published. Also, the KLJN system will be featured and the arguments of Bennett and others addressed. An open-access proceedings will be published.

To conclude this long message in short: I support Skippydo's proposal to delete the Kish cypher page. Thanks for the attention.

Laszlo Kish http://www.ece.tamu.edu/People/bios/bkish.php Laszlo B Kish (talk) 17:35, 14 April 2013 (UTC)

Retrieved from "http://en.wikipedia.org/w/index.php?title=Talk:Kish_cypher&oldid=550337670"