ENHANCED USAGE OF KEYS OBTAINED BY PHYSICAL, UNCONDITIONALLY SECURE DISTRIBUTIONS

LASZLO B. KISH

[1] *Department of Electrical Engineering, Texas A&M University, College Station, TX 77843-3128, USA*

laszlo.kish@ece.tamu.edu

Received (21 August 2014)
Revised (revised date)
Accepted (accepted date)

Unconditionally secure physical key distribution is very slow whenever it is undoubtedly secure. Thus it is practically impossible to use a one-time-pad based cipher to guarantee perfect security because using the key bits more than once gives out statistical information, such as via the known-plain-text-attack or by utilizing known components of the protocol and language statistics. Here we outline a protocol that seems to reduce this problem and allows a near-to-one-time-pad based communication with unconditionally secure physical key of finite length. The unconditionally secure physical key is not used for communication; it is use for a secure communication to generate and share a new software-based key without known-plain-text component, such as keys shared via the Diffie-Hellmann protocol. This combined physical/software key distribution based communication looks favorable compared to the physical key based communication when the speed of the physical key distribution is much slower than that of the software-based key distribution. The security proof of this scheme is yet an open problem.

Keywords: information theoretic security, secure key, one-time-pad.

Unconditionally secure physical key distribution requires specific physical systems, either a quantum system, such as quantum key distribution (QKD) [1] or a classical physical system such as the Kirchhoff-law-Johnson-noise (KLJN) protocol [2-5]. The common characteristic of these systems is that the speed of key exchange when it is undoubtedly unconditionally secure is slow. Thus it is practically impossible to use Shannon's one-time-pad based cipher to guarantee perfect security because using the key bits more than one occasion gives out statistical information such as via the known-plain-text-attack or by utilizing known components of the protocol and language statistics. Here we outline a protocol that seems to reduce this problem and allows a near-to-one-time-pad based communication with unconditionally secure physical key of finite length.

Our goal is to make it difficult to use statistics to identify an unconditionally secure physically distributed key even when it is used for a long time. The core protocol is as follows:

i) First we share a physical hardware based key HBK with an unconditionally secure physical key exchange protocol. If necessary, we make it very clean by privacy amplification of the simplest XOR-type [6] (that does not introduce correlations between bits). For example, KLJN has astronomically low error probability [5] thus it is very favorable for this type of privacy amplification. The resulting hardware based key HBK of length N is virtually perfectly secure.

ii) Then we use Diffie-Hellman-Merkle [7] or other known-plain-text-free, one-way-function method to generate a software based key SBK with length $M>>N$. The trick is that, for the communications making the SBK, we use encryption with a cypher that is using the HBK distilled earlier. *Thus the software-based key is generated via a secure communication*.

iii) These software-based methods communicate with spontaneously generated random numbers, which were unknown earlier, and their combinations. If the communicated random numbers were independent then the resulting SBK key would be perfectly secure. However there are algorithmic relations between some of them (the critical ones are hard to invert, such as on-way functions, etc.), depending on the protocol, thus theoretically there is some information leak about the process. However it seems, it is extremely difficult for Eve to extract useful information because, due to the secure communication protocol that is used for the software-based key exchange, she does not have a clue about the numbers used; not even about those that are public knowledge in the regular software-based key exchange methods. For example, in the Diffie-Hellman-Merkle protocol [7] used in this new way, Eve will be unaware of even the first random prime number that Alice and Bob would publicly select in the regular Diffie-Hellman-Merkle method. Here the whole process is encrypted by using the secure HBK.

Thus even if Eve were able to do efficient prime number factoring (by an hypothetical algorithm, a proper quantum computer or a noise-based logic engine), she does not have the numbers to start with because they are all encrypted. To extract information about the resulting SBK is a much more difficult task than to crack the classical Diffie-Hellman-Merkle key, because even hypothetically efficient integer factoring engines would be insufficient due to the lack of input data.

iv) For data communications, if possible, we use the SBK as a one-time pad. Or if higher speed is needed, a finitely long SBK with $M>>N$.

This combined physical/software key distribution based communication looks favorable compared to the physical key based communication when the speed of the physical key distribution is much slower than that of the software-based key distribution.

The security proof of this scheme is an open problem. For example, what is the *M* (>>*N*) value where the brute force attempt to crack the original HBK becomes less favorable than possible algorithmic methods?

References

1. Horace P. Yuen, "Simple explanation on why QKD keys have not been proved secure", http://arxiv.org/abs/1408.4780 (2014).
2. L.B. Kish, C.G. Granqvist, "On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator", *Quantum Information Processing* (2014), in press; DOI: 10.1007/s11128-014-0729-7 . http://arxiv.org/abs/1309.4112 ; http://vixra.org/abs/1309.0106
3. L.B. Kish, "Totally Secure Classical Communication Utilizing Johnson (-like) Noise and Kirchoff's Law", *Phys. Lett. A* **352** (2006) 178–182
4. R. Mingesz, Z. Gingl, and L.B. Kish, "Johnson (-like) -noise–Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line", *Phys. Lett. A* **372** (2008) 978–984.
5. Y. Saez, L.B. Kish, "Errors and Their Mitigation at the Kirchhoff-Law-Johnson-Noise Secure Key Exchange", *PLoS ONE* **8** (2013) e81103.
6. T. Horvath, L.B. Kish, J. Scheuer, "Effective Privacy Amplification for Secure Classical Communications", *EPL* **94** (2011 April) 28002-p1-p6 ; http://arxiv.org/abs/1101.4264
7. M.E. Hellman, B.W. Diffie, and R.C. Merkle, "Cryptographic apparatus and method", U.S. Patent #4,200,770, 29 April 1980. http://www.google.com/patents/US4200770