Position-based cryptography by means of quantum and classical schemes, using multiple-valued logic computing

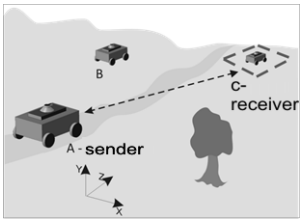
Alexey Yu. Bykovsky

Lebedev Physical Institute of the Russian Academy of Sciences, 119333 Moscow, Russia

Abstract. Quantum and classical schemes of position-based cryprography are to transfer confidential message to an abonent with localised space position. Known verification proceedures are based on time-delay measurements of response signals and can`t provide unconditional security, as the eavesdropper can always cheat verifiers with the help of false signals. In order to raise the relative level of security, it is proposed to combine the quantum verification scheme by D.Unruh with multiple-valued logic methods.

1. Introduction

The quantum key distribution (QKD) networks demonstrate the tendency to be integrated with network-centric and multiagent systems [1]. For successful design of such systems it is necessary to overcome many problems of classical cryptography but known methods of quantum cryptography can`t solve even such well known problems as the position-based cryptography, the random oracle and the bit commitment [2].

a) 

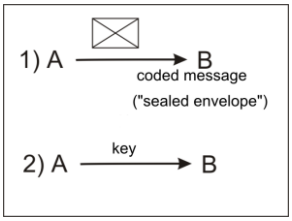
b) 

Fig. 1. a) The idea of position-based cryptography. b) The bit commitment scheme

Position verification methods, see Figure 1a), are well investigated for classical triangulation schemes in mobile telephone networks, where several verifiers jointly estimate the abonent location by measuring the time-delay response for test signals. Known classical and quantum schemes can`t obtain unconditional security [2,3], as the eavesdropper can always cheat the verifiers by installing additional sources of false signals between him and verifiers [2,3]. However D.Unruh in paper [3] has proved theoretically that his protocol based on random oracle scheme and EPR entangled photons source provides relatively greater security level. Here the random oracle is the black box, which provides ideally random output hash function,

which is always reproduced for any repeated query sent by any abonent and can`t be replaced by a random number generator.

The aim of this work is to enhance and to enlarge the position verification quantum protocol by D.Unruh [3] by classical schemes of multiple-valued logic data processing.

2. Route tracking check method for mobile abonents

The method is proposed to form both random and deterministic data arrays during the route passing by a mobile abonent *A*, see Figure 2. These data arrays are to proove the fact of sequentual visits of abonent A to check points B,C... . Random check data formation is produced by means of D.Unruh protocol [3] or (in simplified variant) by the hardware version of the random oracle, earlier proposed in [4]. These methods are to enhance the Unruh`s protocol [3], which is based only on measurements of time-delays for qubits and classical signals. Check points are to be equipped with EPR modules, which generate random data to be written simultaneously in A and control modules B,C... .

The bit commitment scheme, see Figure 1 b), was partially discussed in [1] can also be combined with the protocol [3] in order to prevent the application of false signals.

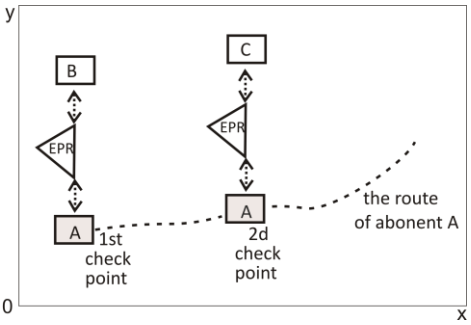


Fig. 2. The EPR **s**cheme for formation of random check data arrays during the ascent of the route, when mobile abonent *A* visits check points (*B*, *C*,...).

3. Multiple-valued logic digital map for the modelling of verification process

Multiple-valued logic (MVL) model of verification procedure in sec.2 is based on Allen - Givonne discrete algebra [1,4,5] with the number of logic levels of $k = 256$ and higher. The full set of non-Boolean operators include constants $C = \{1, \dots, k-1\}$ operators $MINIMUM(x_1, x_2)$, $MAXIMUM(x_1, x_2)$ and LITERAL $X(a, b)$. MVL multiparametric function can describe the whole route check proceedure as the truth table or the equivalent logic expression. MVL input variables can include not only spatial and time coordinates, but also wavelengths λ , time intervals Δt, radiofrequencies f and other parameters. The task here is to form complicated codes, partially resembling “hopping codes”.

References

1. A.Yu.Bykovsky, I.N. Kompanets, Quantum Electronics, **48**, 9, 777 (2018)
2. A. Broadbent et.al. Designs, Codes and Cryptography, **78**,1,351 (2016)
3. Unruh D. In Proc. of EUROCRYPT 2014,1 (2014)
4. A.Yu. Bykovsky, J. of Rus. Laser Res., **40**, 2,130 (2019)
5. A.L. Antipov, A.Yu. Bykovsky et.al., J. of Rus. Laser Res., **27**, 5, 492 (2006)