WSEAS TRANSACTIONS on COMMUNICATIONS , Issue 8, Volume 4, pp. 694-700, August 2005

Adaptive Encryption Protocols

Y. BAKOPOULOS, N. LYGEROS and A. DRIGAS
Department of Applied Technologies
NCSR "DEMOKRITOS"
Ag. Paraskevi
GREECE
yannisbakopoulos@yahoo.com, dr@imm.demokritos.gr
http://imm.demokritos.gr

Abstract - Some new ideas are presented for the improvement of the known QKD protocols and their application to an Internet environment. The full automatization of a technological setup is considered, as a result of the property of most basic QKD protocols to have the appearance of step by step algorithmic procedures and thus to offer themselves to materialization as computer code applications. This is the basis for the creation of a computer network connecting various users to be developed, working as an expert system and making decisions on the best strategy to recognize and counter especially dangerous eavesdropper attacks. The use of robotic technology, knowledge based simulation of the most dangerous and complicated attacks, game theory and neuronal networks to make these decisions, permits the system to adapt its behavior in the face of adverse situations. An elementary example of adaptivity of QKD protocols, by the use of game theory, is given.

1. Introduction

Security on the Internet, in the form of encryption, is a big issue of today [1 – 40], in the days of prospective wireless communications, business transactions, e-learning, e-government, e-health etc. The application of QKD methods and protocols is a new arrival to the networks of today [2], [36], [37] (and references therein).

The authors have done work on Key Creation and Distribution both by classical methods (Chaotic Dynamic Systems Behavior for Random Number Generation) [1], [3], [4], [19], [38], [39], as well as in QKD applications [2], [3], [4].

A QKD protocol is essentially an algorithm, having a finite number of well defined logical steps. Most decisions, about the validity and security of each distributed key, about the quantity of information possibly obtained by potential eavesdroppers, about the interruption of the process and the repetition under better conditions, are based on straightforward numerical calculations. With the help of suitable hardware and software, all such processes may be made to work completely automatically, without the intervention of the human users, except to compose and send the messages as in ordinary e-mail.

Such an advance in the state of the art of QKD would be by itself welcome, since most users of the Internet are not and should not be concerned with quantum mechanics and the technology involved. The automatization, with the added simplicity, ease of use and speed offered along with traditional QKD security should be motivation enough for the idea to be worth to offer to today's security thirsty market.

The largest problem is that QKD protocols, being at this experimental stage rather complicated and cumbersome, relying on sophisticated and expensive photonics technology and offered to clients with little practical experience of their everyday application, are not yet by themselves too attractive for the Internet users. The situation is further complicated by the fact that most protocols so far, having been designed by experimental physicists, are not very well adapted to the peculiarities of the Internet applications (But see [36], [37]). From the point of view of network engineery, a one – to – one protocol like the ones offered today is not the ideal way to exploit the natural advantages of a large scale digital network environment, with its 'oblivious transfer' potentialities through infinitely many and usually unknown to third parties pathways for communicating information from one point to another, or the possibility of using 'proxies', 'decoys' or 'avatars' to break a message into parts and so propagate it through the labyrinth of the Internet with less probability of eavesdropping.

At this stage, the versatility and chaotic complexity of the Internet and the power of modern digital technology and 'know – how' have the most to offer, in terms of advantages in secure communication. During a real time transmission, the users may be faced with critical decisions on whether, when and how to utilize the potential

offered them by the Internet environment. They must act correctly and timely, in order to succeed in continuing, safely and seamlessly, their exchange of sensitive information and the risks involved. Such decision making must be based on concrete facts backed up by fully provable calculations, performed on line in real time. Thus the full automatization of the QKD protocol, using the aforementioned techniques, automatic control, robotic technology, game theory, knowledge based simulation of especially dangerous attacks [2], [36], [37], becomes essential. It is the only way in order to ensure that the decisions and countermeasures necessary for recognizing and countering specific dangerous attacks, so that the users' communications will be as seamlessly and smoothly continued as possible, without compromising either the security or the utility of the services traditionally offered by the Internet. More so if the extension and expansion of these services is to be realized as envisioned by the designers of the Information Society of tomorrow.

This paper is organized as follows: The concept of adaptivity in encryption protocols is described in Section 2. In Section 3 a specific example of adaptivity will be presented. Discussion and conclusions will be given in Section 4.

2. The Idea of an Adaptive Protocol

The basis for the new concept is the full automatization of an encryption protocol, as stated above.

The automatization process is easy to realize with state of the art technology. The idea is described in detail in [2] and utilized in a protocol proposed in [36]. The references in [2] describe a variety of protocols and the application of the idea is more or less the same in every case. It is the utilization and exploitation of the advantages such a setup offers for Internet use.

The next step is to take advantage of full automatization in order to create, install, test and apply in real situations, emergency security protocols, to guard against, discern, counter and eliminate any threats by illegitimate third parties attempting to eavesdrop, intrude and/or in any way disrupt the secure communication, compromise its integrity and obtain part of the protected information exchanged between legitimate users.

The way to satisfy, as best as possible, the above requirement is, as a start, to discover and utilize ways to discern any deviation of the communication characteristics and parameters. To this end, noise in the communication lines may be monitored and examined for variations in quality as well as quantity. Based on traditional methods developed for the detection of eavesdroppers in QKD protocols and further tests with the help of innovative techniques from information theory [12], methods for deciding whether or not there are eavesdroppers obtaining a significant amount of information and compromising the security of the encryption keys, decisions should be reached about the application or not of emergency procedures. These processes should be controlled automatically by the controlling system of the communication setup. The intervention of human users should become necessary in situations where the system decides to call them in for assistance or, at their own volition, for better control of an especially dangerous situation. To enable the controlling system to perform such complicated duties, the it must be enabled to carryout all necessary tests and mathematical calculations and in addition, to be trained as an expert system by the use of specially created simulations of the most dangerous attacks that might be used against it. Furthermore, the controlling system must be enabled to learn from everyday experience to discern new forms of attack, if possible even such as have never been encountered before, by discrepancies and abnormal variations in the communication routine. And it should be instructed as to the performance of tests and processes designed to trap prospective malevolent third parties inducing them to reveal themselves. To this purpose, methods such as dummy messages, line monitoring disguised as key distribution, use of selected very clear lines having been kept in reserve and many other methods offered in a large digital network environment may be utilized and applied by the automatic controlling system.

These methods are useful in increasing security and some or all of them may be applied in any situation, whether the clients are using a QKD protocol or even a traditional, but suitably designed communication protocol in the Internet.

Still this would not be an adaptive protocol.

The meaning of adaptability is that an adaptive protocol has the ability to face attacks dynamically rather than statically, by changing the setup parameters and procedures according to the nature of the attack. Its methodology has to do with the plurality of potential solutions a system may be faced with, trying to decide how to cope with a dangerous attack. It is easier perhaps to discern the attack and notify human users or stop communications. But it is much more difficult to discover and apply a strategy by which to carry on the communication by neutralizing the attack and

trapping its initiators by inducing them to unknowingly accept false and useless information which presents no danger to the security of the protocol. In order to succeed in such a scheme, certain facts must be taken into account about the environment of the Internet.

The fundamental facts are the following: Strangely enough, the Internet is considered to be a very unsafe environment for secure services. Especially so, if the services are offered by wireless communication, where, by common wisdom, "everybody can and will listen in" to what others are saying or doing, and act on what he listens to, to his benefit and to the detriment of legitimate users. It seems that the simple fact that one has to know "where" to listen and "what" to listen for, if one is to make any sense out of the chaos of Internet communications, escapes the traditional mind. If the potential eavesdropper is to eavesdrop at all, he must know beforehand the exact line of communication and use the appropriate attack to intrude upon it. It is here that an adaptive protocol may use the whole potential offered to elude and frustrate the opposition and maintain communication integrity, by making the necessary decisions and minimizing the information available to the eavesdropper to the point where it is essentially useless. The weapons of the defender's arsenal are to change the route or routes of information transfer, making it almost impossible for the eavesdropper to trace it. To break it down to many parts communicated by different routes and modes, so that it will be impossible for the eavesdroppers to get it all. To use proxies, decoy messages of indifferent content, using various obsolete and useless keys, effectively 'spamming' the opposition by the huge volume of nonessential traffic the illegitimate intruders will have to process in order to find the usable content of the real messages. To make use of 'security islands' like the well known Intranet groups within the Internet so that in their collaboration with other distant groups they will extend their security where desired. By depriving the eavesdroppers of any indication of what exactly goes to whom exactly, a user in any form or capacity will be able to supplement his defense arsenal with the formidable weapons of deception and elusion.

All this decision making goes beyond the simple 'continue or abort?' question of a typical QKD protocol. It is essential that the decisions are based on solid facts and are being made in split – second real time, in order for them to be effective. The theory and technology in this decision making must be based on realistic and complete information on the methods and protocols of attack, something that may only be ensured by proper preparation. So it will be essential for the computer systems realizing the adaptive protocol, the 'controllers' of [2], to have the expert ability to recognize the form and danger of the attack and have solid criteria on how to counter it. This may be achieved by the extensive use of detailed simulations, so that the expert systems included in the controller network will be able to be taught beforehand of the various forms of attacks and to be able to learn from experience during everyday routine use and even training in new attack methods as they appear.

This seems the only way to secure communications and business transactions through the Internet. It also seems obvious that a long way is to be traversed if the adaptive protocols are to have a practical application in the foreseeable future. The authors are very hopeful in this direction, considering it an essential part of the Internet of the future [40].

It should be stressed here that a really successful adaptive protocol should combine all the above properties concerning security in the maximum possible degree. But on the other hand the speed and the ease of use of everyday communications should not be compromised. It is the authors' opinion that a secure communication protocol, based on the concept of virtual encryption devices [2 – 4], [19], [39], [40] (also see [5`- 11], [13 – 15], [17], [18], [21 - 29]), with a suitable QKD protocol to be used for initiation of communication and introduction of new users, as well as restarting communications in cases of emergency interruptions and for lines checking and monitoring should be ideal for the application.

Further care should be taken to avoid security compromises by actual intrusions and the utilization of security methods based on various parts of the setup [31], [35].

3. A Mathematical Example of Adaptivity

One of the mathematical tools for the creation of an adaptive protocol is game theory. It should be useful in situations where decisions must be taken to make the best of a situation when it is not clear whether the eavesdroppers might obtain a dangerous amount of information.

In the clear cut world of theoretical study, where the premises of a given situation are well recognized and defined, a 'secure' line is either secure or not, depending on very straightforward statistical tests. The users take for granted that the eavesdropper have the ability to listen in on any public line and assume beforehand that the line 'noise' is totally due to eavesdroppers. So, typically, a QKD protocol is

designed to ensure that the eavesdroppers will be discovered if the information they gain from the line exceeds a certain limit. In fact, the existence of lossy lines and detector noise and losses make the facts a little less clear. There certainly will be a 'gray zone', where the issue is not certain either way. The noise might be eavesdroppers, or not. The information lost due to this noise benefited the eavesdroppers, or not. There are times when the simple answer 'when in doubt abort the attempt and retry' simply doesn't apply.

Furthermore, it is assumed that the eavesdroppers have the ability to monitor any line the legitimate users might have available to them. This may seem logical in a 'one to one' communication, with the legitimate users having a limited number of lines at their disposal. But in an Internet environment and a setup as discussed in [37], the lines available to a pair of legitimate users are so many that it is unreasonable that an eavesdropper will monitor all of them in conjunction with the QKD protocol applied by the specific pair of users. So, as a simple example, it is assumed that Alice and Bob have at their disposal two public lines for the application of their QKD protocol. They know that both these lines are noisy. They have measured the amount of information lost when they apply their protocol and, by repeated tests, have calculated the losses to be I_1 for line 1 and I_2 for line 2 respectively. Both values are percentages of the total information transmitted for key distribution, having numerical values between 0 and1. These values are assumed to be in the 'grey zone'. The users further assume that a potential eavesdropper may not monitor both lines simultaneously, but only one at a time. Taking these premises into account, they are to try and make the best out of a dubious situation.

Let p be the probability that Alice and Bob use line 1. Then the probability that they use line 2 is $1-p$. Similarly, let q be the probability that Eve, the eavesdropper, is eavesdropping on line 1 and $1-q$ the probability that she is eavesdropping on line2. Also let I be the total percentage of information that Eve may obtain. The Equation describing the situation is:

(1): $I = pqI_1 + (1-p)(1-q)I_2$

In order to find maxima and minima of I, the derivative with respect to q must be taken.

(2): $\frac{\partial I}{\partial q} = pI_1 - (1-p)I_2 = p(I_1 + I_2) - I_2$

Finally:

(3): $\frac{\partial I_1}{\partial q} = 0$ a $\quad p = \frac{I_2}{(I_1 + I_2)}$

Then:

(4):

$$I = \frac{I_2}{(I_1 + I_2)} qI_1 + (1 - \frac{I_2}{(I_1 + I_2)})I_2(1-q) = \frac{I_1 I_2}{(I_1 + I_2)}$$

So, I at that point will be independent of q.

In fact, the 3-D plot of I as a function of p and q is a hyperboloid surface (Fig. 1). It is generated by a straight line generator, moving with the straight lines AB and CD as guides, where:

A = ($p = 0$, $q = 0$), B = ($p = 1$, $q = 0$), C = ($p = 0$, $q = 1$), D = ($p = 1$, $q = 1$)

The straight line segment KL, where $p = \frac{I_2}{(I_1 + I_2)}$ and q ε [0, 1], as well as the straight line MN where p ε [0, 1] and $q = \frac{I_2}{(I_1 + I_2)}$ are the intersection of the surface defined by:

$I = pqI_1 + (1-p)(1-q)I_2$

and the plane:

$I = \frac{I_1 I_2}{(I_1 + I_2)}$

Parallel to the p q plane.

The line: $p = \frac{I_2}{(I_1 + I_2)}$, q ε [0, 1] is a line of maxima for every q value, as q varies from 0 to 1. On the other hand, the line: $q = \frac{I_2}{(I_1 + I_2)}$, p ε [0, 1], is a line of minima, as p varies from 0 to 1. The point $p = \frac{I_2}{(I_1 + I_2)}$, $q = \frac{I_2}{(I_1 + I_2)}$ is, therefore, a saddle point. It is the optimum value for both players to seek, the maximum of all minima. If Alice sticks to this strategy and Eve doesn't, Eve will still get the information percentage:

$I = \frac{I_1 I_2}{(I_1 + I_2)}$.

And no more. The same is true if Eve holds on to $q = \frac{I_2}{(I_1 + I_2)}$. Again, whatever Alice does, Eve will get the percentage $I = \frac{I_1 I_2}{(I_1 + I_2)}$. If, on the other hand, both Alice and Eve do not stick to this strategy, they may benefit or loose, in comparison to

this standard value. Since the benefits are not guaranteed, the wisest move is to play it safe and follow the secure strategy.

This way, the information $I = \frac{I_1 I_2}{(I_1 + I_2)} < I_1$ or I_2 that Eve gets is significantly less than what she would get from a straightforward application of communications through the best available line. This simple example demonstrates the principles and the advantages of adaptive protocols. The mathematical method developed here may obviously be generalized for any number of lines, however large, in a more realistic application scenario.

4. Conclusions

In this work, a presentation of the concepts of adaptivity and adaptive protocols is given. An elementary example of game theory application in an adaptive protocol was described. By the use of such methods an adaptive protocol, ideally combining virtual encryption devices, backed up by an automatically controlled QKD protocol, in the sense meant in the above Section 2, the system will stand up against dangerous attacks in a dynamic rather than a static mode of defense.

Acknowledgements

The authors are grateful.to S. Kouremenos, S. Domoxoudis, L. Koukianakis and Y. Loukidis for discussions and suggestions on the functions of the Internet and valuable help.

5. References

[1] Yannis Bakopoulos, 'Application of Dynamic Systems for Cryptographic Key Distribution' *15th Congress on Nonlinear Dynamics*, *Chaos and Complexity* Patras Aug. 19 – 30, 2002 (A. Bountis ed.)

[2] Yannis Bakopoulos, Yannis Vrettaros, Athanasios Drigas, 'An automatic process for the reliable and secure creation and distribution of quantum keys' *National Patent No 1003891*, OBI, 2002.

[3] Yannis Bakopoulos, Vassiliki Soulioti, 'A protocol for secure communication in digital networks' *National Patent No 1004308*, OBI, 2003;

[4] Yannis Bakopoulos, Vassiliki Soulioti, 'A protocol for secure communication in digital networks' *PCT/GR 03/ 00035* 2003

[5] L. O Chua. and T.Lin, (!988) *IEEE Trans. CAS 35*, pp. 648 – 658.

[6] Robert L Devaney, *Physica 10D* (1984), pp. 387-393.

[7] O. Feely and L. O. Chua 'Nonlinear Dynamics of a class of analog - to - digital converters', *Int. J. Bifurcation and Chaos*, Vol. 2, 1992, pp. 325 – 340.

[8] Orla Feely "Nonlinear Dynamics and Chaos in Sigma – Delta Modulation", *Journal of the Franklin Institute*, Vol. 331B, No. 6, 1995 pp. 903 – 936.

[9] Orla Feely 'Nonlinear Dynamics of Chaotic Double-Loop Sigma Delta Modulation', *ISCAS*, 1994: pp.101-104

[10] T Habutsu. et al. 'A secret key cryptosystem by iterating a chaotic map' *International Conference on the Theory and Application of Cryptographic Techniques*, Springer Verlag, DE pp 127 – 140, XP000607774

[11] Leo P. Kadanov, and Chao Tang, Proc. *Natl. Acad. Sci*., USA Vol. 81, pp. 1276 – 1279, February 1984, Physics.

[12] K. Karamanos "Entropy analysis of substitutive sequences revisited" *J. Phys. A, Math. Gen*., 34, (2001) 9231 – 9241.

[13] Stelios Kotsios and Orla Feely, *NDES Congress Spain*, '96.

[14] Stelios Kotsios and Orla Feely 'The model – matching problemfor a special class of discrete systems with discontinuity', *IMA Journal of Mathematical Control & Information*, (1998) Vol. 15, pp 93 – 104

[15] Stelios Kotsios 2000 *Nonlinear Dynamics 22*, pp.175 – 191 (and refs therein)

[16] George Marsaglia "A Current View of Random Generators" Keynote Address, Computer Sciense and Statistics: *16th Symposium on the Interface*, Atlanta, 1984 (It appeared in "The Proceedings" of the Conference, published by Elsevier Press).

[17] S. Papadimitriou, A. Bezerianos, T. Bountis, G. Pavlides, "Secure Communication protocols with discrete nonlinear chaotic maps", *Journal of Systems Architecture*, Vol. 47, No 1, 2001, pp. 61 – 72.

[18] James Rössler et al., *PHYSICAL REVIEW A*, VOLUME 39, NUMBER 11, JUNE 1 1989, pp.5954 – 5960.

[19] V. Soulioti 'A study on Discrete Dynamic Systems with a linear part and discontnuity', *15th Congress on Nonlinear Dynamics, Chaos and Complexity*, Patras Aug. 19 – 30, 2002 (A. Bountis ed.)

[20] Richard J. Hughes et al 'Method and apparatus for free space quantum key

distribution in daylight' *US 2001/055389*, December 27, 2001.

[21] Yuan et al 'Method and system for establishing a cryptographic key agreement using linear protocols', *US 5 966 444*, Oct. 12 1999

[22] Tohru Kohda et al 'Enciphering/Deciphering apparatus and method incorporating random variable and keystream generation' *USPatent 6 014 445*, Jan 11, 2002.

[23] L. O. Chua and T. Lin, 'Chaos in digital filters', *IEEE Trans. Circuits and Systems*, Vol 35, pp. 648-658 (1988).

[24] L.O. Chua and T. Lin, 'Fractal patern of second order non-linear digital filters: Anew symbolic analysis', *International Journal of Circuit theory and Applications*, Vol. 18, pp. 541-550, (1990).

[25] L.O. Chua and T. Lin, 'Chaos and fractals from 3rd order digital filters', *International Journal of Circuit theory and Applications*, Vol. 18, pp. 241-255, (1990).

[26] Zbigniew Galias and Maciej J. Orgozalec, 'On symbolic dynamics of a chaotic second-order digital filter', *International Journal of Circuit theory and Applications*, Vol. 31, pp. 401-409, (1992).

[27] Zbigniew Galias and Maciej J. Orgozalec, 'Bifurcation phenomena in second-order digital filter with saturation-type adder overflow characteristics', *IEEE Transactions on Circuits and Systems*, Vol. 37, No 8, pp.1068-1070, (1990)

[28] Chai Wah Wu and Leon o. Chua, 'Symbolic dynamics of piecewise-linear maps', *IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing*, Vol. 41, No 6, (1994).

[29] Chai Wah Wu and Leon o. Chua, 'Properties of admissible symbolic sequences in a second order digital filter with overflow non-linearity', *International Journal of Circuit theory and Applications*, Vol. 21, pp. 299-307, (1993).

[30] A. Ammar, A. S. S. El – Kabbany, M. I. Youssef and A. Emam, 'A Novel Secure Image Ciphering Technique

[31] Stamatios V. Kartalopoulos Secure Optical Links in the Next Generation DWDM Optical Networks, *WSEAS TRANSACTIONS. on COMMUNICATIONS*. Issue 2, Volume 3, April 2004. ISSN 1109-2742

[32] Chandra B. Panday and Nikos Mastorakis, "Secure Protocols for Variety Cash Transactions", *WSEAS Transactions on Computers*, Issue 1, Volume 3, October 2002, pp.195-200, WSEAS Trans. on Communications, April 2004

[33] Nikolaos Bardis, Echoplex Error Control System Using Avalanche Transformations, *WSEAS Trans. on Communications*, April 2004

[34] N.G. Bardis, A.P. Markovskyy, M. Mitrouli, A. Polymenopoulos, Methods for Design of Balanced Boolean Functions Satisfying Strict Avalanche Criterion (SAC), *WSEAS Trans. on Communications*, April 2004

[35] Chih-Ta Lin, Hira Sathu and Donald Joyce Network Security of Wireless LANs in Auckland's Central Business District *WSEAS Trans. on Communications*, April 2004

[36] Nikolaos Papadakos, Quantum Information Theory and Applications to Quantum Cryptography, *arXive: quant – ph/ 0201057* v1 (2002)

[37] Inventor:TOWNSEND, PAUL DAVID. (GB). *Patent Number: US5953421*, Date: 14 Sept. 1999, Applicant: BRITISH TELECOM (GB).

[38] OUR NEW PATENT

[39] Soulioti, Y. Bakopoulos, S. Kouremenos, Y. Vrettaros, S. Nikolopoulos, A. Drigas, "Stream ciphers created by a Discrete Dynamic System for application in the Internet., *WSEAS TRANSACTIONS ON COMMUNICATIONS*, Issue 2, Vol. 3, April 2004 p.679-687.

[40] Vouliagmeni, December 2004

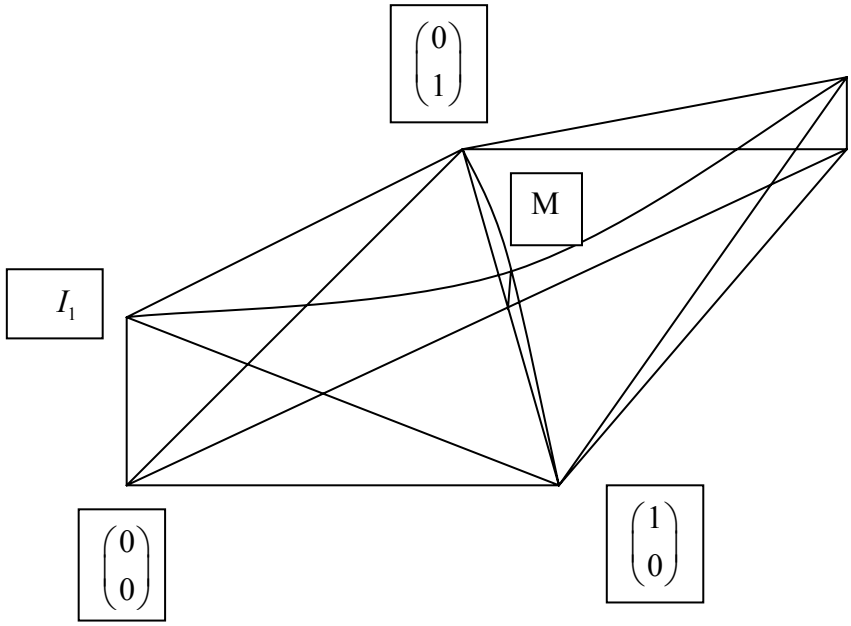
$\begin{pmatrix}0\\1\end{pmatrix}$
I_2
M
$\begin{pmatrix}1\\1\end{pmatrix}$
I_1
$\begin{pmatrix}0\\0\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$

Fig. 1