UDC 004.312.26

YE.TS. ALAVERDYAN, H.V. KERAMAT

REINFORCEMENT OF PUBLIC KEY ENCRYPTION USING MULTI-LEVEL DATA TRANSMISSION

The paper presents three main resolutions in secure data communication, namely, deprivation of hackers from their holistic knowledge over the digital network systems; postulating a numerical base, different from binary, achieving a block cipher system by manipulating high radix blocks and making it quite confounded for the intruders; ensuring an obvious fast speed than the average transfers of data over the net. An algorithmic implementation for the proposed resolutions is also given.

Keywords: block cipher, public key encryption, one-way function, multi-level data.

Analog systems for telecommunication which function with no specific numerical bases used to carry out complicated operations while they face obsolescence issues nowadays. All of them have almost been vanished and were promoted to faster digital systems. On the other hand, cyber security has been weakened since the release of computer networks, and the knowledge over these environments have significantly advanced. Speed also had its own obstacles and was confined to the current digital logics. Since the advent of cyber era, the digital systems have often been promoted to higher numerical bases.

Imperatives for switching to digital systems are not the same imperatives that led us to such an initiative. In previous decades many techniques were provisioned to enforce good security but such attempts were mainly software-based. The unsatisfying issues emerging out of them did not provide any guarantee of cyber security status quo. Any software working with a private key and public key might only be temporarily protected and these ad hoc interim works could not be an endorsement to the end user's security. Here are some examples of cyber-attacks: Farewell Dossier 1982 pipeline explosions in the USSR, and the second in late April 2007, In Estonia [1]; computer attack on the Georgian websites on 29 July, when some of the country's prominent websites were defaced, particularly, the Georgia's National Bank and the Ministry of Foreign Affairs [2].

According to Andrew M. Odlyzko (1984), one of the best-known public-key cryptosystems, the basic Merkle-Hellman additive trapdoor knapsack, was recently shown by Shamir to be easy to break. Subsequently, Adleman proposed attacks on the Graham-Shamir scheme and on the multiply iterated Merkle-Hellman system. Adleman's attack on the multiply iterated knapsack systems does not seem to succeed, but other attacks on the doubly iterated knapsack schemes have been proposed, also attacks on the low-density knapsack cryptosystems were attempted too [3].

The paper presents a method to increase the stability of encryption systems [4] via a multilevel data transmission using a ternary base as a model for laboratory hardware implementation. As the laboratory results succeeded, the overall project could be promoted to even higher numerical bases. Meanwhile cryptographic protection of information used knapsack and one-way function encryption techniques to prove the amount of power that the proposed project maintained in order to be able to stabilize knapsack encryption system.

Consolidating our security by mixing the most advanced methods like "working with memory instead of Hard Disk" principle, along with the proposed dynamic high radix block cipher and utilization of optical science, will rectify the number of threats. Such an approach would be an anti-attack set in the ad hoc configuration and an appropriate base of computations to better protect the users from intruders while data are being transferred over the network.

The project also aims at reinforcing the private keys by embedding them inside the apparatus. All the manipulations of individual units of our high radix were only to make the intruder confounded about the encrypted information. The proposed method exploits multilevel data transmission to manipulate the individual units to scramble the message. For instance, if we have six beams of light to transfer the data, we achieve a 64 numerical base. One good paradigm is to promote the binary level to 256 in order to provide a space for duplicate characters and make unique high radix blocks. With such a configuration, a simple permutation will lead to n! (Here n stands for the number of characters in high radix blocks), whereas at the binary level, it led to $\frac{n!}{n_1!*n_2!}$ where n_0 and n_1 stand for numbers of duplicates of 0s and 1s in a binary block, respectively.

The project is an adherence to regular digital systems, and has been proven in successful ternary transmission in National Instrument's laboratory. MyDAQ controller was used as a supplementary state of the art apparatus. It is worth to note that the proposed system will be best benefited to database systems run over the fiber optics. It can be as large as a WAN network or confined to the scope of a LAN network. Basically the modern circuit technology of National Instrument controllers and the dramatic design of fiber optics make it possible to transfer data from city to city confidently. Small ICs and high radix routers are the additional appliances to the system.

Data Representation. In the experience carried out, the ternary numerical base was postulated. Noting that Oracle database holds the data in hexadecimal numerical base in contrast to its physical binary regime, it will be an advantage to direct hexadecimal transmission of data with no extra computation for promotion of binary data.

What was used was to directly access the data from the computer's RAM via the USB port. DDR4 RAM actually has the performance of 0.63 nanoseconds and this is even abysmally smaller than the latest SSD Hard Disk performance [5]. Consequently HD is not involved in direct read and write while all manipulations are carried out inside RAM.

To handle such a work it was necessary to have two virtual functions, namely, replace the data from ASCII to ternary, and then turn the ternary data to a matrix of two bits formats while it is unneccary in situations where hexadecimal based databases are the case. Then the data was streamed out to a circuit elaborated by Labview software.

An ODBC connection made it possible to connect the circuit to the set up Oracle DB. The data then was read through an SQL command using virtual functions. The returned ternary data from the virtual function were split in two and placed in a matrix structure (see Figure1).

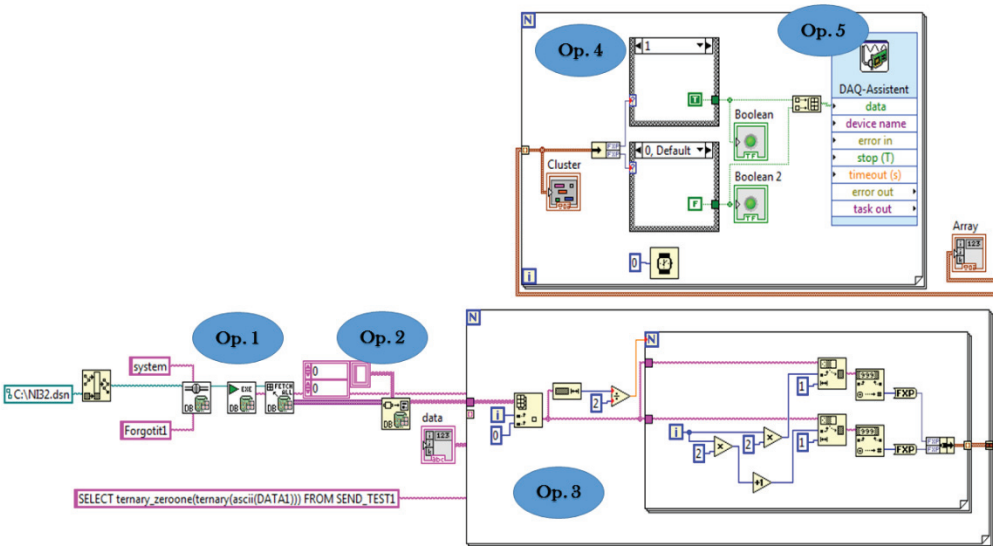

Fig. 1. Data sending apparatus

The details of Figure 1 can further be explained as 5 different operations. Operation 1 uses the standard ODBC connection to maintain a live connection to the database server. Operation 2 uses the database tools of Labview such as, 'Execute Query' and 'Fetch Query' and 'Data type conversion' to retrieve the high radix data from the database after the appropriate authentication. Operation 3 uses the 'Length calculator' to split the data in pairs as we chose ternary for feasibility study. The data then is split into pairs utilizing a loop while simultaneously converted into 'Fixed Point' numbers which makes it able to generate a cluster from the data (National

Instrument controller only uses clusters as inputs). Operation 4 receives the clusters as an array of clusters. While reading, each row of the cluster uses the 'Unbundle' to open up the pairs of each row. If it is one then 'true' is sent and if it is zero, - 'false'. Operation 5 uses the MyDAQ assistant to apply a controller and defines the output ports. The previously achieved results are sent to the controller.

In the laboratory experiment, mapping of '00','01','11' corresponds to '0','1','2', respectively. The MyDAQ controller receives the ternary data according to Figures 2. The details of Figure 2 can further be explained as two subsequent operations. Operation 1 uses myDAQ assistant to configure the receiving port or use the same sending port as the ports of fiber optic connection and it continuously listens to the outputs of photo diodes correspondingly arranged on the controller. Operation 2 receives the output as 'Array of Cluster' from the controller and uses 'Delete rows' tool, first reads each row and then sends it to the 'Case' operation while removing the row. Using two algorithms of "Case" structure combined together, it discerns '0','1','2' from '00','01','11' based on the proposed mapping system. Subsequently the data is manipulated and inserted into the Oracle DB for further decryption purposes and then registered in a queue for further sequential executions.

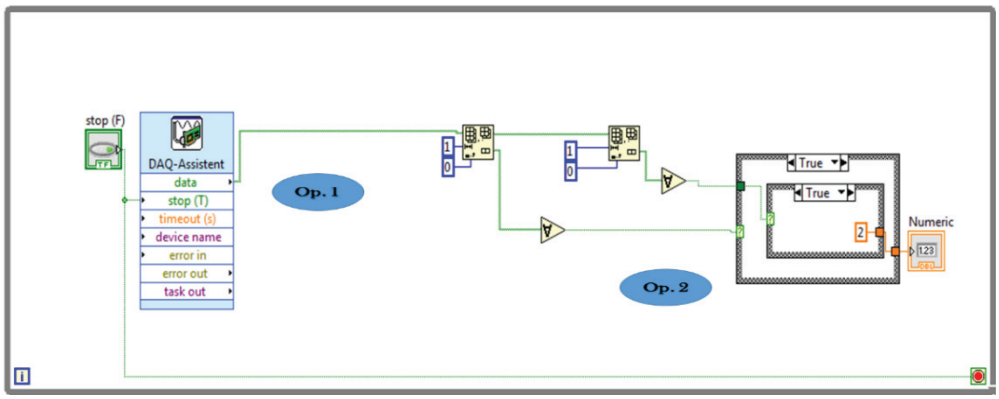

Fig. 2. Data receiving apparatus

This was a paradigm for defining ternary data while for other bases there is a need to involve optical computing in order to achieve frequency-differential optical telecommunication. For this purpose, wavelength division multiplexing technology is proposed to send multiple wavelengths through the same fiber (multiplexing and (de)multiplexing the optical signal on the fiber). Particularly, AWG (Arrayed waveguide grating) devices can be successfully applied for optical (de)multiplexing in wavelength division multiplexed (WDM) systems. A future work will be dedicated to the investigation of capacity and decoding error probability of the communication proposed.

Obtaining public and private key generation and appropriate distribution, the classical knapsack algorithm is applied for data encryption. In fact, reinforcement of the classical knapsack algorithm is implemented through application of multilevel data transmission obtained by modern data transmission techniques consisting of advanced apparatus and state of the art database's data transmission without the hard disk's unnecessary involvements. The project has taken a tougher stance on handling security problems using the proposed multilevel encryption techniques, compared to the previously known techniques.

REFERENCES

1. **Rid T.** Cyber War Will Not Take Place // Journal of Strategic Studies. – 2012.- Vol. 35, N 1. - P. 11.
2. **Rid T.** Cyber War Will Not Take Place // Journal of Strategic Studies. – 2012. - Vol. 35, N 1. - P. 12.
3. **Odlyzko Andrew M.** Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme // Information Theory, IEEE Transactions on. - 1984. - Vol. 30, N 4.
4. **Merkel and Hellman.** Hiding information and Signatures in trapdoors Knapsacks. // IEEE Transaction on Information Theory IT. – 1978. -24(5). - P. 525-530.
5. **Mueller S.** Upgrading and Repairing PCs (22nd Edition) // Que Publishing. – 2015. - 22 edition. Table 6.11.

Ե.Ծ. ԱԼԱՎԵՐԴՅԱՆ, Հ.Վ. ՔԵՐԱՄԱԹ

ԲԱՑ ԲԱՆԱԼԻԱՅԻՆ ԳԱՂՏՆԱԳՐՄԱՆ ԱՄՐԱՊՆԴՈՒՄԸ ԲԱԶՄԱՄԱԿԱՐԴԱԿ ՏՎՅԱԼՆԵՐԻ ՕԳՏԱԳՈՐԾՄԱՄԲ

Ներկայացնում են տվյալների անվտանգ փոխանակման երեք լուծումներ. դրանք են՝ զրկել հեներին թվային ցանցային համակարգերի վերաբերյալ գիտելիքների տիրապետումից, ներմուծել երկուականից տարբեր հիմնային համակարգ, իրականացնել մատրիցային գաղտնագրում՝ յոթչափանի զանգվածի բիթերի այլընտրանքային փոխատեղումների միջոցով՝ դարձնելով գաղտնագիրը հեների համար բավական շփոթեցնող, ինչպես նաև ապահովել ակնհայտորեն ավելի արագ հեռահաղորդակցություն, քան ցանցերում փոխանցումների միջին արագությունն է: Բերված են առաջարկված լուծումների ալգորիթմական իրականացումները:

Առանցքային բառեր. հատվածային գաղտնագիր, բաց բանալիային գաղտնագրում, գաղտնիքով միակողմանի ֆունկցիա, բազմամակարդակ տվյալներ:

Е.Ц. АЛАВЕРДЯН, Х.В. КЕРАМАТ

УКРЕПЛЕНИЕ ШИФРОВАНИЯ ОТКРЫТЫМ КЛЮЧОМ С ПРИМЕНЕНИЕМ МНОГОУРОВНЕВЫХ ДАННЫХ

Представлены три метода защищенного обмена данными, а именно: лишение хакеров их целостного знания цифровых сетевых систем; постулирование численной базы, отличной от двоичной, и достижение системы шифрования посредством матрицы перестановки битов размерности семь, при этом превращая ее в достаточно конфузную для злоумышленников; обеспечение очевидной высокой скорости, чем в среднем передача данных по сети. Приведена алгоритмическая реализация для предлагаемых резолюций.

Ключевые слова: блочный шифр, шифрование открытым ключом, односторонняя функция, многоуровневые данные.

ՀՏԴ 004.312.26:621.394.147.3

Ա.Ա. ԽԵՄՉՅԱՆ

ԳԱՂՏՆԻՔԻ ԲԱՇԽՄԱՆ ՇԵՄԱՅԻՆ ՍԽԵՄԱ՝ ՀԱՄԱՊԱՏԱՍԽԱՆ ՍԽԱԼՆԵՐ ՈՒՂՂՈՂ ՀԵՄՄԻՆԳԻ ԿՈԴԻՆ

Մշակված է գաղտնիքի բաշխման շեմային սխեմա, որի հիմքում ընկած է սխալներ ուղղող Հեմմինգի կոդը: Նկարագրված է Հեմմինգի կոդի այն մոդիֆիկացիան, որն օգտագործվել է բաշխման սխեմայում: Ներկայացված շեմային սխեման հարմար միջոց է մեծ ծավալի գաղտնի ինֆորմացիա բաշխելու համար, երբ կարևոր է նաև արագագործությունը: Ներկայացված են նոր և Շամիրի մեթոդների համեմատական գրաֆիկները:

Առանցքային բառեր. գաղտնիքի բաշխում, շեմային սխեմա, սխալներ ուղղող կոդեր, սխալներ հայտնաբերող կոդեր, Հեմմինգի կոդ:

Ներածություն: Ժամանակակից պայմաններում տվյալների փոխանակման զգալի մասն իրականացվում է գլոբալ բաց ցանցերի միջոցով, որոնցով փոխանցվում է մեծ ծավալիկարևոր տեղեկատվություն: Այս հարցի առանձնակի արդիականությունը պայմանավորված է էլեկտրոնային բիզնեսի զարգացմամբ և էլեկտրոնային փաստաթղթերի շրջանառությամբ: Այս ամենին զուգահեռ միշտ անհրաժեշտություն է առաջանում ապահովել բազմակողմանի տեղեկատվական անվտանգություն՝ գաղտնագրում, ցանցային պաշտպանություն, գաղտնի տեղեկատվության (գաղտնի բանալու) պաշտպանություն և այլն [1]: Ժամանակակից քոմփյութերները, հաշվարկների տեխնոլոգիաները հնարավոր դարձրին դեռ վերջերս գործնականորեն ապահով համարվող գաղտնագրային համակարգերի մեծամասնության կոտրումը: Տվյալների պաշտպանության ժամանակակից եղանակները հատկորոշում են անվտանգության “դիմացկունության կանոնները”, օրինակ՝ սպառողների սարքերում պաշտպանված տվյալներ ապահովելու համար: Ընդհանրապես այս կանոնները ենթադ-