Journal of Zhejiang University SCIENCE A
ISSN 1673-565X (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Improved Feistel-based ciphers for wireless sensor network security

Tamara PAZYNYUK, Jian-zhong LI, George S. OREKU‡

(*Department of Computer Science and Engineering, Harbin Institute of Technology, Harbin 150006, China*)

E-mail: tamara.mymail@gmail.com; lijzh@hit.edu.cn; gsoreku@yahoo.com

Received Dec. 7, 2007; revision accepted Mar. 5, 2008

Abstract: Wireless sensor networks (WSNs) are exposed to a variety of attacks. The quality and complexity of attacks are rising day by day. The proposed work aims at showing how the complexity of modern attacks is growing accordingly, leading to a similar rise in methods of resistance. Limitations in computational and battery power in sensor nodes are constraints on the diversity of security mechanisms. We must apply only suitable mechanisms to WSN where our approach was motivated by the application of an improved Feistel scheme. The modified accelerated-cipher design uses data-dependent permutations, and can be used for fast hardware, firmware, software and WSN encryption systems. The approach presented showed that ciphers using this approach are less likely to suffer intrusion of differential cryptanalysis than currently used popular WSN ciphers like DES, Camellia and so on.

Key words: Security, Cipher, Wireless sensor network (WSN), Feistel scheme
doi:10.1631/jzus.A0720108 **Document code:** A **CLC number:** TP309; TP393

INTRODUCTION

The goal of information security is to provide information safety and integrity (Karlof and Wagner, 2002; Saraogi, 2006). Information transfer through wireless sensor networks (WSNs) needs to be protected from misuse. Modern security methods need to guarantee the safety of data transmission with respect to security needs, i.e., confidentiality, integrity, and availability (CIA). Providing information security in WSN is also necessary especially for those security-sensitive applications and is one of the major concerns of our proposal. There are many countermeasure methods that have been extensively studied to provide WSN communication security (Rasool and Guo, 2004; Hu *et al.*, 2004; Saraogi, 2006; Mauw *et al*., 2006). However, WSN is still exposed to some kinds of attacks as can be seen in (Hu *et al*., 2004; Mauw *et al*., 2006; Kumar *et al*., 2006). These defenses are ineffective against attacks from compromised servers due to the WSN level constantly increasing, and attacks are becoming more and more complicated, as presented in (Karlof and Wagner, 2002; Hu *et al*., 2004; Kumar *et al*., 2006). Moreover WSN has some restrictions when it comes to its applications, like limited power supplies, low bandwidth, small memory sizes and limited energy, which make it more vulnerable (Bilstrup *et al*., 2003). And as information becomes more valuable and costly, intruders use more complicated methods in attacking WSN, this eventually makes the security issue highly sensitive. Due to the increase in new trends of attack, previous security methods cannot combat or resist modern attacks. We present additional steps to create efficient security mechanisms for WSN, with limited resources.

Our study shows that new and more stable security approaches need to be put in place to provide information safety taking into consideration the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation. We propose to use a modified accelerated-cipher using permuta-

‡ Corresponding author

tions presented as a cryptographic primitive approach for WSN. The concept of 'data-dependent permutation' (DDP) is an approach used in many information security systems today (Moldovyan *et al*., 2005; 2007; Moldovyan and Moldovyan, 2007). Confronting the key challenges, we follow this approach by using a Feistel scheme approach to present our improved cipher block using DDP. By cryptanalysis realization, it is necessary to consider differential and linear properties of individual round transformation of crypto primitives of block ciphers. This method allows us to create more stable secure mechanisms against modern types of attacks and also to provide a highly accelerated security program within small sensor devices. In this paper we use a controlled permutation boxes based method for block cipher implementation to provide a modified stable cipher against modern crypto-attacks such as differential cryptanalysis in WSN. The proposed cipher has free key preprocessing which provides high performance in frequent keys exchange. In our work we show the effectiveness of using DDP in cipher design for WSN. DDP-based ciphers demonstrate better experimental results than others.

ATTACK THREATS

Crypto attack methods are very complicated. They combine mathematics, information science and even electronics with unusual thinking. WSN block cipher design needs to consider stability against analytical crypto-attacks. The practice in past years has shown us differential cryptanalysis (DCA) (Schneier, 1996) and linear cryptanalysis (LCA) (Biham and Shamir, 1996) where the most powerful analytical crypto analysis methods were used. The main content of DCA is the propagation analysis of the influence of modifications in the plaintext on the modification in cipher text (propagation properties). Using DCA as a method of complex attack with complicated mathematical methods can be one way of verifying the stability of block ciphers.

In the realization of block cipher cryptanalysis it is necessary to consider the differential and linear properties of individual round transformation crypto primitives of blocks. The cases are complicated to element addition on stable round transformation which sometimes might give negative results for a given cipher algorithm. Block cipher designers who are trying to use theoretical computing constructions that provided distinctness in the evaluation of block ciphers in modern cryptanalysis methods, should give consideration before putting all these into action (Matsui, 1994).

In spite of DCA and security precautions there are many more threats to new modern networks. One of the main challenges is the design of these networks and their vulnerability to security attacks, which leads to network destruction and poor performance. Every year the attack complexity increases as can be seen in Fig.1.

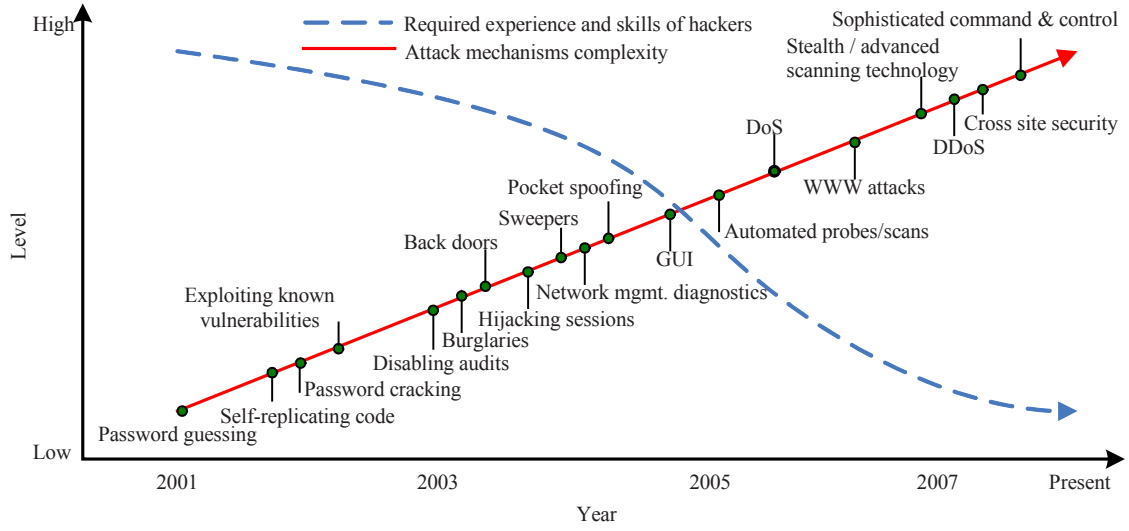

Fig.1 Advancement of the complexity level and mechanisms of the attacks and the evolvement of required experience and skills of the hacker

Fig.1 shows the advancement of the complexity level and mechanisms of the attacks and the evolvement of required experience and skills of the hacker. Every year not only are the quantity and complexity of new threats rapidly increasing but also their appearance and momentum. Resistance against them is becoming more and more complicated. The malicious are using more of these security vulnerabilities especially to attack WSN due to the weakness in wireless security.

EFFICIENCY OF EXISTING WSN ALGORITHMS

We outline briefly the drawbacks of existing algorithmic methods which are being used in many current technologies:

● Widespread algorithms (end to end, single destination communication, IP overlays);

● Probabilistic broadcasts (discrete effort: does not handle disconnection);

● Scalable reliable multicast (multicast over a wired network, latency-based suppression);

● SPIN (propagation protocol: does not address maintenance costs, as discussed in (Levis, 2005));

● Public-key cryptography (too expensive);

● Fast symmetric-key ciphers (must be used sparingly (Saraogi, 2006)).

On designing WSN protocol it is necessary to consider all specific features of WSN. For example, communication bandwidth is extremely limited in these networks: each bit transmitted consumes about as much power as executing 800~1000 operational instructions, and as a consequence, any message expansion caused by security mechanisms comes at a significant cost (Hill *et al*., 2000; Saraogi, 2006).

However, we present sets of requirements for WSN protocols indicated in (Levis, 2005). We use these requirements as the highlight in facilitating the design of our new improved cipher:

● Low maintenance overhead (Minimize communication when everyone is up to date);

● Rapid propagation (When new data appear, they should propagate quickly);

● Scalability (Protocol must operate in a wide range of densities, and cannot require *a priori* density information);

● Technical cryptanalysis stability (high-frequency influence of sensors with the purpose of information distortion. Some of the previous methods allow us to get the key's round value. Latest research shows that block ciphers are resistant to this kind of attack).

TECHNIQUES

The presented techniques are based on an original Feistel scheme which due to its significant properties can be used in WSN security applications. The modified Feistel scheme design can meet today's security challenges and generates high-quality results.

Feistel scheme

All of WSN's block ciphers are designed using a 16-round Feistel data block encoding scheme realized by two sub-blocks of data transformation using the round encoding function. Like many other symmetric block ciphers, DES is also a Feistel network (Schneier, 1996). In a Feistel network the plaintext is divided into two halves from the first round of computations which is repeated a number of times (i.e., in subsequent rounds). Generally the output of the *i*th round is determined from the output of the previous round in the following way:

$$L_i=R_{i-1}, \tag{1}$$

$$R_i=L_i\oplus F(R_{i-1}, k_i), \tag{2}$$

where $F()$ represents the round function; k_i is the key for the *i*th round; L_i and R_i are the left and right input data bits of the *i*th round, respectively.

The advantage of a Feistel scheme is that the block cipher used is very difficult to breach by proportional of one round key (2^m) enumeration (Moldovyan *et al*., 2007). So it is necessary to determine the requirements for one round cipher transformation during the Feistel scheme design. We briefly indicate below the essential design needs:

● Increase size of the transcriptive block to 128 bits and more;

● Increase the round key size;

● Provide round key elements inseparability within the limits of one algorithm round;

● Use the special methods which avoid mathematical and technical analysis especially the addition of some transformations at the beginning of the algorithm and after the last round.

Before implementing Feistel schemes to network security we would also like to analyze the pros and cons of this approach for a network as follows:

● Advantages of a Feistel approach to networks: (1) In a Feistel scheme we can encode and decode in one operation sequence. Encoding an algorithm modification is achieved by queuing a round of sub-keys using modification. (2) It minimizes software coding.

● Disadvantages of a Feistel approach to networks: (1) In a Feistel scheme we have two parts, left and right, but only one part of the block is used for coding in one round. For example, if the block on the right side (***R***) is used for the first time in coding, the second one on the left side (***L***) is only used for ex- changing places, and thus not all parts of the block are participating in the coding process. (2) Transfor- mation is very simple because the round function F depends only on two parameters (***L*** and round key K_i).

For understanding our presentation we give further destabilizations in this paragraph, giving a Feistel scheme (Fig.2) as one of the standards we elaborate in detail how a Feistel scheme works. The right part $\boldsymbol{R}'$ of transcriptive data $\boldsymbol{L}'\|\boldsymbol{R}'$ is a result of group operation XOR ($\oplus$), where F_{K_i} is a round function, i is a round quantity and K_i is a round key. $\boldsymbol{R}' = \boldsymbol{R} \oplus F_{K_i}(\boldsymbol{L})$. For more details about the Feistel scheme, interested readers are referred to (Feistel, 1973).

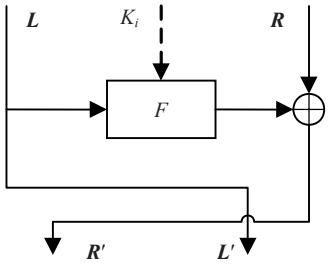

Fig.2 One round of the modified Feistel scheme

This Feistel scheme appeared long before modern crypto-attacks as the original cipher using a block structure. Its modified version is applied further to limited resource devices as well as embedded devices. From the original standard version it is seen that the unmodified version does not meet the new security requirement paradigm. The latest record in cracking DES (as of September, 1999), set by the Electronic Frontier Foundation's "Deep Crack", is 22 h and 15 min (RSA, 1999). It involved about 100 000 PCs on the Internet. It was performed as a 'known cipher text attack' based on a challenge from RSA Laboratories. The task was to find a 56-bit DES key for a given plaintext and a given cipher text. It is well demonstrated in Fig.1, that no matter how much security is installed in different places, every year attack trends are strongly on the increase in many computer applications. Taking a Feistel approach as a key to our methodology we present our modified version to meet the new attack challenges.

Theoretical approach of CPB to our methodology

In our work we propose to use controlled permutation boxes for implementation of a Feistel scheme design for WSN security. DDP can be performed with the so-called 'controlled permutation boxes' (CPBs) which are fast even if implemented in cheap hardware. CPB is one part of the comprehensive forthcoming start of controlled operations in security applications (Moldovyan *et al*., 2005).

The main content of this concept is to create substitution and permutation elements of block ciphers. They provide highly accelerated program realization nonlinear transformations with a small volume of modifications. These transformations are realized by the whole large size data block at once (32 and more bits) and are managed by transcriptive data and the algorithm's keys dynamically. CPB mechanisms and their implementation in block cipher methods provide high stability of such algorithms in modern crypto-attacks such as differential cryptanalysis (Moldovyan *et al*., 2007).

WSNs use the block-algorithm encryption for data transfer. The quality of these algorithms depends on indexes of binary information 'dispersion' and 'interfusion' which provide interchange of substitution and permutation transformations (Schneier, 1996). In the modern block ciphers these transformations are used by applying two types of crypto primitives:

(1) Special nonlinear S-box given at the table view. S-boxes provide a degree of nonlinearity for each block and a degree of error propagation. But the small size of S-boxes also makes it difficult for the encoding data block to achieve high indexes for the following parameters: nonlinearity degree, error propagation degree and guessing correlation level (Schneier, 1996).

(2) Standard arithmetic or algebraic operations realized with computer commands. Arithmetic operations are effective in software implementation and not complicated in hardware implementation. They have high correlation insusceptibility for all encoding blocks but a low degree of nonlinearity and error propagation.

This modern approach does not guarantee maximum security when using a Feistel scheme as it has some disadvantages. Attempting to solve this problem we employ controlled operations to make an important adaptation of controlled permutation boxes. Controlled operations are described as simpler operations 'multiples' that are selected depending on some controlling code. CPBs are an alternative to traditional S-boxes and common mathematical operations that generally use a block cipher synthesis (Moldovyan *et al*., 2007). Thus the availability of special crypto primitive creations is becoming obvious. These crypto primitives combine and optimize the advantages of block cipher substitution transformations.

An improved Feistel scheme for block data transformation

In this subsection we consider one round of a Feistel scheme with CPB (Fig.3a). In an improved scheme vector $\boldsymbol{R}'$ can be calculated as $\boldsymbol{R}'=G_U^{-1}(G_V(\boldsymbol{R}) \oplus F_{K_i}(\boldsymbol{L}))$, where G_V and G_U^{-1} are mutually inverse transformations and depend on control vectors $\boldsymbol{V}$ and $\boldsymbol{U}$, i.e., G_V, $\oplus$ and G_U^{-1} transformations are implemented in series. Generally, control vectors $\boldsymbol{V}$ and $\boldsymbol{U}$ are values of procedure E from two variables (Fig.3b): data block $\boldsymbol{L}$ and round key K_V (or K_U), i.e., $\boldsymbol{V}=E(\boldsymbol{L}, K_V)$ and $\boldsymbol{U}=E(\boldsymbol{L}, K_U)$. The highest possible unity number $\lambda_{\max}(\|\boldsymbol{A}'\|)$ for a given scheme is also $n^2/2+n/2$, but here independence between categories of output block $\boldsymbol{R}'$ is achieved much more easily. Two mutually inverse transformations G_V and G_U^{-1} are provided with the possibility of using one scheme for direct and inverse transformations, but the keying order is more complicated.

Fig.3 shows the main concept for implementing CPB in a Feistel scheme. In our work some ciphers based on CPB have been mentioned as well for later comparison in experimental performance. More detailed information about Cobra-F64a, Cobra-F64b and Spectr-H64 with Feistel characteristics can be found in (Goots *et al.*, 2001; Moldovyan, 2003; Bodrov *et al.*, 2005; Lu *et al*., 2006).

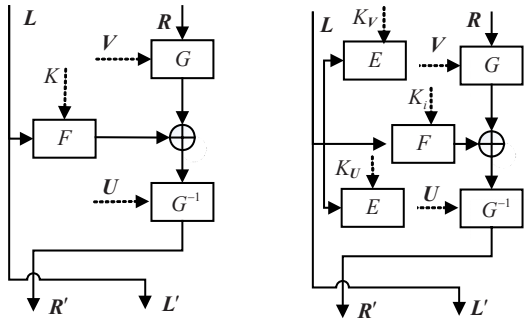

Fig.3 One round scheme of basic (a) and detailed (b) improved Feistel scheme

CPB-FEISTEL SCHEME BASED CIPHERS VS CIPHERS WITH NO CPB

An improved Feistel-scheme with different variations of DDP can be implemented in some encoded WSN algorithms, especially for effectiveness of hardware implementation and nature of its block ciphers which basically fits a packet structure that can be transmitted within WSN. In the case of embedded devices implementation, effectiveness can be achieved from Spectr and Cobra ciphers which are CPB based as well. They provide a performance of about 20 Mbps for microcontroller working at 30 MHz (Moldovyan and Moldovyan, 2007).

We ran an experiment and compared our improved Feistel scheme performance and its stability for data security in different versions of Feistel-based ciphers, i.e., Cobra-F64a, Cobra-F64b, Cobra-S128, Spectr-H64 (Moldovyan and Moldovyan, 2007), Camellia (Keliher, 2007) and DES (Rudolf, 2001) against differential cryptanalysis and we present our results in Table 1. Camellia and DES are examples of block-ciphers based on a traditional Feistel scheme. From Table 1 we can see that DDP-based ciphers have an increased security capability due to less probability of breaking when compared with differential cryptanalysis. Results obtained show that all considered ciphers are secure against differential crypto-attacks and that DDP-based ciphers perform better.

Table 1 Differential cryptanalysis security estimation comparison

Cipher scheme	N_{max}	N	p
Cobra-S128	12	2	2^{-32}
Cobra-F64a	16	3	2^{-21}
Spectr-H64	12	2	1.1×2^{-13}
Cobra-F64b	20	2	2^{-12}
Camellia	24	3	2^{-12}
DES	16	2	2^{-7}

N_{max}: the maximum number of rounds; N: the number of rounds; p: the probability of attack success

From our experiment we have made an evaluation based on the notion of a security margin (SM) on ciphers. This is for more clarification to clearly indicate the characteristics of different ciphers and to thwart their attacks. Using SM we can indicate that the higher the percentage the cipher shows, the more vulnerable it is to attacks.

We estimated SM as $SM=(N-N_{min})/N_{min}\times100\%$, where N_{min} is the minimum number of rounds that are sufficient to provide security against differential analysis, and N is the nominal number of rounds. N_{min} is defined by the block size, probability and number of rounds of the differential characteristics. The results show that for Cobra-S128, SM=50%; for Spectr-H64, SM=33%; for Camellia, SM=50%; and for DES, SM=77%. These results show that modified ciphers based on a Feistel scheme are less vulnerable to attacks when compared to DES or Camellia.

The comparison results show that there is a higher probability of a successful attack on DES when compared to our modified Feistel scheme. However, from Fig.4 we learn that there is less chance of a successful attack on modified Cobra-F64b, Spectr-H64, Cobra-F64a and Cobra-S128 ciphers.

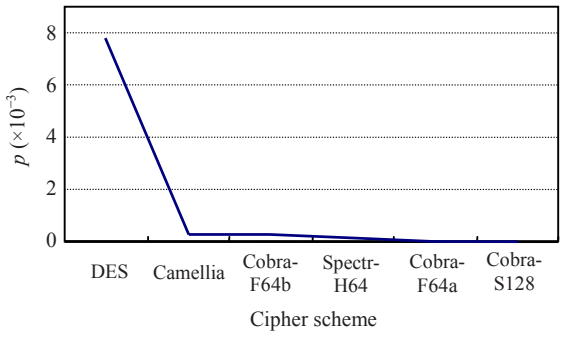

Fig.4 Cipher strength against attack success probability *p*

CONCLUSION

In this paper we have presented an advanced improved Feistel cipher based scheme which can be used in WSN block-cipher design for security by using CPB crypto primitives. Also we have shown how new generation attacks are increasing with time, becoming complicated and mitigating against WSN and other fields. In comparison our analysis verified that there is less probability of code breakage with a modified Feistel scheme.

Our study argues that there is a benefit in using an improved Feistel scheme for WSN security, as it is much easier to encrypt the data packet than to encrypt the data stream, which most of the encryption standards are being used for at present. However, an improved Feistel scheme can attain high and stable WSN security using block-ciphers compared to differential cryptanalysis. Due to the use of energy-efficient sensors, the security design of the modified ciphers is appropriate. This work serves as a notification and milestone in attracting more attention to WSN security and DDP-based block-cipher applications.

References

Biham, E., Shamir, A., 1993. Differential cryptanalysis of the full 16-round DES. *LNCS*, **740**:487-496.

Bilstrup, U., Sjoberg, K., Svensson, B., Wiberg, P.A., 2003. Capacity Limitations in Wireless Sensor Networks. Proc. 9th IEEE Int. Conf. on Emerging Technologies and Factory Automation, Lisbon, Portugal, p.529-536.

Bodrov, A.V., Moldovyan, A.A., Moldovyan, P.A., 2005. DDP-based ciphers: differential analysis of Spectr-H64. *Comput. Sci. J. Mold.*, **13**(3):268-291.

Feistel, H., 1973. Cryptography and computer privacy. *Sci. Am.*, **228**(5):15-23.

Goots, N.D., Moldovyan, A.A., Moldovyan, N.A., 2001. Fast encryption algorithm SPECTR-H64. *LNCS*, **2052**:275-286. [doi:10.1007/3-540-45116-1_27]

Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., Pister, K., 2000. System architecture directions for networked sensors. *ACM SIGPLAN Notices*, **35**(11):93-104. [doi:10.1145/356989.356998]

Hu, F., Ziobro, J., Tillett, J., Sharma, N.K., 2004. Secure wireless sensor networks: problems and solutions. *J. Syst., Cybern. Inf.*, **11**(9):419-439.

Karlof, C., Wagner, D., 2002. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Proc. 1st IEEE Int. Workshop on Sensor Network Protocols and Applications, Anchorage, Alaska, p.1-15.

Keliher, L., 2007. Toward provable security against differential and linear cryptanalysis for camellia and related ciphers. *Int. J. Network Secur.*, **5**(2):167-175.

Kumar, S., Valdez, R., Gomez, O., Bose, S., 2006. Survivability Evaluation of Wireless Sensor Network under DDoS Attack. ICN/ICONS/MCL, Mauritius, p.82.

Levis, P., 2005. Sensor Network Protocol Design and Implementation. CS268. UC Berkeley. Http://csl.stanford.edu/~pal/talks/cs268.pdf

Lu, J.Q., Lee, C.H., Kim, J.S., 2006. Related-key attacks on the full-round Cobra-F64a and Cobra-F64b. *LNCS*, **4116**:95-110.

Matsui, M., 1994. Linear cryptanalysis method for DES cipher. *LNCS*, **765**:386-397.

Mauw, S., van Vessem, I., Bos, B., 2006. Forward secure communication in wireless sensor networks. *LNCS*, **3934**:32-42. [doi:10.1007/11734666_4]

Moldovyan, N.A., 2003. Fast DDP-based ciphers: design and differential analysis of Cobra-H64. *Comput. Sci. J. Mold.*, **11**(3):292-315.

Moldovyan, N.A., Moldovyan, A.A., 2007. Data-driven Ciphers for Fast Telecommunication Systems. Auerbach Publications. Talor & Francis Group, New York, p.202.

Moldovyan, N.A., Moldovyan, A.A., Goots, N.D., 2005. Variable bit permutations: linear characteristics and pure VPB-based cipher. *Comput. Sci. J. Mold.*, **13**(1):84.

Moldovyan, N.A., Moldovyan, P.A., Summerville, D.H., 2007. On software implementation of fast DDP-based ciphers. *Int. J. Network Secur.*, **4**(1):81-89.

RSA, 1999. RSA Code-breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF). Press Releases. Http://www.rsa.com/press_release.aspx?id=462

Rasool, R.U., Guo, Q.P., 2004. Security in Wireless Networks and Users-grid. Course Work Report. Wuhan University of Technology.

Rudolf, D., 2001. Optimized Differential Cryptanalysis of the Data Encryption Standard. Department of Computer Science, University of Saskatchewan. Http://www.cs.usask.ca/~dtr467/400/final/

Saraogi., M., 2006. Security in Wireless Sensor Networks. Project Paper at Computer and Network Security, Sections 494/4 594/9. University of Tennesse.

Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms, and Source Code (2nd Ed.). John Wiley & Sons, New York, p.758.