A LOW-COST PROTOCOL IN SENSOR NETWORK UBIQUITOUS ENVIRONMENT

Dong-heui Lee, Young-bok Cho, Dong-myung Kim, Sang-ho Lee

Dept. fo Network Security Laboratoy Chungbuk National Univ.
E-mail : { easttwo62@kdc.ac.kr, bogi0118@netsec.cbnu.ac.kr,dmkim@mail.ddc.ac.kr, shlee@netsec.cbnu.ac.kr}

ABSTRACT:

In a ubiquitous environment made up of multiple sensors, most sensors participate in communications with limited battery, and the sensor node isn't able to participate in communications when all the battery is used up. When an existing authentication method is used for the sensor node which has to participate in a long term communication with limited battery, it creates a problem by making the length of network maintenance or sensor node's operation time relatively shorte . Therefore, a network structure where RM (Register Manager) node and AM (Authentication Manager) node are imported to solve the energy consumption problem during a communication process is presented in this thesis. This offers a low power protocol based on safety through a mutual authentication during communications. Through registration and authentication manager nodes, each sensor nodes are ensured of safety and the algorithm of key's generation, encryption/descramble and authentication is processed with faster operation speed. So the amount of electricity used up during the communications between sensor nodes has been evaluated. In case of the amount of electrical usage, an average of 34.783% for the same subnet and 36.855 for communications with two different subnets, are reduced. The proposed method is a protocol which maintains the limited battery for a long time to increase the effectiveness of energy usage in sensor nodes and can also increase the participation rate of communication by sensor nodes.

KEY WORDS: Ubiquitous Computing, Authentication, Low Power

1. INTRODUCTION

The ubiquitous computing environment could define ubiquitous sensor network as its first model, so there is a wide range of research and development related to this field during recent years[1]. The ubiquitous sensor network is a component which freely collects and manages information by enabling communications of devices surrounding the user. One of the great limitations by ubiquitous sensor network is the issue of sensor node's conservation of energy, which operates within the limited source of energy called battery. An effective method to effectively process the authentication created during the communications between nodes should be searched pertaining to the issue of energy consumption, especially for the safety of communications. A protocol enabling safe mutual authentication operated by low power under the ubiquitous environment is introduced in this thesis. The proposed protocol is operated by RM and AM, a sensor network environment where usual sensor nodes are composed of shortest nodes, and keeps the sensor node's operation to a minimum to reduce energy consumption and provides a safe communication between sensor nodes requiring communication by issuing the session key through a mutual authentication. This sort of approach would reduce each sensor node's computational burden by many operations executed only at sensor nodes being assigned to RM and AM and ultimately make longer communications possible. The components of this thesis is as follows. Chapter 2 deals with related researches, chapter 3 proposes the low power mutually authenticated protocol, Chapter 4 presents a testing environment of proposed protocol and presents the outcome of evaluation in low power aspect and the conclusion is made in Chapter 5.

2. RELATED WORK

The sensor node of ubiquitous sensor network usually gets energy from batteries, consists of integrated sensor device, has an ability to process very little data and can execute short-distance wireless communications. But the sensor mode depends on a limited amount of energy stored in a battery. Therefore, a plan to save energy consumption caused by many operations due to higher safety becomes an important assignment

Many researches reflected by limited power of sensor nodes such as ultralight or low power encryption techniques are taking place on national and international basis. The theses of [5][6] is a typical example of ultralight, low power encryption techniques and the execution speed of encryption algorithm on various hardware platforms are evaluated in them. These methods were to solve the low power issue by selecting the faster ones among encryption algorithms. [5][6] is symmetrical key method and the node keeps the secret key to be used in advance in this method. But the problem with this method is that if the secret key is leaked from any one of the nodes, it can no longer communicate safely with the node which has this secret key. To solve this problem, there should be minimum information at the sensor node, and a session key should be generated for the safe communication at a desired session using this information. But in ubiquitous sensor network, the sensor node is so lightweight that an operation of encryption/descrambling process for key generations or safety can't be expected of great results. In theses of [5][6], they used a symmetric key method at the sensor node and applied it to ultralight, low power environments such as SmartDust's MOTES or RFID. In [7], they materialized the Rabin Ntru using a low power public key encryption which can be loaded a lightweight sensor node. Robin Scheme is a special type of RSA based on the difficulty of factoring problems and had been

introduced by Rabin in 1979. The NtruEncrypt had been introduced by Hoffstein, Pipher and Silverman in 1996 based on SVP (Shortest Vector Problem), and would require a computation ability for public and private keys of all nodes based on public keys from the sensor node. But the biggest problem is that the sensor node has to execute many operations for key generations while it has limited energy source and low computation ability.

3. THE DESIGN OF LOW-POWER PROTOCOL

In this thesis, the electrical consumption during authentications between nodes is reduced and introduces a safe, low power mutual authentication protocol. At the proposed protocol, the phases are classified into registration and authentication phases. The ubiquitous sensor network is supposed to meet the below requirements.

- *Each sensor node sets up the hop-by-hop path using the AODV routing protocol proposed at [7]*
- *The maximum number of sensors in one subnet is limited to fifty. each one of subnets has a RM and a AM, and the communications between subsystems are composed of the AM.*
- *When the communication to another subnet's sensor node is desired, an authentication between sensor nodes of different subnets is executed through the AM.*
- *The RM and AM maintains related database for execution of their own functions and possesses the sensor node information such as ID, PW, PIN and PK in tables.*

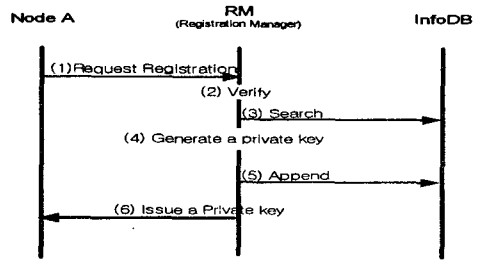
The ubiquitous computing environment is supposed to meet the below requirements, and the main parameters of the proposed low power, mutual authentication protocol is shown on [Table 1].

[Table 1] The System Coefficient of Proposed Protocol

Notation	*Description*
$Node_i$	*'i' the sensor node*
ID_{Ai}	*'i' subnet's ID of Node A*
PW_{Ai}	*'i' subnet's password of Node A*
IDK_{Ai}	*'i' subnet's ID hash value of Node A*
PK_{Ai}	*'i' subnet's private key of node A*
$\{(ID_A, PW_A), TS_A\}$	*Node A's message*
TS	*TimeStemp*
SK_{AMi}	*The session key between the AM and each node*

3.1 Registration Step

All sensor nodes of ubiquitous computing environment requests registration of their own information through RM of their own subnet organization. The user and device information are also registered in this registration step. In subnet 'i' the registration process of sensor node A is as follows. The proposed protocol generates a private key required for authentication through RM 'i'. which differs from existing authentication method. This can prevent electrical consumption due to computational overhead of sensor node by sending the key to the sensor node.



[Fig. 1] The Registration Process Through RM

(1) The registration is requested by Node A transmitting necessary parameters for its registration to the RM_i of its own subnet through the function f . (The function f executes XOR operation for all given information) The RM_i checks the user and device information using the received message.

$NodeA \rightarrow RM_i : f\{(ID_A \parallel PW_A), TS_A)$

$RM_i(Verify) : ID_A, PW_A, TS_A$

(2) The RM_i generates ID_A, IDK_A key and the private key PK_A by searching for the *Node ID* of sensor node requesting the registration through *InfoDB* it maintains.

$RM_i : IDK_A = h(ID_A \mid PIN_A)$

$PK_A = h(IDK_A \mid TS_A)$

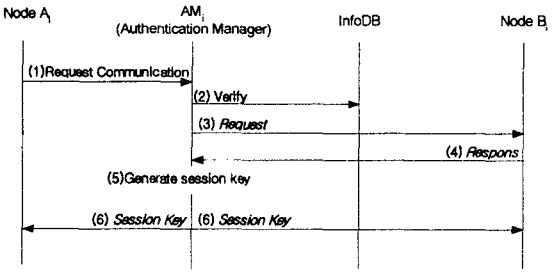
(3) The RM_i adds ID_A, IDK_A, PK_A, TS_A of the corresponding sensor node to the *InfoDB* and stores the value (The attack of re-transmission of message can be prevented by storing the *TS* value) $RM_i : InfoDB : IDK_A, PK_A, TS_A$

(4) The RM_i transmits PK_A and IDK_A values of generated private key to *Node A*. $RM_i \rightarrow NodeA : PK_A, IDK_A$

The proposed protocol generates a private key required for authentication through RM_i . which differs from existing authentication method. This can prevent electrical consumption due to computational overhead of sensor node by sending the key to the sensor node. The sensor node had executed encrypting operation through RC5 over two operations in the registration process of the service in the protocol proposed by [6] and executed encryption/descrambling using SAFER in thesis [5]. But the proposed method is characterized by registration to *RM* getting completed within the sensor node and the private key gets issued using one XOR operation and one encryption using the Rabin

3.2 Authentication Step

The sensor node which has completed the registration process executes the key exchange through the *AM* and generates the session key communicate with any corresponding node. In other words, the *AM* generates and distributes a safe session key to be used in communication after going through the mutual authentication between sensor node A and B. The communication process for authentication is divided into two types: the communication of two nodes within a same subnet and the communication of two sensor nodes by different subnets.



[Fig. 2] The Authentication of AM by Two Nodes of the Same Subnet

The [Fig.2] shows the authentication process for a safe communication of $NodeB_i$ by $NodeA_i$'s issuance of the session key through AM_i within a same subnet, and its process is as follows.

① The $NodeA_i$ delivers an authentication request message to AM_i in order to communicate with $NodeB_i$. The message transmits the function TS result of ID_* by other node requesting the PK_{Ai} communication along with TS_{Ai} . (The message can be secured of re-transmission attacks freshness by transmitting the TS_{Ai} .

$NodeA \rightarrow AM_i : f\{(PK_{Ai} \parallel ID_{Bi}), TS_{Ai})$

② After the AM_i checks whether the message received from $NodeA_i$ is a valid ID on the current subnet through the *InfoDB*, it obtains the ID_{Bi} , PK_{Bi} of $NodeB_i$ through the *InfoDB* if the information exists in the same subnet. This information is used

for the authentication after checking the message delivered to $NodeB_i$.

$AM_i \rightarrow InfoDB : Verify : ID_A, ID_B, TS_{Ai}$

③ The AM_i transmits $(ID_{Bi} \mid PKAi), TS_{Ai}$ messages to $NodeB_i$ (transmitting the notification of $NodeA_i$'s communication request), the $NodeB_i$ transmits a reply message after checking the received message from the AM_i . The $NodeB_i$ gets to obtain the PKA_i of in this process.

$AM_i \dashrightarrow NodeB_i : \mathrm{Re}\,sf\{ID_B \mid PKA_i), TS_{Ai}\}$

④ The $NodeB_i$ delivers a message to AM_i to confirm its PKB_i , and the AM_i checks the message received by the $NodeB_i$ to see whether the value is same the one searched on ② using the *InfoDB*. The AM_i checks the PKA PK_B of $NodeA_i$, $NodeB_i$ the mutual authentication gets performed, and it generates a session key to be used during message exchanges.

$NodeB_i :\rightarrow AM_i : ID_{Bi}, f(PK_{Bi} \mid ID_{Ai}\}, TS_{Bi}$

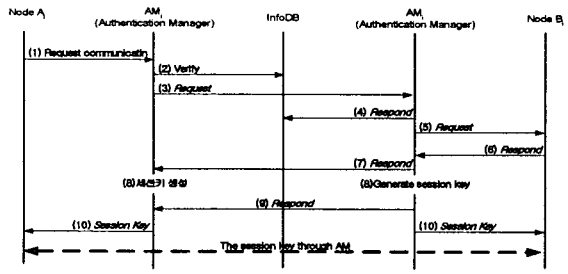
$AM_i : SK_{AM} = h(PK_{Ai} + PK_{Bi})$

⑤ The AM_i delivers generated session keys by encrypting them to private keys of each $NodeA_i$, $NodeB_i$.

$AM_i \rightarrow NodeA_i : \{SK_{AM}\}_{PK_{Ai}}$

$AM_i \rightarrow NodeA_i : \{SK_{AM}\}_{PK_{Bi}}$

As shown above, the AM_i generates the session key through mutual authentication for the communication between $NodeA_i$ and $NodeB_i$, and session keys generated at AM are encrypted into private keys and gets issued to each node. $NodeA_i$, $NodeB_i$ merely executes one descrambling process to obtain the session key.



[Fig.3] The Authentication of AM by Two Nodes of Different Subnets

The [Fig.3] is a process where the session keys ween $NodeA_i$ and $NodeB_j$ existing in two different subnets of $SubNet_i$ and $SubNet_i$

① The $NodeA_i$ delivers a authentication request message to AM_i in order to communicate with the $NodeB_j$. The message transmits the function f 's result of $IDBi$ by other node requesting the PKA_i communication along with $TSAi$

$NodeA \rightarrow AM_i : \mathrm{Re}\,qf\{(PK_{Ai} \parallel ID_{Bi}), TS_{Ai}\}$

② The AM_i checks to see whether the received message from $NodeA_i$ is a valid ID through the *InfoDB*, confirms that two nodes do not exist on the same subnet, finds the subnet AM_j where the $NodeB_j$ exists and delivers the message to the $NodeA_i$.

$AM_i \rightarrow InfoDB : Verify : ID_{Ai}, ID_{Bj}, TS_{Ai}$

③ The AM_j checks the message received from the AM_i through the *InfoDB* and delivers it to the $NodeB_j$.

$AM_j \rightarrow InfoDB : Verify : ID_{Ai}, ID_{Bj}, TS_{Ai}$

$AM_j \rightarrow NodeB_j : \mathrm{Re}\,qf\{(PK_{Ai} \parallel ID_{Bi}), TS_{Ai}\}$

④ The $NodeB_j$ delivers a message to AM_j to confirm its PK_{Bj} , and the AM_j checks the message received from $NodeB_j$ to see whether the value is same as the one searched at

$NodeB_j \rightarrow AM_j : \mathrm{Re}\,sIDB_i, f\{(PK_{Ai} \mid PK_{Ai}), TS_{Aj}\}$

⑤ The AM_i and AM_j gets mutually authenticated through PK_{Ai} , PK_{Bj} of $NodeA_i$ and $NodeB_j$ they generate session keys to be used during message exchanges. Each key generated in AM_i and AM_j are compared to confirm whether they're same keys.

$AM_i : SK_{AMAi} = h(PK_{Ai} + PK_{Bi})$

$AM_i : SK_{AMBi} = h(PK_{Ai} + PK_{Bi})$

$AM_i \leftrightarrow AM_j : Compare(SK_{AMAi} == SK_{AMBj})$

⑥ The AM_i and AM_j get to deliver session keys generated in the same manner after encrypting SK_{AMAi} , SK_{AMBj} to each node's private key.

$AM_i \rightarrow NodeA : \{SK_{AMAi}\}_{PKAi}$

$AM_j \rightarrow NodeB : \{SK_{AMBj}\}_{PKAj}$

The task to cut down the battery's power consumption for the extension of sensor node's duration in a ubiquitous computing environment is a very important assignment. To make this possible, the key generation, encryption/descrambling and authentication processes which used to be executed by sensor nodes were imported by *RM/AM* nodes and the ubiquitous sensor network was structuralized. In sensor nodes, the execution time of algorithm is reduced by their execution of key approval and message confirmation processes for safety. A safe communication is provided by reducing the consumption of power used up during communications using this method.

☐**The number of sensor networks** : The size of each subnet is assumed to be consisted of less than fifty sensors presented at [9] for the evaluation, the *RM/AM* exists within each subnet and maximum number of subnets is composed of nine subnets.

☐**The location of *RM/AM* and setting up their relation to sensor nodes**: The *RM/AM* exists within one subnet and their mutual communication is possible. Every sensor node achieves communications with *RM/AM* and registers using *RM* when the sensor nodes comes into one of the subnets. The sensor node that has completed the registration gets to participate in communications by getting issued with a session key after completing the authentication through the *AM*.

☐**The length of path between two given sensor nodes**: The length of path between sensor nodes for the communication from *NodeA->NodeB* is set to minimum of 5 passing nodes and maximum of 13 passing nodes when two nodes belong to the same subnet. But when two nodes are of different subnets, in other words when the nodes are communicated with the farthest node in the subnet, the length is sent to minimum of 10 passing nodes and maximum of 27 passing nodes.

☐**The operation ability of *RM/AM* and sensor nodes**: The *RM/AM* possesses a greater operation ability than regular sensor modes with the terminal of about 2.4GHz, 250kbps, 868/915Mhz and the sensor nodes possess the operation ability of the node justified in the previously described SmartDust.

Let's make the assessment of low powered mutual authentication protocol under the ubiquitous computing environment in the aspect of power consumption during communication. In order to make an assessment based on the aspect of communication power consumption, it is assumed that all sensor networks transmit equal number of data packets and the power consumption is consistent between communications of each sensor nodes in the proposed protocol. On [Table3], the number of passing nodes when each nodes are communicated to calculate the power consumption are minimum distance of *PN=2*, maximum distance of *PN=5* for same subnets and minimum distance of *PN=4*, maximum distance of *PN=12* for different subnets in case of the KARL method and minimum distance of *PN=5*, maximum distance of *PN=13* for same subnets and minimum distance of *PN=10* and maximum distance of *PN=27* for different subnets in case of the proposed method. In order to calculate the amount of power consumed while communicating at the sensor node, the assessment should be made by comparing the KARL method with the proposed method using the measured value of [10].

- Power Consumption: *(equation 1)*

$$E_{Tx}(k,d) = E_{Tx-elec}(K) + E_{Tx-amp}(k,d) = E_{elec} \times k + e_{amp} \times k \times d2$$

- Receive Message: *(equation 2)*

$$E_{Rx}(k) = E_{Rx-elec}(K) = E_{elec} \times k$$

[Table3] shows the measurement of power consumption created during the communication from *Node A->Node B* based on *(equation 1)* and *(equation 2)*.

[Table 3] Power Consumption During Communications

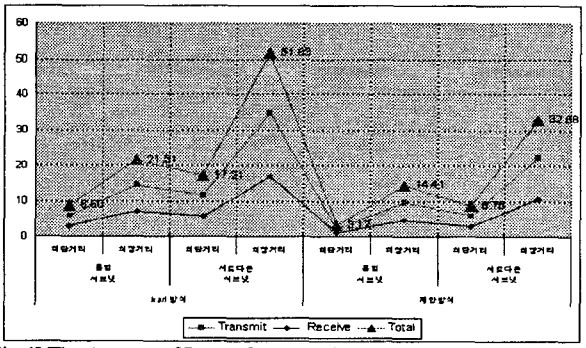
Item	Power Consumption
Effective data rate	12.4kbps
Energy to transmit	59.2mJ/byte
Energy to receive	28.6mJ/byte
ATmega 128L active mode	13.8 mW
ATmega 128L power down mode	0.0075 mW
ATmega 128L MIPS Watt	289MIPS/W

At the proposed protocol, the power consumption of entire network is expressed by each of two nodes' power consumption being added to the number of nodes to be passed. The amount of power consumption are as follows for communications of two nodes in the same subnet and two sensor nodes in different subnets.

$$SN_{equalET} = \sum_{i=1}^{PN} ETi \quad SN_{equalER} = \sum_{i=1}^{PN} ERi \quad (PN : PassNode)$$

$$SN_{otherET} = \sum_{i=1}^{PN} ETi \quad SN_{otherER} = \sum_{i=1}^{PN} ERi \quad (PN : PassNode)$$

450 sensor nodes are needed to assess the power consumption during the communication. One subnet is composed of 50 sensors with a total of 9 subnets as a standard. Each sensor node is placed within the area of 10m×10m. The size of data packet transmitted from a node is set to equal for all nodes. Also, the amount of power transmitted from each node are assumed to be same for all nodes in this thesis, and the power consumption is as follows when two sensor nodes are communicated.



[Fig.4] The Amount of Power Consumption During the Communication Between Two Sensor Nodes

The [Fig.4] shows the average amount of power consumption within one node. Because the amount of power consumption is different with transmissions and receptions when each message is communicated. Although the number of passing nodes in the proposed method are increased compared to the existing KARL method, we can see the decrease of 18.95mJ from 51.63mJ⇒32.68mJ when the maximum distance has been communicated with different subnets.

4. CONCLUSION

In a ubiquitous computing environment, all sensor nodes participate in the communication with limited supply of power stored in a battery. In existing authentication method, a considerable amount of power had been used for safety due to overhead created by operations for key generations, encryption/descrambling and authentications at the sensor node. This thesis has presented a protocol which executes the mutual authentication by importing *RM* and *AM* to solve the problem of sensor nodes power consumption and to generate a safe session key through a mutual authentication between nodes. As a result, although the average length of path between nodes for processing authentication becomes 2.5 times longer, the amount of power consumption has been reduced by 6.4043mJ⇒3.41565mJ= 34.783% for two nodes of same subnet and by 14.21mJ⇒8.29025mJ= 36.855% for communications by two different subnets when the assessment is made based on the amount of power consumption. Also, the proposed thesis is even safer from the MITM attack compared to the existing KARL method which showed weaknesses in the MITM attack.

REFERENCES

[1] Kim, Yun Mi Do, No Sung Park, "The Sensor Network Technology" Korea Information Processing Association Journal, 2003 Page(s):85-95.

[2] Sik Park, "The Ubiquitous Sensor Network and Security Considerations", Korea Information Processing Association Journal, 2004 Page(s):12-20.

[3] Duk-Dong Lee, " Ubiquitous Network and sensor technology", Telecommunications Review, 13-1. 2003 Page(s):91-104.

[4] Gunnar Gaubatz, Jens-Peter Kaps, Berk Sunar, " Public Key Cryptography in Sensor Networks-Revisited" , In Proc. of the European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004),LNCS 3313, Heidelberg, Germany, August 6, 2004

[5] Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu , " Analyzing and Modeling Encryption Overhead for Sensor Network Nodes" , WSNA'03, September 19, 2003 Page(s):151-159.

[6] Kaan Y¨uksel, Jens-Peter Kaps, Berk Sunar, " Universal Hash Functions for Emerging Ultra-Low-Power Networks" , Communications Networks and Distributed Systems Modeling and Simulation Conference(CNDS), San Diego, CA,January, 2004.

[7] J.Hoffstein, J.Pipher, J.H.Silverman, " NTUR:A new high speed public key cryptosystem" , In Proc. of the Algorithmic Number Theory (ANTS Ⅲ), Portland, OR, June 1998, Lecture Notes in Computer Science 1423 (J.P.Buhler,ed). Springer-Verlag. Verlin. 1998 Page(s):267-288.

[8] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, " SPINS: Security Protocols for Sensor Networks" , Mobile Computing and Networking 2001 Rome, Italy Copyright 2001,ACM.

[9] Arvinderpal S.Wander, Nils Gura, Hans Eerle, Vipul Gupta, Sheueling Chang Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks" In Proc. of the 3rd IEEE International conference on Pervasive Computing and Communication 2005, PerCom 2005, 08-12, March 2005, Page(s):324-328

[10] Laurent Bussard, Yves Roudier, " Authentication in Ubiquitous Computing", Workshop on Security in Ubiquitous Computing UBICOMP 2002, Göteborg Sweden, 29 Sept 2002.

[11] L. Echenauer, V. D. Gligor, "A Key-Management scheme for Distributed Sensor Networks", In proceedings of the 9th computer communication security, Nov 2002, Page(s):41-47

[12] Jalal Al-Muhtadh, "A Flexible Privacy-Preserving Authentication Framework for Ubiquitous computing environments", in the International Workshop on Smart Appliances and Wearable Computing(IWSAWC2002),Vienna, Austria, July 2, 2002 Page(s):771-776

[13] Ross Anderson, "A New Family of Authentication Protocols" Operating Systems Review, 1998 Page(s):32-35

[14] Dong-wook Cho, Yeon-yi Choi, Hee-do Kim, Dong-ho Won, " The Designing of Key Distribution Protocol Providing a Mutual Authentication Suitable for Telecommunication Environment", [1] Korea Information Processing Association Journal 2000, 6 v.10,v2, 2000 Page(s):21-30.

[15] Zan Li, Yilin Chang and lijun Jin, " A Novel Family of Frequency Hopping Sequences for Multi-Hop Bluetooth Networks", Consumer Electronics, IEEE Transactions on Vol.49. Issue 4, November 2003 Page(s):1084-1089

[16] http://www.eskimo.com/~weidai/benchmarks.html, "Crypto++ 5.2.1 Benchmarks"