International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 1st Jun 2019. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-06

Title: SIMULATION OF ADVANCED CIPHER SECURITY STANDARD FOR 128-BITS ENCODED AND DECODED IN PIPELINE PROCESS BY VERILOG MODULE

Volume 08, Issue 06, Pages: 138–146.

Paper Authors

Vinodha G, Rangawah L, Abhilasha C. P, R. Gangadhar Reddy

Rajarajsweri College of engineering, Bangalore-74

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

SIMULATION OF ADVANCED CIPHER SECURITY STANDARD FOR 128-BITS ENCODED AND DECODED IN PIPELINE PROCESS BY VERILOG MODULE

Vinodha G[1], Rangawah L[2], Abhilasha C. P[3]., R. Gangadhar Reddy [4]

[1]PG SCHOLAR, Department of ECE, Rajarajsweri College of engineering, Bangalore-74
[2]Professor, Department of ECE, Rajarajeswari College of engineering, Bangalore-74
[3]Assistant professor, Department of ECE, Rajarajeswari College of engineering, Bangalore-74
[4]Associate professor, Department of ECE, Rajarajeswari College of engineering, Bangalore-74
[1]vinodhavini2602@gmail.com

ABSTRACT

The Advanced Encryption Standard (AES) is an algorithm which will be used to protect the electronic data. To encrypt the information AES 128bits pipeline uses AES algorithm.It converts data to an unfathomable form called **cipher text.** This advanced standard is able to work under128bits in cipher key generation process. This module is used for increase the speed as it is perform repeated sequence called round in pipelined.

KEYWORDS

Advanced cipher security standard for 128-bits, encoded, decoded in pipeline process

1. INTRODUCTION

Cryptography security has discretion, disposal and message mixing between source and designation which are major goals in security. One of the major security algorithms that have been used in slab cryptograph is the Advance encryption standard algorithm. In order to support multimedia data transmission great speed retreat decisions are important. Real-time voice transmission requires the VOLP fast security algorithm for QOS.

To rise the output of Advance encryption standard encryption and decryption procedure pipeline technique is used. Depends upon the numeral of sequences and the key compeers elaborate in the procedure only will

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Advanced encryption standard will give Pipelined Advance encryption standard and key pipelining algorithm will be useful for increasing the output of the process.

The expansion of key module is an important components in AES encryption and decryption.. This key expansion algorithm is based on reduplication looping architecture. If the architecture for AES with basic reduplication architecture and restricted loop undoing is compared, the loop undoing increases speed of sequences implementation more than the solo round implementation will perform. The searching process on this block RAMs depends on the speed of S-box substitution in modules of a round. SBMs applied to the substitution -box in Advance encryption standard forthe sequences execution process. In common rate of an system insurances the computational adeptness and storing requirement for changed employments such as hardware, firmware . These process execution will need more litheness and plainness . Advance encryption standard paper proposes will provide a novel scheme incorporating these characters in AES for encrypt and decrypt. These will perform the AES Key generation and AES encryption methods for determined. The key generation will perform based on the secrecy of a key. In Advance encryption standard paper, chapter 2 will describe the advances process, section 3 will describe pipeline for encryption and decryption, section 4 describes the overall function of AES in encrypt and decrypt.

This is penalized on the standard for exchange – transformation network which stays efficient to design both hardware as well as software.

Security and performance criteria for AES:

- The ultimate goal of these algorithms is to improves the security issue in DES algorithm.
- Ability to protect the sensitive data from cipher attackers in cryptography.
- Ability to perform all three key length in both encrypt and decrypt.
- Increase the speed with low cost
- Low ram with required high level processing
- It will perform the variety of 8bit smart cards
- Protect the security 10 times better than AES

2. LITERATURE SURVEY

2.1 Assessment for literature:

In the meantime the overview of Advance encryption standard process in 2002 was published on AES algorithm has been focused on implementation of firmware and hardware cipher analysis of Advance encryption standard procedure .Certain papers derived out with aggressive Sub bytes box constructions with its features.

2.1.1 Advance encryption standard implementation process

Operation of hardware will mostly allocate through single-chip using FPGA pipelined approach, it will leads to throughput tradeoff for Advance encryption standard execution in a 0.185µm. In the CMOS handiness, cipher - memory and SRAM design has great speed non-pipelined FPGA, for a totally sub-pipelined encoded in their process. To realize a output of 21.56 Gbps on device which support the Xilinx, we need proto type bit which is capable of employed expending 0.35µm CMOS technology.

Firmware operation will mainly allocate with profligate execution of algorithm in canny cards. To sheltered the PDA communiqué with Java , an optimal creation of amalgamated pitches for the Advanced encryption standard is required ,and the valuation of altered executions for high end resources ,and the employment lines for Advanced encryption standard process will also performed in C, C++ and MATLAB, for retreat code of behaviorfor automobile key system for less which are the major key role for Advanced encryption standard encryption and decryption.

2.1.2 Analysis of AES algorithm using cryptography

This analysis includes the Fast Algebraic Attacks on Block Cipher with major three important analysis are said by linear analysis, differential analysis, extended Scarce Linearization (XSL) andvigorous round on Advanced encryption standard process .

It is considered with supplementary conflict alongside the variance and linear analysis, and by exhausting the modern effects in cipher research. It is clearly found that after 7 roundsNo attack is known for AES. Though advanced encryption standard has been elected for the regular encrypt process , its sanctuary has a winds and shots of disputation. The statistical flora of advanced encryption standard has absorbingunbolted up probable path for extra attacks like nontraditional one.

These system is centered on suggestion of Sub byte process of Advanced encryption standard in an concluded well-defined classification of MQ equations which are capable to resolved the XSL and it is created on stretched Linearization (XL)process.

The retreat of advanced encryption standard wills fabrications arranged the difficulty of XL, to be update to ruins an undeveloped unruly in cipher. If these procedure could not slog, vestiges to be verified then, different illustration of advanced encryption standard which will made tranquil for cipher inquiry, to inserting advanced encryption standard in a cryptograph we will get the unassuming arithmetic actions called GF(2n).

It will displayed the advanced encryption standard for 31 encrypt which can be labeled as multivariate quadratic system above GF(28), which is the best solution for recover the key . By attackingthe AES which has cipher blocking method to involves single a special well-known output to be prosper. If AES technique will come in practice, foremostrevolt of cipher analysis process. Every block ciphers involve these rectilinear/disparity and extra valuation spells will need a sum of inputs with self-same giant for cultivatesin the amount of sequences.

The procedureof XL will get nose-dives in fairly wretchedly to disruption advanced encryption standard rules and process. However the system is got the advanced encryption standard but that will not be haphazard, and it takesseveral unusual assets with over definedprocess ,by scant which will have the same designed process.Itis nope reservation that XL and XSL will grind in voluminous remarkable cases in cipher process .

2.1.3 Strict Avalanche Criteria (SAC)

It is important characteristic of a Sub byte box. The storm

benchmarks is a little revolution in the effort byte of an Sub byte -box, it results at least 50%byte will change in output. It is also called as SAC (strict avalanche criteria). It was introduced in 1985 by Webster and Tavares when their scheming the facts encrypts process.

Transformation of cryptanalysis will supposed to be 'finish', in case of all single cryptograph transcript moment hinge onall of the plaintext moments. So that only the probable process which will able to bargain the meekest the expression for Boolean in every encryption tad in terms of the plaintext tads, then at every moments it will lexes comprise output encrypt bits. On further spine instead in any unique couples of n-bit vector which fluctuate only in unique bit i, and the cryptogram text routes.

2.1.4 Aggressive S-box

By an algebraic expression with 9 terms will leads to algebraic attack which is shown by

Jingmei.To overcome this defect jingmei will suggested to improve advanced encryption standard Sub byte box to generate inverse action and that will only it will starts to transformation . The algebraic attackswill become complex if it perform 255 bits operations.

Jens Riidingershowed that the algebraic attacks of cipher will become complex algorithm if it is specified by numerical difficulty will be expressively greater in main controlled by Sub byte boxes processes will created a medium with fundamentals of polynomialand has revealed that the replay historical of 256 for Sub byte .

It will act as central prerequisite aimed at a good Sub byte to be nonlinear function. The selected S-boxes are calculated for linear and nonlinear function . Only single tad adjustment in the undisclosed strategic modifications in the sub byte passes, and that will make a multipart aimed at cipher analysis to find the plaintext to cipher text.

2.2 Defined problem in AES

Advanced encryption standard procedure is virtually affected by the branded numerical occurrences at presently. The direct analysis of crypt and distinction outbreaks wills necessity a large expanse of input text and encryption text to pause for encrypt/decrypt key.

In imaginary attitudes, it will specify the narrow extent of well-known normal text and encode text may be potential to halt the key advanced encryption standard for expending XSL round, as it does not presented in practically. The possible algebraic attack on AES algorithm will be XSL attack of cipher only. This is because the number of secret key bits ,in the S-box will be static and all the other blocks are fixed with constant . The designed in AES algorithm will often uses an Affine transformation with a constant 8 × 8 A matrix in static box and a constant C of one byte, a column matrix.

To construct a dynamic S-box with variable A matrix and constant C which are key dependent static box are possible .In the s box there are nearly 21684 possible and keys are dependent, for XSL attack which will become more difficult. Also it will require the GF(28)making the mix column, which is a 4 × 4 matrix with elements in matrix. In A and mix column the satisfied condition will be singular. By

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

introducing these two parameters the modified algorithm will have 22054 keys. In Brute-force attack and all the algebraic attacks become more difficult forcryptanalysis.
In this report we introduce the generation of dynamic S-box and dynamic Mix column matrix and hence the modified AES algorithm. By using the same dynamic S-box, new stream cipher and new Whirlpool hash function are constructed. It is found that the time required to execute the modified AES algorithm is negligible, few milliseconds more than that required for present AES algorithm. Also no extra memory is required the for modified AES algorithm

3.AES PIPELINE ENCRYPTION

Each module in the pipeline cipher are controlled by using

- Clock
- Asynchronous reset
- Input and output valid signals

Substitution Byte

Every byte in the 128 bit data will use the s-box LUT for substitution

Shifting the Rows

Shifting rows of these arrays are declared on the standard document and it is also used for arranging the data in state array.

Mix columns calculations

It will perform the finite filed multiplication which is declared in the standard document.

Adding the round key

It will perform the function of XOR –operation and round key function.

Round operation

It is the connecting modules for all the above functions .

Round key generating function

- It is the basic block for the key expansion module.
- In these stages are to be balanced with 4 round in substitute bytes –transference rows-mix columns –improve round key and these vital data's are meet at add round key modules.
- It will includes the key generation operation of Rot word, sub bytes ,XOR operation
- Fips 197 documentation using RCON.

Key expansion

It is a module which is used to generate the round key using pipeline cipher.
Instantiate number of round key=number of rounds to get number of round keys =number of rounds.

Top module pipeline

This pipeline cipher is designed for rounds and it will connect key expansion using RTL architecture.
Every round in round key will feed by key expansion.
By this algorithm, the first key should be XOR with input plaintext
At initial stage all rounds will connect with key expansion and in the ending rotund it will not take in the assortment columns only three stages delay.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

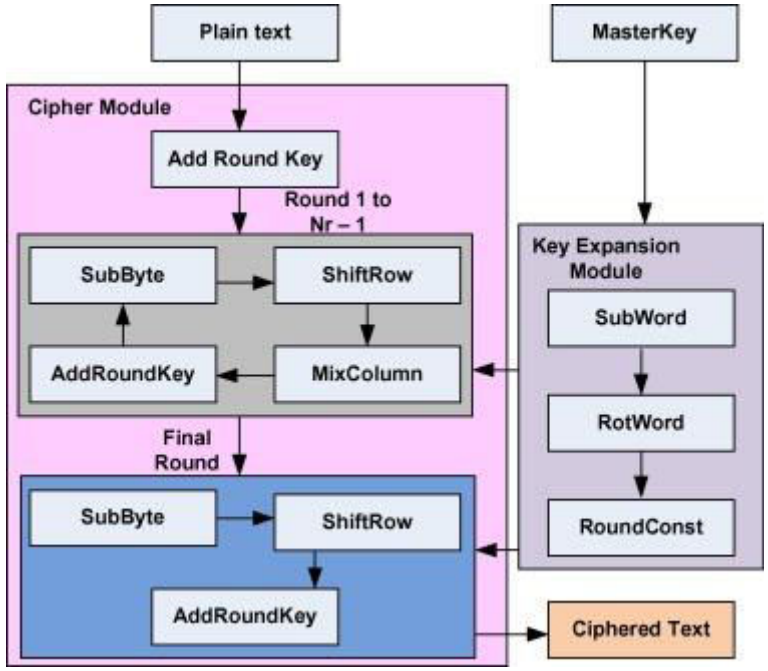


Figure. 3.1. Pipelining of AES encryption algorithm

Cipher encode system Configurable Parameters

Length of key:

It will design the key length like 128,192,256bits depends upon the parameter required .

Mapping the register:

It will control the data flow and operations of AES engine with CMD and which will occurs at set of predefine one

Address	Register	Representation
0X0	STATUS_AES	Status Register with AES engine
0X4	CONTROL_AES	control register with AES
0X8	DATA_AES	Read and Write to/from the AES Engine
0XC	AES_KEY	Key data with write register

Table 3.2 address mapping and register

Bits 6	Bits 5	Bits 4	Bits 3	Bits 2	Bits 1	Bits0
X	CRYPTDONE	EXPDONE	IDATFULL	KEYFULL	RST	BUSY

Table 3.3 register for advance encrypt process

Parameter explanation

• EVENTFUL:

It will conventional at encrypting, decrypting and vital enlargement.

• RESET:

It will reset after set by ADANCED ENCRYPTION STANDARD _REGULATOR and then major effective engrave will access .

. **• KEY PROCESS**

When it is set as 128 bits of key to key data register .if this status bit is said to be cleared when the processor twitches script to encrypt vital index and it enthusiasms energetic when AES engine collects the indispensable number of bits .

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

• **EXPDONE**:
It will indicates the completion of key expansion process for generates an interrupt when it checks the bits..
• **CRYPTDONE**:
It will indicates as mainframe jumps understanding from advanced encrypt for registering the data, When the encrypt operation said to be clear the reading processor from data register.

Commands	Representation
00	NOP
01	RESET
10	KEY-SETUP
11	AES-DECRYPT

Table 3.4 command field register with control function

The valid commands words are define when action requires the AES engine to RESET the operation to clear the key, data, status, and control register.

3.3 Basic operation functions

1. Run the simulation by AES
2. The RTL simulation waveformscripts also runs
3. By RESETTING the FPGA the simulation will starts
4. By supplying the content of control register and address register the signals will get enable usingloading the control register.
5. By supplying appropriate key values the address of key register will enable the signal through loading the key register content.
6. Bysupplying the appropriate data values the address register will enable the signals through loading data register content.
7. And appropriate valid signalswill apply
8. To start key expansion processes send key setup command
9. After key expansion is done then read the status
10. Decrypted key values with help of load data register
11. After loading the data register send start decryption command.
12. After finishing the decryption process then read the status register

4. AES DECRYPTION

The decrypt portion of the AES under a.k.a Rijindael algorithms are described in the FIPS -197 specifications. each key length of 128 will be separate by installation wrapper .Based on FPGA architecture the lookup table logic has been design to take the advantage of 6-input [LUT6].It can able to achieve the peak throughput over 3Gpbs for 256-bit key.

4.1 DECRYPTION HIGHLIGHTS

• It will support 128/192/256-bit AES decryption.
•. Not changeable at runtime. But it will separate wrappers for each key length
•. The computed key schedule is stored internally and can be used on multiple cipher text.
• The main schedule is compute the decryption of each 128-bit cipher text when it will takes 11/13/15 clock cycles.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

• Ciphertext, key text, and plaintext, are separated the interfaces with simple valid/ready style handshaking.
•When the design is fully synchronous then only one clock domain
• System Verilog in source code

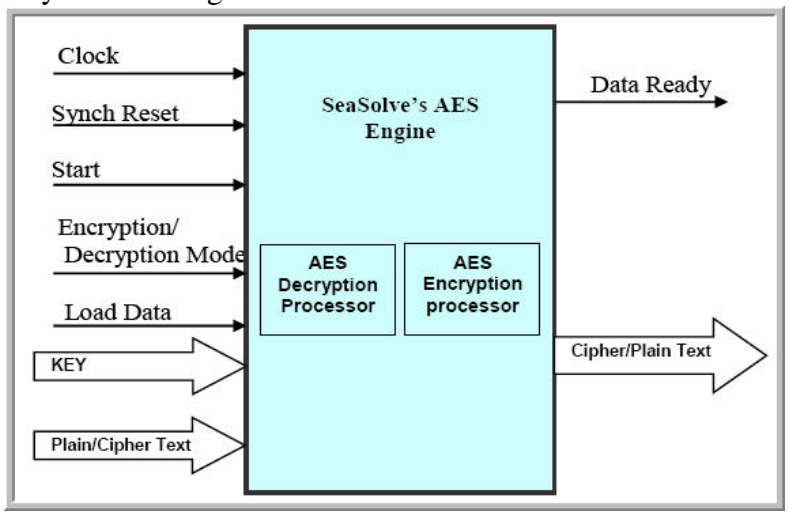


Figure 4.2 sea solves AES engine

4.2 Test conditions

The implemented with Xilinx Vivado 2015.1 using "Performance Explore" implementation strategy with a period constraint for the purpose of benchmarking to the core is wrapped in a shift-register-like structure to reduce I/O pin count, synthesized.
Xilinx Kintex family xc7k325tffg900-3 and Kintex Ultra Scale xcku040- ffva1156-2-e are the target devices. The no of clock cycles starts from the arrival of key text and cipher text whenever the plain text is available at the output. When the previous computed key schedule will be re used the key expansion will be zero then only the decryption engine latency willcount

4.3 Back to back cipher text for decryption cycle

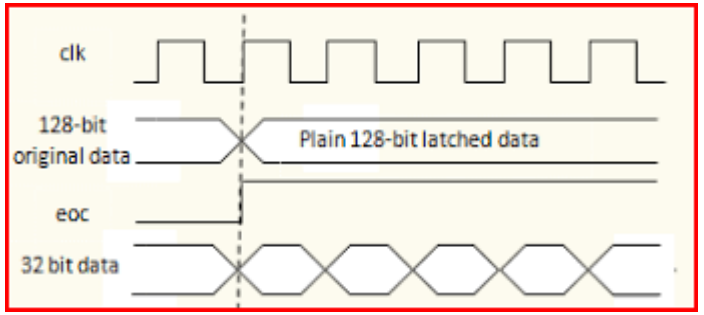


Figure 4.3 Timing diagram for encrypt

The decryption cycle for back-to-back cipher text using the timing diagram above shows
1. When it is ready to accept new cipher text, the core asserts ct_rdy to high
2. To achieve high to inform the core that a valid cryptograph text is present through the application drives the cryptogramtext to ct and asserts ct_
3.To achieve the high again to indicate it is ready to accept a new cipher text, the core asserts pt_vld to high when a valid plaintext is available on pt and at the same time it also asserts ct_rdy
4. To high to inform the core that a new cipher text is present

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

at the application drives the next cipher text to ct and asserts ct_vld.

5. SIMULATION RESULTS

Encryption cipher

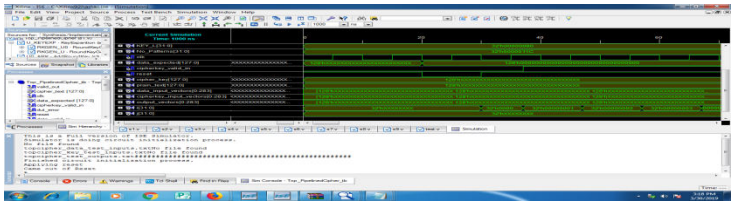
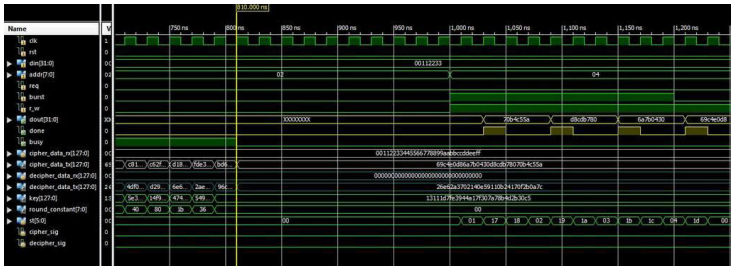


Figure 5.1 simulation of encoded

Both encoded and decoded



6. CONCLUSION AND FUTURE SCOPE:

The purpose of this design is to perform the significant level of security in real time data communication and also to boost the process for extremely fast speed whenever required .Here we are using 128-bit key and the result obtained by using Verilog is success. The length of key will vary varied according to the modified algorithm .However we have perform the encryption and decryption in RS232, the communication system will be comparably similar to that data which is used in communication core process. By using the single FPGA with two processor implementation for which one will be helpful for other at the time of executing the original text in algorithm which will able to design better way in hardware without any inconvenient to hold the processor at stable state forever with better throughput then this proposed model.

7. REFERENCE

[1] Abdel-hafeez S., Sawalmeh. A. and Bataineh S., "High Performance AES Design using Pipelining Structure over GF(28)" IEEE Inter Conf. Signal Proc. and Com., vol.24-27, pp.716- 719, Nov. 2007

[2] J. Yang, J. Ding, N. Li and Y.X. Guo, "FPGA-Based Design and Implementation of Reduced AES Algorithm" IEEE Inter. Conf. Chal Envir Sci Com Engin (CESCE).,Vol.02, Issue.5-6, pp.67-70, Jun 2010.

[3] A.M. Deshpande, M.S. Deshpande and D.N. Kayatanavar, "FPGA Implementation of AES Encryption and Decryption"IEEE IInter. Conf. Cont, Auto, Com, and Ener., vol.01, Issue04, pp.1-6, Jun.2009.

[4] Hiremath. S. and Suma. M.S., "Advanced Encryption Standard Implemented on FPGA" IEEE Inter. Conf. Comp Elec. Engin.

(IECEE), vol.02, issue.28, pp.656- 660,Dec.2009.
[5] AI-Wen Luo, Qing-Ming Yi, Min Shi. "Design and Implementation of Area-optimized AES on FPGA" , IEEE Inter. conf. chalsci com engin.,978-1- 61284-109-0/2011.
[6] Rizk.M.R.M. andMorsy, M., "Optimized Area and Optimized Speed Hardware Implementations of AES on FPGA", IEEE Inter Conf. DesigTes Wor.,vol.1,issue.16,pp.207-217, Dec. 2007.
[7] Liberatori.M.,Otero.F.,Bonadero.J.C. andCastineira.J. "AES-128 Cipher. High Speed, Low Cost FPGA Implementation", IEEE Conf. Southern Programmable ogic (SPL), vol.04, issue.07, pp.195-198,Jun. 2007.
[8] Abdelhalim. M.B., Aslan. H.K. and Farouk.H. "A design for an FPGAbased implementation of Rijndaelcipher",ITICT. EnaTechn N Kn Soc.(ETNKS), vol.5,issue.6,pp.897-912,Dec.2005.
[9] Fedaral Information Processing Standards publication 197 November 26, 2001" ADVANCED ENCRYPTION STANDARD (AES)".
[10] Rijndael. N. Sklavos and O. Koufopavlou "Architectures and VLSI Implementations of the AES-Proposal", IEEE Transactions On Computers, Vol. 51, No. 12, December 2002.