AES and ECC based Cryptography for Random-key generation

by P C

FILE	AES_AND_ECC_BASED_CRYPTOGRAPHY_FOR_RANDOM-KEY_GENERATION.DOC (533.5K)		
TIME SUBMITTED	03-JAN-2017 06:58PM	WORD COUNT	2126
SUBMISSION ID	756592799	CHARACTER COUNT	11122

AES and ECC based Cryptography for Random-key generation

ABSTRACT

As more increase in usage of communications and developing them more user friendly. While developing those communications we need to take care of security and safety of users data. Many researchers have developed many complex algorithms to maintain security in users application. Among those one of the best algorithms are cryptography based, in which user will be safe side mostly from the attackers. We already had some AES algorithm which uses very complex cryptographic algorithm to increase the performance and more usage of lookup tables. So the cache timing attackers will correlates the details to encrypt the data under known key with the unknown key. So for this we provide an improvised solution. This paper deals with an extension of public-key encryption and decryption support including a private key. The private key is generated with the combination of AES and ECC. In general AES key length is 128 bits with 10 times of iterations. But with this, users wont get efficient security for their operations, so to increase the security level we are implementing 196 bit based encryption with 12 times round-key generation iterations. By this enhancement we can assure to users to high level security and can keep users data in confidential way.

Keyword:

Crypto-system ,AES,EC Cipher text, Random-key, Public and private keys

1. INTRODUCTION (10 PT)

For the protection and necessary development of electronic commerce and information security data. Cipher is a data protection technology can be important. AES Advanced Encryption Standard is a scoring system used widely to ensure that privacy is important and necessary. (AES), high performance, and if it is suitable for normal encrypt. Encryption is elliptical (preacher) important principle of encryption and signatures. The preacher and the process of AES and AES AES transfer encryption and preachers confused data communication[1].

1.1. AES block Description:

AES block encryption and replacement of system or network changes. According to the length of the data block and all of the key requirements of the AES. Length: 128, 192, 256, a plurality of repeated cycles with 10, 12 and 14 with the environment used. AES has three main goals: environmental changes and the mainstream media. Each change is a combination of a plurality of linear and non-linear add round important events. AES process is shown in Figure 1.

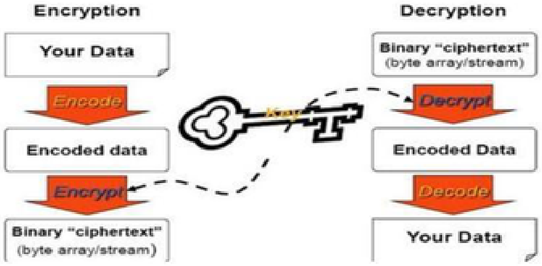


Fig:1. AES Cryptography process.

Each turn consists of four phases:

[1] Sub-Bytes changes: In operation, the box will change with each measure of all measures of the line. Preparation of S-boxes, such as a GF measures Explosion (2 ^ 8), the changes applied to akin TR2.

[2] Shift Row Changes: the market is not changing is the first measure of the country. The update cycle of the second set, the third, fourth and fifth from the left, one, two, three or four bytes respectively[2].

[3] Mix-Columns changes: In the measurement in each column of the matrix solution in many equations in one place. Consequently, the position of the encrypted data, even if modified bytes. changes no-go corporate structure in the second column of parameterization

[4] Add-Round Key Transformation: In this version, the XOR is the other bit round-key (OR). work with columns at once. Even talking about conditions of round-key ground. The work was carried out through the last bit AES matrix2.

The channels so that the attention of breaking the encryption cryptanalysis killed instantly, but are weak. You can stick the channel page information data and time from a variety of options, statistics, energy conservation, and many other eye-AES appear well in this regard. Since the containers are stored, the encrypted cache or physically harmful, change the long-term encryption settings and how to insert text and encryption[3]. Side channel based on a comparison between the information provided in the sewer system and confidential information from falling into two main responses:

1. Reduction of files to prevent, or unnecessary duplication of information
2. The development of relations between the discharge documents and confidential information, confidential information that could be made, or unencrypted text databases randomly directly related to the change, so that back when the finished decoding

(AES), high performance, and if it is suitable for normal encrypt. Encryption is elliptical (preacher) important principle of encryption and signatures. description of the preacher and the mix in this study AES and send the Data[3] encrypted communication.

1.2. Cons and Pros of AES Cryptography

Inputs and outputs the data encrypted in the configuration data information that can be used to stop the channel, because they endanger the safety of some co-systems[4] added. The motivation of this work is to develop sufficient to reduce the approach to the problem of information security algorithms are vulnerable to attacks such solution, the hybrid encryption algorithm that tries to resolve the security and communications solution.

- If the AES encryption key and Ecclesiastes communication, there is no reason, a secret key before sending the communication.
- The secret is the only way out for each other, the only requirement is that the secret encryption management.

Work is a hybrid encryption algorithm, which is a member of encryption systems Advanced Encryption Standard (AES) and Elliptic Curve and encrypts the cipher-text and advanced security agents Security[5]. The study concentrates on the other monitoring and deposit attack for their actions. The model is to provide a server data security environment. Growth and time encryption to encrypt all data that will continue only AES encryption key Preacher preacher elaborate security. Time to time information involve known details of the encryption key channel to reflect on the strange principles. Measures against side channel Wait efficiency[7] test.

2. PROPOSED METHOD HYBRID CRYPTOGRAPHY

AES symmetric encryption algorithm more lookup tables. The tables are encoded outside the result cache and cache error and the second time, the display of text encryption, decryption time changes. Re-cache and the key to the known data encryption and unknown values to a new level. For this work, and the AES, later ECC algorithm for text encryption algorithms used to prohibit the AES encryption and security software development for key security to the offense, for example, improve the parking time. The increasing efficiency is the highest form of data encryption and repeatedly with AES 192-bit key size, so that the circuit 12 in the first AES 128-bit standard active reading[10].

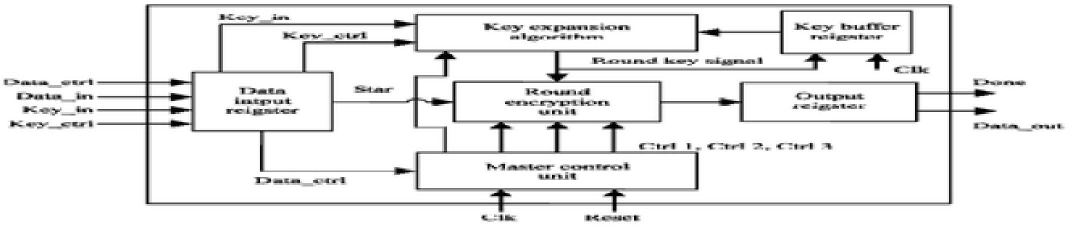


fig 2: Algorithm for proposed System.

2.1 Proposed Model designing.

To design the proposed model, which is a combination of AES and ECC Cryptography will be followed below steps

- Initially the data block from where user can send data to encrypt for security issues and during the encryption section AES based encryption process is used. In which a dynamic security is issued during the encryption process only.
- Then Further after the AES key generation then it is encrypted with EC Cryptography and send to receiver, where the decryption process will be held.
- During above process one dynamic key is generated and given to user for further decryption at the receiver side.
- The total time is calculated for encryption process and will be stored at some memory storage for cross verifying with time taking for the decryption
- At the receiver side decryption starts. In this process, AES key decryption and then data will be decrypted to original format of message sent by sender.
- So in general the module will be calculate the response time of encrypted data from the server/sender by generating various random keys including a valid key.
- In the correlation program of the attacker module comparison of the timing details for both the cases is done and it generates the possible key space according to the timing details which will be used to determine the correct key combination.

2.2. Analysis of AES & EC Cryptography

That begins with the pre-AES algorithm hybrid design should connect the two containers with the graphical user interface. and analysis of model legislation and the comparative study of the hybrid engine ECC AES. This led to the creation of the AES encryption key. The execution of the transfer Preacher Preacher encryption keys and encrypted data and encryption key AES. The central blocks and key data encryption AES decryption. The relationship between the encoded number of errors of a few family members and decoded is not known. on the process requirements analysis:

- Length of Random key generated
- Number of round-key & Algorithm
- Maintenance of randomized keys
- performance of attacker

3. EXPERIMENTAL & SIMULATION RESULTS.

The results are as follows in the book form of data encryption and 192- bit key used in the Advanced Encryption Standard. EU data is 12, replay AES export traffic.

3.1 Simulation Analysis

In Section 3.1, the user will be prompted to enter the value, the text document is encrypted with AES choose fig 2, shows the block analysis at client side. In the fig 3, explains the login page user where we can encrypt or decrypt the data. If the text of the most important, and the user clicks on the "encrypt" to begin the encryption of data. The results do not encrypted in general. question number two AES cipher text. At the edge of the image as a good cooperation. The numbers 1-6 AES Effect encrypted number, text combinations of transport and traffic shows in fig 4a and fig 4b.The other two AES encryption text of influence on the seventh round evening .The second image on the measures that AES-party collaboration. Uncoded text effects, from which seven twelve which is shown in fig 5a and fig 5b. Another AES and mix tags. Make the final phase of the AES Box Mix series no. The main dynamic encryption for the AES encryption method used, and the results should be controlled by user-defined code, need to change the rules.

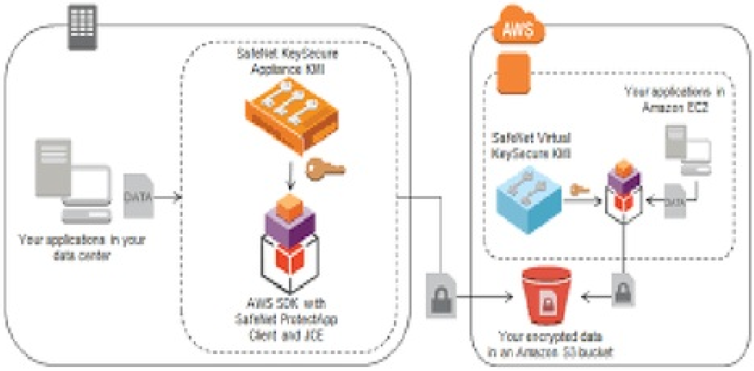
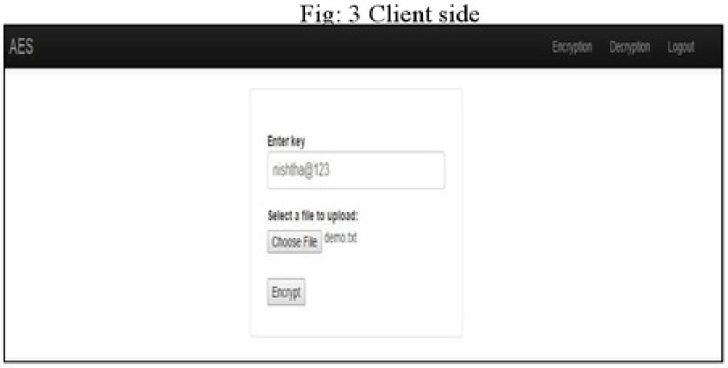

AWS
SafeNet KeySecure Appliance KMI
Your applications in your data center
DATA
AWS SDK with SafeNet ProtectApp Client and JCE
Your applications in Amazon EC2
SafeNet Virtual KeySecure KMI
DATA
Your encrypted data in an Amazon S3 bucket

Fig: 3 Client side



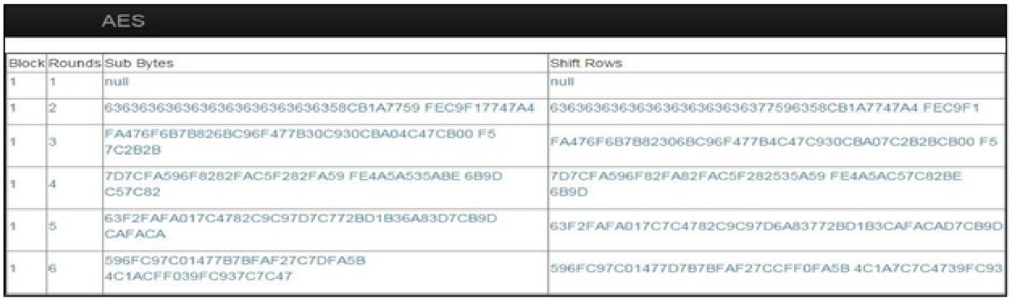
Enter key

nishtha@123

Select a file to upload:

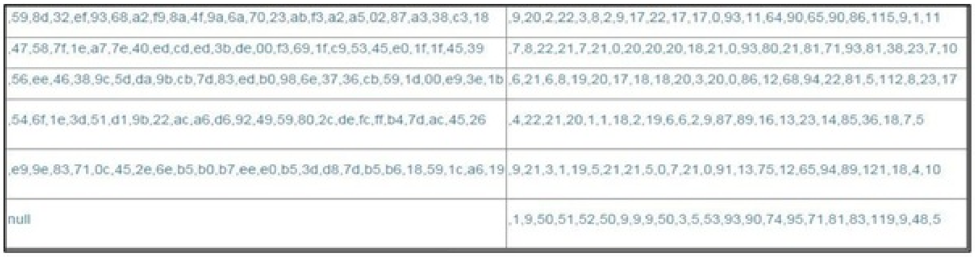
demo.txt

Fig: 3.1 AES random key page



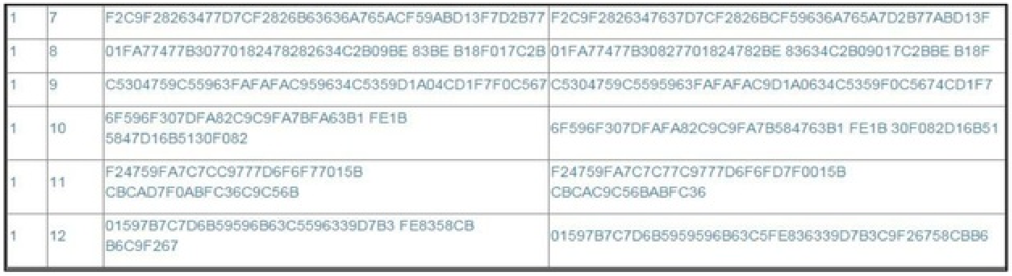
Block	Rounds	Sub Bytes	Shift Rows
1	1	null	null
1	2	63636363636363636363636358CB1A7759 FEC9F17747A4	63636363636363636363636377596358CB1A7747A4 FEC9F1
1	3	FA476F6B7B826BC96F477B30C930CBA04C47CB00 F5 7C2B2B	FA476F6B7B82306BC96F477B4C47C930CBA07C2B2BCB00 F5
1	4	7D7CFA596F8282FAC5F282FA59 FE4A5A535ABE 6B9D C57C82	7D7CFA596F82FA82FAC5F282535A59 FE4A5AC57C82BE 6B9D
1	5	63F2FAFA017C4782C9C97D7C772BD1B36A83D7CB9D CAFACA	63F2FAFA017C7C4782C9C97D6A83772BD1B3CAFACAD7CB9D
1	6	596FC97C01477B7BFAF27C7DFA5B 4C1ACFF039FC937C7C47	596FC97C01477D7B7BFAF27CCFF0FA5B 4C1A7C7C4739FC93

Fig 4a. AES Random key generation for rounds 1-6



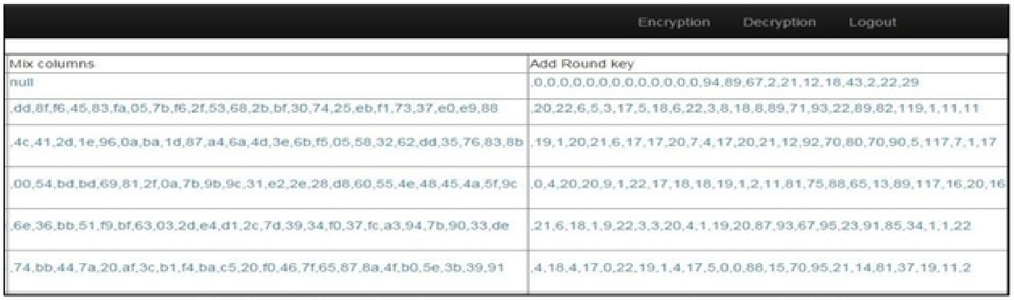
,59,8d,32,ef,93,68,a2,f9,8a,4f,9a,6a,70,23,ab,f3,a2,a5,02,87,a3,38,c3,18	,9,20,2,22,3,8,2,9,17,22,17,17,0,93,11,64,90,65,90,86,115,9,1,11
,47,58,7f,1e,a7,7e,40,ed,cd,ed,3b,de,00,f3,69,1f,c9,53,45,e0,1f,1f,45,39	,7,8,22,21,7,21,0,20,20,20,18,21,0,93,80,21,81,71,93,81,38,23,7,10
,56,ee,46,38,9c,5d,da,9b,cb,7d,83,ed,b0,98,6e,37,36,cb,59,1d,00,e9,3e,1b	,6,21,6,8,19,20,17,18,18,20,3,20,0,86,12,68,94,22,81,5,112,8,23,17
,54,6f,1e,3d,51,d1,9b,22,ac,a6,d6,92,49,59,80,2c,de,fc,ff,b4,7d,ac,45,26	,4,22,21,20,1,1,18,2,19,6,6,2,9,87,89,16,13,23,14,85,36,18,7,5
,e9,9e,83,71,0c,45,2e,6e,b5,b0,b7,ee,e0,b5,3d,d8,7d,b5,b6,18,59,1c,a6,19	,9,21,3,1,19,5,21,21,5,0,7,21,0,91,13,75,12,65,94,89,121,18,4,10
null	,1,9,50,51,52,50,9,9,9,50,3,5,53,93,90,74,95,71,81,83,119,9,48,5

Fig 4b. AES random key generation outcomes for rounds 1-6



1	7	F2C9F28263477D7CF2826B63636A765ACF59ABD13F7D2B77	F2C9F2826347637D7CF2826BCF59636A765A7D2B77ABD13F
1	8	01FA77477B30770182478282634C2B09BE 83BE B18F017C2B	01FA77477B30827701824782BE 83634C2B09017C2BBE B18F
1	9	C5304759C55963FAFAFAC959634C5359D1A04CD1F7F0C567	C5304759C5595963FAFAFAC9D1A0634C5359F0C5674CD1F7
1	10	6F596F307DFA82C9C9FA7BFA63B1 FE1B 5847D16B5130F082	6F596F307DFAFA82C9C9FA7B584763B1 FE1B 30F082D16B51
1	11	F24759FA7C7CC9777D6F6F77015B CBCAD7F0ABFC36C9C56B	F24759FA7C7C77C9777D6F6FD7F0015B CBCAC9C56BABFC36
1	12	01597B7C7D6B59596B63C5596339D7B3 FE8358CB B6C9F267	01597B7C7D6B5959596B63C5FE836339D7B3C9F26758CBB6

Fig 5a. AES Random key generation for rounds 6-12



Mix columns	Add Round key
null	,0,0,0,0,0,0,0,0,0,0,0,0,0,0,94,89,67,2,21,12,18,43,2,22,29
,dd,8f,f6,45,83,fa,05,7b,f6,2f,53,68,2b,bf,30,74,25,eb,f1,73,37,e0,e9,88	,20,22,6,5,3,17,5,18,6,22,3,8,18,8,89,71,93,22,89,82,119,1,11,11
,4c,41,2d,1e,96,0a,ba,1d,87,a4,6a,4d,3e,6b,f5,05,58,32,62,dd,35,76,83,8b	,19,1,20,21,6,17,17,20,7,4,17,20,21,12,92,70,80,70,90,5,117,7,1,17
,00,54,bd,bd,69,81,2f,0a,7b,9b,9c,31,e2,2e,28,d8,60,55,4e,48,45,4a,5f,9c	,0,4,20,20,9,1,22,17,18,18,19,1,2,11,81,75,88,65,13,89,117,16,20,16
,6e,36,bb,51,f9,bf,63,03,2d,e4,d1,2c,7d,39,34,f0,37,fc,a3,94,7b,90,33,de	,21,6,18,1,9,22,3,3,20,4,1,19,20,87,93,67,95,23,91,85,34,1,1,22
,74,bb,44,7a,20,af,3c,b1,f4,ba,c5,20,f0,46,7f,65,87,8a,4f,b0,5e,3b,39,91	,4,18,4,17,0,22,19,1,4,17,5,0,0,88,15,70,95,21,14,81,37,19,11,2

Fig 5b. AES random key generation outcomes for rounds 6-12

4. CONCLUSION:

In general AES is one of the best mechanism for the cryptography internally includes Symmetrical Encryption algorithm series. In SEA series utilizes a table look up, to increase the efficiency of performance. As those tables doesn't occupy total volume of the cache, so some faults arises during the encryption process like various lookup times and encrypting times. By this issue,cache time attacker correlates the time of encryption with known key to an unknown key. To overcome this issues during the encryption,an improvised version of AES algorithm is used to encrypt the plain text and ECC is introduced during the AES encryption process. So there by we can avoid attackers to steal/theft the data which are sending to the users. The advantages and future analysis can be explained in section 5.

5. USAGE AND FUTURE WORK.

By this type of encryption, users data can be saved in very confidential way. For an Example, as todays online payments are more using by everyone and became as one of the daily needs. In this process where payments can be done to by or sell or any transaction should be more secure and should be more safe to all customers/users. During their payment transactions these type of random key generated to encrypt the data will be known to user only. In future this 192 bit Advanced AES Encryption is moved to 256 bit based AES algorithm.

REFERENCES

[1] X Li, J Chen, D Qin and W Wan, "Research and Realization based on hybrid encryption algorithm of improved AES and ECC," in *IEEE International Conference on Audio Language and Image Processing* (ICALIP2010), pp. 396-400, Nov. 2010.

[2] R Pahal and V kumar, "Efficient Implementation of AES ," *in International Journal of Advanced Research in Computer Science and Software Engineering* , Vol. 3, Issue 7, July 2013,pp.290-295.

[3] D Jayasinghe, J Fernando, R Herath and R Ragel, "Remote Cache Timing Attack on Advanced Encryption Standard and Countermeasure," in *IEEE International Conference onInformation and Automation for Sustainability* (ICIAFs),pp. 177-182, Dec. 2010.

[4] R Pahal and V kumar, "Efficient Implementation of AES ," *in International Journal of Advanced Research in Computer Science and Software Engineering* , Vol. 3, Issue 7, July 2013,pp.290-295.

[5] C JunLi, Q Dinghu, Y Haifeng, Z Hao and M Nie,"Email encryption system based on hybrid AES and ECC," in *IET International Communication Conference on Wireless Mobile and Computing* (CCWMC2011), pp. 347 - 350, Nov. 2011.

[6] V Patil, Prof.Dr.Uttam.L.Bombale ,P Dixit, "Implementation of AES algorithm on ARM processor for wireless network, " in *International Journal of Advanced Research in Computer and Communication Engineering* ,Vol. 2, Issue 8, August 2013,pp.3204-3209.

[7] H. Tange and B. Andersen, "Attacks and Countermeasures on AES and ECC," in *IEEE International Symposium onWireless Personal Multimedia Communications* (WPMC), pp. 1-5, Jun. 2013.

AES and ECC based Cryptography for Random-key generation

ORIGINALITY REPORT

%11	%7	%8	%4
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	globaljournals.org Internet Source	%4
2	Ganesh, Anirudh Ramaswamy, P Naveen Manikandan, S PI Sethu, R Sundararajan, and K Pargunarajan. "An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based Wireless Sensor Networks", 2011 International Conference on Recent Trends in Information Technology (ICRTIT), 2011. Publication	%2
3	Fei, Xiongwei, Kenli Li, Wangdong Yang, and Keqin Li. "A secure and efficient file protecting system based on SHA3 and parallel AES", Parallel Computing, 2016. Publication	%1
4	Jayasinghe, D, J Fernando, R Herath, and R Ragel. "Remote Cache Timing Attack on Advanced Encryption Standard and countermeasures", 2010 Fifth International	%1

Conference on Information and Automation for Sustainability, 2010.
Publication

5 Bhattacharya, Sarani, Chester Rebeiro, and Debdeep Mukhopadhyay. "Unraveling timewarp : what all the fuzz is about?", Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy - HASP 13, 2013.
Publication
%1

6 Hussien, Zaid Alaa, Hai Jin, Zaid Ameen Abduljabbar, Mohammed Abdulridha Hussain, Salah H. Abbdal, and Deqing Zou. "Scheme for ensuring data security on cloud data storage in a semi-trusted third party auditor", 2015 4th International Conference on Computer Science and Network Technology (ICCSNT), 2015.
Publication
<%1

7 Aly, Hassan, and Mohammed ElGayyar. "Attacking AES Using Bernstein’s Attack on Modern Processors", Lecture Notes in Computer Science, 2013.
Publication
<%1

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE	OFF		

BIBLIOGRAPHY