DESIGN AN EFFICIENT CRYPTOGRAPHY USING HIGH SPEED MULTIPLIER

K. HARI PRIYA MOUNIKA
M.Tech – SCHOLAR
Dept. of E.C.E
N.R.I INSTITUTE OF TECHNOLOGY
GUNTUR

L. CHANDRA SEKHAR
Assistant Professor
Dept. of E.C.E
N.R.I INSTITUTE OF TECHNOLOGY
GUNTUR

***ABSTRACT*- With the recent rapid advances in multimedia and communication systems, real-timesignal processing like audio signal processing, video/image processing, or large capacity data processing are increasingly being demanded. The multiplier is the essential elements of thedigital signal processing applications. High-performance and fast implementation of existedmultiplication is applied to cryptographic systems. In this paper, we propose efficient andhigh speed architectures to implement cryptography. Cryptography is the operation inwireless communication between transmissions and receiving of data, the secured data iscommunicated in an unsecured channel between transmitter and receiver with highsecurity.At the transmitter side the original data is converted in to secured sequence and at thereceiver side the secured sequence is converted in to original data sequence. Our existedmultiplier is used in that conversion and by using this converter we are designing acryptography application.**

I. INTRODUCTION

Due to the increasing use of computers, security is animportant issue for digital information. Intruder is anunwanted person who reads and changes the informationwhile transmission occurs. This activity of intruder is calledintrusion attack. To avoid such attack data may be encryptedto some formats that is an unreadable by an unauthorizedperson.

Most of the work on reversible data hiding focuses on thedata embedding/extracting on the spatial domain. But, in someapplications, a channel administrator hopes to append someadditional message, such as the origin information, textnotation or authentication data, within the encrypted textthough he does not know the original text content.

It isalso hopeful that the original content should be recoveredwithout any error after text decryption and message extractionat receiver side. Reference presents a practical schemesatisfying the above-mentioned requirements. The owner ofthe information encrypts the original text using an encryptionkey, and a data hacker can embed additional data into theencrypted text using a data-hiding key though he does notknow the original content. With an encrypted text containingadditional data, a receiver may decrypt it according to theencryption key, and then take the embedded data and recoverthe original information according to the data-hiding key.Encryption has long been used by militaries andgovernments to facilitate secret communication.

II. RELATEDWORKS

2.1.USER REGISTRATION

If the user desires to access the info from the server,they ought to have associate account therewithserver. While not having associate account them areaunit not ready to access the files are read the smallprint. Therefore 1st the user can produce associateaccount therewith server by providing the requiredinfo like Username, Password, DOB, Address andsignal. Once this info is provided by the user, servercan get that info and keep it into the information forfuture purpose.

2.2.CLOUD SERVER

Cloud information Service supplier can contain thebig quantity of information in their informationStorage. Conjointly the Cloud Service supplier canmaintain the all the User info to evidence the Useronce area unit login into their account. The User info is keep within the information of the Cloud Servicesupplier. Conjointly the info Server can send the Userrequested job to the Resource assignment Module tomethod the User requested Job. The Request of allthe Users can method by the Resource assignmentModule. To speak with the consumer and therefore thewith the opposite modules of the Network, the info

Server can establish association between them. Forthis Purpose we have a tendency to area unit reachingto produce associate computer program Frame. Conjointly the Cloud Service supplier can send the User Job request to the Resource Assign Module inpaw In 1st Out (FIFO) manner.

2.3. DATA UPLOAD WITH DATA SHARINGPROVISION (SENSITIVE)

Although the Cloud Computing is huge developingtechnology, in security purpose of read the it want alot of growth. To beat this disadvantage, we have atendency to implementing 2 styles of Cloud. Once isPublic Cloud and another one is non-public Cloud. Incamera the patient can set the access privileges' foreach and every user they need. Publicly Cloud, theCloud Server can set the access privileges' for each and every user based mostly on their designation. Solegitimate users will read the info keep within thecloud solely up to their privilege level. They aren'tallowed to look at the info on the far side theirprivileges'.

III. PROPOSED SYSTEM

In existing system they used attribute-based encryption and decryption. As they are using three levels user, role, attribute so depends on that they are providing security and efficiency.

As we are using user, role and attribute they have their own disadvantages. To overcome this we introduced proposed system in that we divide key-selection into four sub dividing.

Key- one used for local level encryption with limited number of bits. This encryption is combination of multiplication and addition. The total probability of chances depends on the number of bits. As the bits are changing we are getting the number of combination. In local level the total channels are low. So we are using key-one as limited number of bits.Key-two used for national level encryption with more number of bits compared with local level. The total wanted channels in national level is more compared with local level. So we use more bit length than local level.

Key-three used for international level with high security. So here we have high bit length compared with national level.

Key-four used for VIP-level encryption with more number of bits compared with international level to provide very high security for their data.

The total description of key-selections depends on their register use. The key is givento key-register to store the key and that key is encrypted with data and gives the output. The output of the encryption is taken as input for decryption part.

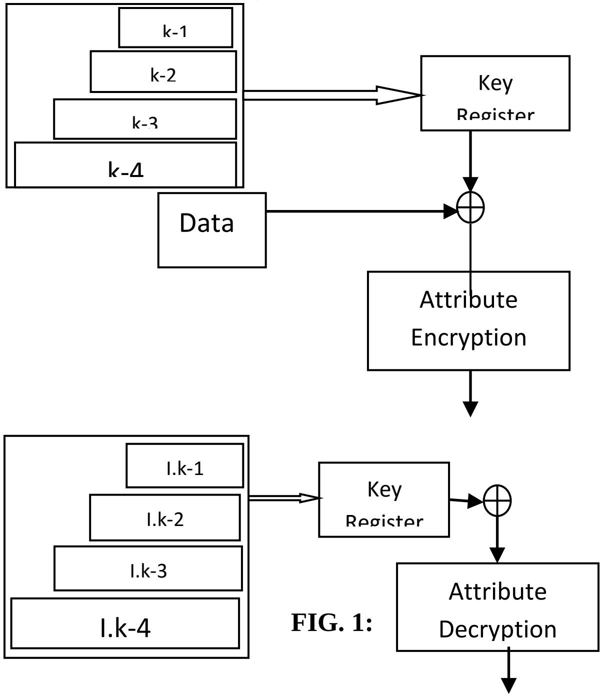


FIG. 1:

PROPOSED SYSTEM

In decryption the receiver key-selection is selected with synchronization with encryption key. The recover key-selection is stored in key register and that key is decrypted the input data which is taken as decryption input and that decryption data is taken as finalized output.

IV. RESULTS

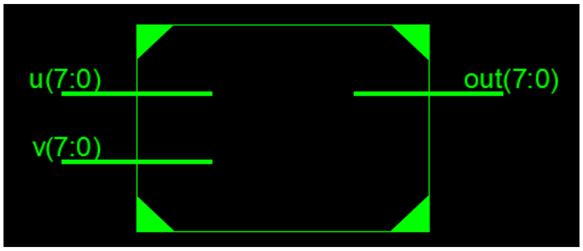
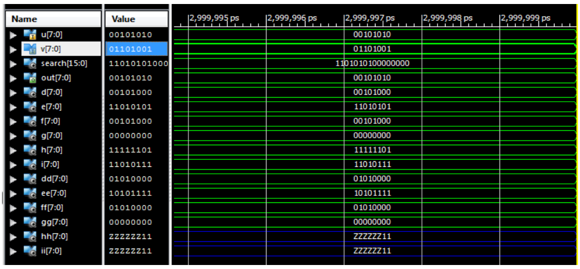


FIG. 2: RTL SCHEMATIC



Name	Value
u[7:0]	00101010
v[7:0]	01101001
search[15:0]	11010101000
out[7:0]	00101010
d[7:0]	00101000
e[7:0]	11010101
f[7:0]	00101000
g[7:0]	00000000
h[7:0]	11111101
i[7:0]	11010111
dd[7:0]	01010000
ee[7:0]	10101111
ff[7:0]	01010000
gg[7:0]	00000000
hh[7:0]	ZZZZZZ11
ii[7:0]	ZZZZZZ11

FIG. 3: OUTPUT WAVEFORM

V. CONCLUSION

The multiplier is the essential elements of the digital signal processing applications. High-performance and fast implementation of existed multiplication is applied to cryptographic systems. In this paper, we execute efficient and high speed architecture ofcryptography. Cryptography is the operation in wireless communication betweentransmissions and receiving of data, the secured data is communicated in an unsecuredchannel between transmitter and receiver with high security. At the transmitter side theoriginal data is converted in to secured sequence as “encryption” as shown in output and atthe receiver side the secured sequence is converted in to original data sequence as“decryption”. Our existed multiplier is used in that conversion and by using this converter weare designing a cryptography application.

VI. REFERENCES

[1] A. Sahai and B. Waters, "Fluffy personality based encryption," in Progresses in Cryptology EUROCRYPT 2005, ser. Address Notes in Software engineering, R.Cramer, Ed. Springer Berlin Heidelberg, 2005, vol. 3494, pp. 457–473.

[2] D. Boneh, A. Sahai, and B. Waters, "Utilitarian encryption: Definitions what's more, difficulties," In principle of Cryptography, ser. Address Notes in Software engineering, Y. Ishai, Ed. Springer Berlin Heidelberg, 2011, vol. 6597, pp. 253–273.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Trait based encryption for fine-grained access control of scrambled information," in Procedures of the thirteenth ACM meeting on PC and correspondences security, ser. CCS '06. New York, NY, USA: ACM, 2006, pp 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Figure content approach trait based encryption," in Procedures of the 2007 IEEE Symposium on Security and Protection, ser. SP '07. Washington, DC, USA: IEEE PC Society, 2007, pp. 321–334.

[5] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the unscrambling of ABE figure writings," IN: Procedures of the twentieth USENIX Meeting on Security, SEC 2011. San Francisco, CA, USA: USENIX Affiliation, Berkeley, 2011.

[6] E. Fujisaki and T. Okamoto, "Secure combination of unbalanced what's more, symmetric encryption plans," in Advances in Cryptology - CRYPTO '99, ser. Address Notes in Software engineering, M. Wiener, Ed. Springer Berlin Heidelberg, 1999, vol. 1666, pp. 537–554.

[7] R. Canetti, O. Goldreich, and S. Halevi, "The arbitrary prophet system, returned to (preparatory rendition)," in Procedures of the Thirtieth Yearly ACM Symposium on Hypothesis of Figuring, ser. STOC '98. New York, NY, USA: ACM, 1998, pp. 209–218.

[8] J. Lai, R. Deng, C. Guan, and J. Weng, "Property based encryption with obvious outsourced unscrambling," IEEE Exchanges on Data Legal sciences and Security, vol. 8, no. 8, pp. 1343–1354, Aug 2013.

[9] B. Waters, "Figure content strategy characteristic based encryption: an expressive, proficient, and provably secure acknowledgment," in Procedures of the fourteenth global meeting on Practice and hypothesis out in the open key cryptography gathering on Open key cryptography, ser. PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.

[10] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "Bland developments for picked cipher extecure quality based encryption," Out in the open Key Cryptography - PKC 2011, ser. Address Notes in Software engineering, D. Catalano, N. Fazio, R. Gennaro, also, A. Nicolosi. Ed. Springer Berlin Heidelberg, 2011, vol. 6571, pp. 71–89.

[11] T. Pedersen, "Non-intelligent and data theoretic secure unquestionable mystery sharing," in Advances in Cryptology - CRYPTO '91, ser. Address Notes in Software engineering, J. Feigenbaum, Ed. Springer Berlin Heidelberg, 1992, vol. 576, pp. 129–140.

[12] D. Boneh and J. Katz, "Enhanced proficiency for CCA-secure cryptosystems assembled utilizing personality based encryption," in Themes in Cryptology - CT-RSA 2005, ser. Address Notes in Software engineering, A. Menezes, Ed. Springer Berlin Heidelberg, 2005, vol. 3376, pp. 87–103.

[13] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a system for quickly prototyping cryptosystems," Diary of Cryptographic Designing, vol. 3, no. 2, pp. 111–128, 2013.

[14] R. Ostrovsky, A. Sahai, and B.Waters, "Characteristic based encryption with non-monotonic access structures," in Procedures of the fourteenth ACM Meeting on PC and Correspondences Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 195–203.

[15] L. Cheung, J. A. Cooley, R. Khazan, and C. Newport, "Collusionresistant bunch key administration utilizing property based encryption," Bunch Situated Cryptographic Conventions, p. 23, 2007.