International Journal for Modern Trends in Science and Technology, 7(03): 205-211, 2021

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0703034
Available online at: http://www.ijmtst.com/vol7issue03.html

AES and RSA Encryption Based Protocols for Cognitive Radio Network Applications

Tumati Ramji Subhas

Krishna University College of Engineering and Technology, Andhra Pradesh, India.

To Cite this Article
Tumati Ramji Subhas, "AES and RSA Encryption Based Protocols for Cognitive Radio Network Applications", *International Journal for Modern Trends in Science and Technology*, Vol. 07, Issue 03, March 2021, pp.: 205-211.

Article Info
Received on 15-February-2021, Revised on 12-March-2021, Accepted on 17-March-2021, Published on 20-March-2021.

ABSTRACT

Cognitive radio networks are intelligent networks that can sense the environment and adapt the communication parameters accordingly. These networks find their applications in co-existence of different wireless networks, interference mitigation, and dynamic spectrum access. Unlike traditional wireless networks, cognitive radio networks additionally have their own set of unique security threats and challenges, such as selfish misbehaviors, self-coexistence, license user emulation and attacks on spectrum managers; accordingly the security protocols developed for these networks must have abilities to counter these attacks. This paper presents a novel cognitive authentication protocol, called CoG-Auth, aimed to provide security in cognitive radio networks against threats to self-co-existence. CoG-Authdoes not require presence of any resource enriched base stations or centralized certification authorities, thus enabling it to be applicable to both infrastructure and ad hoc cognitive radio networks. The CoG-Authdesign employs key hierarchy; such as temporary keys, partial keys and session keys to fulfil the fundamental requirements of security. In this authentication we are going to implement a hybrid encryption algorithm using AES and RSA. By implementing this hybrid algorithm for CoG-Auth we are going to achieve lesscomputational intensive, high performance, more secure and successful authentication and transmission rate.

KEYWORDS: *Authentication; Cognitive Radio; Protocol; Security; Cryptography; AES; RSA*

INTRODUCTION

Cognitive radio networks are becoming an increasingly important part of the wireless networking due to the scarcity of spectrum resources. Cognitive radio (CR) devices, aka secondary users – SUs, can initiate the communication using the spectrum holes spared by the licensed primary users (PUs). Sensed spectrum holes are formed into a list called free channel list (FCL), and a common control channel (CCC) is employed to exchange FCL between base station and SUs, in case of infrastructure CR networks, or among individual SUs in case of ad hoc CR networks. Compared to conventional wireless networks, CR networks additionally suffer from licensed user emulation and attacks on spectrum managers unless robust security mechanisms are in place. One of the most common types of attacks in CR networks is the primary user emulation (PUE) attack which could affect both types of cognitive radio networks. Attacks like these and spectrum sensing data falsification (SSDF) can betackled by a bio-inspired consensus-based spectrum sensingschemes. A puzzle based punishment mechanism ispresented to help counter selfish behavior attacks.Selfishness is also tackled at the medium access control(MAC) layer by providing hindering detection program andcorrection mechanism. Trust establishment is importantto ensure security among the communicating CR nodes.Work proposed investigates trust-based security systemfor CR networks where CR node's trust value is analyzedaccording to its previous behavior in the network. A novelauthentication scheme based on trust value updated model(TVUM) is presented for grouped networks to ensureauthentication. SSDF attacks can also be mitigated byintegration of trust and reputation. Onion Peeling approachis one, where all the CR nodes are initiallyconsidered honest, subsequently they are consideredmalicious when a specific threshold is overcome.

Security and authentication of CR nodes can be achievedthrough cryptographic techniques. An authenticationprotocol is presented that can be integrated with theextensible authentication protocol (EAP). For prettygood privacy (PGP), key authentication is obtained viachains of public key certificates. Theprotocol presented is based on clustered infrastructurebased dynamic spectrum access where the spectrum decisionin each cluster is coordinated by some certification authority(CA). Confidentiality and authentication across the networkcan also be provided by applying cryptographic transforms tothe medium access control (MAC) frames. A security sub layerat the MAC level is implemented in the standards likeIEEE 802.16e, and IEEE 802.22. The mentionedstandards require presence of an infrastructure to performsecurity and other communication related activities. The protocols developed for infrastructure networks cannot bedirectly employed in a multi-hop ad-hoc CR network due tothe absence of a trusted entity to act as a server for controland distribution of keying material. Adversaries canexploit the vulnerabilities of a multi-hop CR MAC and thecommunication taking place in the CCC; therefore, it isnecessary to provide security in pre and post CCCtransactions. It is believed that cognitive radio networks havestrict security requirements at two stages; duringenvironment sensing and during CCC transactions.A robust CCC security scheme is vital and can prevent thespread of falsified information which may result due to weaksecurity during environment sensing. Public keyCryptography (PKC) has also been employed to implementsecurity in CR networks. Notably,both these protocols suffer from the serious problem of manin the middle attacks because of lack of confidentialityamong the communicating entities, also they do not provideany integrity checking of the messages exchanged and thereis no mechanism in place to verify non-repudiation. Thementioned security protocols require thepresence of a CA for the provision of the keys; it is thefundamental drawback of these protocols because, firstly,CA cannot exist for resource constrained infrastructure lessad-hoc cognitive radio networks, and secondly, CA whenattacked itself becomes single point of failure.

Taking into account constraints of CR networks and thedrawbacks of several of the existing protocols describedabove, a novel authentication protocol called CognitiveAuthentication Protocol, *CoG-Auth*, is presented in this paperwhich is aimed to overcome spectrum access related securitythreats. *CoG-Auth*not only overcome shortcomings mentioned above but additionally provide all the salientsecurity features, such as robustness, mutual authentication,confidentiality, integrity and non-repudiation; additionally*CoG-Auth*can be applied equally to both infrastructure andad hoc CR networks.

HYBRID ENCRYPTION PROTOCOL (*COG-AUTH*)

In this hybrid encryption protocol we are going to use two different cryptographic algorithms (AES & RSA). We can go in detail with each algorithm:

A) Advanced encryption Algorithm (AES):

The Advanced Encryption Standard (AES) specifies a FIPS-approvedcryptographic algorithm that can be used to protect electronic data. The AES algorithm is asymmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.Encryption converts data to an unintelligible form called cipher text; decrypting the ciphertextconverts the data back into its original form, called plaintext.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in P. L. 100-235) requires cryptographic protection.

Other FIPS-approved cryptographic algorithms may be used in addition to, or in lieu of, this standard. Federal agencies or departments that use cryptographic devices for protecting classified information can use those devices for protecting sensitive (unclassified) information in lieu of this standard.

In addition, this standard may be adopted and used by non-Federal Government organizations.

Such use is encouraged when it provides the desired security for commercial and private organizations.

The algorithm specified in this standard may be implemented in software, firmware, hardware, or any combination thereof. The specific implementation may depend on several factors such as the application, the environment, the technology used, etc. The algorithm shall be used in conjunction with a FIPS approved or NIST recommended mode of operation. Object Identifiers (OIDs) and any associated parameters for AES used in these modes are available at the Computer Security Objects Register (CSOR).

Implementations of the algorithm that are tested by an accredited laboratory and validated will be considered as complying with this standard. Since cryptographic security depends on many factors besides the correct implementation of an encryption algorithm, Federal Government employees, and others, should also refer to NIST Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal Government*, for additional information and guidance.

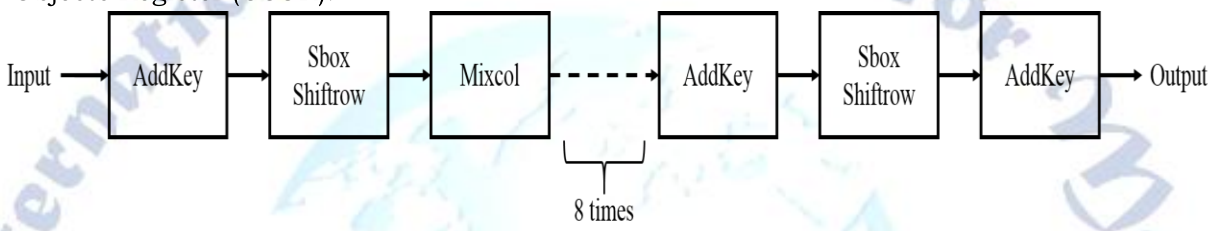

Fig-1.: Basic Architecture

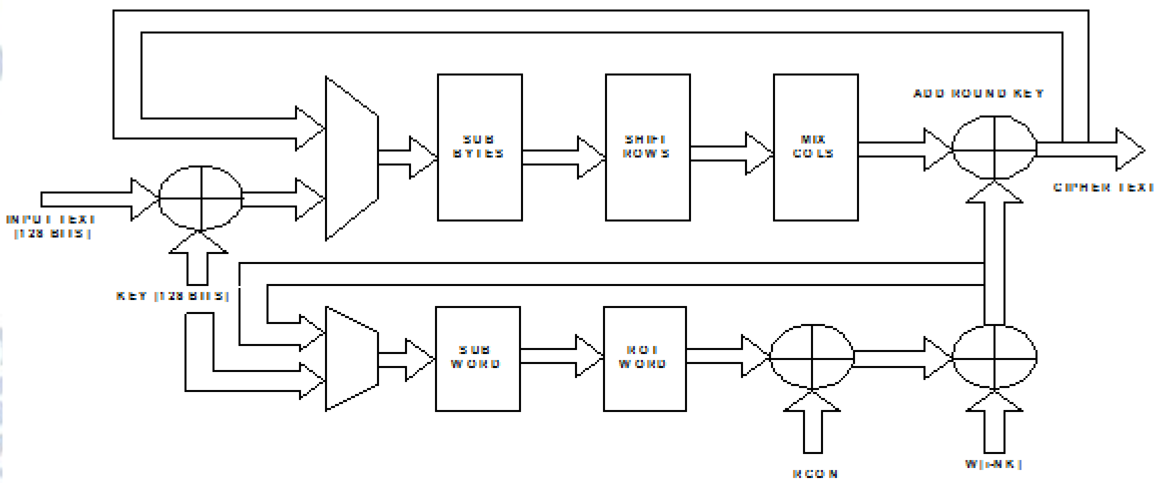

Fig-2.: Architectural Block Diagram

B) RSA (cryptosystem):

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician working for the UK intelligence agency GCHQ, had developed an equivalent system in 1973, but it was not declassified until 1997.

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message. Breaking RSA encryption is known as the RSA problem; whether it is as hard as the factoring problem remains an open question.

RSA is a relatively slow algorithm, and because of this it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

The idea of an asymmetric public-private key cryptosystem is attributed to Diffie and Hellman, who published the concept in 1976. The same two also introduced digital signatures and attempted to apply number theory. Their formulation used a shared secret key created from exponentiation of some number, modulo a prime number. However, they left open the problem of realizing a one-way function, possibly because the difficulty of factoring was not well studied at the time.

Ron Rivest, Adi Shamir, and Leonard Adleman at MIT made several attempts over the course of a year to create a one-way function that is hard to invert. Rivest and Shamir, as computer scientists, proposed many potential functions while Adleman, as a mathematician, was responsible for finding their weaknesses. They tried many approaches including "knapsack-based" and "permutation polynomials". For a time they thought it was impossible for what they wanted to achieve due to contradictory requirements. In April 1977, they spent Passover at the house of a student and drank a good deal of Manischewitz wine before returning to their home at around midnight. Rivest, unable to sleep, lay on the couch with a math textbook and started thinking about their one-way function. He spent the rest of the night formalizing his idea and had much of the paper ready by daybreak. The algorithm is now known as RSA – the initials of their surnames in same order as their paper.

Clifford Cocks, an English mathematician working for the UK intelligence agency GCHQ, described an equivalent system in an internal document in 1973. However, given the relatively expensive computers needed to implement it at the time, it was mostly considered a curiosity and, as far as is publicly known, was never deployed. His discovery, however, was not revealed until 1997 due to its top-secret classification

The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption.

RSA involves a *public key* and a *private key.* The public key can be known by everyone and is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

The basic principle behind RSA is the observation that it is practical to find three very large positive integers e,d and n such that with modular exponentiation for all$m$:

$$(m^e)^d /mod\{n\} = m$$

and that even knowing e and n or even m it can be extremely difficult to find d.

Additionally, for some operations it is convenient that the order of the two exponentiations can be changed and that this relation also implies:

$$(m^d)^e /mod\{n\} = m$$

HYBRID ENCRYPTION PROTOCOL RESULTS

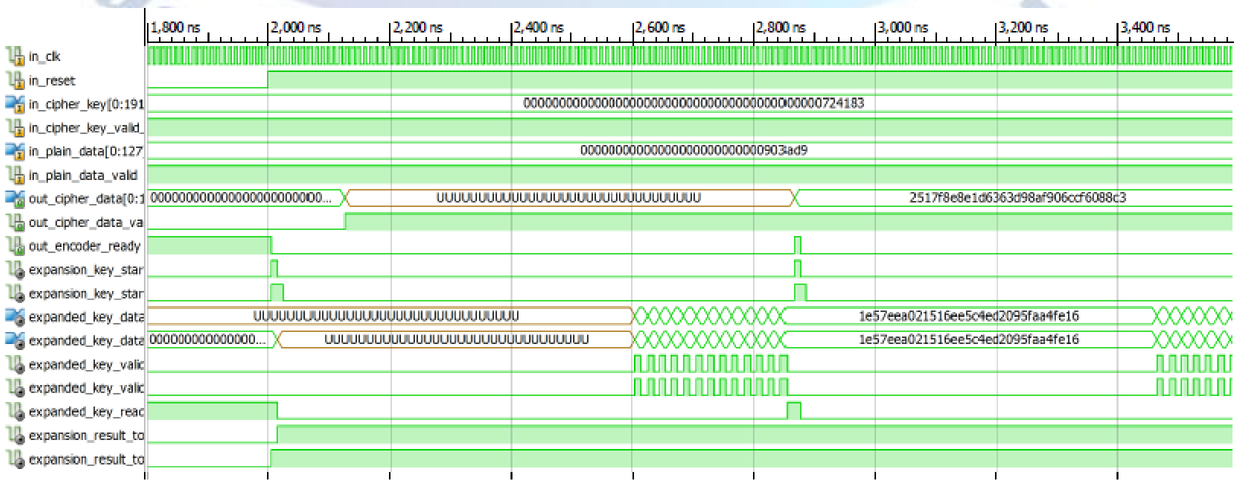

Fig3.: AES encryption

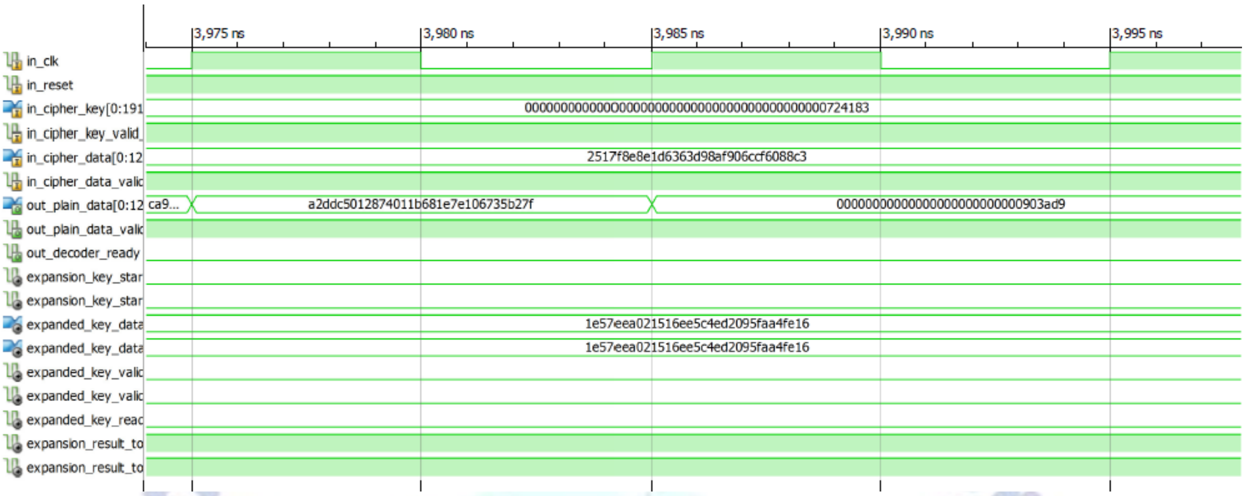

Fig4: AES decryption

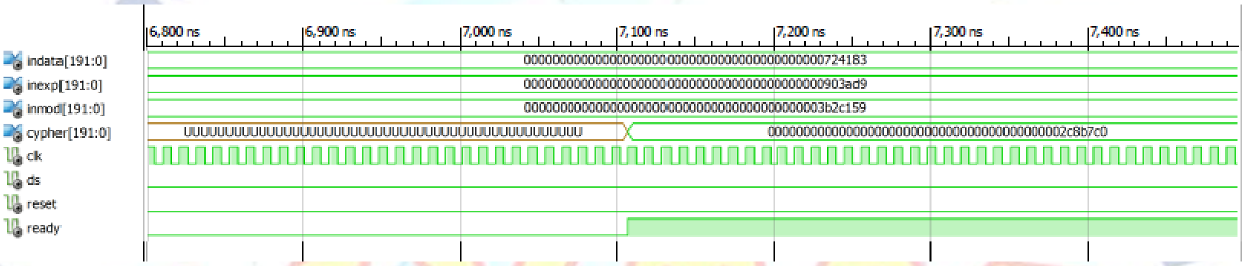

Fig5: RSA encryption

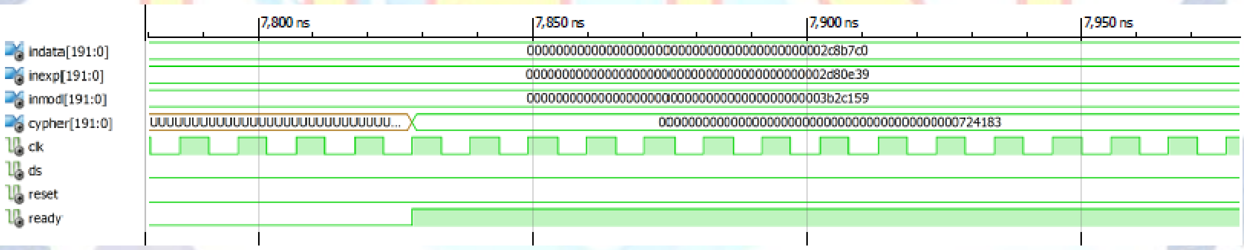

Fig6: RSA decryption

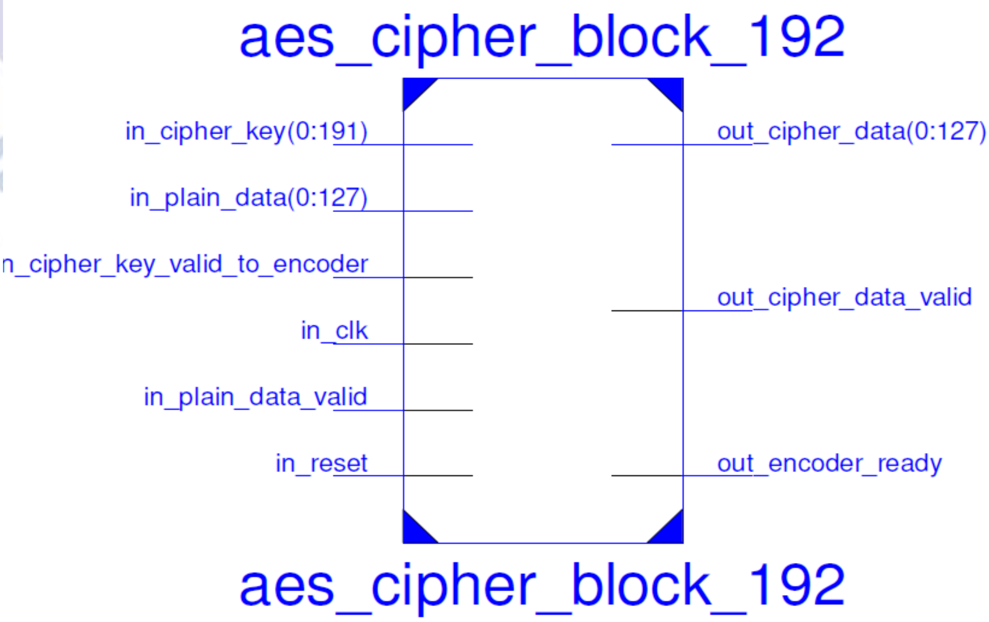

Fig7: AES rtl

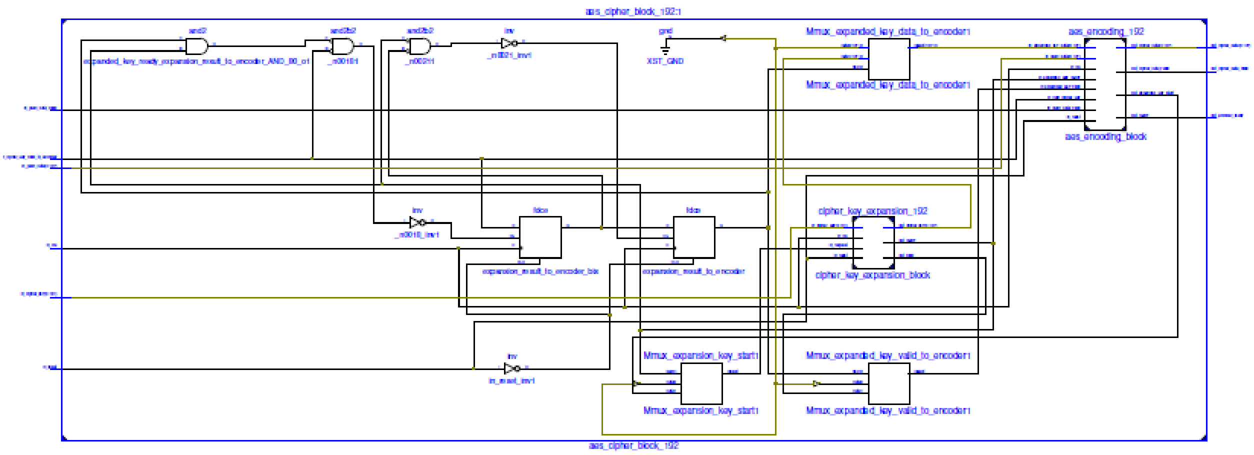

Fig8: AES rtl

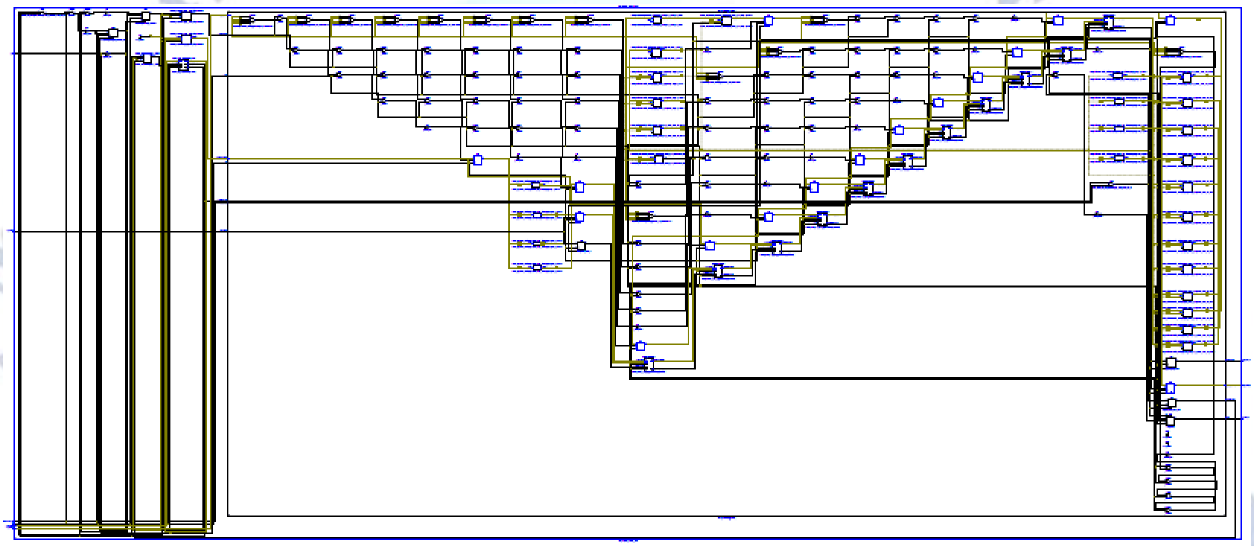

Fig9: AES rtl

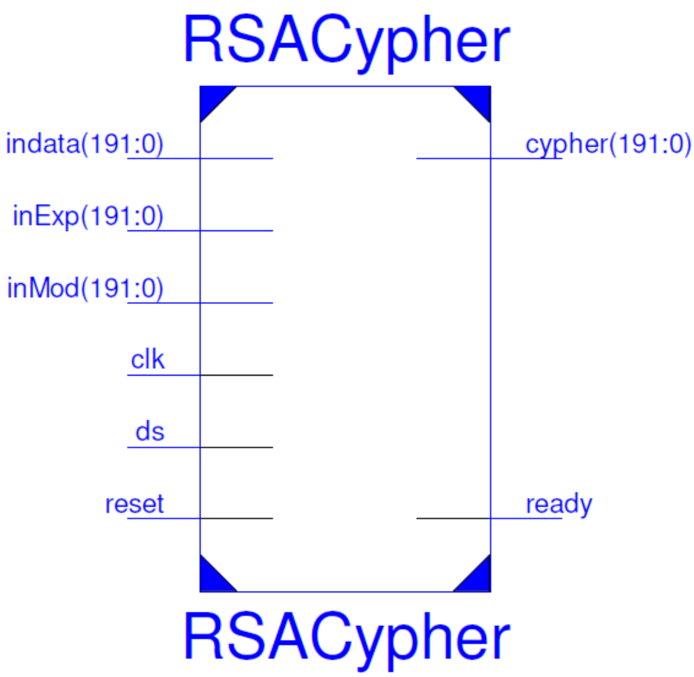

Fig10: RSA rtl

CONCLUSION

CR networks face unique security problems notencountered by conventional wireless networks. In this papera novel authentication protocol for CR networks, *CoG-Auth*,has been proposed by taking into account the security threatsand constraints of the CR devices. The protocol isimplemented using RSA/AES and its performance isanalysed and compared with the standard IEEE 802.16ePKMv2. It is found that *CoG-Auth*is secure and efficientenough, and gave better results for several performanceindicators such as authentication time, successfulauthentication and transmission rate. The *CoG-Auth*alsofulfils the fundamental security requirements, does notrequire the provision of any resource enriched base station orCAs, thus enabling it to be applicable to both Infrastructureand ad hoc CR networks.

REFERENCES

[1] Wyglinski, A. M., Nekovee, and M., Hou, Y.T.: 'Cognitive RadioCommunications and Networks: Principles and Practice', Elsevier,2009

[2] Chao Chen., Hongbing Cheng., and Yu-Dong Yao.: 'CooperativeSpectrum Sensing in Cognitive Radio Networks in the Presence of thePrimary User Emulation Attack', Wireless Communications, IEEETransactionson , vol.10, no.7, pp.2135-2141, 2011

[3] Tang, H., Yu, F.R., Huang, and M., Li, Z.: 'Distributed consensusbasedsecurity mechanisms in cognitive radio mobile ad hoc networks',Communications, IET , vol.6, no.8, pp.974-983, 2012

[4] Huayi Wu., and Baohua Bai.: 'An Improved Security Mechanism inCognitive Radio Networks', Internet Computing &InformationServices (ICICIS), 2011 International Conference on , vol., no.,pp.353-356, 2011

[5] Kyasanur, P., and Vaidya, N.H.: 'Selfish MAC layer misbehavior in wireless networks', Mobile Computing, IEEE Transactions on , vol.4, no.5, pp. 502- 516, 2005

[6] Parvin, S., and Hussain, F.K.: 'Trust-Based Security for Community Based Cognitive Radio Networks', Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on, vol., no., pp.518-525, 2012

[7] Yang Ya-tao., Yuan Zheng., Fang Yong., and Zeng Ping.: 'A Novel Authentication Scheme Based on Trust-value Updated Model in Adhoc Network', COMPSAC, pp. 643-645, 2007

[8] Ruiliang Chen., Jung-Min Park., Hou, Y.T., and Reed, J.H.: 'Toward secure distributed spectrum sensing in cognitive radio networks',Communications Magazine, IEEE , vol.46, no.4, pp.50-55, 2008

[9] Clancy, T.C., and Goergen, N.: 'Security in Cognitive Radio Networks: Threats and Mitigation', Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on , vol., no., pp.1-8, 2008

[10] Wenkai Wang., Husheng Li., Yan Sun., and Zhu Han.: 'CatchIt: Detect Malicious Nodes in Collaborative Spectrum Sensing', Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE ,vol., no., pp.1-6, 2009

[11] Kuroda, M., Nomura, R., and Trappe, W.: 'A Radio-independent Authentication Protocol (EAP-CRP) for Networks of Cognitive Radios', Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on , vol., no., pp.70-79, 2007.

[12] Jyh-Cheng Chen., and Yu-Ping Wang.: 'Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience', Communications Magazine, IEEE , vol.43, no.12, pp. supl.26- supl.32, 2005

[13] Capkun, S., Buttyan, L., and Hubaux, J.-P.: 'Self-organized public-key management for mobile ad hoc networks', Mobile Computing, IEEE Transactions on , vol.2, no.1, pp. 52- 64, 2003

[14] Jakimoski, G., and Subbalakshmi, K.P.: 'Towards Secure Spectrum Decision', Communications, 2009. ICC '09. IEEE International Conference on , vol., no., pp.1-5, 2009

[15] IEEE Std. 802.16e.: 'IEEE Standard for local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless access Systems', IEEE Press, 2005

[16] IEEE 802.22/D0.1, Draft Standard for Wireless Regional Area Networks Part22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands, IEEE Standard, 2006, pp.235–247.

[17] Lima, M., dos Santos, A., and Pujolle, G.: 'A survey of survivability in mobile ad hoc networks', Communications Surveys & Tutorials, IEEE, vol.11, no.1, pp.66-77, First Quarter 2009

[18] Safdar, G.A., and Neill, M.O.: 'A novel common control channel security framework for cognitive radio networks', Int. J. Autonomous and Adaptive Communications Systems, Vol. 5, No. 2, pp.125–145,2012

[19] Burbank, J.L.: 'Security in cognitive radio networks: The required evolution in approaches to wireless network security', Cognitive Radio Oriented wireless Networks and Communications (CrownCom), pp. 1-7, 2008

[20] Li Zhu., and Huaqing Mao.: 'Research on Authentication Mechanism of Cognitive Radio Networks Based on Certification Authority', International Conference on Computational Intelligence and Software Engineering (CiSE), pp.1-5, 2010

[21] Li Zhu., and Huaqing Mao.: 'An Efficient Authentication Mechanism for Cognitive Radio Networks', Asia Pacific Power and Energy Engineering Conference (APPEEC), pp.1-5, 2011

[22] Mills, D.L.: 'Internet time synchronization: the network time protocol', Communications, IEEE Transactions on, vol.39, no.10, pp.1482-1493,1991

[23] Altaf, A., Javed, M.Y., and Ahmed, A.: 'Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005',Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD '08. Ninth ACIS International Conference on , vol., no., pp.335-339, 2008

[24] Rivest R., Shamir A., and Adelman L.: 'A method for obtaining digital signatures and public key cryptosystems', Communications of the ACM, 21, pp.120-126, 1978

[25] National Inst. Of Standards and Technology, 'Federal Information Processing Standard Publication 197, the Advanced Encryption Standard (AES)', 2001