Overview of Safety and Security in Multi-Services Data Transfer Network

Author Details: Mai Anh Nguyen
University of Economics - Technology for Industries, Vietnam
Correspondence: **Mai Anh Nguyen**, 456 Minh Khai, Hai Ba Trung, Ha Noi

Abstract:
Security, safety, and confidentiality of information on data transmission networks are always essential and urgent requirements for each country in the current period, especially when cyber operations are present. With the aim of improving information security efficiency on multi-service data transmission network, the study has reviewed relevant studies and proposed future research directions.

Keywords: *Safety, security, multi-services data transfer network.*

1. Introduction

Data transmission networks are widely used in most areas of life, economy - society, security and defense to meet the needs of information exchange. Building high-speed communication networks with the ability to ensure quality and service is the premise for building and developing a modern information society. Depending on the nature of tasks and requirements of each industry, data transmission networks are built and organized into separate and independent networks. However, today's micro-communication networks have a general tendency to converge to be able to transmit many types of information on a single network platform in which IP / MPL s [1], [2], [4] , [12] are the two fundamental technologies for building such converged networks.

In addition to the development of data transmission networks, ensuring security, safety and security for an information network is one of the top factors determining the quality and availability of the network, because there are always potential risks of information insecurity, serious consequences on economy, politics, military and national security. Especially, for the information network of Party, State and Military agencies, the requirements for information and data safety and confidentiality are always necessary and urgent.

The problem of information security on data transmission networks has been paid special attention by many countries around the world, there have been a lot of research to create security standards, confidential systems and security solutions for the network. multi-service data transmission. In which the security protocol IP s ec can be considered as the best protocol for implementing data encryption at the IP layer [4], [9] on the technological platform of multi-service data transmission network. IPSec is a set of open standards that provide security and access control services at the IP layer. However, since the data transmission network is a high speed transmission network that is rapidly developing, transmitting many types of information services, thus posing a number of problems for IPsec to develop and towards perfection [1], [4]. One of the factors that need to be done is to improve the performance and computational speed of an encryption device because IPsec has to handle many complex and resource-consuming algorithms, especially the cryptographic algorithms used. in the IPSec data encryption protocol E SP or IKE key exchange protocol.

In the world, there have been many innovative research projects to improve the speed and performance of IPSec's processing, typically the works of A. Salman, M. Rogawski and J. Kaps [8] (2011); L.Wu, Yun Niu, X. Zhang [40] (20 13) studied hardened IP sec protocol based on FPGA technology and achieved great success in terms of speed and processing performance. As for the cryptographic solution, the above authors used standard AE s encryption algorithm for E s P and Diffie-Hellman key agreement protocol with parameter RsA 1024, 2048 bits for IKEv2. Regarding the AES encryption standard hardening on FPGA to improve the efficiency of cryptographic processing, there are recent studies such as the work of Kaur A, Bhardwaj P and Naveen Kumar [37] (2013), Ashwini R. Tonde and Akshay P. Dhande [10] (2014), or the results of investigations of the works in this direction by Shylashree.N, Nagarjun Bhat and V. Shridhar [58] (2012) showed that the results are very significant thanks to the optimization and use of advanced techniques (pipeline) when implementing on hardware. However, the research on the installation on hardware related to optimization or improvement of cryptographic components is still very limited. For the IKE key exchange protocol, in [17] we propose a possible alternative to the elliptic curve cipher (ECC) for the RSA parameter in the Diffie - Hallman key agreement protocol, with ECC also a lot of research. Research in theory and practice to increase the efficiency of point multiplication (which is the fundamental and important calculation of ECC) to help reduce key exchange time between entities in information network.

From a cryptographic perspective, most countries in the world organize to build their own cryptographic systems to keep sensitive information as confidential as possible, especially for information systems. used in defense security. In Vietnam, the Government Cipher Committee is a leader in the field of researching and implementing security solutions for information systems. Security products are developed based on the world's standards such as IPSec [9], SSL / TLS [7], OpenVPN [18], towards innovation and specialization of open source products such as OpenSwan, StrongSwan, OpenVPN or some solutions to deploy IP c in the form of specialized equipment [1] are researched, designing and integrating cryptographic techniques in Vietnam, including authentication, security and data integrity. in which the speed of encryption and decoding is about 30Mb / s for the encoding device at the access layer and about 80 Mb / s for the encryption center. Domestic research institutions such as the Institute of Electronics under the Military Institute of Science and Technology have organized state-level research projects on designing high-performance cryptographic equipment [3]. However, the research to improve cryptographic algorithms or in-depth analysis of optimizing the installation of cryptographic solutions on hardware to achieve efficiency in terms of speed and resource usage is rarely mentioned.

2. Literature review

2.1. Features of multi-service data transmission network

Multi-service data transmission network is a high-speed transmission network, modern technology, using multi-protocol label switching transmission (IP / MPL). Network connection at all hubs is using 100 / 1000Mbps fiber optic cable, all connections ensure high privacy, security, safety and redundancy, allowing 24/7 smooth operation. [twelfth].

On the advanced and synchronous infrastructure, the multi-service data transmission network provides for many services such as: Video conferencing connecting to remote access virtual private network (Remote Access IP VPN) data exchange and data, IP voice services.

Multi-service data transmission network uses TCP / IP protocol using OSI model, depending on the nature and tasks of each industry, the network can be built separately and relatively independently for an organization or organ. In which, network resources such as network equipment, network services and users are scattered over a defined geographical area and serve a specific need. Sub-system [1], [2], [4] multi-service network consists of the main layer:

- Core layer: The transmission equipment ensures operation for the whole network.

- Border layer: Including transmission equipment to ensure the provision of network infrastructure for services.

- Access layer: Including transmission equipment to ensure access for users on the whole network.

Backbone network is the backbone of the entire data transmission network, the network has many potential security and safety risks such as unauthorized access or attack from the edge layer, access layer, or existing ATM network. other interconnected network areas. Ensuring the safety and security of the network is very important [1], [2], [18], [45]

2.2. Safety and security in multi-service data transmission network

Network security

Model O I (Op n yst ms Int rconn ction) is an interactive model between open systems proposed by the International Organization for tandardization (ISO) through I O 7498 [29]. Network security is one of the basic problems of the network, so after giving the OI model, IO proposed a security architecture (s security archit ctur) via IO 7 standard 98□2 [30], which defines basic terms and concepts in network security and security architecture for O I. Security in an OI environment is a combination of measures to preserve resources and assets of the network in the process. interaction between open systems. Objects of protection of the network security system include:

Information and data (including software and passive data related to security measures)

Communication services and data processing services

- Network equipment and facilities

Risks are potential problems, which may cause undesirable effects on the data transmission network; A vulnerability is any weakness on the system that can be exploited to create a network failure; An attack is the deliberate act of affecting one or more components of a system to force a certain risk to occur.

Security services

Security services are services that add security to a system and are designed to defend against certain types of attacks. These services are generally categorized as follows [62]:

Authentication: Ensuring a user joining the system is himself, from the initiation to the end of a session.

Access Control: In addition to the authentication service, access control is a service that controls / restricts the access to a system or an application on the network.

Data Security: This service is to protect data against passive attacks. This not only applies to the content of the packets, but also includes keeping the beginning and end of the packet confidential.

Data integrity: The purpose of this service is to detect data changes during communication.

Anti-rejection: This is intended to solve the problem that a media participant refuses to send / receive its data, both sides of a transaction can prove that the other party sent / receive data.

Availability: Resources on the network should be available with valid access at all times. An attacker will not be able to prevent or interrupt access to these resources.

2.3. Security mechanisms are based on cryptography

A security mechanism is a combination of specific technical operations used to create security services [55]. These security mechanisms are detailed in many documents, in I O 7 98–2 they are outlined as follows:

encryption mechanism

An encryption mechanism is used to secure the data transmitted on the channel. The two main types are symmetric and asymmetric ciphers.

- symmetric cipher, also known as secret key system, is the cryptosystem in which it is possible to find out the key used to decrypt (decryption key) the keyword used to encrypt (the encryption key) and opposite.

- Asymmetric cipher, also called public key cryptosystem, is the cryptosystem in which it is impossible to find the key to decrypt the cryptographic key and vice versa. The encryption key is also known as the public key, and the decryption key is also known as the private key.

digital signature mechanism

The essence of the electronic signature mechanism is that the signature can only be generated from private and specific information of the signer. When checking the signature, it is possible to verify that only the person with that particular information can create the signature, in other words an electronic signature is used to confirm the legality of the information sent online. .

The electronic signature mechanism consists of two algorithms: signature creation (which is secret and only available to the signer) and checking the signature (which is publicly available). In message signing procedure, the sender of the message (also the signer) uses the signature algorithm to compute the signature (usually a fixed length binary string) from the message to be signed. . In the signature check procedure, the signature checker (often also the receiver of the message) uses the public signature check algorithm of the sender to verify that the signature sent kms the message is correct. generated from sender or not.

access control mechanism

This type of mechanism uses the authentic identity of an entity to identify and enforce appropriate access rights for that entity. If an entity tries to use a resource that it doesn't have access to or its access patterns are inappropriate, access control blocks that access and can log what happened. as part of the audit trail for later auditing.

data integrity mechanism

Data integrity can be the integrity of a data packet or the integrity of a data stream. Determining the integrity of a data packet is done through two processes, at the sending entity and at the receiving entity. The send entity appends after the packet a value calculated from the packet itself through a one-way function, which is called the message digest value. The receiving entity, after receiving the data packet, separates the data part from the summary value, computes the summary value from the data part and compares it with the received portion, i.e. is attached to the data packet by the sending entity, thereby determining whether the data is modified during transmission or not.

For data flow integrity, in addition to ensuring the integrity of each data packet, people also append some additional information such as the number of packets, ... to the beginning of each packet. data before calculating and appending values to summarize the message. Thus, the data stream will be verified as complete or not.

authentication exchange mechanism

The authentication exchange mechanism is located in a layer of the hierarchical network model to authenticate the associated entities. If an entity fails to authenticate, it will not be able to connect to the target entity, and the system on the target station will log the connection request process, as well as the specific operations it performed on a audit trail records for later inspection. There are many techniques used to create authentication exchange, such as passwords, cryptography techniques, etc., using cryptographic techniques in combination with handshake protocols can prevent the repeated transmission of packets. news on the channel. Authentication exchanges can also be used in conjunction with an anti-tamper service to demonstrate responsibility for sending / receiving information on the network.

the traffic padding mechanism

The media buffering mechanism appends "compensated" data to the packet to ensure that the sizes of all packets transmitted on the channel are equal. This mechanism must be used in conjunction with a new cryptographic mechanism to be effective, since all the packets on the channel are then of the same size, encrypted, thus detecting information through. analyzing the opponent's channel throughput will be difficult to succeed.

routing control mechanism

The route selector control mechanism analyzes and imposes a route on the channel for the data flow, which can be selected automatically (dynamic routing) or pre-set (static routing) to choose the route. Secure data flow. The selection of a route relates to the security label of the data, for each certain security label (determining the sensitivity of the data) needs to choose a route with adequate security.

notary mechanism

An implementation validation mechanism verifies the attributes of data communicated between two or more entities such as data integrity, transmission / receiving time, and destination. This guarantee is trusted and recognized by an intermediary notary organization that all media entities trust. On the route between a pair of communication entities with multiple segments, each communication segment can use appropriate digital signatures, cryptographic techniques and integrity for the notary organization there to verify. When verification is needed, data transmitted between entities will be sent to notaries for confirmation.

2.4. Location of security services according to the hierarchical network model

In fact, when building security solutions in the stratified network, it is necessary to combine many security services for the most effective protection. ISO 7498–2 [30] sets out the following principles to build security systems:

Network security systems are built with security services at many levels.

Functions that are added according to security requirements cannot be identical to those that are available by the layers in the OSI.

- Do not violate the independence of the layers and minimize the number of reliable functions.

The security functions added to a layer need to be defined such that they must be implemented as complete modules.

The security services in TCP / IP are set as follows:

- At the network access layer, you can set the connection-oriented security service and secure the communication flow.
- At the IP layer, it is possible to install non-connection security services and secure communication flow.
- Transport layer can set connection-oriented and non-connection security services.
- At the application floor all security services can be placed. Selected school security services can only be located at the application layer.

2.5. The meaning of using cryptography in security at the IP layer

TCP / IP is a standard protocol of Int rn t and is supported by most applications on the network. TCP / IP-based services such as e-mail, databases, Web services, file transfers, video and audio transmission, etc., data of these applications are contained in IP packets and are protected. protection thanks to safety services at the Network floor. Each subnet needs only one IP packet protection device and a Gat way to allow all IP packets to pass through it before going to the public channel [9], [63].

No need to interfere and modify existing and transparent applications to the user: Due to being located at the N twork layer, security services do not care about the application that generates the data contained in the IP packet. All IP packets of different information services are handled in a common way. Therefore, we do not need to tamper with and modify the structure of the application we need to protect. All IP packet protection operations are performed transparently to the user, no need to intervene in the implementation of the security services and also do not need to perform any work. with the application.

Enhanced Fir wall's capabilities: We know that there are some attacks against packet filtering Fir wall such as packet filtering, spoofing source addresses, hijacking connections, etc. packet filtering rules. When installing cryptographically secure services at the N twork layer, the above attacks will be prevented. Conversely, protecting IP packets with cryptographic techniques cannot intercept the packets by relying on packet filtering rules. If we combine packet filtering and IP packet protection with cryptographic techniques we can create highly secure Fir Walls.

Reducing the number of safety service intervention clues: By implementing the safety service at the application and transport level, we can only create a secure channel between two end systems, that is, between two devices. Terminals whose information needs to be exchanged are protected. As the end system in the intranet is increased, the number of clues that need secure service interventions will also increase. This leads to difficulties in costs, system administration, training and user training ... Due to cryptographic interference at the Network layer, we can create Gat ways that can intercept and protect. IP packet protection of all devices in the local network and secure service only needs to be integrated at this Gat way.

Allows to protect data of some real-time applications: Using cryptography at another layer in the ISO model is not always possible. Moreover, real-time applications require data streams to be transferred almost instantaneously, not allowed for long periods (eg voice, television ...). For such applications, it is appropriate to install secure services at the Network layer and the network access layer. However, the limitation of interfering with the network access layer is to use the online encryption method, at the data intermediary nodes must decode to find the routing information, then re-encoded to go forward. This is very complicated and makes very large packets due to the encoding and decoding process many times. When installing at the N twork layer, we use the end-to-end encryption method [63], in which the communication is kept in a clear format and the IP packet does not need to be decoded, encrypted at the communication nodes. intermediaries.

Some limitations of data protection at IP layer:

It is difficult to install some security services, especially the authentication and anti-denial services.

- Only one protection mechanism for all data of applications.

- When the focal points in the intranet are involved, it is necessary to serve many security services and multiple connection directions at the same time, so it requires high bandwidth, and the speed of processing encryption and decoding must be large to respond. to meet the requirements of reality. This is a problem that is researched and interested in solving.

- It requires system administrators to have good knowledge of technology and network administration.

- The internal network inside the Gat way protecting the IP packet must be proactive in ensuring safety and security.

2.6. Security in multi-service data transmission network

Security studies for multi-service data transmission networks are mainly dealt with at the edge or access layer, the security device is located between the internal network location and the wide area data transmission network. or end-to-end security, the main technology platform at these layers is IP, so the main security solution is to handle security at the IP layer [1], [2], [7], [32]. In this location, transmission equipment (usually r or gat routers) will either be built in or have security service providers using cryptography built in. In fact, the most popular and effective solution is to create virtual private networks (VPN - Virtual Privat N twork). Each VPN will create a virtual tunnel connecting between 2 endpoints. Data exchanged inside the tunnel will be encrypted using cryptographic technology. VPNs provide security by using tunn ling protocol and through security procedures such as encryption. A VPN security model offers:

Confidentiality Even when the network is blocked at the packet level, the attacker can only see encrypted data.

- Sender Authentication Prevent users from unauthorized access to VPN.

Message integrity Detect fake or modified messages. Popular secure VPN protocols developed include [7], [31], [32], such as IPSec (Internet Protocol Security), SSL / TLS (Secure Sockets Layer / Transport Layer Security), DTLS (Datagram Transport Layer Security), MPPE (Microsoft Point-to-Point Encryption), SSTP (Microsoft Secure Socket Tunneling Protocol), SSH VPN (Secure Shell).

In which IPSec protocol meets most security goals: Authentication, integrity and security, IP c encrypts and encapsulates IP packets inside IPSec packets, decrypts the original IPSec packets at the end. tunnel and forward to destination.

All over the world, network security products are available using one of the above protocols. Software solutions such as Open wan, in wan (IPSec), OpenSSH (SSH), Op nVPN, oftEther VPN (SSL / TL), these products can be easily deployed on regular computers but often performance limitations due to the computer processor's ability to process the encoding / decoding. Some software solutions allow to combine with accelerating devices for encryption and decoding to overcome this limitation with hardware solutions. Specialized equipment hardware solutions such as products from Cisco, Checkpoint, Jupiter Network, Fortinet ..., this solution often has higher performance than software solutions due to built-in cryptographic co-processors. (crypto co-proc ssor) design on FPGA / A IC. A series of measures, solutions, technologies and products have been launched based on the above security standards to secure and secure information, of which the most common products are the information flow encryption system (voice , IP flow ...), digital signature authentication system, virtual private network (VPN) system, firewall system (Fir wall), monitoring system, IDP anti-unauthorized access system. In most of the aforementioned product forms the bile systems play a particularly important role. Cryptosystems not only help encrypting data, but also serve as a tool for authenticating the identity, authenticating its origin, and its integrity.

3. Discuss and propose future research directions

The key to security devices deployed at the access layer nodes is securing the bandwidth and speed to secure multiple concurrent connections. IP c has two stages that affect the execution speed, the computation time of the protocol, and from there affect the bandwidth, reduce the performance as well as the time to execute the procedure when there are many secure connections. Move out simultaneously:

- Initialization phase: Setting of safety parameters and key exchange.

- Encryption / decoding of the packet: Use block ciphers to protect data.

When the number of secure connections corresponds to a large number of cryptographic tunnels, IP c integrated devices will not operate effectively, which can affect bandwidth, speed, and stability. operation of the entire network due to some of the following problems:

- The Diffie-Hellman key exchange protocol uses parameter 2048 bit RSA [17] to ensure safety, thus affecting processing and computation speed. This restriction may be proposed to replace the parameters of A with an elliptic curve cipher (ECC).

- The encoding and decoding time are slow due to the complexity of cryptographic algorithms (AE data encoding standard) [9], or the installation method even on hardware or software is not yet optimal. This limitation can be proposed by the research to improve the encryption algorithm and optimize the implementation on hardware.

On the basis of researching and surveying domestic and international studies mentioned in the above section, the study proposes a number of solutions to improve performance, compute speed and improve network security efficiency. Multi-service data transmission is as follows:

Proposing to combine the Diffi-Hellman key exchange protocol in IKEv2 with the use of elliptic curve ciphers (instead of RSA) to reduce the key size while ensuring security while researching, analyzing, and selecting ECC's multiplication algorithm, installs hardware to increase processing efficiency, and reduce key exchange time between links in the system.

- Research and improve the block cipher algorithm and optimize the setting according to criteria to ensure security, safety, and increase performance in data encryption speed.

Select hardware tools, install cryptography (key exchange and encryption / decryption algorithm) on hardware to increase processing efficiency, speed encode / decode computation and improve safety about design.

With the above contents to be addressed, the research will contribute to solving some security limitations for multi-service data transmission networks in the future and towards security for specialized data transmission networks.

References

i. *Government Cipher Committee (20 11), ‘‘ Building up authentication and security system for government information systems ’, Hanoi - 2011.*

ii. *BTL Communication (20 1 0), ‘‘ Building multi-service military data transmission network ’, Hanoi - 2010.*

iii. *Dang Minh Tuan (20 1 3), " Research, design, and manufacture high-performance cryptographic equipment that can be integrated into products used in communication and data transmission ", State level science and technology topic, Institute of Electronics - Institute of Military Science and Technology - 2013.*

iv. *Nguyen Tien Ban (20 11), ‘‘ IP / MPLS technology and virtual private networks ’, Information and Communication Publishing House - Hanoi 2011.*

v. *Nguyen Thuy Van, ‘Digital’, Science & Technology Publishing House - Hanoi 1 999.*

vi. *Tran Tuan Diep, Ly Hoang Tu (1 999), ‘‘ The theory of probability and mathematic statistics ’- Education Publishing House - Hanoi 1 999.*

vii. *Alshamsi, T.s aito (2004), ‘ A Technical Comparison of IPSec and SSL’’*

viii. *A. Salman, M. Rogawski and J. Kaps, “Efficient Hardware Accelerator for IPSec based on partial reconfiguration on xilinx FPGAs, ’’ in Reconfigurable Computing and FPGAs, 2011 International Conférence on, 2011, pp. 242-248.*

ix. *Anirban Chakrabarti, Manimaran Govindarasu, ‘ ‘IP Security-IPSec ’ ’*

x. *Ashwini R. Tonde and Akshay P. Dhande, ‘‘Implémentation of AES Algorithm Based on FPGA ’’ International Journal of Current Engineering and Technology , 2014*

xi. *Menezes, T. Okamoto, and S . Vanstone (1 993), ‘ ‘Re ducing elliptic curve logarithms to logarithms in a finite field’ ’, IEEE Transactions on Information Theory 39, 1993, pp 1639-1646.*

xii. *Bruce S. Davie, Yakov Rekhter (2000). MPLS: Technology and Appl ication. Morgan Kaufmann Press.*

xiii. *B. Kaliski (2003), ‘ ‘Twirl and rsa key size’’, RSASecurity.com, May 2003.*

xiv. *Biryukov, A. Analysis of involutional ciphers: Khazad and Anubis. in Fast Software Encryption. 2003. Springer.*

xv. *Borghoff, J., et al., PRINCE-a low-latency block cipher for pervasive computing applications, in Advances in Cryptology-ASIACRYPT 2012. 2012, Springer; pp 208-225.*

xvi. *Chodowiec, P. and K. Gaj, Very compact FPGA implementation of the AES algorithm, in Cryptographic Hardware and Embedded Systems- CHES 2003. 2003, Springer; pp 319-333*

xvii. *Cre me rs (20 1 1), ‘‘Key Exchange in IPsec revisited: Formal Analysis of IKEv1 and IKEv2 ’ ’.*

xviii. *Chen Lin, Wang Guowei, ‘‘ Security Research of VPN Technology Based on MPLS ’’, August 2010, pp 168-170*

xix. *Darrel Hankerson, Alfred Menezes, Scott Vanstone, ''Guide to Elliptic Curve Cryptography '', Springer - 2004.*

xx. *Daemen, J. and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. 2002: Springer*

xxi. *Daemen, J. and V. Rijmen, The wide trail design strategy, in Cryptography and Coding. 2001, Springer; pp 222-238.*

xxii. *Daemen, J. L. Knudsen and V.Rijmen, The block cipher Square, in Fast Software Encryption, 1997. Springer*

xxiii. *EH3HH, O. and M. HBaHOB, Cмapдapm Kpuпmo^pafu^ecKOü 3a^umu-AES. KomuHbie nom. 2002: Ky^PKU,-OEPA3 M*

xxiv. *Elbirt, A.J., et al., An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, 2001. 9(4): pp 545-557*

xxv. *Elaine Barker, Don Johnson, and Miles Smid, ' 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography '' NIST SP; 800-56A March, 2007*

xxvi. *Guo, J., et al., The LED block cipher, in Cryptographic Hardware and Embedded Systems-CHES 2011. 2011, Springer. pp 326-341.*

xxvii. *Guo, J., T. Peyrin, and A. Poschmann, The PHOTON family of lightweight hash functions, in Advances in Cryptology-CRYPTO 2011. 2011, Springer. pp 222-239.*

xxviii. *H.S oussi, M.Hussain, H.Afifi, D.S eret (20 1 1), ' cIKEv1 and IKEv2: A Quantitative Analyses .International Organization for Standardization (1989), ISO 7498: Information processing systems, Open Systems Interconnection, Basic Reference Model.*

xxix. *International Organization for Standardization (1989), ISO 7498-2: Information processing systems, Open Systems Interconnection, Basic Reference Model, Part 2: Security Architecture IPSec, VPN, and Firewall Concepts. Cisco Press, 2004*

xxx. *Oscar Fajardo, Jon Ander Picó, Alejandro Muñoz (2011)fNew tunnelling capabilities for BGP/MPLS IP VPN in GNU/Linux ' '.*

xxxi. *Jean-Pierre Deschamps, Gustavo D. Sutter Enrique Cantó (2012), ' 'Guide to FPGA Implementation of A rithmetic Functions ' ' Springer - 2012.*

xxxii. *Jean-Pierre Deschamps José Luis Imana Gustavo D. Sutter (2009), ' 'Hardware Implementation of Finite-Field A rithmetic ' '. Electronic Engineering.*

xxxiii. *Jerome A. Solinas (2000), ' 'Efficient A rithmetic on Koblitz Curves ' ', Designs, Codes and Cryptography, 2000; (pp 195-249)*

xxxiv. *Jifi Likes, Josef Laga, "Zâkladni Statiscke Tabulky", SNTL- Nakladatelstvi technicke literatury, Praha 1978.*

xxxv. *Kaur A, Bhardwaj P and Naveen Kumar, ''FPGA Implementation of Efficient Hardware for the Advanced Encryption Standard '', (IJITEE) ISSN: 2278-3075, Volume-2, Issue-3, February 2013.*

xxxvi. *Kapil A. Gwalani, Omar Elkeelany, ' 'Design and Evaluation of FPGA Based Hardware Accelerator for Elliptic Curve Cryptography Scalar Multiplication '', Issue 5, Volume 8, May 2009; pp (884-893)*

xxxvii. *Leon Adams (2002), ' Choosing the Right Architecture for Real-Time Signal Processing Designs'', SPRA879 Texas Instruments - 2002.*

xxxviii. *L.Wu, Yun Niu and X. Zhang, ''An IPSec Accelerator Design for a 10Gbps InLine Security Network Processor '' , Journal Of Computers, Vol. 8, No. 2, February 2013; pp 319-325.*

xxxix. *Langford, S.K. and M.E. Hellman. Differential-linear cryptanalysis. in Advances in Cryptology— CRYPTO'94. 1994. Springer.*

xl. *Liu Bozhong, et al., On the security of 4-bit involutive S-boxes for lightweight designs, in Information Security Practice and Experience. 2011, Springer. pp. 247-256.*

xli. *Mohd Nazri Ismail: European Journal of Scientific Research ISSN 1450-216X Vol.28 No.2 (2009), pp.215-226)* xlii. *Monc e f Amara, Amar S iad (20 1 1), ' Hardware Implementation of Elliptic Curve Point Multiplication over GF(2m) for ECC protocols '' .*

xliii. *Michael H. Behringer, Monique J.Morrow (2005). MPLS VPN Security. Cisco Press.*

xliv. *Mac Williams Florence Jessie and Neil James Alexander Sloane, The theory of error-correcting codes. Vol. 16. 1977: Elsevier.*

xlv. *Masoumi & Mahdizadeh, ' A Novel and Efficient Hardware Implementation of Scalar Point Multiplier '' . Iranian Journal of Electrical & Electronic Engineering, Vol. 8, No. 4, Dec. 2012*

xlvi. *National Institute for Standards and Technology (NIST). ''Recommended Elliptic Curve for Federal Government Use '', July 1999*

xlvii. *P. Barreto and V. Rijmen. The Anubis block cipher. First Open NESSIE Workshop, Leuven, Belgium, November 13-14, 2000.*

xlviii. *Praful Kumar Singh, Mrityunjay Kumar Choudhary (2013), "Scalar Multiplication Algorithms of Elliptic Curve Cryptography over GF (2m) '', (IJITEE) ISSN: 2278-3075, Volume-3, Issue-1, June 2013*

xlix. *RFC 4868, 'HMAC-SHA256, SHA384, and SHA512 in IPsec1 *

l. *RFC 4945, 'The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX '*

li. *Sim S.M, K. Khoo, Thomas Peyrin, ' Lightweight MDS Involution Matrices ''. in Fast Software Encryption. 2015*

lii. *Shannon, C.E., Communication theory of secrecy systems. Bell system technical journal, 1949. 28(4): pp 656-715*

liii. *Susan Strom, Oskar Wiksten (2003), ' 'Important of cryptography in network security ''.*

liv. *Sandeeps, Hameen Shanavas I (2012), ' Design of Hardware Implementation of Elliptic Curve Cryptography over Binary Field'' , International Journal of Electronic and Communication Engineering, Vol 2, No 2 - 2012; pp 78-82.*

lv. *Shylashree N, Nagarjun Bhat, V Shridhar (2012), "FPGA Implementations of high speed elliptic curve cryptography: A survey' '*

lvi. *Shylashree.N, Nagarjun Bhat and V. Shridhar, "FPGA Implementations of Advanced Encrytion Standard: A SURVEY ", International Journal of Advances in Engineering & Technology, May 2012.*

lvii. *Sajadieh, M., Dakhilalian, M., Mala, H., Sepehrdad, P. "Recursive Diffusion Layers for Block Ciphers and Hash Functions". In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 385-401. Springer, Heidelberg (2012).*

lviii. *Xilinx (2015), ' ' ZC706 Evaluation Board for the Zynq-7000 XC7Z045 All Programmable SoC User Guide '' , April 28, 2015.*

lix. *Xilinx (2015), ''Zynq-7000 All Programmable SoC ZC706 Evaluation Kit Getting Started Guide '', January 28, 2015.*

lx. *William Stallings (2011), ' Cryptography and network security - fifth edition '' , 2011.*

lxi. *William Stalling Ph.D (1999), ' 'Cryptography and Network security : Principles and Practice -Second edition ' ', Prentice - Hall, Inc., USA.*

lxii. *Z'aba, M.R. Ph.D, ' Analysis of linear relationships in block ciphers '', Queensland University of Technology, 2010*