Research Intuitions of Asymmetric Crypto System

Rojasree, V.[a], Gnana Jayanthi, J.[b]

[a,B]PG & Research Department of Computer Science,
Rajah Serfoji Govt. College(A), (Affiliated to Bharathidasan University), Thanjavur-613005, Tamilnadu, India
Email:[a]rojasree.v@gmail.com,[b]jgnanamtcy@rsgc.ac.in

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: The fast moving world full of data exchange and communication technology, with all sensitive information of an individual virtually available anywhere and anytime, make the Internet world more critical in security aspects. The areas of risks are attended and assured to be safe by means of some sought of crypto mechanisms. The strength and vulnerability of the crypto mechanism defines the durability of the system. The encryption on the communication channel can implement either public or private key algorithms based on the area of applications. The public key cryptography is specifically designed to keep the key itself safe between the sender and receiver themselves. There are plenty of public key cryptographic algorithms but only a few are renowned. This paper is aimed to collect all possible public key cryptographic methods and analyze its pros and cons so as to find a better algorithm to suite almost all conditions in Internet communication world and e-commerce. Research in quantum computers is booming now and it is anticipated that the supremacy of quantum computers will crack the present public key crypto algorithms. This paper highlights issues and challenges to be faced from quantum computing and draws the attention of network researchers to march towards researching on quantum-safe algorithms.

Keywords: Asymmetric Cryptography, RSA, DHA, Elliptic Curve, Public Key Cryptography, Post Quantum Crypto System, Issues and Challenges in Crypto World.

1. Introduction

This era of information technology creates a majorconcern on thesecurity of the information and themethods of addressing the challenges of data security.Cryptographyisusedinplacesofdatastorageandalso incommunicationofdata.

Moderncryptographyisclassifiedintothree,

(i) SymmetricKeyCryptography(withasinglekey),

(ii) AsymmetricKeyCryptography(withtwodifferent keys), and (iii) Hashing (without any key)whichareshownin figure,Figure-1 below[1,2].

SymmetricKeyCryptographydealswithasinglesecret key shared by both users namely Sender andreceiverwhereasAsymmetricKeyCryptographydeals with pair of relatedkeys called privatekey (tobe maintained secretly by the owner) and public key(shared by both users namely Sender and receiver).Hashingisaone-waycryptographictransformationusinganalgorithm(andnokey).

Acryptographicalgorithmmustbesecureagainstdifferentattacksandmusthaveahighprocessingspeed. The efficiency of a security algorithm is basedonthedifficultyinobtainingtheencryptionkeythroughthecyber-attacks.Itispresumedthatthelarger the key size, the safer the system is.At thesame time the increase in the key size simultaneouslyincreasesthecomputationalcomplexityandtheprocessingtimeofthealgorithm.

Figure-1(a): Symmetric Key CryptographyPrimitives

Figure-1(b): Asymmetric Key CryptographyPrimitives

Figure-1(c): Hashing Cryptography Primitives

The field of quantum computing with its very largescale computing powerwhich has been proposed inthe 1980s, has recently garnered significant attentionduetoprogressinbuildingsmall-scaledevices.However,significanttechnicaladvanceswillberequiredbeforealarge-scale,practicalquantumcomputercanbeachieved.Quantumcomputers,quantumencryption,post-quantumcryptography,quantum security, quantum proof, quantum resistantcryptography,quantumkeyspace,quantumcryptographicinfrastructureetc.allaresimilarsounding yet different. The swift changing era leads toswift changes in theworld of security. The changesare taking so fast that it is difficult to understand thedrift without ambiguity. Quantum security, quantumencryption and quantum cryptography all means thesamewhereinthecryptographyisachievedbyexecuting complex mathematical algorithms to hidethe dataandinformationfromtheeavesdropper.

ManyresearchersfromacademiaandIndustriesforeseethataquantumcomputerwillbeableto

implement Shor's Algorithm at a relevant scale in thenext 10 to 15 years. Most recently, researchers haveshown that quantum computing is capable of breakingthe strong cryptographicprimitives,such as Diffie-Hellmankeyexchange.

This paper is aimed to present a literature review ontheresearchaspectsofasymmetriccryptography.Sincethedesignanddevelopmentofasymmetriccryptography date back from the middle of 1970s, theresearch papers fortheliterature study are coveredfromthemidof1970'sto2020.Itisobservedfromtheliteraturestudythattherearesevéralongoingresearch works on new methods for encryption anddecryption which will be more challenging to attacksby booming of large scale Quantum computers in thedigitalera.

All the research works in the literature papers havebeenthoroughlystudied,analysedanda*ConciseReportoftheLiteratureStudy*ontheasymmetricalgorithmsispresent edinsection-II.SectionIIIoutlines the *Current Scenarioof theCryptoSystem*and summarizes a few of the literature study carriedout for the same. Section IV sketches out the *Post-Quantum Crypto System* and summarizes some of themajor*IssuesandChallengesfacedindevelopingPost-Quantum Crypto System*. Section V summarizesthe*Inferences Observedfrom theLiteratureStudy*.Section VI concludes the paper with a further researchfocus.

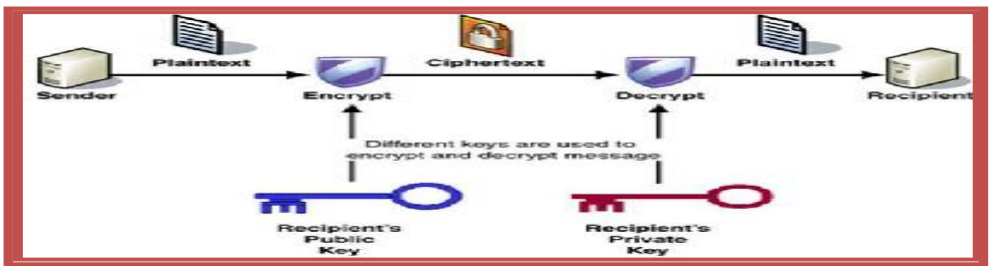

Figure-2: Asymmetric Cryptography Diagram

Diffie-Hellmandesignedtheideaofpublickeycryptographyinwhichthekeysforencryptionareshared between the sender and the receiver publiclybut still the intruder could not get the actual secret key[Diffie *et al.*,1976].Later their algorithm is referredto as '*Diffie Hellman Algorithm' (DHA)* and till date,isconsideredastrongestmethodinpublickeycryptography. The well known RSA, Elliptic CurveCryptography(ECC)allusethisconceptofDiffieHellmanbyjust generatingthesecretand public keys.

Rivest *et al.* presented a method for *Obtaining DigitalSignaturesandPublic-KeyCryptosystems*whichisthe first secure Asymmetric cryptographic algorithm.Later, it is referred to as *RSA Algorithm* and then,followedtheDiffie-Hellmanlogicofpublickeysystem. *This concept gives an idea to a researcher inthefieldofcryptographyofhowtoproceedwhendesigning a new algorithm so that whoever reads thearticlecaneasilyunderstandthevalueofthepieceof*

2.Literature Survey Of Asymmetric Cryptosystem

AsymmetricCryptographyotherwisecalledasaPublic Key Cryptography provides two keys. Thesetwo different keys are private key and public key. Apublic key can be given to anyone and a private keymustbekeptsecretasthekeyinsymmetriccryptography. This asymmetric cryptography has twoprimary use cases:

authentication and confidentiality.Usingasymmetriccryptography,messagescanbesigned with a private key, and then anyone with thepublickeyisabletoverifythatthemessagewascreatedbysomeonepossessingthecorrespondingprivate key. This can be combined with a proof ofidentity system to know the user, actually owns thatprivatekey,providingauthentication.

Encryption with asymmetric cryptography works in aslightlydifferentwayfromsymmetricencryption.Someonewiththepublickeyisabletoencryptamessage, providing confidentiality, and then only thepersoninpossessionoftheprivatekeyisabletodecrypt it and these processes are depicted in figure,Figure-2.

Basedontheseasymmetricconcepts,variousalgorithmsareintroducedbyseveralresearchers.Someoftheremarkablea ndnoteworthyresearchworksbasedtheasymmetriccryptosystemarereviewed, analysed and summarized in this section asfollows.

*research.*Theauthorshaveconcentratedontheprivacy and security issues [Rivest *et al.,* 1978] anddeveloped encryption and decryption algorithms withmathematical prime values. *However, the weakness ofthis algorithm is also discussed in the cryptanalyticapproaches and proves how difficult it is to break theproposedRSAalgorithm*.

TatherElGamalsketchedoutDiffie-Hellmankeyexchange and designed an '*asymmetric key encryptionalgorithmusingalgebraicpropertiesofmodularexponentiation along with discrete logarithm'*. In thisalgorithm, a private key is used to produce the digitalsignature for a message and a public key is used toverify the signer's digital signature [Elgamal, 1985].This algorithm is referred to as ElGamal algorithm,whichisthenpublishedinGNUPrivacyguard.*ElGamalcryptosystemisusuallyusedinhybridcryptosystemsbe causeitislittleslowerthanthesymmetric cryptosystemsandhencenotwidelyused.*

VictorMillerfromIBMandNeilKoblitzfromUniversityofWashingtondesignedanddeveloped'*EllipticCurveCrypto graphy'*independentlyfromtwo different places [Victor, 1986], [Koblitz, 1987].The elliptic curve cryptography methods use the cubiccurves that represent elliptic curves graphically. Theequationofanellipticcurveisusedtocreatethepublickeyandtheprivatekeyinapublickeycryptographic system. A simple affine equation of anelliptic curve is (y2=x3 +ax +b). As the values of andvaries,differentcurvesareobtained.Therearesome

curves on which successful attack can take place insub-exponential time. If identified these curves can betestedandavoided.Thesecurvesarecalledsupersingularcurvesandanomalouscurvesandaredeclaredby NationalInstit uteofStandardsandTechnology (NIST) of United States as not good forusage incryptography.

Zheng *etal.*presentedadistribution based*EllipticCurve Public KeyCryptosystem* (ECPKC)by usingthe chord tangent group laws of Elliptic curve whereinthe private keys are normal integers and the publickeys are points on elliptic curve [Zheng *et al.,* 1993].This is a small variation inserted and implemented bythe authorsinalgorithm.

Bone*hetal.*introduced'*BlackBoxFields'*(BBF)whereintheseBBFcontainsthesecrecyofanalgorithm that makes it strong. It was believed by theauthor that any cryptographic algorithm can be brokenin sub-exponential time. The authors also insist thatthe hardness of solving the elliptic curve or the hyperellipticcurveisthesecurityoftheDiffie-Hellmanprotocol beneath it. Thus the authors generalized thisscenario of manipulating the BBF on the rationales isashardasfactoringofintegers[Bone*het al.*,1996].

Dawn *et al.* designed an algorithm to search and storeencryptedfilesanddocumentsbyqueryingthedatabase where the encrypted information is stored.The authors have classified the queries as (i) queriesfrom authorizedand(ii)queriesfromunauthorizedusers[Dawn*etal.,*2000].Theiralgorithmalsosupportshidden queries whereinthequery isitselfencrypted and then sends to the database server. Thepurpose of encrypting and storing the sensitive data isitself cracked with the notion of the authors; this paperisitselfacryptanalyticapproachoftheencryptiondoneonthedatabase.*Itshouldbekeptinmindthatthesearchengined esignedmaybreaktheentirecryptosystemdondayorother.*

Wander*etal.*presentedaproposalof'*EnergyAnalysisofPublic-KeyCryptographyforWirelessSensor Networks'* wherein the authors quantified theenergycostofkeyexchangeandauthenticationofpublickeycryptographicsystemsusing8-bitmicrocontroller[Wander*etal.,*2005].TheyconcludedthatECCisadvantageousthanRSAasECC takes lesser computational time, amount of datatransmittedislesserandstoreddataisalsosmall.*However, it is now a known fact that the public keysystemshaveoverheadsbasedonthekeysizeused.*

Liu *etal.*delivereda differentapproach of Diffie-HellmanPublickeycryptosystem(DHA)byimplementingtheneuralsynapticmatrixafterpermutation as a public key and a random permutationoperation on the neural synaptic matrix as secret

keyusingJavaProgram.Theauthorstestedforthefeasibility and inferred that their algorithm is feasiblewithbetterperformanceforsecurecommunication.Thisisbasedontheone-wayfunctionbetweenthe

chaotic attractors and the initial states of OverstorageHopfield Neural Networks (OHNN) [Liu *et al.,* 2006].The real time IPng secure communications could bedone by using DHA. *However, the authors themselvesare not sure if this could be implemented in situationsof other new type of attacks and so left it for futureenhancement.*

Silva *et al.* introduced a proposal of direct algorithmthat was very simple and applied to the product of twodifferentbutequalizedprimesandwasbasedonreversing the decimal digits of the modulus [Silva *etal.,* 2010]. *This algorithm required very less memoryand waseasilyparallelized.*

Wu *et al.* with a goal of studying time-efficient andspace-efficient algorithms like RSA cryptography andEl-Gamal Cryptography have mused on the modularexponentiationsalgorithmsthatareofpracticalsignificance in folded substrings which then improvesthe efficiency of the binary algorithm, and reduces thecomputational complexity of modular exponentiation.*Theauthorshavemadeadetailedstudyonthemathematicalconceptsofmodulararithmetic,Square-and-multiplybinarymethod,signed-digitrecoding method and Montgomery's reduction methodandasitistimeconsumingbecausetheyinvolverepeated multiplications and scanning of bits in theplaintext*[Wu*et al.*,2012].

Alese *et al.* performed a comparative study using timelapse for encryption, decryption, key generation andthe encrypted data size of different public key cryptosystemslikeRSA,ElGamalEllipticalCurveEncryptionandMenezes-VanstoneEllipticcurvealgorithm [Alese *et al.,* 2012]. The implementation ofall these three algorithms are discussed in detail andthe authors themselves say that *these algorithms areusedtoeliminatetheproblemsofprimitiveconventionalmethodsbutstilltheyarenotwidelyused as these algorithms are implemented with lots ofoverheads. ECC iswidely usedbecause it involvesfewer overheads. So with no other go we are forced toacceptECCasthereisnobetteralgorithmtoovercometheseoverheadswiththesameefficiency.*

Mandal *et al.* designed an algorithm by combining theDiffie-Hellman algorithm and the RSA algorithm toprovideahigherlevelofsecurityfordata.Theydesigned the algorithms for both small as well as largesized data by choosing a random key pair from the setofRSAkeysandonerandomly chosensecretkeyfrom Diffie-Hellman algorithm and then applied theRSA algorithm to the public components of Diffie-Hellman algorithm to make it more difficult for theeavesdropper to access. Again the authors have usedonly the key generation methods of RSA and DHA;and used these keys in the Symmetric algorithms andevaluated [Mandal *et al.,* 2013]. *All the under benchflaws of these algorithms still persists and is just aneyewashastheattacksonsymmetricencryptionalgorithmsstillexists.*

Mohammed*etal.*haveproposed*AdvancedEncryptionandDecryptionStandard*(AEDS)bycombiningthepropertiesofbothAESandDES[Mohammed*etal.*,2019]. Theauthorsstudiedtheencryption and decryption time of AES and DES andfound that the for a good cryptographicalgorithm theencryption algorithm should take lesser time so thatthehackerscouldn'ttracktheprocessingandthedecryptionalgorithmshouldtakelongertimeasitshouldbedifficulttobreaktheciphertext.Theseauthorshavemadeacomparativeanalysisoftheirproposedwork,AEDSwithAESandDES,onWindows,Linux-OSandMacOSmachinesforencryption,decryption.Theyconsidereddifferentstringsanddifferentfilesizes.Theycalculatedaverage encryption time, and average decryption time,as the parameters for their comparison and prepared acomparison chart for each and every result obtained.Theircomparativestudy concludes thatbruteforceattack isnearly reducedthan inAES andin DES.*However, Encryption and Decryption time for AEDSmore robustandsecure thanin AESandin DES.*

Pradeep*etal.*haveintroducedan*EfficientFramework for Sharing a File in a Secure MannerusingAsymmetricKey DistributionManagementinCloud Environment* [Pradeep *et al.,* 2019]. The dataaccessedor sharedbetweenvarious devices on thecloudenvironmentwhichislikelytofacemanyattackslikeIdentityAccessManagement(IAM),intrudershijackingaserviceoranaccounteitherinternally or externally. Security is mainly resting onthe key and every cloud provider takes more effort toprotect the key. The authors proposed a new systemwherein the exposure of keys and the framework issecured using a third party. The authors compared thenew system using RSA, ELGamal and Paillier andsuggested RSA as a better result. *The authors haveused a third party code for providing security whichcan alsobeathreat totheentire cloudsystem.*

Khider *et al.* have introduced *Hybrid Cryptographyand Steganography Method* to embed encrypted thatmessagewithin image, as ahybridsecurity

systemwhereinthemessagetobetransmittedisfirstencryptedtociphertextbyusingRSAalgorithm[Khider *et al.,* 2019]. Then the produced cipher text isembedded into an 800x600 pixel image using the leastsignificant bit insertion method. The authors took thisinventionastogiveanewmethodofmessagehidinga small application where the security is increased bycombining two different message hiding techniques.The accuracy of the final embedded image is analyzedfor accuracy using Mean Square Error (MSE) metricand Peak Signal to Noise Ratio (PSNR) metrics. AhighPSNRvalueandalowMSEvalueprovesthatthe message hiding is good and had not caused toomuch of drifts in the image. *The Key of RSA is itselfhuge in some situation wherein a smaller system isrequired; here in this system, the key of RSA is hiddenin the image at the cost of more storage space, this isitselfadrawbacktoimplementtheirwork.*

3.Hot Scenario Of Crypto System

In1994PeterShoranAmericanMathematicianinvented an algorithm for integer factorization to findthefactorsofagivenintegernumberN.Thishasbecomeathreattothefieldofcryptographyasquantumcomputersthatcouldworkwithsub-exponentialtimecan function fasterthan expected.The Shor's algorithm is efficient in quantum FouriertransformandmodularexponentiationbyrepeatedsquaringthusitisfeasibletodefeatRSAbyconstructing a large quantum computer. This has leadtoresearchinnewcryptosystemssuchthatitissecure fromquantumcomputers.

Due the high speed in the processing of the quantum-computers the asymmetric-cryptography methods willbecrackedandatthesametimesymmetriccryptographic methods will be able to withstand thequantumattack.Thischangeinthescenariohasdivided the entire cryptography world intotwo partsas post-quantum cryptographic era and pre-quantumcryptographicera.Someofthepost-quantumcryptographicsupportingpapersareasfollows.

Bernstein *et al.* published a paper to ponder into themanycommonlyusedcryptosystemsthatbreaksbytheexistenceoflargequantumcomputers.Post-quantum cryptography is cryptography world where itisassumedthattheattackerhasalargequantumcomputer and the post-quantum cryptosystems fightshard to remain secure even in this situation [Bernstein,2009].Thechallengefortheyoungcryptographicresearchersisthatidentifyingamathematicaloperationthatcouldwithstandthequantumalgorithms.Themajorchallengeistomeettherequirementsforcryptographicusabilityandflexibility without compensatingonconfidence.

Jasmin *et al.* presented another approach of public keyencryption algorithm which was meant to avoid longandcomplexcomputationofconventionalpopularalgorithms. The authors made a detailed survey in thekey generation mathematical foundation of each andeverypopularalgorithmsbothsymmetricandasymmetricalgorithms,foundthatthepublickeycryptographyschemesareallpassiveforthreedecades andfinally concluded to leavethe inventionof a new algorithm to the hands of future researcherstogenerateanewalgorithmthatcouldsolvetheproblemsofalltheavailablealgorithmsofcryptography[Jasmin *et al.*,2018].

William *et al*. is a NIST authorised draft published toinformthepublicaboutthemigrationofcryptographictechnologiestopost-quantumcryptographyafterthestandardizationprocessiscompleted[William*etal.*,2020].Cryptographictechnologies are used almost everywhere in industryandingovernmenttoprotectheconfidentiality,authenticate the source and integrity of informationthatarestoredandcommunicated. Thispaperalsointroduces adoption challenges associated with post-quantumcryptographyafterthestandardization

process is completed. The authors explained how thecryptographictechnologiesgetaffectedbytheintroductionofquantumcomputingincludingthepopular and secure RSA public key cryptography. Theauthors also discussed the planning requirements formigrationtopost-quantumcryptography.Intheconclusionthestepstohelptomigratetopost-quantumcryptographyaregiven.

Fernández *et al.* concentrated on the current situationof post-quantum cryptosystems and their applicationsto block chains and Distributed Ledger Technologies(DLT) [Fernández *et al.,* 2020]. The most apt post-quantum block chain systems and their challenges arestudied.Acomparativeanalysisisdoneonthecharacteristics and performance of the most promisingpost-quantumpublic-keyencryptionanddigitalsignaturesforblockchains.Thearticleprovidesabroadviewandgoodguidelinesforpost-quantumblock chain security as an eye-opener for the futureblockchaindevelopersandresearchers.

Borges *et al.* the two major mathematical primitivesthat assure the security of cryptographic algorithm areFactorization problem and discrete logarithm problem[Borges *et al.,* 2020]. Shor's quantum algorithm easilybreaks these problems and hence a necessity for a newcryptographic algorithmthatcouldrun on classicalcomputersandareresistanttoquantumcomputingarises. This area of research is called post-quantumcryptographyandisusuallydealtwithasymmetriccryptography.

4.Issues And Challenges In Developing Post-

4.1.Quantum Cryptography

Post-quantumcryptographyistheerawhereinthealgorithms like Shor's algorithm came into the sceneand made the attacking process also in the same wayasthecryptographyalgorithmwasused.Nowforevery Quantum-cryptography there can be a Quantumcomputer to break this algorithm. This lead to a threatto the entire cryptographic world, which involves usescomplexmathematicalcalculations,mostlyAsymmetricPublicKeyencryption.Thisissueistemporarilysolvedbyusi ngQuantum-keyspacewhereinthekeysoftheasymmetricpublickeycryptography are transmitted in the form of photonsratherthanbinarydigits.Inthiscaseifaneavesdropper tries to trap the photons it changes stateand key will fail resulting in the loss of information toboth the sender and the receiver too. This is leadingcryptographic science to a new era of post-quantumcryptography. Post-Quantum cryptography (PQC) isalgorithms that could resist the attacks from quantumcomputers.

WithanticipatedQuantumComputing,therearеseveral issues and challenges to be addressed [Helena,2020],[QT_Timeline_Report,2019],[Naoyuki,

2019], [Dinget al., 2017].

Some of the major challenges are the (i) Key Size, (ii)PublicKeyInfrastructure,(iii)DevicesinIoTs,(iv)

Security Services, (v) Composite Keys and SignaturesforUseinInternetPKI,(vi)MultiplePublic-KeyAlgorithmX.509Certificates,and(vii)Multi-AlgorithmPKIand thesearebriefedbelow.

4.1.1Key Size:

The key size is one of the major problems in post-quantumasymmetriccryptographywhereinafewthousands of bits long key is required to be used thuscausingstorageoverhead.

4.1.2.Public Key Infrastructure:

Public key infrastructure (PKI) when used in publickeycryptographyitrequiresmorebandwidthtocommunicate betweenthedevicesontheInternet.

4.1.3.Devices in IoTs

NowadaysedgecomputingandIoTshavebecomemore ubiquitous, and creates a major challenge wherethe edge devices with limited computing and powerprocessingfacilitiesarepronetoquantumattacks.Rambus a standardising organization for electrical andelectronicdevicesbelievethatsecuritybecomeshardwaredependent rather thansoftwaredriven.

4.1.4.Security Services

Themathematicalalgorithmsintheclassicalandquantum cryptosystems are not well studied yet so thepossibilitiestoattacksontheunreadmethodsareeasilypossible.

4.1.5.Composite Keys and Signatures for Use in Internet PKI

The entry of post-quantum cryptography has lead tothe necessity to assign different structures for holdingcomposite public keys in different algorithms. This isbecausethetrustworthinessoftheindividualpost-quantumalgorithmisnot assured.

4.1.6.Multiple Public-Key Algorithm X.509 Certificates:

Thisdocumentdescribesamethodofembeddingalternativesetsofcryptographicmaterialsintо X.509v3digitalcertific ates,X.509v2CertificateRevocation Lists (CRLs), and PKCS #10 CertificateSigning Requests (CSRs). The embedded alternativecryptographicmaterialsallowaPublicKeyInfrastructure(PKI)tousemultiplecryptographicalgorithms in a single object and allow it to transitiontothenewcryptographicalgorithmswhilemaintainingbackwardscompatibilitywithsystemsusing the existing algorithms. Three X.509 extensionsand three PKCS #10 attributes are defined, and thesigning and verification procedures for the alternativecryptographicmaterialcontainedintheextensionsand attributesaredetailed.

4.1.7.Multi-Algorithm PKI:

HybridizedcryptographyiscompelledbyPost-quantumcommunity(forexample,surroundingtheNISTPQCcompetition)thatcombinesRSA/ECCwith new

primitives in order to hedge the challengeagainstbothquantumadversaries.

5.Observations And Inferences

EventhoughmessagehidingexistsfromthePalaeolithicageasEgyptianhieroglyphs,Mesopotamia's clay tablets,Cryptography a scienceofsecretmessagingcameintoexistencewhensubstitutionandtranspositionoflettersofmessagecame intoexistence.

The Ceasar Cipher, Vigenere algorithm, lead to secrettransmission of messages during the World War II asGermany's Enigma machine Japanese's M-1 machine,wheremachineswereusedtosubstituteandtranspositionthelettersofthemessage.

Laterthemoderncryptographywhereinthekeyswere used to digitally gibberish the readable plain textthereweplentyofsymmetriccryptographicmethodswhere same keywas usedtoencryptanddecryptamessage.

Laterarevolutioninthefieldofcryptoscienceevolved from Diffie-Hellman Algorithm (DHA), RSAandECC.TheDHAalgorithmisakeyexchangealgorithm that worked in a public network. Using theconcepts of DHA, RSA was invented as a new era ofpublic key cryptography systems such as Pretty GoodPrivacy (PGP). ECC is also a predecessor of DHAwhere the keys are generated by affine elliptic curves.These algorithms worked with strength of difficulty inFactorization,discretelogarithmicproblemandelliptic-curve discretelogarithmproblem.

Bruteforceisaneffectiveattackingmethodofcollapsingmostformsofcryptographymethodswitha patienceof waitingtillthe keyspaceisexhausted.

Man-in-the-middleattackscouldbreakthecryptographicalgorithm.Usingsimplepassphrasesandpasswordsassecretkeysincryptographicalgorithmscanresultinadverseeffects,andimproperly stored private and public key can cripplethe entirecryptosystem.

Conceptual computer that could work on algorithmsusedinquantummechanicsarecalledquantumcomputers. By the invention of Shor's algorithm thequantum computers were able to break the toughnessoftheasymmetricalgorithms.Thishasbecomeathreattotheworld ofcryptography.

NISTstarted the Open Quantum Safe (OQS) Projectin the late 2016 to fight against attacks called post-quantum cryptography with potentially quantum safecryptographicalgorithms.

Hence, there is a potential need to face post-quantumattacksandrethinkofanewkindofsecuredcrypto

system other than Symmetric / Asymmetric / HashingCryptoSystemsthatwillworkwithquantumcomputing and classical computing as well. Designinganewsetofencryptiondecryptionalgorithms,thefollowingparametersareto beconsidered;

- *Current key sizes and hardware/software limitson futurekeysizesandsignaturesizes*
- *Thekeysizeusedintheexistingsystem,hardwareandsoftwareresourcelimitsandfuture possibilities of the key sizes and signaturesizes*
- *Thresholdofthroughputandlatency*
- *Protocolsandproceduresusedforcryptomechanismsnegotiation*
- *Existing handshake rules and key establishmentprocedures*
- *The place of execution of cryptographic processin thestack*
- *Themethodofcallingandactivatingthecryptographic process (using a function includedintheoperatingsystemorcallinganewapplication, orusingcryptographyasaservice)*
- *Identifytheowner(s),supplier(s)orstandardizer(s)ofthehardwareorsoftwareprocess*
- *Generation Source(s)of keys and itscertificates*
- *Legal conditions and contractual applied on andbythesupplier(s)*
- *Reasonformigrationfromexistingsystemtonewsystem.*

6.Conclusion

The cryptography techniques discussed in this papergivesaclearideathatthecurrentavailablecryptographic methods are becoming bizarre, is like anewwineintheoldwineskin.Henceanewmethodology to meet the current

situation, to survivetheattacksfromaquantumcomputermustbegenerated.

Duringthepostquantumstandardizationanewwineskin is required to hold the new wine. Addingplug-in to the existing crypto algorithms to generatequantum resistant cryptosystem will be an interestingjourneyforbothcryptographersand practitioners.

7.Acknowledgement

The authors sincerely express their special thanks andsinceregratitudetoTamilnaduStateCouncilforHigherEducation(TNSCHE)andDepartmentofScience and Technology (DST), India, for sponsoringthisresearchworks.

We would also like to thank Dr.S.Albert Rabara, Dr.MAni,Mr.ArunGnanaraj,Mrs.ChristySujatha,Mrs.M.Manimozhi as well as other correspondents forproductivediscussionsandimprovementsofearlydraftsofthispaper, and for pointers

References

Evolution of Cryptography. @url: https://sherpasoftware.com/blog/the-evolution-of-cryptography/ Last visited on 21-03-2020.

Mohd Zaid Waqiyuddin Mohd Zulkifli, “Evolution of Cryptography”, 17 January 2007 @url http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.69 8.2641&rank=190, Last Retrieved 20-Mar-2020,

[Diffie et al, 1976], W. Diffie, M. Hellman, "New directions in cryptography," in the publications of IEEE Transactions on Information Theory, ISSN: 0018-9448, Volume: 22, No: 6, PP: 644-654, November 1976, DOI: 10.1109/TIT.1976.1055638.

[Rivest et al., 1978], R. L. Rivest, A. Shamir, L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, In the publications of Communications of ACM, ISSN:000-0782, Vol.21, Issue 2, PP: 120–126, Feb.

1978, DOI: https://doi.org/10.1145/359340.359342.

[Elgamal, 1985], T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in the publications of IEEE Transactions on Information Theory, ISSN: 0018 9448, Volume: 31, No.: 4, PP: 469-472, July

1985, DOI: 10.1109/TIT.1985.1057074.

[Victor, 1986], Victor S. Miller, “Use of Elliptic Curves in Cryptography", In the proceedings of Advances in Cryptology- CRYPTO’85, Springer, PP: 417-426, Berlin Heidelberg, 1986.

[Koblitz, 1987], Niel Koblitz, “Elliptic Curve Cryptosystems”, In the publications of Mathematics of Computation, ISBN: 978-3-642-44649-8, Vol.48. No.177,

PP: 203-209, Springer, Berlin, Heidelberg, January 1987, DOI: https://doi.org/10.1007/978-3-642-04101-3_9.

[Zheng et al., 1993], Y. Zheng, J. Seberry, "Immunizing public key cryptosystems against chosen ciphertext attacks”, In the IEEE Journal on Selected Areas in Communications, ISBN:0-7803-4371-9, Vol.11, No.5, PP: 715-724, Jun. 1993, DOI: 10.1109/49.223871.

[Boneh et al., 1996], Boneh D., Lipton R.J. (1996) Algorithms for Black-Box Fields and their Application to Cryptography. In the proceedings of Advances in Cryptology

— CRYPTO ’96. Lecture Notes in Computer Science, ISBN: 978-3-540-61512-5, Volume: LNCS 1109, PP: 283-

297, Springer, Berlin, Heidelberg DOI: https://doi.org/10.1007/3-540-68697-5_22.

[Dawn et al., 2000], Dawn Xiaoding Song, D. Wagner, A. Perrig, "Practical techniques for searches on encrypted data," In the proceedings of 2000 IEEE Symposium on Security and Privacy S&P 2000, ISSN: 1081-6011, PP: 44-55, Berkeley, CA, USA, 2000, DOI: 10.1109/SECPRI.2000.848445.

[Wander et al., 2005], A. S. Wander, N. Gura, H. Eberle, V. Gupta, S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," In the proceedings of Third IEEE International Conference on Pervasive Computing and Communications, ISBN:0-7695- 2299-8, PP: 324-328, 2005, Kauai Island, DOI: 10.1109/PERCOM.2005.18.

[Liu et al., 2006], Liu N., Guo D., “Security Analysis of Public-Key Encryption Scheme Based on Neural Networks and Its Implementing”, In the Springer Proceedings of International Conference on Computational and Information Science Computational Intelligence and Security (CIS 2006), Lecture Notes in Computer Science, ISBN: 978-3-540- 74377-4, Vol.4456, PP: 443-450, Springer, Berlin, Heidelberg, 2006, DOI: 10.1007/978-3-540-74377-4_47.

[Bernstein, 2009], Bernstein D. J. “Introduction to Post- Quantum Cryptography”, In the publication of Springer, ISBN: 978-3-540-88702-7, Berlin, Heidelberg. 2009,

DOI: https://doi.org/10.1007/978-3-540-88702-7_1

Silva et al., 2010], J. C. L. da Silva, "Factoring semiprimes and possible implications for RSA", In the proceedings of 2010 IEEE 26-th Convention of Electrical and Electronics Engineers, ISBN: 978-1-4244-8682-3, PP: 000182-000183, Israel, 2010, DOI: 10.1109/EEEI.2010.5661953.

[Wu et al., 2012], C. Wu, C. Hu, "Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application," In the proceedings of 2012 Third International Conference on

Innovations in Bio-Inspired Computing and Applications, ISBN:978-1-4673-2838-8, PP: 307-311, 2012, Kaohsiung, DOI: 10.1109/IBICA.2012.9.

[Alese et al., 2012], Alese, B. K., Philemon E. D., Falaki, S. O., "Comparative Analysis of Public-Key Encryption Schemes", In the International Journal of Engineering and Technology (IJET), ISSN: 2049-3444, Vol. 2 No: 9, PP:

1552-1568, Sep. 2012, UK.

Mandal et al., 2013], B. K. Mandal, D. Bhattacharyya, S. K. Bandyopadhyay, "Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm," In the proceedings of 2013 International Conference on Communication Systems and Network Technologies, ISBN:978-1-4673-5603-9, PP: 453-461, 2013, India, DOI: 10.1109/CSNT.2013.101.

[Jasmin et al., 2018], Jasmin Ilyani Ahmad, Roshidi Din, Mazida Ahmad, "Analysis Review on Public Key Cryptography Algorithms", In the Indonesian Journal of Electrical Engineering and Computer Science (IJEECS 2018), ISSN: 2502-4752, Vol.12, No. 2, PP: 447~454, Nov.

2018, DOI: 10.11591/ijeecs.v12.i2.pp447-454

[Mohammed et al., 2019], Mohammed Ali Argabi, I. Alam, "A new Cryptographic Algorithm AEDS (Advanced Encryption and Decryption Standard) for data security", In the International Advanced Research Journal in Science, Engineering and Technology, Corpus ID:214504677, Vol. 6, PP: 1-7, 2019, DOI: 10.17148/iarjset.2019.61001.

[Pradeep et al., 2019], Pradeep, K. V., V. Vijayakumar, V. Subramaniyaswamy. "An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment", In the Journal of Computer Networks and Communications (JCNC), ISSN: 2090-7141, Article ID 9852472, Vol.2019, 8 Pages, 2019,

https://doi.org/10.1155/2019/9852472

[Khider et al., 2019], Khider Nassif Jassim, Ahmed Khudhur Nsaif, Asama Kuder Nseaf, Al Hamidy Hazidar, Bagus Priambodo, Emil Naf'an, Mardhiah Masril, Inge Handriani, Zico Pratama Putra, "Hybrid cryptography and steganography method to embed encrypted text message within image", In the proceedings of International Conference Computer Science and Engineering a Journal of physics: conference series 1339, 012061 (IC2SE), Indonesia, Apr. 2019, DOI: 10.1088/1742-6596/1339/1/012061.

[William et al., 2020], William Barker, William Polk, Murugiah Souppaya, "Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms", In the publications of NIST Cyber Security White Paper (DRAFT), CSRC.NIST.GOV, 26 May 2020,

DOI: https://doi.org/10.6028/NIST.CSWP.05262020-draft. [23]. [Fernández et al., 2020], T. M. Fernández-Caramès, P.

Fraga-Lamas, "Towards Post-Quantum Block Chain: A Review on Block Chain Cryptography Resistant to Quantum Computing Attacks", In the IEEE Special Section on Emerging Approaches to Cyber Security, ISSN: 2169-3536, Vol.8, PP: 21091-21116, 2020, DOI: 10.1109/ACCESS.2020.2968985.

[Borges et al., 2020], F. Borges, P. R. Reis and D. Pereira, "A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography", In IEEE Journal of Special Section on Emerging Approaches to Cyber Security, ISSN: 2169-3536, Vol. 8, PP: 142413-142422,

2020, DOI: 10.1109/ACCESS.2020.3013250.

[Helena, 2020], Helena Handschuh, "What is Post-Quantum Cryptography?", NOV 05, 2020, https://www.electronicdesign.com/technologies/embedded- revolution/article/21146368/rambus-what-is-postquantum- cryptography, Last Retrieved 26-Nov-2020,

[QT_Timeline_Report, 2019], Quantum Threat Timeline Report, Global Risk Institute (2019), https://www.entrust.com/resources/certificate- solutions/learn/post-quantum-cryptography, https://tools.ietf.org/html/draft-ounsworth-pq-composite-

sigs-00, Last Retrieved 23-Mar-2020.

[Naoyuki , 2019], Naoyuki Shinohara, Shiho Moriai, "Trends in Post-Quantum Cryptography: Cryptosystems for the Quantum Computing Era", In the magazine of New Breeze, PP: 9-11, Winter 2019, Last Retrieved 10-May-2020,

https://www.ituaj.jp/wp-content/uploads/2019/01/nb31- 1_web-05-Special-TrendsPostQuantum.pdf

[Ding et al., 2017], Jintai Ding, Daniel Smith-Tone, "Post- Quantum Cryptography—A New Opportunity and Challenge for the Mathematics Community", Notices of the AMS, PP: 709-710, Volume 64, Number 7, August 2017, Last Retrieved 26-May-2020,

https://www.ams.org/publications/journals/notices/201707/rn oti-p709.pdf.

AUTHORS PROFILE

Ms. Rojasree. V, M.C.A., M.Phil., is presently working as a Chief Executive officer of Arangar TV a television channel of Sri Agathiar Sanmaarga Sangam, Ongarakudil. Thuraiyur. Ongarakudil is a Government registered Charitable trust and Arangar TV is their own TV channel. Currently She is persuing he PhD in Computer Science from Bharathidasan University, Tiruchirapalli, India. Rojasree. V has experiences of working as a lecturer in some of the reputed educational institutions namely i. Holy Cross College Trichy, ii, Bharathidasan University Technology Park, Kajahmalai campus Trichy, iii. Nehru Memorial College, Puthanampatti, Trichy. She is a Red Hat Certified Engineer from 2006.

Dr. J. GNANA JAYANTHI, M.C.A., M.Phil., Ph.D., to her capacity, is servicing as an Assistant Professor in the PG and Research Depart. of Comp. Sci., at Rajah Serfoji Government College (A), Thanjavur, affiliated to Bharathidasan University, Tiruchirappalli, India. She received her Ph.D. (2012) in Comp.Sc. from Bharathidasan University, India. She has more than 25 years of service experience in the educational institutions to promote Research and Teaching-Learning processes. During her tenure, she has organized an International Conference which is technically sponsored by the IEEE and Springer; 3 national conferences; Faculty Development program; Workshops; seminars; and for students, technical symposiums. She has travelled to the Cambridge University, U.K. during Feb'2009 and has published more than 50 research papers with more than 40 citations in popular refereed publishers, IEEE, ACM and Springer. She has been invited to chair the technical sessions sponsored technically by the SPRINGER in the International conferences.