Performance Analysis of Elliptic Curves for VoIP Audio Encryption using a Softphone

Nilanjan Sen
NilanjanSen@my.unt.edu

Ram Dantu
Ram.Dantu@unt.edu

Dept. of Computer Science & Engineering, University of North Texas, Denton, Texas, USA

Abstract - The main reason for the growing popularity of Voice over IP or VoIP is that it is more economical among the other present telephone networks. But the security aspect has become a major issue for VoIP applications today. To protect the privacy of the callers, the audio call can be encrypted during the conversation. Major VoIP applications use symmetric key encryption to protect the VoIP media. But this may be vulnerable because the secret key used for the encryption can be intercepted. An asymmetric key encryption scheme can be a better choice in this context. Among other asymmetric key encryption, Elliptic curve cryptography (ECC) performs better due to its comparatively smaller key size and lesser computation time, but it must be chosen judiciously because VoIP audio encryption may cause high latency and jitter which may degrade the quality of the call. In this work, we have implemented an end-to-end ECC based encryption in a softphone to encrypt VoIP audio call. We have used 15 elliptic curves to measure the performance of audio call and based on that we have proposed some suitable elliptic curves for VoIP audio encryption. Our present work can be extended to encrypt smartphones' voice call.

Keywords

ECC VoIP Audio encryption Security

1. INTRODUCTION

Voice over Internet Protocol or VoIP is a very well-known term in the field of IP telephony. It is used to send audio (voice), video and multimedia sessions over IP networks. It has gained its popularity among common people as well as commercial enterprises because it is cheaper than the conventional telephone system. According to Zion Research Analysis, the estimated growth of the VoIP services market will be nearly $140 billion USD by the year 2021 [1]. The probable number of VoIP subscribers was nearly 1 billion at the end of 2018 [2].

But proliferative use of VoIP systems is also increasing the security violation. Some common security threats in VoIP are identity and service theft, phishing attack, eavesdropping etc. [3]. VoIP uses Real Time Protocol (RTP) to transmit audio/ video packets. RTP payloads may contain confidential data, so encryption is required to protect them from snooping attacks [4]. The Secure Real-time Transport Protocol (SRTP) works over RTP which has the provision to encrypt the VoIP media stream. SRTP uses AES encryption, a symmetric key encryption technique, to encrypt its payload, but it is vulnerable to eavesdropper [5]. According to IBM's report, the Session Initiation Protocol (SIP) is the most targeted protocol [18]. VoIP applications like Linphone exchange the security keys via SIP, so the key exchange operation may be vulnerable also. Dantu et al. have classified the VoIP protocols as Signaling protocols and Media transport protocol. They have explained that there are serious security flaws in both type of protocols [19]. The most serious threat of VoIP is eavesdropping. Since UDP datagram packets are used to transmit the media stream, this may lead to information leakage or media tampering by the attackers [20]. Furthermore, there is high possibility that an eavesdropper can get the key information during the call establishment time by intercepting the SIP INVITE and 200 OK messages. To resolve this issue, some softphones like Linphone, Zphone etc. use ZRTP, an extension header for RTP to establish a session key for SRTP sessions using authenticated Diffie-Hellman key exchange. ZRTP does not exchange the key during call establishment through SIP signal, but this also has some limitations. It is vulnerable to DoS attacks.

The shared secrets between the caller and the callee can be compromised also. During the installation, a unique ID, known as ZID is generated which is used to retrieve recipient's cached shared secrets, which is not authenticated. An attacker can intercept the previous call to obtain the callers' ZID to perform Man-in-the-middle attack [16].

In this work, we have implemented an asymmetric key cryptographic transform in SRTP payload based on Elliptic Curve Cryptography (ECC). We have used Linphone, a well-known open-source VoIP-based softphone, for our experiment. In our experiment, the caller and the callee use ECC scheme to generate a fresh set of private and public key pair for every session and exchange the session public keys during the call setup phase in a secured manner to avoid Man-in-the-middle attack. The callers use their session public-private key pair to encrypt and decrypt the call. Our present work is based on finding suitable elliptic curves for VoIP audio encryption without degrading the quality of the call. In our implementation, we have tested and analyzed 15 different ECC curves, and based on the results we have proposed some suitable ECC curves for VoIP audio encryption.

2. RELATED WORK

Most of the works in VoIP security were based on key management and authentication. A very few works could be found for VoIP message encryption using Elliptic Curve Cryptography (ECC). Some works were ECC based where authors discussed different vulnerabilities of AES keys and encryption system and why ECC based encryption technique would be better in this context [10, 11, 12]. On the other hand, many researchers tried to strengthen the encryption part of SRTP using AES encryption technique [13 – 15]. Some used AES-GCM and AES-CCM authenticated encryption to strengthen the integrity and authenticity of SRTP [14]. Some discussed how to encrypt the RTP header extension in SRTP using AES since it contained valuable information [13]. Others pointed out that SRTP and ZRTP cannot perform well in different private network. They modified SRTP protocol and proposed an encryption method to resolve the issue [15]. Some researchers had done comprehensive

survey on VoIP security issues, both on media encryption and key exchange protocols [16, 17].

Subashri et al. [10] pointed out that the VoIP protocols like SIP, IAX, and H.323 are unable to protect the media from attack. The keys used in AES algorithm were weak and vulnerable to different kind of attacks. They applied ECC for strong key generation using ECDHE.

Gunjan and Singh [11] suggested the solutions to different vulnerabilities of VoIP system. They also proposed a solution to DoS attacks through network modelling and used ECC to solve the Man-in-the-middle attacks. They proposed an encryption technique, where a plain text was converted to elliptic curve points. But converting the VoIP media into elliptic curve points is a challenging task.

Wang and Liu [12] developed an algorithm to exchange the key using ECDHE. Their scheme, known as Elliptic Curve-Dynamic Key Change Scheme (EC-DKCS) could generate different set of keys after a certain period of time. In their work, both caller and callee generated two pairs of public and private key using ECC key generation algorithm. They exchanged their public keys using SIP signals and generated two ephemeral keys using the ECC keys for encryption and for another key generation. But they have changed the SRTP packet format to include one extra field to keep track of the changing key.

Gupta and Shmatikov [16] had done a structured security analysis of the VoIP protocol stack, which consists of several protocols such as SIP, SDP, SRTP and different key establishment protocols like SDES, MIKEY, and ZRTP. They showed that SDES key exchange is vulnerable to replay attack where same ephemeral key might be used by SRTP for different session, which could be guessed by the adversaries. The MIKEY key generation procedure was not secured also because of the absence of proper randomness. On the other hand, ZRTP might suffer from unauthenticated user attack.

Apart from these, some works had been done based on application of ECC on smartphone apps or Android OS [28 - 31]. But most of the works were done for secure text/ message transmission, not for voice encryption.

3. MOTIVATION

We have already discussed that SRTP is used for VoIP media encryption using AES encryption scheme. AES works much faster than any asymmetric key encryption scheme. There are multiple key exchange methods for symmetric key scheme. One of them is, sender will encrypt the ephemeral secret key by receiver's public key, and receiver will decrypt it by its private key. Another approach is Elliptic Curve Diffie-Hellman Key Exchange method (ECDHE) where two users first exchange their public keys with each other and then they both will generate the same ephemeral key using their private key and others' public key. But researchers have shown that use of AES for audio message encryption in VoIP may lead to serious security breach [17]. The problems are discussed in following subsections.

3.1 Problem in existing SRTP key exchange mechanism

Gupta and Shmatikov showed that SRTP might use the same keystream that could help the attacker to get the XOR of the plaintext. SRTP generally relies on the key exchange protocol where the session keys are not repeated. But the popular key exchange protocol S/MIME-protected SDES does not have replay protection. SRTP derives the unique master key and master salt in each session. The master key is used to generate the session key for media encryption. If the attacker can replay an older SDES key establishment message, the same keystream will be repeated which will lead to generation of same master key and master salt. If an attacker can eavesdrop a previously carried out VoIP session, he can deceive the SRTP to generate the same old SDES key transfer message encrypted by S-MIME, and thus the same session key will be generated. The attacker may guess the original message by comparing it with the previous session's ciphertext encrypted using the same session key [16].

3.2 Problem in VoIP audio encryption using AES encryption scheme

One serious problem in AES encryption scheme had been shown in [36 – 38]. The default SRTP encryption scheme is AES in the counter mode (AES-CTR). The AES-CTR ciphertext size and the corresponding plaintext size are always same. The attackers may exploit this issue to reveal valuable information from the AES encrypted VoIP call, eg. the language used, some important words and phrases and others [36 - 38]. Even the use of padding may not prevent this attack. ECC uses Elliptic Curve Integrated Encryption Scheme (ECIES) where the encrypted message contains multiple information including the ciphertext [39]. In our experiment, we have tested that size of encrypted VoIP messages is same irrespective of the size of unencrypted VoIP payload.

3.3 VoIP camera video encryption using ECC

Internet of Things (IoT) devices have become an important part of our daily life, and VoIP camera is one of them. IoT devices are resource-constrained, and IoT security is the most important thing now-a-days because they have become the easy prey of the hackers. Lightweight security mechanism is preferred for VoIP cameras since they are resource-constrained devices. Conventional encryption schemes will not be suitable in this context, so ECC may be a better choice here. Some works had been done regarding this matter [40 - 42] where the researchers had shown different ECC-based security mechanism for IoT devices. Our present work is very much related to VoIP video encryption. So, the elliptic curves we have proposed here will be applicable to VoIP cameras also.

3.4 Other attacks against AES encryption scheme

Ramsay and Lohuis showed that AES encryption keys can be covertly recovered by side-channel analysis. They monitored the TEMPEST leakage from two AES-256 implementations using an antenna and some signal processing devices, performed the TEMPEST side-channel analysis, and then covertly recovered the AES encryption keys [35].

Hence, from discussion shows that the symmetric key encryption scheme can be vulnerable for VoIP audio encryption and an asymmetric key encryption scheme may make the system more secure. ECC may be a better choice in this context compared to its counterparts because of its smaller key size and lesser computational time. SRTP framework also has provision to implement a new cryptographic transform [21]. In our present work we have encrypted VoIP audio using Elliptic curve cryptography which is more secured than existing system. We have encrypted the entire RTP payload for better security which no one has done before.

4. ARCHITECTURE

We have used client-server architecture for the experiment. The callers are clients and a SIP server is used to setup a call. We have used MetroPCS 4G-LTE connection to connect one caller to the Internet through WiFi, and the server and another caller are connected to the institutional network through ethernet connection. We have used Ubuntu 16.04 (64 bits) operating system for server and the clients, and Repro server is used as SIP server. For our experiment, we have used Linphone 3.9.1 VoIP application, and opus audio codec. Every call duration is nearly 40 to 50 seconds. We conducted 3 experiments for each curve and then calculated the mean of the corresponding results.

5. METHODOLOGY

The methodology can be divided into two phases:

5.1 Key exchange during call setup

Both callers have their own pair of private-public keys where both public keys are verified by some certificate authority (CA). During the call setup, the caller generates a session private-public key pair, encrypts the session public key by callee's original public key and sends it to the callee via SIP INVITE message. The callee decrypts it using its original private key. The callee

follows the same methodology to send its encrypted session public key via SIP 200 OK message. In this way key exchange is done during the call setup. The CA authorized original public keys of the callers are used for session key exchange to avoid the Man-in-the-middle attack. For new session, a fresh set of session key pairs are generated and exchanged by the callers.

5.2 Conversation phase

During the conversation, the caller encrypts the voice payloads by the callee's session public key and sends it to the callee. The callee decrypts the audio streams by its session private key. The same methodology is followed when the callee sends audio stream to the caller. Encrypted media is sent as RTP payload and UDP is used as transport layer protocol.

6. RESULT ANALYSIS

In this work, we have tested the audio encryption using 15 ECC curves. They are X9.62 standard prime curve prime256v1 and binary curve c2pnb272w1 of key size 256 and 272 bits respectively, Standards for Efficient Cryptography Group (SECG) prime curve secp256k1 of key size 256 bits, NIST recommended prime curves secp384r1 and secp521r1 of key size 384 and 521 bits respectively, and Brainpool prime curves brainpoolp256r1, brainpoolp256t1 of key sizes 256 bits, brainpoolp320r1, brainpoolp320t1 of key sizes 320 bits, brainpoolp384r1, brainpoolp384t1 of key sizes 384 bits, and brainpoolp512r1, brainpoolp512t1 of key sizes 512 bits. We have considered only those elliptic curves with key size more than 224 bits according to NIST recommendation [23] for better security.

Table 1 shows the comparison of our work with similar type of works done by other researchers.

In this section we have analyzed the performance of the 15 ECC curves, 128-bit AES scheme, and the non-encrypted audio calls based on the end-to-end delay, and jitter. In our experiment, we got a few packet losses incidents in some ECC curves, but that couldn't degrade the quality of the audio call.

We have two test cases, first one during day time when we usually have heavy data traffic, and one in the early hours (between 1:30 AM and 3 AM), when the data traffic is comparatively low.

Figure 1 shows the end-to-end delay comparison between non-encrypted, AES-encrypted and other elliptic curves encrypted audio streams in milliseconds during day time when usually there is heavy network traffic. The delays of non-encrypted and AES encrypted audio streams are so negligible that they cannot be seen in this plot. The delay of AES encrypted audio stream is 0.0321 ms. The X9.62 256-bit prime curve's delay is shortest compare to

Table 1

Comparison of our work with other similar type of works

Work	**USE of ECC for key generation**	**Encryption scheme used**	**Elliptic Curve used**	**Implemen-tation**	**Soft-phone used**
Subashri et al. [10]	Yes	AES	Modified NIST P-256	Yes	X-Lite
Gunjan and Singh [11]	Yes	ECC	Binary curve GF(2^m) [NSA suggests prime curves only]	No	None
Wang and Liu [12]	Yes	AES	Not mentioned	Yes	A SIP-based soft phone
Our work	Yes	ECC	15 elliptic curves	Yes	Lin-phone

other ECC curves. The end-to-end delay difference between X9.62 256-bit curve and AES-encrypted audio stream is 0.7 milliseconds only. NIST 256-bit curves and Brainpool 320 and 384-bit curves also have short delays. We have noticed an unusual performance of NIST 521-bit prime curve in our experiment. The test shows that the delay of NIST 521-bit curve is lesser compare to other curves. The similar kind of result is obtained for jitter values also. It is hard to tell the exact reason right now but one of the possibilities may be due to some issues of Linphone application.

Figure 2 shows the end-to-end delay comparison in the early hours. This plot is nearly identical with the previous plot. Here also, the X9.62 256-bit curve has shortest delay among other elliptic curves. The delay difference between this curve and the AES is 0.4 ms only. In both plots we can see that the delays of all binary elliptic curves (c2pnb272w1, sect283k1 and sect283r1) are very high compare to prime curves.

The Brainpool curves' delays are more than the other prime curves in Figure 1 and 2, because Brainpool curves use random prime numbers to generate the field F_p for the elliptic curves, but the NIST prime curves generally use pseudo-Mersenne prime numbers which are used for fast modulo reduction [9].

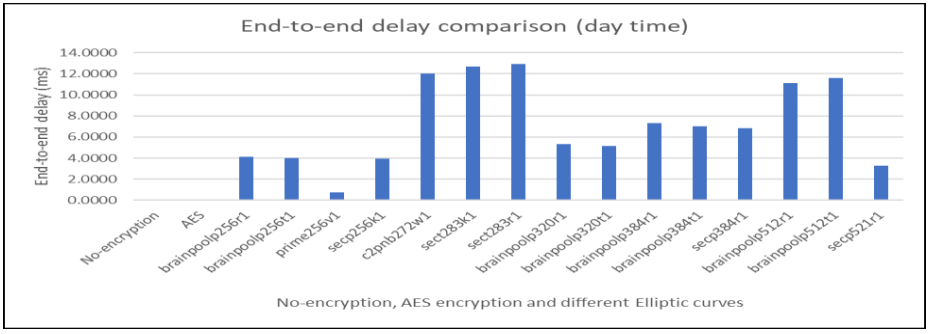

Figure 1: End-to-end delay comparison between non-encrypted, AES encrypted and other ECC-encrypted audio streams during day time. X9.62 256-bit curve, SECG 256-bit, NIST 384-bit and 521-bit, and Brainpool 320-bit and 384-bit curves have less end-to-end delay. X9.62 256-bit curve has lowest delay among all ECC curves. The difference between AES and X9.62 256-bit curve is only 0.7 milliseconds.

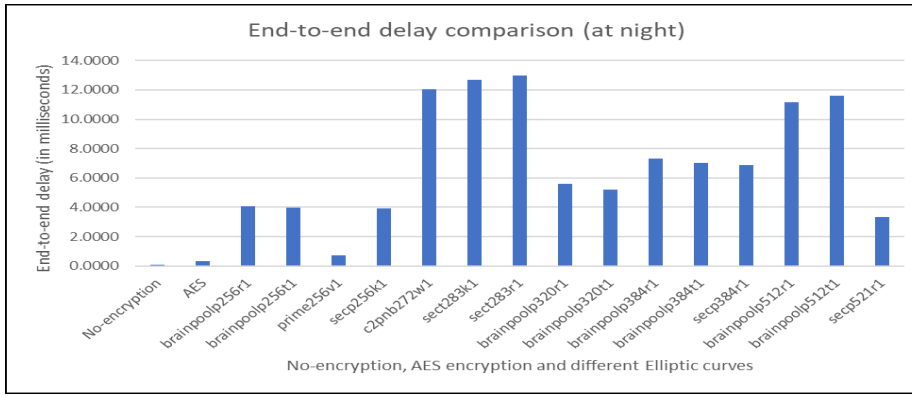

Figure 2: End-to-end delay comparison between non-encrypted, AES encrypted and other ECC-encrypted audio streams at night. X9.62 256 and 272-bit curve, NIST 256 and 521-bit curves, and all Brainpool curves except 320-bit random curve have small end-to-end delay. AES-encrypted audio stream has more delay compare to its day time value, but delay does not always depend on network traffic. Other factors like number of hops are involved also. The delays ECC-encrypted audio streams are nearly same as the delays during the day time.

Figure 3 and 4 depict the mean jitter comparison during day-time and at night respectively. The range of mean jitter here is between 2.50 ms and 9.20 ms. The jitter values of 3 binary curves are very high. X9.62 256-bit prime curve has smaller jitter than other ECC curves. Among other ECC curves, NIST 256 and 521-bit curve, and Brainpool 256-bit curves and 320-bit twisted curve have smaller jitter compare to other curves both during day-time and at night.

9. CONCLUSION AND FUTURE WORK

In this work, we have analyzed the performance of 15 elliptic curves on encrypted VoIP audio call. We have measured the performance of the curves based on two metrics viz. end-to-end delay, and jitter. After considering all aspects, we have concluded that X9.62 256-bit prime curve, NIST 256-bit and 384-bit prime curves, and Brainpool 256-bit random and twisted prime curves can be considered as suitable for VoIP audio encryption, because they have small latency and jitter values compare to other elliptic curves. We have

conducted our experiments in two environments, one during day time where the data traffic is usually heavy, and second one in the early hours when the data traffic is expected to be low. We have found that the performance of all curves is nearly same during two different times.

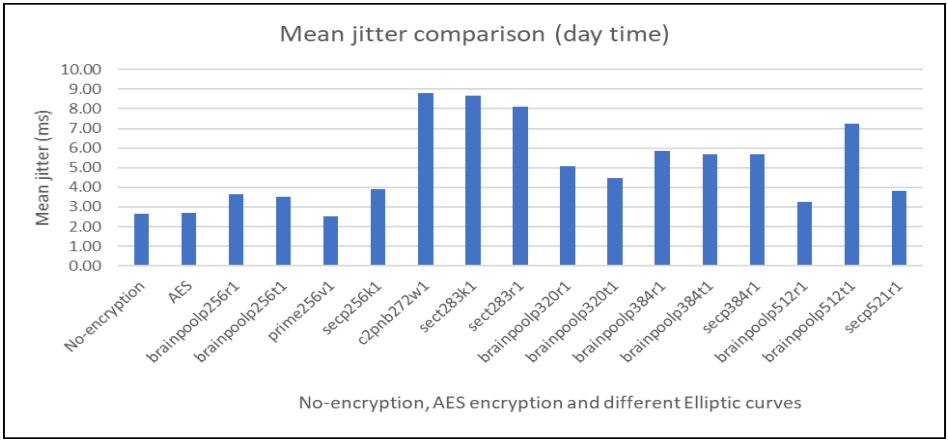

Fig. 3. Mean jitter comparison between non-encrypted, AES encrypted and other ECC-encrypted audio streams during day-time. All 3 binary curves have very high jitter. X9.62 256-bit curve, NIST 256 and 521-bit curves, and Brainpool 256-bit, 320-bit twisted curve and 512-bit random curve have small jitter values.

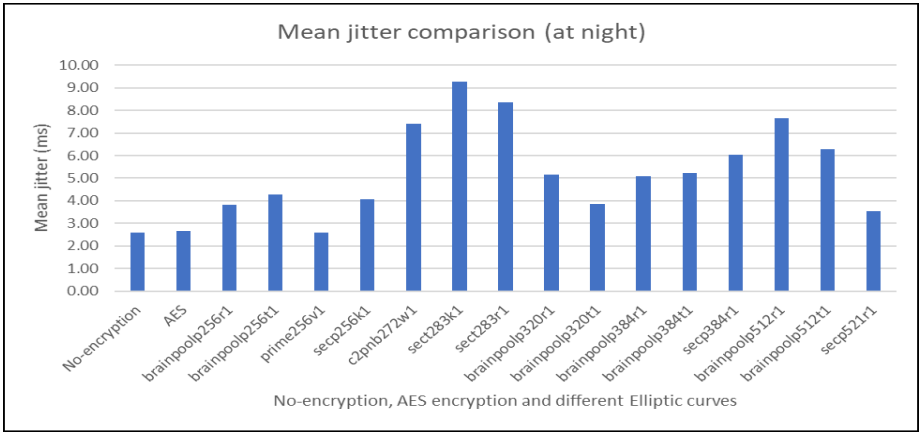

Fig. 4. Mean jitter comparison between non-encrypted, AES encrypted and other ECC-encrypted audio streams at night. Like day-time jitter values, all 3 binary curves have very high jitter. X9.62 256-bit curve, NIST 256 and 521-bit curves, and Brainpool 256-bit curves and 320-bit twisted curve have small jitter value.

Our present work can be further extended to implement ECC based encryption in smartphones' phone apps. We have mentioned some works in section 2 where ECC was implemented in different android applications or smartphone OS. Our work can be used to encrypt voice in VoLTE technology or upcoming 5G technology. Like VoIP, VoLTE also works using SIP and RTP. So, our present work can be applied for smartphone voice encryption after certain modification. Egele et al. have mentioned six rules that a secured application should follow. Two of them are: to be an IND-CPA secure application, an application should not use Electronic Codebook (ECB) mode for encryption, and it should not use a non-random initialization vector (IV) for Cipher Block Chaining (CBC) encryption [32]. They have showed that most of the smartphone apps violate these two rules. These modes are used by symmetric key encryption algorithms like AES. Today's most popular smartphones like iPhone X, Samsung Galaxy phones use AES for data encryption [33]. Some apps such as T-System's mobile encryption app [34] are available using which smartphone calls can be encrypted, but they use AES encryption scheme also. If we can apply ECC to encrypt voice, the smartphone calls will become more secured.

Our present work is also applicable to some IoT devices such as VoIP cameras. VoIP cameras require lightweight security mechanism and ECC may be the suitable choice.

Acknowledgment

We would like to express our profound and deep sense of gratitude to Dr. Jagannadh Vempati and other students of Network Security Lab for their invaluable help without which our work would not have been successful. This research is based upon work supported by the National Science Foundation under awards 1241768 and 1637291.

REFERENCES

[1] https://www.newsmaker.com.au/news/234173/voip-services-market-by-2021-set-for-rapid-growth-to-reach-around-usd-140-billion#.Wul4eYjwbIV.

[2] VoIP Trends in 2017, https://voipstudio.com/voip-trends-2017/

[3] Security Threats In VoIP, https://www.lifewire.com/security-threats-in-voip-3426532.

[4] Securing Internet Telephony Media with SRTP and SDP, http://www.cisco.com/web/about/security/intelligence/securing-voip.html#12

[5] D. P. Botero, and Y. Donoso, "VoIP Eavesdropping: A Comprehensive Evaluation of Cryptographic Countermeasures", Second International Conference on Networking and Distributed Computing, IEEE, 2011, pp. 192-196, DOI 10.1109/ICNDC.2011.46.

[6] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2004

[7] J. Lopez, and R. Dahab, An Overview of Elliptic Curve Cryptography. Technical Report IC-00-10, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.2771

[8] F. Li, X. Xin, and Y. Hu, Identity-based broadcast signcryption, Computer Standard and Interfaces 30, 2008, pp. 89–94

[9] Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf

[10] T. Subashri, A. Arjun, and S. Ashok, "Real Time Implementation of Elliptic Curve Cryptography over a Open Source VoIP Server", 5th ICCCNT, China, IEEE, 2014, pp. 1-6

[11] V. K. Gunjan, and P. Singh, "Security Enhancement of VoIP Protocols using ECC", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3 (12), 2013, pp. 158 – 164

[12] C. H. Wang, and Y. S. Liu, "A dependable privacy protection for end-to-end VoIP via Elliptic-Curve Diffie-Hellman and dynamic key changes", Journal of Network and Computer Applications, Elsevier, Vol. 34, 2011, pp. 1545-1556

[13] J. Lennox, and Vidyo, "Encryption of Header Extensions in the Secure Real-time Transport", 2013; http://tools.ietf.org/html/rfc6904#page-7.

[14] D. McGrew, and K.M. Igoe, “AES-GCM and AES-CCM Authenticated Encryption in Secure RTP (SRTP)”, 2012; https://tools.ietf.org/html/draft-ietf-avtcore-srtp-aes-gcm-02.

[15] Hyung-Jun Oh, and Yoo-Hun Won, “A Design of Encryption Method for Strong Security about Tapping/Interception of VoIP Media Information between Different Private Networks”, Journal of the Korea Society of Computer and Information, Vol. 17 (3), 2012, pp. 113-120

[16] P. Gupta, and V. Shmatikov, “Security Analysis of Voice-over-IP Protocols”, 20th IEEE Computer Security Foundations Symposium, 2007, pp. 49-63, DOI: 10.1109/CSF.2007.31

[17] A. D. Keromytis, “A Comprehensive Survey of Voice over IP Security Research”, IEEE Communicatioans Surveys & Tutorials, Vol. 14 (2), 2012, pp. 514-537.

[18] IBM warns of rising VoIP cyber-attacks, https://www.networkworld.com/article/3146095/security/ibm-warns-of-rising-voip-cyber-attacks.html

[19] R. Dantu, S. Fahmy, H. Schulzrinne, and J. Cangussu, “Issues and Challenges in Securing VoIP”, Computers & Security, Vol. 28, Elsevier, 2009, pp. 743-753

[20] D. Bigot, “Secure VoIP protocols: SIPS & SRTP”, http://wiki.linuxwall.info/doku.php/en:ressources:dossiers:voip:tls_sips_rtps

[21] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, “The Secure Real-time Transport Protocol”, http://www.rfc-editor.org/info/rfc3711

[22] https://github.com/BelledonneCommunications/linphone-desktop

[23] E. Barker, and A. Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST Special Publication 800-131A.

[24] ITU-T, Series G: Transmission Systems and Media, Digital Systems and Networks, file:///C:/Users/nilan/Downloads/T-REC-G.114-200305-I!!PDF-E.pdf

[25] CISCO - Quality of Service for Voice over IP, https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.pdf

[26] The New York Times. Government announces steps to restore confidence on encryption standards, http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards, 2013

[27] J. W. Bos, C. Costello, P. Longa, and M. Naehrig, “Selecting Elliptic Curves for Cryptography: An Efficiency and Security Analysis”, Journal of Cryptographic Engineering, Vol. 6(4), 2016, pp. 259-286

[28] D. Natanael, Faisal, and D. Suryani, “Text Encryption in Android Chat Applications using Elliptical Curve Cryptography (ECC)”, 3rd International Conference on Computer Science and Computational Intelligence, Indonesia, Elsevier, 2018, pp. 283-291

[29] T. Singh Ruprah, V. S. Kore, and Y. K. Mali, “Secure data transfer in android using elliptical curve cryptography”, International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, India, IEEE, 2017

[30] S. Desai, R. K. Bedi, B. N. Jagdale, and V. M. Wadhai, “Elliptic Curve Cryptography for Smart Phone OS”, International Conference on Advances in Computing and Communications, Springer, 2011, pp. 397-406

[31] S. R. Thiyagaraja, R. Dantu, P. L. Shrestha, M. A. Thompson, and C. Smith, "Optimized and Secured Transmission and Retrieval of Vital Signs from Remote Devices", IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, IEEE, 2017, pp. 25-30

[32] M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel, “An empirical study of cryptographic misuse in android applications”, ACM SIGSAC conference on Computer and Communications Security, 2013, pp. 73–84

[33] J. Knight, "The 4 Best Phones for Privacy & Security", https://smartphones.gadgethacks.com/how-to/4-best-phones-for-privacy-security-0176106/

[34] "Mobile Encryption App: Eavesdropping? No chance! – Encrypt cell phone calls and messages", https://www.t-systems.com/de/en/solutions/security/solutions/mobile-encryption-app/cell-phone-encryption-76050

[35] C. Ramsay, and J. Lohuis, White Paper: "TEMPEST attacks against AES covertly stealing keys for 200 euros", Technical Report, Fox-IT, Netherlands, 2017, https://www.fox-it.com/en/wp-content/uploads/sites/11/Tempest_attacks_against_AES.pdf

[36] C. V. Wright, L. Ballard, F. Monrose and G. M. Masson, Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?, 16th Usenix Security Symposium, 2007, pp. 43-54.

[37] C. V. Wright, L. Ballard, S. E. Coull, F. Monrose and G. M. Masson, Spot Me if You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations, IEEE Symposium on Security and Privacy, 2008, DOI: 10.1109/SP.2008.21.

[38] A. M. White, A. R. Matthews, K. Z. Snow and F. Monrose, Phonotactic Reconstruction of Encrypted VoIP Conversations: Hookt on fon-iks, IEEE Symposium on Security and Privacy, 2011, DOI: 10.1109/SP.2011.34.

[39] V. G. Martínez, F. H. Alvarez, L. H. Encinas, C. S. Ávila, A comparison of the standardized versions of ECIES, Sixth International Conference on Information Assurance and Security, 2010.

[40] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, L. Zhou, On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age, IEEE Transactions on Dependable and Secure Computing, Vol. 14(3), 2017, pp. 237-248.

[41] H. Hasan, T. Salah, D. Shehada, M. J. Zemerly, C. Y. Yeun, M. Al-Qutayr, Y. Al-Hammadi, Secure lightweight ECC-based protocol for multi-agent IoT systems, 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2017.

[42] O. Said, Y. Albagory, M. Nofal, F. Al Raddady, IoT-RTP and IoT-RTCP: Adaptive Protocols for Multimedia Transmission over Internet of Things Environments, IEEE Access, Vol. 5, 2017, pp. 16757 - 16773.