# Performance Analysis of Elliptic Curves for VoIP Audio Encryption Using a Softphone

Nilanjan Sen[1(✉)], Ram Dantu[2], and Mark Thompson[2]

[1] Western Illinois University, Macomb, IL 61455, USA
N-Sen@wiu.edu
[2] University of North Texas, Denton, TX 76207, USA
{ram.dantu,mark.thompson2}@unt.edu

**Abstract.** The usage of online media streaming has become an essential part of our daily lives due to COVID-19 pandemic. The security issues have gained in importance as well with the proliferative use of real-time media. Usually, symmetric key encryption schemes are used for encrypting real-time media, which are transmitted as Real-time Transport Protocol (RTP) payload. RTP uses the Secure RTP (SRTP) to secure its payload. Several issues exist in the existing SRTP media protection scheme that can be solved by applying lightweight asymmetric key cryptography such as Elliptic Key Cryptography (ECC). We have proposed some suitable Elliptic Curves for real-time audio encryption, which do not compromise the quality of the audio calls.

**Keywords:** Real-time audio · SRTP · Elliptic curve · ECC · Security · VoIP

## 1 Introduction

Real-time media streaming is a popular mode of entertainment and is used for professional and academic purposes. The present COVID-19 situation has increased the importance of real-time media services even more. VoIP audio calls are the integral part of real-time media. However, the proliferative use of real-time media streaming is simultaneously increasing the security threat, such as eavesdropping, copyright infringement, sensitive data revelation, and more. Real-time media is transmitted through the Real-Time Transport Protocol (RTP) with the help of Voice over IP (VoIP). The Secure Real-time Transport Protocol (SRTP) works over RTP and transmits encrypted RTP payload. SRTP uses a symmetric key encryption scheme. The existing SRTP encryption scheme may be vulnerable to the eavesdroppers due to some problems discussed in Sect. 2. These problems can be rectified using an asymmetric key encryption scheme. Since audio/ video quality is an essential issue in real-time media streaming, we


N. Park et al. (Eds.): SecureComm 2020, LNICST 335, pp. 503–508, 2020.
https://doi.org/10.1007/978-3-030-63086-7_28

should use a lightweight asymmetric key encryption scheme, such as Elliptic Key Cryptography (ECC). Its key size is smaller, and the computation time is lesser than other asymmetric key encryption schemes such as RSA.

ECC is based on Elliptic curves (EC). To maintain real-time media quality, we need to choose suitable elliptic curves, which result in less network latency and jitter. In this paper, we have discussed our work to find suitable ECs to secure real-time audio calls a.k.a. VoIP calls. We have also developed a new short-Weierstrass elliptic curve, $EW_{256357}$ at the 128-bit security level, which is more secure than a widely used NIST-recommended P-256 curve, and suitable for real-time audio encryption.

## 2 Motivation

We have noticed following issues in existing SRTP system:

- Session Initiation Protocol (SIP) is used for real-time audio call establishment [9] and is also used to exchange key information. The SIP messages are not encrypted, so the eavesdroppers can intercept those to get the key information. Security expert Anthony Critelli discussed one such attack in [3].
- Gupta and Shmatikov showed that the sender might unknowingly transmit old key information during the key exchanging phase of a new audio call session. Consequently, the attacker may decrypt the payloads by exploiting that old key information [11].
- The plaintext and ciphertext sizes are the same in the AES-CTR encryption scheme. If the Variable Bit Rate encoder is used during the audio call, the attacker may guess some phrases and words by comparing the bit-rate patterns of the captured packets with the known encrypted data [4–6].

These problems can be rectified using a light-weight asymmetric key encryption protocol such as ECC. Different types of elliptic curves are commercially used, such as X9.62 curves, NIST-recommended curves and Brainpool curves. NIST P-256 curve is an efficient elliptic curve. However, this curve has some security issues, such as lack of transparency in the curve generation process. NIST P-256 curve is weakly twist secure [8], hence vulnerable to specific attacks, such as Invalid-curve attack [7]. So, we developed a new elliptic curve suitable for VoIP audio encryption.

## 3 Methodology

All experiments were performed on 64-bit Ubuntu 16.04 platform. We used C and OpenSSL crypto library for the audio encryption experiments. A softphone, named Linphone, was used in this experiment. The Elliptic Curve Integrated Encryption Scheme was used as an ECC encryption scheme. We implemented


**Fig. 1.** Block diagram of experimental setup.

the newly proposed elliptic curve in Java and Bouncy Castle crypto library to test its real-time audio encryption performance.

For the audio encryption experiment, we used one SIP server and two clients where the server and one client were connected to the institutional network through WiFi. The second client was connected to the Internet. All clients had a pair of an EC-based public and private keys, known as their original keys which are publicly available, and certified by some Certificate Authority. During the call initiation phase, one of the clients (or caller) generated an ephemeral pair of EC-based pubic and private keys, known as session keys. The caller sent its encrypted ephemeral public key to the other client (the callee). The caller's ephemeral public key was encrypted by callee's original public key. The callee decrypted the caller's ephemeral public key by its original private key, generated its ephemeral pair of EC-based session keys, and followed the same steps to send its encrypted ephemeral public key to the caller. In this way, the caller and callee exchanged the EC based session key during the call setup. This method protected the real-time transmission system from the Man-in-the-middle attacks. The two pairs of session keys were used for real-time media encryption. For every session, the caller and callee generated a new pair of EC based session keys. The key exchange operation is described in detail in the next section. Figure 1 depicts the block diagram of our experimental setup.

### 3.1 Key Exchange Phase of Real-Time Audio Encryption

The SIP protocol is used for initiating a real-time media transmission session. SIP packets contain call setup and key exchange information. The later is available in plain text within the Session Description Protocol (SDP) portion of the SIP INVITE and 200 OK packets. SIP packets are generally un-encrypted, so the key information is visible.

We have used the ECC-based encryption technique where the clients' encrypted public keys are exchanged through SIP messages. Since the clients' private keys are not shared, if the attacker can somehow know the clients' public keys from intercepted SIP messages, she/ he cannot decrypt the SRTP payload. In our experiment, the caller had sent its ephemeral public key through SIP INVITE message, and the callee had sent its ephemeral public key through SIP 200 OK messages. The screenshot of such a SIP INVITE message is shown in Fig. 2.

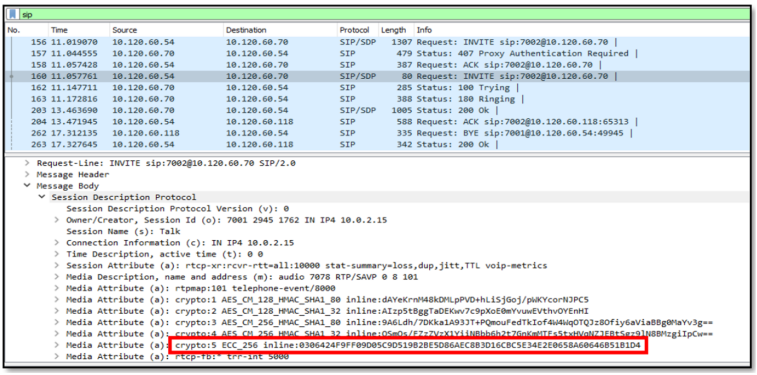


**Fig. 2.** SIP INVITE message with sender's 256-bit Elliptic curve public key.

The figure also shows the presence of AES session key information in SIP INVITE message. Since the AES key information is in plaintext, it becomes vulnerable to attacks.

### 3.2 Replacement of SRTP's Existing AES Scheme by ECC

Due to the security issues discussed in Sect. 2, we have replaced the existing AES scheme of SRTP by ECC. Usually, asymmetric key encryption schemes are not used for payload encryption, but we saw that real-time audio quality was not affected by ECC encryption. The network latency and network jitter are two essential parameters to measure the performance of real-time media transmission. In our experiments, the latency of chosen ECs are within 12 ms, and jitter values are within 9 ms for real-time audio. These values are far below the maximum values recommended by ITU-T G.114 [2] and Cisco [1]. So, we can rectify the problems of the existing SRTP system by ECC implementation for better security. In our proposed scheme, the existing AES-based SRTP system is replaced by an ECC-based encryption system. The proposed SRTP real-time media encryption system is depicted in Fig. 3.

## 4 Results of the Experiments

We experimented with four types of elliptic curves, viz. X9.62 prime and binary curves, SECG prime curve, NIST prime, and binary curves, and Brainpool prime curves. 15 elliptic curves were tested for real-time audio encryption.

### 4.1 Suitable Elliptic Curves for Real-Time Media Encryption

After analyzing the performance of 15 elliptic curves with respect to network latency and jitter, we concluded that X9.62 256-bit prime curve, SECG 256-bit

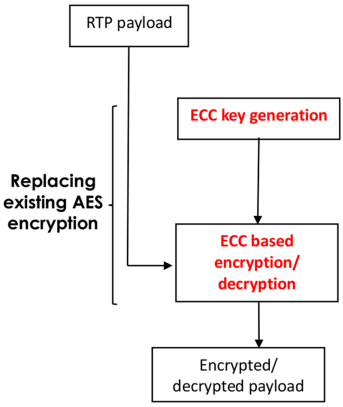


**Fig. 3.** Proposed SRTP media encryption system architecture.

prime curve, and Brainpool 256-bit random and twisted prime curves could be suitable for real-time audio encryption. We have also noticed that the prime curves' performance was better than that of binary elliptic curves on audio encryption.

### 4.2 New Secure Elliptic Curve for Real-Time Media Encryption

Based on all requirements of a secure elliptic curve, we have developed a 256-bit twist secure short-Weierstrass elliptic curve (a prime curve) at 128-bit security level [10]. The equation of our proposed curve $EW_{256357}$ is

$$E : y^2 = x^3 - 3x + 5029 \tag{1}$$

Our newly proposed curve contains all traits that are essential for a secure curve. Our curve is compatible with the NIST P-256 curve, which means it can fit all applications that use the NIST P-256 curve. At the same time, our curve

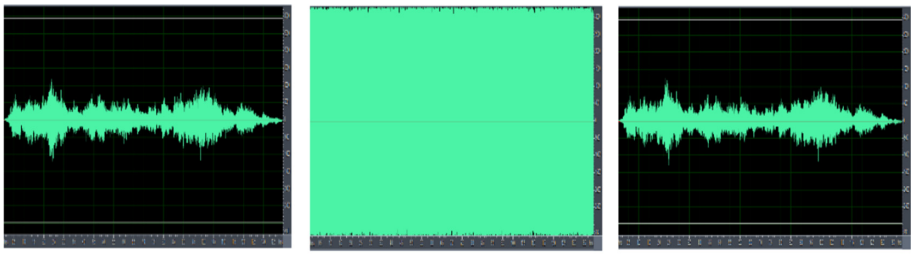


**Fig. 4.** (a) Original waveform of the audio before encryption (b) waveform of the encrypted audio (c) waveform of the decrypted audio.

is more secure than the P-256 curve since it is twist secure, and its generation process is fully transparent, unlike the P-256 curve. We have successfully tested our curves by encrypting real-time audio. Figure 4 shows the original audio waveform, the waveform after encryption, and the waveform after decryption.

## 5 Conclusion

In this paper, we have discussed the existing SRTP scheme's problems regarding secure real-time media transmission. We have proposed an ECC based alternate encryption scheme that can rectify those problems. We have suggested some suitable elliptic curves for real-time audio encryption to protect VoIP audio calls. We have also developed a new 256-bit prime elliptic curve, which is more secure than the widely-used NIST P-256 prime curve and is suitable for real-time audio encryption.

## References

1. 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
2. ITU-T, Series G: Transmission Systems and Media, Digital Systems and Networks. https://www.itu.int/rec/T-REC-G.114-200305-I
3. Critelli, A.: Hacking VoIP: Decrypting SDES Protected SRTP Phone Calls. https://www.acritelli.com/blog/hacking-voip-decryptingsdes-protected-srtp-phonecalls
4. White, A.M., Matthews, A.R., Snow, K.Z., Monrose, F.: Phonotactic reconstruction of encrypted VoIP conversations: hookt on fon-iks. In: IEEE Symposium on Security and Privacy (2011)
5. Wright, C.V., Ballard, L., Monrose, F., Masson, G.M.: Language identification of encrypted VoIP traffic: alejandra y roberto or alice and bob. In: 16th Usenix Security Symposium, pp. 43–54 (2007)
6. Wright, C.V., Ballard, L., Monrose, F., Masson, G.M.: Spot me if you can: uncovering spoken phrases in encrypted VoIP conversations. In: IEEE Symposiumon Security and Privacy **28** (2008)
7. Bernstein, D.J., Lange, T.: SafeCurves: choosing safe curves for elliptic-curve cryptography. https://safecurves.cr.yp.to. Accessed 09 August 2020
8. Bernstein, D.J., Lange, T.: Security dangers of the NIST curves. https://cr.yp.to/talks/2013.05.31/slides-dan+tanja-20130531-4x3.pdf
9. Rosenberg, J., et al.: RFC 3261: SIP: Session Initiation Protocol
10. Sen, N., Dantu, R., Morozov, K.: $EW_{256357}$: a new secure NIST P-256 compatible elliptic curve for VoIP applications' security. In: Accepted in 16th EAI International Conference on Security and Privacy in Communication Networks (2020)
11. Gupta, P., Shmatikov, V.: Security analysis of voice-over-IP protocols. In: 20th IEEE Computer Security Foundations Symposium, pp. 49–63 (2007)