PROTOCOL SAFETY OF VOIP USING THE CRYPTOSYSTEMS BASED ON ELLIPTIC CURVE

Layie Paul[1] and Vivient Corneille Kamla[2]

[1]Department of Mathematics and Computer Science, Faculty of Science, University of Ngaoundere, Cameroon

[2] Departments of Mathematics and Computer Science, ENSAI, University of Ngaoundere, Cameroon

ABSTRACT

VoIP (Voice over Internet Protocol) is used for peer-to-peer or multi-points communications. SRTP (Secure Real-Time protocol) is used for peer-to-peer communications which are no longer suitable when you want to do multi-point of VoIP. SRTP uses DH (Diffie Hellman) for key exchange but does not make the certification. This means that SRTP does not guarantee non-repudiation service and presents security vulnerabilities during exchanges of keys. In this work, we propose ECMSRTP (Elliptic curve Multi-point Secure Real Time Protocol) which is a new VoIP security protocol for multi-point communications. It uses the certification mechanism, ensures non-repudiation and makes encryption using El-Gamal based on elliptic curves. Performance analysis shows that this new protocol has a latency time better than SRTP. It has a complexity of $O(n^2)$ for key exchange against $O(n\sqrt{n})$ for SRTP, $O(n^2)$ for encryption against $O(2^n)$ for SRTP and $O(\sqrt{n})$ for signature against $O(n^2)$ for SRTP.

KEYWORDS

VoIP, Elliptic Curve, Cryptosystem, Protocol safety.

1. INTRODUCTION

VoIP being the transmission of voice over IP (Internet Protocol) networks, is an architecture which currently brings remarkable success due to its advantageous cost. Some authors, such as C. Baillet [3], R. Bouzaïda [7], G. Pujolle [27] [25], mention that many enterprises are interested in this technology and that by 2020, almost all enterprises will use VoIP in their environments. However, the interconnection of the telephony and the IP network brings the risks of the IP network towards a network which was protected because it (telephony) is closed to computer science [3], [14], [19], [21], [30]. It is within this scope that the authors of the reference's document RFC3711 (Describing SRTP [5]) were able to identify several threats and vulnerabilities. In this way, we can realize that the security problem of VoIP can come from the different levels of the TCP/IP (Transmission Control Protocol / Internet Protocol) protocol stack. The threats being thus very wide, it is therefore important to be able to apply security services. Thus, in the literature, several security solutions have been proposed depending on the objectives. So, we can have for example the security provided to the network layer like IPSec (Internet Protocol Security) [30] ; to the transport layer like TLS (Transport Layer Security) [11] ; to the application layer like SIPS [8] for Signalization, SRTP and SRTCP (Secure Real-Time Control Protocol) [5] for the transport and control of real-time's data. For all these security solutions, the most important are those which are applied to the application layer more precisely to the transport protocol of real-time data such as specified by most authors ([22], [3], [4], [12], [14], [23], [5]) who have worked in the field of the VoIP's security. Indeed, for these authors, the security provided to the transport protocol of the real-time data is the best adapted because even if we have an IP network where all of the layers of the TCP /IP protocol stack are not Well-secured, voice data should not be easily decipherable in a polynomial time. In this way, we can say that the best solution for the VoIP's security is the profile of RTP: the SRTP. Indeed, described in RFC3711 (reference document), the SRTP protocol is the security solution of the transport protocol of the voice data which is the most used in practice. So, the SRTP uses the AES (Advanced Encryption Standard) algorithm ([6], [9], [13], [16], [18], [24]) for encryption; the HMAC-SHA-1 (Hash message authentication code - Secure Hash Algorithm 1) algorithm [26] for authentication and the Diffie Hellman (DH) protocol for key exchange [2]. However, this protocol still has several shortcomings, in particular: the key exchange problem imposed by AES, the non-repudiation service which is not well-guaranteed due to the certification system which isn't used, and in addition, this protocol is not suitable for multi-point communications[28]. In this work, we propose a protocol for the security of VoIP architecture especially to the application layer: the security of RTP using cryptosystems based on elliptic curves [10], [15], [17], [20], [31], [34] which we call ECMSRTP for Elliptic Curve Multi-point Secure RTP.

The rest of this article is organized as follows : Section 2 presents the importance of the used of El-Gamal cryptosystem and a signature algorithm based on elliptic curves for VoIP; Section 3 presents what has been done in terms of security of VoIP especially the security of RTP while insisting to the limits of those solutions ; Section 4 presents the ECMSRTP (the new secure RTP) ; Section 5 gives the complexity analysis and the proof of safety is shown in Section 6 ; Section 7 studies performance compared to SRTP.

2. IMPORTANCE OF USING THE EL-GAMAL CRYPTOSYSTEM AND A SIGNATURE ALGORITHM BASED ON ELLIPTIC CURVES FOR VOIP

Encryption using elliptic curves has advantages over other encryption techniques: the level of security is greater and the keys used are shorter [33]. However, since the theoretical developments on elliptic curves are relatively recent, the resolution of the discrete logarithm problem may still be possible. But, the implementation of a good scalar multiplication mechanism of the points of these curves can solve the problem. For our architecture, in order to propose a solution which respects the conditions and objectives, it is important to use an encryption algorithm that uses fewer keys and less computing time. El-Gamal based on elliptic curves is, therefore, better suited for the encryption of VoIP flows. In addition, it is also important that the certification authority uses a signature algorithm based on elliptic curves [15].

3. VOIP'S SECURITY REVIEW

Since the VoIP architecture requires a limited number of speakers (only participants of a communication at a given time), it is necessary to bring out the security policy. In the literature, several VoIP security solutions have been proposed. This is how we can observe that the security is provided at different levels of the TCP / IP protocol stack. However, the most important is the one made at the application layer, so we present in this section the SRTP protocol described in the reference document RFC3711[5]. We will give firstly the generalities of VoIP.

3.1. GENERALITIES ON THE VOIP

The Voice over IP is a technique that enables to communicate by voice over IP-compatible networks, whether it is private or Internet network, wired cable/ADSL/Optical) or not (Satellite, Wi-Fi, GSM ...). This architecture has a very high time constraint and uses three types of protocols: real-time transport protocols, signalling protocols and the TCP/IP protocols stack.The VoIP architecture inherits to all known faults and vulnerabilities of the IP network. According to [19], [14], [3], the vulnerabilities can appear in the various steps of the VoIP infrastructure lifecycle. This is the reason why several types of attacks have been carried out today. In the same way that there are attacks, there are also solutions like SRTP.

3.2. THE SRTP PROTOCOL (DESCRIBED IN [5])

3.2.1. THE SECURITY CONSTRAINTS OF SRTP

To maintain the objectives of the real-time protocols, a good security policy must be applied. Thus, AES (Advanced Encryption Standard) is used for encryption and HMAC-SHA-1 for authentication.

3.2.2. THE SECURITY OF SRTP

3.2.2.1. THE OBJECTIVES AND CHARACTERISTICS OF SRTP

The main objective of SRTP is to provide at the same time: the confidentiality of RTP data, integrity, the RTP packet authentication, and replay protection.

SRTP represents an RTP profile and must be implemented without any RTP modification. Figure 1 shows the format of the SRTP packet.

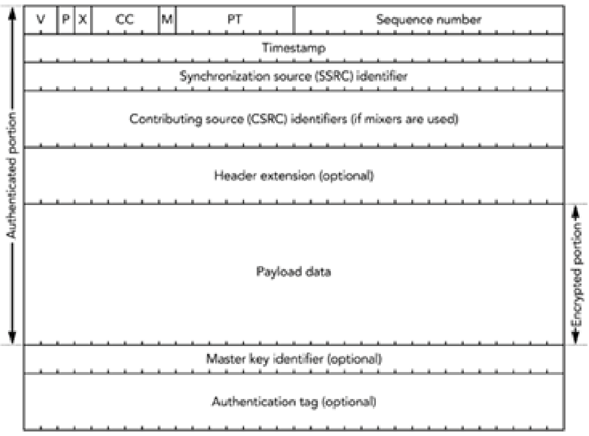

V
P
X
CC
M
PT
Sequence number
Timestamp
Synchronization source (SSRC) identifier
Contributing source (CSRC) identifiers (if mixers are used)
Header extension (optional)
Payload data
Master key identifier (optional)
Authentication tag (optional)
Authenticated portion
Encrypted portion

Figure 1: Format of the SRTP package [5]

The MKI fields and the authentication label are added to the end of the package:

- MKI (Master Key Identifier): this identifier allows to locate the master key from which the session key was generated.
- The authentication tag: the validation of the integrity whose sequence number avoids replay; the encryption is always performed prior to the creation of the authentication tag; the MKI is not protected because it does not provide additional protection.

SRTP authentication mechanisms are not mandatory, but all implementations should be used in order to ensure the integrity.

3.2.2.2. THE KEY EXCHANGE MECHANISM

To exchange the keys, SRTP uses non-RTP means like SIP [29] and the MKI must be used to synchronize the modification of master key. To do this, the Diffie-Hellman key exchange protocol based on the elliptic curves is used [32].

3.2.3. ANALYSIS OF THE SRTP'S COMPLEXITY

The analyzing of SRTP protocol amounts to analyze the three of cryptographic protocols used by SRTP: DH key exchange, AES encryption and HMAC-SHA-1 signature.

Complexity of DH on curves: The complexity of this algorithm was evaluated by Mustapha Hedabou in [15] and is O($\sqrt{n}$). That gives O($\sqrt{n}$) for n participants.

Complexity of the AES encryption protocol: The complexity of this algorithm was evaluated by C. Paar et J. Pelzl in [26] and gives O(2^n), n Being the size of the key.

Complexity of HMAC-SHA-1: The complexity of this algorithm was evaluated by C. Paar et J. Pelzl in [26] and is O(2^n), n being the size of the key.

Although this RTP's security solution respects the real-time constraints and especially that it is well secured, it nevertheless encounters some weaknesses.

3.2.4. The Weaknesses of the SRTP Protocol

It will not be a question here to show the weaknesses of the VoIP architecture in general; But rather to present the weaknesses of the RFC3711's reference document [5] describing the SRTP protocol. So, we may have many weaknesses:

- Only one key (master key) is used for encryption. Thus, the compromise of the key by one of the hosts obviously leads to the suppression of the confidentiality of the entire conversation.
- The key exchange method used is DH. However, this type of exchange is possible only with point-to-point scenarios. Indeed, with this solution, it seems difficult to share the same secret with several hosts. For other scenarios (Point-to-Multipoint, Multipoint to Multipoint) as explained in [5], public-key cryptography is preferred. This makes architecture complex.
- In addition, if DH does not use the certificate system, which is the most recurring case of this architecture, the secret's key should be found by MITM (Man In the Middle) attacker
- The non-repudiation service is not well guaranteed.

Since the SRTP protocol has many security problems, it is therefore important to propose a new RTP security protocol. In fact, since this architecture requires very high constraints, it will be necessary to propose a more adapted solution than the one described in the reference document RFC3711 while respecting the constraints imposed by this architecture.

4. Presentation of ECMSRTP Protocol

In this section, we propose a new RTP security protocol. We call this protocol the ECMSRTP: Elliptic Curve Multipoint Secure RTP.

4.1. Objectives, Characteristics and Constraints of ECMSRTP

The main objective of ECMSRTP is to provide the same security services as SRTP plus non-repudiation. It is therefore characterized by the addition of the EKI (Encryption Key Identifier) fields and the certification label as shown in figure 2 below.

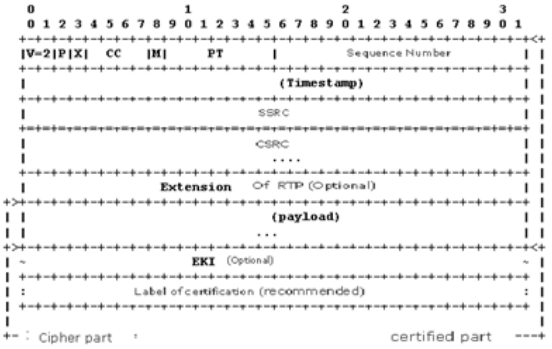


Figure 2: ECMSRTP's package format

The fields which are added are the EKI and the certification label:

- EKI (Encryption Key Identifier): Allows locating the public encryption key.
- The certification label: Validation of integrity whose sequence number avoids replay; Encryption is always performed before the creation of certification label; The EKI field is not protected because it does not provide additional protection.

Concerning the constraints, by comparing the security algorithms, we realize that private key cryptosystems are to be avoided because AES (which is the most suitable private key cryptosystem for SRTP protocol) has several weaknesses. In order to respect the constraints of the RTP, those based on the elliptic curves are better adapted because their computation time is short and in addition, their key is small which is good for the memory occupation (their keys are between 160 and 512 bits).

4.2. PRESENTATION OF THE ECMSRTP PROTOCOL

4.2.1. CRYPTOGRAPHIC TRANSFORMATION

In order that the ECMSRTP protocol will be well secured and the time constraints will be well established, SRTP will undergo the following cryptographic transformations (see figure 3):

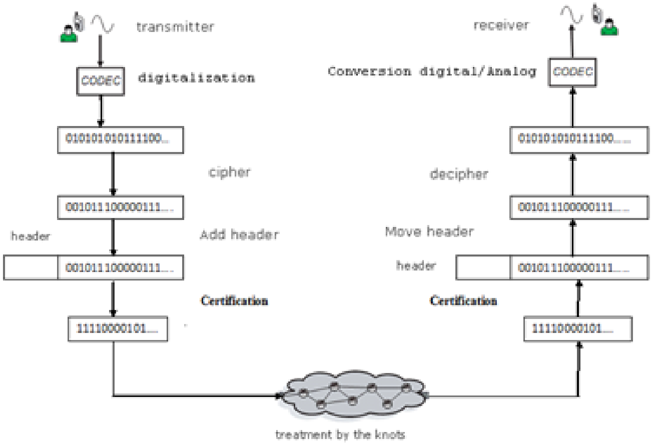


Figure 3. Process step of the ECMSRTP

- Encryption: ECMSRTP uses the El-Gamal algorithm on elliptic curves instead of AES used by SRTP.
- Certification: ECMSRTP uses a signature algorithm based on elliptic curves in place of the HMAC-SHA1 algorithm used by SRTP (to be used by the Certification Authority).

It should be noted that the EMSRTP certification mechanisms are not mandatory, but all implementations should use them to ensure integrity, authentication and non-repudiation.

4.2.2. CRYPTOGRAPHIC CONTEXT

4.2.2.1. CONTEXT

The cryptographic context allows the sharing of information about security between the ends of the communication. For the ECMSRTP, the parameters of the cryptographic context will be:

- Keys: We will use a pair of key for encryption and a pair of key for certification; and this will be done in a non-RTP context.
- An index (i) calculating from the overflow counter, ROC (Roll-Over Counter) : an unsigned 32 bit integer that count and save how many times the 16 bits RTP sequence number has been

reset after passing through 65 535 and the sequence number (SEQ) that ECMSRTP extracts from the RTP packet header. We define the ECMSRTP index corresponding to a certain ROC and RTP sequence number, which is defined as being the quantity of 48 bits : $i = 2^{16} * \text{ROC} + \text{SEQ}$.

- An identifier for the encryption algorithm
- An identifier for the algorithm used to certify the message
- A list of replay, maintained by the receiver only (to ensure authentication and protection against replay data) containing the index of packages for ECMSRTP recently received and certified
- Non-negative integers n_e, and n_c, Which determine the length of encryption keys, and message certification.
- An EKI flag (0/1) to know if the EKI field is present in the ECMSRTP packets
- The value of EKI if it is present
- The {From, To} value, that precise the lifetime of keys, expressed in terms of two index values of 48 bits within the key validity ranges (including the endpoints of the range). {From, To} is an alternative solution to the EKI and assumes that the public keys are in bijective correspondence with the private keys for the security of RTP on which is defined the range {From, To}.

4.2.2.2. TRANSPOSITION OF SECURE RTP PACKETS INTO CRYPTOGRAPHIC CONTEXTS

It is recalled that an RTP session is defined for each participant [RFC3550] by a pair of destination addresses (a network address plus a transport address or port for RTP) and a media session is defined as a collection of RTP sessions. For example, a particular multimedia session includes RTP audio session, RTP video session, and RTP text session. A cryptographic context must be uniquely identified by the context identifier triplet:

Context ID = {SSRC, Destination network address, Destination transport access number}.
Where the destination network address and the destination transport access are those that are in the secure RTP packet. It is assumed that when we present him this information, key management returns a context with the information described in paragraph IV.2.2.1. If no valid context can be found for a packet corresponding to a certain context identifier, the packet must be discarded.

4.2.3. ALGORITHM OF A PACKET'S TREATMENT

The following way is applied to the new form of RTP security. Assuming that the initialization of the cryptographic context(s) took place via key management. Thus, we consider that a protocol outside RTP (for example SIP) allowed the receiver to generate its keys and at the same time to publish the set consisting of its public key. The issuer will, therefore, need to do the following to build an ECMSRTP package:

1. Determine which cryptographic context is used.

2. Determine the index of the ECMSRTP packet using the ROC, the sequence number in the cryptographic context, and the RTP sequence number.

3. Obtain the receiver's public key.

4. Encrypt the RTP payload to produce the encrypted portion of the packet. This step uses the encryption algorithm specified in the cryptographic context.

5. If the EKI flag is set to one, Add the EKI to the packet.

6. Negotiate the certification key with the certification authority (CA)

7. Calculate the certification label of the package. This step uses the flag of the algorithm used for certification specified in the cryptographic context, and the public certification key issued by the CA. Add the certification label to the package.

8. If necessary, update the ROC, using the index determined in step 2.

To verify the certification and decrypt the ECMSRTP, the receiver must do:

1. Determine which cryptographic context to use.

2. Apply the algorithm using the ROC and the sequence number in the cryptographic context with the sequence number to obtain the index of ECMSRTP.

3. Obtain the public certification key

4. To certify the message and the protection against replay, first, check if the packet has been repeated using the list of replay and the index as determined in step 2. If the packet is deemed repeated, it must be discarded, and the event should be recorded. Then, perform the certification label verification, using the public certification key from step 3. If the result is "FAILURE OF CERTIFICATION" the packet must be eliminated from the rest of the processing and the event must be recorded.

5. From the index calculated in step 2, determine the private key corresponding to the public key used for the encryption. If the EKI flag in the context is set to one, use the EKI to determine the private decryption key.

6. Decrypt the encrypted portion of the packet using the decryption algorithm indicated in the cryptographic context, the private encryption key.

7. Update the ROC and the sequence number in the cryptographic context. If repeat protection is provided, also update the list of replay.

8. If present, remove the EKI and Certification Label fields from the package.

4.2.4. INDEX DETERMINATION AND KEY MANAGEMENT

Note that the management of keys is concerned by a protocol except RTP like SIP for example. But, in this subsection, we will discuss how the keys are managed. For predefined transformations, A index i is used in protection against replay, in encryption, and in message certification. When the session begins, the transmitter must set the ROC to zero. Whenever the sequence number RTP, SEQ, returns to zero modulo 2^{16}, the transmitter must increment ROC of one modulo 2^{32}. The index of the packet of the transmitter is then defined by $i=2^{16}*ROC+SEQ$.
With this index, you can manage the different keys. Indeed, as we are in a security context, the same key pair must not be used to encrypt all messages. To manage this key set, an EKI identifier must be added to each encrypted message in order to identify each key pair. To thus identify an El-Gamal encryption key pair, it is, first of all, transformed the points P and B of the public key into an integer modulo 2^{32} then, the index i calculated is added: We will, therefore, have EKI $\equiv (B+P+i)\mathrm{mod}2^{32}$. If the CA uses a signature algorithm based on the number. In the case where it is a signature algorithm based on the elliptic curves that are used, the index is instead transformed into a point: EKI = (B + P + i). From this, we can find the key pair used. An important particular case is that of wireless communication systems, in which the band is a scarce and costly resource. Therefore, we will simply use the {From, To}.

4.2.5. REASONS FOR THE APPLICATION OF SOME DISPOSITIONS OF ECMSRTP

We explain here the reasons behind several important features of ECMSRTP.

4.2.5.1. Keys generation

The generation of several encryption keys prevents an attacker from obtaining large quantities of encrypted texts produced by a single fixed encryption key. Indeed, if the attacker was able to collect a large amount of encrypted text for a certain encryption key, this could help him mount some attacks [32], [5].

Generating multiple keys to encrypt a communication provides forward and backward security in that a compromised session key does not compromise the other encryption keys generated.

4.2.5.2. Changing Key

The recommended way for a particular key management system to provide the key change within the ECMSRTP protocol is by associating an encryption key in a cryptographic context to an EKI. This allows easy rendering of the encryption and decryption key of the receiver but has the disadvantage of adding additional bits to each packet. Note that some wireless links do not load added bits, so the ECMSRTP also defines a more economical way of triggering the key change via the use of {From, To}, Which works in simple specific scenarios.

4.2.5.3. Certification

As shown in Figure 2, the certification label is RECOMMENDED in the new Secure RTP. Indeed, encrypting of the message guarantees only confidentiality. But, Non-repudiation, integrity, authentication and protection against replay are only guaranteed by a certification system which, moreover, preserves us from certain attacks such as the attack of the man in the middle for example.

4.2.5.4. Encryption

With AES, we were only doing point-to-point. However, with El-Gamal, the multipoint is now possible. Indeed, with the publication of the keys imposed by El-Gamal, several receivers will be able to obtain encrypted messages coming from one or more transmitters at a time and vice versa.

5. Complexity Analysis of Ecmsrtp

The ECMSRTP protocol uses three types of algorithms: key generation, encryption and certification. To analyze the complexity of this protocol we will simply have to evaluate the complexity of each algorithm used.

5.1. Analysis of Complexity of the Key Exchange Algorithm

The complexity of a key exchange protocol or algorithm computes at two levels: at the cost of communication and at the cost of computation.

5.1.1. Analysis of Cost into Communication

The number of laps: The protocol runs in one round because each participant broadcasts only one Information to the CA which in turn broadcasts the information to the entire group.

The number of broadcasts: For a set of n participants in the protocol, there are n broadcasts because the participants broadcast each of them a message to the CA, which in turn redisplays the messages to all the participants. This makes a total of n + n = 2n diffusions. The cost will be O(n).

Messages sent by participant: A given participant sends his / her public key to the CA, which rebroadcasts it to the (n-1) other participants plus one feedback of the participant. Which give (n-1) + 1 = n messages for a cost of O(n).

Total messages exchanged: $\sum_{i=1}^{n} n$ Messages because each participant sends n messages. From where we have $\sum_{i=1}^{n} n = n(\sum_{i=1}^{n} 1) = n * n = n^2 \in O(n^2)$ Exchanged messages.

5.1.2. Calculation Cost Analysis

The only basic operation performed here is the scalar multiplication operation.

Scalar multiplication: The N participants choose each of them during the generation keys at a time t_i given, one generator P of the curve. Each of them computes k_iP. Now, according to the scalar multiplication algorithm, if n is the number of bits for each secret k_i Belonging to a given participant, we will have a complexity of 1,86n. Thus, at every moment ti, each participant will have a complexity of 1,86n. If, therefore, at the end of the communication, we have done T = $\sum_{i=1}^{s}(t_i)$ (with T = $t_1 + t_2 + t_3 + ... + t_s$) time, we will have: $\sum_{i=1}^{s}(t_i * 1.86n)$ = 1.86n$\sum_{i=1}^{s}(t_i)$ = (1.86n)T scalar multiplication by a given participant.

5.2. Analysis of Complexity of the Encryption Algorithm

In the ECMSRTP protocol, we use the El-Gamal algorithm based on elliptic curves to manage the confidentiality of the data. However, this algorithm has two levels of execution: encryption for the sender and decryption for the receiver. Therefore, we will evaluate the cost calculation of each basic operation of each execution level. We will at first evaluate the complexity of the encryption before evaluating the complexity of the decryption.

5.2.1. Analysis of Encryption Complexity

The basic operations performed here are: the scalar multiplication, the point addition and the transformation message into point operation.

Transformation of Message into Point: Each participant starts by transforming each message into a point on the curve. Thus, since each transformation has a complexity of $\log_{256}(q)$, we will have $\sum_{i=1}^{n}(\log_{256}(q))$ (with q a prime number of the field IF_q) transformations of the message into a point for the n participants. This give $\sum_{i=1}^{n}(\log_{256}(q))$ = $(\log_{256}(q))\sum_{i=1}^{n}(1)$ = $n(\log_{256}(q))$. Either a complexity of $O(n\log_{256}(q))$.

Scalar multiplication: As soon as the n participants publish their public key, the issuer who wishes to encrypt the message must do k_i*P for each participant. Meaning that for the N participants the sender must do:

$$\sum_{i=1}^{N-1}(K_i * P) = \sum_{i=1}^{N-1}(1.86n) = 1.86n(\sum_{i=1}^{N-1} 1) = (N-1)(1.86n).$$

Addition of points: An addition has a cost of 12M + 2S ≈ 14M with M for multiplication and S for elevation to power. Similarly, the sender will do 14M for each participant. Meaning that $\sum_{i=1}^{N-1} 14M$ = 14M($\sum_{i=1}^{N-1} 1$) = (N-1)(14M) for the N participants.

5.2.2. Analysis of Decryption Complexity

The only basic operation performed in the El-Gamal decoding algorithm is the addition of points of an elliptic curve. Using the same point addition principle of the encryption algorithm, the sender will also obtain 14M. And for the N participants, it will get (N − 1)(14M).

5.3. Analysis of Complexity of the Certification Algorithm

In practice, the certification authority uses a signature algorithm to certify the messages to be sent. The complexity of the certification algorithm will thus depend on the signature algorithm used by the certification authority set up. However, it is possible to say that the signature algorithms based on the elliptic curves have a complexity of O($\sqrt{n}$).

6. Proof Of Safety Of Ecmsrtp

In this section, we start from some axioms to show that ECMSRTP guarantees confidentiality, certification, integrity, authentication, non-repudiation and protection against replay.

Axiom 1: Encryption ensures confidentiality

Axiom 2: Certification guarantees integrity, authentication, non-repudiation, protection against replay

Theorem 1: The ECMSRTP protocol ensures confidentiality.

Proof: Indeed, confidentiality is guaranteed through encryption of El-Gamal [26].

Theorem 2: The ECMSRTP protocol guarantees both integrity, protection against replay, authentication and non-repudiation.

Proof: In fact, these security services are guaranteed through certification [26].

Corollary 1: The ECMSRTP protocol guarantees all the security services given in the main objective.

Proof: Indeed, ECMSRTP guarantees confidentiality through encryption. It also guarantees other security services through certification.

In addition to these security services, the ECMSRTP also respects:

The real-time constraints of the VoIP architecture: by using elliptic curves because the cryptosystems based on the elliptic curves are less intensive in computation time.

The constraints in limited resources of the VoIP architecture: indeed, the size of the keys used by the cryptosystems based on the elliptic curves has generally small sizes.

7. PERFORMANCE STUDY OF ECMSRTP VERSUS SRTP

By comparing the execution times of El-Gamal encryption on numbers and AES, Bhavana Agrawal, Himani Agrawal et Monisha Mishra show in their work (described in [1]) that the El-Gamal encryption based on the numbers is faster than AES. Moreover, according to the Mustapha Hedabou work in [15], cryptosystems based on elliptic curves are faster than those based on numbers.

Another remark to observe here would be that:

- SRTP execution time = Secret Key Exchange Time + AES encryption time + Authentication Time of HMAC-SHA-1
- ECMSRTP execution time = Public Key Publishing Time + El-Gamal based on elliptic curves encryption time + Packet certification time.

Comparing the execution times of the two protocols thus amounts to comparing step by step the time of each algorithm used by the two protocols. In this way, and focusing on everything that has been said before, we have:

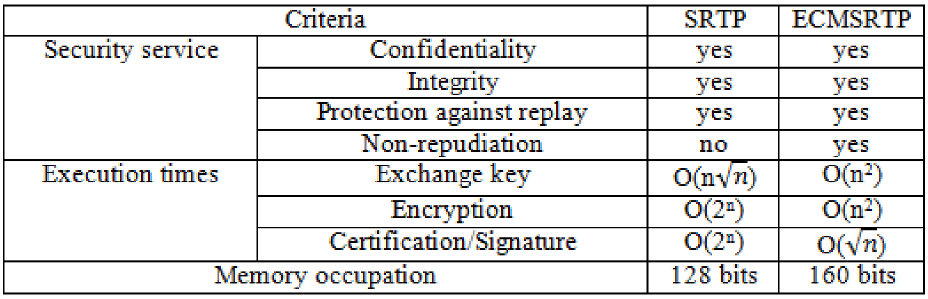
- Secret Key Exchange Time > Public Key Publishing Time (see [15])
- AES encryption time > El-Gamal based on elliptic curves encryption time (see [1])
- Authentication Time of HMAC-SHA-1 w Time of certification of the packet if we consider that the two protocols use the same signature algorithms. But in our case, in addition to the packet signature time, there is the negotiation time of the certification key, so the HMAC-SHA-1 Authentication Time is slightly higher.
- In conclusion, despite the fact that the implementation of a public key infrastructure encumbers the architecture in certification level, we can say that the new secure RTP would be faster than SRTP if the certification authority uses a good Signature algorithm.

In addition, we can also realize that key size is also favourable.

COMPARING ECMSRTP TO SRTP

This table 1 presents a complete result and comparison between ECMSRTP and SRTP.

Table 1. Comparative table



Criteria		SRTP	ECMSRTP
Security service	Confidentiality	yes	yes
	Integrity	yes	yes
	Protection against replay	yes	yes
	Non-repudiation	no	yes
Execution times	Exchange key	$O(n\sqrt{n})$	$O(n^2)$
	Encryption	$O(2^n)$	$O(n^2)$
	Certification/Signature	$O(2^n)$	$O(\sqrt{n})$
Memory occupation		128 bits	160 bits

CONCLUSION

The aim of this work was to propose a new VoIP security protocol that extends the SRTP protocol by taking into account multi-point communications and guaranteeing non-repudiation services and security in key exchanges. The proposed protocol has been named ECMSRTP for "Elliptic curve Multi-points Secure Real-time Transport Protocol". The ECMSRTP protocol has four steps for the transmission of the packet at the transmitter and also four steps upon receiving the packet. At the transmission, a packet that leaves the application layer first undergoes digitization through a codec before being encrypted by the El-Gamal cryptosystem. Thereafter, the packet header is added and then certified by a signature algorithm used by a certification authority. To do this, a key identifier and a certification label are added to the end of the package. On receipt, the origin of the packet is certified by checking the certification label. If this is correct, the headers of the packet are removed in order to decrypt the payload and transform it by a codec in order to be able to obtain the voice information. In addition to non-repudiation and security in key exchanges, ECMSRTP also guarantees confidentiality, protection against replay, integrity and authentication. Compared to SRTP, ECMSRTP is faster and more efficient because it uses elliptic curves in all security protocols, whereas SRTP uses only elliptic curves at the key exchange level.

ACKNOWLEDGMENT

We thank the Laboratory of Experimental Mathematics (LAMEX) and the Group of Research in Computer Science and its Applications (GRIA) of the University of Ngaoundere, for the multifaceted support of this work.

REFERENCES

[1] B.Agrawal, H. Agrawal, and M. Mishra. Implementation of various cryptosystem using chaos. IOSR Journal of Computer Engineering (IOSR-JCE), 13(4): 77–84, 2013.

[2] J.Arkko, E. Carrara, F. Lindholm, K. Norrman and M. Naslund. Mikey: Multimedia internet keying. https://tools. ietf.org/html/rfc3830.

[3] C.Baillet. La sécurité de la téléphonie sur ip en entreprise. Proceedings of the Fifth International Conference on Autonomous Agents, 3030(1): 78–93, 2003.

[4] C.Bassil. SVSP (Secure Voice over IP Simple Protocol) une solution pour la sécurisation de la voix sur IP. PhD thesis, Télécom ParisTech, 2005.

[5] M.Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman. The secure real-time transport protocol (srtp). https:// www.ietf.org/rfc/rfc3711.txt.

[6] M.M.N.Biasizzo. Hardware implementation of aes algorithm. Journal of Electrical Engineering, 56(9-10): 265–269, 2005.

[7] R.Bouzaida. Étude et Mise en place d'une Solution VOIP Sécurisée. PhD thesis, Université Virtuelle de Tunis, 2011.

[8] B.Campbell, J.Rosenberg, H.Schulzrinne, C.Huitema, and D.Gurle. Session initiation protocol (sip) extension for instant messaging. https://www.ietf.org/rfc/rfc 3428.txt..

[9] P.Chown. Advanced encryption standard (aes) ciphersuites for transport layer security (tls). https://www.ietf.org/rfc/rfc3268.txt.

[10] S.Demba. Courbes el liptiques, Cryptographie à clés publiques et Protocoles déchange de clés. PhD thesis, Université Cheikh Anta DIOP de Dakar, 2013.

[11] T.Dierks. The transport layer security (tls) protocol version 1.2. https://www.ietf.org/rfc/rfc5246.txt.

[12] N.Dubée. La voix sur ip (voip) : une opportunité pour la sécurité . Proceeding of SSTIC symposium, 2007.

[13] S.El Adib and N. Raissouni. AES encryption algorithm hardware implementation: Throughput and area comparison of 128, 192 and 256-bits key. International Journal of Reconfigurable and Embedded Systems (IJRES), 1(2) : 67–74, 2012.

[14] P.Gupta and V. Shmatikov. Security analysis of voice-over-ip protocols. In Computer Security Foundations Symposium, CSF07. 20th IEEE, pages 49–63. IEEE, 2007.

[15] M.Hedabou. Amélioration et sécurisation des calculs arithmétiques pour la cryptographie basée sur les courbes elliptiques. PhD thesis, INSA de Toulouse, 2006.

[16] S.Heron. Advanced encryption standard. Network Security, 2009(12): 8–12, 2009.

[17] M.J.Kakish. Authenticated and secure el-gamal cryptosystem over elliptic curves. International Journal of Research & Reviews in Applied Sciences, 10(2), 2012.

[18] U.Kretzschmar. Aes128–ac implementation for encryption and decryption. TI-White Paper, 2009.

[19] D.R.Kuhn, T.J.Walsh, and S. Fries. Security considerations for voice over ip systems. NIST special publication, pages 800–58, 2005.

[20] R.Lercier. Algorithmique des courbes elliptiques dans les corps finis. PhD thesis, Ecole Polytechnique, 1997.

[21] C.Llorens, L. Levier, D. Valois, and B. Morin. Tableaux de bord de la sécurité réseau. Editions Eyrolles, 2011.

[22] G.Madre. Application de la transformée en nombres entiers à l'étude et au développement d'un codeur de parole pour transmission sur réseaux IP. PhD thesis, Université de Bretagne Occidentale, 2004.

[23] D.NGUYEN, F. MERCERON, and C. L'OLLIVIER. La sécurisation du flux média pour la voip . http://kanja.rasta.free.fr/ssr/secufluxvoip /securisationdufluxmediavoip.pdf, consulté en avril 2015.

[24] S.F.NIST. Announcing the advanced encryption standard (aes). Federal Information Processing Standards Publication, 197, 2001.

[25] L.Ouakil and G. Pujolle. Téléphonie sur IP. Editions Eyrolles, 2007.

[26] C.Paar and J. Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.

[27] G.Pujolle. Les réseaux: Edition 2014. Editions Eyrolles, 2014.

[28] J.F.Ransome, J.R. Rittinghouse. VoIP Security. Elsevier Digital Press 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA Linacre House, Jordan Hill, Oxford OX2 8DP, UK, 2005.

[29] J.Rosenberg, H. Schulzrinne, G.Camarillo, A.Johnston, J.Peterson, R.Sparks, M. Handley, and E.Schooler.Sip: session initiation protocol.https://www.ietf.org/ rfc/rfc3261.txt.

[30] K.Seo and S. Kent. Security itecture for the internet protocol. https://tools.ietf.org /html/rfc4301. 2005.

[31] J.H.Silverman. Advanced topics in the arithmetic of elliptic curves, volume 151. Springer Science & Business Media, 1994.

[32] T.Subashri, A. Arjun, S. Ashok. Real time implementation of elliptic curve cryptography over a open source voip server, IEEE – 33044, 5th ICCCNT, 2014.

[33] A.Syed Ahson, M.Ilyas. VoIP HANDBOOK Applications, Technologies, Reliability, and Security. RC Press is an imprint of Taylor & Francis Group, an Informa business, 2009.

[34] J.T.Tate. The arithmetic of elliptic curves. Inventiones mathematicae, 23(3-4): 179–206, 1974.

AUTHORS

LAYIE Paul is born in Kaélé (Djidoma) Cameroon, He obtains his Master's Degree in the University of Ngaoundéré. Since 2015, he is the PhD student

Vivient Corneille KAMLA is born in Cameroon, on January 31, 1976. After completing Master's Degree (with thesis) Success Testimonial in Computer Science at the Yaounde I University (Cameroon) in 2003. He has done a Joint Guardianship Ph.D. thesis in computer science/Applied Mathematics at the University of Yaoundé I / University of Pau (France) in 2008. Presently, he is working as Senior Lecturer in the Department of Mathematics and Computer Science at National School of Agro-Industrial Sciences of the University of Ngaoundéré, Cameroon.