World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:2, No:6, 2008

Application of ESA in the CAVE Mode Authentication

Keonwoo Kim, Dowon Hong, and Kyoil Chung

***Abstract*—**This paper proposes the authentication method using ESA algorithm instead of using CAVE algorithm in the CDMA mobile communication systems including IS-95 and CDMA2000 1x. And, we analyze to apply ESA mechanism on behalf of CAVE mechanism without the change of message format and air interface in the existing CDMA systems. If ESA algorithm can be used as the substitution of CAVE algorithm, security strength of authentication algorithm is intensified without protocol change. An algorithm replacement proposed in this paper is not to change an authentication mechanism, but to configure input of ESA algorithm and to produce output. Therefore, our proposal can be the compatible to the existing systems.

***Keywords*—**ESA, CAVE, CDMA, authentication, mobile communication.

I. Introduction

CDMA mobile communication system starts from IS-95, as it is called 2 generation system, to cdma2000 1x, which is 3 generation system. And now, CDMA2000 1x EV-DO system for high speed packet data is served in many countries and operators [10].

In the authentication point of view, IS-95 and cdma2000 1x Rev.B and before system apply CAVE (Cellular Authentication and Voice Encryption) on their authentication algorithm. CDMA2000 1x Rev.C and later system use both ESA (Enhanced Subscriber Algorithm) and CAVE as its authentication algorithm. ESA is more enhanced authentication method than CAVE. However, most of mobile carriers are providing authentication service using CAVE because CDMA2000 Rev.C is not yet commercialized.

Authentication mechanism by CAVE algorithm [1,4,6,7] uses a symmetry key cryptosystem with Challenge-Response protocol between a base station and a mobile station. This mechanism has several disadvantages in comparison with mechanism by ESA. Only one-way authentication is provided, that is to be, a base station authenticates a subscriber. And, subscriber's anonymity is not offered in the process of authentication. Moreover, CAVE algorithm is a bit weak to some cryptographic attack [12,13] and this is an already known fact.

Authors are with Electronics and Telecommunications Research Institute, 161 Gajeong-Dong Yuseong-Gu, Daejeon, 305-350, Korea (phone: +82-42-860-1521, fax: +82-42-860-5410, e-mail : wootopian@etri.re.kr).

Authentication mechanism using ESA algorithm [2,3,5] uses AKA(Authentication and Key Agreement) to enhance security strength and to provide mutual authentication between a base station and a mobile terminal. AKA with 128-bit key adopts the SHA1 [8,11] hash algorithm as a core function to generate an authentication value and message encryption keys. ESA mechanism has more advantages than CAVE mechanism in the view of various security service and cryptographic algorithm strength. So, we need to analyze whether CAVE can be replaced with ESA in the existing CDMA mobile communication systems.

This paper analyzes to apply ESA instead of CAVE in the authentication process of CDMA mobile communication systems. In our analysis, other protocol or system component except for authentication protocol is not changed. If ESA can be applied in the existing systems, a few demerits of CAVE algorithm can be improved. Chapter 2 of the paper simply describes the authentication system by CAVE and ESA each. In chapter 3, we propose that ESA algorithm can be applied to the CDMA2000 1x Rev.B and before systems instead of CAVE algorithm. And, we show how to generate shared secret data, authentication signature value, voice privacy code, and, signaling message encryption key using ESA algorithm. Chapter 4 is about the application of ESA mechanism as well as ESA algorithm to the established CDMA systems. With message format, air interface, and call flow used by CDMA2000 1x Rev.B and before systems, the authentication mechanism just cannot be replaced by ESA instead of CAVE. Finally, we conclude in chapter 5.

The application of ESA algorithm to the existing CDMA mobile communication systems, which is presented at chapter 3, is not to change the authentication mechanism itself. It is about how to construct input parameter and how to apply authentication algorithm. That is, there are no another changes except for the replacement of authentication algorithm and the construction method of input variable. Therefore, our proposal is compatible with the existing CDMA systems.

II. Authentication by CAVE and ESA

In this chapter, we simply describe the authentication mechanism using CAVE algorithm and ESA algorithm each.

A. CAVE Mode

In the authentication system using CAVE algorithm, a subscriber authentication between a mobile station and a base station is done by confirming the knowledge about a shared

secret data SSD and a subscriber's secret key A-key. In other words, the authentication signature value Auth_Signature is made by using SSD and other information as the input of CAVE algorithm. Authentication process between a mobile terminal and a base station is accomplished if Auth_Signature computed in a mobile terminal and an authentication center coincides with each other. 128-bit length SSD is generated from A-key. Leftmost significant 64 bits of SSD, SSD_A, is used for authentication and the rest 64 bits of SSD, SSD_B, for voice privacy and signaling message encryption. PLCM(Public Long Code Mask) for voice privacy and CMEAKEY for signaling message encryption are made using SSD_B and CAVE algorithm[1,7].

Authentication process can be classified into global challenge procedure and authentication auxiliary procedure. Global challenge is a process that a base station authenticates a mobile terminal when a mobile terminal registers or originates or terminates to connect call with a base station. Authentication auxiliary procedure includes SSD update and unique challenge process according to operator's authentication policy if global challenge procedure fails. The same algorithm is used in the process of authentication for registration, origination, termination, and, SSD update.

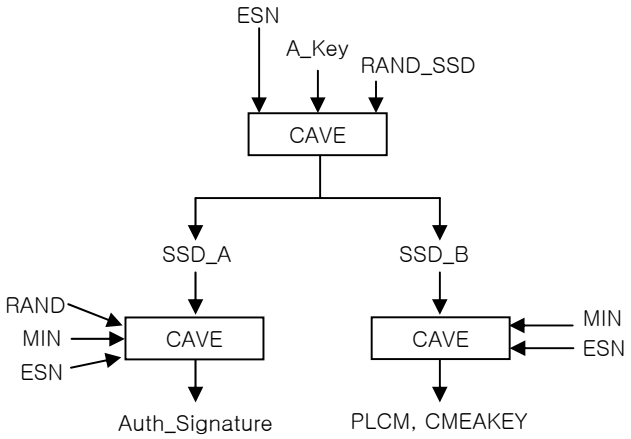

Fig. 1 Generation of authentication value and keys by CAVE

In the mean time, 3GPP2 recommends using ESA algorithm for mutual authentication because vulnerabilities of CAVE algorithm itself were already reported [12,13]. So, ESA will be widely more used than CAVE in the afterward authentication algorithm. ESA can adopt block cipher as well as hash function as its core function. Definite specifications about CAVE algorithm and method to make Auth_Signature, PLCM, and, CMEAKEY refer to 3GPP2 Common Cryptographic Algorithms [1] and Common Security Algorithms [3].

B. ESA Mode

CMDA2000 1x Rev.C and later system has not only CAVE mode authentication mechanism but also ESA mode authentication mechanism. ESA mechanism provides mutual authentication between a base station and a mobile terminal with increased key size, and offers message integrity. It uses AKA as authentication and key generation. ESA mechanism is similar to 3GPP AKA[9] and it selects SHA1 as a core function of its algorithm.

ESA mechanism between a mobile station and a base station is as follows.

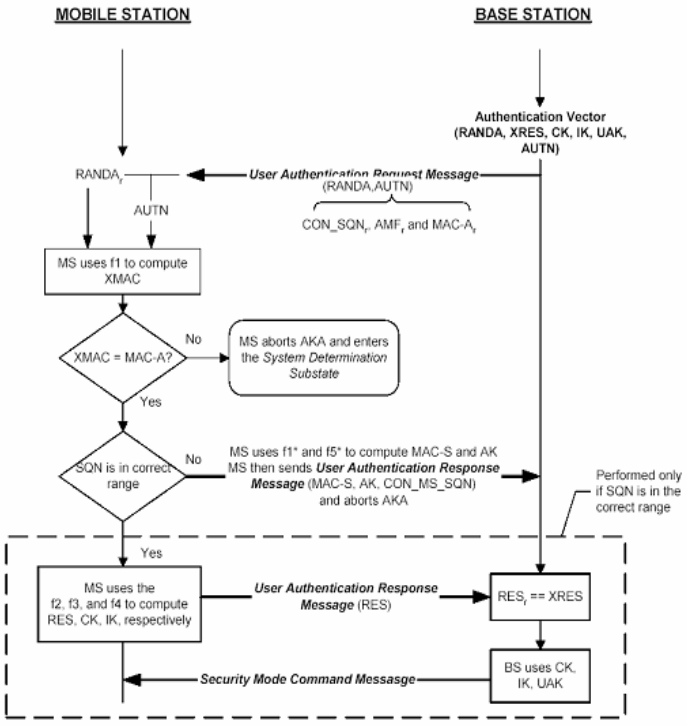

Fig. 2 Authentication and key agreement mechanism by ESA

Input and output parameter, used algorithm, and message transfer times of ESA mechanism are different from them of CAVE mechanism. If the algorithm used in above mechanism is just replaced with CAVE algorithm, the size of input and output parameter and the message format are not in accordance with them of CAVE mechanism. That is, it is a big problem to use CAVE algorithm in ESA mechanism. However, on the contrary, it is not a big problem to use ESA algorithm in CAVE mechanism.

ESA mechanism and algorithm depend on 3GPP2 Enhanced Cryptographic Algorithms [2] and Common Security Algorithms [3] specification.

III. The Application of ESA Algorithm to the Existing CDMA Systems

Chapter 3 proposes three methods to generate a shared secret data, an authentication signature value, and a private long code mask and a signaling message encryption key using ESA algorithm. These methods are done in the authentication mode by CAVE mechanism. Our proposal is not to apply ESA mechanism but just to replace CAVE algorithm with ESA algorithm to the existing systems. Also, we propose to configure parameters of ESA algorithm using input and output used in CAVE mechanism.

A. Generation of SSD from A_Key

In A section, we explain how to make a shared secret data for authentication, SSD_A, and a shared secret data for encryption, SSD_B, using ESA algorithm and a subscriber's secret key A_key. As a preceding work to do this, we propose to construct inputs of ESA algorithm using ESN and RANDSSD, where ESN is an electronic serial number uniquely allocated at a mobile terminal and RANDSSD is random information transmitted from a base station to a mobile terminal. Parameters and algorithm used in this process are as following table.

TABLE I
CAVE MODE PARAMETERS USED IN ESA ALGORITHM

1	Input	A_Key(64 bits)
		ESN (32 bits)
		RANDSSD (56 bits)
2	Output	SSD_A (64 bits)
		SSD_B (64 bits)
3	Algorithm	ESA including SHA1
4	Mechanism	CAVE mode authentication

- Construction of ESA input to produce SSD

Fig. 3 shows to construct inputs of ESA algorithm to make SSD. 512-bit length Input #1 is comprised of 16 words and size of each word is 32 bits. First word is the value XORed Index into standard SHA1 constant value. Index with 32-bit length can be increased by 1 according to the method to make SSD and its initial value is zero. SHA1 constant value can be any value with 32-bit length. In this paper, we choose 0x5C5C5C5C suggested in the FIPS 180-2[8] as a constant value. Second word is the value XORed ESN into SHA1 constant value. And, third and fourth words are each XORed first and second word of RANDSSD into SHA1 constant value. About the 64-bit RANDSSD, a mobile terminal receives 56-bit random number from a base station and fills up lower 8 bits with 0. Words from fifth to sixteenth are each filled with the SHA1 constant value.

Next is to construct 160-bit Input #2. Input #2 cosists of 5 words. First and second words are each XORed A_Key into first and second words of standard SHA1 Initial Vector, where Initial Vector with 160-bit length is comprised of 5 words and represented in FIPS 180-2. Words from third to fifth are filled with words from third to fifth of Initial Vector.

• Construction of Input #1

W[0]	W[1]	W[2]	W[3]	W[4]	.....	W[15]
Index xor Constant	ESN xor Constant	RANDSSD[0] xor Constant	RANDSSD[1] xor Constant	Cons tant	.....	Cons tant

• Construction of Input #2

W[0]	W[1]	W[2]	W[3]	W[4]
A_Key[0] xor IV[0]	A_Key[1] xor IV [1]	IV[2]	IV[3]	IV[4]

Fig. 3 Construction of ESA input to make SSD

- Generation of SSD_A and SSD_B

Now, using Input #1 and Input #2, the process to make SSD_A and SSD_B is as follows. We depict it in Fig. 4.

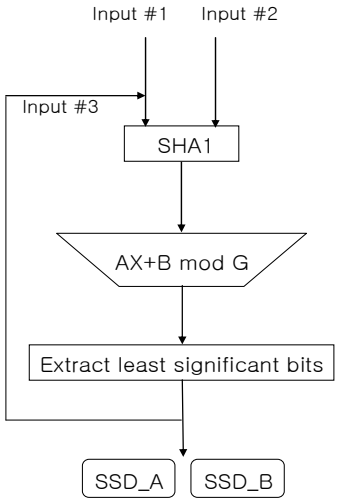

Fig. 4 Generation of SSD_A and SSD_B by ESA algorithm

- Load Input #1 and Input #2 into SHA1. Input #3, that is Index, is initially 0 and becomes a part of Input #1.
- Run SHA1 to produce 160-bit output. And then, polynomial $AX + B \bmod G$ is computed, where A and B are predetermined 160-bit random numbers and treated as polynomials with binary coefficients in the variable T. X is a 160-bits output from SHA1 operation and treated as a polynomials with binary coefficients in the variable T. And, G is an irreducible polynomial represented by $G = T^{160} + T^5 + T^3 + T^2 + 1$.
- 160-bit output value through the polynomial computation is used as one of following two methods.
  First, extract lower 128 bits of 160 bits. Least significant 64 bits of 128 bits is a shared secret data for authentication, SSD_A, and the remainder 64-bit value is set up as a shared secret data for encryption, SSD_B. Input #3 is not increased in this method. And then, all procedure is ended. Second, extract lower 64 bits of 160 bits. This value is for SSD_A. And then, Index is increased by 1. Input #1 with the updated Index is again constructed. After the same step from entering input parameters is repeated, lower 64 bits of $AX + B \bmod G$ computation output is set up as SSD_B. In this method, Input #3 is increased just one time.

B. Generation of Auth_Signature from SSD_A

B section is about the method to make an authentication signature value Auth_Signature using ESA algorithm. And, we propose to construct inputs of ESA algorithm using ESN, MIN, RAND, and SSD_A.

- Construction of ESA input to produce Auth_Signature

To configure inputs of ESA algorithm in Fig. 5 is almost similar to the method in Fig. 3 besides some parameters are changed as follows.

Referring to the construction of Input #1 of Fig. 3, first word of Input #3 is filled with SHA1 constant value which is the same value used in the Fig. 3. Second word is the value XORed ESN into SHA1 constant value. In third word, MIN is applied instead of RANDSSD on the Fig. 3, where 32-bit MIN consists of 24-bit mobile identity number to distinguish a mobile terminal and lower 8 bits with 0. Fourth word is the value XORed RAND into SHA1 constant value, where 32-bit RAND is one of fields contained in Access Parameter Message transmitted from a base station to a mobile terminal.

The construction of Input #4 is identical with the construction of Input #2 besides A_key is replaced with SSD_A.

• Construction of Input #3

W[0]	W[1]	W[2]	W[3]	W[4]	.....	W[15]
Constant	ESN xor Constant	MIN xor Constant	RAND xor Constant	Cons tant	.....	Cons tant

• Construction of Input #4

W[0]	W[1]	W[2]	W[3]	W[4]
SSD_A[0] xor IV[0]	SSD_A[1] xor IV [1]	IV[2]	IV[3]	IV[4]

Fig. 5 Construction of ESA input to make Auth_Signature

- Generation of Auth_Signature

Process to make Auth_Signature is shown in figure 6 using Input #3 and Input #4.

Most steps are similar to Fig. 4, however, only least significant 18 bits of final 160 bits is extracted as Auth_Signature and Index is not used in this process.

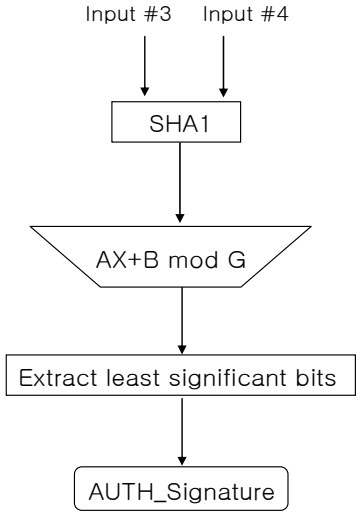

Fig. 6 Generation of Auth_Signature by ESA algorithm

C. Generation of PLCM and CMEAKEY from SSD_B

This section is about a procedure to make voice privacy code, PLCM (Public Long Code Mask), and signaling message encryption key, CMEAKEY, using ESA algorithm. Also, we simply explain a method to configure inputs of ESA algorithm using ESN, MIN, and SSD_B.

Configuration of ESA algorithm inputs is almost similar to the Fig. 5, besides first word of Input #3 is the value XORed Index into SHA1 constant value, fourth word is SHA1 constant, and SSD_A in Input #4 is replaced with SSD_B.

Similarly to Fig. 4, 40-bit PLCM and 64-bit CMEAKEY are produced using above new inputs.

ESA algorithm in chapter 3 adopts SHA1 as its core function. But, we can apply hash functions such as HAS160 and RMD160 if block and key length is same to that of SHA1. Even though the length of block and key is different, other hash function can be applied according to the method to extract some bits of algorithm output. Moreover, we can use block cipher such as AES and ARIA by controlling how to extract specific bits and how to configure inputs of algorithm.

IV. The Application of ESA Mechanism to the Existing CDMA Systems

In this chapter, we analyze to apply ESA mechanism as well as ESA algorithm to the IS-95 and CDMA2000 1x systems.

Mobile communication systems have various authentication version and protocol on the air interface. In other words, authentication procedure, message format, and air protocol in IS-95 system by CAVE mode is different from them in CDMA2000 1x Rev.C by ESA mode. Therefore, we can know that authentication mechanism by CAVE should not be replaced with mechanism by ESA if IS-95 system is not change message format and air protocol and etc.

Information for CAVE mode authentication is recorded in fields contained in Parameter access message, Registration message, Origination message, and Page response message. For example, AUTHR field with 18-bit size used in the authentication mechanism by CAVE can not contain ESA authentication value with 64-bit length. To utilize ESA information in the authentication mechanism by CAVE, the size of AUTHR field should be 64 bits. This means message format of IS-95 is changed. As well, IS-95 needs to change air interface and call flow as well as message format to replace CAVE mechanism with ESA mechanism.

It is responsible for mobile communication operators to decide whether they accept those changes or not.

V. Conclusion

Authentication using ESA algorithm in CDMA systems such as IS-95 and CDMA2000 1x has some benefits.

Firstly, our proposed method is compatible to the existing CDMA systems because only algorithm, not mechanism, is substituted into ESA, and input parameters remain the existing systems.

Secondly, various hash function can be selected. In this paper, we made a use of SHA1 with 512-bit length input block and 160-bit output. Moreover, other hash function and block cipher can be applied as a core function of ESA algorithm.

Thirdly, we can vary method to extract final output according to Index increase and repetition times of algorithm.

In conclusion, we can know that our proposal is adequate for the existing mobile communication systems. On the other hand, it is determined that the change of message format and air interface should be changed to apply ESA mechanism in the existing CDMA systems.

REFERENCES

[1] 3GPP2 S.S0053, "Common Cryptographic Algorithms", 2002.
[2] 3GPP2 S.S0055, "Enhanced Cryptographic Algorithms", 2005.
[3] 3GPP2 S.S0078, "Common Security Algorithms", 2005.
[4] 3GPP2 S.S0054, "Interface Specification for Common Cryptographic Algorithms", 2002.
[5] 3GPP2 S.R0032, "ESA and ESP", 2000.
[6] 3GPP2 N.S0014, "Authentication Enhancements", 2000.
[7] TIA-95-B, "Mobile Station-Base Station Compatibility Standard for Wideband Spectrum Cellular System", 2004.
[8] FIPS 180-2, "Secure Hash Standard", NIST, 2002.
[9] 3GPP TS 33.102, "Security Architecture", 2004
[10] Vijay K. Grag, "IS-95 CDMA and CDMA2000", Prentice Hall, 2000
[11] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Chapter 9: Hash Functions and Data Integrity", HandBook of Applied Cryptography, CRC Press, pp. 321-383, 1997.
[12] W. Millan and P. Gauravaram, "cryptanalysis of the cellular authentication and voice encryption algorithm," IEICE Electronics Express, Vol. 1, No. 15, pp.453-459, 2004..
[13] P. Gauravaram and W. Millan, "Improved Attack on the Cellular Authentication and Voice Encryption Algorithm," Proc. International workshop on Cryptographic Algorithms and their Uses, pp. 1-13, 2004.