A New Bio-Crypto System Approach to Enhance Security of 4G Mobile Networks

Saeed Ashry
ITIDA
Cairo, Egypt
sashry@itida.gov.eg

Abdulatif Elkouny
Ain Shames University
Cairo, Egypt
aelkouny@gmail.com

Hesham Elbadawy
NTI
Cairo, Egypt
heshamelbadawy@ieee.org

Salwa Elramly
Ain Shames University
Cairo, Egypt
sramlye@netscape.net

Ahmed ElSherbini
ITU
Geneva, Switzerland
sherbini@mcit.gov.eg

Abstract— **This research paper examines the vulnerable security elements that MAC management messages in WiMAX initial network entry faces. The paper proposes an innovative hybrid approach to resolve such vulnerability problem and establish secret communication channels via insecure domains. The proposed protocol is based on Bio-crypto systems and to improve current security level of authentication and Key Exchange between the Subscriber Station SS and the Base Station BS. AES-BDK system is defined as the integration of Advanced Encryption Standard and Biometric Digital Key. Within this integration, AES is used for the encryption process for initial ranging Request/Response messages RNG_REQ/RSP, while BDK generates the secret key.**

Keywords- initial ranging; MAC Management Messages; key exchange; key genertion; bio-crypto systems.

I. INTRODUCTION

Computer security experienced a significant and grew rapidly over the past few years. Worldwide Interoperability for Microwave Access (WiMAX) based on IEEE 802.16e-2005 for Mobile WiMAX [1]. Bolsters a large number of enhanced security features compared to the fixed IEEE 802.16-2004 [2]. based on security schemes. The initial network entry is the most critical process in WiMAX networks as it is the foremost step to establish network connection while carrying multiple parameters such as performance factors and security context between the Base Station (BS) and the Subscriber Station (SS) determined in the middle of this process. However, security schemes are utilized and applied only to normal data traffic after the initial network entry process, but not to control messages during the initial network entry. BS and SS communication in the initial network entry is susceptible to forgery. As a result, there can be various security vulnerabilities especially unauthenticated messages and unencrypted management communication that uncover important management data. As a consequence, no common key to generate message digest is the source of difficulty to authenticate these types of messages. According to literature survey, little pertinent papers discuss the security issues of messages in this process whilst most of these messages are very short [3]. Thus, it is an area worthy of interest. Due to this fact, a tradeoff between security and effectiveness is being considered in this paper through a new approach of enhancing MAC management message security during network entry initialization. The proposed scheme is applicable to Point to – Multi- Point (PMP), while it could be scalable to multiple zones depending on the security channels between different Trusted Third Parties (TTP).

The paper proposes a hybrid protocol relying on Bio-crypto system. The biometric-crypto system is a combination of biometrics and cryptography and is considered a very promising technique [3]. Bio-cryptography is an emerging technology that inherits the advantages of both and provides strong means of protection against attacks targeting MAC Management messages: Ranging Request/Response (RNG_REQ/RSP) messages.

The objective of biometric data is to provide privacy, cryptographically- secure authentication of human users, and non-repudiation by using biometric template of fingerprint. Fingerprint minutiae matrix is produced to generate the Biometric Digital Key (BDK). To guarantee the security of the key, the proposed protocol adds a new message to the standard control message. BS uses stored biometric templates in the Trusted Third Party (TTP) to fulfill the authentication key exchange protocol banking on biometric system to authenticate user messages. The produced key is used in Advanced Encryption Standard (AES) to encrypt user messages. Bio-Crypto system establishes a secure channel between SS and BS and vice versa.

The remaining of this paper is structured along these lines: Section II describes the initialization of WiMAX network in accordance with amendment IEEE 802.16e, while Section III shows cases of the security vulnerabilities of MAC management messages. Section IV discusses the previous work. Section V introduces the projected approach, while Section VI shows the experimental results. Finally, Section VII concludes this paper.

ISBN: 978-1-61208-284-4

II. Network Entry Initialization

When a SS initializes some synchronization, parameter adjustments take place to establish a robust and well-fitted link between SS and BS. The performed initial tasks, when a SS turns on in the network, include, but not limited to, channel acquirement, PHY (Physical Layer) synchronization, channel descriptors identification and interpretation. After PHY synchronization, MAC (Medium Access Control Layer) can detect and identify MAC management messages such as DCD (Downlink Channel Descriptors), UCD (Uplink Channel Descriptors), DL-MAP (Downlink Map) and UL-MAP (Uplink Map). MAC management messages determine the contention slots to initial ranging on the UL sub-frame. These messages are transmitted by BS on the first available DL burst. Different SS and BS messages are exchanged to stabilize signal power, frequency and time offset [4].

The initial ranging adjusts transmission until an adequate profile is achieved for the link, including synchronization issues. After network entry, when SS is already transmitting data, takes place, the periodic ranging, which guarantees that transmission, will react to channel changes as well as maintain link quality. Periodic ranging exchanges MAC-PDU (Packet Data Unit) messages between BS and SS, while initial ranging uses both contention slots on the UL sub-frame and MAC-PDU messages. The SS will transmit a ranging request message (RNG-REQ) in one of the initial ranging slots. If collision occurs, the SS uses a truncated exponential back-off. This message is described in [1]. The BS could receive or not the RNG-REQ. If the SS doesn't receive an answer from BS, it retransmits the RNG-REQ message after a timeout. If the BS successfully received the RNG-REQ, it would return a RNGRSP message using the initial ranging CID (Connection Identification) [5]. A ranging response message (RNG-RSP) is sent in one of the available DL bursts containing the CIDs of the Basic and Primary connections to this SS. The RNG-RSP could contain power, frequency and time corrections to the SS. This message is described in [1].

III. Security Vulnerabilities of MAC Management Messages

With a reference to IEEE 802.16-e amendment, the security schemes are only applied to standard data traffic after the initial network entry process not to control messages during the initial network entry. The initial network entry is considered the main process in Mobile WiMAX network. It is the first gateway to set up a connection to Mobile WiMAX. Consequently, numerous physical parameters, factors of performance, and security contexts between SS and BS are set during the process. In Figure 1 the initial network entry in normal process is illustrated.

A. RNG_REQ/RSP vulnerabilities

This section studies vulnerabilities contained by RNG_REQ/RSP in the initial network process. The ranging Request (RNG_REQ) message is transmitted by an SS requesting and seeking a network join. The message integrates the SS's existence meanwhile acts as a request for transmission timing, power, frequency and burst profile information. The BS responds to the SS request using a Ranging Response (RNG_RSP) message. This message is composed of important information, such as ranging status, time adjusts information and power adjusts information. Nonetheless, the RNG_RSP message is neither encrypted nor authenticated, it holds no definite status. An attacker would manipulate such a leak and execute an attack using DoS because SS's action could be conducted by any validly formatted RNG/RSP that addresses to it [6][7].

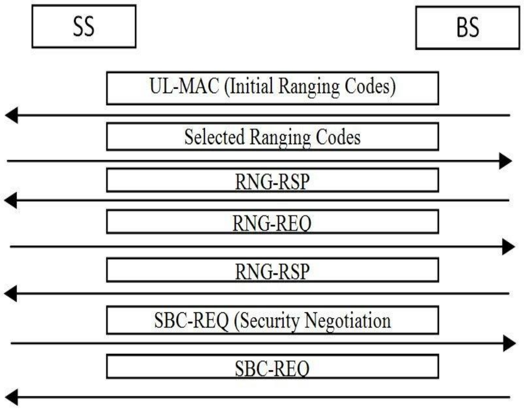

Figure 1. Normal Initial Network Entry Procedure.

B. Rouge BS

Other distinguished attacks on wireless networks include man-in-the-middle (MITM) attack, namely, Rouge BS. The attacker could intercept messages during the process of communication establishment or a public key exchange. The attacker then retransmits them, counterfeiting the contained information in the messages, so that the two original parties still seem to be contacting with each other [8].

IV. PREVIOUS SOLUTIONS

This work is inspired from a number of preceding works concerning key exchange during initial network entry. Some messages in the initial network entry inject some vulnerability such as RNG-REQ/RSP. T. Shon 'et al.' [9]. Introduces a solution to secure these messages counting on the Diffie-Hellman (DH) key agreement. De facto, it can secure the message during initial network entry process and boost the security grade; however it is still liable to man-in-the-middle attack. T. Han 'et al.' [10]. proposed an alternation to DH key agreement protocol to fit into mobile WiMAX relying on the presumption that every MS possesses its own International Subscriber Station Identity *(ISSI)* from which the MS could generate its Temporary *ISSI*

(TSSI) and the authors postulate that the legitimate BS has the hash value H *(TSSI).* Then they launch their protocol which is based on five steps to avert the former attack. T. Shon 'et al.' [10]. has a concern on the previous solution, as it could cause additional overhead when distributing initial DH random number. The perspective of this paper contrives that this solution does not clarify the source of private and public key *(p&q)* calculations, in addition to time limitation for p&q calculation. Furthermore, they have to disseminate TSSI to the entire neighbor BS. Hence, there is no security for *ISSI*. M. Rahman 'et al.' [11]. utilizes DH key agreement so as to secure the initial network entry and encrypt the initial management communication. Their adjustment on the DH is carried out to dismiss man-in-the-middle breach by employing cryptographic sealing function. T. Shon 'et al.' [9]. are debating over this approach explicating it as obscure and providing no clear vision of how the random number is generated and distributed to others to use DH scheme. Consequently, those authors suggested a modernistic altered DH scheme [11]. The schema can be performed using hash authentication as well as one of the ranging codes as a prime number seed. Furthermore, it uses hash authentication when SS singles out one of ranging codes RCi which consists of A1 and A2, then transmits only part of RCi (A1 *or A2)* and hash value of *RCi*. When BS receives a segment of *RCi (A1)* and the hashed value *H (RCi),* BS obtains *A2* from ranging code pool using *A1,* then authenticates MS throughout received hash value verification [12]. Therefore, they could produce a prime number "p" from the chosen ranging code. In a subsequent phase, SS generates the other global variables "g" and public/private key pair then sends them to BS. If the received key and variables are verified, BS sends its public key to MS. Thence, BS and SS commence sharing DH global variables and public key with each other at the hand of initial network entry ranging process. It is unclear whether the protocol steps could counteract the bogus BS from sending *RCi* or not.

V. Proposed Protocol

This paper suggests an approach of securing the RNG_REQ/RSP messages. The model is composed of SS, BS, and TTP server to manage the authentication and key exchange between SS and BS. The protocol assumes that the channel between BS and Trusted Third Party (TTP) is secured, as illustrated in Figure 2. The protocol uses Advanced Encryption Standard (AES) as the most popular algorithm used in symmetric key cryptography with a combination of Biometric data (e.g fingerprint, iris, etc.) to generate the BDK.

A. Setting up a SS User Device

The SS user firstly captures its biometric data, then registers itself to the TTP, and asks the system make its biometric template (i.e., fingerprint minutiae matrix), which will be stored on both SS device and TTP server.

B. Biometric Template Protection

The TTP saves biometric template of SS's secured. Biometric data is stored on protected storage. The confidentiality of biometric template can be assured by implementing permutation module using obscure scheme. Firstly, TTP generates fake minutiae set and inserts it to the user's biometric template. Secondly, for hiding private key, polynomial for real minutiae set and polynomial for fake minutiae set are established. Finally, the protected biometric template is made by combining these results. It consists of minutiae's (location, angle, result) value set [13].

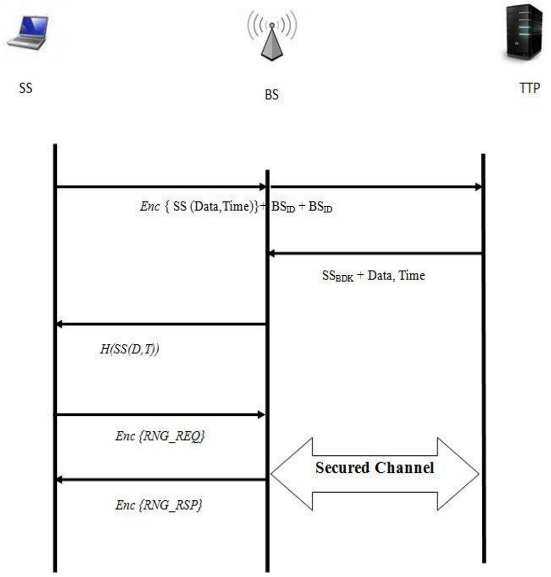

Figure 2. Proposed secure initial network entry using AES-BDK

C. Biometric Key Generation

The protocol proposed Biometric Digital Key with uniqueness, randomness property that cannot be falsified. The SS holds a stored biometric template on its device [13][14]. (i.e., fingerprint minutiae). The fingerprint minutiae matrix acted as the seed data in Secure Hash Algorithm (SHA). The seed data length is selected considering the length of key lengths of 128 bits, 256 bits, and 512 bits. Then SS starts to generate the initial BDK. The initial BDK is formed based on minutiae points. For extracting minutia points from fingerprint preprocessing phases should done, Image enhancement, Binarize, ridge ending and ridge bifurcation. Figure 3 clarifies key generation from minutiae. Further to strengthen the security of the key and to randomize the BDK between SS and BS, the seed data will be based on Data and Time.

D. Encryption and Decryption phases

Advanced Encryption Standard (AES) is used in this protocol as a block cipher which is the most popular algorithm used in symmetric key cryptography; see Figure 4 that clarifies encryption and decryption process using BDK. As AES supports key sizes of 128 bits, 256 bits, and recently

512 bits. Security increases with the larger key sizes as well as the number of rounds (10, 12, and 14, respectively). Therefore, the complexity of AES encryption and decryption also grows. The proposed protocol is evaluated with the different key lengths.

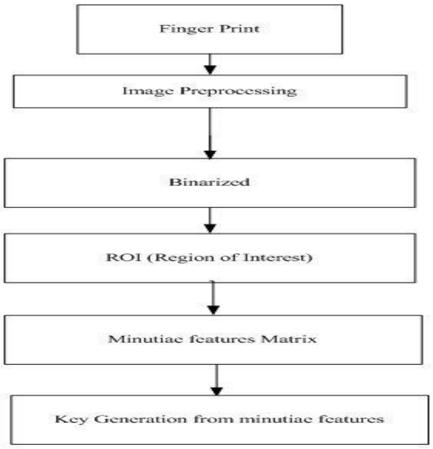

Figure 3. Key Generation from Minutiea Feature.

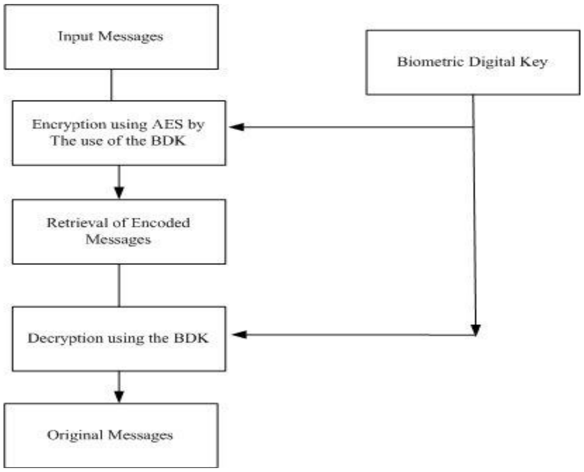

Figure 4. Encrypt and Decrypt using BDK.

E. Protocol Steps

The following steps describe the proposed protocol:

- SS starts sending a new message including Data and Time encrypted by the initial BDK to the BS Enc {Data, Time} + BS_{ID} + SS_{ID}.
- BS receives the Enc message, and then delivers it to TTP.
- TTP starts searching on its Database by SS_{ID}, if TTP verifies that it is a real SS, and then the TTP retrieves the stored biometric template of SS starting to generate the SS initial BDK, and Dec the message.
- TTP pass the SS initial BDK, the Data and Time to the BS.
- BS sends the hash value of SS (Data and Time) $H (D, T)$, as a challenge message to the SS.
- SS starts sending the Enc {RNG_REQ} to the BS using the new BDK.
- SS starts sending the Enc {RNG_REQ} to the BS using the new BDK.
- BS starts Dec (RNG_REQ).
- BS sends the Enc (RNG_RSP) to the SS.
- SS starts Dec (RNG_RSP).

VI. EXPERIMENTAL RESULTS

A prototype implementation of MAC frame structure has been developed. PC specifications are CPU Intel Core 2 Duo CPU 2GHZ, RAM 4GB, O/S Windows 7 SP2.

The physical layer of model system uses Orthogonal Frequency Division Multiplex (OFDM) with basic OFDM parameters and with 20 MHz bandwidth TDD mode while the frame length is set to 10 ms, modulation code QPSK [4]. The scenario frame is illustrated in Figure 5. The illustrated protocol, in the previous section, deployed MATLAB script for AES encryption, decryption phases, and key generation phase conjointly with Secure Hash Algorithm (SHA), to produce various key lengths.

CASIA fingerprint database version 5[16]. is used to produce biometric data. To extract biometric templates, 1000 fingerprint samples were taken from this database. The average total time of reading fingerprint image and enhancement process is 3.7 sec. The average time process of generating the BDK is 0.0003808 sec. The consuming time of encryption and decryption processes for the proposed protocol is presented in Table 1 in msec.

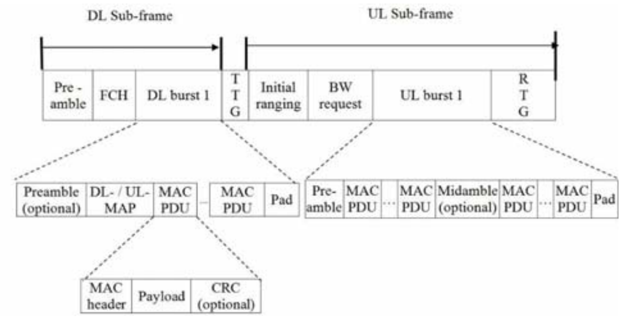

Figure 5. Example of MAC frame structure scenario.

This performance comparison is made in terms of time consumed for encryption and decryption of AES-128 bits, AES-256 bits and AES-512 bits. The model employed measures time at the start of encryption process and its end time while the same process is repeated for decryption. The evaluation results show that due to the increase in the key length used in AES-512 bits, and consequently, the number of rounds for both encryption and decryption boosts.

But, the encryption and decryption procedures become more complex thereby degrading the speed of the 512 bit AES algorithm. Figures 6 and 7 show the consumed time of Encrypted/Decrypted REG_REQ and RNG_RSP messages using various key lengths, respectively.

TABLE I. ENCRYPTION/DECRYPTION TIME

	Enc (RNG_REQ)	**Dec (RNG_REQ)**	**Enc (RNG_RSP)**	**Dec (RNG_RSP)**
AES-128	3.23	3.5575	5.1414	6.491
AES-256	3.4005	3.8486	5.3823	6.8198
AES-512	4.05	4.4035	5.9293	7.3486

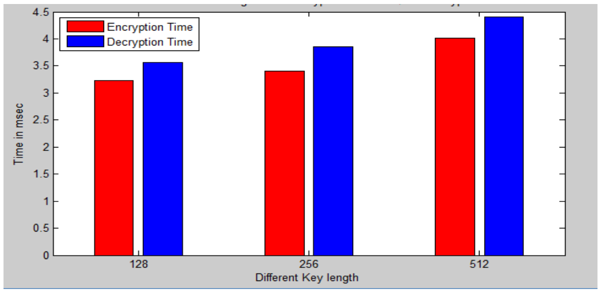

Figure 6. Time of Encrypt/Decrypt RNG_REQ with different key lengths.

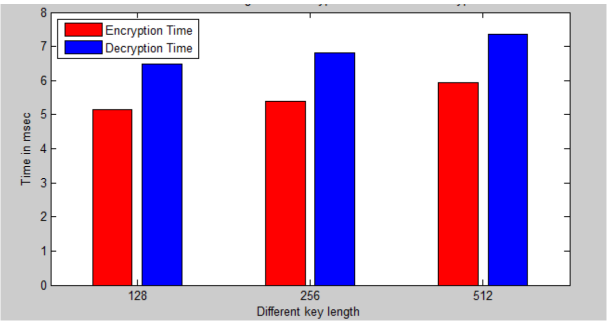

Figure 7. Time of Encrypt/Decrypt RNG_RSP with different key lengths.

VIII. CONCLUSION AND FUTURE WORK

The contributions of this paper are meant to enhance a security of PMP initial network entry. This paper proposed a new authentication key exchange protocol that enables SS and BS exchange parameters securely. The generated BDK from fingerprint minutiae is utilized to encipher data messages thereafter more securely derived and produced. Consequently, this key is not liable to be cracked easily [17]. The approach compared AES-256 bits and AES-512 bits in terms of time taken for encryption and decryption. Thus there is a tradeoff between speed and security. The proposed approach substantially considers the items of privacy, authentication and non-repudiation, to reduce the probability of some threats such as eavesdropping, MITM attacks.

In the future, further efforts will be focused to find the solution for Mesh network to guarantee the security of the network entry. As the PKI authentication uses ECC and is an area worth of more research and analysis, a Mesh Biometric Certificate X.509 V.3 with ECC is an important component of the network security system.

ACKNOWLEDGMENT

I would like to express my gratitude to Yasser Hashem for the useful comments, remarks and engagement through the learning process of this research paper. Also, I like to thank AbdelRahman El-Mawawi for his great efforts in proof reading and reviewing this research.

REFERENCES

[1] IEEE 802.16e-2005, ‘IEEE standard for local and Metropolitan Area Networks-part 16; Air Interface for Fixed Broadband Wireless Access Systems”, IEEE press, 2005.

[2] IEEE 802.16-2004, ‘IEEE standard for local and Metropolitan Area Networks-part 16; Air Interface for Fixed Broadband Wireless Access Systems” , IEEE press, 2004.

[3] P. Stavroulakis and M. Stamp, Handbook of Information and Communication Security., Ch.7, BioCryptography, pp. 129-157, Springer,2010.

[4] C. Hoymann. “Analysis and performance evaluation of the OFDM-based metropolitan area network IEEE 802.16”, pp.. 341-363, June 2005.

[5] H. Hernadnes, F. Quinelato, and A. Alberti. “A Simplified Simulation Model for Initial Ranging in IEEE 802.16d WirelessMAN-OFDM”, [Online] Available: http://www.iiis.org/CDs2010/CD2010SCI/CCCT_2010/Abstract.asp?myurl=TB807EH.pdf /06.2013

[6] T.Shon and W.Choi, “An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions”, Lecture Notes in Computer Science, vol. 4658, Augest 2007, pp. 88-97.

[7] T. Nguyen. “A Survey of WiMAX Security Threats”, Aug. 2009. [Online] Available: http://www1.cse.wustl.edu/~jain/cse57109/ftp/wimax2.pdf /05.2013.

[8] P. Rengaraju, C. Lung, Yi Qu, and A. Srinivasan, ”Analysis on Mobile WiMAX Security”, IEEE TIC-STH, Information Assurance in Security and Privacy, Toronto, Ontario: Canada, Sept. 2009, pp. 27-29.

[9] T.Han, N.Zhang, K.Liu, B.Tang and Y.Liu, “Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions”, Proc. of 5th int. Conf. on Mobile Ad Hoc and Sensor Syst., Germany, Aug. 2008, pp.828-833.

[10] A. Deininger, S. Kiyomoto, J. Kurihara, and T. Tanaka.“ Security Vulnerabilities and Solutions in Mobile WiMAX”, International Journal of Computer Science and Network Security (IJCSNS), Vol. 7, No. 11, Novemeber, 2007.

[11] M. Rahman, Mir Md. S. Kowsar, "WiMAX Security Analysis and Enhancement", proc. of 12th Int. Conf. on Comput. and Inform. Tech (ICCIT), Dhaka, Dec.2009, pp. 679 – 684, doi:10.1109/ICCIT.2009.5407321.

[12] T. Shon, B. Koo, J. Park, and H. Chang, “Novel Approach to Enhance Mobile WiMAX”, EURASIP J. on Wireless Communication and Networking, Republic of Korea, 2010, pp.1-11.

[13] Y. Chung and K. Moon, “Biometric Certificate Based Biometric Digital Key Generation with Protection Mechanism”, IEEE comput.

Soc. Frontiers in the Convergence of Biometric and Inform. Technologies, Jeju City,2007, pp. 709-714. doi:10.1109/FBIT.2007.151.

[14] P. Arul and. A. Shanmugam "Generate a Key for AES using Biometric for VOIP Network Security", Journal of Theoretical and Applied Information Technology, Vo.5,No.2,2005, pp. 107- 112.

[15] H. Lee and T. Kwon "Biometric Digital Key Mechanisms for Telebiometric Authentication Based on Biometric Certificate", pp. 428-437, 2007.

[16] "Biometrics Ideal Test" from http://iris.idealtest.org/findTotalDbByMode.do?mode=Fingerprint/6.2013

[17] J. Kim, S. Hong, and B. Preneel "Related-key rectangle attacks on reduced AES-192 and AES-256," In FSE'07, volume 4593 of LNCS, Springer, 2007, pp. 225-241.