International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

A New Message Authentication Code Scheme Based on Feature Extraction of Fingerprint in Cloud Computing

Ali A. Yassin[*1], Mushtaq A. Hasson[1], Hesham Saleh Ridha[2]
[1]Computer Science Dept., Education College for Pure Science,
[2]College of Dentistry, Basic Science Dept.
Basrah University,
Basrah, 61004, Iraq,

***Abstract*— An era of cloud computing which leads to quick growth and deployment of information technology, it has also commanded to worries that user's identity could be penetrated by the prohibited copying and modification of message exchanged between two entities (Sender and Receiver) inside cloud environment. There are several schemes in this field which suffered from many attacks such as dictionary, insider, and modification attacks. In order to enhance this state, we need a strong scheme to assurance and strengthen of user's message. In this paper, we propose a new scheme of message authentication code based on features extraction of user's fingerprint used to prove the integrity of user's message. Features are extracted from user's fingerprint to generate message code for each user's login and prevent malicious attacks such as *Man-In-The-Middle* (MITM), replay, and insider attacks. Additionally, our proposed scheme includes many security characteristics like user's message anonymity, data integrity for user's message, session key agreement, and one time message code for each user's session. The experimental results view the efficiency and sturdiness of ourproposed scheme.**

Keywords- Cloud Computing; Fingerprint; Features Extraction; Message Authentication Code; Security.

I. INTRODUCTION

Digital images become a significant amount of our life due to the fast development of the Internet and the growing demand of multimedia fields from users. The efficient and automatic methods are required to identify and validate the contents of digital images. Additionally, image authentication is such an emboldening technique to automatically recognize whether a query image is another one, or a construction. Image authentication schemes commonly contain conventional cryptography, watermarking, and digital signature. However, hash functions consider a good start to confident access to security systems but, when we used the hash functions alone without any keys such as salt key; these functions don't appear enough to support the security of the user's identification used in many systems such as e-business, e-banking. The authentication development can be aided with the digital image where image authentication schemes depended on crypto-hash function to calculate the message authentication code (MAC) from images. The created hash is further encrypted with a shared key from the sender, and then added to the digital image as an overhead, which considers easy to be deleted. On the other hand, biometrics depended on a user's unique biological features, and can be an active extra solution to the entity authentication issue for financial schemes. One challenge in employing biometric authentication is, conversely, the dependability of the system with respect to faults in frequent measurements of the equivalent biometric data, such as face recognition, voice messages, or fingerprint [1-3].

With the development of information technology, the challenges of information security are increasing especially after appearing modern computing such as cloud computing, green computing.

Cloud Computing environment appears to be the superlative solution for solving the online access to server's services that seemed ubiquitous, authentication is becoming a pivotal topic for security professionals [4, 5]. The issue of securing access to the online data is critical today when entrance to bank accounts, intellectual property, health care records, and e-commerce are completed by only a few clicks. Simultaneously, ever more of these accesses are finished from handsets. This introduces security weaknesses and difficulties, because handsets have computational and control restrictions compared with old-style computers and they are forced in terms of text input existence more prone to robbery than conventional computers. It is also significant to idea out that tablets input restrictions make hard for users to enter complicated passwords. Cloud Computing is exceedingly suitable for solving problems connected to limited client resources and presents dynamic supplying of compute resources. So, cloud computing arises as a modern computing paradigm which objects to support on-demand scalable services via the Internet over Cloud sellers to multi-tenant establishments. Enterprises are involved to transport their on-premises infrastructure into cloud environment. On the other hand, they are still anxious about the security risks embraced by the act of inserting

their resources inside the cloud computing environment. Incessantly, cloud-based outsourced storage mitigates the client's charge for storage management and preservation by supporting a comparably low-cost, accessible, location-independent platform. Furthermore, users do not need to have physical possession of their data that they are suffering from a potentially formidable jeopardy for omitting or modified data. To overcome the security jeopardies, audit services are serious to guarantee the integrity and availability of cloud's outsourced data and to accomplish digital forensics and reliability on cloud computing.

In this paper, profiting from the features extraction of user fingerprint (level 2) and crypto-hash function, we propose a new MAC scheme to prevent the fraudulence of user's message (soundness property), the leakage of verified data, and resists the malicious attacks such as insider attack. Our proposed provides once time message code from sender to receiver, and vice versa. We also propose a well-organized procedure with respect to probabilistic queries and regular verification to cut down the audit costs per verification phase. Our proposed scheme contains important merits as follows: (1) the service provider and a user can achieve authenticated session's keys; (2) it describes by low cost and simple integration with available infrastructure; (3) Our scheme can resist many attacks such as replay attack, insider attacks, and reflection attacks; (4) we propose an efficient scheme for choosing a best parameter value to reduce computational cost of cloud audit services.

The rest of this paper is organized as follows. The necessary primitives and requirements of our scheme exist in Section II. An overview of related work is displayed in Section III. Our proposed scheme is presented in Section IV. We detail the security analysis and implementation results in Section V, and Section VI concludes the paper.

II. PRIMITIVES AND REQUIREMENTS

A. Features Extraction of Fingerprint

The wide majority of modern automated fingerprint authentication schemes are minutiae (level 2 features) used biometric systems [6, 7]. The two most distinguished kinds of minutiae are: ridge termination and ridge bifurcation [8]. The minutiae-based systems generally implement well with high-accuracy fingerprint images and an adequate fingerprint surface area. These conditions, however, may not any time be attainable. In several cases, only a small part of the test fingerprint can be comparative with the reference fingerprint. Additionally, comparing fingerprints gained via small-area sensors is hard due to the potentiality of having too little interference between different gains of the same finger [8]. Furthermore, the image of fingerprint is a unique pattern that consists of ridge and valley points on the surface of a finger. The ridge is well-defined as a single curved section, and a valley is the region between two adjacent ridges. Minutiae points (see Fig. 1) represent the local ridge cavities, which classify into two classes: bifurcations and ridge endings. A good quality fingerprint-image has minutiae from 40 to 100 [8]. Continuously, these minutiae points employed to detect theuniqueness of a user's fingerprint. Ultimately, the minutiae are relatively regular and sturdy to contrast, and image has a good resolution.

(a) (b)

Figure 1. Minutiae Points. (a) Ridge ending (b) Bifurcation

B. Hash Functions

There are several famous and acknowledged hash algorithms such as Message-Digest algorithm (MD), Message-Digest algorithm 5 (MD5), SHA-0, SHA-1, and RIPEMD-160 in information security fields [9, 10]. Now, we briefly review those hash functions:

*1) MD Family:*In 1992, Ronald L. Rivest successively presented two hash functions called MD and its revised version named MD5. In cryptography field, MD5 is used hash function based on 12 -bit hash value as output of this function. The input is worked in 512-bit blocks. Additionally, the MD5 function is aimed to be quite fast on 2-bit machines. Furthermore, it does not limit to use any large substitution tables, here; MD5 have ability to cod quite compactly. MD5 considers slightly more difficult and slower than MD, but it increases the security level in design.

*2) SHA Family:*The secure hash function (SHA) family is a set of associated with cryptographic hash functions and presented by the National Institute of Standards and Technology (NIST). SHA-0 considers the first member of SHA, was issued in 1993. SHA-1 represents as a developed version of SHA-0, was issued in 1995. Four irregular models have been published by NIST with improved output ranges and a marginally different design as follow: SHA-22, SHA-256, SHA-384, and SHA-512. However, SHA-1 runs on digital message blocks contained 512 bits for a 160-bit digest is produced. SHA-1 is considerably sturdier against malicious attacks [9,10].

*3) Image Authentication Schemes:*Authentication considers one of the image security concerns solved by hash function and another one problem is supporting security for illegal processing of digital image is solved by an encryption function. Image authentication schemes commonly include traditional cryptography, digital signature, fragile and semi-fragile watermarking, and steganography and so on. Any authentication scheme can be aided with the original image to check the validity of user. Image authentication schemes use a crypto-hash function to compute the message authentication code (MAC) based on images. However, the sender generated hash by encrypting message with his secrete key, and then added to the image as an overhead. Additionally, an image hashing procedures are extract a set of distinguished features from the digital image that can be used for authentication process. Hashing function is necessary to prove authentication, content integrity and avoid forgery. An authenticity of image is evaluated by means of digital signature while the image is

affected by related distortions. Furthermore, cryptography is very vital to provide secrecy and security to resist traditional attacks and other types of attacks when exchange digital images between two entities on the network [11].

III. RELATED WORK

In [12], Xie et al. have proposed a new scheme to use the Approximate Message Authentication Codes (AMAC) for image authentication. This scheme is a probabilistic checksum computed by using a sequence of XOR operations and two games of popular bit voting in DCT domain. Finally, the similarity ratio between two images is detecting based on hamming distance of their AMACs.

C. Lin and S. F. Chang [13] have suggested an image authentication scheme that depends on the constant relationship between any two picked DCT coefficients that are at the same location of two different (8 x 8) digital image blocks. Their technique is sensitive to prevent malicious managements made in a part of an image and simultaneously is flexible to JPEG compression.

Q. Sun and S. F. Chang [14] have presented a semi-fragile image authentication scheme merging Error Correction Codes (ECC) and image watermarking. By applying ECC, they support a mechanism that permits minor variation of content features which caused by acceptable operations such as loss compression and addend noise.

Shensheng Yu et al. [15] have suggested an authentication scheme in which content relied on watermark is created from the LL3 factor of three-level Haar wavelet decomposition based on Sobel edge detection technique and then the hash is calculated using MD5 as the main hash function. Additionally, the computed hash is then entrenched in the middle frequency coefficients.

Fridrich and Goljan [16] presented a scheme for self-embedding an image as a scheme of preserving the content of image. Their proposed scheme also permits the regions of the image that have been interfered with, cropped, or changed, to be partially repaired. The main principle of this scheme is to embed a compressed version of the image inside the LSB of image's pixels. The major weakness of this scheme is that embedded information is not strong.

In [17] AshwinSwaminathan et al. have improved an algorithm for producing an image hash, using Fourier-Mellin transform features which are constant to two-dimensional affine transformations. The method also includes key-dependent randomization into the Fourier-Mellin transform productions to form a secure and strong image hash.

MACs consider one of the most principal, well-known and widely studied primitives in recent cryptography, exclusively in practice and a wide variety of buildings have been established in the past. Most applicable to this work presented by Dodis et. al [18] that here work focuses primarily on theoretical creations of MACs with the aim of growing the class of assumptions upon. However specified practical efficiency constraints and the struggle in designing secure symmetric key cryptographic tools much attention has been based on creating secure MACs from other existing symmetric key tools like block-ciphers [19], compressionfunctions [20], and even fixed-input distance PRFs [21].

In this paper, we proposed a new image authentication technique based on secure hash generated with features extracted from user's fingerprint. Features are first extracted from user's fingerprint with the k-largest local total variations, and used second level of fingerprint feature extraction. Then features in the query fingerprint and the entered fingerprint are matched into pairs based on discrete wavelet transform. Then the scheme decisions about the integrity and authenticity of image which enters by user. Additionally, our proposed scheme includes many security characteristics like user's message anonymity, data integrity for user's message, session key agreement, and one time message code for each user's login. The experimental results view the efficiency and sturdiness of our proposed scheme.

IV. OUR PROPOSED SCHEME

The common notations in Table I will be used throughout this paper. Our proposed scheme consists of two phases—Configuration and Verification. In the configuration phase, the main components $(CSP, Sender, Reciver)$ also uses a cryptographic hash function $h(.)$, symmetric key encryption/decryption $Enc(.)/Dec(.)$, CSP sets up $n = p * q$; where both p and q are two large primes. The both sender (S) and receiver (R) send their fingerprints (Fp_s, Fp_r) to the Cloud Service Provider (CSP) through a secure channel.

TABLE I. NOTATIONS OF OUR PROPOSED SCHEME

Symbol	*Definition*
$h(.)$	A cryptographic hash function.
CSP	Cloud Service Provider.
$Enc(.)$ /$Dec(.)$	Symmetric key encryption/decryption function.
n, p, q	Large primes numbers to compute shared key.
S, R	Sender and Receiver.
Fp_s, Fp_r	Fingerprints of sender and receiver, respectively.
FX	Features extraction of fingerprint (level 2).
Sk	Salt-Key
Sh	Shared key computes based on feature extraction of users' fingerprint.
M'	Sender sends Message Authentication Code to the receiver.
M''	Receiver computes Message Authentication Code.
r_i, r_i'	Random number uses to generate one time anonymous message code.
P_i, P_i'	Position of random number that extracted from fingerprint's feature extraction
$\|\|$	Concatenation function.

After that, CSP stores (Fp_s, Fp_r), generates two keys: Saltkey $(Sk \in Z_n)$ and shared key $(Sh = h(FX(Fp_s)) \oplus h(FX(Fp_r)))$; Where FX is function to compute features extraction (level 2) of user's fingerprint.

After that, CSP sends keys (Sk, Sh, Fp_r), (Sk, Sh, Fp_s) to Senders and Receiver, respectively, in the secure channel. After registration phase, the sender/receiver can use his secret key to complete verification phase. The verification session is qualified as follows (see Figure 2).

1. $S \rightarrow R: M, M', P_i'$. S performs the following steps:
   - Assume sender's message is M.
   - Generate random number $r_i \in FX(Fp_r) = FX(Fp_r(Index))$ and compute one time anonymous message code (If the sender resends the same message to the receiver or vice versa) $M' = h(M||Sk||r_i)$ and compute the position of r_i inside feature extraction of fingerprint vector $P_i = Index\,(FX(Fp_r))$.(see Figure 3)
   - Compute $P_i' = P_i \oplus Sh$.
   - Send M, M', P_i' to R.
2. R checks the integrity of receiver's message as follows:
   - Compute $P_i'' = P_i' \oplus Sh$ and extract r_i' based on $r_i' = Index\left(FX\left(Fp_r(P_i'')\right)\right)$. Then, R computes $M'' = h(M||Sk||r_i')$; If the M'' matches with M', the Receiver ensures from integrity of message that submitted from the sender. Otherwise, R terminates verification phase.

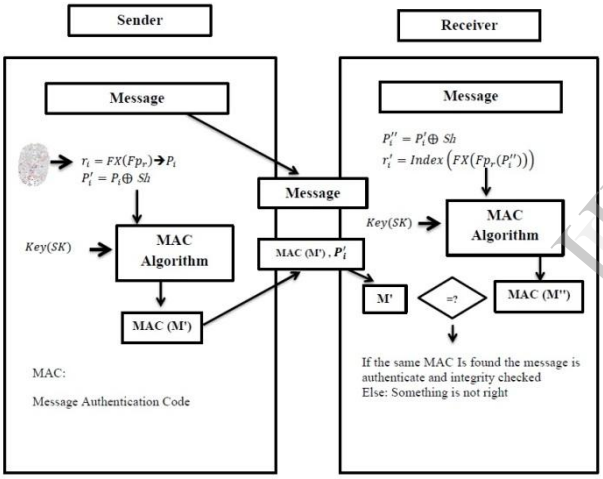

Figure 2. Our proposed scheme diagram

Position/Index →	0	1	2	3	4	5	6	7	.....	n
Elements of FX →	22	251	140	170	132	245	211	40	.....	80
	FX(0)	FX(1)	FX(2)	FX(3)	FX(4)	FX(5)	FX(6)	FX(7)	.....	FX(n)

Figure 3 explains the position ofFX vector's elements

V. EXPERIMENTAL RESULTS

A. Security Analysis

In this section, we offer the security analysis of our proposed scheme. We will view that our scheme is secure against well-known attacks such as MITM attack, replay attack, insider attack. Moreover, our proposed scheme enjoys several merits, containing one time anonymous message code, and session key agreement.

Theorem 1. Our proposed scheme can supply user's message anonymity.

*Proof.*In general, the standard message authentication codes (MACs) warranty authenticity of digital messages, they do not have ability to generate the anonymity of the sender and receiver. For example, it may be easy for a witness to detect whether or not two valid messages were sent by the same user even without any information about the shared key used.

Assume a sender/receiver tries to resend the same message which has been sent previously. If an adversary attempts to eavesdrop on the sender's login request, he cannot use the same the sender's message authentication code (M′) because the sender generates r_i once for each request. So, r_i has been extracted from receiver's fingerprint ($r_i \in FX(Fp_r) = FX(Fp_r(Index))$) existed just in R and S. Additionally, an adversary does nothave main keys (Fp_r, Sk, r_i) to compute crypto hash function $M' = h(M, Sk, r_i)$. Hence, it is difficult for an adversary to disclose the sender's message authentication code. Clearly, our proposed scheme can support user's message anonymity.

Theorem 2. The proposed scheme can support Known-key security and session key agreement.

Proof. In our proposed scheme, when the sender sends the hi messages to the receiver or vice versa, he uses secret Salt-key Sk to compute $M' = h(M, Sk, r_i)$. Furthermore, he uses shared key Sh to encrypt the position (P_i) of r_i . An adversary cannot access to the session keys, he is still unable to get fresh values of Sh which generates at registration phase by CSP. So an adversary cannot get these secret parameters.

Theorem 3. Our scheme can preventa replay attack.

Proof. An adversary performs a replay attack by eavesdropping the loginmessage which sent by a rightful sender to the receiver. Then an adversary reuses this message to impersonate the user when logging into the system in a next session. In our proposed scheme, each new sender's request should be identical with CSP′s keys (Sh, Sk, r_i, $P_i' = P_i \oplus Sh$) . Therefore, an adversary cannot pass any replayed message to the R′s verification. Moreover, our work can resist this attack without synchronization clocks. So,our scheme depends on random r_i instead of timestamp. As a result, an adversary fails to apply this type of attack.

Theorem 4. Our scheme can resistthe forgery attack and parallel-session attack.

Proof. If any adversary tries to impersonate, he should be accessed a valid session message (M, M', P_i') by using secret parameters $(Sh, Sk, r_i, Fp_r, P_i')$ .An adversary does not possess any idea about (Sh, Sk, Fp_r) to compute (M', P_i'). Lastly, an adversary will fail to forge a valid session message and therefore, cannot use a forgery attack.

Theorem 5. Our proposed scheme can resistthe MITM attack.

*Proof.*This type of attack is intended that an adversary has the ability to intercept the messages between a sender and a receiver. Then, he uses this message when the one entity signs out the cloud service provider. In our proposed

scheme, the parameters are securely encrypted and sent from sender to receiver or vice versa. Generation of the random value r_i is through the creation of sensitive data (M', r_i, Fp_r, P_i') by the sender as a session request to the receiver. This sensitive data becomes useless when sender/receiver signs off theCSP. Therefore, an adversary spotting communication between sender and receiver can learn r_i which is used only once; he is unable to compute M'. As a result, the proposed scheme can resist MITM attack.

B. Implementation and Results

In this section, we conduct several experiments for gauging the efficiency and the effectiveness of our work. Figure 4 shows time processing of verification phase. However, the average time for the verification phase of our work is equal to 0.0314 seconds for each user who indicates the high speed of our solution. The estimation parameters are declared in Table II. The time requirement of our scheme is brief in Table III. We test the effectiveness in terms of authentication accuracy. We have registered during our experiments 1000 users.

TABLE II. ESTIMATION PARAMETERS

Symbol	***Definition***
T_h	Time processing of a hash function.
T_{Xor}	Time processing of Xor function.
T_{Opr}	Time processing of mathematical operations such as multiplication, addition and subtraction.
$T_{\|\|}$	Time processing of concatenation function.

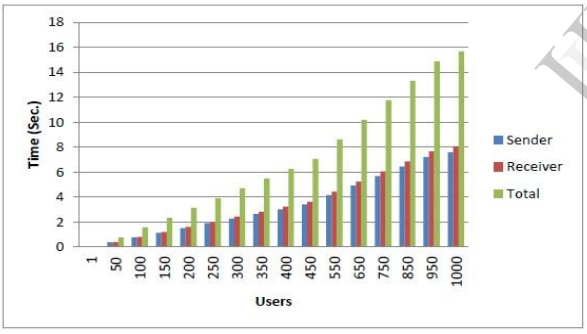

Figure 4 shows the performance of our proposed scheme

TABLE III. PERFORMANCE OF OUR PROPOSED SCHEME

Phase	***CSP***	***Sender***	***Receiver***
Setup & Registration	$2T_h + T_{Xor}$	-------	-------
Verification	-------	$T_h + T_{Opr} + 2T_{\|\|} + T_{Xor}$	$T_h + 2T_{Opr} + 2T_{\|\|} + T_{Xor}$
Total	$2T_h + T_{Opr}$	$T_h + T_{Opr} + 2T_{\|\|} + T_{Xor}$	$T_h + 2T_{Opr} + 2T_{\|\|} + T_{Xor}$

VI. CONCLUSION

In this paper, we have proposed a newer message authentication code scheme for cloud computing environment based on feature extraction of fingerprint. Our proposed scheme aims to support more functionalities and to resist familiar attacks. These vital merits include (1) the valid user can freely to submit his message; (2) our proposed scheme supports secret MAC between sender and receiver; (3) it achieves one-time message anonymity; (4) Using fingerprint as a secret factor to extract secret keys that making an adversary fails to obtain main keys; (5) our proposed scheme can provide revocation and security of the stored data. Moreover, our scheme can resist MITM attacks, replay attacks, and forgery attacks. In performance evaluation, our scheme has been proven to obtain strong security with lower communion cost than previous works.

REFERENCES

[1] L. Xie and G. R. Arce, "Image enhancement toward soft image authentication," In Proc. IEEE ICME, vol. 1, New York, Aug. 2000.

[2] B. Schneier, Applied Cryptography: Protocols, Algorithms, and SourceCode, 2nd ed. New York: Wiley, 1996.

[3] M. S. Fu and O. C. Au, "Data Hiding Watermarkingfor Halftone Images," IEEE Trans. Image Processing,vol. 11, no. 4, pp. 477-484, 2002.

[4] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications , vol. 34, no.1, pp.1-11, 2011.

[5] A. A. Yassin, H. Z. Neima,Z. A. Abduljabbar, H. Sh.Hashim, " Efficient and Secure Mutual Authentication Scheme in Cloud Computing", IJEAT, vol.3, no. 1, pp. 133-139, 2013.

[6] H. Robert,"Ridge Enhancement in Fingerprint Images Using Oriented Diffusion", Digital Image Computing Techniques and Applications, In Proc. the 9th BiennialConference of the Australian Pattern Recognition Society on ,Vol 3, No.5 , pp.245 – 252, 2007.

[7] L. Hong, J. Anil,Y.Wan, "Fingerprint imageenhancement:algorithm and performance" , IEEE transaction on pattern analysis and machine intelligence, vol. 20, no.8, pp.777-789, 1998.

[8] A. Kisel, A. Kochetkov, J. Kranauskas, "Fingerprint minutiae matching without global alignment using local structures", Informatica , vol. 19, no. 1, pp. 31–44, 2008.

[9] R.L. Rivest. "The MD message digest algorithm",In S. Vanstone, editor, Advances in Cryptology -CRYPTO' 0, LNCS 5 , pp. 0 - 11 , 201 1.

[10] W. Stallings, Cryptography and Network Security:Principles and Practices. 2nd ed. Prentice HallInternational, 2010.

[11] V. Monga, D. Vats, B. Evans, "Image authentication under geometric attacks via structure matching," In Proc. EEE International Conference on Multimediaand Expo, 2005. ICME 2005, pp. 229–232, 2005.

[12] L. Xie, G. R. Arce, R. F. Graveman, "Approximate message authentication codes," IEEE Transactions on Multimedia, vol. 3, no. 2, pp.242-252, 2001.

[13] C. Y. Lin and S. F. Chang, "A robust image authentication method distinguishing jpeg compression from malicious manipulation," IEEE Transactions Circuits and Systems for Video Technology, vol. 11, no. 2, pp.1453-1468, 2001.

[14] M. Juneja, P. S. Sandhu,"Improved LSB based Steganography Techniques for Color Images in Spatial Domain," International Journal of Network Security, vol. 16, No.4, pp. 366-367, 2014.

[15] S. Yu, Y. Hu and J. Zhou, "Content-based watermarking scheme for image authentication," in Proc. of the 8th International Conference on Control, Automation, Robotics and Vision, pp. 1083-1087, Kunming, China, 2004.

[16] J. Fridrich and M. Goljan, Protection of Digital Images Self Embedding, Symposium on Content Security and Data Hiding in Digital Media, New Jersey Institute of Technology, New York, NJ, USA, 1999.

[17] A. Swaminathan, Y. and M. Wu, "Robust and secure image hashing," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 215-229, 2006.

[18] Y. Dodis, E. Kiltz, K. Pietrzak, and D. Wichs. Message authentication, revisited. In EUROCRYPT, pp. 355-374, 2012.

[19] M. Bellare, K. Pietrzak, and P. Rogaway. Improved security analyses for CBC MACs. In CRYPTO, pp. 527-545, 2005.

[20] M. Bellare. New proofs for NMAC and MAC. In CRYPTO, pp. 602-619, 2006.

[21] Y. Dodis and J. P. Steinberger. Message authentication codes from unpredictable block ciphers. In CRYPTO, volume 5677 of Lecture Notes in Computer Science, pages 267{285. Springer,2009.