Securing Fuzzy Vault Enabled Authentication in Body Area Networks based Smart Healthcare

Jack Hodgkiss and Soufiene Djahel
Department of Computing and Mathematics, Manchester Metropolitan University, UK

***Abstract*—The emergence of Body Area Networks (BANs) has paved the way for real-time sensing of human biometrics in addition to remote control of smart wireless medical devices, which in turn are beginning to revolutionize the smart healthcare industry. However, due to their limited power and computational capabilities they are vulnerable to a myriad of security attacks. To secure BAN sensors against these threats processor-intensive cryptographic techniques need to be avoided as they are not suitable in this context. This paper focuses on authentication service for BAN sensors and proposes an original scheme named "RAFV: Rotational Assisted Fuzzy Vaults" to harden the security of any authentication solution using the fuzzy vault construction approach. The evaluation results have shown that RAFV can successfully conceal the secret of the vault even if the locking elements are known to the adversary. Also, RAFV may improve upon communication overhead by enabling a reduction in the size of the vault without compromising its security. It has achieved all of this while remaining competitive with regards to additional computational overhead.**

I. Introduction

Body Area Networks (BANs) are expected to play a major role in enabling "smart healthcare", which is the inclusion of technology to help sense, evaluate and react to the environment and patients to deliver high-quality care. BAN sensors are a type of network devices small enough to be worn on or implanted within the human body [1]. These devices enable continuous patient vital sign monitoring in addition to remote control of medical devices such as insulin pump, pacemaker, or continuous glucose monitoring. Due to their nature (i.e., limited power resources, memory usage and computational capabilities) and the environment, they operate within, securing these devices along with their network is crucial to the success and wide adoption of this technology.

Authentication is a crucial process in safeguarding BANs and their operations such as the transmission of patients' health data or receiving commands. Many lightweight authentication schemes have been proposed over the years to ensure the required security level for BAN sensors while meeting their stringent constraints [2]. Authentication enables BAN sensors or devices to prove their identity for verification by completing an authentication process or challenge. Without any form of authentication, BAN sensors are vulnerable to various security attacks that may be carried out by a motivated adversary. In [3], the authors outline the security requirements for BANs based smart healthcare and highlight the unique challenges that need to be overcome to develop robust biometrics based authentication schemes for BAN. Moreover, using fingerprints as an authentication mechanism to unlock mobile devices for payment authorization purpose was investigated in [4]. This study raised some concerns about fingerprint-based authentication and potentially other biometrics, such as ECG, due to their associated vulnerabilities. Issues discussed include how fingerprints may be captured, how users cannot easily avoid leaving their fingerprint behind and how once an adversary compromises it, the revocation is impossible. A review of the developed authentication protocols for deployment within implanted medical devices (IMDs) was presented in [5]. This paper outlines the security challenges and functionality requirements for authentication schemes targeting IMDs that can be classified as either proximity-based, biometric-

based or a combination of the two.

Fuzzy vaults are one such scheme that is being used to facilitate a key agreement between communicating BAN nodes to achieve a robust authentication. Fuzzy vault [6] is a cryptographic construction that allows a user to conceal a secret value (e.g., message, password or cryptographic key) by locking it using elements obtained from a publicly known universe. Any attempt to unlock the vault and uncover the secret contained within it requires significant overlap between the set of elements used to lock the vault and the set being used to attempt unlocking it. The order in which these elements are used when unlocking the vault has no impact on success due to the fuzzy vault's possessing order invariance. These two properties make unlocking a fuzzy vault possible without a perfect or near-perfect recall of the elements used to lock the secret. This may appear as a security vulnerability, however, the fuzzy vault scheme is more suitable for environments where shared knowledge of the elements used to lock the vault originates from a source that is incapable of 100% successful capture. An appropriate example of such a source is "fingerprint minutiae" [7] where the positioning of the finger, the moisture present and any movement can have a significant impact on the sensor's ability to extract identifying markers. Even successive readings of the same finger by the same device can vary to such an extent that they would appear to be from separate users.

II. Fuzzy vault overview

The fuzzy vault scheme was first introduced in [6] to conceal a secret (S) using a set of elements A known at the time of vault construction. Once locked, the vault can only be unlocked using another set of elements B that has significant overlap with the set A. The fuzzy vault can be constructed in such a way to allow unlocking through the use of either error correction codes or polynomial interpolation. For the sake of simplicity, we will be using polynomial interpolation, specifically Lagrangian Interpolation. The vault is constructed as follows: 1) Generate an n^{th} order univariate polynomial P over the indeterminate x whose coefficients are an encoding of the secret S, 2) Evaluate $P(X)$ using the elements of the set A creating a new set $R = \{A_{\text{i}}, P(A_{\text{i}})\}$, 3) Randomly generate a set of chaff points C which do not share the same x with any point within R or any other chaff point, also no chaff point may imitate a legitimate point $C = \{(C_{\text{x}}, C_{\text{y}}) | C_{\text{x}} \notin A,\ C_{\text{y}} \neq P(x)\}$, 4) Combine the sets R and C together then order the resulting set in ascending order. Any attempt to reconstruct the polynomial, and by extension the secret S, will require knowledge of $n+1$ features (elements) present within the set A. The fuzzy vault construction steps are shown in Fig. 1.

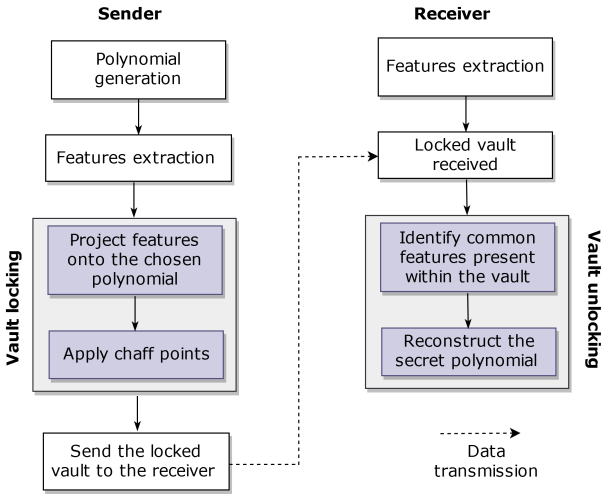


Figure 1: The main steps of the fuzzy vault construction process

An illustrative use case of the fuzzy vault scheme would be the following; $Alice$ wishes to exchange her contact details (i.e., phone/mobile number or email address) on travel forums with individuals who share the same interest with regards to international travel. Since $Alice$ does not want everyone to have access to her contact information she may distribute them using a fuzzy vault, by concealing within the vault her contact information as a secret to be recovered. Only those who have similar travel interests may successfully recover $Alice$'s contact information. $Alice$ will start by encoding her contact information within the coefficients of a polynomial $P(X)$ which has a degree that determines the error tolerance of the vault. The smaller the degree the fewer overlapping features are required for a successful unlock, whereas the higher the degree the more overlapping features are needed. $Alice$ will then

construct a set of elements A which represents travel locations (i.e., features) around the world; $A = \{Manchester,\ Berlin,\ LosAngeles, ...\}$. These features will be mapped onto $P(X)$ followed by the generation of chaff points which must not fall upon the polynomial. The vault is then shuffled to ensure that the legitimate features are concealed amongst the chaff points. This vault can then be exchanged with other individuals with an interest in travelling. For example, Bob may attempt to unlock the vault using his features contained in the set $B = \{Berlin,\ LosAngeles,\ NewYork...\}$ and will achieve this as long as $|A \bigcap B| > 1+n$, where n is the degree of the polynomial. Any other user who does not meet this requirement will be unable to acquire Alice's contact information.

III. Fuzzy vault Security Vulnerability

Two pioneer solutions use the fuzzy vault or a similar construction known as PSKA (Physiological Secure Key Agreement) [8] and OPFKA (Ordered-Physiological-Feature-based Key Agreement) [9]. These schemes enable key agreement between BAN nodes that are equipped with either ECG (electrocardiogram) or PPG (photoplethysmogram) sensors, as these physiological signals are used to conceal the symmetric key to be agreed upon. While these schemes provide a novel way of agreeing upon a key accompanied with a high-security level, they do not account for the possibility of the physiological signals being captured remotely off the body, without knowledge or consent of the patient. This remote capture of physiological signals may allow an adversary to successfully impersonate a genuine body sensor and enable them to carry out further attacks within the BAN, such as data manipulation in which they send fake readings that can mislead medical professionals and have serious consequences for the patient. In [10], the authors investigated the potential of using prediction filters, such as a Kalman filter, to unlock PSKA based fuzzy vaults using leaked physiological signals such as PPG. As stated in [11], the remote capture of PPG signals using UWB (Ultra-Wide Band) radars is possible, thanks to advancements in remote sensing technology. This presents a serious security risk for devices aiming to achieve authentication and key agreement using PSKA or similar schemes as the key could be unlocked by an adversary and neither the user nor the network administrator would be aware of the intrusion. In [12], a concern is raised regarding the security of PSKA vaults with the advent of remote sensor technology and its potential to capture the necessary information to unlock a vault. This fear is reinforced with the use of electric potential probes that enable remote capturing of ECG and PPG [13], [14].

Due to this development in adversary capabilities, it is necessary to explore new ways of protecting the fuzzy vault construction and the schemes that rely upon it while minimising the incurred overhead. We, therefore, propose an original scheme named RAFV (Rotation Assisted Fuzzy Vault) that builds upon the fuzzy vault scheme by leveraging channel side characteristics known as RSSI (Received Signal Strength Indicator) to obfuscate the locked vault. If an adversary is capable of collecting physiological signals originating from the target BAN sensors then they would be able to carry out impersonation attacks if the current iterations of PSKA, OPFKA and schemes similar in nature are used. This is because adversaries can utilize a remotely captured signal to unlock the vault and obtain the key concealed within it, compromising all future communication between the nodes targeted. However, RAFV will ensure that knowledge of the physiological signal alone does not provide access to the secret concealed within the vault. This is because any attempt to acquire the secret requires knowledge of how the vault has been obfuscated, which is not impacted by the leakage of locking elements to an adversary.

IV. Our Proposal

In this section, we will present the main idea of our original scheme named RAFV, describe its locking and unlocking process and discuss its robustness against brute force attacks that may target the constructed vault.

A. RAFV: an overview

The objective of RAFV is to secure any authentication scheme that uses the fuzzy vault construction mechanism, wherein the elements used for locking and unlocking the vault are susceptible to leakage within a wireless network. RAFV can be seen as

an extension to the fuzzy vault scheme and is situated within the post-locking and pre-unlocking phase of this scheme (See shaded areas in Fig. 1). RAFV shall transmit an obfuscated fuzzy vault from the sender to the receiver, any attempt by an adversary to unlock the intercepted vault would fail even if the adversary is aware of the full set of locking elements. This is because RAFV does not conceal the polynomial but rather 'corrupts' it preventing successful unlocks until the vault has been 'repaired'. The vault shall be obfuscated by dividing it into quadrants and rotating the points within each quadrant around its centre.

RAFV relies on the ability to agree upon a sequence of bits in an out-of-band manner to ensure that an adversary cannot obtain this sequence. This sequence can be seen as a symmetric key that is used to lock and unlock the vault itself. To achieve this, RAFV makes use of RSSI (received signal strength indicator) which is a measurement of the power contained in the received signal. This measurement is only computed locally on the device and cannot be obtained by an adversary, which makes it ideal for attempting to harden the security of the fuzzy vault scheme. RSSI reconciliation is a process that enables the two BAN nodes to agree upon the key that shall be used to secure the vault. RSSI values between two wireless devices are prone to discrepancies and need to be corrected, therefore we model the errors as communication errors and use error correction codes, such as Reed-Solomon (RS), to ensure that the sender and the receiver are in agreement (i.e., they measure the same value). This process has been used in many key generation and key agreement schemes, including the ones applied in BAN such as [15]–[17].

B. Locking and unlocking process in RAFV

RAFV locking phase consists of the following steps: 1) Measuring the RSSI value between the two BAN devices, 2) The sender generates RS coefficients and sends them to the receiver, 3) The receiver uses the received RS coefficients to correct its 'copy' of RSSI, if the receiver fails to correct the errors the process should be restarted from the first step, 4) The sender constructs the locked fuzzy vault, 5) Dividing the vault into several quadrants, 6) Assigning a rotation direction and order for each quadrant, 7) Executing the rotation. These steps are summarized in Fig. 2.

As for the unlocking phase, upon reception of the fuzzy vault from the sender BAN device the following actions are taken: 1) Generating the original direction and order of rotation for each quadrant using the agreed RSSI values, 2) Reversing the order and direction of rotation for each quadrant, 3) Executing the rotation, 4) And finally proceed with unlocking the fuzzy vault. These steps are depicted in Fig. 2.

C. Vault division and quadrants rotation in RAFV

In the context of RAFV, a quadrant is used to split the vault into evenly spaced partitions. If a quadrant is selected all the points contained within its boundaries shall be rotated either clockwise or counterclockwise around the center point of the quadrant. More quadrants can be created by dividing all of the quadrants in the current deepest layer into four smaller ones. In doing so each newly created quadrant (child) shall cover $\frac{1}{4}$ of the area of its parent. Quadrants can be represented using the quadtree data structure where the deeper layers contain more quadrants, however each quadrant represents a smaller area of the vault.

Once the vault has been divided into the desired number of quadrants the angle and order of rotation can be assigned. In RAFV, the angle of rotation is either 90° or -90°. This is because other angles, such as 45°, 135° or 215° will cause quadrants to overlap with one another making the reconstruction of the original locked fuzzy vault, by the receiver, impossible. The angle of rotation is obtained from the RSSI values that have been agreed upon before vault construction. The RSSI values are assigned to the deepest layer of quadrants within the vault. Starting from the bottom left and moving across and up, each quadrant will be assigned an RSSI value in the order they occur in the list. If there are more quadrants than RSSI values then the list will loop back to the start. As for quadrants in layers above, their values are determined by summing their children's RSSI values. Once each quadrant has been assigned a value it can then be converted into an angle by looking at the parity (odd or even) of the value. If the assigned value is odd then the

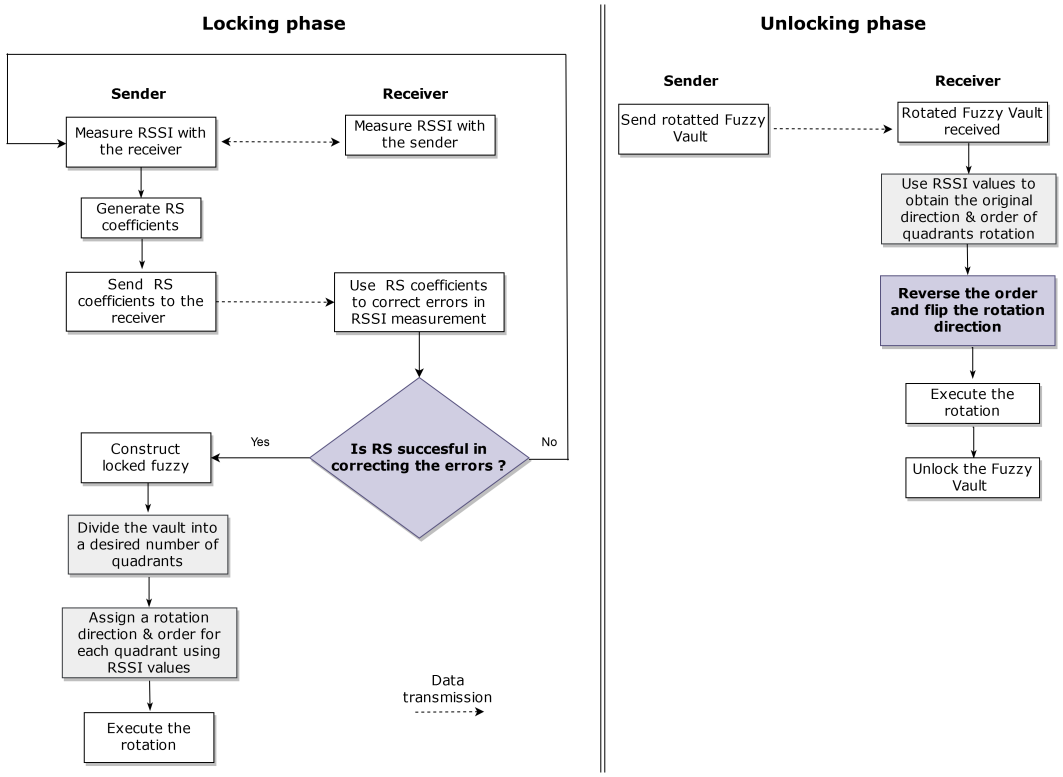


Figure 2: The fuzzy vault locking and unlocking process in RAFV

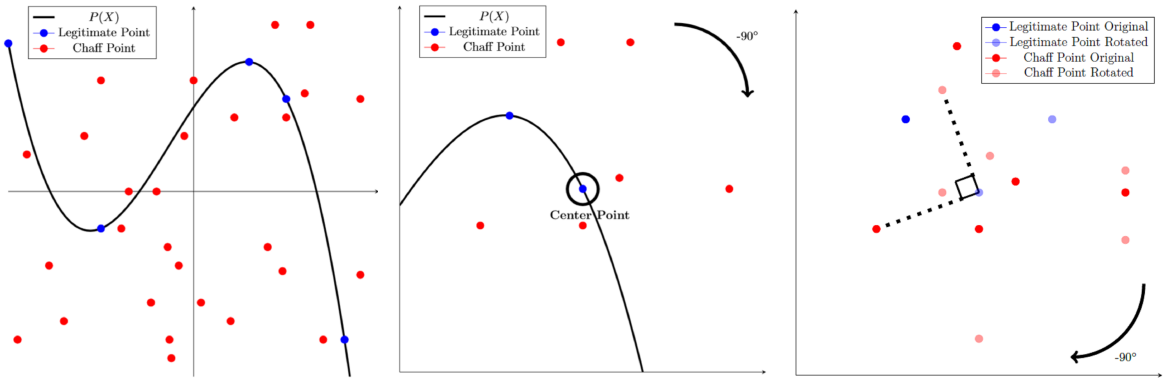
quadrant shall be rotated -90° and if the value is even then the angle of rotation is 90°.

Regarding the order of rotation, this also is obtained via the same RSSI values as the angle of rotation. However, the difference consists in using the collection of RSSI values to seed a random number generator which will randomly choose which quadrant shall be rotated next. The order of rotation has a significant impact on the obscured vault as each rotation carried out will fundamentally change the result. An illustration of the rotation applied to the content of a vault is shown in Fig. 3. The first sub-figure (Fig. 3(a)) shows a fully constructed fuzzy vault divided into 5 quadrants where there is a set of legitimate points (highlighted in blue) on a polynomial and chaff points (highlighted in red) that are used to conceal the secret. The second sub-figure (Fig. 3(b)) depicts a close up of the top-right quadrant of the vault where its center point has been marked and a rotation direction has been assigned to it. The final sub-figure (Fig. 3(c)) shows the same quadrant after -90° rotation has been applied, where the rotated legitimate and Chaff points are highlighted using the same colour as their corresponding original points but with increased transparency.

To be able to recover the locked fuzzy vault the receiver should know the number of layers present within the vault in addition to how many rotations have been carried out. This information must be communicated to the receiver, alongside the obfuscated locked vault, and be sent as plain text in a message appended to the fuzzy vault. This is because such information does not give the adversaries any advantage in their attempts to recover the vault. Once this information is obtained, the receiver can divide the vault the same way the sender did in addition to assigning the RSSI values and rotation order to each quadrant. The only difference, however, is that the receiver must swap 90° rotation with -90° and vice versa in addition to reversing the order of rotation.

D. Security analysis of RAFV

Two parameters can be used to calculate the size of the search space an adversary may face when



(a) Fully constructed fuzzy vault with 5 quadrants

(b) Overview of the top right quadrant of the vault before rotation

(c) Overview of the top right quadrant of the vault after rotation

Figure 3: Illustration of the rotation process in RAFV for both legitimate and Chaff points

attempting to directly brute force the rotation of the vault. These two parameters are the number of quadrants assigned a unique RSSI bit and the number of rotations carried out during the locking phase. The search space can be calculated using the following equation:

$$Search_{space} = 2^n \times r^n \tag{1}$$

where n is the number of quadrants and r is the number of rotations. For example, a RAFV based vault that is locked using 85 quadrants and 32 rotations would yield $2^{85} \times 32^{85} = 3.15 \times 10^{153}$. However, whilst the search space is exponentially large it is ultimately limited by the size of the key agreed upon by the sender and receiver within the RSSI reconciliation because this key determines the rotation. Therefore, an appropriate sized key must be picked to ensure strong bit-security for the scheme to function. For example, a 128-bit key that has been agreed upon by the two BAN nodes will ensure sufficient protection against brute force attack as an adversary would, on average, have to search half of the key space, **e.g** 2^{127}, and use each key to generate its rotation pattern and attempt the unlocking process in full. As mentioned earlier in Section IV-A, RAFV will allocate the direction of rotation to the quadrants in the deepest layer and quadrants in the layers above will derive their direction from the sum of their children. For the 128-bit key to have a maximum effect there must be at least 128 quadrants in the deepest layer to ensure that this key is represented throughout the rotation pattern. It is therefore required that a vault must be at least four layers deep to ensure a minimum of 128 quadrants in the last layer. The number of quadrants in each layer can be determined using the following equation.

$$Quadrants_{number} = 4^{m-1} \tag{2}$$

Where m refers to the layer order. The layers are ordered starting from 1 until the deepest layer of the vault. To compute the total number of quadrants present within the entire vault we use the following the equation.

$$Quadrants_{total} = 4^{m-1} + 4^{m-2} + ... + 4 + 1 \tag{3}$$

Therefore, the fifth layer of a divided vault (i.e, the result of applying the division 4 times starting from the main layer) would contain 256 quadrants and the total number of quadrants in the entire vault would be 341. It is important to note that if an adversary had half of the rotation pattern used by the vault they would not be able to infer the other half. For example, if an adversary had managed to acquire the order of rotation used within a given iteration of the scheme they would not be able to determine what direction has been assigned to each quadrant within the vault.

Furthermore, two types of adversaries may attempt to compromise the security of the RAFV based key agreement. Adversary A is an adversary

that is unaware of any of the locking elements used by the underlying fuzzy vault. This means that for every iteration of the rotated vault they would have to attempt to brute force the fuzzy vault unlocking process with no guarantee that they have the original vault. Adversary B, however, is aware of the elements used to lock the vault due to their ability to remotely capture the physiological signals being leaked by the wearer. Therefore, they will be able to process each vault much quicker because they will only be concerned with the points that overlap with the features they have illegitimately acquired, allowing them to discard chaff points. However, this does not give the adversary B any advantage to unlocking the vault as the knowledge of the locking elements does not provide any insight into how the vault has been rotated.

V. Performance Evaluation

To evaluate the performance of RAFV we will compare it against the fuzzy vault scheme with regards to the required execution time. Such a comparison will enable an accurate assessment of the additional overhead induced by RAFV. Both schemes have been implemented in C++17 running on an Intel 8809G (3.10 GHz / 4.20 GHz) processor with a RAM of 2400 Mhz C16. Whilst the performance of such a processor far exceeds the performance of wireless sensor devices used in the intended application area (i.e, Body Area Networks) this evaluation aims to provide a like-for-like comparison between the two schemes. Future work could, however, look at implementing both schemes on more appropriate hardware devices.

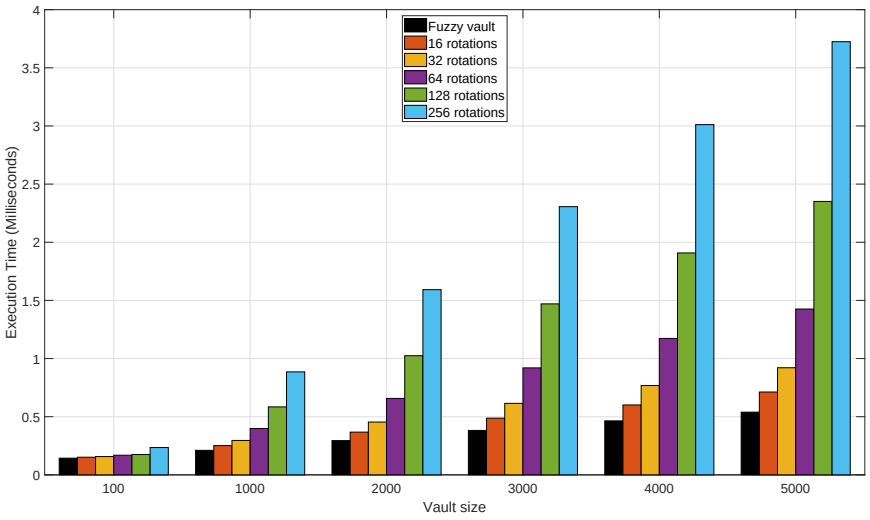
The evaluation scenario consists of running both schemes sequentially 100000 times to measure their performance for equally sized vaults. In addition to varying the vault size, from 100 to 5000, to assess its impact on the achieved execution time for both schemes, the quadrant layers (and consequently the total number of quadrants) and the number of applied rotations, relevant for RAFV only, are also varied to assess how they affect the execution time and the resulting search space. More specifically, we evaluated 3 and 4 quadrant layers with 5 different number of rotations: 16, 32, 64, 128 and 256.

Fig. 4(a) shows the time taken to construct a RAFV over many parameters: various sizes, number of rotations in addition to the time taken to construct an identically sized fuzzy vault. This figure demonstrates that the execution time for either the fuzzy vault or RAFV scheme increases in line with the vault size. With regards to RAFV, its execution time increases further as more rotations are carried out, this is expected as more quadrants are being selected for rotation and, therefore, more points are being rotated. The biggest impact on the performance for RAFV is the number of rotations carried out, for example, a 5000 point vault rotated 16 times is 5.2 times quicker when compared with a vault rotated 256 times.

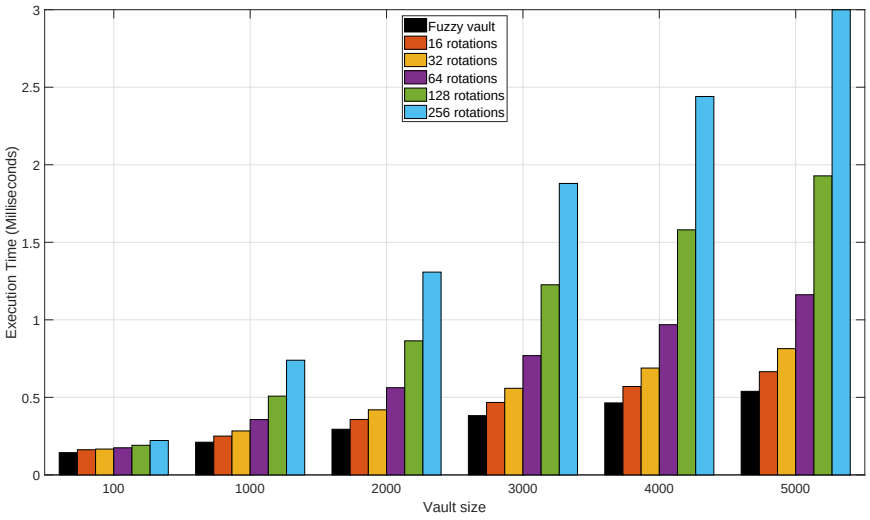
Fig. 4(b) shows the construction time for RAFV with 341 quadrants present within the vault. This graph shows that a vault rotated 256 times produces similar results to a vault with 1000 fewer points but divided into 85 quadrants (see Fig. 4(a), the case of a vault size equals to 4000). This is because the vault used for producing the results shown in Fig. 4(b) has been divided once more, compared to the vault used in Fig. 4(a), introducing an additional layer of smaller yet more abundant quadrants. These smaller quadrants are more likely to be selected for rotation as there is more of them, however, they each represent a smaller area of the vault, so if they are chosen fewer points will be rotated, which contributes to these performance uplift.

RAFV sees an increase in run time due to the extra operations it carries out on top of the underlying fuzzy vault scheme. However, this increase in execution time provides a fuzzy vault that is resilient against brute force attacks due to the rapid increase in complexity, as shown in Fig. 5 which is a plot of the Equation 1. Fig. 5 plots the function shown in this equation with various values of r (i.e., the number rotations performed). This figure highlights that a small increase in the number of quadrant rotations leads to an exponential increase in the search space. This is designed to make brute force attack infeasible due to the required time to exhaust the search space.

However, this figure shows also the search space posed by the 128-bit key which is used to derive the rotation lock pattern. Whilst the search space



(a) RAFV with 85 quadrants and varying number of rotations



(b) RAFV with 341 quadrants and varying number of rotations

Figure 4: Time taken to construct a fuzzy vault and RAFV over various sized vaults

generated using the key is many magnitudes smaller than even the smallest search space generated by the lowest number of rotations evaluated (i.e., 16), it is important to realize that RAFV is limited by this key. Although it may seem that there is no purpose for rotating beyond the limit imposed by the chosen key size, there may be advantages to picking a large number of quadrants and quadrant rotations to prevent or hinder any attempt of unlocking the vault using smart analysis techniques or efficient search algorithms. Currently, there is no known efficient search algorithm, to the best of our knowledge, that the adversary may use to rotate the vault back to its original form, therefore the security of RAFV is defined by the size of the key used.

Table I shows the obtained execution time from the performed experiments for the fuzzy vault and RAFV schemes in terms of the measured minimum, maximum, average, standard deviation and delta (the difference between average execution times for

Table I: Impact of the vault size on the achieved execution time: fuzzy vault scheme vs. RAFV (341 quadrants and 128 rotations)

	100 Points		1000 Points		2000 Points		5000 Points	
Execution Time (ms)	**Fuzzy Vault**	**RAFV**	**Fuzzy Vault**	**RAFV**	**Fuzzy Vault**	**RAFV**	**Fuzzy Vault**	**RAFV**
Minimum	0.132	0.178	0.208	0.487	0.288	0.837	0.531	1.890
Max	0.760	0.791	1.043	1.367	1.594	1.267	2.424	4.725
Average	0.144	0.191	0.213	0.508	0.295	0.864	0.540	1.928
Standard Deviation	0.005	0.006	0.007	0.014	0.007	0.012	0.013	0.026
Delta	0.046		0.295		0.570		1.388	

both schemes) values under varying vault sizes. For RAFV, the vault has been divided into 341 quadrants with 128 rotations being applied. These results reveal that as the vault size increases the average execution time increases with the delta between the two schemes increases rapidly as well. However, even with RAFV being applied to 5000 point vault it is only 1.388 ms slower than the fuzzy vault, which would not have any meaningful impact on the performance of the authentication scheme nor would the user be able to perceive such a small increase.

VI. Conclusion

Due to the exceptional increase in adversaries' capabilities, the fuzzy vault construction scheme and all BAN authentication protocols that reply on it become vulnerable to a wide range of security threats. To counter such threats, we proposed "RAFV: Rotational Assisted Fuzzy Vaults" to further enhance the security of any fuzzy vault based authentication scheme with minimum additional communication and computational overhead. RAFV extends the fuzzy vault scheme by leveraging channel side characteristics namely RSSI (Received Signal Strength Indicator) to obfuscate the locked vault by dividing it into many quadrants and rotating them following a given pattern. This obfuscation aims at preventing adversaries from using remotely captured BAN signals to unlock the vault and obtain the key concealed within it. RAFV has been evaluated against the fuzzy vault scheme and the obtained results have proven its effectiveness in enhancing the security level of the fuzzy vault scheme with a slight increase in the required computational overhead. Future work will look at what reduction can be achieved concerning the communication overhead as RAFV allows fewer chaff points to be present without sacrificing the achieved security level.

Acknowledgement

The authors are very grateful to Prof. Rene Doursat for the advice provided, for the fruitful discussions during the meetings held as part of this work and for reviewing an early draft of this paper.

References

[1] S. Movassaghi et ali. Wireless body area networks: A survey. *IEEE Communications Surveys Tutorials*, 16(3):1658–1686, 2014.

[2] M. Li, W. Lou, and K. Ren. Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1):51–58, February 2010.

[3] S. Pirbhulal et al. Medical information security for wearable body sensor networks in smart healthcare. *IEEE Consumer Electronics Magazine*, 8(5):37–41, 2019.

[4] G. Paul and J. Irvine. Ieds on the road to fingerprint authentication: Biometrics have vulnerabilities that pins and passwords don't. *IEEE Consumer Electronics Magazine*, 5(2):79–86, 2016.

[5] S. Challa et al. Authentication protocols for implantable medical devices: Taxonomy, analysis and future directions. *IEEE Consumer Electronics Magazine*, 7(1):57–65, 2018.

[6] A. Juels and M. Sudan. A fuzzy vault scheme. In *Proceedings IEEE International Symposium on Information Theory,*, pages 408–, June 2002.

[7] U. Uludag et al. Fuzzy vault for fingerprints. In *Lecture Notes in Computer Science*, pages 310–319. Springer Berlin Heidelberg, 2005.

[8] K. K. Venkatasubramanian et al. PSKA: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 14(1):60–68, Jan 2010.

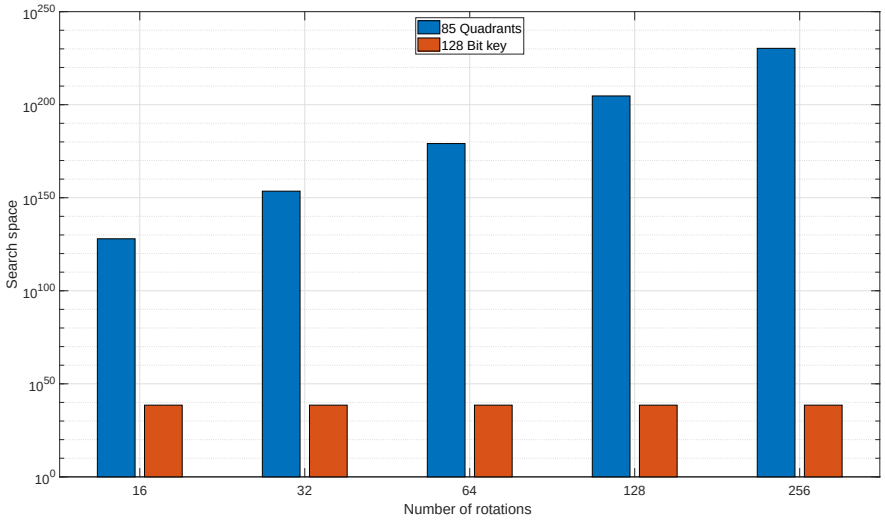


Figure 5: Evolution of search space size faced by an adversary when attempting to brute force the rotations of RAFV directly vs. the search space size generated by the 128 bit key

[9] C. Hu et al. OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. In *2013 Proceedings IEEE INFOCOM*, pages 2274–2282, April 2013.

[10] Juyoung Kim, Kwantae Cho, and Sang Uk Shin. A study on the security vulnerabilities of fuzzy vault based on photoplethysmogram. In James J. Park, Vincenzo Loia, Kim-Kwang Raymond Choo, and Gangman Yi, editors, *Advanced Multimedia and Ubiquitous Engineering*, pages 359–365, Singapore, 2019. Springer Singapore.

[11] Y. Lee et al. A novel non-contact heart rate monitor using impulse-radio ultra-wideband (IR-UWB) radar technology. *Scientific Reports*, 8(1), aug 2018.

[12] H. Zhao et al. Physiological-signal-based key negotiation protocols for body sensor networks: A survey. *Simulation Modelling Practice and Theory*, 65:32 – 44, 2016. Analyzing and Visual Programming Internet of Things.

[13] C J Harland, T D Clark, and R J Prance. Electric potential probes - new directions in the remote sensing of the human body. *Measurement Science and Technology*, 13(2):163–169, dec 2001.

[14] A E Mahdi and L Faggion. Non-contact biopotential sensor for remote human detection. *Journal of Physics: Conference Series*, 307:012056, aug 2011.

[15] Zhouzhou Li and H. Wang. A key agreement method for wireless body area networks. In *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 690–695, April 2016.

[16] Z. Li et al. Secure and efficient key generation and agreement methods for wireless body area networks. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2017.

[17] S.T. Ali et al. Zero reconciliation secret key generation for body-worn health monitoring devices. In *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WISEC '12, pages 39–50, New York, NY, USA, 2012. ACM.

Jack Hodgkiss received a Bachelor in Computer Science Degree from Manchester Metropolitan University in 2018. He now works towards a PhD focusing on authentication within body area networks. Contact him at jack.hodgkiss@stu.mmu.ac.uk.

Soufiene Djahel (M'11–SM'16) is a Senior Lecturer at the department of Computing and Mathematics, Manchester Metropolitan University, U.K.. His main research interests include Security and QoS issues in wireless networks, Intelligent Transportation Systems, and e-health. He has published more than 50 papers in top tier peer reviewed conferences and journals. Contact him at s.djahel@mmu.ac.uk.