International Journal of Cryptology Research 4(1): 84 - 101 (2013)

## Design and Implementation of Key-Policy Attribute-Based Encryption in Body Sensor Network

<sup>1</sup>Yar-Ling Tan, <sup>2\*</sup> Bok-Min Goi, <sup>3</sup>Ryoichi Komiya, and <sup>4</sup>Raphael Phan

<sup>1</sup>Universiti Tunku Abdul Rahman, Building PD No.9, Jalan Bersatu 13/4, 46200 Petaling Jaya, Selangor, Malaysia

<sup>4</sup>Multimedia University, Jalan Ayer Keroh Lama, 75450, Ayer Keroh, Melaka, Malaysia

*E-mail:* yarling@lutar.my, goibm@utar.edu.my, ryoichi@utar.edu.my and raphael@mmu.edu.my

\*Corresponding author

#### ABSTRACT

Body sensor network (BSN) is a set of sensors attached to patients' body to collect vital signs. The vital signs will be sent from patients' smart phone or personal computer via BSN coordinator to the remote healthcare provider's server. This will enable patients' vital signs to be monitored by healthcare people via internet. However, security is necessary for the patients' personal data including vital signs. The patients' personal data and vital signs are referred to as medical information. Therefore, encryption needs to be applied to patient's medical information. In this paper, we propose an implementation of key-policy attribute-based encryption (KP-ABE) in order to encrypt the medical information and present an encryption/decryption prototype system of KP-ABE in BSN. KP-ABE allows fine-grained sharing of encrypted data. It is able to provide differential access rights for different users. Thus, the encryption allows flexibility in changing access rights of individual users over the encrypted data.

#### **1. INTRODUCTION**

The current technology has brought remarkable contribution and advancement to the electronic healthcare devices today. The advancement of electronic healthcare devices is essential for monitoring and early prevention of various diseases such as heart diseases, diabetes, hypertension, chronic obstructive pulmonary disease (COPD), and other chronic diseases.

Body sensor network [1-4], is one of the smallest personal electronic healthcare networks which has been studied and tested its availability all over the world. Body sensor network (BSN) is composed of wearable computing device with a set of sensors attached to different parts of human body to collect vital signs. The vital signs to be collected are body temperature, blood pressure, pulse rate (or heart rate), respiratory rate and etc. BSN is a wireless network that enables sensors to send the vital signs to mobile computing device (e.g. smart phone) or a computing unit via BSN coordinator. Then they will be sent to the third party remote server to be stored. In this way, patient can be monitored in real time or non-real time basis remotely from the hospital [5].

The medical information stored at the remote server will be shared among different users (e.g. doctors, nurses, pharmacies, patient and etc.). Thus, privacy, confidentiality and security issues for the medical informationshould be a major concern in this topic. Therefore, it is important for the medical information to be encrypted before sending to the third party remote server. Encryption is one of the potent approaches to secure medical information. Many research works have been done in order to secure the medical information of the BSN [6-10].

Attribute-based encryption (ABE) [11-14], is a fine-grained access control system, which enables a set of users to have differential access rights. On the other hand, ABE is also flexible in defining the access rights of each user. There are two major types of ABE; key-policy attribute-based encryption (KP-ABE)[15-16], and ciphertext-policy attribute-based encryption (CP-ABE) [17-19]. In this paper, we propose an implementation of KP-ABE scheme to apply the encryption to patient's medical information. KP-ABE encryption time is shorter than CP-ABE. Besides that, KP-ABE has less restriction and limitation on the authorized users who are able to apply decryption to the encrypted medical information. Authorized user (e.g. medical operator) is able to perform decryption if his/her access policy matches the attributes assigned to the encrypted vital signs. In hardware implementation, KP-ABE is also advantageous. KP-ABE scheme is able to realize the lightweight encryption and producing smaller ciphertext size than CP-ABE in a resource constraint device [20]. We have implemented a prototype which is composed of BSN to collect vital signs from human body and a laptop to perform the encryption/decryption of patient's medical information.

## 2. BACKGROUND

In 1984, Shamir introduced a novel type of public encryption scheme called Identity-Based Encryption scheme (IBE) [21], which enable users to securely communicate, verify and exchange each other's signatures without any exchange of private or public keys. Thus, eliminates the need to keep key directories. Instead of generating a random pair of public/secret 85

International Journal of Cryptology Research

key and made the public key known to everyone, the public key can be in a form of any arbitrary string. For example, names, home address, phone number, e-mail address and etc. provided that the user can be uniquely identified which he cannot later deny. In year 2001, Boneh and Franklin proposed the first secure and practical IBE [22] from the Weil pairing on elliptic curves.

In 2005, Sahai and Waters introduced a new type of IBE scheme called Fuzzy Identity-Based Encryption (FIBE) [23]. In IBE, identities are viewed as arbitrary strings. While in FIBE, identities are being viewed as a set of descriptive attributes. FIBE scheme allows a user with private key corresponding to a set of identity, *ID* to decrypt a ciphertext encrypted with the public key, *ID'* if and only if *ID* and *ID'* overlap each other by some distance metric, *d*. Therefore, FIBE system allows a certain amount of error-tolerance in the identities. The authors also mentioned on the application of FIBE termed as Attribute-Based Encryption (ABE). In an ABE system, a user's private key and ciphertext are labeled with a set of attributes. A particular private key can decrypt a particular ciphertext only if there is a match between the attributes of the user's private key and ciphertext.

After ABE was first introduced in the work of Sahai and Waters, in year 2006, Goyal et al. proposed the Key-Policy Attribute Based Encryption (KP-ABE) for fine-grained sharing of encrypted data [15]. Encryption of data usually limits the ability of encrypted data to be shared among different users. In other words, the encrypted data can only be selectively shared at a coarse-grained level. For example, in order to perform data decryption, user needs to give his/her private key to another party. This somehow allows another party to have all the access of the user's data. Another alternative, user can act as an intermediary to perform decryption on the relevant data but this method is arduous. Both approaches are not appealing as they are impractical and inefficient.

In KP-ABE, each ciphertext is labeled with a set of descriptive attributes, while the access structure is embedded in the user's private key. User is able to decrypt a ciphertext if the access structure embedded in the private key matches the descriptive attributes labeled in the ciphertext. Finegrained sharing of encrypted data enables different authorized users to retrieve and decrypt ciphertext based on their access structure. KP-ABE scheme is able to grant different access rights to different users.

In year 2007, Bethen court et al. provides the first construction of a ciphertext-policy attribute-based encryption (CP-ABE) scheme [17]. In 86 International Journal of Cryptology Research

CP-ABE scheme, access structure is use in data encryption while the descriptive attributes are embedded in the user's private key. A user is able to decrypt the ciphertext if his descriptive attributes satisfy the access structure associated to the ciphertext. Table 1 summarizes the terminology definition in this section.

Terminology	Definition	Example
Attributes	Identities of a person	Name, home address, e-mail address, identity number, phone number
Access Structure	A policy/structure to define an authorized person	{("Dept of Medical Services" AND "Specialist") AND ("Kuala Lumpur" OR "Penang") OR "Name: Dr. Jehovah"}
Private Key Generator	A trusted third party that handles the issuance of private keys	

TABLE 1: Terminology List
---------------------------

# **3. IMPLEMENTATION**

This section shows the implementation of our work. This section is divided into a few subsections; body sensor network, attribute-based encryption scheme, and our prototype setup.

## 3.1 Body Sensor Network

BSN is applicable to healthcare, well-being monitoring, sports and entertainment [24-26]. Different activities require different set of sensors. In our work, we focus on the healthcare applications by using BSN. The needs of healthcare applications are emanate from the increase of chronic diseases, aging population and early diseases prevention and detection.

BSN for healthcare application is dynamic. It can be used at anytime, anywhere and for anybody. It provides continuous medical information collections and transmissions on real time or non-real time basis to hospital server which helps the hospital personnel to diagnose the patients outside the hospital.

International Journal of Cryptology Research

#### Yar-Ling Tan, Bok-Min Goi, Ryoichi Komiya & Raphael Phan

The BSN which we have implemented has four major components which are the processor, radio frequency transceiver, battery and sensor. It is designed to have three modules. The three modules are battery, sensor and BSN node. The BSN node consists of processor and radio frequency transceiver. The BSN is a stackable design to connect and interface between the modules. We have implemented two types of body sensor nodes which measure temperature and 3D motion. The BSN node can transmit and receive vital signs within the range of approximately 50 meters indoor. Figure 1 shows the body sensor node manufactured by Sensixa Ltd. Company[27].



Figure 1: Body Sensor Node

#### **3.2 Attribute-Based Encryption Scheme (ABE)**

Comparisons between KP-ABE and CP-ABE schemes are studied and analysed to determine their propriety in BSN [11]. Comparisons were conducted in terms of encryption efficiency/time, attribute and access structure's assignment, access control and hardware implementation.

In our work, we have intended to achieve a lightweight and secure encryption. In KP-ABE, encryption is performed by using descriptive attributes. Access structure is embedded in the private key which is issued by private key generator (PKG). In CP-ABE, encryption is performed by using the access structure. Descriptive attributes are embedded in the private key issued by PKG.

Encryption performs by using descriptive attributes has lower encryption complexity and shorter computation time than encryption to be performed by using access structure. Moreover, medical information is being encrypted at a continuous basis, while key generation for each authorized users is being generated once. Therefore, KP-ABE encryption scheme is more appropriate to be implemented in our work.

International Journal of Cryptology Research

Patients are involved in the assignment of descriptive attributes or access structure with the assistance from medical agents. Assignment of descriptive attributes in KP-ABE for encryption purpose is much simpler and less time consuming than assignment of access structure in CP-ABE encryption. This is because a slight update mistake in the access structure would cause a complication in the entire encryption and decryption system.

Furthermore, in terms of access control, KP-ABE allows higher flexibility and efficiency in the modification of access control towards any authorized personnel compared to CP-ABE. This is because the updates made on the descriptive attributes are much simpler than updates made on access structure.

In KP-ABE, the encryption time is shorter and ciphertext size is smaller than CP-ABE. This is because the high complexity and processing work to embed the access structure in private keys are done by the PKG. However, for CP-ABE, the encryption computation time is longer and the ciphertext size is larger. Therefore, in terms of hardware implementation, KP-ABE is advantageous.

For our prototype, we have implemented the KP-ABE scheme as this scheme is more suitable than CP-ABE in terms of light weight and less power consumption [11]. In KP-ABE scheme as shown in Figure 2, attributes are labeled in the encrypted medical information (vital signs and patient's personal data). Access structure is embedded in the private key. The private key is issued by a trusted private key generator (PKG). This is an advantage of KP-ABE scheme where attributes label in the encrypted medical information can be easily created and altered. The tedious task of access structure creation and alteration is handled by professional PKG creator.

The KP-ABE scheme consists of four algorithms [15].

- Setup (1<sup>k</sup>): The setup algorithm takes as input a security parameter, 1<sup>k</sup> and outputs the public parameters, *PK* and a master key, *msk* which is known only to the private key generator (PKG).
- Encrypt (m, PK, γ): The encryption algorithm takes as input a message, m, a set of attributes, γ and the public parameters, PK. It outputs the ciphertext, c.

International Journal of Cryptology Research

Yar-Ling Tan, Bok-Min Goi, Ryoichi Komiya & Raphael Phan

- Key Generation (*PK*, msk, ): The key generation algorithm takes as input the public parameters, *PK*, the master key, *msk* and an access policy, . It outputs the private key, *D*.
- Decrypt (c, PK, D): The decryption algorithm takes as input the ciphertext, *c* which was encrypted under the set of attributes,  $\gamma$ , the public key parameter, *PK* and the private key, *D* for access control structure, . It outputs the message *m* if  $\gamma \in$ .

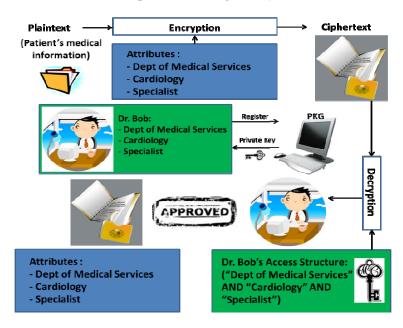


Figure 2: Key-Policy Attribute-Based Encryption and Decryption

## 3.3 Prototype Setup

We have attached the sensor nodes to the human body as shown in Figure 3 to collect temperature and 3D motion readings. The readings are transmitted to the BSN coordinator which is connected to a personal computer (PC). In the PC, KP-ABE encryption and decryption is performed.

International Journal of Cryptology Research

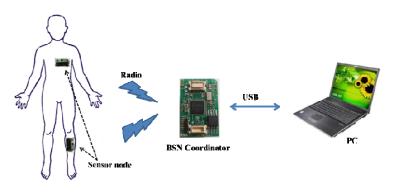


Figure 3: Prototype configuration

# PC:

Send commands to, and receives vital signs from the BSN-network. Encrypt the vital signs using KP-ABE encryption.

#### **BSN-coordinator**:

Receives commands from, and sends vital signs to the laptop.

### (i) Connection between BSN nodes and BSN coordinator

Vital signs are sent from sensor nodes to the BSN coordinator via radio transceiver – CC2420, as shown in Figure 4. The CC2420 is a single-chip 2.4 GHz IEEE 802.15.4 compliant RF transceiver with an effective data transfer rate of 250 kbps. It is designed for low-voltage and low-power wireless RF applications. The CC2420 provides hardware support for AES-128 based data encryption and data authentication.



Figure 4: BSN-Network

International Journal of Cryptology Research

#### **RF Transmitter:**

Toggles the red LED and send the vital signs in packet. Each packet contains a sequence number in the packet header, which increases by one after a packet is sent out.

#### **RF Receiver:**

92

Toggles the red LED and receives data packets sent from RF Transmitter and check their sequence numbers in the packet header.

#### (ii) Connection between BSN coordinator and PC

Vital signs sent from the sensor nodes will then be received by the BSN coordinator and be transmitted to the PC via universal serial bus (USB) as shown in Figure 5. In order to collect the vital signs, PC first sends out a request. The BSN coordinator will then transmit a message to all the BSN sensor nodes or only to the selected sensor nodes. When the BSN sensor nodes receive the message, they will then transmit the vital signs to the BSN coordinator. After that, through the USB connection, the PC will receive the vital signs. The number of nodes can be altered accordingly to accommodate the number of vital signs types require to be collected.

In our work, BSN sensor node 1 will retrieve the human body temperature, and BSN sensor node 2 retrieves the 3D motion of human body.

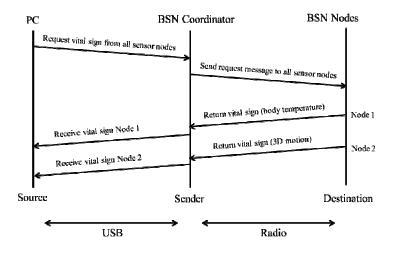


Figure 5: Connection between PC, BSN coordinator and sensornodes

International Journal of Cryptology Research

#### **3.4 KP-ABE Encryption in PC**

Once the vital signs are sent to the PC, the PC will perform the KP-ABE encryption on the vital signs. In our implementation, we used the key-policy attribute-based encryption library (*libcelia*). It is a subroutine library implementing KP-ABE scheme and kpa be toolkit created by Yao Zheng [28].

Figure 6 illustrates the process flow of the encryption and decryption. Figure 9shows the screenshot of correct encryption and decryption.

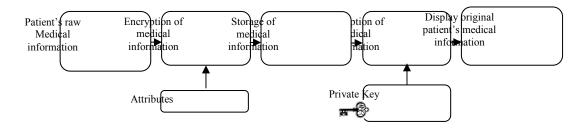


Figure 6: Diagram of Process Flow of Encryption and Decryption

- *kpabe-setup* : The setup algorithm generates system parameters, a public key, and a master secret key under set of attributes.
- *kpabe-enc*: Encryption algorithm encrypt medical information of patient under a set of attributes.
- *kpabe-keygen*: The key generation algorithm generates a private key and sends to the authorized medical operators.
- *kpabe-dec*: The decryption algorithm takes as input the encrypted medical information under a set of attributes, the public key parameters and the private key generated by kpabe-keygen. It then outputs the message original file if access structure embedded in the private key matched the attributes.

#### 4. RESULTS OF EXPERIMENT

Section 4 shows the results of the experiment. The results shown are correct encryption and decryption as well as the incorrect encryption and decryption. We show 2 types of incorrect encryption and decryption; decryption using incorrect key and decryption using incorrect wording.

International Journal of Cryptology Research

## 4.1 Correct Encryption and Decryption

#### **Original Data**

#### Encryption

Onginari	Pala
1226.0, NaN, 1835.968017578125, 60161.	0,1735.0,NaN,1885.0,NaN,
1216.0, NaN, 1935.577392578125, 63425.	0,1759.0,NaN,1858.0,NaN,
1213.0, NaN, 2035.186767578125, 1153.0	,1767.0,NaN,1885.0,NaN,
1222.0, NaN, 2134.796142578125, 4417.0	,1742.0,NaN,1879.0,NaN,
1229.0, NaN, 2234.405517578125, 7681.0	,1758.0,NaN,1890.0,NaN,
1231.0, NaN, 2334.014892578125, 10945.	0,1752.0,NaN,1875.0,NaN,
1230.0, NaN, 2433.624267578125, 14209.	0,1753.0,NaN,1891.0,NaN,
1217.0, NaN, 2533.233642578125, 17473.	0,1736.0,NaN,1876.0,NaN,
1231.0, NaN, 2632.843017578125, 20737.	0,1770.0,NaN,1888.0,NaN,
1207.0, NaN, 2732.452392578125, 24001.	0,1745.0,NaN,1893.0,NaN,
1213.0, NaN, 2832.061767578125, 27265.	0,1765.0,NaN,1889.0,NaN,
1235.0, NaN, 2931.671142578125, 30529.	
1213.0,NaN,3031.280517578125,33793.	
1224.0,NaN,3130.889892578125,37057.	
1219.0,NaN,3230.499267578125,46321.	
1216.0, NaN, 3330.108642578125, 43585.	
1215.0,NaN,3429.718017578125,46849.	
1212.0,NaN,3529.327392578125,50113.	
1220.0,NaN,3028.930707578125,53377.	
1222.0,NaN,3728.546142578125,56641.	
1214.0,NaN,3828.155517578125,59905.	
1221.0,NaN,3927.764892578125,63169.	
1216.0,NaN,4027.374267578125,897.0,	
1203.0,NaN,4126.983642578125,4161.0	
1214.0,NaN,4226.593017578125,7425.0	
1227.0, NaN, 4326.202392578125, 10689.	
1221.0,NaN,4425.811767578125,13953.	
1218.0,NaN,4525.421142578125,17217.	
1218.0,NaN,4625.030517578125,26481.	
1234.0,NaN,4724.639892578125,23745.	
1201.0,NaN,4824.249267578125,27009.	
1228.0,NaN,4923.858642578125,30273.	0,1753.0,NaN,1878.0,NaN,
Private K	lev
1 111 000 11	

Private Kcy gAN9cQAcMAYAABbb2xpY3LxAVgYAAAAKChPTkUgb3IgVFdPKSBhb@Qg VehSRuupcgJYwaAABbb2xpY3LxAVgYAAAAKChPTkUgb3IgVFdPKSBhb@Qg V2daU5tvRFhBK1HzK0WLe1pRekJHTU2CQ1F4X3VDMVV2bFVMVhkbV3E QMLLeDduQncxbnFCekpNsy92dFZuHX3VTLVVUUUSQFWAVhkbV3E WISANIRYHF1REY5bXVSbNVeE1C2Csx2LbvsGJhan9EUndLQuheeV2C Ty80MKAwbms179EEXJbXFSbNVeE1C2Csx2LbvsGJhan9EUndLQuheeV2C Ty80MKAwbms179EEXJbXFSbJLETBUWTRHdnV3SXB5CmNSY3dBPXEC ZygAaAAxFLSTVSJLXChONJ B6VKLWSZTHZTM7XTb0No2CIXvVRM Tk2zbCSsWcTTVLHSYStSJA4VLwv2LV1CudCHD043gFTLB445epqa5J2 R2FUT3WCJMUMP13Ha40S1BFME2Cd113s5n23BR713xCnVVAAAA RXT3ELXCRMEKNAMTpE4TVDRHb12C0VFCzd113s5n23BR713xCnVVAAAA RXT3ELXCRMEKNAMTpE4TVDRHb12C0VFCzd113s5n23BR713xCnVVAAAA RXT3ELXCRMEKNAMTpE4TVDRHb12C0VFCzd113a5n23BR713xCnVVAAAA PXT3EJXCRMEKNAMTpE4TVDRHb12C0VFCzd113a5n23BR713xCnVVAAAA PXT3EJXCRMEKNAMTpE4TVDRHb12C0VFCZd113A5n23BVC22FF1BKE0 BEFHTNT5TVPURCHWB5SWGDLB713 UVG52MWCHWB5SUUDURB12C0VC22FF1BKE0 BEFHTN5TVPURCHWB0LWBABKB1FF23GGF5VULAYKRRE1nTFp25HNQ QStXd09BQ4kVZFKBUDNLH3KSNB1FAJ

LUFFFPXF07XUu

cch1citLeteig10.4it/gtx2ccF244.jh08Hx4uvHz5g0bweH1.0UVTd1hchz2cfLUkckti WrXpU04ecd01bt152vht8L10Lc010UX3y6vHX2tN1V34dUH025UFd12k2025 Zkpkan_hnt2F2Vht8Vx1neU30Hatf12k20114000450F418412005205205205205205205205205205205205205	gAN9cQAoWAIAAABjMnEBfXECKFgDAAAAbXNncQNYyR8AAHsiQUxHIjogMCwgIkNp
Likokana JINK2F EVIYWHI JIXV ZIGHU JIIMBAL TDJ (JAIN LEVEK'D ANT OVI KROVICE HARZL HEB (DI) KLI JIAKA JIKI FY JAIS BINNI JIAJ JIAKA	
<pre>(n)tota.Rckd.NLFyakSBM01.DF3bEt12jYtsSMBHFVTSK21QUBBS1dwVHC3dH) S3tutdEUB9Nkd8d2HT234VAMBhpT3bbUKK2,DL621zCa2NCvTSTUD2L4A MeijYULKQ3pka128x2V9ThK5x4VB5ytBAxCeE1r42poendle460HT3cTUbdkg6 HstactsSL7mB14kii,Ytg2yDUH07bUH07b4FVL68kx2L512F22B50HT3cTUbdkg6 HstactsSL7mB14kii,Ytg2yDUH07b4FVL68kx2L512F22B50HT3cTUbdkg6 V23a221L337zT17dK4gEL38kx3CETUB42V5(14NL)THHT80gE3M194MU55HF53V7 HstUSUB80F09CH181d60V2:C2DUB6D5;FChNF48kV52G4ML)TAST2d65MEU 25d4CFT1b620h47B4x2L68Ht5427L1522ME13NQuLC51bKF41J3a51cx4V1X5Hg70UF FT13b620h47B4x2L68Ht5427L1522ME13NQuLC51bKF41J3a51cx4V1X5Hg70UF 51d4CFT1b620h47B4x2L68Ht5427L1522ME13NQuLC51bKF41J3a51cx4V1X5Hg70UF 51d4CFT1b620h47B4x2L68Ht5427L1522ME13NQuLC51bKF41J3a51cx4V1X5Hg70UF 51d4CFT1b620h47B4x2L68Ht5427L1522ME13NQuLC51bKF41J3a51cx4V1X5Hg70UF 51d4CFT1b64h47B4x2L68Ht5427L1522ME13NQuLC51bKF41J3a51cx4V1X5Hg70UF 51d4CFT1b64h47B4x2L68Ht5427L1522ME13NQuLC52D575VF70g80F100H354200H 51d4CFT1b64h47B425L28Ht5427L1522ME13NQuLC52D575VF70g80F10H34528020 51d4CFT1b64h47B425L28Ht5427L1244F5427L548854016427E1D52052M2472F3 51d4CFT1b64h47B425L28H542000H54210497544844548016427E1D52052M2472F3 51d4CFT1b64h47B42542B542000H5421049754484454425428044544212402424243444544444444444444444444444444</pre>	
Sastukztuupenkidödzilt 72334/vinhip fühilubiki.2 på Let 126 30/vin 5110/2144 enkiy TUES,3 på kää Zäkky Tinkskörkälles jä på kää Cirk vappendile köhön Tää Undekjä Neisen 25 12 million taaki Zäkky Tinkskörkä Kää Kää Kää Kää Kää Esimeri Valka Valka Kää Kää Kää Kää Kää Kää Kää Kää Kää Kä	
Inity TUE KQ Dje AL 2014 (Jy TrikSK 2015 Syr Jehks CE, ET Y 20 poord Bel-BOIT 3 (TURH signal Field System) (BOS ALL SYSTEM	
HEbickSS Lävikb 314kkl, 192ppJ21 ufbyva6Fnkl, 086ikcJLLsza La bF21d 69MEL[0 EI 2bm2UN90gwldW ILEXENUTCHEM 20005C14NU JIHHEGOE 3NI 94MLs 59HEF3 yf HEBICJBIOEDDWSgeldW ILEXENUTCHEM 20005C14NU JIHHEGOE 3NI 94MLs 59HEF3 yf HEBICJBIOEDDWSgeldW ILEXENUTCHEM 20005C14NU JIHHEGOE 3NI 94MLs 59HEF3 yf HEBICJBIOEDDWSgeldW ILEXENDS JOB 300 STAFF 50H AND 59HEF3 yf HEBICJBIOEDDWSgeldW ILEXENDS JOB 300 STAFF 50H AND 59HEF3 yf HEBICJBIOEDDWSGELW ADDWSGELW ADDWSGELW 2000 STAFF 50H AND 59HEF3 YF HEBICJBIOEDDWSGELW 2000 STAFF 50H AND 59HEF3 ADDWSGELW 2000 STAFF 50H HEBICJBIOEDDWSGELW 2000 STAFF 50H AND 59HEF3 ADDWSGELW 2000 STAFF 50H HEBICJBIOEDDWSGELW 2000 STAFF 50H AND 59HEF3 ADDWSGELW 2000 STAFF 50H HEBICJBIOEDDWSGELW 2000 STAFF 50H AND 59HEF3 ADDWSGELW 2000 STAFF 50H HEBICJBIOEDDWSGELW 2000 STAFF 50H AND 59HEF3 ADDWSGELW 2000 STAFF 50H F30H AND 59HEF3 ADDWSGELW 2000 STAFF 50H AND 59HEF3 ADDWSGELW 2000 STAFF 50H F30H AND 59HEF3 ADDWSGELW 2000 STAFF 50H AND 59HEF3 ADDWSGELW 2000 STAFF 50H F30H AND 59HEF3 ADDWSGELW 2000 STAFF 50H AND 59HEF3 ADDWSGELW 2000 STAFF 50H F30H AND 59HEF3 ADDWSGELW 2000 STAFF 50H STAFF 50H AND 50H AND 50H F30H AND 59HEF3 ADDWSGELW 2000 STAFF 50H STAFF 50H AND 50H AND 50H F30H AND 59H AND 59H 57H F40H AND 59HEF3 ADDWSGELW 2000 ADDS 50H AND 50H F40H SHQ 1000 ADDWSGELW 2000 ADDWSGELW	
TEJDRUZYUBZWUBGHUT IKE-KYULLEWI ZQUUBÇKJSUK DSAKTNTEN YTT. EN YTT. EN HUTUT VEGUJABZE JIZI TI KANGEL BINA JSOTBVSCI EUN UTHARISO EIN YTAMUS SHET SYN KESUJABROBOCKUT RUGOV SCZ LOBENDS JF. CHINSKIK YSGG WILLUT ESMENT YEL 1254 deligi VILMARGUIZABZE JZZEME 111 QUUCLE UMARISO JEL IS YANIS SHET SYN ET JIAO DING FINESAL BINNEY JANY ZESTMI LI KOLIVIT GUY ZEBUZ LI SAZBALT LI SALEN TI, KOLING JALING YSGU ZI KUNCKOON SIN YKON YKON JANIS JALING YKON SILVEN TI KOLING JALING YSGU ZI KUNCKOON SIN YKON YKON JALING YKON SILVEN TI KOLING JALING YSGU ZI KUNCKOON SIN YKON YKON JALING YKON SILVEN TI KANA JALING YKON YKON YKON YKON YKON YKON YKON SILVEN YKON YKON YKON YKON YKON YKON YKON YKO	
evg3a271L33721T14044464E334H330T8V5CL34W13TH4HE306E31N194MU55SHEr53YT HE3UQJ80690240HTR Ld00:X52 L00Eh055/FL01K84V55G4MU175SHC724F3 H2246H191YL1M9492L48A7F1L527ME11N3Qu1C81LM84V5G4MU175SHC74F3 H2246H191YL1M9492L48A7F1L527ME11N3Qu1C81LM84V5G4MU175SHC74F3 H2146T1048453L439H5590752140487400579479405902527292425615444504270178 H2146T1048744243542642711242475217428789U16C40FbC106784784444 H225H2274734Ny8Fc42893C57211244755274857801624756106748752444 H225H227473446245405647112462450467447915285481926428561244420427477841 H21467111240H486434424741525747444444444444444444444444444	NENxK25iZHRBb3I4WkljN2ppU2luRVpva0FmVkl0S0kzWlIxZnI1bFZId05MNElQ
HEEDQISRORBOPCHIMT KIDDOV SCZ LOBENDS /FCNRSKIN CYSCILWAM LUT ESMETY ÉLI KZSAMBIGY UTYMAPUZIKAPZI LZZMENI SI NQULEV LUKAY LI SA SCALIWA CYSAMBIGY UTYMAPUZIKAPZI LZZMENI SI NQULEV LUKAY LI SA SCALIWA UTYMAPUZIKAPZI KANA SCALIWA SCALIWA SCALIWA SCALIWA SCALIWA SCALIWA UTYMAPUZIKAPZI KANA SCALIWA SCALIWA SCALIWA SCALIWA SCALIWA UTYMAPUZIKAPZI KANA SCALIWA SCALIWA SCALIWA SCALIWA SCALIWA SCALIWA UTYMAPUZIKAPZI KANA SCALIWA	TEJDMUZhVU9XU0gwdUFlNExKYUtEeWFzQVU0QXJsUkpSakFNTEN4Ymt4Wm16WUVt
R23-648831711 STATURADULTARASZTIL SZZNIET INIĞULCI B.IMK-INI J.AS.I.C.YMIZ SINGZOUFF   R23-648171 STATURADULTARASZTIL SZZNIET, INIĞULCI B.IMK-INIĞULTARU J.AS.I.C.YMIZ SINGZOUFF   SLIJA-C.TILĞÜRMANDJ.B.AZĞARASZTON ZZ SUKKANOD SYLVI PONIQT TEIDEN DI B.Z.B.C.M.I.D.S.F.G.Z.B.C.M.I.D.S.F.G.Z.B.C.M.Z.T.M.S.F.G.Z.B.C.M.Z.F.G.Z.S.F.G.Z.Z.F.G.Z.F.G.Z.Z.F.G.Z.F.G.Z.Z.F.G.Z.Z.F.G.Z.Z.F.G.Z.Z.F.G.Z.F.G.Z.Z.F.G.Z.Z.F.G.Z.Z.F.G.Z.Z.F.G.Z.Z.F.G.Z.Z.F.G.Z.Z.Z.F.G.Z.Z.F.G.Z.Z.Z.F.G.Z.Z.Z.F.G.Z.Z.Z.F.G.Z.Z.Z.F.G.Z.Z.Z.F.G.Z.Z.Z.F.G.Z.Z.Z.Z	
ert Jmcs Toleman Heizen, Laammer, mer zez servi il vebir rour zennue til sa zehsen i foa simu Especit hij (Karlindi sa zabyta 30000 tizi duk occoord Sirvi Pennie truppen Beck Liubevon Um heiner gert zurmeinteurt mitzen giv ji nearly trens vup esvizez zis el ja lattous vur tin ka Veluti Wick Rail Sa zabyta 30000 tizi duk occoord Sirvi Pennie truppen Beck Liubevon Versten Sirvi Pennie Sirvi Pennie Sirvi Pennie Sirvi Pennie Tennie Sirvi Pennie Tennie Sirvi Versten Sirvi Pennie Sirvi P	
slpecthlqkRnudSia2dqk33600V32LdUkdxx00F3VTP0nqFTUprd]RebUtubdvg UThPbrFq732VTpmRUTTAEQUYJRX7F83VL 45UUVMXR3dJYVdzKX9S52TIdzeVF1b2Y1KX85UbLCGNPbCLncM6VYFEAbbd 222r8t223F12A950KprC42b2CC-0x42TVEdAv0K1UBKd2UF2abbd2LLUK1EV600 RV3eC21baCvTTn12dCKd0deCkEbU6E43LExtEdv125h1btFTTrVDsUbmc7Dr0250 RV3eC21baCvTTn12dCKd0deCkEbU6E43LExtEdv125h1btFTTrVDsUbmc7Dr0250 RV3eC21baCvTTn12dCKd0deCkEbU6E43LExtEdv125h1btFTTrVDsUbmc7Dr0250 RV3eC21baCvTTn12dCKd0deCkEbU6E43LExtEdv125h1btFTTrVDsUbmc7Dr0250 RV3eC21baCvTTn12dCKd0deCkEbU6E43LExtEdv125h1btFTTrVDsUbmc7Dr0250 RV3e22pf22b12b2F52b2F52b2F52b2F52b2F52b2F52b2F52	
Uninburg vir 22 romentuur in taceg vir gleany refers vuo pesso zaise is ju kaietous vuo this ey tuuliseks 2014 vir 24 konstantiise van en	
eyetUvukki 33 (Yvúzki 28) scóre (Tidzev Fibry HXKB9Ub) COUPDCI nevMOYXEE Alake ezzetezzi a Takinger cickyoo Ccenter Viet denovi Urakid azur sangabe Lisutiet verba Rivelez Uba Gevinni Zaket Alaket Alaket Alaket Alaket Alaket Alaket Alaket Alaket Alaket Alaket zakit Tinkis etti Lindohendi Alaket Alaket Alaket Alaket Alaket Alaket Alaket Alaket Alaket zazit Lindohendi Alaket Alaket Alaket Alaket Alaket Alaket Alaket Alaket Alaket Alaket zazit Lindohendi Alaket Alak	
122 zmr23 at 73 kypie relignoct. Con N42 TVE denovin Lusiki dzazu sawącka LELURUT w opie trow ce 21 kadro tra 26 dc con 6 dc 21 po 20 rm Tm 25 strait 10 rm 26 kwa 10 po 20 rm 26 km 26	
INVACE2 UhaGVT/h12dCKzdo/e6cksu02642a1Ert dovj 25ExtrahjEGORI3 JARZCXBJ str.Thristr II. Johnembal JOHO CS21.pj OhT-h1123 ThL H17TH/JCHABVC TOMB/CTM2264 220 Lingd(hpac/LVM (dody/Mn/MVGUJJBK) (1RM2.JGL CMB 1pc/UbX/THZYF)0 LJ322 R6b1 Fh5/VIX.HIS SZYK CERME CTF.VKISWI LHINK Lusg/d222.VIZ.FHL LUBAZ FB0 H15/VIX.HIS SZYK CERME CTF.VKISWI LHINK Lusg/d22.VIZ.FHL LUBAZ FB0 H15/VIX.HIS SZYK CERME CTF.VKISWI LHINK LUSG/USZ/LIX.HIS LUS/VIX. cn (LDBpndEpHI dsAFZL C2NVDI 5 ThXZZDF LID LIVUX/VIX.HINK LIVV.SYK z SSIK LHNOST davGD NIL VVX.VKISMI LZ ZKK VXIX.HIS LIVV.D3 zZ SIK LHNOST davGD NIL VVX.VKISK LIVX.HIS LIVX.HIS LIVX.JSZ LIVX.HINK LIVX.HIS LUBAZ VXIX.HINK LIVX.HINK LUSZ/KZCZDF JUD ZZ ZKK LIVX.HINK LIVX.SFG ZKK SGK RKASHJ V0RGO VXIZ.SGK JVG VXIX.HINK LIVX.HINK LIVX.JSZ GKZ SGK LIVX.HINK LIVX.HINK LIVX.HINK LIVX.HINK LIVX.JSZ GKZ SGK ZKK ZKK SGK ZKK SGK ZKK SGK ZKK SGK ZKK SGK ZKK ZKK ZKK Z	
Inst Time Structure The Standard Structure The Standard Structure	
azd Lappdkpac U kni dudownomou Jujesný cznob z Joči Zoma Jočubs Zirvy F Jo Lista Zara Bób Freb Stvuk XII SSX Vice Centor Christik SSU U Linku Luka J doče Zule Zirvi I u Ulav Zir dlu J Juči Zi U Janki I Sa I Se Jel Povrt i krine Ji u cji Nuj Zi Jařov Mivi Jan Ko Joři V Vir pro z Viz Kobi Trakvil I Liub Lavi Zi Za Vjezi An Kolupital K Hoti SY Lo Janu Kobi Joři V Vir pro z Viz Kobi Trakvil I Liub Lavi Zi Za Vjezi An Kolupital K Hoti SY Lo Janu Kobi Joři V Vir pro z Viz Kobi Trakvil I Liub Lavi Zi Za Vjezi An Kolupital K Hoti SY Lo Janu Kobi Joři V Vir pro z Viz Kobi Trakvil I Liub Lavi Zi Za Vjezi An Kolupital K Hoti SY Lo Janu Kobi Joři V Vir SV La Viz Kobi Kobi V Viz Kobi Kobi Kobi Kobi Kobi Kobi Kobi Kobi	
L3d2zP6b3E7bb2FxVL3NC55VFCCFPR0CTh7VKSVULHUNU,MIZ/d0Z2VFZ2H1L UMWZ7g1dU3UZCYUJANK5SISBSC4FVCVFLACHCD3UG/b1U2/g2APhv3Hv3dy WExp01VCxpNH23VFYSTNFTHA3MKUxcPBNaK5x2tE20U3KEVB0JIK5T4V3MX K0xj0FVVYPVCVZXK09ETCh4VIII UD134V2/g24/g24/sM1K0jNPd14H07NV13UJUQ cnl0bnpdEpyRldsF2LC2XW0F3ThkZZEFLU0IWVUXUERUUNK7T3K5KVVD3YX a25Ukth805Tb4MC2NULMVUXUU7UKAUSDNPACF000x2U3ZeEUUVUXUU SUSUK10505Tb4MC2NULMVUXUU7UKAUSDNPACF000x2U3ZeEUUVUXUU 200000000000000000000000000000000000	
IUIIba2Tg1 dU3 2UL2TQU30HK1 SB TEASUF0CVT dK cnc 3) Lc [1 LU] ZyaFhv1 Shv1 ydf UKcg) DK VCPB ZyMF5 XIFF YN THA XIAU AC BHABK ZK 12 EQ01 SBK1 ZW 2ULFS THA YBK1 KG JGYVYTPJK C'Y2 KOB CT TKVI LI UD1 24K2 J 24 yc 3H KIGJPB LHOD XY1 J 3HUJP CIL DBynd Egy KL 45 FL C2 XWH1 I UD1 24K2 J 24 yc 3H KIGJPB LHOD XY1 J 3HUJP CIL DBynd Egy KL 45 FL C2 XWH1 I UD1 24K2 J 24 yc 3H KIGJPB LHOD XY1 J 3HUJP DF XH 45 YL 45 FL C2 XWH1 I XW1 ZH 24 XW1 ZH 2	
HELPOTI V. CAPHED VIETYS TINFTHA SIMULACEBNIK AZ L 12000 SSLEDBALLRST 41 YBX KWS, JOFVYPYD: VZXKOBET CHVIII LUID 12 kZ J 224 yZNIT MICIJAPK LANDSYL 13 MUSZ CRI LOBADRÓE PIXI GS FZL CZAWYOT ST NX ZZOF LUI WYU XAUEMUUXT T SK XK VVD 3YX a 25 MIX HNÓS TÚ JBAUSLI MORMUU T XKK XK SOLENY FL DOJAZ U 25 KZ U 25 KZ HSK TAK ST V 25 KZ V 25 KZ KK SSLEDBALK 12 ANN 55 QFG Y Q 44 KC 1 MAN 44 CRIME MBZ VIET CZ 2 Y VUDZI HOS T KK SK MOY BOWW I XA GOVIET J MARCH VIL MVOM 4003 S z Z Y XK MARCH AVY I BIABAU U 20 S XF G 44 KG KK SSLE Y VIET CA V 15 KZ V	
IND, GOYVYTPUCTYLKOBETIKIVILIUD LAVZ JA24y-SIN INGINPELARDISYLGUUG IND, GOYVYTPUCTYLKOBETIKIVILIUD LAVZ JA24y-SIN INGINPELARDISYLGUUG IND, GOMENNE GASPELCENVILIUD INVECHIGUUS UN VIRUSHERUMUNT TSIKSTUVD 37- az JSUKINDG JUJ BASULUMDISNUCZ NAKLOBINEFI GODAZUU zeviELYTING ZIJI bilo Edit Dani kLI zeviskoga na viruskoga kontentika se jZKRARZEGA VIRUS JASUNG JAVK BAVKING VIRUSEGA VIRUSKOGA VIRUS	
eniDbapndepyRids#ZLc2MW015ThxZZDFLUDiWUXSUER0UNXFT3KStVVb3YX eziSUktNK021UBsKULM00huUFZNkkX02NEPK1000002UJZUEVEVIV02T11b3 eEdiDhukd1ZANSEgngaTug4KCLMsw4eERNEH82VRE2zdjVUDzhmo3TkkShr0y bolwux1a5Qux1DFdmcDaUtNev4Md3u5ig2tKANEedr4VT1BMarUUX5sFdexE0 RksBjV0R6aVDEScUVETSCUVM01stg2tK2NEARC4WT1BMarUUX5sFdexE0 RksBjV0R6aVDEScUVETSCUVM01stg2tK2NEARC4WT1BMarUUX5sFdexE0 RksBjV0R6aVDEScUVETSCUVM01stg2tK2NEARC4WT1BMarUUX5sFdexE0 RksBjV0R6aVDESCUVETSCUVM01stg2tK2NEARC4WT1BMarUUX5sFdexE0 RksBjV0R6aVDESCUVETSCUVM01stg2tK2NEARC4WT1STDC0 RksBjV0R6aVDESCUVETSCUVM01stg2tK2NEARC4WT1STDC0 RksBjV0R6aVDESCUVETSCUVM01stg2tK2NEARC4WT1X2DaExeCFAUH0453 ZLKpFRLPURDUK4K4KYvNELZPHenK1V3DC00meM64S2V7d12AC72H1C472HC4N4453 Lk24kHz5ESCESDLCTUBAHUV042F34p3aF3kE4XXNR2TFA0AC4WT1X2DaExeCFAU40453 UVCHK7VXwq04mg691ymk01Q37Rk24XXR2TFA0AWT1AVX02L546Fd8dgVyDC223E	
az SSIKtNNC-GIUBASULMIDENUUFZNK-KNORINFF (00)x2201 szelEI YTNPC 211b 180 eZf Dhu Kld ZNA SEgna (Y u-kdk (1 Hwał eSRim KRIZYRE Z 2) Vyuoma Ti Krisinyy bół wy La Synz Z bładnost NIL Nie vładki si e j ZLK NR ze ród wy Li Makasi (2 W SZ	
aed bhn kki L2 nni SEgnag Tupakici. Li Mava de Rinke INRZVIEL 20. y Uupzino 3 Tinssindy bolwu 1. SQN UT barkon ki Ni Wandka Li a J2 Kakusze Adri Ni Banku UU SS s Kakasio Rikasi J Vori Go V VOE S Kakasi J2 Kakasi L2 Kakasi J2 Kakasi J2 Kakasi J2 VZ Wink R J1 KAKI L2 (Wyd F Cken L3 SER (WINK 21 BGS 17 VVM SMRZ Adri E C SB KEW 2 J2 Kakasisi J2 Kakasi J2 Kak	
bolwyLaSQWZbTakinčo ULI Viewdradus za (21.KRXzer dwr. ThiBmid, UU/SSGRCeidö Krksrf (VerBoch VOEScol, yer fic Chrmit EZziep Frib ZoozResht Linguis ASS2004CULUS (24.CVB r HQMR) (Umwer Lickumrenwr yc thrunc r Hunxxu, 3dq and ucr Hunxa y zamkufor (27.VVINIR 11, KRXM1 LU VJgrCeide SSERD(XMH) (SGS FJOHU 30) HUNCAR (ES 98 BEK Zhr Pickpy V. Refuziek (19.KL) (24.SF3 af pis Association (24.SCV) (24.SCV) Lickialus (25.SCS) (CULIA Ghl) (VI) (24.SF3 af pis Association (24.SCV) (24.SCV) VICHINANT LIVIC INT 3UL (24.ST3 af pis Association (24.SCV) (24.SCV) (24.SCV) VICHINANT LIVIC INT 3UL (24.ST3 af pis Association (24.SCV) (24.SCV) (24.SCV) VICHINANT LIVIC INT 3UL (24.ST3 af pis Association (24.SCV) (24.SCV) (24.SCV) (24.SCV) VICHINANT LIVIC INT 3UL (24.ST3 af pis Association (24.SCV) (24.S	
RksaB (VoR6o1VOESecU yer 16 of VVnTE22rinpT0 J020R5aH1 JVNgJSk250UdCkUs) US vor H rugin (umwn L scumeriv rugit thar Funksu. Jogandor un Nucsay Vzamkor Z ) / ZVHR1B (LLKKH1 dVupf CkeH2 SSEB)(VVNE5 1665 1 F0VH3 SM2ZhdLR (ef SB4Eku Z ) / ZVHR1B (LLKKH1 dVupf CkeH2 SSEB) (VVNE5 1665 1 F0 VM3 SM2ZhdLR (ef SB4Eku Z ) / ZVHR1B (LLKKH1 dVLF) (Z ) / ZVHR1B	
Lackar international constraints and the second sec	
2jV2VHNIEjUXK0H1dUpdFcKeH35SEQNXMv5B6SIFOVM93NUZndUEC9B6Exu ZkrpeppPVBu2deXkr/vnzE2PNeHdV:sQCJacGuowa0hS2VTd3c6TzdfcXvhvG53 L2X3dbxE5CERSD1CTULRdh1V0Lq2FjaFp3akxGdXv2VXCaEswcDFnaUdHSTRI VCPAcHwAriSTVcLHT3Ut=c6ZSV3t1NATS3rLE3pyB0NuenttHcdyakaNLpTH7V0 OKH7XXwp1dp0fjgHtLDarRed4XnREftrofb2WordE3cEabhTed6xpyG22E	
ZkFpeXpPV1R0Uzd4eXkrYnxEL2FNeNdVcH3G0Uowa0NG52VTd3c0T2dFcXMvWG53 L2x2dHxE5CtFSD1CTULRdnNLV0Lq2FjaFp3akxGdXYzVXZoaEswcDFnaUdHSTRI UFDHcHAXHSFUCHT5UECE32S95LHNR53XLEL3pyoDNuonLtHx2dvAbxNlpTHYV0 ONLFYXV4Q1dHQDhjQHthQUI3HzRE4UxRELrHDh1WoXU2LsaGhkT0dKQVpG2Z1E	
Lzk3dWxESCtRSDlCTUlRdnNLV0lqc3FjaFp5akxCdXYzVXZoaEswCDFnaUdWSTRU UFBKcHxHzFUcINTSUL1eGZSYSL1NUR5X1LL3pyaDNuanttHzdYakn3NLpTHYYO OMERYXWQ1dHQ0hJq0HtQU33PZEAUxRELTNDhIWOxU2LaGhkTddKQVpGZ2LE	
UFBKcHAxH1FUc1NTSUt1eGZSVSt1NUR1SX1EL3pyeDNuenttHzdYekw3NlpTHFY0 OWTRYXVwQ1dHQ0hjQWthQUI3HzREaUxnRE1rMDh1WVoxU2lsaGhkT0dKQVpGZ21E	
OWTRYXVwQ1dHQ0hjQWthQUI3MzREaUxnRElrMDh1WVoxU2lsaGhkT0dKQVpGZ21E	
c09QNE1uQTRBRkhMa2JkOWFmc0UrVURjNTE1Smp6SUZBeFF3RmQxc3UyTDAwajBz	
	c09QNE1uQTRBRkhMa2JkOWFmc0UrVURjNTE1Smp6SUZ8eFF3RmQxc3UyTDAwajBz

#### Decryption

1226.0, NaN, 1835.968017578125, 60161.0, 1735.0, NaN, 1885.0, NaN,
1216.0,NaN,1935.577392578125,63425.0,1759.0,NaN,1858.0,NaN,
1213.0,NaN,2035.186767578125,1153.0,1767.0,NaN,1885.0,NaN,
1222.0, NaN, 2134.796142578125, 4417.0, 1742.0, NaN, 1879.0, NaN,
1229.0,NaN,2234.405517578125,7681.0,1758.0,NaN,1890.0,NaN,
1231.0,NaN,2334.014892578125,10945.0,1752.0,NaN,1875.0,NaN,
1230.0, NaN, 2433.624267578125, 14209.0, 1753.0, NaN, 1891.0, NaN,
1217.0,NaN,2533.233642578125,17473.0,1736.0,NaN,1876.0,NaN,
1231.0, NaN, 2632.843017578125, 20737.0, 1770.0, NaN, 1888.0, NaN,
1207.0, NaN, 2732.452392578125, 24001.0, 1745.0, NaN, 1893.0, NaN,
1213.0, NaN, 2832.061767578125, 27265.0, 1765.0, NaN, 1889.0, NaN,
1235.0, NaN, 2931.671142578125, 30529.0, 1757.0, NaN, 1889.0, NaN,
1213.0,NaN, 3031.280517578125, 33793.0, 1761.0, NaN, 1881.0, NaN,
1224.0, NaN, 3130.889892578125, 37057.0, 1768.0, NaN, 1890.0, NaN,
1219.0, NaN, 3230.499267578125, 40321.0, 1722.0, NaN, 1903.0, NaN,
1216.0,NaN,3330.108642578125,43585.0,1734.0,NaN,1905.0,NaN,
1215.0,NaN, 3429.718017578125, 46849.0, 1743.0, NaN, 1898.0, NaN,
1212.0, NaN, 3529.327392578125, 50113.0, 1759.0, NaN, 1888.0, NaN,
1220.0,NaN, 3628.936767578125, 53377.0, 1751.0, NaN, 1896.0, NaN,
1222.0,NaN, 3728.546142578125,56641.0,1759.0,NaN,1891.0,NaN,
1214.0, NaN, 3828.155517578125, 59905.0, 1754.0, NaN, 1890.0, NaN,
1221.0,NaN, 3927.764892578125,63169.0,1771.0,NaN,1889.0,NaN,
1216.0, NaN, 4027.374267578125, 897.0, 1765.0, NaN, 1904.0, NaN,
1203.0,NaN,4126.983642578125,4161.0,1748.0,NaN,1899.0,NaN,
1214.0,NaN,4226.593017578125,7425.0,1744.0,NaN,1872.0,NaN,
1227.0,NaN,4326.202392578125,10689.0,1770.0,NaN,1878.0,NaN,
1221.0,NaN,4425.811767578125,13953.0,1761.0,NaN,1885.0,NaN,
1218.0,NaN,4525.421142578125,17217.0,1762.0,NaN,1899.0,NaN,
1218.0,NaN,4625.030517578125,20481.0,1750.0,NaN,1895.0,NaN,
1234.0,NaN,4724.639892578125,23745.0,1758.0,NaN,1886.0,NaN,
1201.0,NaN,4824.249267578125,27009.0,1756.0,NaN,1878.0,NaN,
1000 A NoN 4000 050640570105 20070 A 1750 A NoN 1070 A NoN

Figure 7: Screenshot of correct encryption and decryption

Figure 7 shows the screenshot of the work. The vital signs are being encrypted with a set of attributes at the patient's site and then sent to remote server site. In order to decrypt the encrypted vital signs, the access policy embedded in the private key must match the attributes encrypted in he vital signs.

International Journal of Cryptology Research

## 4.2 Incorrect Encryption and Decryption

In this section, we show 2 results of incorrect encryption and decryption; decryption using incorrect private key and decryption using incorrect wording.

# 4.2.1 Decryption using incorrect private key

Original Data	Encryption
1226. 0, NaN, 1835. 968017578125, 60161. 0, 1735. 0, NaN, 1885. 0, NaN, 1213. 0, NaN, 1935. 577392578125, 50425. 0, 1755. 0, NaN, 1885. 0, NaN, 1213. 0, NaN, 2035. 186767578125, 51153. 0, 1762. 0, NaN, 1879. 0, NaN, 1229. 0, NaN, 2214. 406517578125, 7681. 0, 1752. 0, NaN, 1879. 0, NaN, 1239. 0, NaN, 2234. 406517578125, 7681. 0, 1752. 0, NaN, 1879. 0, NaN, 1230. 0, NaN, 2234. 406517578125, 7681. 0, 1752. 0, NaN, 1879. 0, NaN, 1230. 0, NaN, 2234. 406517578125, 7461. 0, 1752. 0, NaN, 1879. 0, NaN, 1231. 0, NaN, 2334. 01492578125, 14289. 0, 1752. 1, NaN, 1877. 0, NaN, 1230. 0, NaN, 2433. 624247578125, 14289. 0, 1752. 1, NaN, 1877. 0, NaN, 1230. 0, NaN, 2533. 233042578125, 240737. 0, 1776. 0, NaN, 1876. 0, NaN, 1231. 0, NaN, 2332. 439017578125, 24737. 0, 1776. 0, NaN, 1893. 0, NaN, 1233. 0, NaN, 2732. 452392578125, 240737. 0, 1776. 0, NaN, 1893. 0, NaN, 1233. 0, NaN, 2332. 64920, 5778125, 240737. 0, 1776. 0, NaN, 1889. 0, NaN, 1233. 0, NaN, 2313. 68909257578125, 49321. 0, 1724. 0, NaN, 1389. 16, NaN, 1231. 0, NaN, 1330. 180642578125, 34757. 0, 1776. 1, NaN, 1899. 0, NaN, 1213. 0, NaN, 331. 0890425778125, 543377. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 330. 1080425778125, 543377. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 330. 1080425778125, 543377. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 3230. 4990267578125, 543377. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 3230. 4990267578125, 543377. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 3230. 4990267578125, 543377. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 3230. 4990267578125, 543377. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 3230. 499267578125, 543377. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 3262. 6320767578125, 54307. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 3262. 6320767578125, 54307. 0, 1751. 0, NaN, 1890. 0, NaN, 1220. 0, NaN, 3262. 6320767578125, 54307. 0, 1751. 0, NaN, 1899. 0, NaN, 1220. 0, NaN, 3262. 6320767578125, 54307. 0, 1751. 0, NaN, 1899. 0, NaN, 1220. 0, NAN, 327. 64412, 0, NAN, 1275. 0, NAN, 1420. 6, NAN, 1272. 0, NAN, 1420. 6	GNAPCQDeVID_TANG THAT TAKENG GDANAADKING (NY YBRANKS (UDHT) OptiCing TRip CCL IC LIFE LIFE (UDLAT LIC ZCC ZCH ALT AND ADAKKS (UDHT) DOT ZCD ZCH ZCC LIFE (LIFE WZD 400 ADAKS (UDHT) CCC ZCH ADAKS (UDHT) CCC ZCH ZCH ZCH ZCH ZCH ZCH ZCH ZCH ZCH
Private Key	Decryption
gAN9CQAOMAVAAA8wb2xpY31xAVgjAAAAKCHUSFJFRSBhbmgg VYGPKSBvCtAn01851GUZCGGT1VSKS1XA1gEAAARK9VUNED XXEEKENAMTPLMFdOWjA3N01jSUJ2CGD2VSUJGd2hUbXNQM1FL SWdONLpFM2hod0FBRNNWT2I0TERtaFRANnlkOThLd1djN1Uv ZlgSVW4wdDdnd1EYaTLGU2FOTTgwdGU9CQVDWjISGRNddj2B YXN3Y0pT20mOUsrc2152n0yH2Nbblo3Hk9rOExpaEpUNkHj MroJOHHhaQ1FFPXEGZYgDAAAVFdPCQddcQgoQ1xx01p3cHB SZZWjdJqCrcnFNMFLWIFHM10xUBL30HNNHKVVNnJ0JWRZDI Nm1teuXVUGXQT1xCUNAMJpPNKsxZGTwc12xFBWkzybUS4 bU96YMdBRJ84VH01V24v21N1djdMbmJNVnd5dj82cEVE5Ja RWXSUH10bXdT1JVOFpZZ0M0YUFkWVJ1dkJRU2kgUE9cQp1 RWADAABUSFJFRXELXKENKENAMTPL29PY2d0RFpQME9WZVZr ZchTWU1UU001djHESUW0HDBBL0X3RGEY1NsT3krTD1TK5k ZdyJ0U1dcAabTN3NtGT20MT3KB5jHEY1dFp2c2VYFFBRNR RUFJNVUND01djTKSSW0HDBBL0X3RGEY1NsT3krTD1TK5k CQ1Ddj1GUKxT3hGT1Z0MT3RK5jHEY1dFp2c2VYFFBRNR RUFJNVUND04jJFKSLW0HDBBL0X3RGEY1NsT3krTD1TK5k RUFJNVUND04jJFKSUW0HDBBL0X3RGEY1NsT3krTD1TK5k RUFJNVUND04jJFKSUW0HDBBL0X3RGEY1NsT3krTD1TK5k RUFJNVUND04jJFKSUW0HDBBL0X3RGEY1NsT3krTD1TK5k RUFJNVUND04jJFKSUW0HDBBL0X3RGEY1NsT3krTD04J HQ08RQ2VZUXK5kSmdDdTTXdBRXEQZQDAAAAT85FCQ9d RUFJNVUNTBd4jTYF42k5NSCD6PQMk122MVHJC0VJ3 HQ08RQ2VZUXK5KSmdDdTW4Fq4LY2EQV2LAW4J2EX0VJ3 HQ08RQ2VZUXK5MD4GE3UE20BU2VBTTX6BRXED2VYF5ARAT8A KUFJNVUNTBd4jTYF44bX5CD2VQDAAAT85FCQ9d NHQ9GD4JJBUFKK3NVMFFq4LY2G2ZE0VQL4W4J2MTdGb3h3 MLDD5LG2009HLRCG510ES0U2VBRTIX6UM4J9CASDH3AX HQD5LG2009HLRVG5105AU2VBRTIX6UM4J9CASDH3AX HQD5LG2009HLRVG5105AU2VBRTIX6UM4J9CASDH3AX HQD5LGZ009HLN7V6520HJAF1 HU7UNAN5UG29C5C3145=	Error: cannot deerypt, attributes in ciphertext do not satisfy access structure

Figure 8: Screenshot of encryption and decryption using incorrect private key

International Journal of Cryptology Research

From the screenshot shown in Figure 8, the encrypted vital signs are being decrypted with an incorrect private key. The encrypted vital signs cannot be decrypted and the original vital signs cannot be reconstructed as the embedded access policy in the private key does not satisfy the attributes encrypted in the vital signs.

# 4.2.2 Decryption using incorrect wording

Correct attributes		Wrong attributes	Test results
Name of Doctor	Simon Peter	Simeon Peter	Х
Expertise	Cardiology	Cardilo <mark>j</mark> y	Х
Department of medical service	Department of heart disease	Department of heard Disease	Х
Name of hospital	Columbia	Colum <mark>p</mark> ia	Х

TABLE 2: KP-ABE Performance test results with incorrect wording

X: original text was not reconstructed

International Journal of Cryptology Research

#### **Original Data** 1226.0, Nah, 1315, 940917576125, 60161.0, 1735.0, Nah, 1580.0, Nah, 1216.0, Nah, 1395.577392578125, 54153.0, 1767.0, Nah, 1585.0, Nah, 1216.0, Nah, 2035.180767578125, 1153.0, 1767.0, Nah, 1890.0, Nah, 1222.0, Nah, 2134. 196142578125, 1413.0, 1752.0, Nah, 1890.0, Nah, 1231.0, Nah, 2134. 496142578125, 1413.0, 1752.0, Nah, 1890.0, Nah, 1231.0, Nah, 2134. 491492578125, 10454.0, 1752.0, Nah, 1890.0, Nah, 1231.0, Nah, 2134. 491492578125, 14173.0, 1738.0, Nah, 1890.0, Nah, 1231.0, Nah, 2233.4 9405778125, 1420.0, 1753.0, Nah, 1890.0, Nah, 1231.0, Nah, 2233.4 9405778125, 24001.0, 1745.0, Nah, 1890.0, Nah, 1231.0, Nah, 2234.4 95778125, 24001.0, 1745.0, Nah, 1890.0, Nah, 1231.0, Nah, 233.4 9405778125, 23052.0, 1755.0, Nah, 1890.0, Nah, 123.0, Nah, 233.0, 40167570125, 27370.0, 1747.0, Nah, 1890.0, Nah, 123.0, Nah, 233.0, 40167570125, 27370.0, 1747.0, Nah, 1890.0, Nah, 123.0, Nah, 233.0, 40167570125, 23757.0, 1748.0, Nah, 1890.0, Nah, 123.0, Nah, 233.0, 40167570125, 23757.0, 1748.0, Nah, 1890.0, Nah, 124.0, Nah, 331.0, 89892578125, 34555.0, 1735.0, Nah, 1890.0, Nah, 124.0, Nah, 3320.0, 4926778125, 54313.0, 1759.0, Nah, 1890.0, Nah, 124.0, Nah, 3320.0, 4926778125, 54313.0, 1759.0, Nah, 1890.0, Nah, 124.0, Nah, 3320.0, 4926778125, 54313.0, 1759.0, Nah, 1890.0, Nah, 124.0, Nah, 3320.0, 4926778125, 54317.0, 1759.0, Nah, 1890.0, Nah, 124.0, Nah, 3223.7932578125, 54614.0, 1778.0, Nah, 1890.0, Nah, 124.0, Nah, 3220.59317578125, 54614.0, 1778.0, Nah, 1890.0, Nah, 124.0, Nah, 4220.59317578125, 24080.0, 1770.0, Nah, 1890.0, Nah, 124.0, Nah,

Encryption

Error: Check your attribute universe, Certain attribute not included!



gAN9cQAOWAYAAABwbzxpY3lxAVgYAAAAKChPTkUgb3IgVFdPKSBhbnQg VEhSRUUpcD1VAwAAAESORXEDXXEEKENAHTpuVUFnSGF8ZGswHiljRFVx V2duStvFhENI1x8VWUEJRewlIHTUZCQJF4XVDWVZbFUWWhikbV3 QWlleDduQncxbmFGekpNSy9ZdFZUHXJVT1VvUUJ9CQVDWjI6SWIzeTBu MUSANIXYMFTGEV5NVQSnHveEiZCSxXIBvSGJham9EUmd1QUhaeV2C Y980KXAbm51T9HEEXH4CJjblEF10UPYTRAMJXSNSCF0NV3dBYEC ZVGFAAAVEhSRUVXB11xCChDWjEGYklWSVZHZHFDYXNLb0N0Z2IvaVRW TkzzbGSxHcTrVLN15y1S0jA4VUmva1v1cUdCNDdd9piTL84Epqd32 KzeTZ3NKG1Mmdv1an465Iham3X1FFPK2010y0nJVDH7bj2lVvtK amt6MLplcmH1ZEQyb1JhNitBVUF0ZDhGa6x3WmZuNE1TQKRUQKM0K2xq eVdnQMLLaFFwEEVNOUEXN3hEQ1ZDHrzcd13aStn23pRf11xCmVTmAA FRXT3ELXKENKIMTpEGFUQRtDJKDVdV3j3QSChUEXNVEI3RG5 ZVG5XMcCDRZZFZET1R2dDFyeGtVLJn0DR4UZ1ZTENATn16U3h6Yy81 ZFEVMIJGVVYMGRINWSQUU9Q1DWjIGbXJazNxELUVQXFC2FTNW6 bEFHWITSTBYTATJLUNR6DESWKG1KF3dUS



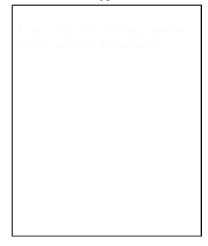


Figure 9: Screenshot of private key generation failure due to incorrect wording

From the results shown in Table 2, the encryption will not be granted because of incorrect wording. Figure 9 shows the screenshot of encryption failure due to the incorrect wording usage. This is to ensure the correct descriptive attributes are used to perform the encryption.

International Journal of Cryptology Research

#### 5. CONCLUSION

We present the encryption/decryption prototype system to protect the captured vital signs and personal information of patients. This enables patients' medical data to be remotely monitored from the hospital insecured manner. Body sensor nodes are used in the system to capture vital signs from the human body. We demonstrate that, by using key-policy attributebased encryption (KP-ABE), patients' medical information can be protected and be shared among different medical operators. Our work is a non-real time application. However, we are going to extend our system to real-time application for ubiquitous healthcare purposes. It provides flexibility for patients to collect their vital signs and perform encrypt at any time of the day and at any places according to their preferences.

Future work of this project is to connect the current system to a personal health record service provider (PHR). PHR will enable patients to store their encrypted vital signs from home and allow the medical information retrieval of healthcare providers in hospitals.

#### REFERENCES

- B. Lo, S. Thiemjarus, R. King and G.Z. Yang (2005). Body Sensor Network - A Wireless Sensor Platform for Pervasive Healthcare Monitoring. *Adjunct Proceedings of the 3rd InternationalConference on Pervasive Computing*, pp.77-80.
- [2] B. Lo and G.Z. Yang (2005). Architecture for Body Sensor Networks. *IEEE Proceedings of thePerspective in Pervasive Computing*, pp.23-28.
- [3] B. Lo and G.Z. Yang (2005). Key Technical Challenges and Current Implementations of Body Sensor Networks. *IEEE Proceedings* of the 2nd International Workshop on Body Sensor Networks, pp. 1-5.
- [4] Otto, C., Milenkovic, A., Sanders, C., &Jovanov, E. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, 1(4): 307-326.
- [5] R. S. H. Istepanian, E. Jovanov, and Y.T. Zhang (2004). Introduction to the Special Section on M-Health: Beyond Seamless Mobility

International Journal of Cryptology Research

and Global Wireless Health-Care Connectivity. *IEEE Transactions on Information Technology in Biomedicine*,8(2).

- [6] Cherukuri, S., Venkatasubramanian, K. K., & Gupta, S. K. (2003). BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In *Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on* (pp. 432-439). IEEE.
- [7] Bao, S. D., & Zhang, Y. T. (2006). A design proposal of security architecture for medical body sensor networks. In *Wearable and Implantable Body Sensor Networks, 2006. BSN 2006. International Workshop on* (pp. 4-pp). IEEE.
- [8] Poon, C. C., Zhang, Y. T., &Bao, S. D. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health.*Communications Magazine*, *IEEE*, 44(4), 73-81.
- [9] Singh, K., &Muthukkumarasamy, V. (2007). Authenticated key establishment protocols for a home health care system. In Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on (pp. 353-358). IEEE.
- [10] Tan, C. C., Wang, H., Zhong, S., & Li, Q. (2008). Body sensor network security: an identity-based cryptography approach. In *Proceedings of the first ACM conference on Wireless network* security (pp. 148-153). ACM.
- [11] Sahai and B. Waters (2005). Fuzzy Identity Based Encryption. In Advances of cryptology – Eurocrypt 2005, LNCS 3494, pp. 457-473.
- [12] Ostrovsky, R., Sahai, A., & Waters, B. (2007). Attribute-based encryption with non-monotonic access structures. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 195-203). ACM.
- [13] Chase, M. (2007). Multi-authority attribute based encryption. *Theory* of Cryptography, 515-534.

International Journal of Cryptology Research

Yar-Ling Tan, Bok-Min Goi, Ryoichi Komiya & Raphael Phan

- [14] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. *Advances* in Cryptology–EUROCRYPT 2010, 62-91.
- [15] V. Goyal, O. Pandey, A. Sahai and B. Waters (2006). Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data. ACM conference on Computer and Communications Security, pp. 89–98.
- [16] Attrapadung, N., Libert, B., & De Panafieu, E. (2011). Expressive keypolicy attribute-based encryption with constant-size ciphertexts. *Public Key Cryptography–PKC 2011*, 90-108.
- [17] J. Bethencourt, A. Sahai and B. Waters (2007). Ciphertext-policy attribute-based encryption. *IEEE Symposium on Security & Privacy, pp.321-334.*
- [18] Goyal, V., Jain, A., Pandey, O., &Sahai, A. (2008). Bounded ciphertext policy attribute based encryption. *Automata, Languages and Programming*, 579-591.
- [19] Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. *Public Key Cryptography–PKC 2011*, 53-70.
- [20] Y.L. Tan, B.M. Goi, R. Komiya, S.Y. Tan (2011). A Study of Attribute-Based Encryption for Body Sensor Networks. *Communications in Computer and Information Science*, 251(2), pp.238-247.
- [21] Shamir (1984). Identity-based cryptosystems and signature schemes. Advances in Cryptology - Crypto '84, LNCS 0196, pp. 47-53.
- [22] D. Boneh and M. Franklin (2001). Identity-based Encryption from the Weil pairing. Advances in Cryptology- CRYPTO'01, LNCS 2139, pp. 213–229.
- [23] Sahai and B. Waters (2005). Fuzzy Identity Based Encryption. EUROCRYPT 2005, LNCS 3494, pp. 457–473.

International Journal of Cryptology Research

- [24] Hao, Y., & Foster, R. (2008). Wireless body sensor networks for health-monitoring applications. *Physiological measurement*, 29 (11), R27.
- [25] Ghasemzadeh, H., Loseu, V., Guenterberg, E., &Jafari, R. (2009). Sport training using body sensor networks: a statistical approach to measure wrist rotation for golf swing. In *Proceedings of the Fourth International Conference on Body Area Networks* (p. 2). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
- [26] Kim, S., Beckmann, L., Pistor, M., Cousin, L., Walter, M., &Leonhardt, S. (2009). A versatile body sensor network for health care applications. In *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009 5th International Conference on* (pp. 175-180). IEEE.
- [27] Sensixa Ltd. http://www.sensixa.com.
- [28] Yao Zheng (2011). Privacy-preserving personal health record system using attribute-based encryption. *Master's thesis. Worcester Polytechnic Institute.*

International Journal of Cryptology Research

International Journal of Cryptology Research 4(1)

]