

**SCHOOL OF INFORMATION TECHNOLOGY AND**

**ENGINEERING**

**A Project Report**

**On**

**AUTHENTICATION BASED HYBRID CRYPTOSYSTEM**

*Submitted in partial fulfilment of the requirements for the degree of*

**Bachelor of Computer Applications**

*By*

LINGAMOORTHY V (20BCA0060)

GURUPRASATH A (20BCA0118)

**Under the guidance of**

Prof CHANDRASEGAR.T

**Signature of Guide:**

**ABSTRACT:**

Currently, a multimedia revolution of medical data in health information becomes part of our computing environment. However, the interchange of medical information is typically out sourced by third parties, which may affect the disclosure of confidentiality. To address this Issue, we address high security and confidentiality through our proposed HYBRIDCRYPTOSYSTEM The proposed scheme uses a Diophantine equation to have the three stage of decryption for high security, but ESRKGS and RSA has one level of decryption. The results show that the proposed cryptomata has efficient encryption and decryption time when compared to the existing systems. At 10 K-bit moduli of key generation, CHAN-PKC consumes only 0.65 times of RSA, but ESRKGS takes 1.83 times of RSA. The timing similarity shows that both CHAN-PKC and RSA has a 100% correlation, but ESRKGS has only 90%. Hence our CHAN scheme is robust against side channel and also has a large key space than RSA. The security analysis confirms that our CHAN-PKC is very fast, secure against brute force and side channel attacks; therefore, it is feasible for real-time applications.

**INRODUCTION:**

Patient’s health record system has attained a phenomenal growth in health information exchange. It Is used to keep track of the patient’s health status viewed by the doctor. Digital medical images use a large number of applications for predicting patient disease. These use public channels to store and transmit the medical images, which make them unprotected to security threats. In medical applications, the patient’s privacy and security should be a top priority. Based on the country regions, the standards and guidelines vary on healthcare information exchange. Application security has based on the IT service layers and application specific; hence, the security services are applied accordingly.

With long-term efforts, several researchers proposed different medical encryption schemes for secure transfer of medical information. Some of the recent works includes asymmetric encryption, chaotic system, orthogonal matrix, dual encryption, pixel-based scrambling, and other schemes. We propose in this paper CHAN-PKC cryptomata for medical data security to resist against side channel attack.

Our technique applies Pell’s form of an equation for encryption and decryption process. Model results are delivered to demonstrate the performance of the proposed scheme while preserving a high level of security and confidentiality. We further show that the CHAN-PKC scheme is strong against side channel and key space attacks. Through wearable devices like a watch, blood pressure (bp) monitor, are becoming more popular, patients can explore more on their health indication. After a regular interval of time, patients can upload their records to the cloud. The doctor or the physician or through the learned threshold functions, the record are analysed and then convey the appropriate signals such as low bp, normal, high, very high to the patient accordingly. Based on the health record status report, the doctor may advise the patient to take medicine. Moreover, a doctor or an analyst can explore new findings from the patient’s personal health history such as the medicine played an impact on a patient’s health or change the medicine based on sex or age.

**PROBLEM DEFINITION**

1) The RSA apply one level of encryption and decryption, whereas proposed CHAN-PKC scheme generates three levels of encryption and decryption.

2) Integrate Blind Signature in Chan-PKC and obtaining the private and public keys.

3) Obtain the Blind factor and Blind message.

4) Sign generation and sharing the sign.

5) Verifying the signature by verifying blind message and message.

6) The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their functions.

PROJECT OBJECTIVIES AND SCOPE OF PROJECT

The CHAN-PKC scheme based on improved RSA public key cryptography with Diophantine equation to have the three stage of decryption for high security. The proposed scheme aims to resolve the problem of guessing the private key (e, 2Yl, N) from the public key (α, Re, N). The robustness of the CHAN-PKC depends on key generation parameters bit-length. And integrating Blind signature protocol to provide Authenticity, Integrity and Non-repudiation to electronic documents and to use the Internet as the safe and secure medium for e-Commerce and e-Governance.

**Literature survey:**

## 1.Hybrid IT architecture by gene-based cryptomata (HITAGC) for lightweight security services

**Abstract:**

In the computing world, the digital transformation of data grows exponentially with every year. However, these situations are predominantly tackled by leading enterprises through by adopting a hybrid IT model. This model effectively supports the organization through strategic design to provide standard delivery to customers from independent multi-sourced entities. An experimental design method is applied using hybrid IT architecture with gene-based cryptomata (HITAGC) which is well suited to real-time cloud environments to store and retrieve the cloud space data efficiently. The CSC primarily relies on the service of CSP to keep their confidential data, and this system ultimately uses the PKC crypts. To address this security demand, we propose two different schemes such as HITAGCPKC and hybrid HITAGC. The first model is designed to generate robust asymmetric keys for the Internet of Things, and the other hybrid HITAGC is for efficient sharing of big data over the cloud in a secure manner. The performance of these crypts is compared with the traditional systems like standard RSA, ESRKGS, SED2, EDCon, and AES. Keywords Symmetric encryption · Hybrid model Asymmetric cryptography · Big data · Internet of Things · Lightweight

## Author: Viswathan P

## 2. An efficient public key secure scheme for cloud and IoT security

**Abstract:**

According to the National Institute of Standard and Technology (NIST), the security level of RSA is safe when it is N-bit modulus ≥2048 bits. Because of this, the processing time to generate asymmetric keys also increases. Taking this into account, an efficient and non-shareable Public Key Exponent Secure Scheme (ENPKESS) is proposed by using a non-linear Diophantine equation to have high security against side-channel attacks like timing attacks. This scheme has three-stage of encryption and two-stage of decryption, whereas other schemes like ESR and RSA has one level in encryption and decryption. Due to this, extraction of the secret key is extremely hard to determine from our public exponents α, R, N. Our methodology is well suited for secure cloud computing environments used in the Internet of Things (IoT). Here we have also applied the Knapsack method to encrypt our ENPKESS keys to enrich high security in cloud systems. We show a strong performance evaluation on standard RSA, Enhanced and Secured RSA Key Generation Scheme (ESRKGS), and ENPKESS on its key generation, encryption and decryption by varying the N-bit moduli size up to 10K bits. From the overall result, ENPKESS consumes 89% of standard RSA and 27% of ESRKGS.

**Author: Senthil kumar mohan**

3 **Physical Layer Cryptographic Key Generation by Exploiting PMD of an Optical fiber Link**

**Abstract:**

We present a symmetric physical layer based secret key generation scheme for Point-to-Point Optical

Link (PPOL) communication by exploiting Polarization Mode Dispersion (PMD) as a random and

inimitable channel characteristic. The randomness and security strength of generated cryptographic

keys based on PMD is significantly high. In this paper, we present that random modulation of a probe

signal caused by PMD in a high-speed data communication network (40 Gb/s and 60 Gb/s) is

reciprocal with average Pearson correlation coefficient of 0.862, despite the presence of optical

nonlinearities, dispersion, and noise in the system. 128-bit symmetric cryptographic key has been

successfully generated using the proposed scheme. Moreover, PMD-based encryption keys passed the

National Institute of Standards and Technology (NIST) tests. We have shown through simulations with a 50 km link that, with optimal key generation settings, symmetric keys can be generated with high randomness (high P-values for NIST randomness tests) and with sufficient generation rates (>50%). Furthermore, we considered an attack model of a non-invasive adversary intercepting at 10 km into the link and found that the generated keys have high average key bit mismatch rates (>40%)

**Author: Imam Uz Zaman**

4. **A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its**

## Applications to Storage Security

**Abstract:**

Existing biometric-based security mechanisms to ensure storage security follow Biometric Enrolment, Key Binding, Secure Sketch, Fuzzy vault or template store along with key of a user. Also, they use threshold-based comparison or error calculation to authenticate the user. The storage of biometric data or key put the system under threats. Further, the user verification mechanism may not be accurate as the threshold selection is challenging. To alleviate this problem, we have proposed a novel approach to storage security. In our proposed approach, we extract biometric based statistical features to generate codeword of a user. To generate a codeword, we use Reed-Solomon encoding (RS). Later, this codeword will be used to generate a key. Prio to decryption, we authenticate user using SVM Ranking mechanism without threshold value. The major contributions include generation of unique and strong biocrypto keys from users’ biometric data, Reed-Solomon encoding has been used to maintain the codeword and generation of key and SVM based ranking mechanism is used for the user verification where the storage of neither templates nor keys is required.

**Author: Gaurang Pancha**

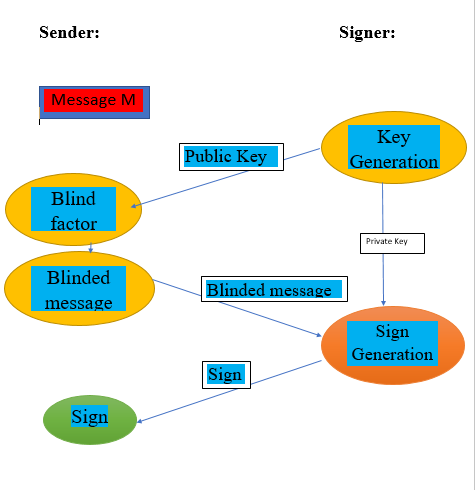
**5.****Memory efficient multi key (MEMK) generation scheme for secure transportation of sensitive data over cloud and IoT devices**

**Abstract:**

A new variant of RSA has been proposed called Memory Efficient Multi Key (MEMK) generation scheme. For sensitive data, our scheme will aid in exchanging the information between cloud to IoT and IoT to IoT devices. When cryptography belongs to the asymmetric type, then it has public and private keys. For memory efficiency, our scheme reuses the RSA scheme with a Diophantine form of the nonlinear equation. Moreover, our scheme performance comparatively performs well and this mainly due to the use of RSA public key alone. Due to this, our MEMK does not require multiplicative inverse function or Extended Euclid's algorithm. Finally, we have made an experimental result on various phases of MEMK PKC such as key generation, encryption, and decryption by varying the Nbit modulo bits from 1K to 10K.

**Author: Himanshu**

**SYSTEM ARCHITECTURE :**



**Proposed System:**

The proposed CHAN-PKC scheme outflow from the traditional method of sharing the keys and produces the public key as (α, Re, N) is resultant in algorithm 1. This scheme of KGS takes (R, p, q) plus RSA public key as input and produces valid private key components (e, 2Yl, N) as output, and it reveals the same in Fig. 2. The performance measure of this scheme assessed in standings of key generation, encryption and decryption by varying its input bits as shown in Table 3. Here, the bit length of RSA public key e lies in half of its N-bit moduli size. Our CHAN-PKC scheme works by solving the Pell’s essential form, α + Re2 + 2RYle ≡ 1 mod  (N). The chief merit of our system is that it does not need Extended Euclid’s algorithm as like RSA-PKC. This merit has shown in the below CHANPKC key generation scheme. The proposed scheme applies two levels of encryption to create the ciphertexts CT1, and CT2 using the public key (α, Re, N). Using the private key (e, 2Yl, N) three levels of decryption is applied which produces a high level of security and confidentiality. The existing cryptographic strength depends on the factorization complexity. The guessed private key ′d′ has made through the factors of common modulus ′N′ and public key ′e′. However, our proposed scheme strength depends on the complexity of RSA (e, (N)) parameters and Pell’s coordinates bit length. Our CHANPKC scheme is, at its core, very related to the original system. Since it practices the similar mechanisms to exchange a public key and the ciphers, it inherits the security structures from it. The proposed PKC also keeps or recovers on its security and confidentiality. The primitives used in the proposed key interchange have differed from the original scheme. This approach also makes the guessing attack much difficult than the existing system. The quadratic Diophantine equation of the form is given as X2 − RY2 = a where a is an integer denoted as a Pell-type equation