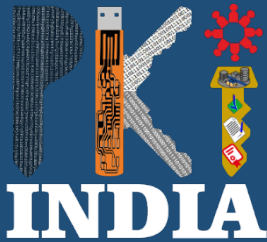




International Conference
on
PKI and Its Applications
(PKIA-2017)
November 14-15, 2017

Hotel Chancery Pavilion, Bangalore



An Online Signature Method Using DNA based Bio-Hash for Positive Identification and Non-Repudiation

Sreeja C.S.

Mohammed Misbahuddin

Dept. of Computer
Science

Computer Networks & Interne
Engineering Division

Christ University

C-DAC, Electronic City

Bengaluru, India

Bengaluru, India



www.pkiindia.in



www.facebook.com/pkiindia



[PKIIndia](https://www.youtube.com/PKIIndia)



[@pkiindia](https://twitter.com/pkiindia)

Outline

- Introduction
- Background
- Related Work
- Research Gap Analysis
- Methodology
- Proof of Concept
- Security Analysis
- Formal Analysis
- Conclusion

Introduction

- Modern Cryptography vs Nano Cryptography
- Biological features which are unique in nature forms a biological fingerprint.
- DNA of an individual is unique and it 's hard to duplicate.
- A digital document must be traceable to an individual.



Background

- DNA
- STR
- DNA Bases
- DNA Profiling.



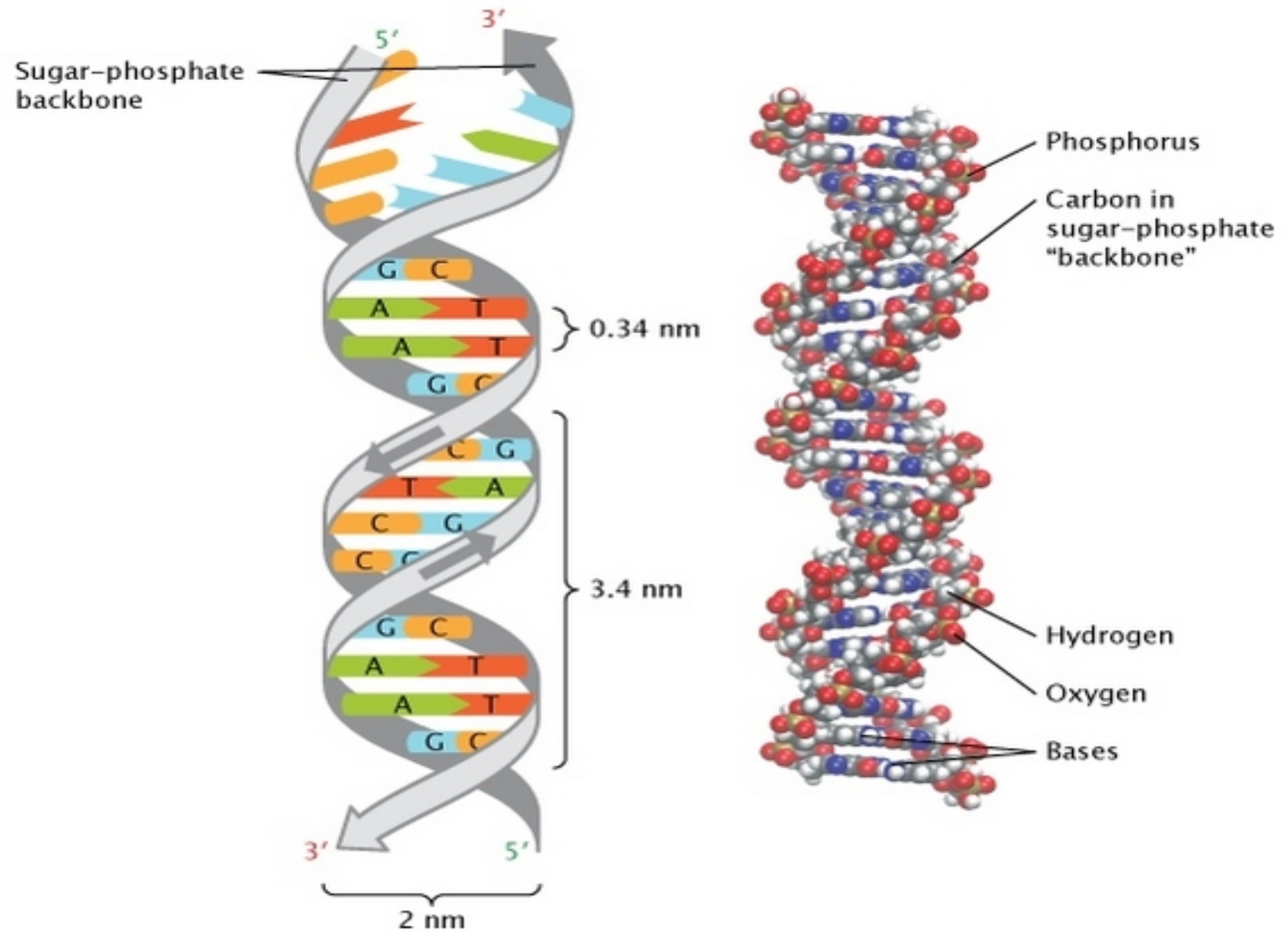


Fig.1: Helical structure of DNA [1]

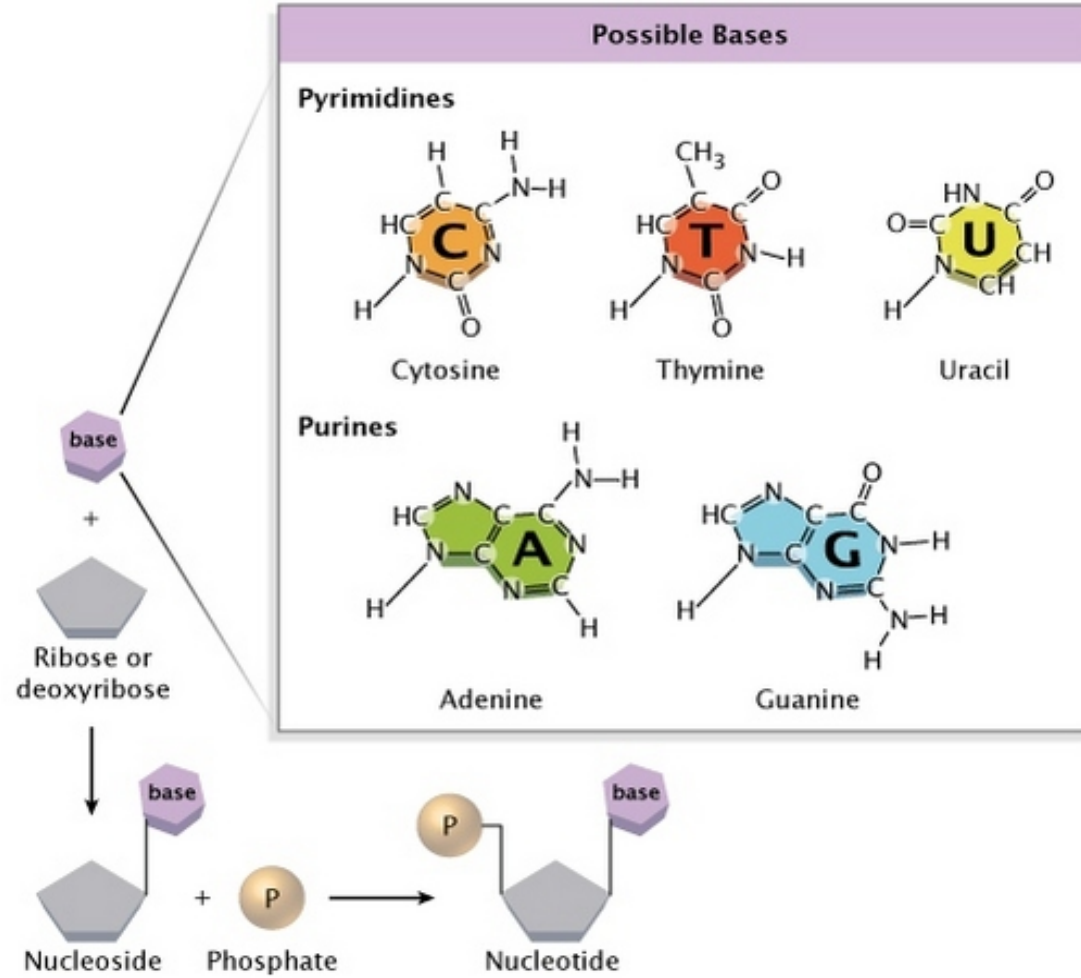


Fig.2: The chemical structure of DNA bases[2]

Related Work

- A.K. Jain et al.[3] describes biometrics as a tool for information security.
- J. Kar and B. Majhi [4] is based on ECDLP using biometric features. The method uses biological features to generate keys.
- Padgett et al.[5] proposed a method for using biological information for digital signature, but the PKI ensures the validity of unique biological information of the registrant.

Related Work

- YUKIO et al. [6] proposed a DNA ID for uniquely identifying DNA based on the individual difference in repeat count of Short Tandem Repeats
- Biometrics generated pattern is used to generate a prime number for RSA key generation by R. Nagpal and S. Nagpal [7] to generate a biometric based digital signature by converting the biometric pattern of iris to the prime number.
- DNA Profiling [8].

Research Gap Analysis

- Unique biological features has applications in personal authentication.
- DNA make it acceptable for personal identification compared to other biometric features.
- Non-Repudiation and signature schemes based on biological feature need more attention.

Proposed Methodology

Phase 1: Generating the Signature DNA and DNA-Hash

Phase 2: Generating the Bio-Sign

Phase 3: Verification of the e-Document and Bio-Sign

Phase 4: Providing Non-Repudiation using Positive Identification

Proposed Methodology

Table 1: Notations used in the Proposed Methodology

Notations used	Description
D_s	Signature DNA
$D(D_s)$	Digital representation of Signature DNA
BH	Bio-Hash
R_i	Random Number
H_i	Hash of the e -Document

Algorithm1: Generating DNA and DNA-Hash Signature

Step1. Collecting the Sample DNA of the registrant from raw biological Data \rightarrow DNA Extraction.

Step2. Selecting DNA of the registrant \rightarrow DNA Isolation

Step3. Identifying the unique sequences in the genome, characteristic features for personal identification.

Step4: Selecting two or more unique sequences (S_1, S_2, \dots, S_n) to generate the Signature DNA (D_s)

It will be unique in every aspect. This process can be done based on Short Tandem Repeats or RFLP - PCR analysis in similar manner for DNA fingerprint.

Step5: Generating Signature DNA by hybridization of the unique fragments.

$D_s = (S_1 \parallel S_2 \parallel S_3 \dots \parallel S_n) \rightarrow$ Signature DNA

Step6: Converting the Signature DNA to digital form,

$D = \sum (A, G, C, T)$, which are the bases.

Digital form of DNA $\rightarrow D(D_s)$.

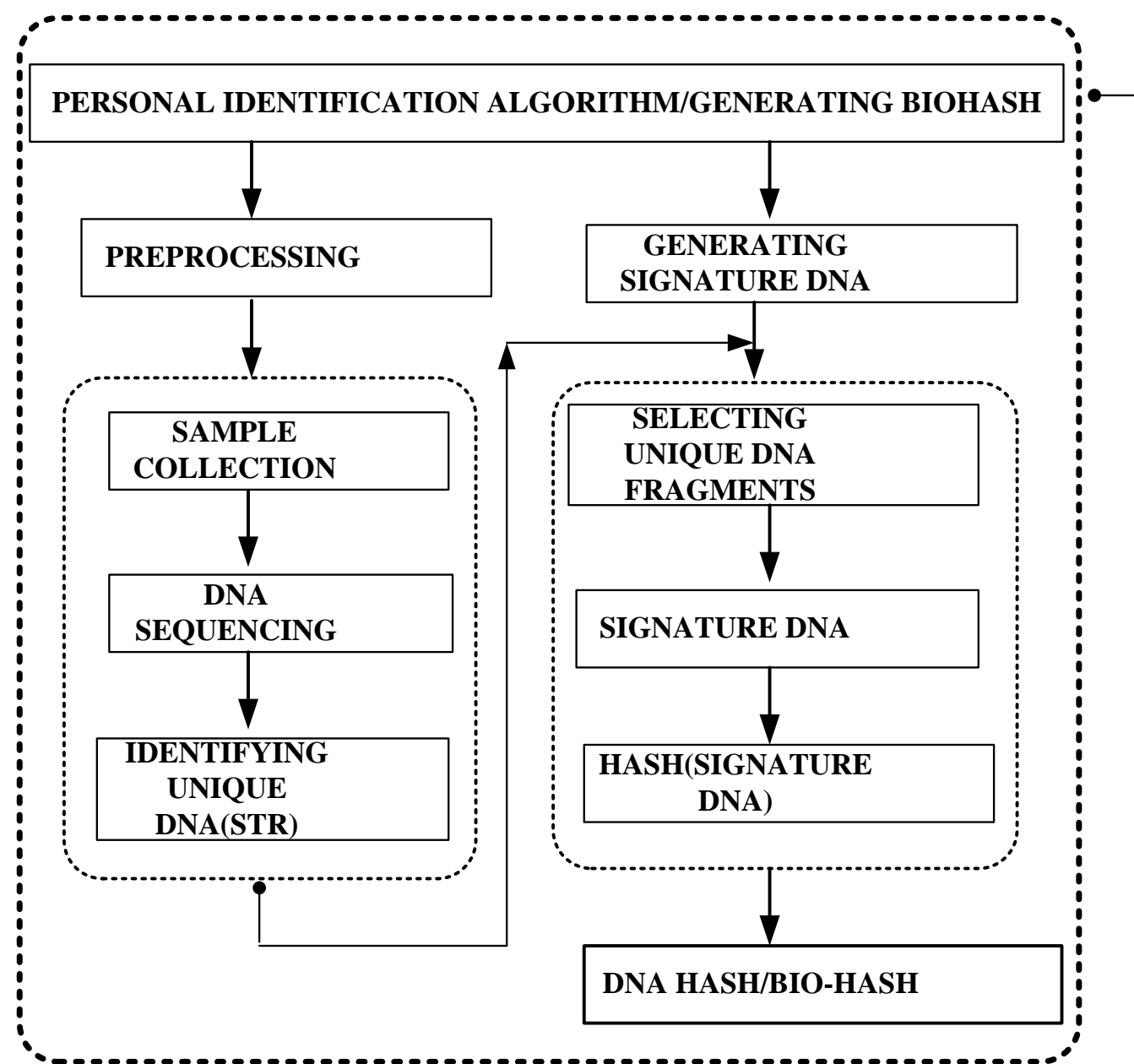


Fig.3: Process flow of Generating Bio-Hash Algorithm

Algorithm2: Generating Bio-Sign

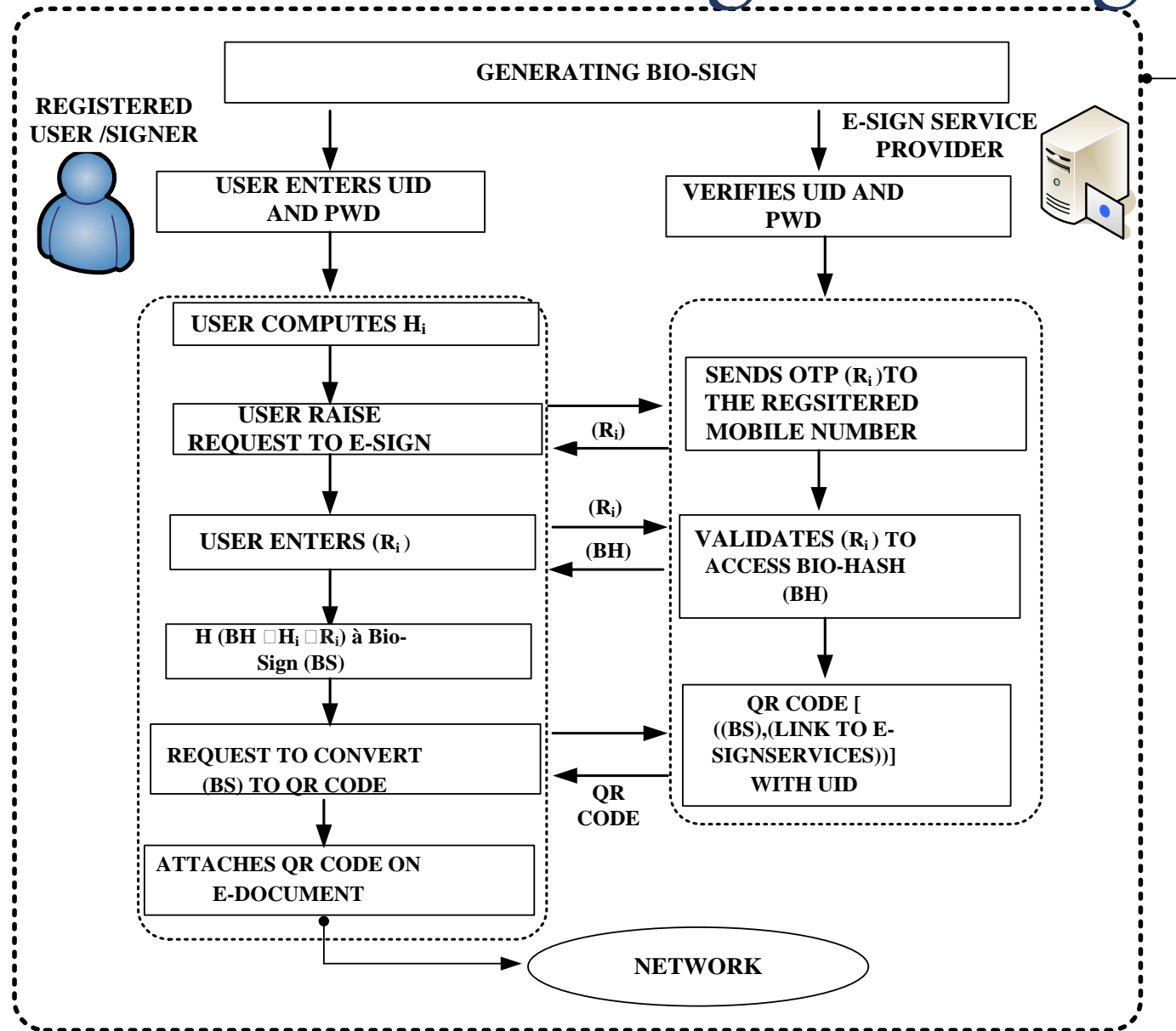


Fig.4: Process flow of Generating Bio-Sign for the e-Document

Verification of Bio-Sign and e-Document

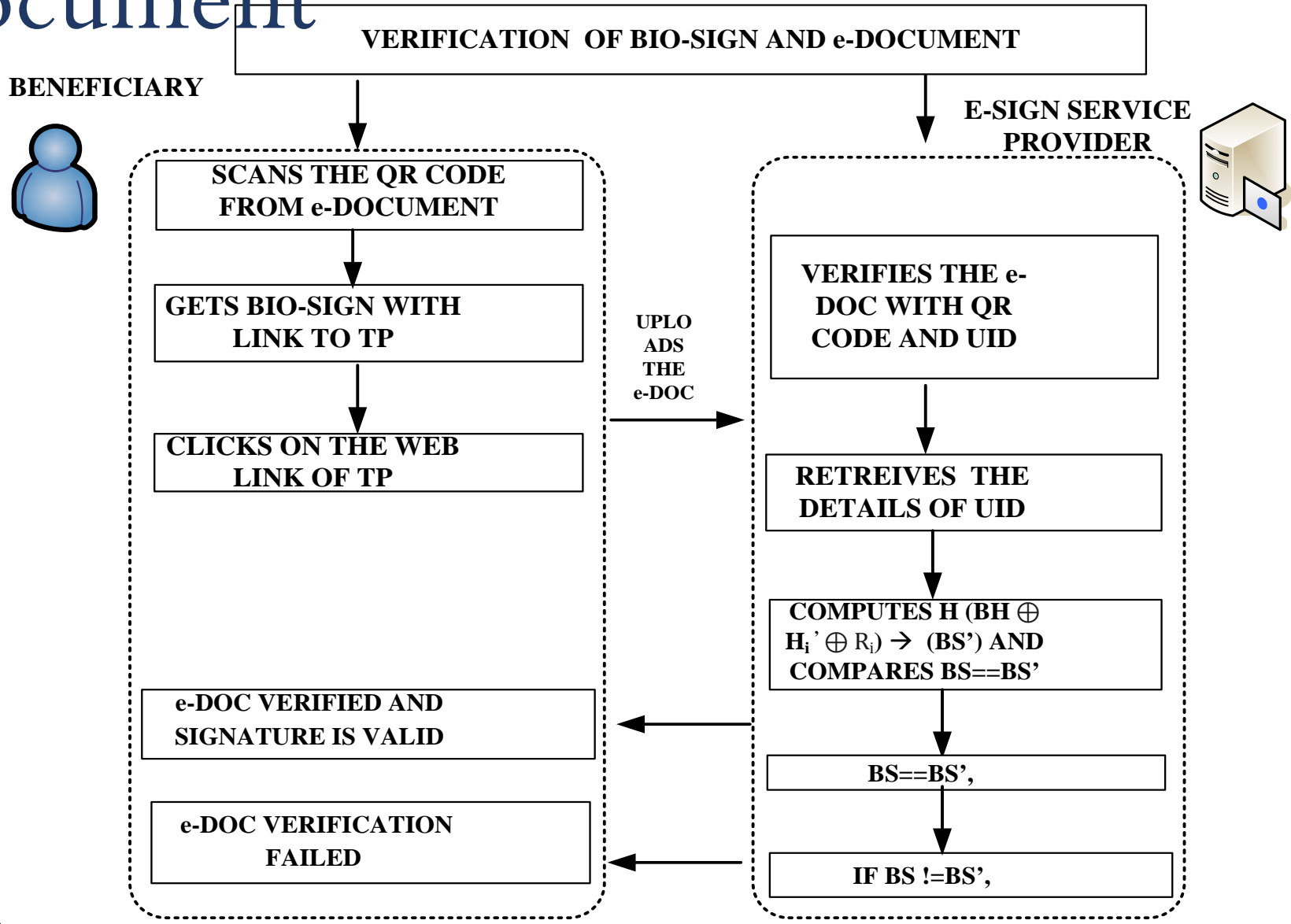


Fig.5: Process flow diagram of verification of Bio-Sign and the e-Document



Providing Non – Repudiation using Positive Identification

Step1: If registrant repudiate sending the signed e-Document, positive identification of the registrant can be done using his Bio – Hash.

Step2: The DNA of the registrant will be collected and based on the DNA extraction protocol and STR the Signature DNA will be generated and computes Bio – Hash.

Step3: Comparing original Bio-Hash (BH) with Bio-Hash (BH') stored with the trusted third party proves the matching probability of DNA based Bio – Hash.



Proof of Concept

- The QR code with Sample Bio – Sign and link to the service provider.



Fig.6: QR code with Bio-Sign and a link to the e-Sign service provider.

Security Analysis

Authentication

- User Authentication
- e – Document Authentication

Non – Repudiation

Data Integrity

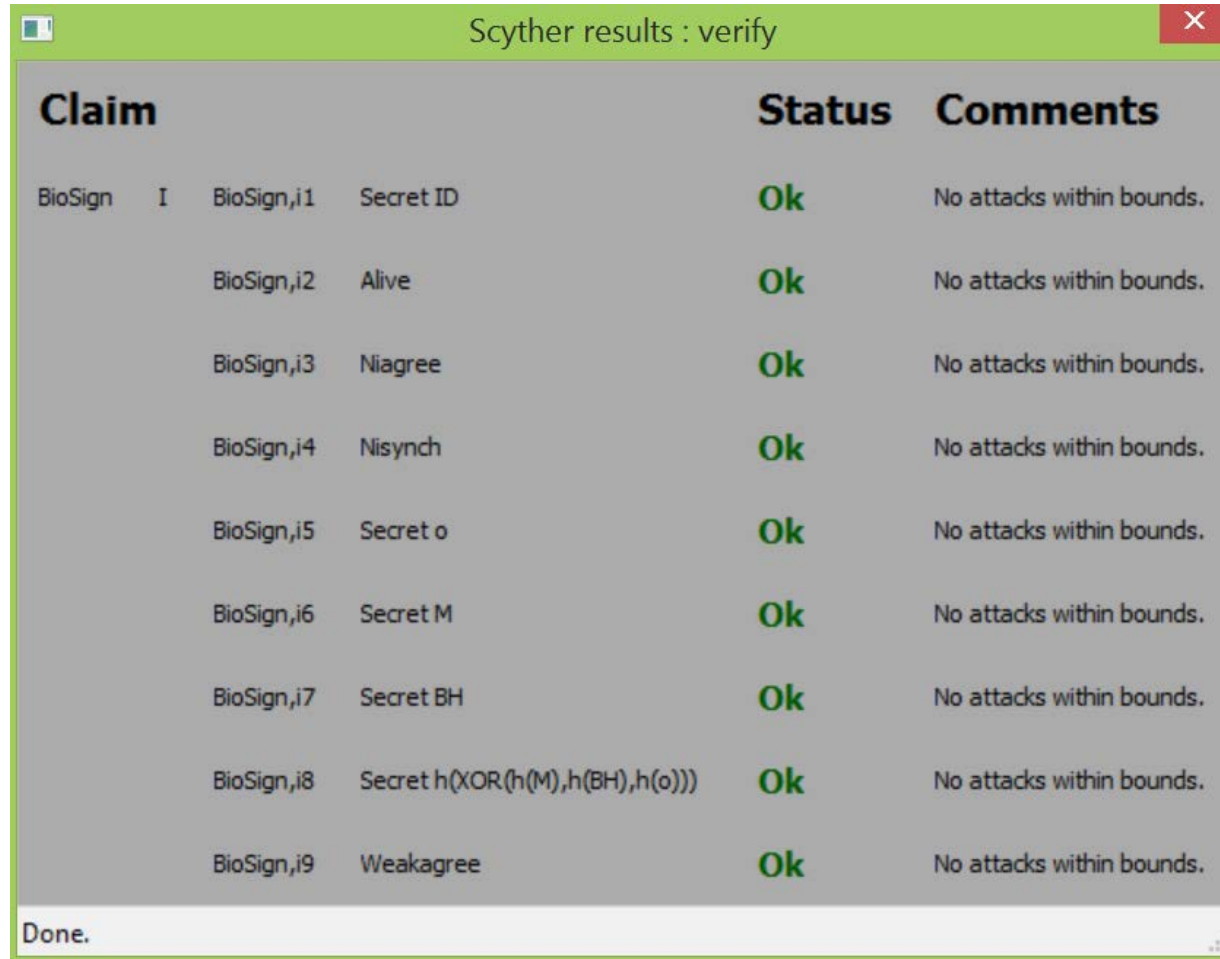
$$H (BH \oplus H_i \oplus R_i) \rightarrow \text{Bio - Sign (BS)} \rightarrow (1)$$

During the verification process equation (2) ensures the integrity of the document and signature,

$$H (BH \oplus H_i' \oplus R_i) = H (BH \oplus H_i \oplus R_i),$$

$$BS == BS' \rightarrow (2)$$

Formal Analysis using Scyther



Claim				Status	Comments
BioSign	I	BioSign,i1	Secret ID	Ok	No attacks within bounds.
		BioSign,i2	Alive	Ok	No attacks within bounds.
		BioSign,i3	Niagree	Ok	No attacks within bounds.
		BioSign,i4	Nisynch	Ok	No attacks within bounds.
		BioSign,i5	Secret o	Ok	No attacks within bounds.
		BioSign,i6	Secret M	Ok	No attacks within bounds.
		BioSign,i7	Secret BH	Ok	No attacks within bounds.
		BioSign,i8	Secret $h(\text{XOR}(h(M), h(BH), h(o)))$	Ok	No attacks within bounds.
		BioSign,i9	Weakagree	Ok	No attacks within bounds.

Done.

Fig.7: Formal Analysis of the proposed protocol using Scyther

Conclusion

- A methodology is proposed to create a DNA based Bio- Signature for e – Document which ensures Authentication, Integrity and Non – Repudiation.
- The proposed technique also has a verification method for the verifier with zero knowledge about Bio – Hash which also ensures the privacy of the signer.
- Formal analysis of the protocol is performed using Scyther and security claims are validated.

References

1. Discovery of DNA Double Helix: Watson and Crick | Learn ScienceatScitable.” [Online]. Available: <https://www.nature.com/scitable/topicpage/discoveryof-dna-structure-an-function-Watson-397>. [Accessed: 4 - Nov -2017].
2. The chemical structure of a nucleotide. | Learn at Scitable.” [Online]. Available: <https://www.nature.com/scitable/content/thechemical-structure-of-anucleotide104573606>. [Accessed: 4 - Nov -2017].
3. A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: A tool for information security,” IEEE Trans. Inf. Forensics Secur., vol. 1, no. 2, pp. 125–143, 2006.
4. J. Kar and B. Majhi, “Personal Authentication Protocol based on www.pkiindia.in www.facebook.com/pkiindia [PKIIndia](https://www.youtube.com/channel/UC...) [@pkiindia](https://twitter.com/pkiindia)

References

ECDLP using Biometric Feature Values, "IJCSNS International Journal of Computer science Network Security., vol. 9, no. 6, 2009.

5. Padgett, Robert D., and John C. Maxwell III. "Digital signature providing non-repudiation based on biological indicia." U.S. Patent 6,535,978, issued March 18, 2003.
6. Y. Itakura and S. Tsujii, "Proposal on Bio-PKI in which DNA Personal Identifier is embedded in Public Key."
7. J. Wayman, A. Jain, D. Maltoni, and D. Maio, "An Introduction to Biometric Authentication Systems," Biometric Syst., pp. 1–20, 2005.
8. DNA profiling in India," Nature. Methods, vol. 12, no. 11, pp. 995–995, 2015.



Thank You

