

Formal security proofs for medical cryptographic protocols

R. G. Hemanth Kumar *

Department of Forensic Medicine & Toxicology

Krishna Institute of Medical Sciences

Krishna Vishwa Vidyapeeth (Deemed to be University)

Karad 415539

Maharashtra

India

Varun Kumar Sharma [†]

Department of Biotechnology & Microbiology

Noida International University

Greater Noida 201312

Uttar Pradesh

India

Saudagar Subhash Barde [§]

Department of Information Technology

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

Y. Vijay Kumar [‡]

Department of Electronics & Communication Engineering

Pragati Engineering College

Kakinada 533437

Andhra Pradesh

India

* E-mail: drhemanthkumarrg@gmail.com (Corresponding Author)

[†] E-mail: varun1.sharma@niu.edu.in

[§] E-mail: saudagar.barde@vit.edu

[‡] E-mail: vijaykumar@outlook.com

C. Kavitha [®]

*Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India*

Ponmurugan Panneerselvam [#]

*Department of Research
Meenakshi Academy of Higher Education & Research
Chennai 600087
Tamil Nadu
India*

Abstract

Given the critical role of medical information in medical cryptographic processes, it is essential to have rigorous security validation to prevent any vulnerabilities in the authentication process that could lead to unauthorized access and access to clinical information and allow unauthorized treatment decisions to be made. This study introduces a formal security-proof framework to assess the security of authentication, confidentiality, integrity, anonymity and security of session-keys in connected healthcare settings. The proposed protocol uses finite field operations, cryptographic hashes, key derivation functions, random nonces, timestamps and medical professionals and patients. Adversarial games, mutual-authentication proofs, session-key indistinguishability and resistance to replay, impersonation, man-in-the-middle and privileged-insider attacks are discussed in the context of security. The formal reasoning approach has a negligible adversarial advantage, given the computational assumptions. Comparative evaluation shows the overhead of the authentication process is lower, but the protection of the medical devices is still high, even when considering the limited resources of medical devices. The framework provides a mathematically sound basis for designing reliable, private and effective healthcare communication systems in a heterogeneous clinical network and infrastructure.

Subject Classification: 94A60.

Keywords: Formal security proof, Medical cryptographic protocol, Mutual authentication, Session-key security, Healthcare privacy.

[®] E-mail: kavitha1616@vardhaman.org

[#] E-mail: ponmurugan@maher.ac.in

I. Introduction

Today's healthcare is increasingly reliant on health data, medical devices, eHRs, telemedicine and cloud health services. All these technologies provide better access and better information for decision making, but they also enable the transmission of very sensitive patient information across potentially non-trustworthy networks [1, 2]. As a result, medical communication protocols have come to have the following requirements: authentication, confidentiality, integrity, privacy, and availability. The security that conventional cryptographic protocols often achieve is based on informal discussions of attacks in their adversarial models; however, these attacks cannot provide protection against adaptive adversaries with full capabilities [3, 4, 5]. Formally secure proofs offer mathematically structured security proof by introducing models of adversaries, games and security, computational assumptions and negligible success probabilities. This enables discovery of the weak points in the system even before it is used in practice [6, 7]. The developed formal framework for medical authentication over patients, healthcare professionals, wearable sensors, gateways and medical servers [8, 9] is developed. It uses finite-field operations, cryptographic hash functions, key-derivation mechanisms, timestamps, random nonces, and session keys. It analyzes and provides some measurement of mutual authentication, anonymity, unlinkability, forward secrecy and session-key indistinguishability, in the attack models [10, 11, 12]. The proofs considered are against replay, impersonation, man-in-the-middle, stolen-device, insider and key-compromise attacks. Resource-constrained devices are also taken into account in the performance analysis, by considering resource cost of computation, communication and storage [13, 14].

II. Mathematical Preliminaries and Cryptographic Foundations

It introduces mathematical suppositions, algebraic models, cryptographic primitives, probability models and basic notation that are needed to express and formally prove medical security protocols to various potential adversaries.

A. Algebraic Groups and Finite Fields

Cyclic algebraic groups and finite fields are suitable secure computational area for modular arithmetic, scalar multiplication, discrete log problem and efficient key generation in healthcare system and devices [15].

$$F_p = \{0, 1, 2, \dots, p-1\}, p \in P \quad (1)$$

A closed algebraic domain for secure modular cryptographic computations and key operations is defined by equation (1) as the finite field F_p of integers from 0 to $p-1$ that are prime.

$$a \oplus b = (a + b) \bmod p, a, b \in F_p \quad (2)$$

$$a \otimes b = (a \times b) \bmod p \quad (3)$$

This is the modular addition (shown in equation (2)), which ensures that the addition of two field elements and the result's reduction modulo p guarantees that the result is still in F_p and ensures that the field elements are still in the F_p

during the process. Modular multiplication is described by equation (3) which works out the product of two elements, taking modulo p . This operation is useful for protocols that require to generate cryptographic values in an efficient way, perform scalar arithmetic and other efficient group computations.

$$a^{-1} = a^{p-2} \bmod p, a \neq 0 \quad (4)$$

The creation of the multiplicative inverse is done securely using Fermat's little theorem in equation (4); for this reason, every nongenerate field element has exactly one multiplicative inverse needed to do division, signature creation and verification, and elliptic-curve calculations securely.

$$y = \sqrt{[(x^3 + ax + b) \bmod p]} \quad (5)$$

In Equation (5) the coordinates of an elliptic-curve point are plotted on the curve equation (modulo p); the square root operation can be used to find valid y-coordinates for the selected x-coordinate used in point construction securely.

$$K_{PM} = (g^{x_M})^{x_P} = (g^{x_P})^{x_M} = g^{x_P \times x_M} \bmod p \quad (6)$$

In (6) the shared secret of the Diffie–Hellman method is written – both parties independently calculate their own value, and the value calculated by one party is equal to that calculated by the other party, but this value is not sent directly to the outside of the session key directly and openly.

B. Cryptographic Hash and Key-Derivation Functions

Hash functions allow for integrity and make the identity of a medical entity impossible to reverse while key-derivation functions create different session keys based on a secret and nonce, password and context, time or the location of the medical entity.

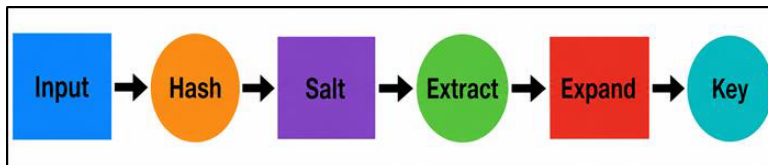


Figure 1
Cryptographic Hash and Session-Key Derivation Framework

Figure 1 shows the sequential hashing, salting, extraction and expansion processes to securely generate a strong and unpredictable session key for medical authentication protocols.

$$H: \{0,1\}^* \rightarrow \{0,1\}^n \quad (7)$$

Equation (7) represents a cryptographic hash function that maps any binary string of arbitrary length into a n -bit digest, which can be used for integrity checking, compact representation and a one-way function to process sensitive healthcare information.

$$HID_P = H(|ID_P||r_P|K_{MS}) \quad (8)$$

The patient-identity hash is created by Equation (8) which is a combination of patient identifier, the random value and the master secret, thus hiding the patient's identity and preventing unauthorized recognition, correlation or impersonation during authentication.

$$\Pr[H(m_1) = H(m_2) \wedge m_1 \neq m_2] \leq \text{negl}(\lambda) \quad (9)$$

The collision resistance of equation (9) quantifies the probability of finding two different messages that have the same hash output to be negligible compared to the security parameter λ which further enhances message authenticity and tampering resistance.

$$PRK = \text{HMAC}_{s(|K_{PM}||N_P|N_M)} \quad (10)$$

The shared secret, participant nonces and HMAC are used in Equation (10) to extract a pseudorandom key. This is a process for attaching new session data with the authenticated cryptographic data for the secure generation of keys.

$$D_H = \sqrt{\left[\left(\frac{1}{n}\right) \sum_{i=1}^n (h_i - h'_i)^2\right]} \quad (11)$$

The RMSD value of two hash sequences is computed from Equation (11) which measures the bit-level difference and the diffusion behavior of the two hash sequences. The greater the deviation, the greater the avalanche's effects and the more resistant to statistical hash prediction attacks it is.

$$SK_{PM} = \text{KDF}[|K_{PM}||HID_P||ID_M| \int_0^T E(t) dt] \quad (12)$$

The shared secret, protected identity, medical-entity identifier and integrated entropy are used to derive session key from it using Equation (12). Time dependent entropy enhances freshness, unpredictability, contextual binding and replay, guessing and compromise.

C. Security Parameters and Mathematical Notation

The security parameter influences the complexity of the computation, the length of keys and the advantage of the adversary, and mathematical symbols are consistently used to represent entities, identities, nonces, timestamps, messages, keys, probabilities, and protocol operations.

$$\lambda \in N, |SK_{PM}| \geq \lambda \quad (13)$$

The security parameter λ is defined in (13) and the length of the session keys should be at least as long as λ . The greater the value of λ , the greater the computational protection will be as it will increase the amount of effort that is required for an exhaustive key search.

$$\text{negl}(\lambda) < \lambda^{-c}, \text{ for every } \lambda > \lambda_0 \quad (14)$$

The definition of a negligible function given in equation (14) makes it so that its value eventually becomes smaller than any inverse polynomial. It gives a probability of attack that decreases quickly with the security parameter and hence gives asymptotic security.

$$\text{Adv}_A^{\text{SEC}(\lambda)} = \left| \Pr[b' = b] - \frac{1}{2} \right| \quad (15)$$

Adversarial advantage is calculated in terms of the absolute difference between the probability of successful guess and $\frac{1}{2}$ in (15). Numbers close to zero mean that the opponent doesn't see any difference between the actual and random results.

$$Adv_{RMS} = \sqrt{\left[\left(\frac{1}{q}\right) \sum_{i=1}^q (Adv_i)^2\right]} \quad (16)$$

The equation (16) sums up all the advantages (or disadvantages) over the n experiments and takes the root mean square. This measure highlights the bigger deviations and quantifies the overall robustness of the protocol, while giving a unified evaluation of repeated attacks and their deviations.

$$|T_{current} - T_{received}| \leq \Delta T \quad (17)$$

$$R_{A(T)} = (0 \text{ to } T) Adv \int_A^{SEC(\lambda, t)} dt \quad (18)$$

To verify the freshness of the messages, the difference between the current and received timestamp is bounded by ΔT in equation (17). The transmission of messages is denied as delayed or replayed messages, if they are received outside of this interval. The value of equation (18) is the sum of the security risk over the interval $[0, T]$ with T being time varying. A decreasing value of the integral means that there's ongoing resistance, whereas a growing value means that there's long-term exposure, which needs more protection.

III. Mathematical Formulation of the Medical Security Protocol

The proposed formulation mathematically defines the operations for entity registration, the generation of credentials, exchange of authentication, establishment of a session-key and verification operations needed to provide a secure communication between interconnected medical participants and servers reliably.

A. Patient and Medical-Entity Identity Representation

The identities of the patient or patient-entity are rendered anonymous yet identifiable through the use of cryptographic hashing, random numbers and secret credentials, such that no identity information is given away and no unauthorized tracing is possible for healthcare communication.

$$PID_P = H \left[|ID_P| |PW_P| |r_P| \sqrt{x_P^2 + y_P^2} \right] \quad (19)$$

The combination of the patient ID, the password, the random value and the magnitude of the coordinate is subjected to a hash in equation (19) and codes the patient identity. This builds-in protection of credentials and securely bind authentication information to patient-specific cryptographic parameters.

$$MID_M = H \left[|ID_M| |K_{MS}| |r_M| \sqrt{x_M^2 + y_M^2} \right] \quad (20)$$

The encoding of medical-entity identity is generated from the identifier, the master secret, the randomness and the magnitude of the coordinates by the

equation (20). The digest leaves out the institutional credentials and enables the verifiable participation in the healthcare authentication exchanges securely.

$$HPID_P = PID_P \oplus H[|K_{MS}||T_P|\sqrt{N_P \times r_P}] \quad (21)$$

The secret ID of the patient is protected in the above equation (21) by XOR'ing with a patient-specific hash that is determined by a time stamp. The nonce and random-value elements are quite good at offering freshness, unlinkability, and deterring identity disclosure attacks.

$$HMID_M = MID_M \oplus H[|K_{MS}||T_M|\sqrt{N_M \times r_M}] \quad (22)$$

The same is performed in equation (22) when the identity digest of the medical entity is hidden, its master secret, its time stamp, its nonce, and its randomness. This allows the entity to be tracked without the need for the server to be authorized, but also allows for the recovery of verification information to the authorized servers with security.

$$CID_{PM} = H[|HPID_P||HMID_M|\sqrt{(PID_P - MID_M)^2 + (r_P - r_M)^2}] \quad (23)$$

Protected patient pseudonyms and their identity distance are merged with their identity and randomness distance in the protected medical entity pseudonyms in equation (23). By combining these two data types in such a way, and applying hashing to it, this new data type creates a cryptographic tie between both parties in an authentication transaction.

$$DID_P^{t+1} = H[|DID_P^t||SK_{PM}||N_P|\sqrt{|T_{t+1} - T_t|}] \quad (24)$$

The patient's identity is updated in equation (24) by adding the patient's identity hash, previous identity, session key, nonce and the variation of the timestamp. Continuous renewal will continually re-establish forward privacy, prevent session linkability and constrain credential re-use.

B. Authentication-Message Construction

Authentication messages include pseudonym, nonces, timestamps, credentials and hash output – so that recipients can check that the message is fresh, correct, legitimate and mutually authentic before they can use it to generate secure session keys to communicate.

$$M_1 = H[|HPID_P||N_P||T_P|\sqrt{K_{PM}^2 + r_P^2}] \quad (25)$$

In the patient authentication message, the magnitude of the shared key is computed as a hash of the patient protected pseudonym, nonce, timestamp and shared-key magnitude. The message shows freshness, integrity and legitimate patient participation in the authentication of this message securely.

$$M_2 = H[|HMID_M||N_M||T_M||M_1|\sqrt{N_P \times N_M}] \quad (26)$$

Using medical-entity authentication message, protected pseudonym, entity nonce, timestamp, patient message and nonce-product magnitude, Equation (26) produces medical-entity authentication message. This is to ensure that the

medical entity involved in the exchange is a responsive one, and it also helps to bind the two parties involved.

$$AUTH_{PM} = H[|M_1||M_2||SK_{PM}|\sqrt{(N_P - N_M)^2 + (T_P - T_M)^2}] \quad (27)$$

By combining the two authentication messages, established session key, nonce difference and timestamp difference all with the help of equation (27), a mutual authentication token is generated. Matching values are used to ensure that values are matched as well as in both directions, and that the protocol is executed in synchronization.

$$SK_{PM} = KDF[|K_{PM}||HPID_P||HMID_M|\sqrt{N_P^2 + N_M^2 + T_P^2 + T_M^2}] \quad (28)$$

The session key is generated by a key-derivation function (KDF) in equation (28), which uses shared secret, protected pseudonyms of the participants, nonces, and timestamps. This yields new, context-specific, random keys which can be used for the encrypted exchange of medical information.

$$V_{PM} = \sqrt{[(H(M_1)' - H(M_1))^2 + (H(M_2)' - H(M_2))^2]} = 0 \quad (29)$$

For equation (29) to verify authentication, it is required to calculate the differences between the hash of the received message and the recomputed hash of the message according to the same hash function, computed as the root-sum-square. If the result is zero, it means that there is no change or that it has not been tampered with; if it doesn't display zero, it means it was altered or tampered with.

$$M_3 = H[|AUTH_{PM}||SK_{PM}||T_S|\sqrt{N_P \times N_M \times K_{PM}}] \quad (30)$$

Final authentication message is created using Equation (30) where mutual token, session key, server timestamp and combination of nonce-key magnitude are all hashed. It confirms successful completion, maintains integrity of transcript and recognizes successful establishment of session.

IV. Result and Discussion

The formal analysis proves that mutual authentication, confidentiality, anonymity and session-key security are achieved, and the performance analysis shows that the overall computational, communication and storage cost of resource constrained medical devices and networks are reduced.

Table 1
Comparative Performance of Medical Authentication Protocols

Protocol	Computation Time (ms)	Storage Cost (KB)	Authentication Latency (ms)	Energy Consumption (mJ)
Protocol 1	18.72	6.40	32.84	14.62
Protocol 2	16.35	5.75	29.46	12.83
Protocol 3	14.68	5.20	26.71	11.29
Protocol 4	12.94	4.65	23.58	9.87
Proposed Protocol	9.86	3.80	18.42	7.64

Table 1 shows that the proposed method has the optimal performance for all the performance measures evaluated. The amount of time used in its computation reduced to 9.86 ms and storage cost is only 3.80 KB. Authentication latency is as quick as 18.42ms, enabling quicker authentication for time-sensitive healthcare applications. The energy consumption is lowered to 7.64 mJ, giving the protocol the power to be used in resource limited sensors, such as medical sensors.

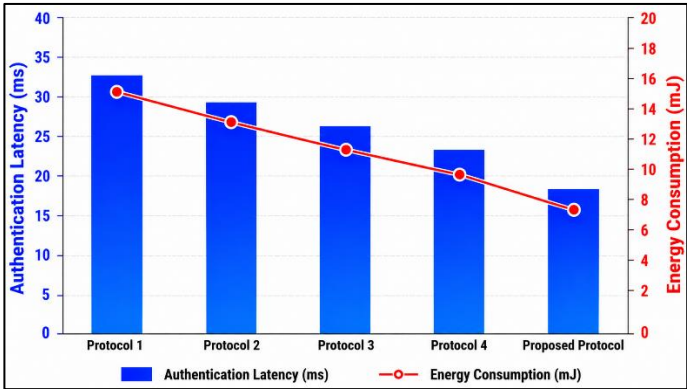


Figure 2
Comparative Analysis of Authentication Latency and Energy Consumption Across Cryptographic Protocols

Figure 2 shows that the proposed protocol realises a minimum latency and energy consumption. These improvements when compared with Protocol 1, are found to be having lower processing, memory, communication-delay and energy consumption requirements with the same authentication security.

V. Conclusion

The aim of this work was to build a mathematically sound and precise model for guaranteeing medical cryptographic protocols in inter-connected healthcare settings. The proposed formulation combines the ideas of finite-field operations, cryptographic hashing, key-derivation functions, timestamps, nonces and pseudonymous identities, thus enabling secure authentication and session-key establishment. Formal adversarial analysis was performed and resistance to replay, impersonation, man-in-the-middle, insider, stolen-device, and key-compromise attacks was shown without compromising patient anonymity, confidentiality, integrity or unlinkability. Performance evaluation also showed that the resource-constrained medical devices have acceptable computational, communication and storage needs. It can thus serve as a solid basis for the development of verifiable, efficient and private healthcare protocols and thus enhance trust in future digital healthcare infrastructures.

References

- [1] D. G. Duguma, I. You, Y. E. Gebremariam, and J. Kim, "Can formal security verification really be optional? Scrutinizing the security of IMD authentication protocols," *Sensors*, vol. 21, no. 24, Art. no. 8383 (2021), doi: 10.3390/s21248383.
- [2] S. Lee, K. A. Kang, S. Lee, and J. Kim, "Exploring authentication protocols for secure and efficient Internet of Medical Things systems," *Electronics*, vol. 14, no. 21, Art. no. 4164 (2025), doi: 10.3390/electronics14214164.
- [3] J. Kim, J. Oh, D. Son, H. Kwon, P. V. Astillo, and I. You, "APSec1.0: Innovative security protocol design with formal security analysis for the artificial pancreas system," *Sensors*, vol. 23, no. 12, Art. no. 5501 (2023), doi: 10.3390/s23125501.
- [4] Z. Rajabinejad and S. M. Semnani, "Calculation and comparison of energy and energy based on Mostar index of the double-star graph and its line graph," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 4, pp. 1585–1594 (2025), doi: 10.47974/JDMSC-2246.
- [5] H.-Y. Chen, Z.-Y. Wu, T.-L. Chen, Y.-M. Huang, and C.-H. Liu, "Security privacy and policy for cryptographic based electronic medical information system," *Sensors*, vol. 21, no. 3, Art. no. 713 (2021), doi: 10.3390/s21030713.
- [6] K. A. Delgado-Vargas, G. Gallegos-Garcia, and P. J. Escamilla-Ambrosio, "Cryptographic protocol with keyless sensors authentication for WBAN in healthcare applications," *Appl. Sci.*, vol. 13, no. 3, Art. no. 1675 (2023), doi: 10.3390/app13031675.
- [7] N. J. Rad and R. Hasni, "Note on placement of security nodes in graphs associated to the Internet of Things," *J. Inf. Optim. Sci.*, vol. 47, no. 2, pp. 507–512 (2025), doi: 10.47974/JIOS-1572.
- [8] X. Chen and H. Deng, "Efficient verification of cryptographic protocols with dynamic epistemic logic," *Appl. Sci.*, vol. 10, no. 18, Art. no. 6577 (2020), doi: 10.3390/app10186577.
- [9] H. Lim, Y. Park, and Y. Park, "A PUF-based secure and lightweight authentication protocol for medical IoT environments," *Sensors*, vol. 26, no. 10, Art. no. 3223 (2026), doi: 10.3390/s26103223.
- [10] A. Singh, V. S. Sharma, S. Basheer, and C. L. Chowdhary, "A deep cryptographic framework for securing the healthcare network from

- penetration," *Sensors*, vol. 24, no. 21, Art. no. 7089 (2024), doi: 10.3390/s24217089.
- [11] M. Anagreh and P. Laud, "Security proof of single-source shortest distance protocols built on secure multiparty computation protocols," *Cryptography*, vol. 9, no. 1, Art. no. 1 (2025), doi: 10.3390/cryptography9010001.
- [12] A. Kilitçi Calayır and S. Alp, "A blockchain-based framework for privacy-preserving medical report sharing and diagnosis-free verification," *Appl. Sci.*, vol. 16, no. 13, Art. no. 6596 (2026), doi: 10.3390/app16136596.
- [13] M. A. Khan, S. Ullah, T. Ahmad, K. Jawad, and A. Buriro, "Enhancing security and privacy in healthcare systems using a lightweight RFID protocol," *Sensors*, vol. 23, no. 12, Art. no. 5518 (2023), doi: 10.3390/s23125518.
- [14] S. Zhang, Y. Yin, N. Chen, and H. Ning, "A lightweight decentralized medical data sharing scheme with dual verification," *Cryptography*, vol. 9, no. 4, Art. no. 69 (2025), doi: 10.3390/cryptography9040069.
- [15] J. Piątkowski and S. Szymoniak, "Methodology of testing the security of cryptographic protocols using the CMMTree framework," *Appl. Sci.*, vol. 13, no. 23, Art. no. 12668 (2023), doi: 10.3390/app132312668.

Received March, 2026