Table 1: Overview of the reviewed papers that present novel works regarding PKI for IoT.

Name/ authors	Architecture	Technology used	Security analysis	Performance analysis	Comparison
IoT-PKI [1]	Decentralized	Blockchain	Mitigations / solutions for: • Private key compromise • Stolen IoT device • Weak random number generator on client • No available blockchain nodes	Certificate verification time: • At blockchain node: 10 ms • At IoT device: 128 ms	3 to 26 times faster than traditional PKI
Schukat and Cortijo [2]	Centralized	X.509 optimizations	Analysis not present	Analysis not present	Analysis not present
DECKIN [3]	Decentralized	Blockchain, PUF	Secure against: • Spoofing key updates • Spoofing key revocations	• Certificate verification time: 0.025 ms • Average protocol runtime: 35 ms	Analysis not present
Chanda et al. [4]	Centralized	PUF, ECC	• Proven secure under RoR model Resilient against: • Denial of Service • Malicious public key changes	Key generation: • Duration: 4.68 μs • Energy: 1.31 μJ Memory usage: • 680 KB on device • 2280.67 KB in communication	• $14-16\times$ faster • Requires $18-25\times$ less power
Aljadani and Gazdar [5]	Distributed	Clustering technique	Resilient to: • Sinkhole attacks • DoS	Analysis not present	Analysis not present
Siddiqui et al. [6]	Decentralized	PUF	Secure against: • Chosen plaintext attack • Session hijacking • Session forgery • Impersonation attacks • Message tampering • Replay attacks	Analysis not present	Provides more security features than other related works, such as device security and privacy
Singla and Bertino [7]	Decentralized	Blockchain	Analysis not present	• Certificate verification: 128-250 ms • Storage required: 0-382 MB • Cost: $0.07-0.18 per certificate • Time to issues certificate: 1-10 minutes	• $1.6-3\times$ faster than traditional PKI (with OCSP check) • $2.2-4.2\times$ slower than traditional PKI (without OCSP check)

Continued on next page

Table 1 – *Continued from previous page*

Name/ authors	Architecture	Technology used	Security analysis	Performance analysis	Comparison
μPKI [8]	Centralized	ECC	Ensures: • Confidentiality • Authentication • Integrity	• Encrypting session key: 22.82 mJ • Sending session key: 3.78 mJ • Receiving session key: 1.83 mJ • Sensor handshake: 3.70 mJ	• $1.23 - 1.48\times$ less energy than simplified Kerberos • $2.92\times$ less energy than simplified SSL
Magnusson [9]	Decentralized	Blockchain, smart contracts	Analysis not present	"Significant" CPU and RAM utilization	Analysis not present
Pintaldi [10]	Decentralized	Blockchain	Analysis not present	Handshake is $5 - 13.5\times$ slower than in conventional PKI	Analysis not present
LPKI [11]	Centralized	ECC	Analysis not present	Analysis not present	Analysis not present
Champagne [12]	Decentralized	Blockchain	Some identities are not verified, which could result in a DoS attack.	• Certificate signing: ~ 1.2 min • Memory usage: 20 Kb • Network usage: Up: 22 Kb/s, down: 15 Kb/s	Analysis not present
Höglund et al. [13]	-	X.509 optimizations	Analysis not present	• Average header size: 10 bytes • Compressed ECC certificate: ~ 150 bytes in size • ROM use: 3.7 KB • RAM use: 1.1 KB	• Average CoAP header size is $16\times$ smaller than HTTP
PKIoT [14]	Centralized	X.509 optimizations	Potentially vulnerable to: • Denial of Service • Eavesdropping • Tampering • Masquerading	• Key generation: 348 ms • Signature generation: 434 ms • Signature verification: 429 ms	• Key generation: $\sim 11.7\times$ faster • Signature generation: $\sim 9.5\times$ faster • Signature verification: $\sim 12.2\times$ faster
Diaz-Sanchez et al. [15]	-	Certificate pinning, certificate transparency	Analysis not present	Analysis not present	Analysis not present

Table 2: Overview of the reviewed papers that present novel works regarding cryptography for IoT.

Name/ authors	Technology used	Security analysis	Performance analysis	Comparison
Yu and Li [16]	Pairing-based encryption	Secure against: • User impersonation attack • Replay attack • Insider attack Other properties: • Key forward secrecy • Strong key establishment • Proven secure through BAN logic	• Whole scheme cost: 3.1 s	$1.48 - 8.38\times$ slower than peer works
Tiwari and Kim [17]	DNA	• Through the proposed DNA mapping, existing ECC is more resilient to timing and SPA attacks. The scheme: • Converts repetitive data to pseudo-random data	• Encryption and decryption take a linear amount of time in relation to the input size	Analysis not present
Tewari and Gupta [18]	ECC	Properties: • Mutual authentication • Anonymity • Confidentiality • Availability • Resistant to DoS	• Storage cost: 576 bits • Communication cost: 1152 bits	• $0.69 - 1.64\times$ less storage required • $0.88 - 1.63\times$ more communication required
Szczechowiak et al. [19]	Pairing-based cryptography	Analysis not present	• The first pairing scheme requires on average 33.54 KB of ROM on the tested platforms • The second pairing scheme requires on average 46.73 KB of ROM on the tested platforms • The fastest implementations at the time of writing	Analysis not present

Continued on next page

Table 2 – *Continued from previous page*

Name/ authors	Technology used	Security analysis	Performance analysis	Comparison
Shi and Gong [20]	ECC	Provides: • Mutual authentication • Perfect forward secrecy Resistant to: • Replay attack • User impersonation attack • Sensor impersonation attack • Gateway impersonation attack • Man-in-the-middle attack • Insider attack	Approx. 30% faster than its predecessor [21]	Approx. 30% faster than its predecessor [21]
ECIOT [22]	ECC, DH	Analysis not present	Analysis not present	Analysis not present
Rajendiran et al. [23]	ECC	Highly resilient to: • Sybil attack • Random attack • Brute force attack	Analysis not present	Superior resilience to attacks like brute force and Sybil
Qazi et al. [24]	ECC	Provides: • User anonymity • User untraceability • Resistance to various attacks • Session key agreement • Mutual authentication	• Key generation between two nodes: 50 ms • Authentication between two nodes only requires six packets	Analysis not present
Louw et al. [25]	ECC	Analysis not present	Analysis not present	Analysis not present
Ju [26]	ECC	• Resilient against MITM • Perfect forward secrecy	• Storage linear to number of nodes • 10 seconds to establish a 10-node network	Analysis not present
Elhoseny et al. [27]	ECC	Secure against: • Passive attack • Brute force attack • Compromised CH • Sinkhole attack • DoS attack • HELLO flood attack	• CPU cycles: 66201 • Time: 8.619 ms • RAM 281 bytes • ROM 3845 bytes	• 0.94 – 8.9 fewer CPU cycles • 0.99 – 9.16× faster • 1.04 – 3.47× less RAM • 1.37 – 1.88× less ROM

Continued on next page

Table 2 – *Continued from previous page*

Name/ authors	Technology used	Security analysis	Performance analysis	Comparison
Pinol et al. [28]	ECC	Analysis not present	For a 256-bit key size: • Key generation: $\sim$5000 ms, 75.93 mJ • Signature verification: $\sim$11 s, 153.84 mJ • Signature generation: $\sim$5 s, 76.23 mJ	Analysis not present
Bai et al. [29]	ECC	Provides: • Authentication • Integrity • Confidentiality	Analysis not present	Analysis not present
Liu and Seo [30]	ECC	Protected against: • Timing attacks • Simple side-channel attacks	Clock cycles: • NUMS256: 543/429 • Ted37919: 1126/884 • NUMS384: 1139/898	NUMS256 is 1.6× faster than Curve25519
Al-Husainy et al. [31]	DNA	• Peak signal-to-noise ratio comparable to AES	• Key size: 24 bit	• $1.5-5.4\times$ faster than AES • Peak signal-to-noise ratio comparable to AES
Lara-Nino et al. [32]	ECC	Analysis not present	Runtime: 2.69-6.72 ms	• Requires fewer slices • $0.01-8.6\times$ faster
Forsby et al. [33]	X.509 optimizations	Analysis not present	• Optimized X.509 certificate: 484 bytes • Compressed: 146 bytes	• 4.5× smaller than a regular certificate • 14.8× smaller than a regular certificate (with compression)
Anggorojati and Prasad [34]	Identity-based cryptography	• Mutual authentication	Analysis not present	Analysis not present
Khari et al. [35]	ECC	• Mean squared error: 0.02 • Peak signal-to-noise ratio: 70 dB	• Time for encryption and decryption: 0.4 sec	• $1.5-2\times$ faster • $52.5-75\times$ lower mean squared error • $1.5-2.3\times$ higher peak signal-to-noise ratio

Continued on next page

Table 2 – *Continued from previous page*

Name/ authors	Technology used	Security analysis	Performance analysis	Comparison
Albalas et al. [36]	ECC, CoAP	Ensures: • Confidentiality • Authorization • Integrity • Authentication	Power required: ~ 0.7 W	Requires $1.14 - 1.57\times$ less power than regular CoAP
TinyECC [37]	ECC	Analysis not present	• Initialization: 5.64-5202 ms, 1.4-83.84 mJ • 11.40-20.77 KB of ROM • 1.5-2.1 KB of RAM	Analysis not present
Henriques and Vernekar [38]	(A)symmetric cryptography	Analysis not present	Analysis not present	Analysis not present

References

[1] Jongho Won, Ankush Singla, Elisa Bertino, and Greg Bollella. Decentralized public key infrastructure for internet-of-things. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, pages 907–913. IEEE, 2018.

[2] Michael Schukat and Pablo Cortijo. Public key infrastructures and digital certificates for the Internet of Things. In *2015 26th Irish signals and systems conference (ISSC)*, pages 1–5. IEEE, 2015.

[3] Mathijs Hoogland. A Distributed Public Key Infrastructure for the IoT. 2018.

[4] Susovan Chanda, Ashish Kumar Luhach, Waleed Alnumay, Indranil Sengupta, and Diptendu Sinha Roy. A lightweight device-level Public Key Infrastructure with DRAM based Physical Unclonable Function (PUF) for secure cyber physical systems. *Computer Communications*, 190:87–98, 2022.

[5] Nouf Aljadani and Tahani Gazdar. A New distributed PKI for WSN-Based Application in Smart Grid. In *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*, pages 1–5, 2020.

[6] Zeeshan Siddiqui, Jiechao Gao, and Muhammad Khurram Khan. An Improved Lightweight PUF-PKI Digital Certificate Authentication Scheme for the Internet of Things. *IEEE Internet of Things Journal*, 2022.

[7] Ankush Singla and Elisa Bertino. Blockchain-based PKI solutions for IoT. In *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, pages 9–15. IEEE, 2018.

[8] Benamar Kadri, Mohammed Feham, and Abdallah M'hamed. Lightweight PKI for WSN μPKI. *The Journal of Security and Communication Networks*, 10(2):135–141, 2010.

[9] Sebastian Magnusson. Evaluation of Decentralized Alternatives to PKI for IoT Devices: A literature study and proof of concept implementation to explore the viability of replacing PKI with decentralized alternatives, 2018.

[10] Lorenzo Pintaldi. *Implementation of a Blockchain-based Distributed PKI for IoT using Emercoin NVS and TPM 2.0.* PhD thesis, Politecnico di Torino, 2022.

[11] Mohsen Toorani and A Beheshti. LPKI-a lightweight public key infrastructure for the mobile environments. In *2008 11th IEEE Singapore International Conference on Communication Systems*, pages 162–166. IEEE, 2008.

[12] Loïc Champagne. Replacing Public Key Infrastructures (PKI) by blockchain IoT devices security management. 2021.

[13] Joel Höglund, Samuel Lindemer, Martin Furuhed, and Shahid Raza. PKI4IoT: Towards public key infrastructure for the Internet of Things. *Computers & Security*, 89:101658, feb 2020. doi: 10.1016/j.cose.2019.101658. URL https://doi.org/10.1016%2Fj.cose.2019.101658.

[14] Francesco Marino, Corrado Moiso, and Matteo Petracca. PKIoT: A public key infrastructure for the Internet of Things. *Transactions on Emerging Telecommunications Technologies*, 30 (10), jul 2019. doi: 10.1002/ett.3681. URL https://doi.org/10.1002%2Fett.3681.

[15] Daniel Diaz-Sanchez, Andrés Marín-Lopez, Florina Almenárez Mendoza, Patricia Arias Cabarcos, and R Simon Sherratt. TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications. *IEEE Communications Surveys & Tutorials*, 21 (4):3502–3531, 2019.

[16] Binbin Yu and Hongtu Li. Anonymous authentication key agreement scheme with pairing-based cryptography for home-based multi-sensor internet of things. *International Journal of Distributed Sensor Networks*, 15(9):155014771987937, sep 2019. doi: 10.1177/1550147719879379. URL https://doi.org/10.1177%2F1550147719879379.

[17] Harsh Durga Tiwari and Jae Hyung Kim. Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices. *ETRI Journal*, 40(3):396–409, jun 2018. doi: 10.4218/etrij.2017-0220. URL https://doi.org/10.4218%2Fetrij.2017-0220.

[18] Aakanksha Tewari and Brij B Gupta. A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. *International Journal of Advanced Intelligence Paradigms*, 9(2-3):111–121, 2017.

[19] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier. On the application of Pairing Based Cryptography to Wireless Sensor Networks. pages 1–12, 2009. doi: 10.1145/1514274.1514276. URL https://doi.org/10.1145/1514274.1514276.

[20] Wenbo Shi and Peng Gong. A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *International Journal of Distributed Sensor Networks*, 9(4):730831, apr 2013. doi: 10.1155/2013/730831. URL https://doi.org/10.1155%2F2013%2F730831.

[21] Hsiu-Lien Yeh, Tien-Ho Chen, Pin-Chuan Liu, Tai-Hoo Kim, and Hsin-Wen Wei. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, 11:4767–4779, 2011.

[22] Darshana Pritam Shah and Pritam Gajkumar Shah. Revisting of elliptical curve cryptography for securing Internet of Things (IOT). In *2018 Advances in Science and Engineering Technology International Conferences (ASET)*, pages 1–3. IEEE, 2018.

[23] Kishore Rajendiran, Radha Sankararajan, and Ramasamy Palaniappan. A Secure Key Predistribution Scheme for WSN Using Elliptic Curve Cryptography. *ETRI Journal*, 33 (5):791–801, oct 2011. doi: 10.4218/etrij.11.0110.0665. URL https://doi.org/10.4218%2Fetrij.11.0110.0665.

[24] Rosheen Qazi, Kashif Naseer Qureshi, Faisal Bashir, Najam Ul Islam, Saleem Iqbal, and Arsalan Arshad. Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, 12(1):547–566, apr 2020. doi: 10.1007/s12652-020-02020-z. URL https://doi.org/10.1007%2Fs12652-020-02020-z.

[25] J Louw, G Niezen, TD Ramotsoela, and Adnan M Abu-Mahfouz. A key distribution scheme using elliptic curve cryptography in wireless sensor networks. In *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, pages 1166–1170. IEEE, 2016.

[26] Song Ju. A lightweight key establishment in wireless sensor network based on elliptic curve cryptography. In *2012 IEEE International Conference on Intelligent Control, Automatic Detection and High-End Equipment*, pages 138–141. IEEE, 2012.

[27] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan. A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption. *Journal of King Saud University - Computer and Information Sciences*, 28(3):262–275, 2016. doi: 10.1016/j.jksuci.2015.11.001. URL https://doi.org/10.1016/j.jksuci.2015.11.001.

[28] Oriol Pinol Pinol, Shahid Raza, Joakim Eriksson, and Thiemo Voigt. BSD-based elliptic curve cryptography for the open Internet of Things. In *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5. IEEE, 2015.

[29] T Daisy Premila Bai, K Michael Raj, and S Albert Rabara. Elliptic curve cryptography based security framework for Internet of Things (IoT) enabled smart card. In *2017 World Congress on Computing and Communication Technologies (WCCCT)*, pages 43–46. IEEE, 2017.

[30] Zhe Liu and Hwajeong Seo. IoT-NUMS: evaluating NUMS elliptic curve cryptography for IoT platforms. *IEEE Transactions on Information Forensics and Security*, 14(3):720–729, 2018.

[31] Mohammed Abbas Fadhil Al-Husainy, Bassam Al-Shargabi, and Shadi Aljawarneh. Lightweight cryptography system for IoT devices using DNA. *Computers and Electrical Engineering*, 95:107418, 2021.

[32] Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval. Lightweight elliptic curve cryptography accelerator for internet of things applications. *Ad Hoc Networks*, 103:102159, 2020.

[33] Filip Forsby, Martin Furuhed, Panos Papadimitratos, and Shahid Raza. Lightweight x. 509 digital certificates for the internet of things. In *Interoperability, Safety and Security in IoT: Third International Conference, InterIoT 2017, and Fourth International Conference, SaSeIot 2017, Valencia, Spain, November 6-7, 2017, Proceedings 3*, pages 123–133. Springer, 2018.

[34] Bayu Anggorojati and Ramjee Prasad. Securing communication in inter domains Internet of Things using identity-based cryptography. In *2017 International Workshop on Big Data and Information Security (IWBIS)*, pages 137–142. IEEE, 2017.

[35] M. Khari, A.K. Garg, A.H. Gandomi, R. Gupta, R. Patan, and B. Balusamy. Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1):73–80, 2020. doi: 10.1109/TSMC.2019.2903785. URL https://doi.org/10.1109/TSMC.2019.2903785.

[36] Firas Albalas, Majd Al-Soud, Omar Almomani, and Ammar Almomani. Security-aware CoAP application layer protocol for the internet of things using elliptic-curve cryptography. *Power (mw)*, 1333:151, 2018.

[37] A. Liu and P. Ning. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. pages 245–256, 2008. doi: 10.1109/IPSN.2008.47. URL https://doi.org/10.1109/IPSN.2008.47.

[38] Michelle S Henriques and Nagaraj K Vernekar. Using symmetric and asymmetric cryptography to secure communication between devices in IoT. In *2017 International Conference on IoT and Application (ICIOT)*, pages 1–4. IEEE, 2017.