Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

G20 भारत 2023 INDIA

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

4TH INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2023)

SEPTEMBER 8-9TH, 2023

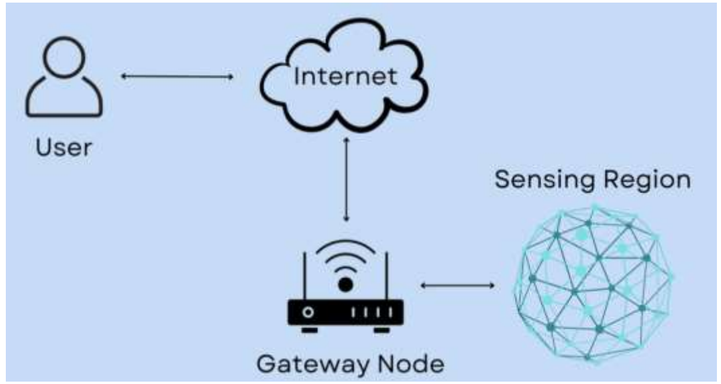
Lightweight Certificateless Digital Signature Scheme for WSNs

Rhithick Murali, NIT Trichy

Vivek Arunachalam, NIT Trichy

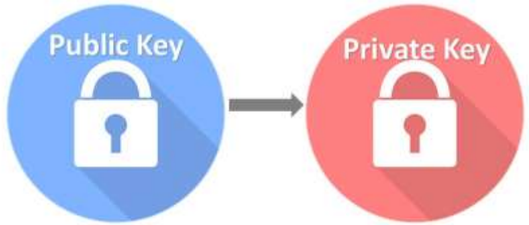
Introduction

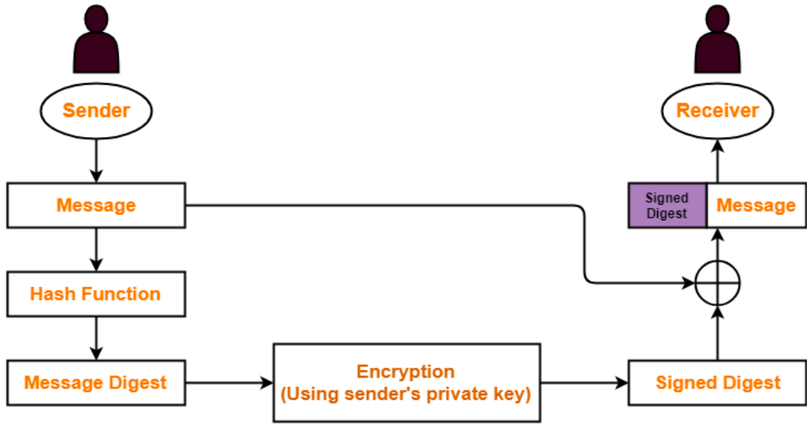
- *Several types of smart devices have emerged in this era.*
- *Ensuring safety and security of each node and to protect the data is important.*
- *In a public network how to ensure the security?*



Background

- *Authentication, Integrity and Confidentiality - 3 important factors in security.*
- *Encryption and digital signatures are different.*
- *Hash functions are irreversible.*
- *Public and private keys - mathematically generated.*



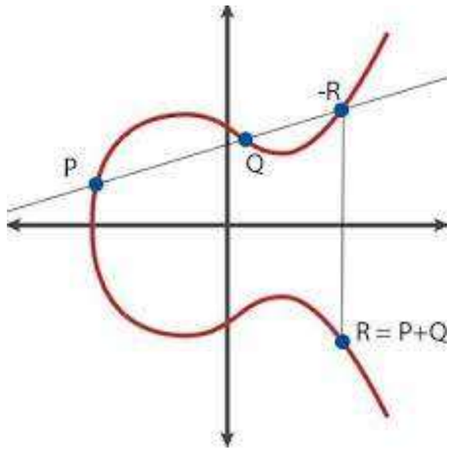


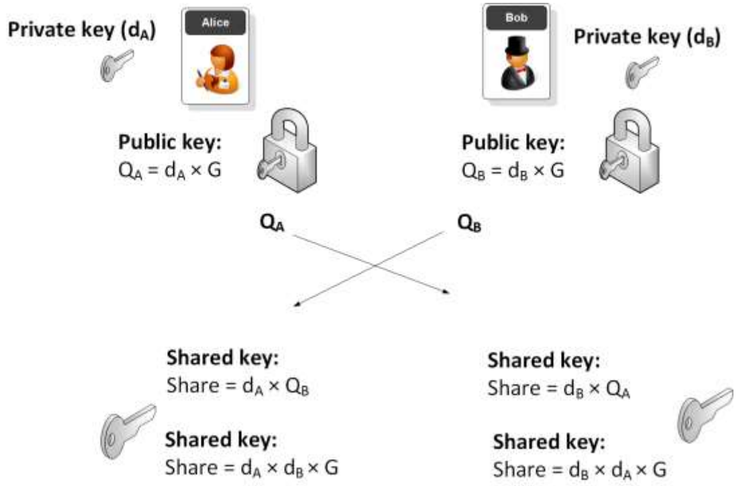
At Sender Side

Background - ECC and ECDLP

- *In Elliptic Curve Cryptography (ECC), the keys are coordinates of an Elliptic Curve. Why ECC?*
- *160 bit key length in ECC is equivalent to 1024 bit key length in RSA.*
- *ECC is intractable under the assumption of Elliptic Curve Discrete Logarithmic Problem (ECDLP).*

$y^2 = x^3 + ax + b$



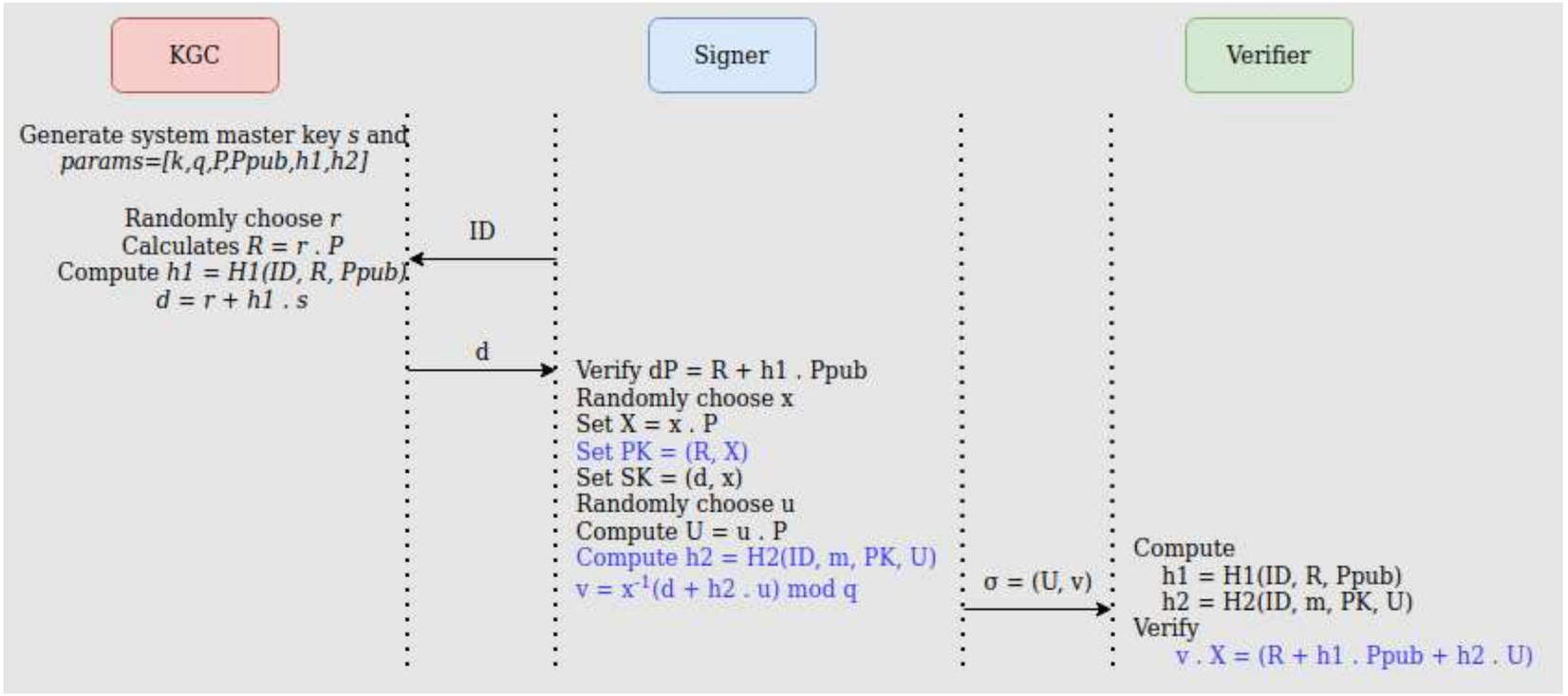


Problem & Solution

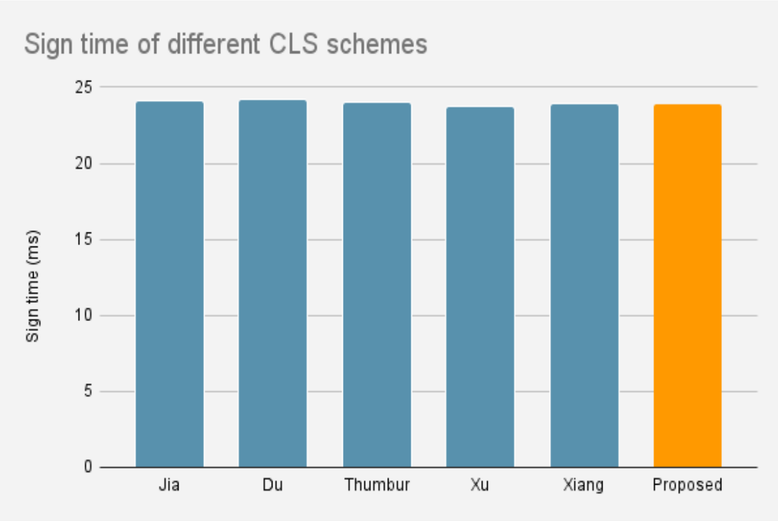
Scheme	Working	Drawbacks
Traditional Scheme	Uses certificates from trusted third party as authentication	High complexity, requires more resources
ID-based cryptography	Uses trusted third party to distribute private public keys to each node	Key escrow problem
Certificateless Signature Scheme (CLS)	In addition to ID based methodology each node generates its own private public private key pairs	If the algorithm is weak, it can become insecure against adversary attacks

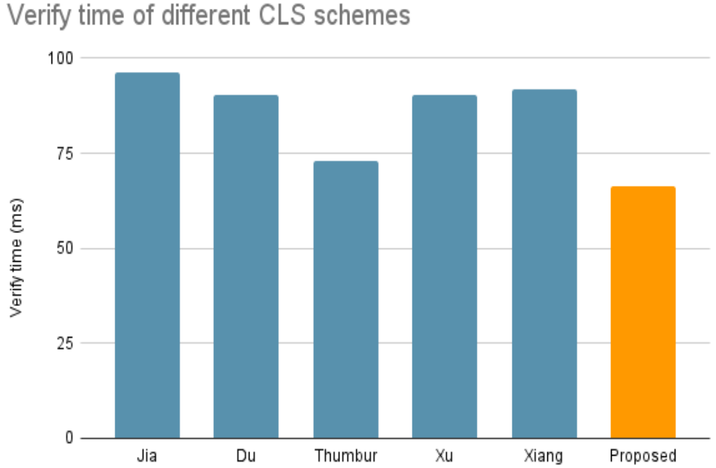
- *Develop a digital signature scheme that has the following properties*
  - *Lightweight*
  - *Requires less sign time and verify time*
  - *Provides good level of security against adversary attacks*

System Model



Results





Scheme	Sign Operation	Verify Operation	Type I security	Type II security
Jia [1]	$T_{sm} + T_{inv}$	$4T_{sm} + 2T_{pa}$	Insecure	Insecure
Du [2]	$T_{sm} + T_{inv}$	$4T_{sm} + 2T_{pa}$	Secure	Secure
Thumbur [3]	T_{sm}	$3T_{sm} + 2T_{pa}$	Insecure	Secure
Xu [4]	T_{sm}	$4T_{sm} + 3T_{pa}$	Secure	Secure
Xiang [5]	$T_{sm} + T_{inv}$	$4T_{sm} + 2T_{pa}$	Secure	Secure
Proposed	$T_{sm} + T_{inv}$	$3T_{sm} + 2T_{pa}$	Secure	Secure

Conclusion and Future work

- *Algorithms with ECC provides more security compared to RSA in lesser key length. So CLS schemes that uses ECC leans towards lightweight nature.*
- *Our proposed scheme is 28% faster than the fastest existing CLS scheme.*

- *In future, we intend to evaluate the performance of proposed scheme in real life WSNs.*
- *Conduct energy analysis on the scheme to improve efficiency and design new solutions.*

References

- *Xiaoying Jia, Debiao He, Qin Liu, Kim-Kwang Raymond Choo, An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment, Ad Hoc Networks, Volume 71, 2018, Pages 78-87, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2018.01.001.*
- *Hongzhen Du, Qiaoyan Wen, Shanshan Zhang, Mingchu Gao, A new provably secure certificateless signature scheme for Internet of Things, Ad Hoc Networks, Volume 100, 2020, 102074, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2020.102074.*
- *G. Thumbur, G. S. Rao, P. V. Reddy, N. B. Gayathri and D. V. R. K. Reddy, "Efficient Pairing-Free Certificateless Signature Scheme for Secure Communication in Resource-Constrained Devices," in IEEE Communications Letters, vol. 24, no. 8, pp. 1641-1645, Aug. 2020, doi: 10.1109/LCOMM.2020.2988818.*
- *Z. Xu, M. Luo, M. K. Khan, K. -K. R. Choo and D. He, "Analysis and Improvement of a Certificateless Signature Scheme for Resource-Constrained Scenarios," in IEEE Communications Letters, vol. 25, no. 4, pp. 1074-1078, April 2021, doi: 10.1109/LCOMM.2020.3042648.*
- *Dengmei Xiang, Xuelian Li, Juntao Gao, Xiachuan Zhang, A secure and efficient certificateless signature scheme for Internet of Things, Ad Hoc Networks, Volume 124, 2022, 102702, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2021.102702.*
- *X. Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, “Lattice-based proxy-oriented identity-based encryption with keyword search for cloud storage,” Inf. Sci., vol. 494, pp. 193–207, Aug. 2019.*
- *Kyung-Ah Shim, Security models for certificateless signature schemes revisited, Information Sciences, Volume 296, 2015, Pages 315-321, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2014.10.055.*

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

G20 भारत 2023 INDIA

THANK YOU

भगत संगणन विकास केंद्र
सीडैक CDAC
॥ज्ञानादेव तु कैवल्यम्॥
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

IEEE COMPUTER SOCIETY
Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY
Linking Research to Practice
Bangalore Chapter