

REFERENCES

- Angrisani, L., et al. (2020, May). Experimental test of ECDSA digital signature robustness from timing-lattice attack. In *2020 IEEE, International Instrumentation and Measurement Technology Conference (I2MTC)* (pp. 1-6). IEEE. <http://ieeexplore.ieee.org/document/9129144>
- Aufa, F.J., et al. (2018, August). Security system analysis in combination method: RSA encryption and digital signature algorithm. In *2018 4th International Conference on Science and Technology (ICST)* (pp. 1-5). <https://doi.org/10.1109/icstc.2018.8528584>
- Aziz, M.I & Akbar, S. (2005). Introduction to cryptography. *International Conference on Microelectronics* (pp. 144–147).
- Batten, L.M. (2013). *Public key cryptography: applications and attacks*. IEEE E-Books: IEEE Xplore. Topics: Computing and Processing; Communication, Networking, and Broadcast Technologies; Components, Circuits, Devices and Systems; Pages: 224 / Chapters 1-14. IEEE Xplore: Wiley-IEEE Press. <http://ieeexplore.ieee.org/book/6480474>
- Bisheh-Niasar, M., et al. (2021, July). Cryptographic accelerators for digital signature based on Ed25519. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 29(7), (pp. 1297–1305).
- Boneh, D. (1999). Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2), pp. 203-213. <https://crypto.stanford.edu/~dabo/pubs/abstracts/RSAattack-survey.pdf/>
- Briliyant, O. C., & Baihaqi, A. (2017, October). Implementation of RSA 2048-bit and AES 128-bit for Secure e-learning web-based application. In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)* (pp. 1-5). IEEE.
- Chakraborty, M., Jana, B., Mandal, T., & Kule, M. (2018, July). An performance analysis of RSA scheme using artificial neural network. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.
- D. R. Prathama, P. A. W. Putro, and D. I. Naviangga, "Secure mobile payment based on elliptic curve cryptography," in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2018.

- Dua, A., & Dutta, A. (2019, April). A study of applications based on elliptic curve cryptography. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 249-254). IEEE.
- Gobi, M., Sridevi, R., & Rahini, R. (2015). A comparative study on the performance and the security of RSA and ECC algorithm. *International Journal of Advanced Network and Application* (pp. 168–171).
- Gui-hong, L., Hua, Z., & Gui-zhi, L. (2010, May). Building a secure web server based on OpenSSL and apache. In *2010 International Conference on E-Business and E-Government* (pp. 1307-1310). IEEE. <https://doi.org/10.1109/icee.2010.334>
- Haywood, A., Sherbeck, J., Phelan, P., Varsamopoulos, G., & Gupta, S. K. (2012, May). Investigating a relationship among CPU and system temperatures, thermal power, and CPU tasking levels. In *13th InterSociety Conference on Thermal and Thermomechanical Phenomena in Electronic Systems* (pp. 821-827). IEEE. <https://doi.org/ieeexplore.ieee.org/document/6231511>
- Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International journal of information security*, 1(1), 36-63.
- NIST, CORPORATE. "The Digital Signature Standard." *Communications of the ACM*, vol. 35, no. 7, 1 July 1992, pp. 36–40, <https://doi.org/10.1145/129902.129904>
- Paar, C. & Pelzl, J. (2010). Introduction to Public-Key Cryptography, *Understanding Cryptography*, (pp. 149–171).
- Pointcheval, D., & Stern, J. (1996, May). Security proofs for signature schemes. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 387-398). Springer, Berlin, Heidelberg.
- Shaikh, J. R., Nenova, M., Iliev, G., & Valkova-Jarvis, Z. (2017, November). Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications. In *2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS)* (pp. 1-4). IEEE.
- Stallings, W. (2006). *Cryptography and network security. Upper Saddle River: N.J., Pearson/Prentice Hall.*
- Vasumathi, S. V. (2014). A study on RSA algorithm for cryptography. *International Journal of Computer Science and Information Technologies*, 5(4).