was run on macOS environment, Mojavi version 10.14.Implementation results are discussed in Table III-C.

TABLE I
SYSTEM PARAMETERS FOR BOTH KAWACHI'S AND CAYREL'S IDENTIFICATION SCHEMES

Parameter	Value
n	512
m	2048
q	257
Commitment length	256-bits

Proceedingly, we entegrated our *sparseVectorMatrixProduct* and *sparseMatrixVectorProduct* functions that are mentioned in Implementation Details section. These functions were implemented to save time without wasting it for multiplying all elements in a matrix, whilst there is a chance to use just corresponding elements. Experimentaln results are demonstrated in Table II (running time is measured in milliseconds(ms)).

TABLE II
IMPLEMENTATION RESULTS AFTER OUR CONTRIBUTION

Functions	Kawachi's IDscheme (ms)	Cayrel's IDscheme (ms)	Improvement (%)
vectorbyMatrix (standard)	9	-	
sparseVectorbyMatrix (proposed)	10	-	-
matrixbyVector (standard)	-	19	
sparseMatrixbyVector (proposed)	-	10	52.6%

The implementation of identification schemes presented in this study is available at https://github.com/msAzhar/pqc-id_schemes/

IV. CONCLUSION

In this study, we present a sparse vector by matrix multiplication and binary matrix by vector multiplication for Kawachi's and Cayrel's identification schemes. Firstly, we run those schemes using traditional ways of computing matrix and vector multiplication. As a traditional way we first implement the schoolbook method. For efficient implementation we consider a property-specific algorithm.

From Table II, we can see that implementation results of Kawachi's identification scheme are same, however, there are some enhancements in implementation of Cayrel's identification scheme. By using a *sparseMatrixVectorProduct* function, Cayrel's scheme's execution performance got better. Computation is accelerated approximately for 52.6%.

ACKNOWLEDGMENT

This research was partially supported by TUBITAK under grant no.EEEAG-117E636.

REFERENCES

[1] U. Feige, A. Fiat, A. Shamir, "Zero-knowledge proofs of identity," J. Cryptology 1988; pp. 77–94.
[2] A. Fiat, A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," Advances in Cryptology — CRYPTO'86; 1987; pp. 186-194.
[3] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J Comput 1997; 26: 1484-1509.
[4] L. Chen, S. Jordan, Y.K. Liu, et al., "Report on post-quantum cryptography," National Institute of Standards and Technology; 2016.
[5] A. Kawachi, K. Tanaka, and K. Xagawa, "Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems," J. Advances in Cryptology - ASIACRYPT 2008; pp. 372–389.
[6] P.-L. Cayrel, R. Lindner, M. Ruckert, and R. Silva, "Improved Zero-Knowledge Identification with Lattices," J. Tatra Mountains Mathematical Publications, vol: 53, 2010; pp. 1-17.
[7] A. Karatsuba and Y. Ofman, "Multiplication of multidigit numbers on automata," J. Soviet physics doklady, vol: 7, 1963; p. 595.
[8] S. Winograd, "Arithmetic Complexity of Computations," CBMS-NSF Regional Conference Series in Applied Mathematics, 1980; p. 5. doi:10.1137/1.9781611970364
[9] M. Ajtai, "Generating Hard Instances of Lattice Problems", J. Electronic Colloquium on Computational Complexity (ECCC), vol:3, 1996.
[10] P.-L. Cayrel, S.M.E. Yousfi Alaoui, F. Gunther, G. Hoffmann and H. Rother, "Efficient implementation of code-based identification schemes," In: Security Engineering and Intelligence Informatics. CD-ARES 2013. Lecture Notes in Computer Science, vol: 8128. Springer, Berlin, Heidelberg; pp. 122-136.
[11] R. E. Bansarkhani and J. A. Buchmann, "Improvement and Efficient Implementation of a Lattice-Based Signature Scheme," Selected Areas in Cryptography 2014; pp. 48-67. doi: 10.1007/978-3-662-43414-7
[12] A. Boorghany and R. Jalili, "Implementation and Comparison of Lattice-based Identification Protocols on Smart Cards and Microcontrollers", 2014.
[13] V. Lyubashevsky. F. Shamir, "Applications to lattice and factoring-based signatures," Advances in Cryptology –ASIACRYPT 2009, Lecture Notes in Computer Science; Springer Berlin Heidelberg, 2009; pp. 598–616.
[14] T. Guneysu, V. Lyubashevsky and T.Poppelmann, "Practical lattice-based cryptography: A signature scheme for embedded systems," Cryptographic Hardware and Embedded Systems –CHES 2012, Lecture Notes in Computer Science; Springer Berlin Heidelberg, 2012; pp. 530–547.
[15] J. Menezes, P. C. Oorschot, S. A. Vanstone, (1996), Handbook of Applied Cryptography, http://www.cacr.math.uwaterloo.ca/hac/
[16] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, D. Stebila, "Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE," In ACM Conference on Computer and Communications Security (CCS) 2016. doi:10.1145/2976749.2978425, eprint: http://eprint.iacr.org/2016/659.
[17] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, D. Stehlé, "CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM," In IEEE European Symposium on Security and Privacy, 2018, doi:10.1109/EuroSP.2018.00032
[18] T.Prest, P. A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte and Z. Zhang, "Falcon," Technical report, National Institute of Standards and Technology, 2017, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/ round-2-submissions