Another attack is when the token is stolen. In other proposals in the literature, the stolen-token scenario refers to the secret key (or the seed to generate it) which is known by an attacker (because this information is recovered from its storage) [19]. In our proposal, it is not possible to recover the stored hardware identifier because it is not stored anywhere. The only way to recover the hardware identifier is to access the PUF when it is operating or to physically steal the token so that an impostor can use it. Basically, in this scenario, the evaluation results only correspond to the biometric recognition component. Although PUF-based identifiers generated by the same device are not exactly equal (because some fit flipping is unavoidable), these differences are low. The results are included in Table II.

VI. Conclusions

A dual-factor recognition scheme based on feature level fusion of P-MCCs and SRAM PUF-based identifiers has been proposed, resulting in a secure identifier named as P-MCC-PUFs. The best performance was obtained using P-MCC-PUF1024 which considers 1024-bit feature vectors. The approach provides revocability and unlinkability to P-MCCs and also stronger template protection because the biometric information stored is obfuscated by sequences of random bits provided by SRAM PUFs.

Acknowledgment

This work was supported by TEC2014-57971-R project from Ministerio de Economía y Competitividad of the Spanish Government (with support from the PO FEDER-FSE), 201750E010 (HW-SEEDS) project from CSIC, and US National Science Foundation (NSF) Award No. 1617466. The work of R. Arjona was supported by VI Plan Propio de Investigación through the University of Seville. The work of M. A. Prada-Delgado was supported by V Plan Propio de Investigación through the University of Seville.

References

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, Introduction to Biometrics: A Textbook. Springer Publishers, 2011.

[2] A. K. Jain, K. Nandakumar and A. Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics, vol. 2008, no. 113. Hindawi Publishing Corporation, 2008.

[3] P. Campisi, Security and Privacy in Biometrics. Springer, 2013.

[4] E. J. Kindt, Privacy and Data Protection Issues of Biometric Applications. Springer, 2013.

[5] N. Ratha, J. Connell, and R. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems", IBM Systems Journal, vol. 40, no. 3. IEEE, 2001, pp. 614–634.

[6] A. Nagar, K. Nandakumar and A. K. Jain, "A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates", Pattern Recognition Letters, vol. 31, no. 8. Elsevier, 2010, pp. 733–741.

[7] A. K. Jain, K. Nandakumar, and A. Ross, "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities", Pattern Recognition Letters, vol. 79. Elsevier, 2016, pp. 80–105.

[8] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable Biometrics: A Review", IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 54–65, 2015.

[9] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number", Pattern Recognition, vol. 37, no. 11. Elsevier, 2004, pp. 2245–2255.

[10] D. Samyde, S. Skorobogatov, R. Anderson, and J.-J. Quisquater, "On a New Way to Read Data from Memory", Proc. First International IEEE Security in Storage Workshop (SISW), 2002, pp. 65–69.

[11] P. A. Grassi et al., Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B, 2017: https://doi.org/10.6028/NIST.SP.800-63b

[12] R. Maes, PUF-Based Entity Identification and Authentication Physically Unclonable Functions. Physically Unclonable Functions, Chapter 5, pp. 117–141. Springer, 2013.

[13] I. Baturone, M. A. Prada-Delgado, and S. Eiroa, "Improved Generation of Identifiers, Secret Keys, and Random Numbers from SRAMs", IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2653–2668, 2015.

[14] R. Arjona, and I. Baturone, "A Dual-Factor Access Control System based on Device and User Intrinsic Identifiers", Proc. 42nd Annual Conference of the IEEE Industrial Electronics Society (IECON), pp. 4731–4736, 2016.

[15] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 12, pp. 2128–2141, 2010.

[16] R. Cappelli, M. Ferrara, and D. Maltoni, "Fingerprint Indexing based on Minutia Cylinder Code", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 5, pp. 1051–1057, 2011.

[17] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible Minutia Cylinder-Code Representation", IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1727–1737, 2012.

[18] L. Mirmohamadsadeghi, and A. Drygajlo, "A Template Privacy Protection Scheme for Fingerprint Minutiae Descriptors", Proc. IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), 2013.

[19] M. Ferrara, D. Maltoni, and R. Cappelli, "A Two-Factor Protection Scheme for MCC Fingerprint Templates", Proc. IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), 2014.

[20] R. Cappelli, M. Ferrara, D. Maltoni, and M. Tistarelli, "MCC: A Baseline Algorithm for Fingerprint Verification in FVC-onGoing", Proc. 11th International Conference on Control Automation Robotics & Vision (ICARCV), 2010.

[21] M. A. Prada-Delgado, A. Vázquez-Reyes, and I. Baturone, "Physical Unclonable Keys for Smart Lock Systems using Bluetooth Low Energy", Proc. 42nd Annual Conference of the IEEE Industrial Electronics Society (IECON), pp. 4808–4813, 2016.

[22] A. A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics. Springer, 2006.

[23] C. Watson, G. Fiumara, E. Tabassi, S. L. Cheng, P. Flanagan, and W. Salamon, "NIST Fingerprint Vendor Technology Evaluation", 2014.

[24] Minutia Cylinder-Code SDK: http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=82&pathSubj=111%7C%7C8%7C%7C82&Req=&

[25] M. Gomez-Barrero, J. Galbally, A. Morales, and J. Fierrez, "Privacy-Preserving Comparison of Variable-Length Data With Application to Biometric Template Protection", IEEE Access, vol. 5, pp. 8606–8619, 2017.