6. CONCLUSIONS AND SUBSEQUENT WORK

We have presented a protocol that allows two parties sharing a low entropy secret to extract a shared key of optimal length—if the shared secret has entropy m, then the length of the extracted key is $m - \Theta(\kappa)$, where κ is the security parameter. We obtain our result through a somewhat unexpected application of edit distance codes. While our protocol has optimal entropy loss, it has a round complexity of $\Theta(\kappa)$. On the other hand, Dodis and Wichs [2009] showed nonconstructively, through the use of nonmalleable extractors, that there exists a protocol with both optimal entropy loss and optimal round complexity (2 rounds, which is shown to be necessary by Dodis and Wichs [2009]). Until recently, the problem of finding a polynomial-time protocol with optimal round complexity and optimal entropy loss was open. Li [2012b] made progress on the open problem by showing two-round protocol for w whose entropy rate is an arbitrary constant; his work was using explicit constructions of nonmalleable extractors and novel protocol techniques shown in Dodis et al. [2011], Cohen et al. [2011], and Li [2012a] (which achieve optimal entropy loss when the entropy rate of w is at least 1/2). In other related work, the work of Bouman and Fehr [2011] studies the reusability of authentication schemes by using (unlike in our work) one-time sessions derived from weak long-term keys for authentication. In this setting, in order to ensure re-usability, it is essential to guarantee privacy of the long-term key.

ACKNOWLEDGMENTS

We thank Alexandr Andoni, Yevgeniy Dodis, and Madhu Sudan for helpful discussions. We also thank the anonymous reviewers of *STOC 2010* and *Journal of the ACM* for their detailed comments. We thank Gil Segev for pointing out a subtle flaw in the definition of privacy amplification which appeared in an earlier version of this article.

REFERENCES

Charles Bennett, Gilles Brassard, and Jean-Marc Robert. 1988. Privacy amplification by public discussion. *SIAM J. Comput. 17*, 2, 210–229.

Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer. 1995. Generalized privacy amplification. *IEEE Trans. Inf. Theory 41*, 6, 1915–1923.

Niek J. Bouman and Serge Fehr. 2011. Secure authentication from a weak key, without leaking information. In *Proceedings of EUROCRYPT*. 246–265.

Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. 2005. Secure remote authentication using biometric data. In *Proceedings of Advances in Cryptology—EUROCRYPT 2005*, Ronald Cramer Ed., Lecture Notes in Computer Science, vol. 3494, Springer-Verlag, 147–163.

J. L. Carter and M. N. Wegman. 1979. Universal classes of hash functions. *J. Comput. Syst. Sci. 18*, 143–154.

Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky, and Leonid Reyzin. 2010. Privacy amplification with asymptotically optimal entropy loss. In *Proceedings of STOC*, Leonard J. Schulman Ed., ACM, 785–794.

Gil Cohen, Ran Raz, and Gil Segev. 2011. Non-malleable extractors with short seeds and applications to privacy amplification. *Electron. Colloq. Computat. Complex. 18*, 96.

Yevgeniy Dodis, Bhavana Kanukurthi, Jonathan Katz, Leonid Reyzin, and Adam Smith. 2012. Robust fuzzy extractors and authenticated key agreement from close secrets. *IEEE Trans. Inf. Theory 58*, 9, 6207–6222.

Yevgeniy Dodis, Xin Li, Trevor D. Wooley, and David Zuckerman. 2011. Privacy amplification and nonmalleable extractors via character sums. In *Proceedings of FOCS*, Rafail Ostrovsky Ed., IEEE, 668–677.

Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. 2008. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput. 38*, 1, 97–139.

Yevgeniy Dodis and Daniel Wichs. 2009. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (Bethesda, MD)*. 601–610.