[55] Y. Li, Y. Zhang, J. Li, and D. Gu. iCryptoTracer: Dynamic Analysis on Misuse of Cryptography Functions in iOS Applications. In *Proc. International Conference on Network and System Security (NSS)*, 2014.

[56] C. Luk, R. Cohn, R. Muth, H. Patil, A. Klauser, G. Lowney, S. Wallace, V. Reddi, and K. Hazelwood. Pin: Building Customized Program Analysis Tools with Dynamic Instrumentation. In *Proc. ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)*, 2005.

[57] C. Maartmann-Moe, S. E. Thorkildsen, and A. Årnes. The persistence of memory: Forensic identification and extraction of cryptographic keys. *Digital Investigation*, 6:132–140, 2009.

[58] F. Matenaar, A. Wichmann, F. Leder, and E. Gerhards-Padilla. CIS: The Crypto Intelligence System for Automatic Detection and Localization of Cryptographic Functions in Current Malware. In *Proc. International Conference on Malicious and Unwanted Software (Malware)*, 2012.

[59] J. Newsome and D. Song. Dynamic Taint Analysis for Automatic Detection, Analysis, and Signature Generation of Exploits on Commodity Software. In *Proc. 12th Annual Network and Distributed System Security Symposium (NDSS)*, 2005.

[60] S. Rahaman and D. Yao. Program analysis of cryptographic implementations for security. In *Proc. IEEE Secure Development Conference (SecDev)*, 2017.

[61] B. Schneier. Cryptography: The Importance of Not Being Different. *Computer*, 32(3):108–109, 1999.

[62] B. Schneier. Schneier on Security: The Doghouse: KRYPTO 2.0. https://www.schneier.com/blog/archives/2006/06/the_doghouse_kr.html, 2006.

[63] E. J. Schwartz, T. Avgerinos, and D. Brumley. All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask). In *Proc. 31st IEEE Symposium on Security and Privacy (S&P)*, 2010.

[64] A. Shamir and N. Van Someren. Playing "hide and seek" with stored keys. In *Proc. International conference on Financial Cryptography (FC)*, 1999.

[65] R. Wang, Y. Shoshitaishvili, C. Kruegel, and G. Vigna. Steal This Movie: Automatically Bypassing DRM Protection in Streaming Media Services. In *Proc. USENIX Security Symposium*, 2013.

[66] Z. Wang, X. Jiang, W. Cui, X. Wang, and M. Grace. Reformat: Automatic reverse engineering of encrypted messages. In *Proc. 14th European Symposium on Research in Computer Security*. 2009.

[67] H. Wu. The Misuse of RC4 in Microsoft Word and Excel. *IACR Cryptology ePrint Archive*, 2005.

[68] D. Xu, J. Ming, and D. Wu. Cryptographic function detection in obfuscated binaries via bit-precise symbolic loop mapping. In *Security and Privacy (SP), 2017 IEEE Symposium on*, pages 921–937. IEEE, 2017.

[69] Z. Yang, B. Johannesmeyer, A. T. Olesen, S. Lerner, and K. Levchenko. Dead Store Elimination (Still) Considered Harmful. In *Proc. 26th Usenix Security Symposium*, 2017.

[70] R. Zhao, D. Gu, and J. Li. Detection and Analysis of Cryptographic Data Inside Software. In *Proc. Information Security Conference (ISC)*, 2011.