Yevgeniy Dodis January 7, 2022

RESEARCH STATEMENT

My main research interest is in *cryptography*. Cryptography is a broad and rapidly evolving field that aims to develop mathematically rigorous methods to protect various applications from malicious behavior. The need for cryptography is ever growing in our digital world, since more and more sensitive information is traveling every second over potentially insecure channels. Correspondingly, new cryptographic challenges arise continuously, and it is of utmost importance to develop efficient and secure solutions for these challenges.

As a result, my research interests have been pretty broad, and I worked in many areas of cryptography, both established and emerging. Over the years, I have published over 150 papers (90 of which appeared at CRYPTO, EUROCRYPT, TCC, STOC and FOCS) with over 150 different co-authors, and my research has received over 18,500 citations (with nearly 50 papers having 100+ citations, and current h-index of 67). My research is deeply rooted in theory, and many of my works focus on fundamental questions in the field, with far-reaching implications and connections to other areas, such as complexity theory and combinatorics. At the same time, much of my work (especially more recently) focuses on solving real-world problems and analyzing practical cryptosystems that are already deployed or should be deployed. I am excited to work on both theoretical and practical problems, and enjoy successfully collaborating with researchers across many different communities.

I have recently became the youngest-ever Fellow of the International Association for Cryptologic Research (IACR) — the highest recognition in Cryptography. I also served/will serve as the program co-chair of TCC'15 and CRYPTO'22 — two of the main conferences in the field of Cryptography. I am also the recipient of 2021 and 2019 IACR Test-of-Time Awards for my work on Fuzzy Extractors and Verifiable Random Functions, National Science Foundation CAREER Award, Faculty Awards from Facebook, Google, IBM, Algorand Foundation and VMware, and Best Paper Award at 2005 Public Key Cryptography Conference.

While I cannot fully touch on all the areas I am interested in, below I will focus on several research topics I am particularly excited about.

Randomness in Cryptography. Cryptography fundamentally relies on randomness. However, natural sources of randomness are often "weak" and, although they have entropy, they rarely produce uniformly random bits. Some of my most influential works explore how to properly use weak sources of randomness in cryptography. My research examines this topic across its full spectrum, from theoretical foundations to analyzing real-world systems.

RANDOMNESS EXTRACTION. A fundamental problem is how to extract (nearly) uniform randomness from weak sources. My foundational results [DOPS04, BD07] from FOCS '04 and TCC '07 show that randomness extraction is indeed fundamental in cryptography: any crytosystem secure under weak randomness implicitly gives a deterministic randomness extractor from the corresponding source. The latter is known to be impossible for the most general weak sources (only having entropy). To overcome this impossibility, the following 3 restrictions were believed essential prior to my work: (1) the extractor should take an additional random-but-public input, called the "seed"; (2) seed must be independent of the source, and (3) large "entropy loss" is essential: weak source should have noticeably more entropy than the number of bits output by the extractor. Obviously, satisfying all three restrictions is often problematic.

Fortunately, my work significantly weakened these assumptions in many settings. For (1), at CRYPTO'19 [CDKT19] we managed to introduce a new notion of entropy likely satisfied by "real-world" entropy sources, under which widely used hash functions SHA-2/3, HMAC and HKDF are provably secure seedless randomness extractors, for the first time adequately explaining the seeming mismatch between theory and practice of key derivation. For (2), at EUROCRYPT'20 [DVW20] (resp. TCC'12 [DRV12]) we showed a very unexpected feasibility of (seeded) randomness extraction (resp. key derivation) in the setting where the entropy source could depend on the prior extractor outputs (resp. seed). And for (3), at CRYPTO'11, TCC'13 and EUROCRYPT'14 [BDK+11, DY13, DPW14], we showed how to build provably secure "key derivation functions" for variety of cryptographic applications, having almost no entropy loss and provably outperforming traditional randomness extraction.

FUZZY EXTRACTORS. Some sources of randomness, such as biometrics, have the additional challenge that they are "unreliably reproducible"; subsequent scans of the same biometric will differ somewhat from one to another. Can we reliably extract consistent uniform randomness from such sources? Our result [DRS04, DORS08] from Erocrypt'04 and SIAM J. of Computing'08 shows how to do so. This result, with over 3,500 citations, has had tremendous impact on both theory as well as practical systems. It was awarded the 2019

IACR Test of Time Award. Beyond solving this important problem, the solution elegantly combines ideas from coding theory and randomness extractors in a novel way, and the develops important concepts that have since become "textbook notions", commonly used in many areas of cryptography and beyond.

NON-MALLEABLE EXTRACTORS/CODES. One of the most basic questions in this area asks whether a weakly random secret shared between two parties (Alice and Bob) suffices for them to communicate securely over an insecure channel controlled by a computationally unbounded adversary (Eve). Our results [DW09, DLWZ11] from FOCS'09 and FOCS'11 showed that this can be done optimally in only 2 rounds, using a very elegant new primitive called a non-malleable extractor. Aside from giving a clean and nearly optimal solution to the problem (a big contribution by itself), it turned out that non-malleable extractors had far-reaching impact beyond privacy amplification. In particular, they were one of the key components of a breakthrough work of Chattopadhyay and Zuckerman (best paper at STOC'16), which solved a 25-year old major open problem in complexity theory (constructing 2-source extractors), and even older problem in combinatorics (explicit constructions of certain Ramsey graphs). In later works [ADL14, ADKO15] at STOC'14 and '15, we gave the first explicit constructions of a related primitive, called a (split-state) non-malleable code, which has also turned out to have major implications in cryptography and beyond.

SYSTEM RANDOM-NUMBER GENERATORS. Motivated by my foundational work on the use of randomness, my co-authors and I also studied real-world random-number generators (RNGs). In our work [DPR+13, DSSW14, CDKT19, DGSX21] from CCS '13, CRYPTO'14,'19,'21, we noticed a huge disconnect between practical RNGs used in popular operating-systems such as Linux, Windows and Apple OS, and the theoretical treatment of RNGs in prior works. One of the main goals of practical RNGs designs – namely, the ability to accumulate entropy even if it comes at slow and unknown rate – was completely ignored by the prior theory works. In a collaboration with theoreticians and practitioners, we developed the first formal models of RNGs that capture this requirement, showed that Linux RNG */dev/random* is not secure according to the new model, while Windows RNG Fortuna meets this requirement, albeit in a suboptimal way. We also analyzed a super-efficient (and previously heuristic) entropy accumulation inside Windows10 and MacOS. These works are a great example of rigorous theory being used to solve real-world problems.

Leakage-Resilient Cryptography. I am one of the pioneers of the area of leakage-resilient cryptography (which is related to my PhD thesis work on exposure-resilient cryptography) and Bounded Retrieval Model. This area studies the question how to build cryptographic systems resilient to dramatic leakage of sensitive information, such as secret keys. In practice, attacks of this sort are, in many cases, more likely than attacks which directly "crack" the cryptographic assumptions on which the security of the scheme is based. My many works [CDD+07, ADW09, ADN+10, DP10, CDRW10, DHLW10b] heavily use techniques from randomness extraction (and many other areas) to design cryptographic systems resilient to almost complete (and sometimes continuous [DHLW10a, DLWW11, ADVW13]) exposure of secrets.

Analysis of Symmetric-Key Primitives. Yet another area where I made a large number of important contributions is the analysis of symmetric-key primitives (e.g., block ciphers and hash functions) and their modes of operation. The design of symmetric-key primitives is frequently considered to be more of an art than a science, and their security often rests on unproven ad-hoc assumptions. My work strives to bring rigorous and provable analysis to many aspects of such designs and to minimize the role of as-hoc techniques as much as possible.

RANDOM ORACLES AND PREPROCESSING. A common way to analyze security of using cryptographic hash functions in applications is to model them as (ideal) random oracles (ROs). However, it turns out that the RO model gives overly optimistic prediction about exact (non-asymptotic) security of such constructions when the adversary is allowed to perform unbounded-time "preprocessing" on the hash function before attacking a particular instance. Our works [DGK17, CDGS18, CDG18] at EUROCRYPT'17,'18 and CRYPTO'18 develop highly sophisticated and powerful tools to analyze (so called "non-uniform") security of such cryptosystems with unbounded preprocessing, and therefore get realistic assessments of their "non-uniform" security levels. In many cases, these works show for the first time that the known generic non-uniform attacks (e.g., rainbow tables for function inversion) are optimal and cannot be improved.

INDIFFERENTIABILITY. At CRYPTO'05 [CDMP05], my co-authors and I advocated the use of indifferentiability in the design of hash functions and block ciphers. This paper got over 600 citations, and played a major role in many exciting results in the field, such as the equivalence of the random oracle and the ideal cipher models (early version of the paper won the best paper at CRYPTO'08), and also became a de facto

requirement for SHA-3 competition. Following this work, we showed several foundational results in the field, such as first indifferentiability results for key-alternating ciphers (CRYPTO'13 [ABD+13]), confusion-diffusion networks (EUROCRYPT'16 [DSSL16]) and HMAC/hash-of-hash schemes (CRYPTO'12 [DRST12]). These results are complemented by our more traditional results on designing hash functions and block ciphers, such as indistinguishability of substitution-permutation networks (CRYPTO'18 [CDK+18]) and domain extension of MACs (EUROCRYPT'07,'08,'11 [DP07, DPP08, DS11] and CRYPT0'09 [DS09]). Some of these results [ABD+13, DSSL16, CDK+18] have implications towards understanding the security of ubiquitous Advanced Encryption Standard (AES) — a major open problem.

End-to-End Encryption. Building on my earlier foundational work on symmetric- and public-key authenticated encryption [ADR02, DA03, DFJW04], I recently started to work in an emerging area of secure messaging and end-to-end (E2E) encryption, where even the service provider cannot decrypt the content of users' messages. Our CRYPTO'18 [DGRW18] paper laid foundations of message franking used by Facebook, and led to a prestigious "Secure the Internet" grant from Facebook. At EUROCRYPT'19 [ACD19], we provided the first complete analysis of the famous Signal protocol, which is ubiquitously used by WhatsApp and most other secure messaging applications. This influential paper introduced a novel primitive called Continuous Key Agreement, which turns out to be a key component for achieving so called Post-Compromise Security in modern E2E schemes, and was already used in dozens of follow-up works.

At CRYPTO'20 [ACDT20], we found a serious weakness in (and an elegant fix for) the upcoming Internet Engineering Task Force standard for secure group messaging, called Message Layer Security (MLS), and, at CCS'21 [ACDT21], we gave a complete (over 100 pages) analysis of all aspects of the MLS protocol.

Finally, I am now actively collaborating with Zoom security team to analyze and improve their massive efforts to bring E2E protection to the entire Zoom ecosphere, a topic of hot criticism from the press.

Summary. These and other examples show that, although I am primarily a theoretical cryptographer, I am also one of the leaders in the field of system-oriented cryptography, where theoretically-sound solutions are built around existing systems and motivated by real-life applications. Not surprisingly, my past practice-oriented research was partially supported by gifts from such industrial partners as IBM, Google, Facebook, Algorand and VMware, and many of my theoretical results have had noticeable impacts among applied security researchers.

Overall, it is clear that cryptography is an exciting young field, and I plan to continue working on unexpected new challenges that are bound to arise.

References

[ABD+13] Elena Andreeva, Andrey Bogdanov, Yevgeniy Dodis, Bart Mennink, and John P. Steinberger. On the indifferentiability of key-alternating ciphers. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 531–550. Springer, Heidelberg, August 2013.

[ACD19] Joël Alwen, Sandro Coretti, and Yevgeniy Dodis. The double ratchet: Security notions, proofs, and modularization for the Signal protocol. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part I*, volume 11476 of *LNCS*, pages 129–158. Springer, Heidelberg, May 2019.

[ACDT20] Joël Alwen, Sandro Coretti, Yevgeniy Dodis, and Yiannis Tselekounis. Security analysis and improvements for the IETF MLS standard for group messaging. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 248–277. Springer, Heidelberg, August 2020.

[ACDT21] Joël Alwen, Sandro Coretti, Yevgeniy Dodis, and Yiannis Tselekounis. Modular design of secure group messaging protocols and the security of MLS. In Yongdae Kim, Jong Kim, Giovanni Vigna, and Elaine Shi, editors, *CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*, pages 1463–1483. ACM, 2021.

[ADKO15] Divesh Aggarwal, Yevgeniy Dodis, Tomasz Kazana, and Maciej Obremski. Non-malleable reductions and applications. In Rocco A. Servedio and Ronitt Rubinfeld, editors, *47th ACM STOC*, pages 459–468. ACM Press, June 2015.

[ADL14] Divesh Aggarwal, Yevgeniy Dodis, and Shachar Lovett. Non-malleable codes from additive combinatorics. In David B. Shmoys, editor, *46th ACM STOC*, pages 774–783. ACM Press, May / June 2014.

[ADN+10] Joël Alwen, Yevgeniy Dodis, Moni Naor, Gil Segev, Shabsi Walfish, and Daniel Wichs. Public-key encryption in the bounded-retrieval model. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 113–134. Springer, Heidelberg, May / June 2010.

[ADR02] Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 83–107. Springer, Heidelberg, April / May 2002.

[ADVW13] Shweta Agrawal, Yevgeniy Dodis, Vinod Vaikuntanathan, and Daniel Wichs. On continual leakage of discrete log representations. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 401–420. Springer, Heidelberg, December 2013.

[ADW09] Joël Alwen, Yevgeniy Dodis, and Daniel Wichs. Leakage-resilient public-key cryptography in the bounded-retrieval model. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 36–54. Springer, Heidelberg, August 2009.

[BD07] Carl Bosley and Yevgeniy Dodis. Does privacy require true randomness? In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 1–20. Springer, Heidelberg, February 2007.

[BDK+11] Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira, Krzysztof Pietrzak, François-Xavier Standaert, and Yu Yu. Leftover hash lemma, revisited. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 1–20. Springer, Heidelberg, August 2011.

[CDD+07] David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard J. Lipton, and Shabsi Walfish. Intrusion-resilient key exchange in the bounded retrieval model. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 479–498. Springer, Heidelberg, February 2007.

[CDG18] Sandro Coretti, Yevgeniy Dodis, and Siyao Guo. Non-uniform bounds in the random-permutation, ideal-cipher, and generic-group models. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 693–721. Springer, Heidelberg, August 2018.

[CDGS18] Sandro Coretti, Yevgeniy Dodis, Siyao Guo, and John P. Steinberger. Random oracles and non-uniformity. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 227–258. Springer, Heidelberg, April / May 2018.

[CDK+18] Benoît Cogliati, Yevgeniy Dodis, Jonathan Katz, Jooyoung Lee, John P. Steinberger, Aishwarya Thiruvengadam, and Zhe Zhang. Provable security of (tweakable) block ciphers based on substitution-permutation networks. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 722–753. Springer, Heidelberg, August 2018.

[CDKT19] Sandro Coretti, Yevgeniy Dodis, Harish Karthikeyan, and Stefano Tessaro. Seedless Fruit is the sweetest: Random number generation, revisited. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 205–234. Springer, Heidelberg, August 2019.

[CDMP05] Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle-Damgård revisited: How to construct a hash function. In Victor Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 430–448. Springer, Heidelberg, August 2005.

[CDRW10] Sherman S. M. Chow, Yevgeniy Dodis, Yannis Rouselakis, and Brent Waters. Practical leakage-resilient identity-based encryption from simple assumptions. In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *ACM CCS 2010*, pages 152–161. ACM Press, October 2010.

[DA03] Yevgeniy Dodis and Jee Hea An. Concealment and its applications to authenticated encryption. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 312–329. Springer, Heidelberg, May 2003.

[DFJW04] Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, and Shabsi Walfish. Versatile padding schemes for joint signature and encryption. In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick McDaniel, editors, *ACM CCS 2004*, pages 344–353. ACM Press, October 2004.

[DGK17] Yevgeniy Dodis, Siyao Guo, and Jonathan Katz. Fixing cracks in the concrete: Random oracles with auxiliary input, revisited. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 473–495. Springer, Heidelberg, April / May 2017.

[DGRW18] Yevgeniy Dodis, Paul Grubbs, Thomas Ristenpart, and Joanne Woodage. Fast message franking: From invisible salamanders to encryptment. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 155–186. Springer, Heidelberg, August 2018.

[DGSX21] Yevgeniy Dodis, Siyao Guo, Noah Stephens-Davidowitz, and Zhiye Xie. No time to hash: On super-efficient entropy accumulation. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part IV*, volume 12828 of *Lecture Notes in Computer Science*, pages 548–576. Springer, 2021.

[DHLW10a] Yevgeniy Dodis, Kristiyan Haralambiev, Adriana López-Alt, and Daniel Wichs. Cryptography against continuous memory attacks. In *51st FOCS*, pages 511–520. IEEE Computer Society Press, October 2010.

[DHLW10b] Yevgeniy Dodis, Kristiyan Haralambiev, Adriana López-Alt, and Daniel Wichs. Efficient public-key cryptography in the presence of key leakage. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 613–631. Springer, Heidelberg, December 2010.

[DLWW11] Yevgeniy Dodis, Allison B. Lewko, Brent Waters, and Daniel Wichs. Storing secrets on continually leaky devices. In Rafail Ostrovsky, editor, *52nd FOCS*, pages 688–697. IEEE Computer Society Press, October 2011.

[DLWZ11] Yevgeniy Dodis, Xin Li, Trevor D. Wooley, and David Zuckerman. Privacy amplification and non-malleable extractors via character sums. In Rafail Ostrovsky, editor, *52nd FOCS*, pages 668–677. IEEE Computer Society Press, October 2011.

[DOPS04] Yevgeniy Dodis, Shien Jin Ong, Manoj Prabhakaran, and Amit Sahai. On the (im)possibility of cryptography with imperfect randomness. In *45th FOCS*, pages 196–205. IEEE Computer Society Press, October 2004.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam D. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008.

[DP07] Yevgeniy Dodis and Prashant Puniya. Feistel networks made public, and applications. In Moni Naor, editor, *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 534–554. Springer, Heidelberg, May 2007.

[DP10] Yevgeniy Dodis and Krzysztof Pietrzak. Leakage-resilient pseudorandom functions and side-channel attacks on Feistel networks. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 21–40. Springer, Heidelberg, August 2010.

[DPP08] Yevgeniy Dodis, Krzysztof Pietrzak, and Prashant Puniya. A new mode of operation for block ciphers and length-preserving MACs. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 198–219. Springer, Heidelberg, April 2008.

[DPR+13] Yevgeniy Dodis, David Pointcheval, Sylvain Ruhault, Damien Vergnaud, and Daniel Wichs. Security analysis of pseudo-random number generators with input: /dev/random is not robust. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM CCS 2013*, pages 647–658. ACM Press, November 2013.

[DPW14] Yevgeniy Dodis, Krzysztof Pietrzak, and Daniel Wichs. Key derivation without entropy waste. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 93–110. Springer, Heidelberg, May 2014.

[DRS04] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 523–540. Springer, Heidelberg, May 2004.

[DRST12] Yevgeniy Dodis, Thomas Ristenpart, John P. Steinberger, and Stefano Tessaro. To hash or not to hash again? (In)differentiability results for H^2 and HMAC. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 348–366. Springer, Heidelberg, August 2012.

[DRV12] Yevgeniy Dodis, Thomas Ristenpart, and Salil P. Vadhan. Randomness condensers for efficiently samplable, seed-dependent sources. In Ronald Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 618–635. Springer, Heidelberg, March 2012.

[DS09] Yevgeniy Dodis and John P. Steinberger. Message authentication codes from unpredictable block ciphers. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 267–285. Springer, Heidelberg, August 2009.

[DS11] Yevgeniy Dodis and John P. Steinberger. Domain extension for MACs beyond the birthday barrier. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 323–342. Springer, Heidelberg, May 2011.

[DSSL16] Yevgeniy Dodis, Martijn Stam, John P. Steinberger, and Tianren Liu. Indifferentiability of confusion-diffusion networks. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 679–704. Springer, Heidelberg, May 2016.

[DSSW14] Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too - optimal recovery strategies for compromised RNGs. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 37–54. Springer, Heidelberg, August 2014.

[DVW20] Yevgeniy Dodis, Vinod Vaikuntanathan, and Daniel Wichs. Extracting randomness from extractor-dependent sources. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 313–342. Springer, Heidelberg, May 2020.

[DW09] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 601–610. ACM Press, May / June 2009.

[DY13] Yevgeniy Dodis and Yu Yu. Overcoming weak expectations. In Amit Sahai, editor, *TCC 2013*, volume 7785 of *LNCS*, pages 1–22. Springer, Heidelberg, March 2013.