Темы БДЗ для выполнения на сайте cryptowiki.net, группа М19-517, 2019/20 уч.г.:

№	Тема на русск.яз.	Тема на англ.яз.	Ссылки на статьи по теме (указан минимум, можно использовать любую другую литературу)	ФИО студента
1	Компактные неинтерактивные доказательства знания с нулевым разглашением	Zero-knowledge Succinct non-interactive arguments of knowledge (zk-SNARKs)	https://eprint.iacr.org/2014/349.pdf https://eprint.iacr.org/2013/879.pdf https://z.cash/technology/zksnarks/	Бучинская А.В.
2	Криптографические доказательства типа Bulletproofs и их применения	Bulletproofs and their applications	https://eprint.iacr.org/2017/1066.pdf https://medium.com/digitalassetresearch/monero-becomes-bulletproof-f98c6408babf	Кварацхелия Л.Д.
3	Протоколы защищенного двустороннего асинхронного канала передачи данных с максимальными свойствами безопасности	Optimal secure asynchronous data transfer protocols	https://eprint.iacr.org/2018/553.pdf https://eprint.iacr.org/2018/296.pdf https://eprint.iacr.org/2018/889.pdf	
4	Субоптимальные протоколы защищенного двустороннего асинхронного канала передачи данных	Suboptimal secure asynchronous data transfer protocols	https://eprint.iacr.org/2018/954.pdf https://eprint.iacr.org/2018/1037.pdf	Сосновый М.С.

5	Семейство протоколов доказательства обладания долей Ouroboros	Ouroboros: Proof-of-stake protocols	https://eprint.iacr.org/2018/1132.pdf https://eprint.iacr.org/2018/1049.pdf https://eprint.iacr.org/2018/378.pdf https://eprint.iacr.org/2017/573.pdf https://eprint.iacr.org/2016/889.pdf	
6	Схемы электронной цифровой подписи на основе скрученных эллиптических кривых Эдвардса	Digital signatures based on twisted Edwards curves	https://signal.org/docs/specifications/xeddsa/ https://eprint.iacr.org/2008/013.pdf https://cr.yp.to/ecdh/curve25519-20060209.pdf https://ed25519.cr.yp.to/ed25519-20110705.pdf	Дильмиев Т.Б.
7	Протоколы защищенного многостороннего асинхронного канала передачи данных	Group secure asynchronous data transfer protocols	https://eprint.iacr.org/2020/066 https://eprint.iacr.org/2019/1189.pdf https://eprint.iacr.org/2019/477 https://eprint.iacr.org/2017/666	Капранов И.В.
8	Разграничение доступа к файлам на основе блокчейн-технологий	Blockchain-based access control schemes	https://eprint.iacr.org/2019/418 https://eprint.iacr.org/2019/880 https://eprint.iacr.org/2020/011 *Zhang Y., Kasahara S., Shen Y. et al.* Smart contract-based access control for the Internet of Things // IEEE Internet of Things Journal, Vol. 6, No. 2, April 2019. Pp. 1594 – 1605. *Aggarwal S., Chaudhary R., Aujla G.S. et al.* Blockchain for smart communities: Applications, challenges and opportunities // Journal of Network and Computer Applications, 144 (2019), pp. 13-48.	Молчан Н.О.
9	Постквантовые примитивы в защищенных каналах передачи данных	Post-quantum cryptography in secure data transfer channels	https://eprint.iacr.org/2020/071 https://essay.utwente.nl/77239/1/Duits_MA_EEMCS.pdf https://eprint.iacr.org/2019/1447 https://eprint.iacr.org/2019/858	Крапивенцев Д.М.
10	Конфиденциальная		https://eprint.iacr.org/2019/1158	

	кластеризация данных		https://arxiv.org/pdf/1904.04475.pdf	
11	Конфиденциальное обучение и применение решающих деревьев		https://eprint.iacr.org/2019/1282 https://eprint.iacr.org/2018/1099	Севанькаев А.В.
12	Конфиденциальное обучение и применение нейронных сетей	Privacy-preserving neural networks	https://eprint.iacr.org/2020/050 https://eprint.iacr.org/2020/042 https://eprint.iacr.org/2019/1365 https://eprint.iacr.org/2019/947 https://eprint.iacr.org/2019/338 https://eprint.iacr.org/2018/442	Штанов Е.Ю.
13	Конфиденциальное глубокое обучение	Privacy-preserving deep learning	https://eprint.iacr.org/2020/155 https://pdfs.semanticscholar.org/c0c6/44cbf23341f7732f46209e5d2f5ccfc97d1e.pdf	
14	Конфиденциальное обучение и применение линейной и логистической регрессии	Privacy-preserving linear and logistic regression	https://eprint.iacr.org/2020/171 https://eprint.iacr.org/2020/042 https://eprint.iacr.org/2019/1365	
15	Конфиденциальные платежные системы на основе блокчейн-технологий	Blockchain-based privacy-preserving payments	https://eprint.iacr.org/2020/004 https://eprint.iacr.org/2019/1058 https://github.com/zcash/zips/raw/master/protocol/protocol.pdf https://web.getmonero.org/technical-specs/	Михайлин М.В.
16	Практичные GC-схемы	Practical garbled circuits	https://eprint.iacr.org/2019/1210 Shay Gueron, Yehuda Lindell, Ariel Nof, and Benny Pinkas. Fast garbling of circuits under standard assumptions. In Indrajit Ray, Ninghui Li, and Christopher Kruegel:, editors, ACM CCS 15, pages 567–578. ACM Press, October 2015.	

			Vladimir Kolesnikov, Payman Mohassel, and Mike Rosulek. FleXOR: Flexible garbling for XOR gates that beats free-XOR. In Juan A. Garay and Rosario Gennaro, editors, CRYPTO 2014, Part II, volume 8617 of LNCS, pages 440–457. Springer, Heidelberg, August 2014. Vladimir Kolesnikov and Thomas Schneider. Improved garbled circuit: Free XOR gates and applications. In Luca Aceto, Ivan Damg˚ard, Leslie Ann Goldberg, Magn´us M. Halld´orsson, Anna Ing´olfsd´ottir, and Igor Walukiewicz, editors, ICALP 2008, Part II, volume 5126 of LNCS, pages 486–498. Springer, Heidelberg, July 2008. Benny Pinkas, Thomas Schneider, Nigel P. Smart, and Stephen C. Williams. Secure two-party computation is practical. In Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings, pages 250–267, 2009. Samee Zahur, Mike Rosulek, and David Evans. Two halves make a whole - reducing data transfer in garbled circuits using half gates. In Elisabeth Oswald and Marc Fischlin, editors, EUROCRYPT 2015, Part II, volume 9057 of LNCS, pages 220–250. Springer, Heidelberg, April 2015.	
17	Конфиденциальное вычисление пересечений множеств	Private set intersection	https://eprint.iacr.org/2020/300.pdf V. Kolesnikov, R. Kumaresan, M. Rosulek and N. Trieu. Efficient Batched Oblivious PRF with Applications to Private Set Intersection. In the 23rd ACM CCS, pages 818–829, 2016. B. Pinkas, M. Rosulek, N. Trieu and A. Yanai. SpOT-Light: Lightweight Private Set Intersection from Sparse OT Extension. In CRYPTO 2019, Springer (LNCS 11694), pages 401–431, 2019. B. Pinkas, T. Schneider and M. Zohner. Scalable Private Set Intersection Based on OT Extension. In ACM Transactions on Privacy and Security, 21(2):7:1–35, 2018.	
18	Безопасные	Honest-majority multi-party computations with	https://eprint.iacr.org/2020/300.pdf Z. Beerliov´a-Trub´ıniov´a and M. Hirt. Perfectly-Secure	Левкина У.С.

	многосторонние вычисления на основе схем разделения секрета	Secret Sharing	MPC with Linear Communication Complexity. TCC 2008, Springer (LNCS 4948), pages 213–230, 2008. K. Chida, D. Genkin, K. Hamada, D. Ikarashi, R. Kikuchi, Y. Lindell and A. Nof. Fast Large-Scale Honest-Majority MPC for Malicious Adversaries. In CRYPTO 2018, Springer (LNCS 10993), pages 34–64, 2018. I. Damg˚ard and J. Nielsen. Scalable and Unconditionally Secure Multiparty Computation. In CRYPTO 2007, Springer (LNCS 4622), pages 572–590, 2007. J. Furukawa and Y. Lindell. Two-Thirds Honest-Majority MPC for Malicious Adversaries at Almost the Cost of Semi-Honest. In the 26th ACM CCS, pages 1557–1571, 2019	

Для закрепления темы за Вами необходимо прислать письмо на адрес svzapechnikov@yandex.ru. Приоритет выбора темы определяется по времени получения письма. В случае, если тема уже занята, необходимо будет выбрать другую тему из числа свободных. Обновлённые списки закреплённых за Вами тем будут публиковаться на главной странице сайта cryptowiki.net.