Темы БДЗ для выполнения на сайте cryptowiki.net, группы М18-507,517, 2018/19 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/	
2	Масштабируемые прозрачные доказательства знания с нулевым разглашением	Zero-knowledge Scalable Transparent Arguments of Knowledge (zk-STARKs)	https://eprint.iacr.org/2018/046.pdf	Ермаков К., гр. М18-517
3	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	
4	Механизм двойного храповика	Double ratchet	https://signal.org/docs/specifications/doubleratchet/ https://signal.org/docs/specifications/x3dh/	Филиппов А.И., гр. М18-507
5	Протоколы защищенного двустороннего асинхронного канала передачи данных с максимальными свойствами	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	

	безопасности			
6	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	
7	Постквантовые протоколы обмена ключами на основе изогений эллиптических кривых	Post-quantum isogeny-based key exchange	https://eprint.iacr.org/2018/882.pdf https://eprint.iacr.org/2018/730.pdf https://eprint.iacr.org/2011/506.pdf	Булычев И.Г., гр. М18-507
8	Стойкость криптосхем после компрометации ключей	Post-compromise security	https://eprint.iacr.org/2016/221.pdf https://eprint.iacr.org/2015/486.pdf	Цыганов М., гр. М18-507
9	Анонимные атрибутные удостоверения	Anonymous credentials	https://camenisch.org/eprivacy/ https://camenisch.org/eprivacy/ePrivacy_F04b.pdf https://camenisch.org/eprivacy/ePrivacy_F05.pdf https://camenisch.org/eprivacy/ePrivacy_F06.pdf https://camenisch.org/eprivacy/ePrivacy_F07.pdf	Япаров Д.А., гр. М18-517
10	Неинтерактивные системы доказательства Грота-Сахаи	Groth-Sahai non-interactive proof systems	https://eprint.iacr.org/2013/662.pdf https://eprint.iacr.org/2007/155.pdf	Космынин Н., гр. М18-517
11	Луковичное шифрование и его применение в	Onion encryption and its application for Tor anonymous	https://eprint.iacr.org/2018/162.pdf https://eprint.iacr.org/2018/126.pdf http://cs.brown.edu/~anna/papers/cl05.pdf	Стуканов А.А., гр. М18-507

	протоколах анонимной сети Tor	communication		
12	Конфиденциальное обучение нейронных сетей	Privacy-preserving neural networks learning	https://eprint.iacr.org/2018/073.pdf http://proceedings.mlr.press/v48/gilad-bachrach16.pdf https://eprint.iacr.org/2017/396.pdf	Перекос В., гр. М18-517
13	Подписи, сохраняющие алгебраическую структуру	Structure-preserving signatures	https://eprint.iacr.org/2017/524.pdf https://eprint.iacr.org/2015/824.pdf	Мазуров М. гр М18-517
14	Прямая анонимная аттестация	Direct anonymous attestation	https://eprint.iacr.org/2015/1246.pdf https://eprint.iacr.org/2004/205.pdf	Руденок Д., гр. М18-517
15	Аутентичный обмен ключами, основанный на паролях	Password authenticated key exchange (PAKE)	https://www.iacr.org/archive/eurocrypt2000/1807/18070140-new.pdf https://www.iacr.org/archive/eurocrypt2005/34940406/34940406.pdf	Яковлева Е.А., гр М18-517
16	Семейство масштабируемых протоколов консенсуса Algorand	Algorand: Scaling Byzantine agreements	https://eprint.iacr.org/2017/454.pdf https://arxiv.org/pdf/1607.01341.pdf	Политов Н.С., гр. М18-517
17	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	
18	Схемы электронной цифровой подписи на основе скрученных		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	

	эллиптических кривых Эдвардса			
19	Конфиденциальное вычисление пересечения множеств	Private set intersection	https://eprint.iacr.org/2017/738.pdf https://eprint.iacr.org/2016/799.pdf https://eprint.iacr.org/2017/769.pdf	Коновалов Н., гр. М18-517
20	Конфиденциальное обучение линейной регрессии	Private linear regression	https://eprint.iacr.org/2016/892.pdf	Ковалёва А.И., гр. М18-517
21	Конфиденциальное агрегирование данных для машинного обучения	Secure data aggregation for machine learning	https://eprint.iacr.org/2017/281.pdf https://www.usenix.org/system/files/conference/nsdi17/nsdi17-corrigan-gibbs.pdf	Ханнанов В.С., гр. М18-517

Для закрепления темы за Вами необходимо прислать письмо на адрес svzapechnikov@yandex.ru. Приоритет выбора темы определяется по времени получения письма. В случае коллизии необходимо выбрать другую тему из числа свободных.