Baek, Joonsang (ed.); **Susilo, Willy (ed.)**; **Kim, Jongkil (ed.)**
Provable security. 12th international conference, ProvSec 2018, Jeju, South Korea, October 25–28, 2018. Proceedings. (English) Zbl 1398.94007
Lecture Notes in Computer Science 11192. Cham: Springer (ISBN 978-3-030-01445-2/pbk; 978-3-030-01446-9/ebook). xi, 424 p. (2018).

The articles of this volume will be reviewed individually. For the preceding conference see [Zbl 1426.94002].

Indexed articles:

Dupin, Aurélien; Pointcheval, David; Bidan, Christophe, On the leakage of corrupted garbled circuits, 3-21 [Zbl 1421.94084]

Dupin, Aurélien; Robert, Jean-Marc; Bidan, Christophe, Location-proof system based on secure multi-party computations, 22-39 [Zbl 1421.94085]

Tsaloli, Georgia; Liang, Bei; Mitrokotsa, Aikaterini, Verifiable homomorphic secret sharing, 40-55 [Zbl 1421.94087]

Fujioka, Atsushi; Yoneyama, Kazuki, Single private-key generator security implies multiple private-key generators security, 56-74 [Zbl 1421.94048]

Ateniese, Giuseppe; Kiayias, Aggelos; Magri, Bernardo; Tselekounis, Yiannis; Venturi, Daniele, Secure outsourcing of cryptographic circuits manufacturing, 75-93 [Zbl 1421.94035]

Zhao, Shuoyao; Yu, Yu; Zhang, Jiang, Secure outsourcing of cryptographic circuits, 94-108 [Zbl 1421.94082]

Paul, Arinjita; Srinivasavaradhan, Varshika; Sharmila Deva Selvi, S.; Pandu Rangan, C., A CCA-secure collusion-resistant identity-based proxy re-encryption scheme, 111-128 [Zbl 1421.94065]

Yasuda, Takanori, Multivariate encryption schemes based on the constrained MQ problem, 129-146 [Zbl 1421.94081]

Attrapadung, Nuttapong; Hanaoka, Goichiro; Hirano, Takato; Kawai, Yutaka; Koseki, Yoshihiro; Schuldt, Jacob C. N., Token-based multi-input functional encryption, 147-164 [Zbl 1421.94036]

Persichetti, Edoardo, On the CCA2 security of McEliece in the standard model, 165-181 [Zbl 1421.94068]

Xu, Shengmin; Yang, Guomin; Mu, Yi; Liu, Ximeng, Efficient attribute-based encryption with blackbox traceability, 182-200 [Zbl 1421.94079]

Branco, Pedro; Mateus, Paulo, A code-based linkable ring signature scheme, 203-219 [Zbl 1421.94083]

Chatterjee, Sanjit; Kabaleeshwaran, R., Towards static assumption based cryptosystem in pairing setting: further applications of DéjàQ and dual-form signature (extended abstract), 220-238 [Zbl 1421.94043]

Hiromasa, Ryo, Digital signatures from the middle-product LWE, 239-257 [Zbl 1421.94057]

Derler, David; Ramacher, Sebastian; Slamanig, Daniel, Generic double-authentication preventing signatures and a post-quantum instantiation, 258-276 [Zbl 1443.94090]

Zhao, Gongming; Tian, Miaomiao, A simpler construction of identity-based ring signatures from lattices, 277-291 [Zbl 1443.94102]

Sato, Shingo; Hirose, Shoichi; Shikata, Junji, Generic construction of sequential aggregate MACs from any MACs, 295-312 [Zbl 1443.94101]

Zhang, Xiangyang; Shen, Yaobin; Yan, Hailun; Zou, Ying; Wan, Ming; Wu, Zheyi; Wang, Lei, Length-preserving encryption based on single-key tweakable block cipher, 313-326 [Zbl 1443.94086]

Yang, Zheng; Järvinen, Kimmo, Modeling privacy in WiFi fingerprinting indoor localization, 329-346 [Zbl 1443.94084]

Boyd, Colin; Davies, Gareth T.; Gjøsteen, Kristian; Raddum, Håvard; Toorani, Mohsen, Security notions for cloud storage and deduplication, 347-365 [Zbl 1443.94048]

Becerra, José; Ostrev, Dimiter; Škrobot, Marjan, Forward secrecy of SPAKE2, 366-384 [Zbl 1443.94045]

Hale, Britta, User-mediated authentication protocols and unforgeability in key collision, 387-396 [Zbl 1443.94091]

Helsloot, Leon J.; Tillem, Gamze; Erkin, Zekeriya, BAdASS: preserving privacy in behavioural advertising with applied secret sharing, 397-405 [Zbl 1443.94093]

Sato, Shingo; Shikata, Junji, Signcryption with quantum random oracles, 406-414 [Zbl 1443.94078]

Yasuda, Satoshi; Koseki, Yoshihiro; Sakai, Yusuke; Kitagawa, Fuyuki; Kawai, Yutaka; Hanaoka, Goichiro, Formal treatment of verifiable privacy-preserving data-aggregation protocols, 415-422 [Zbl 1443.94085]

MSC:

94-06	Proceedings, conferences, collections, etc. pertaining to information and communication theory	Cited in **1** Review
94A60	Cryptography	
94A62	Authentication, digital signatures and secret sharing	
00B25	Proceedings of conferences of miscellaneous specific interest	

Full Text: DOI