

## Author Index

- Albrecht, Martin R. I-622  
Alwen, Joël II-358  
Ambrona, Miguel II-822  
Andrychowicz, Marcin II-586  
Aono, Yoshinori I-789
- Bader, Christoph II-273  
Badrinarayanan, Saikrishna II-764  
Ball, Marshall II-881  
Barthe, Gilles II-822  
Batina, Lejla I-403  
Belaïd, Sonia II-616  
Bellare, Mihir I-566, I-729, II-792  
Benhamouda, Fabrice II-616  
Bernstein, Daniel J. I-566  
Biryukov, Alex I-372  
Bishop, Allison I-58  
Bootle, Jonathan II-327  
Brakerski, Zvika II-852  
Brzuska, Christina I-670
- Canetti, Ran I-117  
Carlet, Claude I-311  
Castrycck, Wouter I-147  
Cerulli, Andrea II-327  
Chaidos, Pyrros II-327  
Chen, Binyi II-358  
Cheon, Jung Hee I-509  
Ciampi, Michele II-63  
Costello, Craig I-403  
Cramer, Ronald II-559  
Dachman-Soled, Dana II-649, II-881
- Damgård, Ivan II-420  
Deshpande, Apoorvaa II-124  
Dinur, Itai I-484  
Dodis, Yevgeniy II-679  
Ducas, Léo I-294, II-559  
Durvaux, François I-240  
Dziembowski, Stefan II-586
- Faust, Sebastian II-586  
Fehr, Serge II-477
- Fillinger, Max II-477  
Fouque, Pierre-Alain I-509  
Fuller, Benjamin I-117
- Gama, Nicolas II-528  
Garg, Sanjam II-448  
Gay, Romain I-1  
Gaži, Peter I-87  
Granger, Robert I-263  
Groth, Jens II-305, II-327  
Guo, Jian I-196
- Hayashi, Takuya I-789  
Hofheinz, Dennis I-1  
Hu, Yupu I-537
- Iliashenko, Iliia I-147  
Izabachène, Malika II-528
- Jacobsen, Håkon I-670  
Jaeger, Joseph I-758  
Jager, Tibor II-273  
Jia, Huiwen I-537  
Jiao, Lin I-168  
Journault, Anthony I-311  
Jovanovic, Philipp I-263
- Kamath, Chethan II-358  
Karpman, Pierre I-459  
Katz, Jonathan II-649  
Khurana, Dakshita II-184, II-213  
Kiayias, Aggelos II-705  
Kiltz, Eike I-1  
Kiss, Ágnes I-699  
Kiyoshima, Susumu II-93  
Kolmogorov, Vladimir II-358  
Komargodski, Ilan II-852  
Koppula, Venkata II-124  
Kraschewski, Daniel II-213  
Kulkarni, Mukul II-881
- Lee, Changmin I-509  
Leurent, Gaëtan I-344

- Li, Ruilin I-196  
 Li, Yong II-273  
 Libert, Benoît II-1  
 Lin, Huijia I-28  
 Ling, San II-1  
 Liu, Meicheng I-196  
 Liu, Tianren II-679  
 Luykx, Atul I-596
- Mahmoody, Mohammad II-243  
 Maji, Hemanta K. II-184, II-213  
 Malkin, Tal II-881  
 Méaux, Pierrick I-311  
 Mennink, Bart I-263  
 Micciancio, Daniele I-820  
 Miles, Eric II-764  
 Minaud, Brice I-509  
 Mohammed, Ameer II-243  
 Mukherjee, Pratyay II-448, II-735
- Neves, Samuel I-263  
 Nguyen, Khoa II-1  
 Nguyen, Phong Q. II-528  
 Nielsen, Jesper Buus II-420  
 Nishimaki, Ryo II-388
- Ostrovsky, Rafail II-420
- Pandey, Omkant II-448  
 Paneth, Omer I-117  
 Passelègue, Alain II-616  
 Pastro, Valerio I-58  
 Paterson, Kenneth G. I-622  
 Peikert, Chris II-559  
 Perrin, Léo I-372  
 Persiano, Giuseppe II-63  
 Petit, Christophe II-327  
 Peyrin, Thomas I-459  
 Pietrzak, Krzysztof II-358  
 Polychroniadou, Antigoni II-448  
 Prabhakaran, Manoj II-213  
 Preneel, Bart I-596  
 Prouff, Emmanuel II-616
- Rajaraman, Rajmohan I-58  
 Regev, Oded II-559  
 Renes, Joost I-403  
 Reyzin, Leonid I-117
- Rijmen, Vincent I-196  
 Ristenpart, Thomas I-758  
 Rosén, Adi II-420  
 Ryu, Hansol I-509
- Sahai, Amit II-184, II-213, II-764  
 Sarkar, Palash I-429  
 Scafuro, Alessandra II-63  
 Schäge, Sven II-273  
 Schmidt, Benedikt II-822  
 Schneider, Thomas I-699  
 Segev, Gil II-852  
 Singh, Shashank I-429  
 Siniscalchi, Luisa II-63  
 Smith, Adam I-117  
 Stam, Martijn II-679  
 Standaert, François-Xavier I-240, I-311  
 Stebila, Douglas I-670  
 Stehlé, Damien I-294  
 Steinberger, John II-154, II-679  
 Stepanovs, Igors II-792  
 Stevens, Marc I-459  
 Strenzke, Falko I-644  
 Sun, Bing I-196  
 Szepieniec, Alan I-596
- Tackmann, Björn I-729  
 Takagi, Tsuyoshi I-789  
 Tang, Qiang I-758  
 Tessaro, Stefano I-87, I-566, II-358  
 Thillard, Adrian II-616  
 Thiruvengadam, Aishwarya II-649  
 Tiessen, Tyge I-214
- Udovenko, Aleksei I-372  
 Unruh, Dominique II-497
- Vercauteren, Frederik I-147  
 Vergnaud, Damien II-616  
 Visconti, Ivan II-63
- Walter, Michael I-820  
 Wang, Huaxiong II-1  
 Wang, Mingsheng I-168  
 Wang, Yuntao I-789  
 Waters, Brent II-124, II-792  
 Wee, Hoeteck I-1  
 Wicks, Daniel I-58, II-388, II-735

Xie, Xiang [II-528](#)

Yamada, Shota [II-32](#)

Yasuda, Kan [I-596](#)

Yu, Yu [II-154](#)

Zhandry, Mark [II-388](#), [II-764](#)

Zhang, Bin [I-168](#)

Zhou, Hong-Sheng [II-705](#)

Zikas, Vassilis [II-705](#)