

Biography: Dr. Josh Benaloh

Josh Benaloh is Senior Cryptographer at Microsoft Research and an Affiliate Faculty Member of Computer Science and Engineering at the University of Washington. He earned his S.B. degree from the Massachusetts Institute of Technology and M.S., M.Phil., and Ph.D. degrees from Yale University where his 1987 doctoral dissertation “Verifiable Secret-Ballot Elections” introduced the use of homomorphic encryption as a means to allow individual voters to confirm that their votes have been correctly counted. Dr. Benaloh served seventeen years on the Board of Directors of the International Association for Cryptologic Research and currently serves on the Coordinating Committee of the Election Verification Network. He has been granted over fifty U.S. patents and has written and spoken extensively on cryptographic primitives and protocols, election technologies, and cryptographic policy. Dr. Benaloh is an author of the influential “Keys Under Doormats” expert report which details the damage that would be created by mandating exceptional government access to encrypted data. He is also an author of the U.S. Vote Foundation report on the viability of end-to-end verifiable Internet voting systems and recently completed service on the National Academies of Science, Engineering, and Medicine Committee on the Future of Voting whose final report “Securing the Vote – Protecting American Democracy” has been cited in numerous articles and deliberations.

Outside of professional activities, Dr. Benaloh served eight years on and chaired the Citizen Oversight Panel for Sound Transit which is investing \$2 billion annually on expanding the public transit infrastructure for the Seattle region. He has also authored numerous puzzles for competitive puzzle-solving events.