References

AB96

Anderson, R., Biham, E., “Two Practical and Provably Secure Block Ciphers: BEAR and LION”, 1996.

AEZV5

Hoang, V., Krovetz, T., Rogaway, P., “AEZ v5: Authenticated Encryption by Enciphering”, March 2017, http://web.cs.ucdavis.edu/~rogaway/aez/aez.pdf.

BRIDGING

Danezis, G., Syverson, P., “Bridging and Fingerprinting: Epistemic Attacks on Route Selection”, Proceedings of PETS 2008, Leuven, Belgium, July 2008, https://www.freehaven.net/anonbib/cache/danezis-pet2008.pdf.

COMPULS05

Danezis, G., Clulow, J., “Compulsion Resistant Anonymous Communications”, Proceedings of Information Hiding Workshop, June 2005, https://www.freehaven.net/anonbib/cache/ih05-danezisclulow.pdf.

ED25519

https://www.rfc-editor.org/rfc/rfc8032.

FINGERPRINTING

Danezis, G., Clayton, R., “Route Finger printing in Anonymous Communications”, https://www.cl.cam.ac.uk/~rnc1/anonroute.pdf.

KATZMIXNET

Angel, Y., Danezis, G., Diaz, C., Piotrowska, A., Stainton, D., “Katzenpost Mix Network Specification”, June 2017, https://katzenpost.network/docs/specs/pdf/mixnet.pdf.

KATZMIXPKI

Angel, Y., Piotrowska, A., Stainton, D., “Katzenpost Mix Network Public Key Infrastructure Specification”, December 2017, https://katzenpost.network/docs/specs/pdf/pki.pdf.

KATZMIXWIRE

Angel, Y., “Katzenpost Mix Network Wire Protocol Specification”, June 2017, https://katzenpost.network/docs/specs/pdf/wire.pdf.

KEMCOMB

Federico Giacon, Felix Heuer, Bertram Poettering, “KEM Combiners”, 2018, https://link.springer.com/chapter/10.1007/978-3-319-76578-5_7

LOCALVIEW

Gogolewski, M., Klonowski, M., Kutylowsky, M., “Local View Attack on Anonymous Communication”, https://cs.pwr.edu.pl/kutylowski/articles/LocalView-WWW.pdf.

LOOPIX

Piotrowska, A., Hayes, J., Elahi, T., Meiser, S., Danezis, G., “The Loopix Anonymity System”USENIX, August 2017, https://arxiv.org/pdf/1703.00536.pdf.

MIRANDA

Leibowitz, H., Piotrowska, A., Danezis, G., Herzberg, A., “No right to remain silent: Isolating Malicious Mixes”, 2017, https://eprint.iacr.org/2017/1000.pdf.

MIXMINION

Danezis, G., Dingledine, R., Mathewson, N., “Mixminion: Design of a Type III Anonymous Remailer Protocol”, https://www.mixminion.net/minion-design.pdf.

MIXMINIONDIRAUTH

Danezis, G., Dingledine, R., Mathewson, N., “Type III (Mixminion) Mix Directory Specification”, December 2005, https://www.mixminion.net/dir-spec.txt.

MIXRELIABLE

Dingledine, R., Freedman, M., Hopwood, D., Molnar, D., “A Reputation System to Increase MIX-Net Reliability”, 2001, Information Hiding, 4th International Workshop, https://www.freehaven.net/anonbib/cache/mix-acc.pdf.

MIXTOPO10

Diaz, C., Murdoch, S., Troncoso, C., “Impact of Network Topology on Anonymity and Overhead in Low-Latency Anonymity Networks”, PETS, July 2010, https://www.esat.kuleuven.be/cosic/publications/article-1230.pdf.

MPRA11

Maines, L., Piva, M., Rimoldi, A., Sala, M., “On the provable security of BEAR and LION schemes”, May 2011, arXiv:1105.0259, https://arxiv.org/abs/1105.0259.

NOISE

Perrin, T., “The Noise Protocol Framework”, May 2017, https://noiseprotocol.org/noise.pdf.

NOISEHFS

Weatherley, R., “Noise Extension: Hybrid Forward Secrecy”, https://github.com/noiseprotocol/noise_hfs_spec/blob/master/output/noise_hfs.pdf.

PEERFLOW

Johnson, A., Jansen, R., Segal, A., Syverson, P., “PeerFlow: Secure Load Balancing in Tor”, July 2017, Proceedings on Privacy Enhancing Technologies, https://petsymposium.org/2017/papers/issue2/paper12-2017-2-source.pdf.

PQNOISE

Yawning Angel, Benjamin Dowling, Andreas Hülsing, Peter Schwabe and Florian Weber, “Post Quantum Noise”, September 2023, https://eprint.iacr.org/2022/539.pdf.

RFC2119

Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, http://www.rfc-editor.org/info/rfc2119.

RFC5246

Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, DOI 10.17487/RFC5246, August 2008, http://www.rfc-editor.org/info/rfc5246.

RFC5322

Resnick, P., Ed., “Internet Message Format”, RFC 5322, DOI 10.17487/RFC5322, October 2008, https://www.rfc-editor.org/info/rfc5322.

RFC6234

Eastlake 3rd, D. and T. Hansen, “US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)”, RFC 6234, DOI 10.17487/RFC6234, May 2011, https://www.rfc-editor.org/info/rfc6234.

RFC7049

C. Bormann, P. Hoffman, “Concise Binary Object Representation (CBOR)”, Internet Engineering Task Force (IETF), October 2013, https://www.rfc-editor.org/info/rfc7049.

RFC7515

Jones, M., Bradley, J., Sakimura, N., “JSON Web Signature (JWS)”, May 2015, https://www.rfc-editor.org/info/rfc7515.

RFC7539

Nir, Y. and A. Langley, “ChaCha20 and Poly1305 for IETF Protocols”, May 2015, RFC 7539, DOI 10.17487/RFC7539, http://www.rfc-editor.org/info/rfc7539.

RFC7693

Saarinen, M-J., Ed., and J-P. Aumasson, “The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)”, RFC 7693, DOI 10.17487/RFC7693, November 2015, http://www.rfc-editor.org/info/rfc7693.

RFC7748

Langley, A., Hamburg, M., and S. Turner, “Elliptic Curves for Security”, RFC 7748, January 2016, https://www.rfc-editor.org/info/rfc7748.

SECNOTSEP

Miller, M., Tulloh, B., Shapiro, J., “The Structure of Authority: Why Security Is not a Separable Concer”, http://www.erights.org/talks/no-sep/secnotsep.pdf.

SEDA

Welsh, M., Culler, D., Brewer, E., “SEDA: An Architecture for Well-Conditioned, Scalable Internet Services”, 2001, ACM Symposium on Operating Systems Principles, http://www.sosp.org/2001/papers/welsh.pdf.

SFMIX03

Danezis, G., “Forward Secure Mixes”, Proceedings of 7th Nordic Workshop on Secure IT Systems, 2002, https://www.freehaven.net/anonbib/cache/Dan:SFMix03.pdf.

SP80038A

Dworkin, M., “Recommendation for Block Cipher Modes of Operation”, SP800-38A, 10.6028/NIST.SP.800, December 2001, https://doi.org/10.6028/NIST.SP.800-38A.

SPHINCS256

Bernstein, D., Hopwood, D., Hulsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schwabe, P., Wilcox O'Hearn, Z., “SPHINCS: practical stateless hash-based signatures”, http://sphincs.cr.yp.to/sphincs-20141001.pdf.

SPHINX09

Danezis, G., Goldberg, I., “Sphinx: A Compact and Provably Secure Mix Format”, DOI 10.1109/SP.2009.15, May 2009, https://cypherpunks.ca/~iang/pubs/Sphinx_Oakland09.pdf.

SPHINXSPEC

Angel, Y., Danezis, G., Diaz, C., Piotrowska, A., Stainton, D., “Sphinx Mix Network Cryptographic Packet Format Specification”, July 2017, https://katzenpost.network/docs/specs/pdf/sphinx.pdf.

TORDIRAUTH

“Tor directory protocol, version 3”, https://spec.torproject.org/dir-spec/index.html.

TORSRV

“Tor Shared Random Subsystem Specification”, https://spec.torproject.org/srv-spec/index.html.

XWING

Manuel Barbosa, Deirdre Connolly, João Diogo Duarte, Aaron Kaiser, Peter Schwabe, Karoline Varner, Bas Westerbaan, “X-Wing: The Hybrid KEM You’ve Been Looking For”, https://eprint.iacr.org/2024/039.pdf.