Benjamin J. Kaduk

15 October 2019

kaduk@mit.edu bjk@FreeBSD.org https://github.com/kaduk

Education

- **Massachusetts Institute of Technology (MIT)**, Cambridge, MA
  Ph.D., Chemistry, June 2012.
- **University of Illinois at Urbana-Champaign (UIUC)**, Champaign-Urbana, IL
  B.S., Chemistry, May 2007; B.S., Mathematics, May 2007.

Employment

- **Akamai Technologies**, Saint Louis, MO
  Senior Software Engineer, *June 2015 to present*
- **MIT Consortium for Kerberos and Internet Trust (MIT KIT)**, Cambridge, MA
  Programmer/Analyst, *July 2012 to February 2015*
  DevOps Engineer, *February 2015 to June 2015*

Software and Standards Experience

- **Internet Engineering Task Force (IETF)**
  Security Area Director, *March 2018 to present*
  IETF Sergeant-at-Arms, *May 2017 to September 2019*
  Author/coauthor of several RFCs and WG/RG internet-drafts, *May 2014 to present*
  Chair of the Authentication and Authorization for Constrained Environments (ace) working group, *October 2017 to March 2018*
  Chair of the Common Authentication Technology Next Generation (kitten) working group, *July 2014 to March 2018*
- **OpenSSL**
  OpenSSL committer, *June 2017 to present*
  Help to maintain the OpenSSL distribution, through feature development, code and design review, and documentation.
- **MIT Kerberos**
  Kerberos security team member, *February 2013 to present*
  Co-maintainer of packaging for Debian Linux, *August 2013 to present*
  Primary maintainer of Kerberos for Windows, *July 2012 to June 2015*
  MIT krb5 maintainer, *June 2012 to June 2015*
- **MacOS 64-bit SAP SNC Shim for System GSS-API Support**
  Developed the shim library at `https://github.com/kaduk/osxsnc`, which implements a SAP Secure Network Communications (SNC) adaptor, to bridge the ABI incompatibility between the 64-bit SAP GUI on MacOS and the system (and MIT Kerberos) GSS-API library.
- **AFS-3 Standardization Group**
  Chair, *October 2015 to October 2017*
  Finalized the specification for the rxgk (GSS-API) Rx security class and improved the specification for rxgk integration with the AFS-3 protocol, currently awaiting working group last call.
- **OpenAFS Network File System**
  OpenAFS Guardian (development lead) and Security Officer, *August 2015 to present*
  Packaging maintainer for Debian Linux, *August 2014 to present*
  Packaging maintainer for FreeBSD, *May 2011 to May 2019*
- **MIT Athena Release Team**
  Debathena maintainer, *March 2009 to June 2015*
  Managed a set of 200 Debian packages on top of Debian/Ubuntu that implement the MIT Athena environment on the full set of supported releases, including compatibility layers as needed.
- **Q-Chem**
  Contributor, *September 2007 to June 2012*
  Implemented new methods for computing excited-state energies, maintained existing code, and fixed bugs in the Q-CHEM *ab initio* computational chemistry package (`https://q-chem.com`). Helped review infrastructure and buildsystem changes at the request of upstream.

- **FreeBSD**
  Documentation committer, *March 2012 to present*
  Maintainer of `net/openafs`, `net-im/zephyr`, and `devel/e2fsprogs-libss` in the Ports Collection, *May 2011 to present*
  Primary editor on the Quarterly Status Report team, *July 2014 to March 2018*

- **MIT Student Information Processing Board (SIPB)**
  Member, *Fall 2007 to present*
  Treasurer, *February 2008 to February 2012*
  As a member of MIT's computer club, which provides many services to the community above and beyond MIT IS&T, maintained two AFS cells, a Solaris dialup, the mail archive/everything-else server, and documentation offerings, and provided user support for computing-related issues and a webhosting service.

Skills and Languages

- Expert knowledge of C99; proficient in C/Fortran linkage, Debian packaging, LaTeX, and Bourne shell; familiar with C++ and Python; limited proficiency in French.

Honors, Awards, and Recognitions

- MIT IS&T Spotlight Award, August 2013
- MIT Presidential Fellowship, September 2007
- 35th International Chemistry Olympiad Bronze Medalist, July 2003

Publications and Research

- Kaduk B., Short M. (2018) Deprecate 3DES and RC4 in Kerberos. IETF RFC 8429, BCP 218.
- Wilkinson S., Kaduk B. (2014) rxgk: GSSAPI based security class for RX. AFS-3 Standardization Group Experimental document.
- Kaduk B. (2014) Structure of the GSS Negotiation Loop. IETF RFC 7546.
- Kaduk B., Tsuchimochi T., and Van Voorhis T. (2014) Analytic energy gradients for constrained DFT-configuration interaction. *J. Chem Phys.*, **140**, 18A503.
- Shao Y. *et al*. (2014) Advances in molecular quantum chemistry contained in the Q-Chem 4 program package. *Mol. Phys.*, **113**(2), 184–215.
- Kaduk B., Kowalczyk T., and Van Voorhis T. (2012) Constrained density functional theory. *Chem. Rev.*, **112**(1), 321–370.
- Kaduk B., Van Voorhis T. (2010) Conical intersections using constrained density functional theory–configuration interaction. *J. Chem. Phys.*, **133**, 061102
- Van Voorhis T., Kowalczyk T., Kaduk B., Wang L.-P., Cheng C.-L., and Wu Q. (2010) The Diabatic Picture of Electron Transfer, Reaction Barriers, and Molecular Dynamics. *Annu. Rev. Phys. Chem.*, **61**(1), 149–170.
- Wu Q., Kaduk B., and Van Voorhis T. (2009) Constrained density functional theory based configuration interaction improves the prediction of reaction barrier heights. *J. Chem. Phys.*, **130**(3), 034109
- Yang S., Coe J.D., Kaduk B., and Martínez T.J. (2009) An "optimal" spawning algorithm for adaptive basis set expansion in nonadiabatic dynamics. *J. Chem. Phys.* **130**, 134113.