Joseph Ayo Akinyele

Curriculum Vitae

318 Paladium Court
Owings Mills, MD
Baltimore, MD 21117
☎ *(443) 570 9776*
✉ *akinyelj@cs.jhu.edu*
🖱 *cs.jhu.edu/~akinyelj*

Education

2009–2013 **Ph.D., Computer Science**, *Johns Hopkins University (JHU)*, Computer Science, Baltimore, MD.
Advised by: Dr. Avi Rubin, Dr. Matthew Green and Dr. Susan Hohenberger Waters
Thesis: Enabling Machine-aided Cryptographic Design

2006–2007 **M.S., Software Engineering**, *Carnegie Mellon University (CMU)*, Pittsburgh, PA.
Advisor: Dr. Jonathan Aldrich

2003–2006 **B.S., Computer Science**, *Bowie State University*, Laurel, MD.
Graduated summa cum laude

Research Interests

privacy-preserving cryptography in the cloud and mobile platforms

automating the design and verification of cryptographic transformations

Publications

Conference Publications

2015 J. A. Akinyele, C. Garman, S. Hohenberger. “Automating a Fast and Secure Translation from Type-I to Type-III Pairing Schemes.” In Proceedings of the 22nd ACM conference on Computer and Communications Security, (CCS), 2015.

2014 J. A. Akinyele, G. Barthe, B. Grégoire, B. Schmidt, P. Strub. “Certified Synthesis of Efficient Batch Verifiers." IEEE Computer Security Foundations (CSF) Symposium, 2014.

2013 J. A. Akinyele, M. Green, S. Hohenberger. “Using SMT Solvers to Automate Design Tasks for Encryption and Signature Schemes." In Proceedings of the 20th ACM conference on Computer and Communications Security, (CCS), 2013.

2012 J. A. Akinyele, M. Green, S. Hohenberger, M. Pagano. “Machine-generated Algorithms, Proofs and Software for the Batch Verification of Digital Signature Schemes." In Proceedings of the 19th ACM conference on Computer and Communications Security, (CCS), 2012.

2011 J. A. Akinyele, M. Pagano, M. Green, C. Lehmann, Z. Peterson and A. Rubin. “Securing Electronic Medical Records (EMRs) Using Attribute-Based Encryption On Mobile Devices." 1st ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), 2011.

Journal Publications

2014 J. A. Akinyele, M. Green, S. Hohenberger, M. Pagano. “Machine-generated Algorithms, Proofs and Software for the Batch Verification of Digital Signature Schemes." Journal of Computer Security (JCS), Volume 22, Number 6, pages 867-912, 2014.

2013 J. A. Akinyele, C. Garman, I. Miers, M. Pagano, M. Rushanan, M. Green, A. Rubin. “Charm: A Framework for Rapidly Prototyping Cryptosystems." Journal of Cryptographic Engineering (JCEN), Volume 3, Issue 2, page 111-128, 2013.

Technical Reports

2010 J. A. Akinyele, C. Lehmann, M. Green, M. Pagano, Z. Peterson, and A. Rubin. “Self-protecting EMRs using Attribute-Based Encryption." http://eprint.iacr.org/2010/565.

2008 C. Waits, J. Akinyele, R. Nolan, and L. Rogers. “Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis." August, 2008. CMU/SEI-2008-TN-017.

Experience

Dec, 2013 – Present **Research Scientist**, *Zeutro, LLC: Encryption & Data Security*, Baltimore, MD.

- Developing a commercial-grade attribute-based encryption toolkit to provide data-at-rest protections for cloud and mobile applications.
- Researching practical ways to improve the state-of-the-art for managing attribute-based encryption keys to support a variety of applications.
- Developing an advanced data protection and key management product around the attribute-based encryption toolkit for securing enterprise data.

Jan, 2010 – Dec, 2013 **Research Assistant**, *Johns Hopkins University*, Baltimore, MD.

- Developed Charm, a new cryptographic framework in Python and C++, to assist security researchers in rapidly and easily implementing advanced cryptographic primitives.
- Researched automated design of cryptographic transformations on encryption and signature schemes in terms of improving efficiency and/or increasing security using SMT solver techniques.

May – Aug 2012 **Intern**, *MIT Lincoln Laboratory*, Lexington, MA.

- Worked on a team for developing the Lincoln Open Cryptographic Key Management Architecture (LOCKMA) software library to provide real-time key management protections to Unmanned Aerial Vehicles (UAVs).
- Applied Charm-like design concepts to facilitate usability, modularity and extensibility in the implementation of LOCKMA's cryptographic backend.
- *Mentors*: Dr. Roger Khazan (rkh@ll.mit.edu) and Dan Utin (danu@ll.mit.edu)

Sep, 2007 – Jan, 2010 **Software Engineer**, *Johns Hopkins University Applied Physics Laboratory*, Laurel, MD.

- Implemented information and application assurance solutions that leverage virtualization technologies and trusted computing for sponsors.
- Applied techniques for verifying the integrity of the Linux Kernel in virtualized and non-virtualized environments.
- *Supervisor*: Ginny Walker (Ginny.Walker@jhuapl.edu)

Open-Source Software Projects

libfenc Part of a team that developed an experimental functional encryption library in C for advanced cryptographic primitives such as ciphertext-policy and key-policy attribute-based encryption.

Project webpage: `http://code.google.com/p/libfenc`.

Charm Co-designer with Prof. Matt Green, lead and primary developer for a new cryptographic framework for rapidly prototyping advanced cryptographic primitives and protocols. Charm is a Python and C/C++ library in which several cryptographic constructions in the research literature have been implemented to demonstrate implementations of complex cryptographic algorithms.

Project webpage: `http://charm-crypto.com`. **Impact**: Charm boasts an active user base and has been used by several researchers from various institutions such as MITRE, Stanford Research Institute (SRI), Raytheon BBN technologies, University of Texas (UT) at Austin, University of Illinois at Urbana-Champaign (UIUC), George Washington University (GWU) and many more institutions.

AutoTools A collection of automation tools developed as a byproduct of research at Johns Hopkins.

AutoBatch: a tool that automatically finds efficient batch verification algorithms from high-level descriptions of signature schemes. The correctness and security of this tool has been certified using the EasyCrypt framework in collaboration with researchers from INRIA Sophia-Antipolis and the IMDEA Software Institute.

AutoGroup: a tool that automatically optimizes pairing-based encryption and signature schemes based on a number of metrics. There is ongoing work to improve the security of this tool without sacrificing efficiency.

AutoStrong: a tool that automatically converts an existentially unforgeable signature into a strongly unforgeable signature.

CloudSource: a (work-in-progress) tool that automatically outsources the computation of pairing-based encryption schemes to untrusted cloud servers.

Project webpage: `https://github.com/jhuisi/auto-tools`.

Professional Activities

External Reviewer USENIX 2011-2013, PKC 2012, ESORICS 2012