

Ian Miers

Curriculum Vitae

160 Malone Hall
3400 North Charles Street
Baltimore, MD, USA 21218

✉ imiers@cs.jhu.edu
📁 cs.jhu.edu/~imiers

Education

- 2014–2017 **Doctorate of Philosophy (*expected*)**, Computer Science.
The Johns Hopkins University, Baltimore, MD, USA
Advisor: Matthew Green
- 2013–2014 **Masters of Science in Engineering**, Computer Science.
The Johns Hopkins University, Baltimore, MD, USA GPA 3.95 out of 4.0
- 2006–2010 **Bachelor of Science (with honors)**, Computer Science.
The Johns Hopkins University, Baltimore, MD, USA
GPA 3.69 out of 4.0

Publications

Peer Reviewed Journal Articles

Markulf Kohlweiss and Ian Miers. “[Accountable Metadata-Hiding Escrow: A Group Signature Case Study](#)”. In: *Proceedings on Privacy Enhancing Technologies* 2015.2 (2015).

Joseph A. Akinyele, Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, and Aviel D. Rubin. “[Charm: a framework for rapidly prototyping cryptosystems](#)”. In: *Journal of Cryptographic Engineering* 3.2 (2013).

Peer Reviewed Conference and Workshop Publications

Christina Garman, Matthew Green, and Ian Miers. “Accountable privacy for decentralized anonymous payments”. In: *Financial Cryptography and Data Security*. 2016.

Matthew Green and Ian Miers. “[Forward Secure Asynchronous Messaging from Puncturable Encryption](#)”. In: *Proceedings of the 2015 IEEE Symposium on Security and Privacy*. 2015.

Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. “[Zerocash: Decentralized Anonymous Payments from Bitcoin](#)”. In: *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. 2014.

Christina Garman, Matthew Green, and Ian Miers. “[Decentralized Anonymous Credentials](#)”. In: *Proceedings of the 21st ISOC Network and Distributed System Security Symposium (NDSS)*. 2014.

Christina Garman, Matthew Green, Ian Miers, and Aviel D Rubin. "[Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity](#)". In: *Proceedings of the 2014 Workshop on Bitcoin Research*. 2014.

Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. "[Zerocoin: Anonymous Distributed E-Cash from Bitcoin](#)". In: *Proceedings of the 2013 IEEE Symposium on Security and Privacy*. 2013.

Ian Miers, Matthew Green, Christoph U. Lehmann, and Aviel D. Rubin. "[Vis-a-vis Cryptography: Private and Trustworthy In-person Certifications](#)". In: *Proceedings of the 3rd USENIX Conference on Health Security and Privacy*. 2012.

Professional Service

- 2014 **1st Workshop on Bitcoin Research**, *Barbados*, March 7 2014, PC Member.
- 2013 **Graduate Representative Organization**, *JHU*, Communications Chair.
- 2014–Present **Graduate Representative Organization**, *JHU*, Social Chair.

Work Experience

- summer 2015 **Research Intern**, *Yahoo*, Sunnyvale, USA.
Worked with Paranoids (Yahoo's security engineering org.) and Payman Mohassel of Yahoo Labs on scaling Dynamic Searchable Encryption to millions of users with commodity hardware. This is ongoing work which aims to deploy a system that need not store indexes or updates in memory or on SSDs.
 - summer 2014 **Research Intern**, *Microsoft Research*, Cambridge, UK.
Worked on cryptography for accountable surveillance with Markulf Kohlweiss in the Constructive Security Group.
 - 2011–2013 **Research Programmer**, *Johns Hopkins University*, Baltimore, MD.
Developed software supporting cryptographic research in the Health and Medical Security lab.
 - Worked on core portions of the Charm cryptographic framework
 - Spearheaded setup and use of continuous integration systems during development
 - Conducted various research projects leveraging cryptography for securing medical records and preserving user privacy (see publications)
 - 2010–2011 **Software Development Engineer**, *Microsoft*, Redmond, WA.
Developed backend infrastructure for email security and spam filtering for Office 365.
 - Worked to scale Forefront Online Protection For Exchange (FOPE) database systems
 - Developed a framework for the audit and rollback of writes to FFO multi-partition, multi-master data storage system
 - Maintained and audited the single session sign on (SSO) system for FOPE
 - Fixed security exploits in FOPE components
 - Planned/developed features for Data Leak Protection for FOPE
-