Ian Miers

Curriculum Vitae

2 West Loop Road
New York, NY, USA 10044
✉ *imiers@cs.cornell.edu*
cs.jhu.edu/~imiers

Research Interests

Applied cryptography, computer security, and privacy enhancing technologies.

Education

2014–2017 **Doctorate of Philosophy**, Computer Science.
The Johns Hopkins University, Baltimore, MD, USA
Advisor: Prof. Matthew Green

2013–2014 **Masters of Science in Engineering**, Computer Science.
The Johns Hopkins University, Baltimore, MD, USA

2006–2010 **Bachelor of Science (with honors)**, Computer Science.
The Johns Hopkins University, Baltimore, MD, USA

Publications

(Unless otherwise noted, author ordering is alphabetical by last name not contribution.)

Peer Reviewed Journal Articles

Markulf Kohlweiss and Ian Miers. "Accountable Metadata-Hiding Escrow: A Group Signature Case Study". In: *Proceedings on Privacy Enhancing Technologies* 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

Sinisa Matetic, Karl Wüst, Moritz Schneider, Ian Miers, Kari Kostiainen, and Srdjan Capkun. "ZLiTE: Lightweight Clients for Shielded Zcash Transactions using Trusted Execution". In: *Financial Cryptography and Data Security*. 2019. Authors ordered by contribution.

Gabriel Kaptchuk, Ian Miers, and Matthew Green. "Giving State to the Stateless: Augmenting Trustworthy Computation with Ledgers". In: *Proceedings of the 26th ISOC Network and Distributed System Security Symposium (NDSS)*. 2019. Authors ordered by contribution.

Nirvan Tyagi, Muhammad Haris Mughees, Thomas Ristenpart, and Ian Miers. "Burn-Box: Self-Revocable Encryption in a World Of Compelled Access". In: *27th USENIX Security Symposium, USENIX Security*. 2018. Authors ordered by contribution.

Jens Groth, Markulf Kohlweiss, Mary Maller, Sarah Meiklejohn, and Ian Miers. "Updatable and Universal Common Reference Strings with Applications to zk-SNARKs". In: *Advances in Cryptology - CRYPTO*. 2018.

Ian Martin, Ian Miers, and Eric Wustrow. "Proof-of-Censorship: Enabling centralized censorship-resistant content providers." In: *Financial Cryptography and Data Security*. 2018.

Matthew Green and Ian Miers. "Bolt: Anonymous Payment Channels for Decentralized Currencies". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS*. 2017.

Arka Rai Choudhuri, Matthew Green, Abhishek Jain, Gabriel Kaptchuk, and Ian Miers. "Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS*. 2017.

Alessandro Chiesa, Matthew Green, Jingcheng Liu, Peihan Miao, Ian Miers, and Pratyush Mishra. "Decentralized Anonymous Micropayments". In: *Advances in Cryptology – EUROCRYPT*. 2017.

Ian Miers and Payman Mohassel. "IO-DSSE: Scaling Dynamic Searchable Encryption to Millions of Indexes By Improving Locality". In: *Proceedings of the 24th ISOC Network and Distributed System Security Symposium (NDSS)*. 2017.

Matthew Green, Watson Ladd, and Ian Miers. "A Protocol for Privately Reporting Ad Impressions at Scale". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS*. 2016.

Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan. "Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage". In: *25th USENIX Security Symposium, USENIX Security*. 2016.

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, 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.

Christina Garman, Matthew Green, and Ian Miers. "Decentralized Anonymous Credentials". In: *Proceedings of the 21st ISOC Network and Distributed System Security Symposium (NDSS)*. 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. Authors ordered by contribution.

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 Workshop on Health Security and Privacy*. 2012. Authors ordered by contribution.

Professional Service

2018 **Financial Cryptography and Data Security 2019**, PC Member.

2018 **25th ACM Conference on Computer and Communications Security**, PC Member.

2017 **5th Workshop on Bitcoin Research**, PC Member.

2016 **4th Workshop on Bitcoin Research**, PC Member.

2016–2017 **Graduate Representative Organization**, *JHU*, Chair.

2014–2016 **Graduate Representative Organization**, *JHU*, Social Chair.

2013–2014 **Graduate Representative Organization**, *JHU*, Communications Chair.

2013 **1st Workshop on Bitcoin Research**, PC Member.

Work Experience

2017– 2019 **Postdoctoral Researcher**, *Cornell Tech*, New York, USA.
Advisor: Thomas Ristenpart

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 resulted in the paper "IO-DSSE: Scaling Dynamic Searchable Encryption to Millions of Indexes By Improving Locality."

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