RESEARCH ROAD-MAP MRL-R001

Priorities for Monero Research Lab

June 12, 2017

Brandon Goodell

Correspondence:
bggoode@g.clemson.edu
Monero Research Lab

Abstract

We outline the various ideas currently under investigation by the Monero Research Lab, provide context for each task, and present some informative sources regarding each task.

We present a partial MRL "to-do" list of research items. We rank the list according to approximate urgency and time-line, beginning with the short-term/high-priority projects and ending with the long-term/lower-priority projects. This is a partial list because each item comes equipped with many sub-items, and other items not included on this list will undoubtedly find their way onto future Research Road-maps.

We wish to emphasize that this list is incomplete, and we invite the members of the Monero community to make suggestions for changes to this list. Future Research Road-maps will include comments on the progress for each of these items.

1. **Zero-knowledge Lit Review**: We are listing this item first because it is rather exciting news: Jeffrey Quesnelle, a computer science graduate student at the University of Michigan at Dearborn is pursuing his thesis and has decided this includes some work with Monero Research Lab. Jeffrey has offered to prototype implementations of new cryptographic schemes, crunch numbers, evaluate performances, and try his hand at some cryptographic proofs. Together, we are publishing a literature review of zero knowledge schemes and their application in cryptocurrencies, for submission for peer review (journal to be determined) by the end of August 2017, although I am optimistic that we will complete this sooner rather than later. We will make available a pre-print on ArXiV after a few revisions.
2. **Correcting RingCT Proofs**: In [13], there are certain flaws in the proofs that should be corrected. This could take a few weeks, more or less, but is likely quite short-term. As far as we are aware, the claims made are still valid but at least one proof is inadequate.
3. **Recent criticisms**: Recently, critics have claimed the Monero blockchain is traceable, as in [12] and [10]. Some of the concerns and claims made in these papers appear in the list below already, but we will not comment directly on these criticisms until our review is complete. We will take as much time as necessary for this, but it is urgent.

4. **Threshold multisignatures**: Shen Noether once proposed an algorithm for k-of-N multisignatures in Monero. These signatures are currently under development and testing; checking and developing rigorous proofs for this method is necessary. After revisions are made to Shen's original paper, we will publish an MRL Research Bulletin detailing the method.
5. **Churning, Mandatory Minimum Mix-ins**: Detailed by `knaccc` in [9], an attack is described where a merchant, Bob, and his customer, Alice, use an exchange, Eve, to convert cryptocurrency to fiat and back again. If Bob immediately converts all cryptocurrency to fiat after each transaction to limit his exposure to the volatility of cryptocurrency-to-fiat exchange rates, then Bob unintentionally provides information Eve needs to determine the identity of Alice. Urgency on this problem is not high because an interim solution exists, churning, but the urgency is not low either because that interim solution is expensive to users and causes blockchain bloat. However, we have not quantified the threat of this attack; it is not clear how serious this attack is. Determining more suitable solutions is not immediately obvious, and so this problem could require quite a bit of thought.
6. **Signature Size and RingCT**: Blockchain bloat can be mitigated with efficient signatures. RingCT already uses more efficient signatures than signatures in the CryptoNote reference code (as described in [13]). Some schemes, such as [4], [1], [2], exhibit sub-linear sizes of ring signature and have been investigated by MRL in the past. Trusted set-ups must be avoided at all costs, so there will be some significant development required in this area before implementation becomes plausible. This problem is annoying in its urgency, since the Monero blockchain is already quite large and will not slow in its space requirements until this problem (and other related problems) are solved.
7. **The Distributional Problem**: Most of the time, the true signer of a ring signature in Monero is the owner of the newest transaction in that signature. How should the distribution for mix-ins depend on transaction age? This corresponds to certain interesting approximation problems in statistics, but also certain game-theoretic questions reminiscent of [3], for example. As a matter of user privacy, the urgency of this problem is rather low, due to the one-time addresses in Monero, but this problem may have some interesting low-hanging fruit.
8. **Testing Blockchain Dynamics with Population-driven Modeling**: It may be obvious, but making different choices for different dynamical computations in a cryptocurrency leads to different dynamical systems. Testing choices of computation (for example, difficulty) for their "goodness" with respect to some desired task seems to be a wise decision. Using deterministic (as in [15]) and stochastic (as in [5], [6], [8], [7]) population models of both users and mining nodes inspired by ecology, we can develop stochastic models of block arrival rates and blockchain creation. We can parameterize these models with a miniature testnet, we can optionally couple these models with other models (such as economic models), and we can use the results to gain dynamical insight towards constructing better-behaved control systems for cryptocurrencies. Low urgency, but very low resistance to obtain results.

9. **Hardness of blockchain analysis**: We wish to establish lower bounds on complexity, cost, and hardness in finding approximate solutions to a general ring ownership problem. To this end, we construct a formal model of blockchain forensics for a ring-signature-like system using directed trees with unknown edges. This problem may be a novel puzzle. This is not particularly urgent, and will require a lot of thought.
10. **Blockchain Design**: Various proposals for different protocols and data structures to represent a ledger of transaction have been proposed, as in [14] (which is known to incentivize bad behavior) and [11]. This is also not particularly urgent and will require a lot of thought.
11. **Traceability, extending RingCT**: We wish to investigate the plausibility of modifying RingCT (or using RingCT-like approaches) to obscure block height of transactions. Any such scheme is approaching zero-knowledge and is likely to be monstrously large and implausible. This is medium urgency, because such a scheme would dramatically improve user privacy. However, the tractability of this problem is not yet clear.
12. **Future-proofing Monero**: For each cryptographic component underlying the function of Monero, in case a breakthrough in technology renders that component obsolete, we ought to have one or more components waiting in the wings for an upgrade.
13. **Post-Quantum Future-proofing Monero**: Pie in the sky. We wish to answer three questions about this. First, given all post-quantum recommendations by international communities of cryptographers, exactly how big and slow is a *transparent*, Bitcoin-like cryptocurrency going to be? Second, where are the bottlenecks? Third, how badly does increased anonymity cause bulkiness to scale in the post-quantum world? We are fairly confident that we can demonstrate the requirements for a truly post-quantum currency will be infeasible to satisfy for many years.

Certainly, this (partial!) list is quite long, even with the help of Mr. Quesnelle; expansion of the Monero Research Lab may very well become a point of concern in the future, however we can cross that bridge when we come to it.

We request members of the community contribute their opinions on this list and ideas they would like to see added. Areas of research, possible vulnerabilities to the Monero system, new cryptographic schemes, new models, and new insights are always welcome. Please do not hesitate to contact us.

The Monero Research Lab wishes to state emphatically that our concern is to report our findings on Monero, which is an open source project, as honestly and transparently as possible. Our goal is not to persuade, re-assure, or enrich speculators or investors; our goal is to assist the Monero community and the Monero Core Team in the design of a robust and strong cryptocurrency with an emphasis on user privacy. Consequently, all findings will be responsibly disclosed to the Monero community. Responsible disclosure may involve maintaining secrecy regarding security flaws for a period of time before disclosure to the public, which provides the development team time to correct known issues and protect our users. This also provides time to discreetly contact the developers of other cryptocurrencies so they, also, may protect their users.

Special Thanks: We would like to issue a special thanks to the members of the Monero community who used the GetMonero.org Forum Funding System to support the Monero Research Lab. Readers may also regard this as a statement of conflict of interest, since our funding is denominated in Monero and provided directly by members of the Monero community by the Forum Funding System.

References

1. Man Ho Au, Joseph K Liu, Willy Susilo, and Tsz Hon Yuen. Constant-size ID-based linkable and revocable-iff-linked ring signature. In *International Conference on Cryptology in India*, pages 364–378. Springer, 2006.
2. Man Ho Au, Willy Susilo, and Siu-Ming Yiu. Event-oriented k-times revocable-iff-linked group signatures. In *Australasian Conference on Information Security and Privacy*, pages 223–234. Springer, 2006.
3. T. E. Caywood and C. J. Thomas. Applications of game theory in fighter versus bomber combat. *Journal of the Operations Research Society of America*, 3, 11 1955.
4. Nishanth Chandran, Jens Groth, and Amit Sahai. Ring signatures of sub-linear size without random oracles. In *International Colloquium on Automata, Languages, and Programming*, pages 423–434. Springer, 2007.
5. Joseph L Doob. Topics in the theory of Markoff chains. *Transactions of the American Mathematical Society*, 52(1):37–64, 1942.
6. Joseph L Doob. Markoff chains–denumerable case. *Transactions of the American Mathematical Society*, 58(3):455–473, 1945.
7. Daniel T Gillespie. A general method for numerically simulating the stochastic time evolution of coupled chemical reactions. *Journal of computational physics*, 22(4):403–434, 1976.
8. Daniel T Gillespie. Exact stochastic simulation of coupled chemical reactions. *The journal of physical chemistry*, 81(25):2340–2361, 1977.
9. knaccc. Potential privacy leaks in Monero and churning. https://github.com/monero-project/monero/issues/1673#issuecomment-278509986, 2017.
10. Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. A traceability analysis of Monero's blockchain. 2017.
11. Bob McElrath. Braiding the blockchain. https://scalingbitcoin.org/hongkong2015/presentations/DAY2/2_breaking_the_chain_1_mcelrath.pdf, 2017.
12. Andrew Miller, Malte Möser, Kevin Lee, and Arvind Narayanan. An empirical analysis of linkability in the Monero blockchain. *arXiv preprint arXiv:1704.04299*, 2017.
13. Shen Noether, Adam Mackenzie, et al. Ring confidential transactions. *Ledger*, 1:1–18, 2016.
14. Yonatan Sompolinsky and Aviv Zohar. Accelerating Bitcoin's transaction processing. fast money grows on trees, not chains. *IACR Cryptology ePrint Archive*, 2013:881, 2013.
15. Steven H Strogatz. *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. Westview press, 2014.