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. 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 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. Contextual sources are included where possible together with a small justification for investigation into each topic.

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 by the end of August 2017 (journal to be determined).
2. **Correcting some problems**: In [9], 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.
3. **Recent criticisms**: Recently, critics have claimed the Monero blockchain is traceable, as in [8] and [6]. 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. **Signature Size and RingCT**: Blockchain bloat can be mitigated with efficient signatures. Some schemes, such as [4], [1], [2], exhibit sub-linear sizes of ring signature and have been investigated by MRL in the past and RingCT uses more efficient signatures than signatures in the CryptoNote reference code (as

described in [9]). 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, and a large blockchain is an obstacle to adoption. Moreover, this problem should see some results, either positive or negative, quite quickly.

5. **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.
6. **Churning, Mandatory Minimum Mix-ins**: Detailed by `knaccc` in [5], an attack is described: if a user Bob regularly receives moneroj from Alice and spends that moneroj with Charlene, information leaked from Charlene can inform Alice about the spending habits of Bob. One could say Bob was "pinned and betrayed." Churning is an adequate interim solution, so urgency is low, and the tractability of this problem is not immediately clear to me.
7. **Population-driven Modeling**: We developed some population-based models of block arrival rates and blockchain creation in the past but did not attempt to parameterize them with a miniature test-net, couple them with economic models, or use them to assess the "goodness" of a difficulty metric for the next block. All of these are possible and could provide dynamical insight towards constructing better-behaved control systems for cryptocurrencies. Low urgency, but very low resistance to obtain results.
8. **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 are constructing a formal model of blockchain forensics for a ring-signature-like system using directed trees with unknown edges. This is not particularly urgent, and will require a lot of thought.
9. **Blockchain Design**: Various proposals for different protocols and data structures to represent a ledger of transaction have been proposed, as in [10] (which is known to incentivize bad behavior) and [7]. This is also not particularly urgent and will require a lot of thought.
10. **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 clear to me.
11. **Future-proofing Cryptocurrency**: 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. Low priority, probably very hard.

12. **Future-proofing Monero, Post-Quantum edition**: 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? Low priority, probably very hard.

We are actively soliciting opinions and ideas from members of the community to add to this list. 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. Future Research Road-maps will include comments on the progress that has been made for each of the above tasks. The Monero Research Lab wishes to emphasize that we make no guarantees about results in any of the above directions.

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.

Special Thanks: I would like to issue a special thanks to the member of the Monero community who used the GetMonero.org Forum Funding System to support my work with Monero. Readers may also regard this as a statement of conflict of interest, since my salary was provided 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. knaccc. Potential privacy leaks in monero and churning. https://github.com/monero-project/monero/issues/1673#issuecomment-278509986, 2017.
6. Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. A traceability analysis of monero's blockchain. 2017.
7. Bob McElrath. Braiding the blockchain. https://scalingbitcoin.org/hongkong2015/presentations/DAY2/2_breaking_the_chain_1_mcelrath.pdf, 2017.
8. Andrew Miller, Malte Möser, Kevin Lee, and Arvind Narayanan. An empirical analysis of linkability in the monero blockchain. *arXiv preprint arXiv:1704.04299*, 2017.
9. Shen Noether, Adam Mackenzie, et al. Ring confidential transactions. *Ledger*, 1:1–18, 2016.
10. Yonatan Sompolinsky and Aviv Zohar. Accelerating bitcoin's transaction processing. fast money grows on trees, not chains. *IACR Cryptology ePrint Archive*, 2013:881, 2013.