Quarterly update

August 31, 2017
Brandon Goodell

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

This document is intended to inform the community of the work done at MRL in the past quarter, sort of as a response to the first MRL Roadmap, MRL-R001, and sort of as a newsletter to inform everyone about Monero Research Lab. We try to address the partial MRL "to-do" list of research items from the first MRL Research Bulletin, MRL-R001, and document the work that has been done both directly and indirectly toward those ends. We document which items on those lists are being de-prioritized on the next MRL Roadmap, and we introduce a few new items that came up over the past few months that will make it onto the next MRL Roadmap (which we expect to put out in the next two to three weeks).

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, subject to the restriction that we do not compromise the safety or security of the funds of our users by doing so. 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.

Now that is out of the way, here is what we did with our summer:

1 RingCT Security Proofs

We have combined this topic with the threshold signature topic (see next item). In [4], there are certain flaws in the proofs of security for MLSAG signatures that need correction, but in the construction of the threshold signature security proofs, we must first establish the security of the MLSAG signatures and then generalize to the threshold setting. Due to this, the corrected RingCT proofs are now part-and-parcel with the threshold multisignature paper.

2 Threshold multisignatures

We are fleshing out an implementation proposed by former contributor `shen` of t-of-n threshold MLSAG multisignatures in Monero. The details of this implementation have been available to the community for months, and vetting those implementations and developing security proofs has been one of the more pressing areas of work for surae, especially in the past six weeks. We currently have a partial draft of MRL Research Bulletin MRL-0006 detailing the implementation in preparation (see the MRL github for a current copy). However, this is only partial because completing this document requires novel security models against insider attacks, where an adversary may corrupt a subthreshold number of private keys. Novel security models require novel security proofs, and so we are "in the weeds" on that right now. We hoped this would be accomplished before the end of August but the novelty of the security models have taken MRL a little by surprise. A delightful, surprise, but a surprise nonetheless: the novelty of these results may lead to a peer-reviewed publication on behalf of MRL!

On a related note, surae began in June approaching the threshold multisignature scheme as a mere problem of *computing private keys jointly*, and this was a complete misunderstanding of the problem at hand, which is to *compute signatures without directly computing the private key*. Consequently, our work on this topic was initially unified with our work on the sub-address scheme described by kenshi84 and knaccc, by considering these both as problems involving revamping Monero's addressing schemes. This is also one of the reasons that MRL-R001 failed to elaborate upon the sub-address scheme. Once this mis-understanding was clarified to us (after several very educational and helpful conversations with luigi and kenshi84), MRL is once again approaching these two topics separately. We anticipate an MRL Research Bulletin on the sub-address scheme very soon after MRL-0006 describing threshold signatures is released; security proofs for the sub-address scheme are (ostensibly) remarkably easier than in the threshold case.

3 Recent criticisms

Critics have claimed the Monero blockchain is traceable, as in [3] and [2]; these papers make use of the *distributional problem* mentioned in the first roadmap together with a few other routes of analysis. Some of the concerns and claims made in these papers are irrelevant because they only apply to pre-RingCT Monero outputs. Some of the concerns are relevant and related to the so-called EABE attack (see next item).

4 Churning, EABE Attack, Large Rings

Detailed by knaccc in [1], the EABE (Eve-Alice-Bob-Eve) attack is described. A merchant, Bob, and his customer, Alice, use an exchange, Eve, to convert cryptocurrency to fiat and back again. If Eve sends some moneroj to Alice, who uses it to purchase items from the merchant Bob several times, and 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 purchasing habits of Alice. This problem is exacerbated if Eve is a know-your-customer exchange. Urgency on this problem is higher than our original estimation: most merchants who accept cryptocurrency enact this behavior, most users do not churn to avoid this problem, and moreover churning transactions can leave a statistical signal (in the sense of the Miller and Kumar criticisms) that is quite undesirable.

This work dovetailed nicely with our road map item **hardness of blockchain analysis**. In the study of this (as well as the Miller and Kumar criticisms), `surae` established three separate probabilistic models of transaction output ownership in a ring signature setting in analyzing this problem. None of these models will see publication soon, however, because each one, a refinement of the previous, is insufficient to describe the problem at hand. We do, however, anticipate some explanatory details to be made public over the coming months. MRL has been reluctant to provide more details, as we stated very clearly in our first MRL Roadmap, *we will not comment thoroughly on these criticisms until our review is complete for security reasons.* We will take as much time as necessary for this, and we recognize that issues such as this one are urgent.

In the current CryptoNote framework, an elegant solution would be to simply increase ring sizes dramatically. This seems impractical, however, unless ring signatures can be made small (perhaps sub-linearly sized with respect to the number of ring members) which leads us to the next item.

5 Signature Size and RingCT

Blockchain bloat can be mitigated with efficient signatures. MRL was made aware of research by two separate international teams of researchers (see Section 10) making progress on compact Ring Confidental Transactions. One scheme (put forth by Sun, Au, Liu, and Yuen) is very efficient and fast but requires a trusted set-up. Another scheme (put forth by Ruffing, Thyagarajan, Ronge, and Schröder, or RTRS) does not use a trusted set-up, but experiences a trade-off since the computation and verification times are quite beastly. An RTRS RingCT may contain thousands of ring members and take up the space of a classic RingCT signature with only a few dozen ring members, but the RTRS RingCT could take hours, days, or more to compute. We believe verification time may be optimized to an extent, but it is also quite slow. Currently, `knaccc` is working with `surae` and `sarang` on a Java prototype of the implementation for testing purposes, and discussions with `smooth`, `moneromooo`, and `luigi` on the practicalities of implementation are constant. MRL anticipates that the scheme may be made sufficiently stream-lined to include in Monero for a moderate increase ring size that was previously unreasonable, but not the epic increase initially hoped for.

6 Zero-knowledge Lit Review

We began communication with Jeffrey Quesnelle, a computer science graduate student at the University of Michigan at Dearborn, at the start of this quarter. Jeffrey wrote an extremely helpful and detailed literature review on zero-knowledge schemes with an eye toward ZK-SNARKS. We listed this zero-knowledge literature review first in MRL-R001 because it was rather low-hanging fruit... but it also did not present a high priority compared to practical implementation issues (threshold signatures, sub-addresses) or security issues (the EABE attack, see below). Our original date for pushing this out was the end of August 2017, which has come and gone. To be clear, this work has not come to a stop, it is merely delayed; now that `sarang` has joined MRL, `surae` has more time to put into finishing this project. MRL anticipates movement on this document before the end of September (in fact, the first week of September).

7 Future-proofing Monero

Unlike the above topics, this is actually a constant "in-the-background" thing to keep in mind. For example, when we use Pedersen commitments, we have certain hiding and binding properties, but when we use El Gamal commitments, which are similar, these properties change and the commitments are no longer sufficiently hiding against adversaries with quantum computing. Making decisions such as these throughout algorithm design is a constant issue to be considered. Consequently, this item will be removed from future MRL road maps, as it is more of a design philosophy.

8 New stuff

We have put effort into projects not initially on the MRL Roadmap either due to merit of those projects or urgency. Something related to these items will each make it onto the next MRL Roadmap.

i. **Viewkey solutions**. Since the CryptoNote framework is not *unlinkable* in the sense of the original CryptoNote whitepaper, an adversary can infer much information about whether a certain address has received transactions without knowing the associated viewkey (as in the EABE scenario). Moreover, viewkeys lack functionality. For example, users may desire revocable viewkeys, or viewkeys only valid for certain periods of time, or may desire viewkeys that grant visibility to outgoing transactions (which should also be revocable). Discussions on viewkey solutions have begun between contributors `endogenic`, `knaccc`, `moneromooo`, `surae`, and `fluffypony`.

ii. **Zidechains**. Even with very large ring sizes, since the CryptoNote framework is not zero-knowledge, information is leaked with each transaction by definition. One method proposed by `fluffypony` to mitigate this is to construct a zero-knowledge sidechain to peg to the Monero blockchain which we are tentatively calling *zidechains*.

iii. **Blacklisting provably spent outputs**. Wallet software should avoid including provably-spent outputs in ring signatures if possible, because doing so reduces the relative signer ambiguity of the signature, degrades Monero's claims toward untraceability, and degrades the fungibility of all other Monero outputs. Recently, `fluffypony` had a conversation with `gmaxwell` on maintaining curated blacklists of provably spent outputs, and `surae` has begun work on algorithms for finding provably-spent transaction outputs.

9 Dead Items

Recall that the items deeper on the MRL Roadmap were items of lower priority. We did not have an opportunity to make progress on the following issues, all of which are very long-term, in terms of priority. These items are worthwhile side hustles for future research, but do not have a lot of immediate pay-off.

i. **Testing Blockchain Dynamics with Population-driven Modeling.**

ii. **Blockchain Design**.

iii. **Traceability, extending RingCT to obscure transaction time.**

10 Academic Engagement

In the past three months, Monero Research Lab has had some great interaction with the broader academic community, briefly mentioned above. We wish to highlight the following, which is big news!

(i) Shi-Feng Sun at Hong Kong Polytechnic University, Man Ho Au at Shanghai Jiao Tong University, Joseph K Liu at Monash University, and Tsz Hon Yuen at Huawei Technologies wrote "RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero," a paper proposing a much more efficient and speedy implementation of Ring Confidential Transactions. These researchers have been instrumental in ID-based cryptography and ring signatures, so their contribution directly to Monero, literally mentioning us in their paper title was surprising, exciting, and a huge honor!

(ii) Nearly at the same time, Tim Ruffing at Saarlang University together with Sri Aravinda Thyagarajan, Viktoria Ronge, and Dominique Schröder at Friedrich-Alexander-Universität contacted us directly with a separate Ring Confidental Transaction scheme, with a very different Ring Confidential Transaction scheme (see below). We have had a few conversations with him about implementation choices; thanks to hard work by `knaccc` and `surae`, we have a nearly-working prototype (to Ruffing's surprise! `knaccc` works quick).

(iii) In implementing the Ruffing scheme, Monero Research Lab has also been in contact with Jonathan Bootle at University College in London about a set-up presented in one of his papers used in the Ruffing scheme; not only are we the first (to his knowledge) to implement his set-ups, but we also identified a small mistake in the notation of his paper that will be corrected.

(iv) Thanks to community donations to the Forum Funding System, hired Sarang Noether! He recently graduated with his Ph.D. in Computational Physics (and has a strong background in pure and applied mathematics, computer science, and network security) and was a contributor to MRL several years back. We are already enjoying his contribution to our work. We are extremely grateful that the community has welcomed him; he was facing several competitive offers for some very interesting and varied jobs in a few different engineering sectors, so we are lucky to have sniped him away from the traditional economy!

11 Conclusion

We request members of the community contribute their opinions on our above work and ideas they would like to see added. Please do not hesitate to contact us. We will make the current threshold MRL Bulletin (which will be MRL-0006) available on the MRL github upon publication of this quarterly update so that contributors and community members can monitor our progress on that front.

In the next four weeks, we anticipate MRL-R002 roadmap to be put out, the second draft of the zero-knowledge literature review with Jeffrey Quesnelle to be made available to the community, and MRL-0006 to be completed and put out (unless the novelty of the security proofs becomes a rabbit hole of uknown depth). We also anticipate that the RTRS Ring Confidential Transaction scheme to be finished prototyping and beginning testing very soon. Once MRL-0006 is finished, we will begin an MRL Research Bulletin describing the sub-address scheme invented by kenshi84 and knaccc to be fleshed out (MRL-0007).

12 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. knaccc. Potential privacy leaks in Monero and churning. https://github.com/monero-project/monero/issues/1673#issuecomment-278509986, 2017.
2. Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. A traceability analysis of Monero's blockchain. 2017.
3. Andrew Miller, Malte Möser, Kevin Lee, and Arvind Narayanan. An empirical analysis of linkability in the Monero blockchain. *arXiv preprint arXiv:1704.04299*, 2017.
4. Shen Noether, Adam Mackenzie, et al. Ring confidential transactions. *Ledger*, 1:1–18, 2016.