RESEARCH ROAD-MAP MRL-R002

Priorities for Monero Research Lab

September 18, 2017

Brandon Goodell* and Sarang Noether

*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.

This bulletin serves as an update to the Monero community about the recent work, current priorities, and intended future work of the Monero Research Lab (MRL) team. A particular focus of this bulletin is also providing general history and information for the community about the particular types of research problems that are the foci of the Lab, especially since many projects are related. For each topic, we indicate a non-binding but reasonable time line for completion. At the end, we reserve discussion for items that were on the first road map that require reconsideration.

1 A few brief announcements...

On a personnel note, the Lab is pleased to announce that Sarang Noether joined the team as a full-time researcher under a Forum Funding System proposal. Many thanks to the generous supporters who funded his work for the next few months.

Coming soon! Monero Research Labs is scheduling bi-monthly *research meetings* to alternate with bi-monthly *office hours* on freenode. At research meetings, contributors can describe their progress, challenges, and bring questions up about their projects. At office hours, any member of the Monero community can come on down and ask any questions they like. Right now we are considering every Monday at 17:00-18:00 UTC, pending feedback from the community, to alternate between research meetings and office hours. Official times and dates will be posted soon.

On another note, Monero Research Lab would also like to thank contributor `knaccc` for volunteering his time for three straight weeks to get RTRS RingCT off the ground. Thanks to his efforts, we now have a Ring Confidential Transaction scheme with sub-linear space complexity in the number of signers! This is extremely great news, and `knaccc` deserves a pat on the back.

2 Signature sizes and confidential transactions

2.1 Summary:

We have completed an implementation of a sub-linearly-sized Ring Confidential Transaction scheme (RTRS Ring CT) with operational Java code and slightly-out-

of-date pseudo-code at https://github.com/monero-project/research-lab. We are investigating the security models, the consequences of implementation, and the possibility of extending the scheme to a Schnorr-like threshold multisignature scheme. In the process of verifying the security of the new Ring CT scheme, we are correcting old proofs for the current MLSAG Ring CT scheme.

2.2 Timing and Urgency:

This project is of moderate urgency. We anticipate a significantly greater understanding of the ramifications of implementing RTRS Ring CT by the end of October 2017 and we anticipate our recommendations for or against implementation in the Spring 2018 hard fork before the end of November 2017. If a Schnorr-like generalization toward threshold multisignatures is possible, we anticipate an MRL Research Bulletin on the matter before the Spring 2018 hard fork.

2.3 History and Details:

The size of signatures has been an ongoing subject of intense discussion, growing concern, and research for the MRL team. Blockchain bloat is directly affected by the size of ring signatures, and research toward traceability analyses for CryptoNote has demonstrated that larger ring sizes improve resistance to traceability. However, it is critical that increased ring sizes not be tied to excessive blockchain bloat. Additionally, any signature scheme that permits large rings should also ensure efficient verification times. Hence there are two (often competing) factors: signature size and verification time.

The current Monero protocol uses multi-layered linkable spontaneous anonymous group signatures (MLSAGs), described in [6], to implement a ring signature version of Confidential Transactions first proposed by Greg Maxwell. We call this scheme the MLSAG Ring CT scheme. In the MLSAG Ring CT scheme, transaction amounts (with multiple inputs and outputs) are replaced by commitments to those amounts. This approach masks both the spender and the amounts, while still allowing any party to verify that the transaction balances without double spending. The set-up increases privacy of Monero (compared to the reference CryptoNote protocol which did not mask transaction amounts), but comes equipped with drawbacks. First, the presented security proofs contains flaws, and second, the size of the signatures increases linearly with the size of the ring: doubling ring sizes leads to doubling the weight of the blockchain. We are informally confident that the security definitions are satisfied despite the incorrect proofs and are working to correct the old proofs. Additionally, we are constantly seeking more efficient schemes.

A paper was shared with MRL by Tim Ruffing, Sri Aravinda Thyagarajan, Viktoria Ronge, and Dominique Schröder, (Ruffing et. al., personal communication, August 2017) proposing a novel construction of Ring CT together with new security definitions. The proposal modifies previous work on ring signatures by Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit [2]. We are formally calling this scheme the RTRS Ring CT.

Space complexity for RTRS Ring CT is logarithmic in the size of the ring, so the limiting factor in large ring sizes has shifted to verification time, which is linear in the ring size. One of the authors, Tim Ruffing, also posted a proof that the verification

time for any secure ring signature scheme is linear in the ring size. The RTRS Ring CT scheme uses keys that are twice as large as the MLSAG scheme, resulting in (asymptotically) twice the verification time as the MLSAG scheme. In this sense, the MLSAG Ring CT protocol is as fast as we can reasonably expect verification to proceed, in terms of number of operations. The only remaining possible optimization therefore would involve changing elliptic curves, using different implementations of elliptic curve arithmetic, using specialized hardware specifically for signature verification, or implementing amortization by re-using rings. The RTRS scheme doubles verification time complexity in exchange for logarithmic space complexity.

The development of the prototype in Java (which went under the super-top-secret tongue-in-cheek title RuffCT) was done by `knaccc` with the assistance of `surae` and `sarang`. Each of these contributors were instrumental. The Lab has verified that RuffCT does, in fact, produce and verify signatures as claimed and we have produced a working implementation in Java (available at https://github.com/monero-project/research-lab).

We have moved onto investigating the presented security models and proofs, and investigating the ramifications of implementing RTRS Ring CT into Monero: how large can we make our rings and still keep our transaction verification time on the order of a few seconds? Associated ongoing projects include: (i) the proper inclusion of fees in an RTRS Ring CT in a secure manner, (ii) the process of converting to the new addressing system, (iii) threshold multisignature versions of the RTRS Ring CT, and (iv) various methods to improve average verification time (constrained by the theoretical minima previously described). This topic is considered to be of moderate priority. We expect a more complete understanding of the differences between MLSAG and RTRS Ring CT by the end of October 2017.

3 Threshold multisignatures

3.1 Summary:

We are in the midst of completing our analysis of the Schnorr-like threshold multisignature implementation of MLSAG Ring CT as described in [6] and our comparison to the code produced by contributor `luigi`. Demonstrating security requires appropriate (novel) security models and definitions. In the process of constructing security proofs (and overlapping with our work on RTRS Ring CT above), we are correcting old proofs for the current MLSAG Ring CT scheme as we go.

3.2 Timing and Urgency:

This project is of high urgency, as the scheme is already implemented and would provide additional security features to users immediately. The novelty of our security schemes delayed our previous estimate as completing this by the end of August 2017. We anticipate an MRL Research Bulletin describing the scheme and presenting security proofs by the end of November 2017 at the latest.

3.3 History and Details:

In [6], Shen Noether proposed a t-of-N threshold multisignature approach for MLSAG ring signatures where the number of participants in the signature generation is not discernible from the signature. We are currently investigating security models

for such signature schemes, in particular for N-of-N and $(N-1)$-of-N cases, for multi-factor authentication purposes. Good security models for ring signatures are tough to come by, and we believe that we must incorporate novel definitions in the analysis. In particular, we are currently looking into expanding the definitions presented in [1] to account for threshold multisignature schemes.

In particular, attacks involving a corruption of a sub-threshold number of keys by an attacker must be considered. The goal is to ensure that given an adversary with the ability to corrupt honest user key pairs as well as the ability to maliciously generate their own key pairs, even if they generate or corrupt up to $(t-1)$ keys by an attacker, the security of our t-of-N threshold multisignature is not reduced. This is akin to the security guaranteed by a classical Shamir secret-sharing scheme [8], where an attacker must control a "critical mass" of keys before gaining any secret information from honest participants.

In order to ensure correct security proofs of the threshold scheme, work is also underway to complete proofs of security for the original N-of-N MLSAG multisignature scheme. Errors must be addressed for a proper extension to the threshold model. We consider this topic to be of high priority and intend that the scheme is demonstrated to be sufficiently secure for live implementation in wallet software before the end of November 2017.

4 Sub-addresses

4.1 Summary:

We are in the midst of completing our analysis of the sub-address scheme first described by contributors `knaccc` and `kenshi84`. This scheme allows for a single "master" key pair to generate a family of Monero addresses, all of which share a common view key. We are taking care to verify that the security of either the MLSAG Ring CT or the RTRS Ring CT schemes are not compromised using these schemes.

4.2 Timing and Urgency:

This project is of high urgency, as the scheme is mostly implemented and would provide additional convenience features to users immediately. The Lab has begun a more complete review of the proposal. We expect an MRL Research Bulletin detailing the sub-address scheme by the end of November 2017, with inclusions of the necessary proofs to show that the scheme is at least as secure as previous implementations. The goal is to release both the sub-address and threshold multisignature papers at or around the same time.

4.3 History and Details:

A sub-address scheme addresses solves the problem of address reuse. In such a scheme, a user maintains a "master" key pair from which she generates new addresses as needed. Unlike an approach where the user simply generates independent key pairs, sub-addresses should not require that the user verify every incoming transaction with each of her view keys. Instead, the construction of sub-addresses should permit single transaction verification and hence not scale poorly. With such

an approach, a user can publish as many addresses as she wishes and be assured that a third party cannot link the addresses.

A implementation proposal has been submitted (by researchers `kenshi84` and `knaccc`) that claims compatibility with existing key structure and multiple outputs, solving initial concerns about issuing change. The Lab has begun a more complete review of the proposal. Any Ring CT scheme using these sub-addresses should enjoy at least the same security properties as the address scheme in the CryptoNote standards.

The proof that the sub-addressing scheme as currently described does not degrade security is very close to trivial. Unfortunately, the triviality is not so simple that we may leave the proof to the reader, so we are presenting the formal security definitions and proof in our write-up. We expect a white paper detailing the sub-address scheme by the end of November 2017, with inclusions of the necessary proofs to show that the scheme is at least as secure as previous implementations.

5 Range proofs

5.1 Summary:

Work on range proofs is going in two simultaneous directions: compact, fast-to-verify proofs, and utilizing the space complexity of range proofs for storing cipher texts.

5.2 Timing and Urgency:

This project is of medium urgency; the increased utility of the Monero blockchain is balanced by other issues with greater urgency regarding security. We anticipate a review of different implementations of range proofs and a sketch of an encrypt-then-authenticate scheme utilizing range proofs by Spring 2018.

5.3 History and Details:

An essential component to confidential transactions is a range proof. A naive confidential transaction scheme might only ensure that transaction amounts balance, but this introduces the possibility of attacks using negative values or modular wrapping. A range proof offers assurances that each input is in a numerical range appropriate for the transaction, while not compromising the confidentiality of the amounts involved. Unfortunately, range proofs are larger than is preferable in both space and verification-time complexity. Rather than perceiving this as a drawback (or rather, as a waste of space on the blockchain), utilizing this extra space to store cipher texts has been suggested; together with a strongly unforgeable ring signature scheme, this would qualify as an encrypt-then-authenticate scheme (satisfying the gold standard of security models). Hence, we have two directions that do not directly conflict: improve the space and time efficiency of range proofs or use the large space complexity to add utility to the blockchain as more than a ledger.

The matter is somewhat complicated because ring signatures are a fundamental component to the working of our current range proof implementations. Hence, any progress on ring signatures has consequences for range proofs. Work is ongoing to produce range proof constructions that are both efficient and secure; for example `luigi` is working on implementing a change of base that should improve

space complexity, and both `sarang` and `surae` are constantly on the lookout for new schemes. The recent introduction of the RTRS Ring CT test implementation (discussed above) brought with it new proofs involving commitments that may be applicable to range proofs. This reduces the space available for encryption and increases verification time. Improving the space and verification-time complexity of range proofs now faces similar trade-offs as those described in Section 2, and so any optimization made in that area (as in choice of elliptic curve or more efficient elliptic curve arithmetic implementation) will also improve this area.

Currently, the Lab is under the impression that we should be rather satisfied by large but fast-to-verify range proofs together with small but slow-to-verify Ring CT schemes (i.e. the Borromean ring signatures from the original MLSAG Ring CT description acting as range proofs, and the RTRS Ring CT acting as ring signatures).

6 Blockchain Pruning and Generalizations

6.1 Summary:

We are currently investigating methods of blockchain pruning and generalizations of blockchain-like data structures that may lead to different properties.

6.2 Timing and Urgency:

This project is of moderate urgency; the increased utility of the Monero blockchain is balanced by other issues with greater urgency regarding security, and we are not anticipating immediate progress.

6.3 History and Details:

We are investigating the abstract data structure of a blockchain. Some of this includes different methods of forming blockchains, and some of this includes blockchain pruning. Pruning of the blockchain is deeply connected to minimizing the information necessary to protect against double-spends and malicious blockchain rewrites.

In terms of pruning, we hope to implement blockchain pruning to reduce the amount of information needed in the blockchain. It is of critical importance that any method of pruning the blockchain only negligibly degrades protection against double spends and only negligibly influences an adversary's advantage in traceability analyses. To be precise, we seek a data structure asymptotically smaller than the Monero blockchain, such that an adversary in control of a fixed proportion p of network nodes can successfully execute a double-spend attack with a probability of success at most $f(p)$ where f is some function that is negligible in some security parameter.

A naive implementation of such a rule, for example, would be to discard any blocks from more than 10 years in the past. In this scenario, any double-spend attack might require referencing invalid transactions from more than 10 years ago and, unless an adversary has control over a high proportion of the network for most of those 10 years, other miners would have probably discovered the invalid transactions some time in the previous decade. You'll notice these previous two sentences are filled with hedging words "naive," "might," "high proportion," "most," and "probably." The

point is we have not yet finished formalizing these notions, and yet all these notions can be quantified and made precise yielding straightforward analysis. Although all of the above seems reasonable, the math is going to determine exactly whether this decision

These issues were high priority in the last road map. These are being downgraded to a lower priority since, with access to RTRS Ring CT, the limiting factor in the efficiency of the Monero blockchain is time, not space. Our primary concern for any blockchain pruning method or any alternative implementation of the blockchain is, therefore, to improve verification time (especially for new nodes catching up to the tip).

7 Monero Traceability Analyses

7.1 Summary:

We are currently investigating previous criticisms of Monero's traceability, as in [5] and [4], and the attack detailed by `knaccc` where an AML/KYC exchange knows ownership information of some of their customer's one-time addresses and can use this to determine the flow of money between their customers.

7.2 Timing and Urgency:

This project is of high urgency due to concern in the community, but we are not self-imposing a deadline on our analysis. Our assessment of these security concerns will be made available when we are confident in the correctness of our analysis.

7.3 History and Details:

For any two incoming transactions, if all possible senders are equiprobable then we say that set-up is *untraceable*. It is known that Monero is not strictly untraceable, which was a result we exploited when investigating chain reactions in [7], and is exploited in [5] and [4]. The claims in each of these documents were made before MLSAG Ring CT was implemented; as of the most recent hard fork, MLSAG Ring CT signatures are now required for all Monero transactions and many of the routes of degrading Monero's untraceability presented are no longer relevant. Although the specific criticisms presented in these papers are (mostly) no longer directly relevant to Monero in particular, they present interesting heuristics and approaches that MRL finds sufficiently important to study in some detail.

To ease concerns in the community, we first show how Monero may be regarded as traceable, and then we explain some of the mitigating properties that the protocol enjoys. To see how Monero may be regarded as traceable, consider the first case: a transaction appears whose ring T has transaction output public keys $T = \{T_1, T_2\}$ where the key T_1 appears in N_1 other ring signatures elsewhere on the blockchain and T_2 appears in N_2 other ring signatures. If $N_1 = 1$ and $N_2 = 10^5$, the *a priori* likelihood that T_1 has been spent is much lower than the likelihood that T_2 has been spent. After all, T_2 has had $10,000$ different possible outgoing transactions reference it, but T_1 has only had one. Hence, if we receive a transaction with ring T, without any additional information, we can be reasonably sure that T_1 and T_2 are not equiprobable as possible senders of the transaction. Consider the second case: if two transactions both have ring signatures with the same ring $T = \{T_1, T_2\}$,

it is impossible that both T_1 and T_2 remain unspent, allowing an adversary to be able to determine spent transactions.

Nevertheless, these examples also demonstrate the inherent problem with these approaches, especially when the mitigating properties of Monero are taken into account. The use of one-time addresses ensures that the *sensitivity and specificity* of these tests are not both directly estimable (direct estimation would require unmasking the one-time addresses). Sensitivity and specificity are both critically important to assessing the goodness of any test. To see the relevance of this in the first case, note that we can *estimate* the differences in likelihood that T_1 or T_2 has been spent, but we cannot be sure and we have no reasonable way of measuring the goodness of our estimate. If a malicious user wishes to frame an innocent user in an illegal transaction, they could simply use one of their own transaction outputs that has appeared in many rings to perform an illegal transaction filled with ostensibly innocent public keys. Hence, in isolation, such analyses are unsuitable for establishing anything except circumstantial association between addresses, although they can be leveraged together to provide rather interesting analyses.

Note that the use of ring signatures also brings a combinatorial explosion to the problem of analyzing traceability, and this is exacerbated as ring sizes improve. Due to this, in the second case, although we can tell that both T_1 and T_2 have been spent, we cannot determine, for example, which was spent first. This provides two possible states (T_1 was spent first or not). In this case, we have two outputs, so we have two possibilities; if minimum ring sizes are N, then we end up with N possibilities, and repeated transactions leads to an N-ary tree of possibilities. To establish the chain of ownership of M transactions long would therefore require exploration of a space of N^M possibilities. The above approaches would allow us to assign a priori likelihoods to each of these possibilities, but it is clear that a large chain of transactions (say 86 or more transactions) with large ring sizes (say 10) will lead to more possibilities than there are fundamental particles in the universe.

We here at the Lab previously thought that one possible solution to `knaccc`'s described attack would be *churning*, where one sends funds to oneself multiple times before using at a merchant. Unfortunately, this leads to chains of self-referential transactions, which leave an undesirable and identifiable statistical signal. Investigating and improving the untraceability in Monero is a high urgency but never-ending problem. We have reason to believe that the hardness of analyzing the Monero blockchain currently is sufficient to protect user security in the short-term, especially if we implement larger ring sizes using RTRS Ring CT.

8 Federated ZK-Side Chains

8.1 Summary:

We at the lab are looking into temporally-restricted federated side chains running ZK-SNARK technology to improve the traceability issues described above.

8.2 Timing and Urgency:

This project is of unknown urgency and has been presented to us by `fluffypony` only recently. If traceability analyses seem to improve, the urgency will become quite high.

8.3 History and Details:

Zero knowledge succinct non-interactive arguments of knowledge (ZK-SNARKs) use a trusted set-up to ensure proof against double-spend attacks. Monero does not require a trusted set-up to ensure against double-spend attacks, but suffers some traceability criticisms made as in [5] and [4]. One possible solution is to run side chains utilizing zk-snark technology with finite lifespans; funds would be "deposited" from the Monero blockchain to the zero-knowledge side chain (zidechain), transactions on the zidechain would proceed in zero-knowledge, and then users can "withdraw" from the zidechain back to the main Monero blockchain before the zidechain self destructs. Double spend protection in Monero would provide users confidence that any trusted set-up used in the construction of the zidechain would not allow for double spends making it back onto the Monero blockchain *without detection*; if any double-spends are detected, the zidechain can be terminated early and begun again.

Some questions have been raised about the feasibility of zero knowledge succinct transparent non-interactive arguments of knowledge (ZK-STARKSs). While such constructions remove the requirement for a trusted set-up, they are currently not available in a usable and well-reviewed form. However, once rigorously-tested ZK-STARK technologies become more generally accessible, the Lab would investigate a transition from temporary ZK-SNARK zidechains toward more permanent ZK-STARK constructions.

9 New Cryptoschemes

9.1 Summary:

The Lab is constantly on the lookout for new cryptoschemes that may be useful in the Monero protocol.

9.2 Timing and Urgency:

This project is of low to moderate urgency, but is a constant area of research with no particular goal in mind.

9.3 History and Details:

Before RTRS Ring CT and before Ruffing's linearity proof, the primary focus of this area was to find more efficient signatures; this is an ongoing area of research (rather than a to-do-list item) that *produces new areas of research*. Every element of the Monero protocol must be considered for possible replacement in the event that various cryptoschemes are broken or if new security models are made available.

10 Long-term ASIC Proofing

10.1 Summary:

The Lab is composing a plan of action in the case that devices are manufactured that are many orders of magnitude more power-efficient at executing proof of work with our current cryptographic hash function, CryptoNight, than current computers. Our plan includes investigating alternative problems that may be helpful for a Nakamoto Proof of Work model of blockchain write access, and includes looking into variations on the Nakamoto Proof of Work model.

10.2 Timing and Urgency:
Like many other projects, this one is low to moderate urgency. We plan on having a sketch of an ASIC-proofing plan for Monero by the end of Spring 2018.

10.3 History and Details:
One of the unspoken elements of the CryptoNote white paper was a dedication to a social contract of decentralized currency. To this end, the CryptoNote creators manufactured their own memory-hard cryptographic hash function for use in Proof-of-Work; due to the access of this hash function to the L3 cache, modern computer architecture ensures that making CryptoNight ASICs will be difficult for at least several more years. However, contingency plans are great to have.

The Lab is currently investigating other memory-hard problems not involving cryptographic hash functions that would be suitable for Proof of Work; we have our eye on problems that provide some utility to global economies or scientific pursuits, so that the Monero blockchain becomes not only a record of transactions but a record of solutions to difficult-to-solve problems. We are also investigating alternatives to proof of work itself, such as Proof of Storage.

11 Technical Papers
11.1 Summary:
The Lab has several technical papers in preparation, some for peer review, some for internal usage at Monero, and some intended as white papers to be made public.

11.2 Timing and Urgency:
Varies by paper.

11.3 Details:
In addition to the items above, the following upcoming technical papers are also in the works:

(i) **Updating the CryptoNote Standards**: While the Monero code is (now) well-documented, the protocol has moved above and beyond the original CryptoNote 2.0 white paper. Especially with the advent of Ring CT, sub-addresses, and threshold multisignatures, and with the possibility of implementing RTRS Ring CT in the coming months, the need for a complete, accurate technical document is becoming quite clear. Moreover, we wish to include certain technical standards in future implementations that we should codify sooner rather than later. As a low-level urgency project, we will be writing a new white paper (or a sequence of them) describing the current Monero protocol in detail for completion by late spring or middle summer 2018.

(ii) **Zero-knowledge Lit Review**: This document is still in progress. 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. He wrote a literature review of zero knowledge schemes and their application in cryptocurrencies, for submission for peer review (journal to be determined). We initially expected this to be done by the end of August 2017, but there have been delays. We will make available a

pre-print on ArXiV after a few revisions. Currently, this is one of the two top priorities for `surae` and he hopes to have a draft ready for submission before the end of September 2017.

(iii) **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. This item is identical to the previous road map and we do not anticipate significant progress on this before Spring 2018.

12 Back burner

In MRL-R001, we were ambitious and listed many projects that we anticipated movement on and thought could be fun. Unfortunately, many of these have seen no movement, because they are of low urgency. These include **testing blockchain dynamics with population-driven modeling** and **hardness of blockchain analysis** (see above about combinatorial explosions). Many late undergraduate math and computer science students may be able to assist us with these. Interested contributors with (i) experience in coding and differential equations or (ii) experience in numerical analysis can contact Monero Research Lab at `sarang.noether@protonmail.com` in the interest of collaboration.

In MRL-R0001, we also included the idea of future-proofing Monero, which is more of a design philosophy when approaching new schemes rather than a specific active area of research. Consequently, we are removing this as a specific item on the list and incorporating this as an attitude in our design philosophy.

Conclusion

As always, the MRL team strives to provide thorough research to the community, balancing cutting-edge research with user trust, community transparency, and security of funds. The team thanks the Monero community for its support and guidance, and looks forward to continuing its mission with precision and passion. Monero remains the strongest, most innovative, and sexiest coin we know, and the Lab is proud to support its future.

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 *eventually* 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.

Some members of the Lab are supported financially by the community through the Forum Funding System and are paid in Monero for their work. Readers may view this as a conflict of interest. However, researchers are not paid for particular projects or implementations of proposals, offering some separation from direct outside influence.

References

1. Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In *TCC*, volume 6, pages 60–79. Springer, 2006.
2. Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit. Short accountable ring signatures based on ddh. In *European Symposium on Research in Computer Security*, pages 243–265. Springer, 2015.
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. Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. A traceability analysis of Monero's blockchain. 2017.
5. Andrew Miller, Malte Möser, Kevin Lee, and Arvind Narayanan. An empirical analysis of linkability in the Monero blockchain. *arXiv preprint arXiv:1704.04299*, 2017.
6. Shen Noether, Adam Mackenzie, et al. Ring confidential transactions. *Ledger*, 1:1–18, 2016.
7. Surae Noether and Adam Mackenzie. A note on chain reactions in traceability in cryptonote 2.0. *Technical report*, 2014.
8. Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.