# CLSAG Audit Results

Contributing researchers to the [Monero Research Lab](https://web.getmonero.org/resources/research-lab/) and the Monero Audit Workgroup are pleased to announce the results of a recent audit of the [CLSAG](https://eprint.iacr.org/2019/654) ring signature construction. As described in this post, CLSAG enables smaller and faster transactions with rigorous security. Users can expect to see these benefits seamlessly integrated into Monero software at the next network upgrade, which will occur later this year.

The complete audit report by Jean-Philippe Aumasson and Antony Vennard is available.

## What is CLSAG?

Monero uses a signer-ambiguous transaction protocol that includes many cryptographic components. One of these is a ring signature construction called [MLSAG](https://getmonero.org/resources/research-lab/pubs/MRL-0005.pdf). When you generate a transaction, one or more MLSAG signatures are generated to obfuscate the signers and amounts in the transaction.

Monero Research Lab contributing researchers developed CLSAG as a drop-in replacement to MLSAG to improve efficiency. Using some simple but clever mathematics, CLSAG signatures achieve the same functionality as MLSAG signatures, but at a much smaller size. And thanks to some optimizations of the underlying cryptographic plumbing, Monero software can verify CLSAG signatures more quickly.

Security is also improved. Good cryptographic constructions are built with a formal security model in mind. Security models are a way of formalizing the capabilities of hypothetical attackers, and then rigorously proving that such attackers cannot break particular security properties. In the case of CLSAG, for example, the imaginary attacker is given the ability to corrupt honest users to obtain their keys, and to convince honest users to generate specific transactions. CLSAG holds up to a much more robust security model than was originally used for MLSAG, and it provides strong confidence in the practical security of CLSAG.

Compared to the current ring signature construction used in the Monero protocol, CLSAG signatures are smaller and faster than before, with rigorous security.

## What does this mean?

A network upgrade will take place later this year, and will deploy CLSAG signatures as a mandatory consensus requirement. Provided you keep your software updated, you'll start using CLSAG signatures once the upgrade takes place. It will be a seamless change.

The size of Monero transactions depends on the number of previous transaction outputs you spend, and the number of new transaction outputs you generate. Most transactions spend at most two previous outputs and generate two new outputs; these transactions currently take up around 2.5 kB of space on the blockchain. With CLSAG, the same transaction takes only 1.9 kB of space, a 25% improvement!

Whenever your Monero software sees new transactions, it must verify their signatures to ensure the transactions are valid (else someone could spend money they don’t have). This is very fast (usually a few tens of milliseconds), but it becomes appreciable when a new installation needs to check the entire blockchain. While the exact verification times depend on how fast your computer or device is, tests suggest that most users will see a XX% improvement!

## Security audit

Because ring signatures are a critical component of the Monero protocol, the Monero community commissioned a formal security audit of both the CLSAG cryptography (algorithms, security model, and proofs) and the implementation code that will be deployed. The audit was conducted by expert cryptographers [JP Aumasson](https://aumasson.jp/) and [Antony Vennard](https://diagprov.ch/), funded by [community donations](https://ccs.getmonero.org/proposals/clsag-audit-take2.html), and conducted with coordination support from the Monero Audit Workgroup and the nonprofit [Open Source Technology Improvement Fund](https://ostif.org/). The review process took place in two stages.

In the first stage, the reviewers carefully examined the security of CLSAG as described in its preprint. They concluded that the security model is suitable for the intended use case, and that the algorithms used in the construction are secure. The auditors recommended significant changes to two of the security proofs, which were completed to their satisfaction. They also made several other non-security recommendations to improve the preprint. Updates are included in the current version. None of these updates required changes to the implementation code.

In the second stage, the reviewers examined the security of the [implementation code](https://github.com/SarangNoether/monero/tree/clsag-device). They concluded that the implementation was secure and well written, and that it is a correct implementation of the CLSAG algorithms. The reviewers made some informational suggestions to simplify the code, but they found no security issues.

This audit provides additional confidence that migrating the Monero protocol from MLSAG signatures to CLSAG signatures can be done safely and securely. Once deployed, users will see more efficient transactions with the same functionality.

We would like to thank the Monero community again for supporting this project.