Counter Galois Onion (CGO): Fast Non-Malleable Onion Encryption for Tor

Jean Paul Degabriele

Abstract: In 2012 the Tor project expressed the need to upgrade Tor's onion encryption scheme to protect against tagging attacks and thereby strengthen its end-to-end integrity protection. In 2016 Nick Matthewson described a concrete onion encryption in Tor proposal 261, where each encryption layer is processed by a strongly secure, yet relatively expensive, tweakable wide-block cipher. Shortly after, Ashur, Dunkelman, and Luykx argued that replacing Tor's Counter-mode encryption with an tweakable wide-block cipher would be an overkill and replacing it instead with the RUP-secure AEAD scheme should suffice. Their intuition turned out to be fairly correct, however, translating said intuition into a secure onion encryption scheme for Tor is far from straightforward. In fact, several unsuccesful attempts followed at describing a concrete scheme for Tor in proposal 295.

Currently, CGO (described in proposal 359) is the main candidate to become the new onion encryption scheme for Tor and it is already being integrated in Arti, Tor's next-generation implementation in Rust, with plans to be deployed in the near future. Proposal 359 does not describe the design rationale of Counter Galois Onion (CGO), but rather refers to our work instead (eprint 2025/583), where we identify the functionality and security desiderata for Tor's onion encryption, and propose CGO, an alternative onion encryption scheme that follows a minimalistic, modular design and includes several improvements over proposals 261 and 295.

In this talk, we will explain the design rationale behind CGO and the challenges that need to be overcome for successful deployment in the real world. We will concentrate on the technical side, where we discuss how to turn a relatively simple underlying primitive (think wide blockcipher) into a fully-fledged onion encryption scheme, but we will also detail our interactions with Mathewson to ensure that CGO would actually solve the problems the Tor community cares most about. For instance, for Tor latency is key, requiring an efficient onion encryption scheme. In CGO's case, we use as underlying primitive an updatable tweakable split-domain cipher, which is an augmentation of the recently introduced rugged pseudorandom permutation (Degabriele and Karadzic, CRYPTO 2022) that allows for more efficient designs than the tweakable wide-block cipher suggested in proposal 261.

We will also address the choices behind our concrete instantiation for the updatable tweakable split-domain cipher, called UIV+ and use it to benchmark our full CGO scheme against Tor's existing onion encryption scheme, demonstrating a clear performance gain at the proxy and at exit and entry routers, at the expense of a mild slowdown at intermediate routers. Both CGO and UIV+ are accompanied by formal security proofs that solidify the informal security claims. For this talk, we will concentrate on the informal, intuitive security that is provided by CGO.