Privacy Preserving and Resilient Resource Public Key Infrastructure

Abstract:
Resource Public Key Infrastructure (RPKI) is vital to the security of inter-domain routing. However, RPKI enables Regional Internet Registries (RIRs) to unilaterally takedown IP prefixes - indeed, such attacks have been launched by nationstate adversaries. The threat of IP prefix takedowns is one of the factors hindering RPKI adoption.
In this work, we proposed the first distributed RPKI system, based on threshold signatures, that requires the coordination of a number of RIRs to make changes to RPKI objects; hence, preventing unilateral prefix takedown. We performed extensive evaluations using our implementation demonstrating the practicality of our solution. Furthermore, we shown that our system is scalable and remains efficient even when RPKI is widely deployed.