Signal adiciona nova defesa criptográfica contra ataques quânticos

Data: 2025-10-03 19:30:40

Autor: Inteligência Against Invaders

A Signal anunciou a introdução do Sparse Post-Quantum Ratchet (SPQR), um novo componente

criptográfico projetado para resistir a ameaças de computação quântica.

O SPQR servirá como um mecanismo avançado que atualiza continuamente as chaves de criptografia usadas nas conversas e descarta as antigas.

O Signal é um aplicativo de mensagens e chamadas criptografadas de ponta a ponta gerenciado pela organização sem fins lucrativos Signal Foundation, com uma base de usuários ativos mensais estimada em até 100 milhões.

O novo componente garante sigilo de encaminhamento e segurança pós-comprometimento, garantindo que, mesmo em caso de comprometimento ou roubo de chave, as mensagens futuras trocadas entre as partes sejam seguras.

Em termos de criptografia, o SPQR utiliza mecanismos de encapsulamento de chave pós-quânticos (ML-KEM) em vez de Diffie-Hellman de curva elíptica e apresenta codificação eficiente de fragmentação e eliminação para lidar com grandes tamanhos de chave sem inchar a largura de banda.

O sinal tem usado o CRYSTALS-Kyber (um KEM pós-quântico) juntamente com uma implementação da Curva Elíptica Diffie-Hellman desde 2023 para proteger contra ataques de computação quântica que ameaçam quebrar a criptografia atual.

No entanto, o SPQR vem no topo do sistema de catraca dupla existente, formando o que o Signal chama de Triple Ratchet, formula uma “chave mista” hiper-segura.

“Quando você deseja enviar uma mensagem, você pergunta ao Double Ratchet e ao SPQR “Qual chave de criptografia devo usar para a próxima mensagem?” e ambos lhe darão uma chave”, lê o anúncio do Signal.

“Em vez de qualquer chave ser usada diretamente, ambas são passadas para uma função de derivação de chave – uma função especial que recebe entradas aleatórias o suficiente e produz uma chave criptográfica segura que é tão longa quanto você precisa. Isso lhe dá uma nova chave “mista” que tem segurança híbrida.”

O novo sistema foi projetado em colaboração com PQShield, AIST (Japão) e Universidade de Nova York, com sua base técnica baseada em parte nos artigos USENIX 2025 e Eurocrypt 2025.

O projeto também foi formalmente verificado usando o ProVerif, e a robustez da implementação do

Rust foi testada usando a ferramenta hax. A verificação contínua agora será aplicada a todas as compilações futuras, garantindo que as provas sejam reproduzidas a cada alteração de código.

O Signal diz que o lançamento do SPQR na plataforma de mensagens será gradual e os usuários não precisam tomar nenhuma ação para que a atualização seja aplicada, além de manter seus clientes atualizados para a versão mais recente.

O novo sistema será compatível com versões anteriores no sentido de que, quando um cliente habilitado para SPQR se comunicar com alguém que ainda não oferece suporte à tecnologia, o modelo de segurança será rebaixado.

Assim que o SPQR for disponibilizado para todos os clientes, o Signal o aplicará em todas as sessões.

[IMAGEM REMOVIDA]