Re-Cryptography: the Art of Key Translation

In key translation schemes, a proxy is given special information which allows her to change a cryptographic object created under one key into the same object under another key, without being able to do anything else (e.g., decrypt the message or sign arbitrarily).

Such schemes help alleviate key management problems. We formally model, design, analyze and implement new constructions.

Applications include secure storage, program obfuscation, and web integrity (WISPR).

Selected Recent Publications