Unbreakable Shared-Key Cryptography Implementation

Internship proposal

Main advisor: Axel Legay, axel.legay@inria.fr
Other advisors: Fabrizio Biondi, fabrizio.biondi@inria.fr ; Thomas Given-Wilson thomas.given-wilson@inria.fr

Required skills: Strong programming skills; Familiarity with shared-key encryption protocols

Context: The TAMIS team has worked on generalize Shannon's perfect secrecy results with the aim of developing shared-key cryptosystems that are mathematically provable to be impossible to break. Recently, we have created a new cryptosystem, named Apollonian cell encoder, that is provably optimal at preserving message equivocation and allows for unlimited key reuse.

Description:
Unconditional cryptography guarantees that the hardness of a cryptographic scheme derives from proven entropic properties instead of unproven complexity results. In a recent breakthrough, we have proven the practical feasibility of unconditionally secure cryptographic schemes in the form of Apollonian cell encoders. Contrarily to perfectly secret schemes like one-time pad, Apollonian cell encoders allow for the transmission of messages larger than the key and unlimited key reuse, while guaranteeing the highest message equivocation mathematically possible. Finally, Apollonian cell encoders have an elegant and compact mathematical representation, making them easy to implement and use in practice.

The objective of this internship is to develop a reference implementation for a shared-key cryptosystem based on Apollonian cell encoders. Such an implementation will generate an encoder for a given message distribution and apply the encoder to encrypt and decrypt messages, following a scheme that cannot be broken even by an attacker with unlimited computational power. This provides users with ultimate security and privacy for their secret communications.

Keywords: shared-key cryptography, unconditional security, network protocols, implementation

References:
Claude E. Shannon, Warren Weaver. The Mathematical Theory of Communication. Univ of Illinois Press, 1949. ISBN 0-252-72548-4

Fabrizio Biondi, Thomas Given-Wilson, Axel Legay: Attainable unconditional security for shared-key cryptosystems. Inf. Sci. 369: 80-99 (2016)

Fabrizio Biondi, Thomas Given-Wilson, Axel Legay. Universal Optimality of Apollonian Cell Encoders. 2017. <hal-01571226>

Fabrizio Biondi, Thomas Given-Wilson, Axel Legay. On the Attacker's Knowledge in Shared-Key Cryptosystems. 2015. <hal-01241374>