# RAVe: Robuste Authentisierte Verschlüsselung

Professur: Mediensicherheit
Prof. Dr. Stefan Lucks

Fakultät Medien

Drittmittelgeber: DFG

Fördersumme: 271.800,00 Euro

**Beschreibung:**

Der Begriff der "Authentisierten Verschlüsselung" entwickelte sich zwischen den Jahren 2000 und 2004. Bellare und Namprempre (2000) beschreiben die Chosen-Ciphertext-Sicherheit als Kombination von Chosen-Plaintext-Vertraulichkeit und Fälschungssicherheit. Empfänger dürfen vertrauliche Klartexte nur preisgeben bzw. nutzen, wenn deren Authentizität feststeht. Eine Verletzung dieses Prinzips wird heute als "Release of Unverified Plaintexts" (RUP) bezeichnet. Rogaway (2002) beschreibt die "Authenticated Encryption with Associated Data" (AEAD) als die zusätzliche Authentisierung relevanter Kontext-Information. Rogaway (2004) formalisiert die "Nonce-basierte" Verschlüsselung und AEAD.

Kryptographische Robustheit bezeichnet die bestmögliche Sicherheit eines Kryptosystems auch bei unvorhergesehener oder fehlerhafter Nutzung. Zwar hat sich die seit 2004 etablierte Formalisierung der AEAD bewährt, doch wurde fehlende Robustheit zunehmend als Mangel empfunden, zunächst bezogen auf einen "Nonce Misuse" (NM), seit kurzem zunehmend auch auf Fälle von "Release of Unverified Plaintexts" (RUP).

Das Projekt dient der Weiterentwicklung des Begriffs der "Robustheit". Es verfolgt insbesondere die folgenden Ziele:

1. Die Entwicklung neuer Systeme zur Authentisierten Verschlüsselung, die sowohl NM- als auch RUP-robust sind.
2. Ein verbessertes Verständnis der Leakage Resilience, insbesondere der leakage-resilienten Authentisierten Verschlüsselung.
3. Grundlegende Erkenntnisse über einen möglichen Zusammenhang zwischen Authentisierter Verschlüsselung und implizitem Key Stretching.
4. Die Untersuchung neuer Trade-Offs für die Entwicklung von schwergewichtigen softwareeffizienten Blockchiffren und die tatsächliche Entwicklung einer derartigen Blockchiffre.

Weitere Informationen: Mediensicherheit

**Kontakt:**

Bauhaus-Universität Weimar
Mediensicherheit
Prof. Dr. Stefan Lucks
stefan.lucks@uni-weimar.de

Bauhausstr. 11
99423 Weimar
Tel. 03643/ 58 37 27