MASARYKOVA UNIVERZITA
Fakulta informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Student: Bc. Radovan Lapár

Program: Informatika

Obor: Teoretická informatika

Garant oboru: prof. RNDr. Jozef Gruska, DrSc. (TEI)

Vedoucí práce: doc. RNDr. Tomáš Brázdil, Ph.D.

Konzultant: RNDr. Petr Švenda, Ph.D.

Katedra: Katedra teorie programování

Název práce: Hluboké učení v kryptografii

Název práce anglicky: Deep learning in cryptography

Zadání: Cílem práce je prostudovat použitelnost metod hlubokého učení v oblasti kryptografie. Práce by měla shrnout aktuální stav problematiky a podat přehled použití hlubokých sítí pro analýzu vlastností kryptografických algoritmů, např. detekce vzájemně závislých bitů ve výstupu generátorů náhodných čísel nebo systematické závislosti zanášené konkrétním způsobem implementace hledání velkých prvočísel. Následně by se měla zaměřit na šifru RSA a řešit zejména následující problémy:

- Identifikace algoritmu použitého pro generování náhodných velkých prvočísel
- Identifikace společných vlastností vekého množství veřejných klíčů generovaných shodnou kryptografickou knihovnou
- Vytvoření klasifikátoru využívajícího hlubokých neuronových sítí pro identifikaci knihovny, která vygenerovala poskytnutý RSA klíč(e).

Součástí práce je implementace vybraných typů neuronových sítí (pokud možno s využitím frameworku TensorFlow) a extensivní experimentální vyhodnocení zahrnující srovnání s tradičními metodami (Bayes).

Literatura:

ŠVENDA, Petr, Matúš NEMEC, Peter SEKAN, Rudolf KVAŠŇOVSKÝ, David FORMÁNEK, David KOMÁREK a Václav MATYÁŠ. *The Million-Key Question – Investigating the Origins of RSA Public Keys*. In Thorsten Holz, Stefan Savage. *Proceedings of 25th USENIX Security Symposium*. Austin, Texas: USENIX Association, 2016. s. 893-910, 18 s. ISBN 978-1-931971-32-4.

Martín Abadi, David G. Andersen. Learning to Protect Communications with Adversarial Neural Cryptography. https://arxiv.org/abs/1610.06918

Zadání bylo schváleno prostřednictvím IS MU.