Bundesamt
für Sicherheit in der
Informationstechnik

Anwendungen der künstlichen Intelligenz in der Kryptographie

Prof. Dr. Werner Schindler

Bundesamt für Sicherheit in der Informationstechnik (BSI)

OMNISECURE 2020
Berlin, den 22. Januar 2020

Übersicht

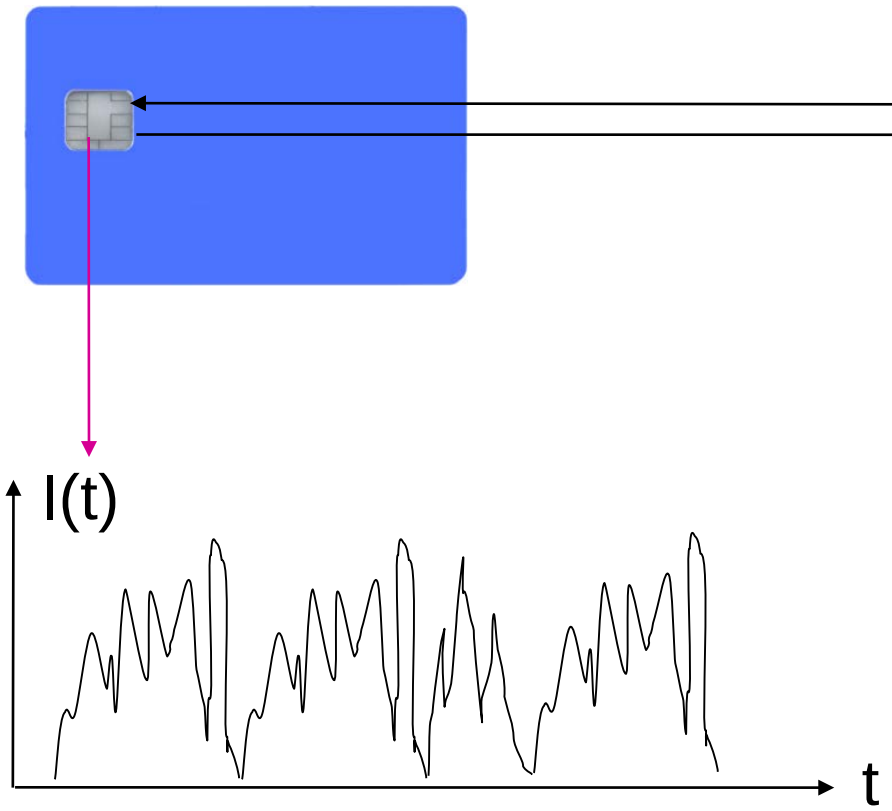
- Künstliche Intelligenz (KI) in der Seitenkanalanalyse
- Techniken des maschinellen Lernens (ML) in der mathematischen Kryptoanalyse
- Fazit und Ausblicke

Allgemeines

- Die heute angewandten KI-Ansätze gehören zur so genannten *schwachen künstlichen Intelligenz und* verwenden normalerweise an zentraler Stelle maschinelles Lernen (neuronale Netze, Deep Learning, Entscheidungsbäume, Clusteralgorithmen, support vector machines usw.).

Powerangriffe: Grundidee

- **Target:** Chipkarte, Mikrocontroller, FPGA etc.
- **Ziel:** Rekonstruktion des kryptographischen Schlüssels anhand der Stromaufnahme



Powerattacken nutzen schlüsselabhängige Unterschiede im Stromverbrauch.

Powerangriffe in Zertifizierungsverfahren

- Seitenkanalangriffe (Powerangriffe, Abstrahlangriffe, Laufzeitangriffe etc.) sind zentraler Bestandteil von CC-Zertifizierungsverfahren von Chipkarten.
- Von zentraler Bedeutung: Vertrauenswürdigkeit der Zertifizierungsergebnisse (erfordert Kenntnis der stärksten Angriffe!)
- „konventionelle“ Powerangriffe: DPA, CPA, Templateangriffe, stochastischer Ansatz, ...

Powerangriffe und maschinelles Lernen (I)

- **Frage:** Können ML-Verfahren verborgene / verwischte Korrelationen und Strukturen besser ausnutzen als konventionelle Angriffsverfahren?
- Die konventionellen Verfahren setzen bestimmte Annahmen voraus (z.B. Alignment der Stromkurven, z.T. Normalverteilung des Rauschens).
- **Vermutung:** Sind diese Annahmen (nahezu) erfüllt, sollte der Effizienzgewinn durch ML-Verfahren nicht allzu groß sein.

Powerangriffe und maschinelles Lernen (II)

- Wie verhält sich das, wenn diese Annahmen deutlich verletzt sind?
- **Beispiel:** Random Delays, um ein Alignment der Powertraces zu erschweren
  - Konventionelle Verfahren erfordern normalerweise eine Vorbearbeitung der Stromkurven (Identifikation und entfernen der „inaktiven“ Zeitintervalle)
  - Tiefe neuronale Netze können solche Gegenmaßnahmen *unter Umständen* (automatisch) kompensieren; vgl. z.B. (Cagli, Dumas, Prouff (2017) [1])

Powerangriffe und maschinelles Lernen (III)

- Seit mehreren Jahren existieren in der Literatur Arbeiten zu ML-basierten Ansätzen in der Poweranalyse.
  Vergleichbarkeit? Übertragbarkeit und Extrapolierbarkeit der Resultate?
- *Deutliche Effizienzgewinne* durch ML-Verfahren hätten Einfluss auf das Design von Sicherheitsimplementierungen oder zumindest auf deren Gebrauch!
- Weiterer Forschungsbedarf ist gegeben.
- Das BSI baut eigene Expertise in diesem Gebiet auf.

CHES 2018 – Seitenkanalwettbewerb (CTF)

- Juli 2018: Stromkurven von DES-, AES- und RSA-Implementierungen veröffentlicht
- September 2018: Zu jedem Algorithmus wurden zwei Challenges veröffentlicht.
- 58 Teams hatten sich registriert.
- BSI-Team (*A. Gohr, S. Jacob, W. Schindler*) gewinnt beide AES-Challenges.

- AES (Advanced Encryption Standard) [maskierte Implementierungen]
  - zur Vorbereitung: 40.000 Stromkurven
  - für Angriff: je 1.000 Stromkurven pro Challenge

CHES CTF 2018 / AES - Challenges: Resultate

- Unser Angriff (2018) ist auch mit viel weniger Powertraces erfolgreich.
  - **Non-Portability Challenge** (Angriff gegen gleiches Device): meistens genügt 1 Powertrace
  - **Portability-Challenge** (Angriff gegen neues Device):
    - immer erfolgreich mit 5 Powertraces
    - in mehr als der Hälfte der Fälle genügen 2 Powertraces
- Der Angriff verbindet maschinelles Lernen mit einem SAT-Solver („konventionelles“ Verfahren).
- Das neuronale Netz erlaubt Rückschlüsse auf Implementierungseigenschaften.
- Details: [3]

Konventionelle Ansätze und ML-Methoden im Vergleich

- Nachträglich hat ein anderes BSI-Team die Wettbewerbstraces (Portability Challenge) mit Templateattacken angegriffen und ähnliche Resultate erzielt (Damm, Freud, Klein (2019) [2]).
- Ein verbesserter ML-basierter Angriff (tiefes neuronales Netz + SAT-Solver) kommt in den meisten Fällen (Non-Portability Challenge: ≈ 100 %, Portability Challenge: ≈ 75 %) mit sogar einer einzigen Powertrace aus (+ erweiterte Erkenntnisse über Implementierung) (Gohr, Jacob, Schindler (2020) [5]).

- **Ziel:**
  - „Faire“ Vergleiche zwischen konventionellen Verfahren (DPA, CPA, Templateattacken, stochastischer Ansatz etc.) und ML-basierten Ansätzen.
  - Konzentration auf stärkere Implementierungen

Kryptoanalyse von Blockchiffren

- Mathematische Kryptoanalyse untersucht die Stärke von kryptographischen Algorithmen.
- Wichtige Eigenschaft von Blockchiffren: Ununterscheidbarkeit zwischen (Klartext/Geheimtext)-Paaren (bei unbekanntem Schlüssel) und Zufallspaaren
- Aus einem Unterscheider können üblicherweise Angriffe entwickelt werden.
- Gut entwickelte wichtige Standardtechnik: Differentielle Kryptoanalyse

ML-basierte Kryptoanalyse von Speck 32/64 (Lightweight-Blockchiffre)

- Speck 32/64: kleinster Repräsentant der Speckfamilie
  - 32-Bit Klartext → 32-Bit Geheimtext, 64-Bit-Schlüssel
  - 22 Runden

- ML-basierter 7-Runden-Unterscheider ist signifikant besser als optimierter differentieller Unterscheider
- ML-basierter 7-Runden-Unterscheider → ... → Angriff gegen 11 Runden-Speck (von 22 Runden)
- Effizienzgewinn (Rechenaufwand) durch ML-basierten Ansatz (+ in Kombination mit weiteren KI-Techniken bei Schlüsselsuche) ≈ Faktor 200
- Details: (Gohr (2019) [4])

Fazit und Ausblicke

- Seitenkanalanalyse: Es bleibt zu klären, unter welchen Voraussetzungen ML-basierte Ansätze signifikante Vorteile gegenüber konventionellen Ansätzen aufweisen.
- Maschinelles Lernen ist auch dazu geeignet, neue Werkzeuge für die mathematische Kryptoanalyse zu entwickeln.
- Es ist wichtig, die stärksten Angriffe zu kennen.
- Von Interesse sind auch Kombinationen von ML-Methoden mit konventionellen Ansätzen.
- Weiterer Forschungsbedarf ist gegeben.

Literatur (I)

[1] E. Cagli, C. Dumas, E. Prouff: Convolutional Neural Networks with Data Augmentation Against Jitter-Based Countermeasures – Profiling Attacks without Pre-Prepocessing. In: W. Fischer, N. Homma: Cryptographic Hardware and Embedded Systems – CHES 2017, Springer, LNCS 10529, Berlin 2017, 45-68.

[2] T. Damm, S. Freud, D. Klein: Dissecting the CHES 2018 AES Challenge. IACR Cryptology ePrint Archive, Version of July 4, 2019, https://eprint.iacr.org/2019/783

[3] A. Gohr, S. Jacob, W. Schindler: CHES 2018 Side Channel Contest CTF – Solution of the AES Challenges. IACR Cryptology eprint Archive, https://eprint.iacr.org/2019/094

Literatur (II)

[4] A. Gohr: Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning.

In: A. Boldyreva, D. Micciancio (Hrsg.): Crypto 2019 (Part II), Springer, LNCS 11693, Berlin 2019, 150-179.

Code ist auf github verfügbar: https://www.github.com/agohr/deep_speck

Vortrag: https://youtu.be/weX1itU9VrM

[5] A. Gohr, S. Jacob, W. Schindler: Efficient Solutions of the CHES 2018 AES Challenge Using Deep Residual Neural Networks and Knowledge Distillation on Adversarial Examples.

Wird in Kürze eingereicht

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Prof. Dr. Werner Schindler
Referatsleiter
Prüfung von Kryptoverfahren

Werner.Schindler@bsi.bund.de
Tel. +49 (0) 228 9582 5652
Fax +49 (0) 228 10 9582 5652
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik