Komplexitätstheorie

Sommersemester 2019

Mario Holldack, M. Sc.
Prof. Dr. Georg Schnitger
Hannes Seiwert, M. Sc.

GOETHE UNIVERSITÄT
FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

Übungsblatt 7

Ausgabe: 03.06.2019
Abgabe: Di, 11.06.2019

Aufgabe 7.1 *IND-CPA-Sicherheit durch PRGs* (8 Punkte)

Wir betrachten die Situation aus der Aufgabe 6.3 b) für ein Polynom $p(n)$. Sei $x \in \{0,1\}^{p(n)}$ eine Klartextnachricht, $z \in \{0,1\}^n$ ein geheimer Schlüssel und G ein Pseudo-Random-Generator mit Streckung $p(n)$. Bob schickt eine verschlüsselte Nachricht $y = f(x,z) = x \oplus G(z)$ an Alice.

Zeigen Sie: Die Funktion f ist IND-CPA-sicher.

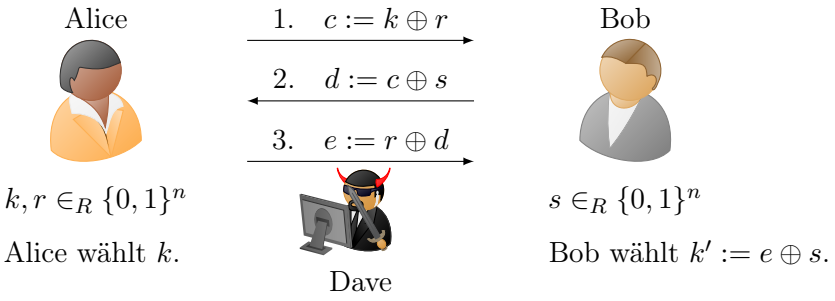
Hinweis: IND-CPA kann auch für Private-Key-Kryptographie betrachtet werden. In diesem Fall teilt $\mathcal{F} = f$ dem Angreifer $\mathcal{A}$ im ersten Schritt keinen öffentlichen Schlüssel mit. Nehmen Sie an, die Funktion f wäre nicht IND-CPA-sicher. Folgern Sie, dass dann eine Familie $T = (T_n : n \in \mathbb{N})$ von Schaltkreisen polynomieller Größe existiert, sodass für ein $x \in \{0,1\}^{p(n)}$ die absolute Differenz

$$\left| \mathbf{pr}_{z \in_R \{0,1\}^n} \left[T_n(x \oplus G(z)) = 1 \right] - \mathbf{pr}_{u \in_R \{0,1\}^{p(n)}} \left[T_n(u) = 1 \right] \right|$$

als Funktion von n nicht vernachlässigbar ist.

Aufgabe 7.2 *Ein Schlüsseltauschprotokoll* (3 + 5 = 8 Punkte)

Alice und Bob möchten sich auf einen Schlüssel einigen und gehen gemäß dem folgenden Protokoll vor:



Zu Beginn wählen Alice und Bob rein zufällige Bitstrings k, r bzw. s und tauschen anschließend die Nachrichten c, d und e aus.

a) Zeigen Sie: Das Protokoll ist korrekt, d. h. es gilt $k = k'$.
(Alice und Bob einigen sich auf denselben Schlüssel.)

b) Angenommen, Dave kann die ausgetauschten Nachrichten c, d und e beobachten. Wir wollen herausfinden, ob Dave das Protokoll „knacken“ und den geheimen Schlüssel k bestimmen kann.

Welche der beiden folgenden Aussagen ist richtig? Beweisen Sie Ihre Antwort.

I) Für jeden deterministischen Algorithmus D gilt: Die Wahrscheinlichkeit

$$\mathbf{pr}_{k,r,s \in \{0,1\}^n} [D(c,d,e) = k],$$

dass D bei Eingabe der Nachrichten (c,d,e) den geheimen Schlüssel k ausgibt, ist vernachlässigbar.

II) Es existiert ein deterministischer Algorithmus D mit Worst-Case-Laufzeit $\mathcal{O}(n)$, der bei Eingabe der Nachrichten (c,d,e) den geheimen Schlüssel k ausgibt.

Aufgabe 7.3 *El-Gamal-Verfahren und Diffie-Hellman-Vermutung* (4 + 4 = 8 Punkte)

Wir betrachten in dieser Aufgabe Sicherheitsgarantien für das El-Gamal-Verfahren.

a) Wir nehmen an, dass Bob zur Verschlüsselung zweier Nachrichten x und y zweimal denselben quadratischen Rest $b \in R$ verwendet hat, d. h. es gelte

$$\text{Enc}(x) = (g^b, h^b \cdot x) \text{ und } \text{Enc}(y) = (g^b, h^b \cdot y).$$

Zeigen Sie: Falls Dave die verschlüsselten Nachrichten Enc(x) und Enc(y) sowie die Klartextnachricht y kennt, dann kann er die Klartextnachricht x bestimmen, ohne den privaten Schlüssel a zu besitzen.

Hinweis: Sei $z \in R$. Dann kann das multiplikative Inverse $z^{-1} \in R$ von z effizient mit dem erweiterten euklidischen Algorithmus bestimmt werden.

Fazit: Das El-Gamal-Verfahren ist anfällig gegen Known-Plaintext-Angriffe[1].

b) Seien das erzeugende Element g und der Modulus p gegeben. Die Diffie-Hellman-Vermutung besagt, dass effiziente, nicht-uniforme Algorithmen die Tripel (g^x, g^y, g^{xy}) und (g^x, g^y, g^z), jeweils modulo p, für zufällige $x, y, z \in \mathbb{Z}_p$ nur mit vernachlässigbarem Vorteil unterscheiden können.

Zeigen Sie:

Wenn die Diffie-Hellman-Vermutung gilt, dann ist das El-Gamal-Verfahren IND-CPA-sicher.

[1] https://en.wikipedia.org/wiki/Known-plaintext_attack