Komplexitätstheorie

Sommersemester 2020

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: 08.06.2020
Abgabe: 15.06.2020

Die Abgabe erfolgt per E-Mail an Mario Holldack (holldack@em.uni-frankfurt.de).

Aufgabe 7.1 *RSA und Padding* $(3 + (3 + 2) = 8$ Punkte)

Wir betrachten das RSA-Kryptoverfahren mit dem öffentlichen Schlüssel (N, e) für $N = pq$, dem privaten Schlüssel d und dem Sicherheitsparameter $n = \lceil \log_2 N \rceil$. In Aufgabe 6.3 haben wir uns mit Known-Plaintext-Angriffen auf das El-Gamal-Verfahren beschäftigt. Nun geht es um *Chosen-Ciphertext-Angriffe* auf RSA.

a) Sei O ein Orakel, das jede Anfrage $x^e \in \mathbb{Z}_N^*$ mit dem Klartext x beantwortet. Beschreiben Sie einen effizienten deterministischen Algorithmus, der bei der Eingabe von N, e und z^e unter Verwendung des Orakels O den Klartext z bestimmt, ohne z^e anzufragen.

Hinweis: Es gilt $a^c \cdot b^c = (a \cdot b)^c$ für alle $a, b \in \mathbb{Z}_N^*$ und $c \in \mathbb{N}$.

b) Um das in Teil a) beschriebenen Angriffsszenario zu vermeiden bzw. zu erschweren, verwendet man Padding-Verfahren, beispielsweise das in Abschnitt 7.4.6 in S. Goldwasser und M. Bellare: Lecture Notes on Cryptography beschriebene OAEP (Optimal Asymmetric Encryption Padding)[1]. Dabei werden zunächst die n Bits des Klartextes mithilfe von k_0 Zufallsbits und k_1 Padding-Bits, eines Generators G und einer Hashfunktion H modifiziert, sodass ein $(n+k_0+k_1)$-stelliger Bitstring entsteht; anschließend erfolgt die konventionelle RSA-Verschlüsselung.

i) Beschreiben Sie die Rechenschritte des OAEP-Verfahrens: Wie wird aus dem Klartext die verschlüsselte Nachricht berechnet? Wie wird aus einer verschlüsselten Nachricht wieder der Klartext bestimmt?

ii) Sei z der Klartext einer RSA-OAEP-verschlüsselten Nachricht $f(z)$.
Untersuchen Sie die Rolle der Anzahl k_0 der Zufallsbits: Wieso wählt man k_0 so groß, dass jeder Angreifer eine Rechenkapazität von deutlich weniger als 2^{k_0} besitzt?

Hinweis: Wie könnte ein Angreifer vorgehen, wenn er Zugriff auf ein Orakel wie in Teil a) und auf die bei der Berechnung von $f(z)$ verwendeten Zufallsbits hat, ohne dem Orakel die Anfrage $f(z)$ zu stellen?

Anmerkung: Tatsächlich genügt für praktische Angriffe ein schwächeres Orakel-Modell. Das Orakel muss lediglich beantworten, ob es sich bei dem angefragten Text um eine verschlüsselte Nachricht handelt[2]*, d. h. ob es überhaupt einen Klartext gibt, sodass nach der Anwendung eines Paddingverfahrens und der RSA-Verschlüsselung der angefragte Text entstehen kann. Zur Implementierung von Orakeln kommen in der Praxis vorab berechnete Rainbow Tables zum Einsatz.*

[1] Hinweis zur verwendeten Notation: Der Konkatenationsoperator $\|$ bindet schwächer als das XOR $\oplus$.

[2] D. Bleichenbacher. *Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1.* https://doi.org/10.1007%2FBFb0055716

Aufgabe 7.2 *Shortest Independent Vectors* (2 + 6 = 8 Punkte)

a) Sei $A \in \mathbb{Z}^{n \times n}$ eine unimodulare Matrix. Zeigen Sie: Die inverse Matrix A^{-1} ist unimodular.

Hinweis: Sei M eine invertierbare Matrix. Für jede Zeile i und jede Spalte j sei $M^{(i,j)}$ die Matrix, die aus M entsteht, indem Zeile i und Spalte j entfernt werden. Die Adjunkte $\mathrm{adj}(M)$ ist eine Matrix mit den Einträgen

$$\mathrm{adj}(M)_{i,j} = (-1)^{i+j} \cdot \det(M^{(i,j)}).$$

Verwenden Sie die Cramersche Regel

$$M^{-1} = \tfrac{1}{\det(M)} \cdot \mathrm{adj}(M).$$

b) Die Pascal-Matrix $P^{(n)}$ ist die untere Dreiecksmatrix mit den Einträgen

$$P^{(n)}_{i,j} = \begin{cases} \binom{i}{j}, & \text{falls } 0 \le j \le i \le n-1, \\ 0, & \text{falls } 0 \le i < j \le n-1. \end{cases}$$

Bestimmen Sie eine Basis B für das Gitter $\mathcal{G}(P^{(n)})$ aus möglichst kurzen Basisvektoren, d. h. lösen Sie das Shortest-Independent-Vectors-Problem ($\mathbf{SIVP}_\gamma$ für $\gamma = 1$) für $\mathcal{G}(P^{(n)})$.

Aufgabe 7.3 *Eine obere Schranke für Shortest Vector* (8 Punkte + 5* Extrapunkte)

a) Sei $n \ge 2$. Sei $\mathcal{G} := \mathcal{G}(B)$ ein Gitter in $\mathbb{R}^n$ Zeigen Sie: Für die Länge $\lambda_1(\mathcal{G})$ eines kürzesten Basisvektors von $\mathcal{G}$ gilt

$$\lambda_1(\mathcal{G}) \le \sqrt{n} \cdot |\det(B)|^{1/n}.$$

Hinweis: Sie dürfen die folgende Aussage ohne Beweis verwenden: Sei $S \subseteq \mathbb{R}^n$ eine beliebige konvexe[3], punktsymmetrische[4] Menge mit $0 \in \mathbb{R}^n$ als Symmetriepunkt und Volumen $\mathrm{vol}(S) > 2^n \cdot |\det(B)|$. Dann enthält S einen Gitterpunkt $g \in \mathcal{G}$ mit $g \neq 0$.

b*) Geben Sie (für beliebig große n) ein Gitter $\mathcal{G}(B) \subseteq \mathbb{R}^n$ an, für das die in a) gezeigte Schranke möglichst schlecht ist, d. h. der Approximationsfaktor

$$\alpha_n := \frac{\sqrt{n} \cdot |\det(B)|^{1/n}}{\lambda_1(\mathcal{G}(B))}$$

soll möglichst groß sein.

[3] Eine Menge S ist *konvex*, wenn für alle $x, y \in S$ und alle $\lambda \in [0,1]$ gilt: $\lambda x + (1-\lambda)y \in S$.

[4] Eine Menge ist *punktsymmetrisch*, wenn sie durch die Spiegelung an einem Symmetriepunkt auf sich selbst abgebildet wird.