Übungsblatt 13

Besprechung der mündlichen Aufgaben am 2. 2. 2023
Abgabe der schriftlichen Lösungen bis 7. 2. 2023, 23:59 Uhr

Aufgabe 75 ***mündlich***

Betrachten Sie den BBS-Generator $\mathsf{BBS}_{n,l}(x_0)$.

(a) Überlegen Sie, wie sich aus dem Keim x_0 jedes x_i möglichst effizient berechnen lässt, falls die Primfaktorzerlegung von n bekannt ist.

(b) Lässt sich x_i mit vergleichbarem Aufwand auch aus jedem beliebigem x_j bestimmen? Betrachten Sie insbesondere den Fall $j > i$.

(c) Zeigen Sie, dass die Periode des BBS-Generators höchstens $t = \mathrm{kgV}(u_1, v_1)$ ist, wobei u_1 die Ordnung von 2 in $\mathbb{Z}^*_{(p-1)/2}$ und v_1 die Ordnung von 2 in $\mathbb{Z}^*_{(q-1)/2}$ ist.

(d) Zeigen Sie, dass diese Schranke im Fall $p = 103$, $q = 127$ scharf ist.

Hinweis: Benutzen Sie den Keim 49.

Aufgabe 76 ***mündlich***

Wir betrachten »Bit Commitment«, d.h. Alice muss sich auf ein Bit b festlegen, will es aber noch nicht verraten. Später gibt Alice b bekannt, soll es aber zwischendurch nicht (oder nur mit kleiner Wahrscheinlichkeit) ändern können.

(a) Alice legt sich auf b fest, indem sie Bob $y := a^b x^2 \mod n$ sowie n und a sendet, wobei a ein beiden bekannter quadratischer Nichtrest modulo n ist. Unter welchen Voraussetzungen kann Bob b nicht selbst aus y ermitteln?

(b) Wie kann Alice b offenlegen und Bob überzeugen, dass sie es nicht geändert hat?

(c) Wie kann Alice die Voraussetzung, dass a als quadratischer Nichtrest bekannt ist durch gezielte Wahl von n loswerden?

(d) Bob wählt sich nun zwei Primzahlen p, q mit $p = mq + 1$, sowie $\alpha \in \mathbb{Z}_p$ mit $\mathrm{ord}_p(\alpha) = q$ und für ein a mit $\mathrm{ggT}(a, q) = 1$ zusätzlich $\beta = \alpha^a$. Alice legt sich erneut auf ein Bit b fest und sendet Bob $y := \alpha^z \beta^b$, wobei sie z zufällig wählt und geheim hält. Kann Bob b aus y berechnen?

(e) Wie kann Alice b offenlegen und Bob überzeugen, dass sie es nicht geändert hat? Mit welchem Wissen könnte Alice b ändern?

(f) Vergleichen Sie beide Verfahren hinsichtlich der Vorteile für Bob und Alice. Gäbe es einen Vorteil, beide Verfahren gleichzeitig zu verwenden?

Aufgabe 77 ***mündlich***

Wir betrachten »Oblivious Transfer« (OT_p), d.h. Alice hat eine Nachricht x, die sie mit Wahrscheinlichkeit p Bob zur Verfügung stellen will. Bob weiß am Ende, ob er die Nachricht erhalten hat, Alice soll dies nicht erfahren können.

(a) Rabins $\mathrm{OT}_{1/2}$-Protokoll arbeitet wie folgt für Nachricht $x \in \mathbb{Z}_n$:

  (1) Alice generiert ein RSA-Schlüsselpaar $(n = pq, d, e)$ mit $p \equiv_4 q \equiv_4 3$ und sendet Bob den öffentlichen Schlüssel (n, e) sowie $x^e \mod n$.

  (2) Bob sendet $z^2 \bmod n$ für zufälliges $z \in \mathbb{Z}_n^*$ (Bob rät $z \in \mathbb{Z}_n$ und testet, ob $\mathrm{ggT}(z, n) = 1$).

  (3) Alice berechnet ein z' und sendet dieses an Bob.

  (4) Bob kann mit Wahrscheinlichkeit $\frac{1}{2}$ aus z, z', n den geheimem Exponenten d ermitteln und so x berechnen.

Wie muss Alice z' berechnen, damit Bob d im letzten Schritt mit Wahrscheinlichkeit $\frac{1}{2}$ berechnen kann? Wie berechnet Bob dann d?

Bemerkung: Wegen Schritt (2) ist Bobs Erfolgswahrscheinlichkeit $\frac{1}{2} + \Theta(1/\sqrt{n})$.

(b) Wieso weiß Bob, ob Alice z' tatsächlich nach a) berechnet hat?

(c) Warum weiß Alice nicht, ob Bob die Nachricht lesen kann?

(d) Wie lässt basierend auf dem Fall $\mathrm{OT}_{1/2}$ mit $p \approx \frac{1}{2}$ ein Protokoll OT_p mit $p \geq 1 - \varepsilon$ bzw. $p \leq \varepsilon$ konstruieren (für beliebiges, festes ε)?

Aufgabe 78 ***10 Punkte***

Beschreiben Sie eine Modifikation des Algorithmus von Shanks, die den diskreten Logarithmus von β zur Basis α in Zeit $\mathcal{O}(\sqrt{r - l})$ berechnet, falls bereits bekannt ist, dass dieser im Teilintervall $[r, l]$ von $[0, \mathrm{ord}(\alpha) - 1]$ liegt.