

Übungsblatt 12

*Besprechung der mündlichen Aufgaben am 12. 2. 2021
Abgabe der schriftlichen Lösungen bis 16. 2. 2021, 23:59 Uhr*

Aufgabe 69

mündlich

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

- Überlegen Sie, wie sich aus dem Keim x_0 jedes x_i möglichst effizient berechnen lässt, falls die Primfaktorzerlegung von n bekannt ist.
- Lässt sich x_i mit vergleichbarem Aufwand auch aus jedem beliebigem x_j bestimmen? Betrachten Sie insbesondere den Fall $j > i$.
- Zeigen Sie, dass die Periode des BBS-Generators höchstens $t = \text{kgV}(u_1, v_1)$ 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.
- Zeigen Sie, dass diese Schranke im Fall $p = 103$, $q = 127$ scharf ist.

Hinweis: Benutzen Sie den Keim 49.

Aufgabe 70

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.

- Alice legt sich auf b fest, indem sie Bob $y := a^b x^2 \pmod n$ sowie n und a sendet, wobei a ein beidseitig bekannter quadratischer Nichtrest modulo n ist. Unter welchen Voraussetzungen kann Bob b nicht selbst aus y ermitteln?
- Wie kann Alice b offenlegen und Bob überzeugen, dass sie es nicht geändert hat?
- Wie kann Alice die Voraussetzung, dass a als quadratischer Nichtrest bekannt ist durch gezielte Wahl von n loswerden?
- Bob wählt sich nun zwei Primzahlen p, q mit $p = mq + 1$, sowie $\alpha \in \mathbb{Z}_p$ mit $\text{ord}_p(\alpha) = q$ und für ein a mit $\text{ggT}(a, q) = 1$ 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?
- Wie kann Alice b offenlegen und Bob überzeugen, dass sie es nicht geändert hat? Mit welchem Wissen könnte Alice b ändern?
- Vergleichen Sie beide Verfahren hinsichtlich der Vorteile für Bob und Alice. Gäbe es einen Vorteil, beide Verfahren gleichzeitig zu verwenden?

Aufgabe 71**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 $[0, \text{ord}(\alpha) - 1]$ liegt.