TECHNISCHE UNIVERSITÄT BERLIN WS 2007-2008
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. Florian Heß
Assistent: Osmanbey Uzunkol
www.math.tu-berlin.de/∼hess/krypto-ws2007
Abgabe: 01.02.2008
in der Übung

12. Übung Kryptographie

(Effiziente Implementierung der Arithmetic, digitale Signaturen)

---

1. Aufgabe

Seien $f : \{0,1\}^n \to \{0,1\}^n$ eine Einwegfunktion und A ein Algorithmus, welcher nach Eingabe von poly(n) Bildwerten y_i für ein y_j ein Urbild x_j mit in n signifikanter Wahrscheinlichkeit in Zeit poly(n) berechnet. Zeigen Sie, dass man unter Verwendung von A ein Urbild eines vorgegeben Bildwerts y in Zeit poly(n) mit in n signifikanter Wahrscheinlichkeit berechnen kann.

(5 Punkte)

2. Aufgabe

- Zeigen Sie, dass DSA ohne die Verwendung von SHA-1 nicht sicher bezüglich existenzieller Fälschung unter einem key-only Angriff ist.
- Zeigen Sie, dass DSA ohne den Größencheck von h und u universell gefälscht werden kann, wenn nur eine Signatur gegeben ist.

(6 Punkte)

3. Aufgabe

Beweisen Sie die im Skript beschriebenen Behauptungen für die Undeniable Signature Schemes.

(5 Punkte)

4. Aufgabe

(a) Zeigen Sie mittels des im Skript beschriebenen Algorithmus zur Punktaddition einer elliptischen Kurve, dass der in der Übung erwähnte Algorithmus zur Punktaddition einer elliptischen Kurve mit projektiven Koordinaten korrekt ist.

(b) Implementieren Sie den in der Übung erwähnten Algorihmus zur Punktaddition elliptischer Kurven mit projektiven Koordinaten. Eingabe und Ausgabe des Algorithmus müssen die Punkte mit affinen Koordinaten sein.

(c) Vergleichen Sie Punktaddtionsalgorithmen mit Hilfe einiger konkreten Beispiele im KASH3.

(8 Punkte)