Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Dr. Christopher Wolf
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 2

SS 2010

Blatt 3 / 12. Mai 2010 / Abgabe 31. Mai, 13:00 Uhr, Kasten NA 02

AUFGABE 1. ElGamal mal anders. (5 Punkte)
Betrachten Sie das folgende Public Key Verschlüsselungsverfahren. Der öffentliche Schlüssel $(\mathcal{G}, g, q, h)$ und der private Schlüssel x werden analog zur ElGamal Verschlüsselung generiert. Um ein Bit b zu verschlüsseln berechnet der Sender den Chiffretext folgendermaßen:

1. Falls $b = 0$ ist, dann wählt er $y \leftarrow_R \mathbb{Z}_q$ und berechnet $c = \langle c_1, c_2 \rangle = \langle g^y, h^y \rangle$.
2. Falls $b = 1$ ist, dann wählt er unabhängig gleichverteilt $y, z \leftarrow_R \mathbb{Z}_q$ und berechnet $c = \langle c_1, c_2 \rangle = \langle g^y, g^z \rangle$.

Zeigen Sie, dass mit Hilfe des privaten Schlüssels x eine effiziente Dechiffrierung Dec möglich ist (hierbei darf es zu Entschlüsselungsfehlern kommen, Sie sollten aber begründen, warum diese nur mit vernachlässigbarer Wahrscheinlichkeit auftreten). Beweisen Sie, dass das Verschlüsselungsschema CPA-sicher ist, falls das *Decisional Diffie Hellman Problem* schwer bzgl. der Gruppe $\mathcal{G}$ ist.

AUFGABE 2. Konstruktives. (5 Punkte)
Sei $\mathcal{G}$ ein Algorithmus der bei Eingabe 1^n eine n-bit Primzahl p, die multiplikative Gruppe $\mathbb{Z}_p^*$ und einen Generator g ausgibt. Zeigen Sie, dass die Schwierigkeit des *diskreten Logarithmus Problems* bezüglich einer von $\mathcal{G}$ ausgegebenen Gruppe die Existenz einer Familie von Einwegpermutationen impliziert, d.h. konstruieren Sie ein Tupel $\Pi = (\mathsf{Gen}, \mathsf{Samp}, f)$ gemäß Folie 57 und zeigen Sie die Einwegeigenschaft.

Die nächste Aufgabe benutzt sogenannte *längenerhaltende* Einwegfunktionen. Wir nennen $f : \{0,1\}^* \to \{0,1\}^*$ *längenerhaltend*, falls $|f(x)| = |x|$ für alle $x \in \{0,1\}^*$ gilt.

AUFGABE 3. Fehlkonstruktion. (10 Punkte)
Widerlegen Sie die folgende Aussage: Wenn f eine längenerhaltende Einwegfunktion ist, so ist auch $f'(x) := f(x) \oplus x$ eine (längenerhaltende) Einwegfunktion. Gehen Sie hierbei wie folgt vor:

a) Zeigen Sie, dass wenn g eine längenerhaltende Einwegfunktion ist, so ist auch $f(y,z) := (g(y) \oplus z, z)$ eine längenerhaltende Einwegfunktion (wobei y und z zwei Strings gleicher Länge sind).

Hinweis: Beim Nachweis der Einwegeigenschaft kann es hilfreich sein, zunächst die Mengengleichheit $f^{-1}(a,b) = g^{-1}(a \oplus b) \times \{b\}$ zu zeigen.

b) Benutzen Sie das in a) konstruierte f und betrachten Sie das entsprechende f'. Zeigen Sie, dass dieses f' keine Einwegfunktion sein kann.

AUFGABE 4. Harter Kern. (5 Punkte)
Betrachten Sie folgende Variante der Verschlüsselung mit Hilfe einer Familie von Trapdoor-Permutationen:

> Sei $\widehat{\Pi} = (\widehat{\mathsf{Gen}}, f)$ eine Familie von Trapdoor-Permutationen und hc ein Hardcore-Prädikat für $\widehat{\Pi}$. Wir konstruieren daraus ein Public Key Verschlüsselungsverfahren Π durch
>
> - Gen: Starte $(I, td) \leftarrow \widehat{Gen}(1^n)$, öffentlicher Schlüssel $pk \leftarrow I$, geheimer Schlüssel $sk \leftarrow td$.
> - Enc: Eingabe pk und $m \in \{0,1\}$. Wähle gleichverteiltes $x \leftarrow_R \mathcal{D}_I$ so dass $\mathsf{hc}_I(x) = m$ und gebe den Chiffretext $c = f_I(x)$ aus.
> - Dec: Eingabe sk und $c \in \mathcal{D}_I$. Berechne $x := f_I^{-1}(c)$ und gebe die Nachricht $\mathsf{hc}_I(x)$ zurück.

a) Warum kann die Verschlüsselung in (erwarteter) Polynomialzeit durchgeführt werden?

b) Zeigen Sie, dass falls $\widehat{\Pi}$ eine Familie von Trapdoor-Permutationen ist und hc ein Hardcore-Prädikat für $\widehat{\Pi}$, dann ist die Konstruktion CPA-sicher.