Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Eike Kiltz
Gottfried Herold

**Hausübungen zur Vorlesung**

# Kryptographie II

**SS 2012**

Blatt 2 / 26. April 2012 / Abgabe **bis spätestens Mittwoch, 09.05.2012 10:00 Uhr**

## AUFGABE 1:

Sei $\mathcal{G}(1^n)$ ein Algorithmus, der eine zyklische Gruppe $G$ der bekannten Ordnung $q$ und einen Generator $g$ für $G$ erzeugt. In der Vorlesung wurde gezeigt, dass ElGamal (bzgl. $\mathcal{G}$) CPA-sicher unter der DDH-Annahme für $\mathcal{G}$ ist. Zeigen Sie, dass diese Annahme auch notwendig ist, indem sie zeigen:
ElGamal bzgl. $\mathcal{G}$ ist CPA-sicher $\Rightarrow$ DDH-Annahme gilt bzgl. $\mathcal{G}$. [4 Punkte]

## AUFGABE 2:

Sei $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec})$ ein CPA-sicheres PK-Verschlüsselungsverfahren und $\Pi' = (\mathbf{Gen}', \mathbf{Enc}', \mathbf{Dec}')$ ein KPA-sicheres SK-Verschlüsselungsverfahren. Sei $\Pi^{\text{hy}}$ das resultierende hybride Verfahren (siehe Foliensatz 3 im Skript). Wir wollen den 1. (und analog 3.) Schritt der Beweisskizze (Skript S.35) formal beweisen.
Zeigen Sie hierzu [3 Punkte]:
Für jeden (Orakel-)ppt Algorithmus $(m_0, m_1, S) \leftarrow B^{\mathbf{Enc}^{\text{hy}}_{\text{pk}}}$ sind die Verteilungen

$$(\text{pk}, m_0, m_1, S, \mathbf{Enc}_{\text{pk}}(k), \mathbf{Enc}'_k(m_0))$$

und

$$(\text{pk}, m_0, m_1, S, \mathbf{Enc}_{\text{pk}}(0^n), \mathbf{Enc}'_k(m_0))$$

durch beliebige ppt Angreifer $A^{\mathbf{Enc}^{\text{hy}}_{\text{pk}}}$ mit Orakelzugriff auf $\mathbf{Enc}^{\text{hy}}_{\text{pk}}$ ununterscheidbar. Dabei sind die Verteilungen so definiert, dass
$(\text{pk}, \text{sk}) \leftarrow \mathbf{Gen}(1^n), k \leftarrow \mathbf{Gen}'(1^n)$ und $(m_0, m_1, S) \leftarrow B^{\mathbf{Enc}^{\text{hy}}_{\text{pk}}}(\text{pk})$.

Bemerkung: Im Gegensatz zum Vorlesungsskript sind hierbei $\text{pk}, m_0, m_1, S$ in der Verteilungen enthalten, was codiert, dass diese dem Angreifer bekannt sind. $B$ kodiert dabei die Wahl von $m_0, m_1$ durch den CPA-Angreifer und $S$ den internen Status des Angreifers nach dieser Wahl (siehe Präsenzübungsblatt 2). Die Orakel sind hierbei eigentlich unnötig, da $A$ und $B$ den public key kennen.

**AUFGABE 3:**

Zeigen Sie, dass padded RSA mit $l = 2$ *nicht* CCA-sicher ist: [5 Punkte]

Zur Erinnerung (siehe Skript S. 39): padded RSA mit $l = 2$ ist das folgendes PK-Verschlüsselungsverfahren:
**Gen** : $(N, e, d) \leftarrow \text{GenRSA}(1^n)$
**Enc** : Für $m \in \{0,1\}^2$ und $r \in_R \{0,1\}^{\log_2 N - 3}$ berechne $c \leftarrow (r \,||\, m)^e \bmod N$ und gib $c$ aus.
**Dec** : Berechne $c^d \bmod N$ und gib die untersten 2 Bits davon aus.

Hinweise:
Benutzen Sie die Malleability von Textbook RSA mit Faktor 2 und das CCA-Orakel. Das Problem, dass das CCA-Orakel nur die untersten 2 Bits von $c^d$ ausgibt, kann man umgehen, indem man ausnutzt, dass $2m_b \bmod N$ entweder $2m_b$ oder $2m_b - 1 \cdot N$ ist. Das 2. Bit, dass man wegen $l = 2$ hier zur Verfügung hat, kann benuzt werden, um zu entscheiden, welcher der Fälle eingetreten ist. Ggf. (nicht unbedingt nötig, kann aber die Analyse vereinfachen) kann man versuchen durch Verwendung weiterer CCA-Anfragen $N \bmod 4$ lernen.

**AUFGABE 4:**

Wir wollen zeigen, dass man aus einem 2-Runden-Schlüsselaustauschprotokoll stets ein PK-Verschlüsselungsverfahren konstruieren kann:
Sei $\Pi_K$ ein 2-Runden-Schlüsselaustauschprotokoll (d.h. es werden 2 Nachrichten gesendet, wobei o.B.d.A. die 1. Nachricht von Alice, die 2. Nachricht von Bob gesendet wird), dessen Schüsselraum $\mathcal{K}$ eine (durch den Sicherheitsparameter $n$ deterministisch festgelegte, öffentlich bekannte) *Gruppe* sei.
Wir können $\Pi_K$ stets schreiben als

| Alice(A) | | Bob(B) |
|---|---|---|
| $(\text{msg}_1, S) \leftarrow A_1(1^n)$ | | |
| | $\xrightarrow{\text{msg}_1}$ | |
| | | $(\text{msg}_2, k_\text{B}) \leftarrow B(\text{msg}_1, 1^n)$ |
| | $\xleftarrow{\text{msg}_2}$ | |
| $k_\text{A} \leftarrow A_2(S, \text{msg}_2)$ | | |
| Ausgabe $k_\text{A}$ | | Ausgabe $k_\text{B}$ |

mit ppt Algorithmen $A_1, A_2, B$, wobei gelten soll, dass $k_A = k_B \in \mathcal{K}$. Dabei dient $S$ zum Speichern des internen Status von Alice zwischen den Algorithmen $A_1$ und $A_2$, die sie nacheinander ausführt.
Konstruieren Sie aus $\Pi_K$ (d.h. aus $A_1, A_2, B$) ein PK-Verschlüsselungsverfahren $\Pi$ mit Nachrichtenraum $G$, zeigen Sie dessen Korrektheit und beweisen Sie, dass $\Pi$ CPA-sicher ist, wenn $\Pi_K$ sicher gegen passive Angriffe ist. [7 Punkte]

Hinweis: Beim DH-Schlüsselaustausch etwa ist $\mathcal{K} = G$ ein Gruppe mit festgelegtem Erzeuger $g$ (der in dieser Version der Einfachheit halber nicht jedesmal neu festgelegt wird), $\text{msg}_1 = g^x$, $S = x$, $\text{msg}_2 = g^y$ und $k_A, k_B = g^{xy}$. Versuchen Sie Ihre Konstruktion so zu wählen, dass, angewendet auf den DH-Schlüsselaustausch, ihre Konstruktion das ElGamal-Verschlüsselungsverfahren liefert.