Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 13 / 27./28. Januar 2014

AUFGABE 1:

Betrachten Sie folgende Variante der Goldwasser-Micali Verschlüsselung: $\mathsf{GenModulus}(1^n)$ liefert (N, p, q), der öffentliche Schlüssel ist N, der geheime Schlüssel ist (p, q). Um eine 0 zu verschlüsseln wählt der Sender n zufällige Elemente $c_1, \ldots, c_n \in_R \mathcal{QR}_N$. Um eine 1 zu verschlüsseln wählt der Sender n zufällige Elemente $c_1, \ldots, c_n \in_R \mathcal{J}_N^{+1}$. Der Chiffretext ist $c := (c_1, \ldots, c_n)$.

(a) Zeigen Sie, dass der Sender ein zufälliges Element aus $\mathcal{J}_N^{+1}$ in (erwarteter) Polynomialzeit erzeugen kann.

(b) Wie kann der Empfänger effizient den Chiffretext entschlüsseln? Mit welcher Wahrscheinlichkeit tritt dabei ein Entschlüsselungsfehler auf?

(c) Zeigen Sie, dass das Verfahren CPA-sicher ist, wenn die Quadratische Residuositätsannahme bzgl. $\mathsf{GenModulus}$ gilt.

AUFGABE 2:

Sei $\mathsf{GenModulus}$ wie aus der Vorlesung bekannt ein Algorithmus der eine *Blumzahl* $N = p \cdot q$ und die zugehörige Faktorisierung p, q liefert. Wir betrachten nun eine Rabin-Variante (Folie 103) des ROM-RSA Verfahren aus der Vorlesung (Folie 74). Sei $H : \mathcal{QR}_N \to \{0,1\}^{\ell(n)}$ ein Random Oracle. Wir konstruieren daraus wie folgt ein asymmetrisches Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ für Nachrichten $m \in \{0,1\}^{\ell(n)}$.

$\mathsf{Gen}(1^n)$: Berechne $(N, p, q) \leftarrow \mathsf{GenModulus}(1^n)$. Setze $\mathsf{pk} = N$ und $\mathsf{sk} = (p, q)$.

$\mathsf{Enc}_{\mathsf{pk}}(m)$: Wähle $r \in_R \mathcal{QR}_N$ und setze $c := (r^2 \bmod N, H(r) \oplus m)$.

(a) Geben Sie eine Entschlüsselungsfunktion an und zeigen Sie die Korrektheit.

(b) Zeigen Sie, dass im ROM Π CPA-sicher unter der Faktorisierungsannahme ist.

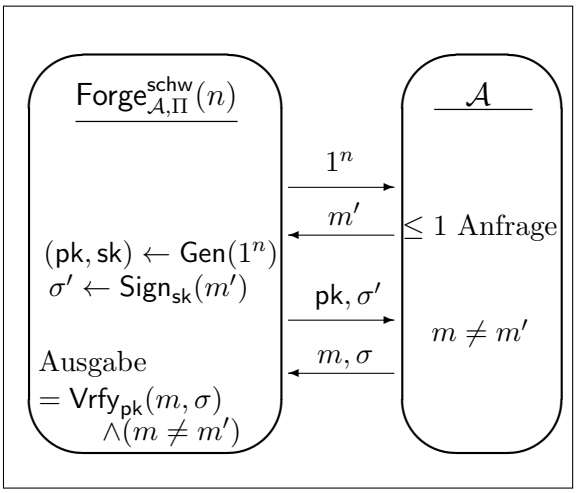
AUFGABE 3:

Sei $A_N := \{(a, 1) \in \mathbb{Z}_N \times \mathbb{Z}_N^* \mid a \in \mathbb{Z}_N\}$. Zeigen Sie, dass es *nicht* schwer ist zu unterscheiden, ob ein Element $y \in_R \mathbb{Z}_{N^2}^*$ oder $y \in_R A_N$ ist.

AUFGABE 4:

Wir definieren zunächst einen neuen Sicherheitsbegriff, der auch in der Hausaufgabe untersucht wird.

Definition: Ein Signaturverfahren $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ heißt *schwach* CMA-sichere *Einweg*signatur, falls für alle ppt-Angreifer $\mathcal{A}$ gilt $\mathsf{Ws}[\mathsf{Forge}^{\mathsf{schw}}_{\mathcal{A},\Pi}(n) = 1] \leq \mathsf{negl}(n)$.



Im Vergleich zur gewöhnlichen CMA-sicheren Einwegsignatur erhält der Angreifer $\mathcal{A}$ den öffentlichen Schlüssel folglich erst *nach* der Anfrage der Nachricht.

Wir betrachten zudem das folgende Signaturverfahren $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ mit Nachrichten- und Signaturraum $\mathbb{Z}_p$. Sei $\mathcal{G}$ ein Algorithmus, der eine Gruppe primer Ordnung p erzeugt.

$\mathsf{Gen}(1^n)$: $(g, p) \leftarrow \mathcal{G}(1^n)$, $x \in_R \mathbb{Z}_p^*$, $y \in_R \mathbb{Z}_p$, $u := g^x$, $v := g^y$, $\mathsf{pk} := (g, p, u, v)$, $\mathsf{sk} := (x, y)$.

$\mathsf{Sign}_{\mathsf{sk}}(m)$: Gib $\sigma := (y - m) \cdot x^{-1} \bmod p$ zurück.

$\mathsf{Vrfy}_{\mathsf{pk}}(m, \sigma)$: Falls $v = g^m \cdot u^\sigma$ gib eine 1 zurück, sonst eine 0.

(a) Zeigen Sie, dass Π korrekt ist.

(b) Zeigen Sie, dass Π eine schwach CMA-sichere Einwegsignatur ist, wenn das Diskrete Logarithmus Problem hart bzgl. $\mathcal{G}$ ist.

Hinweis: Wählen Sie in der Reduktion $u := g^x$ (wobei p, g, g^x die Eingabe des Unterscheiders ist) und wählen Sie v abhängig von der angefragten Nachricht, indem Sie die zugehörige Signatur uniform aus $\mathbb{Z}_p$ wählen. Der private Schlüssel ist dem Unterscheider damit nicht bekannt. Überlegen Sie, wie Sie schließlich mit Hilfe der ausgegebenen Nachricht m und ausgegebenen Signatur σ (zusammen mit m' und σ') das Diskrete Logarithmus Problem lösen.