

Kryptographie

Blatt 4, 06.05.2005, Abgabe 13.05.2005

Generische ElGamal Verschl. im ROM

Öffentlich $G = \langle g \rangle$, $|G| = q$, $h \in_R G$

$H \in_R (\{0, 1\}^n)^G$ sei durch ein Orakel gegeben

privat $x = \log_g h \in_R \mathbb{Z}_q$

Verschl.: von $m \in \{0, 1\}^n : r \in_R \mathbb{Z}_q, m \mapsto (g^r, m \oplus H(h^r)) = \text{cip}$

Entschl.: $\mathcal{D}_x(\text{cip}_1, \text{cip}_2) = (\text{cip}_2 \oplus H(\text{cip}_1^x))$

Aufgabe 1. Verallgemeinere den CCA-Angriff von der ElGamal-Verschl. auf die generische ElGamal-Verschl. Um ihn abzuwehren, lasse man nur Nachrichten m aus einer kleinen Teilmenge $M \subset \{0, 1\}^n$ zu und ändere \mathcal{D}_x entsprechend ab in \mathcal{D}'_x so dass $\mathcal{D}'_x(\text{cip}) = 0$ falls $\mathcal{D}_x(\text{cip}) \notin M$. Diskutiere die Sicherheit gegen CCA-Angriffe. Wie klein muss $|M|/2^n$ sein?

Aufgabe 2. Zeige, dass für die generische ElGamal-Verschl. die Aufgabe zu gegebenem m gültige von ungültigen Ziffertexten von m zu unterscheiden, so schwierig ist wie DDH: $\text{DDH} \leq_{\text{pol}} \text{IND}$.

Aufgabe 3. Sie sollen zu $a_1, a_2, a_3 \in [0, 2^{100}[$ und $g \in G \mapsto g^{a_1}, g^{a_2}, g^{a_3}$ mit möglichst wenigen Mult./Quad. nach Lim-Lee berechnen. Welche Variante wählen Sie für $\leq 7, 15, 31$ vorberechnete Elementen in G ? Die Vorbereitung sei kostenlos.

Aufgabe 4. Bestimme die Ordnung von $E_{1,b}(\mathbb{Z}_q)$ für alle $b \in \mathbb{Z}_q$ für $q = 13$. Gehe geschickt vor und erläutere die Vorgehensweise. Warum ist die Ordnung im Mittel $q + 1 = 14$?