Institut für Theoretische Informatik
Prof. Dr. Dennis Hofheinz
Übungsleiter: Thomas Agrikola

Stammvorlesung Sicherheit im Sommersemester 2017

Übungsblatt 4

Aufgabe 1. Wir instanziieren das ElGamal-Verschlüsselungsverfahren aus der Vorlesung über einer Untergruppe $\mathbb{G}$ der Gruppe $\mathbb{Z}_{59}^\times$ (die Gruppenoperation ist die Multiplikation modulo 59). $\mathbb{G}$ sei dabei die Untergruppe der Quadrate. Wir wählen als Erzeuger von $\mathbb{G}$ das Element $g := 27$ (Sie müssen nicht beweisen, dass g ein Erzeuger ist). Der Einfachheit halber sei der geheime Schlüssel sk in dieser Aufgabe direkt der geheime Exponent und der öffentliche Schlüssel $pk = g^{sk}$. (In der Vorlesung enthielten die Schlüssel jeweils noch die Gruppe $\mathbb{G}$ und g.)

(a) Berechnen Sie zum geheimen Schlüssel $sk := 20$ den öffentlichen Schlüssel pk.

(b) Berechnen Sie das Chiffrat c zur Nachricht $m := 22$ unter dem in (a) berechneten Schlüssel pk, wobei Sie $r := 12$ als Zufall verwenden.

(c) Es sei $c := (51, 8)$ ein Chiffrat. Verwenden Sie den geheimen Schlüssel aus (a), um die als Gruppenelement codierte Nachricht $m \in \mathbb{G}$ zu berechnen.

Hinweis: Versuchen Sie, sich die Rechenregeln der Modulo-Arithmetik und für endliche Gruppen zunutze zu machen. Sie sollten dann in der Lage sein, diese Aufgabe größtenteils „im Kopf“ zu lösen.

Zur Erinnerung: Die verwendete Gruppenoperation ist die Multiplikation modulo 59. $\mathbb{Z}_{59}^\times$ ist die Einheitengruppe von $\mathbb{Z}_{59}$ (d.h. die Gruppe der invertierbaren Elemente). Da 59 eine Primzahl ist, gilt $\mathbb{Z}_{59}^\times = \mathbb{Z}_{59} \setminus \{0\}$. Die Ordnung von $\mathbb{Z}_{59}^\times$ ist 58 (Warum?). Die Untergruppe der Quadrate von $\mathbb{Z}_{59}^\times$ besteht aus den Elementen $\{x^2 \bmod 59 \colon x \in \mathbb{Z}_{59}^\times\}$ von $\mathbb{Z}_{59}^\times$ und hat Ordnung 29. Die Gruppenoperation einer Untergruppe ist identisch zur Gruppenoperation der Obergruppe.

Aufgabe 2. Wir wollen uns damit beschäftigen, wie geeignet die in Aufgabe 1 verwendete Gruppe $\mathbb{Z}_{59}^\times$, beziehungsweise generell Gruppen der Art $\mathbb{Z}_p^\times$ für eine Primzahl $p > 2$, für ElGamal sind. Wir nennen

$$Q(\mathbb{G}) := \{x^2 : x \in \mathbb{G}\}$$

die *Menge der Quadrate* in der Gruppe $\mathbb{G}$. In Gruppen $\mathbb{Z}_p^\times$ lässt sich die Zugehörigkeit zu $Q(\mathbb{Z}_p^\times)$ effizient prüfen: Ist $y^{\frac{p-1}{2}} \bmod p = 1$, so ist $y \in Q(\mathbb{Z}_p^\times)$; andernfalls nicht.

Wie können wir uns die Eigenschaften von Quadraten in $\mathbb{Z}_p^\times$ zunutze machen, um einen erfolgreichen Angreifer auf die IND-CPA-Sicherheit von ElGamal über $\mathbb{Z}_p^\times$ zu konstruieren? Beschreiben Sie ein möglichst realistisches Szenario, in dem ein solcher Angriff nützlich ist.

Hinweise: $Q(\mathbb{Z}_p^\times)$ ist eine Untergruppe von $\mathbb{Z}_p^\times$ und daher insbesondere abgeschlossen unter Multiplikation. Was lässt sich für $x \cdot y$ mit $x \in Q(\mathbb{Z}_p^\times)$ und $y \in (\mathbb{Z}_p^\times \setminus Q(\mathbb{Z}_p^\times))$ über die Zugehörigkeit zu $Q(\mathbb{Z}_p^\times)$ sagen? $Q(\mathbb{Z}_p^\times)$ enthält für $p > 2$ genau $|\mathbb{Z}_p^\times|/2 = (p-1)/2$ Elemente.

Aufgabe 3. Es sei $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ ein EUF-CMA-sicheres Signaturverfahren. Wir verwenden die Algorithmen von Σ um zwei weitere Signaturverfahren zu konstruieren:

(1.) Betrachten Sie das Signaturverfahren Σ' mit den folgenden Algorithmen:

- $\mathsf{Gen}'(1^k) := \mathsf{Gen}(1^k)$,

- $\mathsf{Sig}'(sk, M) := (\mathsf{Sig}(sk, M \oplus r), r) = (\sigma_1, \sigma_2)$, wobei r ein zufällig gezogener Bitstring mit $|r| = |M|$ ist,
- $\mathsf{Ver}'(pk, M, \sigma) = \mathsf{Ver}'(pk, M, (\sigma_1, \sigma_2)) := \mathsf{Ver}(pk, M \oplus \sigma_2, \sigma_1)$.

(a) Zeigen Sie die Korrektheit von Σ', d.h. zeigen Sie, dass Ver' Signaturen die mit Sig' erstellt wurden, korrekt verifiziert.

(b) Zeigen Sie, dass Σ' nicht EUF-CMA-sicher ist.

(2.) Betrachten Sie das Signaturverfahren Σ^* mit den folgenden Algorithmen:

- $\mathsf{Gen}^*(1^k) := \mathsf{Gen}(1^k)$,
- $\mathsf{Sig}^*(sk, M) := \mathsf{Sig}(sk, \overline{M})$ (wobei $\overline{M}$ das bitweise Inverse von M ist),
- $\mathsf{Ver}^*(pk, M, \sigma) = \mathsf{Ver}(pk, \overline{M}, \sigma)$

(a) Zeigen Sie die Korrektheit von Σ^*.

(b) Zeigen Sie, dass Σ^* EUF-CMA-sicher ist.

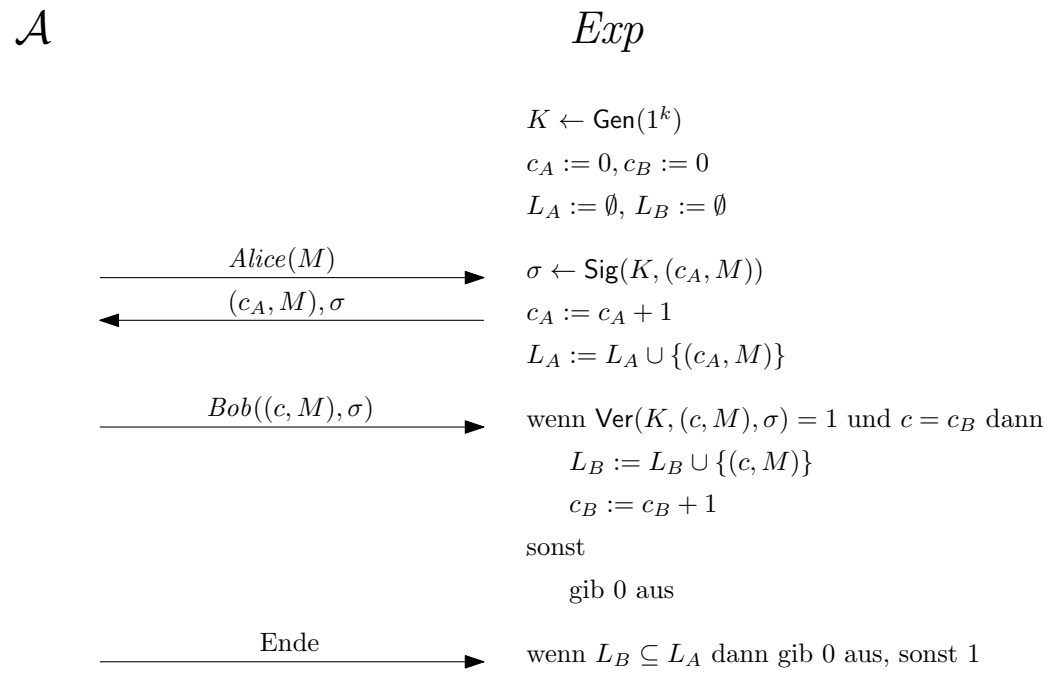

Abbildung 1: Sicherheitsexperiment für einen authentifizierten Kanal.

Aufgabe 4. Es sei $\mathsf{MAC} = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ ein MAC-Verfahren. Wir wollen MAC benutzen, um einen authentifizierten Kanal zwischen zwei Parteien $A(lice)$ und $B(ob)$ zu realisieren. (Genau genommen betrachten wir der Einfachheit halber nur Nachrichten, die von A an B geschickt werden). Wir gehen davon aus, dass A und B bereits einen gemeinsamen Schlüssel K ausgetauscht haben. Die Sicherheit des Kanals beschreiben wir mit dem Spiel in Abbildung 1: Das Experiment generiert zunächst einen Schlüssel K und initialisiert Zähler c_A, c_B für die Parteien A und B sowie Listen der akzeptierten Nachrichten L_A und L_B. Der Angreifer kann nun (polynomiell oft) eine der folgenden Anfragen stellen:

- $Alice(M)$: Der Angreifer kann Alice eine Nachricht M schicken lassen. Alice signiert das Paar aus Nachricht und ihrem aktuellen Zähler. Das Zähler/Nachrichten-Paar wird der Liste L_A der von Alice geschickten Nachrichten hinzugefügt und der Zähler c_A hochgezählt.
- $Bob((c, M), \sigma)$. Der Angreifer kann Bob ein Zähler/Nachrichten-Paar (c, M) und eine Signatur σ empfangen lassen. Bob prüft Signatur und Zählerstand. Ist beides valide, fügt er das Zähler/Nachrichten-Paar der Liste seiner empfangenen Nachrichten hinzu und zählt seinen Zähler hoch. Ansonsten bricht das Experiment mit 0 ab (der Angreifer verliert).
- *Ende*: Der Angreifer beendet das Experiment. Sind die Nachrichten, die Bob akzeptiert hat, eine Untermenge der Nachrichten, die Alice geschickt hat, so verliert der Angreifer (0-Ausgabe). Ansonsten gewinnt er (1-Ausgabe).

Beweisen Sie, dass kein Angreifer das beschriebene Spiel für ein EUF-CMA-sicheres MAC-Verfahren MAC mit nicht-vernachlässigbarer Wahrscheinlichkeit gewinnen kann. Geben Sie hierzu an, wie Sie einen Angreifer $\mathcal{A}$ für das Spiel in Abbildung 1 benutzen können, um einen Angreifer $\mathcal{B}$ für das EUF-CMA-Spiel zu konstruieren. Hierbei sollte $\mathcal{B}$ nicht-vernachlässigbaren Erfolg haben, sofern $\mathcal{A}$ nicht-vernachlässigbaren Erfolg hat.

Diese Konstruktion eines authentifizierten Kanals aus einem MAC unter Zuhilfenahme von Zählern ist in der Praxis üblich und wird (sehr ähnlich) beispielsweise in Transport-Layer-Security-Verschlüsselungsprotokoll (TLS-Protokoll) verwendet. Überlegen Sie sich, warum ein Zähler eingeführt und mit der Nachricht authentifiziert wird.