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

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 6 / 10. Januar 2011 / Abgabe 24. Januar, 16 Uhr, Kasten NA 02

AUFGABE 1. Geburtstagsparadoxon. (5 Punkte)
Betrachten Sie den Geburtstagsangriff auf beliebige Hashfunktionen H_s (siehe Folie 125). Beweisen Sie, dass für $q = 2^{\ell/2} + 1$ mit Wahrscheinlichkeit $\geq 1 - \exp(-\frac{1}{2})$ eine Kollision $H(x_i) = y_i = y_j = H(x_j)$ mit $x_i \neq x_j$ gefunden wird.

Hinweis: Sie dürfen hierbei H_s durch eine Zufallsfunktion modelieren, d.h. betrachten Sie die Menge $Y = \{y_1, \ldots, y_q\}$ mit $y_i \in_R \{0,1\}^\ell$ und definieren Sie Zufallsvariablen

$$Y_{ij} = \begin{cases} 1 & \text{falls } y_i = y_j \\ 0 & \text{sonst} \end{cases}$$

für alle $1 \leq i < j \leq q$. Berechnen Sie dann $\mathbf{Ws}\left[\sum_{1 \leq i < j \leq q} Y_{ij} \geq 1\right]$. Hierbei ist die Abschätzung $\exp(-1) \geq (1 - \frac{1}{n})^n$ für jedes $n \geq 1$ nützlich.

AUFGABE 2. Merkle-Damgard Variation.
Betrachten Sie folgende Variante der Merkle-Damgard Konstruktion (siehe Folie 126). Anstelle von $z_{B+1} = h_s(z_B||x_{B+1}) = h_s(z_B||L)$ gib nun direkt $z_B||L$ aus. Ist die Konstruktion weiterhin kollisionsresistent? Welchen Nachteil hat die Konstruktion?

AUFGABE 3. MAC Schreck. (5 Punkte)
Sei $(\widetilde{\mathsf{Gen}}, H)$ eine kollisionsresistente Hashfunktion, welche mittels Merkle-Damgard Transformation konstruiert wurde. Betrachte folgenden MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$.

- $\mathsf{Gen}(1^n)$ berechnet (s, k) mit $s \leftarrow \widetilde{Gen}(1^n)$ und $k \in_R \{0,1\}^n$.
- $\mathsf{Mac}_{s,k}(m)$ gibt den Tag $t = H_s^k(m)$ aus, d.h. $z_0 := k$ wird als Initialisierungsvektor in der Merkle-Damgard Transformation benutzt.
- $\mathsf{Vrfy}_{s,k}(m, t)$ gibt 1 aus genau dann, wenn $t = H_s^k(m)$ gilt.

Zeigen Sie, dass Π nicht sicher ist. Gehen Sie hierbei davon aus, dass s öffentlich, d.h. dem Angreifer bekannt ist.

Exkurs: Gitter

In der nächsten Aufgabe wollen wir eine konkrete Hashfunktion untersuchen, die auf dem sogenannten *kürzeste Vektoren Problem*, kurz SVP, aus der Gittertheorie basiert. Hierzu betrachte die Menge

$$\Gamma_q(\mathbf{S}) := \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{S}\mathbf{y} = \mathbf{0} \in \mathbb{Z}_q^n\}$$

für eine Matrix $\mathbf{S} \in \mathbb{Z}_q^{n \times m}$. Diese Menge ist ein *Gitter*. Das zugehörige SVP-Problem lautet wie folgt:

Definition 1. Das *kürzeste Vektoren Problem* mit Parametern n, m, q besteht darin, zur Eingabe $\mathbf{S}$ einen kurzen Vektor $\mathbf{y} \in \Gamma_q(\mathbf{S})$ zu finden, d.h. einen Vektor mit (relativ) kleiner Norm $||\mathbf{y}||_1 := \sum_{i=1}^m |y_i| \leq m$.

Sei nun $\mathbf{S} \in_R \mathbb{Z}_q^{n \times m}$ eine zufällige Matrix mit vollem Rang $\text{rank}(\mathbf{S}) = n$. Im Folgenden nehmen wir an, das das zugehörige SVP mit folgenden Parametern *hart* ist, d.h. das kein ppt-Algorithmus zur Eingabe $\mathbf{S}$ einen kurzen Vektor $\mathbf{y}$ berechnen kann.

Annahme 1. Für Parameter n und $m = 2n \log_2 q$ sowie $q = n^2$ ist das SVP-Problem für zufälliges $\mathbf{S}$ (mit vollem Rang) hart.

Basierend auf dieser Annahme wollen wir nun eine (beweisbar) kollisionsresistente Hashfunktion konstruieren.

AUFGABE 4. Gitterbasierte Hashfunktion. (5 Punkte)
Für Parameter n und $m = 2n \log_2 q$ sowie $q = n^2$ betrachte die Hashfunktion (Gen, H) mit $H : \{0,1\}^m \to \mathbb{Z}_q^n$ definiert durch

- $\mathsf{Gen}(1^n)$ gibt zufälliges $\mathbf{S} \in \mathbb{Z}_q^{n \times m}$ mit vollem Rang aus.
- $H_{\mathbf{S}} : \{0,1\}^m \to \mathbb{Z}_q^n$ via $\mathbf{x} \mapsto \mathbf{S}\mathbf{x} \mod q$.

a) Zeigen Sie, dass (Gen, H) für die obigen Parameter eine Kompressionsfunktion ist.

b) Zeigen Sie, dass (Gen, H) kollisionsresistent ist, sofern Annahme 1 gilt. Konstruieren Sie hierzu aus einem Algorithmus $\mathcal{A}$, der Kollisionen für $H_{\mathbf{S}}$ berechnet, einen Algorithmus $\mathcal{A}'$, welcher kurze Vektoren in $\Gamma_q(\mathbf{S})$ findet.