Prof. C. P. Schnorr Sommersemester 2016

Gitter und Kryptographie

Blatt 8, 10.06.2016, Abgabe 17.06.2016

Identifikation $(P,V)_{\mathrm{MV}}$

(geh. Schl. $\mathbf{w}$ mit $||\mathbf{Bw}-\mathbf{y}|| \le t$, $\mathbf{u}=\mathbf{y}-\mathbf{Bw}$, $(\mathbf{B},\mathbf{y},t)$ ist JA - Instanz)

1. $\mathcal{P}$ wählt $\mathbf{r}_i \in_R \mathcal{B}_m(\mathbf{0},\gamma t/2-t)\cap\mathbb{Z}^m$ für $i=1,...,k$ verschiebt $\mathbf{r}_i$ zu $\mathbf{m}_i := \mathbf{r}_i+\mathbf{Bv}_i \in P(\mathbf{B})$ (Grundmasche) und sendet $\mathbf{m}_1,...,\mathbf{m}_k$ an $\mathcal{V}$.

2. $\mathcal{V}$ sendet $\mathbf{q}=(q_1,\ldots,q_k)\in_R\{0,1\}^k$

3. $\mathcal{P}$ sendet für $i=1,\ldots,k$: den Vektor $\mathbf{Bv}_i - q_i(\mathbf{u}+\mathbf{y})$

4. $\mathcal{V}$ akzeptiert wenn $||\mathbf{m}_i-\mathbf{Bv}_i+q_i(\mathbf{u}+\mathbf{y})-q_i\mathbf{y}|| \le \gamma t/2$ für $i=1,\ldots,k$.

Korrektheit: $\mathcal{V}$ akzeptiert immer, wenn $\mathcal{P}$ dem Protokoll folgt.

Aufgabe 1: Der triviale $\mathcal{P}^*$ hat mit Ws 2^{-k} Erfolg, indem er $\mathbf{q}=(q_1,\ldots,q_k)$ errät und $\mathbf{m}_1,\ldots,\mathbf{m}_k$ "entsprechend" bestimmt. Die Ws bezieht sich auf die Zufallsbits von $\mathcal{P}^*$.

Aufgabe 2. Angenommen $\mathcal{P}^*$ kennt zu $\mathbf{m}_i$ Werte $\mathbf{v}_{i,q}\in\mathbb{Z}^n$ so dass $||\mathbf{m}_i-\mathbf{Bv}_{i,q}-q\mathbf{y}|| \le \gamma t/2$ für $q\in\{0,1\}$. Dann gilt $||\mathbf{Bv}_{i,0}-\mathbf{Bv}_{i,1}-\mathbf{y}|| \le \gamma t$.

Aufgabe 3. Skizziere einen Extraktor $\mathrm{AL}^{\mathcal{P}^*}$ zum pol.- Zeit $\mathcal{P}^*$ von Aufgabe 2. P^* bestehe mit Ws $\frac{1}{2}(1+\varepsilon)$ für beide $q_i\in\{0,1\}$ den Test $||\mathbf{m}_i-\mathbf{Bv}_i+q_i(\mathbf{u}+\mathbf{y})|| \le \gamma t/2$. Zeige dass $\mathrm{AL}^{\mathcal{P}^*}$ die von P^* in Schritt 3 gesendeten erfolgreichen Werte $\mathbf{Bv}_{i,q_i}-q_i(\mathbf{u}+\mathbf{v})$ für beide $q_i=0,1$ und ein geeignetes $i, 1\le i\le k$ extrahiert so dass $||\mathbf{Bv}_{i,0}-\mathbf{Bv}_{i,1}-\mathbf{y}|| \le \gamma t$.

Punktzahl pro Aufgabe 1, 2, 3 : 4, 4, 6

Korrektheit von $(P,V)_{\mathrm{MV}}$**:** $||\mathbf{m}_i-\mathbf{Bv}_i+q_i(\mathbf{u}+\mathbf{y})-q_i\mathbf{y}|| = ||\mathbf{m}_i-\mathbf{m}_i+\mathbf{r}_i+q_i\mathbf{u}|| \le ||\mathbf{r}_i||+||\mathbf{u}|| \le \gamma t/2-t+t=\gamma t/2$