פתרון תרגיל מספר 1 ־ מבוא לקריפטוגרפיה ואבטחת תוכנה

שם: מיכאל גרינבאום, **ת.ז:** 211747639

18 במאי 2022

1. **צ"ל:** Π היא בעלת סודיות מושלמת אס"ם לכל התפלגות מרחב ההודעות M מעל $\mathcal{M}$ והודעה $m \in \mathcal{M}$ כך ש־ $\mathbb{P}\left(M=m\right)>0$ ו־ $c \in \mathcal{C}$ מתקיים $\mathbb{P}\left(C=c \mid M=m\right)=\mathbb{P}\left(C=c\right)$

הוכחה:

תהי $\Pi=\left(Keygen, Enc, Dec\right)$, נסמן ב־ M משתנה מקרי של ההודעות וב־ C משתנה מקרי של ההצפנות, נוכיח כל כיוון בנפרד:

$\Leftarrow$: נניח כי Π היא בעלת סודיות מושלמת.

תהי $m \in \mathcal{M}$ הודעה כך ש־ $\mathbb{P}\left(M=m\right)>0$, ויהי $c \in \mathcal{C}$:

(א) אם $\mathbb{P}\left(C=c\right)>0$: נשים לב כי $\mathbb{P}\left(M=m \mid C=c\right)=\mathbb{P}\left(M=m\right)$ מכך ש־ Π בעלת סודיות מושלמת ולכן

$$\mathbb{P}\left(C=c \mid M=m\right)=\frac{\mathbb{P}\left(M=m \mid C=c\right)\cdot\mathbb{P}\left(C=c\right)}{\mathbb{P}\left(M=m\right)}=\frac{\mathbb{P}\left(M=m\right)\cdot\mathbb{P}\left(C=c\right)}{\mathbb{P}\left(M=m\right)}=\mathbb{P}\left(C=c\right)$$

(ב) אחרת, מתקיים כי $\mathbb{P}\left(C=c\right)=0$ ולכן

$$0 \le \mathbb{P}\left(C=c \mid M=m\right)=\frac{\mathbb{P}\left(M=m \mid C=c\right)\cdot\mathbb{P}\left(C=c\right)}{\mathbb{P}\left(M=m\right)}=0$$
$$\Rightarrow \boxed{\mathbb{P}\left(C=c \mid M=m\right)=0=\mathbb{P}\left(C=c\right)}$$

כלומר קיבלנו כי לכל התפלגות M מעל $\mathcal{M}$, הודעה $m \in \mathcal{M}$ כך ש־ $\mathbb{P}\left(M=m\right)>0$ ו־ $c \in \mathcal{C}$ מתקיים $\mathbb{P}\left(C=c \mid M=m\right)=\mathbb{P}\left(C=c\right)$, כנדרש!

$\Rightarrow$: נניח כי לכל התפלגות M מעל $\mathcal{M}$, הודעה $m \in \mathcal{M}$ כך ש־ $\mathbb{P}\left(M=m\right)>0$ ו־ $c \in \mathcal{C}$ מתקיים $\mathbb{P}\left(C=c \mid M=m\right)=\mathbb{P}\left(C=c\right)$

תהי $m \in \mathcal{M}$ הודעה ויהי $c \in \mathcal{C}$ כך ש־ $\mathbb{P}\left(C=c\right)>0$:

(א) אם $\mathbb{P}\left(M=m\right)>0$: נשים לב כי $\mathbb{P}\left(C=c \mid M=m\right)=\mathbb{P}\left(C=c\right)$ מההנחה ולכן

$$\mathbb{P}\left(M=m \mid C=c\right)=\frac{\mathbb{P}\left(C=c \mid M=m\right)\cdot\mathbb{P}\left(M=m\right)}{\mathbb{P}\left(C=c\right)}=\frac{\mathbb{P}\left(C=c\right)\cdot\mathbb{P}\left(M=m\right)}{\mathbb{P}\left(C=c\right)}=\mathbb{P}\left(M=m\right)$$

(ב) אחרת, מתקיים $\mathbb{P}\left(M=m\right)=0$ ולכן

$$0 \le \mathbb{P}\left(M=m \mid C=c\right)=\frac{\mathbb{P}\left(C=c \mid M=m\right)\cdot\mathbb{P}\left(M=m\right)}{\mathbb{P}\left(C=c\right)}=0$$
$$\Rightarrow \boxed{\mathbb{P}\left(M=m \mid C=c\right)=0=\mathbb{P}\left(M=m\right)}$$

כלומר קיבלנו כי לכל התפלגות M מעל $\mathcal{M}$, הודעה $m\in\mathcal{M}$ ו־ $c\in\mathcal{C}$ כך ש־ $0<\mathbb{P}\left(C=c\right)$ מתקיים $\mathbb{P}\left(M=m\mid C=c\right)=$ $\mathbb{P}\left(M=m\right)$.
כלומר Π בעלת סודיות מושלמת מההגדרה, כנדרש

מ.ש.ל.☺

2. **צ"ל:** כל הצפנה בעלת סודיות מושלמת Π היא בלתי־ניתנת לאבחנה

הוכחה:
יהי $\mathcal{A}$ אלגוריתם PPT, נסמן את המשתנים המקריים של ההודעות m_0,m_1 ב־ M_0,M_1 וב־ M את ההודעה שנבחרה וב־ K את המשנה המקרי של המפתחות, נגדיר משתנה מקרי $C=Enc\left(K,M\right)$
נשים לב כי בשאלה 1 הוכחנו כי אם Π בעלת סודיות מושלמת אז

$$\mathbb{P}\left(C=c\mid M=m_0\right)=\mathbb{P}\left(C=c\mid M=m_1\right)$$

לכן

$$\begin{aligned}
&\mathbb{P}\left(\mathcal{A}\left(Enc\left(K,M_0\right)\right)=1\right)\\
=&\sum_{m_0,m_1\in\mathcal{M}_n}\mathbb{P}\left(M_0=m_0\wedge M_1=m_1\right)\cdot\mathbb{P}\left(\mathcal{A}\left(C\right)=1\mid M=m_0\right)\\
=&\sum_{m_0,m_1\in\mathcal{M}_n}\mathbb{P}\left(M_0=m_0\wedge M_1=m_1\right)\cdot\left[\sum_{c\in\mathcal{C}_n}\mathbb{P}\left(C=c\mid M=m_0\right)\cdot\mathbb{P}\left(\mathcal{A}\left(c\right)=1\right)\right]\\
=&\sum_{m_0,m_1\in\mathcal{M}_n}\mathbb{P}\left(M_0=m_0\wedge M_1=m_1\right)\cdot\left[\sum_{c\in\mathcal{C}_n}\mathbb{P}\left(C=c\mid M=m_1\right)\cdot\mathbb{P}\left(\mathcal{A}\left(c\right)=1\right)\right]\\
=&\sum_{m_0,m_1\in\mathcal{M}_n}\mathbb{P}\left(M_0=m_0\wedge M_1=m_1\right)\cdot\mathbb{P}\left(\mathcal{A}\left(C\right)=1\mid M=m_1\right)\\
=&\mathbb{P}\left(\mathcal{A}\left(Enc\left(K,M_1\right)\right)=1\right)
\end{aligned}$$

לכן

$$\begin{aligned}
&\mathbb{P}\left[IND_{\Pi,\mathcal{A}}\left(n\right)=1\right]=\Pr_{b\leftarrow\{0,1\}}\left[\mathcal{A}\left(Enc\left(K,M_b\right)\right)=b\right]\\
=&\frac{1}{2}\cdot\left[\mathbb{P}\left(\mathcal{A}\left(Enc\left(K,M_0\right)\right)=0\right)+\mathbb{P}\left(\mathcal{A}\left(Enc\left(K,M_1\right)\right)=1\right)\right]\\
=&\frac{1}{2}\cdot\left[\left[1-\mathbb{P}\left(\mathcal{A}\left(Enc\left(K,M_0\right)\right)=1\right)\right]+\mathbb{P}\left(\mathcal{A}\left(Enc\left(K,M_1\right)\right)=1\right)\right]\\
=&\frac{1}{2}+\frac{1}{2}\cdot\left[\mathbb{P}\left(\mathcal{A}\left(Enc\left(K,M_1\right)\right)=1\right)-\mathbb{P}\left(\mathcal{A}\left(Enc\left(K,M_0\right)\right)=1\right)\right]\\
=&\frac{1}{2}+\frac{1}{2}\cdot 0=\frac{1}{2}
\end{aligned}$$

תהי ν פונקציה זניחה אזי $\mathbb{P}\left[IND_{\Pi,\mathcal{A}}\left(n\right)=1\right]=\frac{1}{2}<\frac{1}{2}+\nu\left(n\right)$ ולכן הראנו כי לכל יריב PPT שנסמנו $\mathcal{A}$ קיימת פונקציה זניחה ν כך ש $\mathbb{P}\left[IND_{\Pi,\mathcal{A}}\left(n\right)=1\right]\leq\frac{1}{2}+\nu\left(n\right)$,
כלומר Π היא בלתי ניתנת לאבחנה, ובפרט OTP היא בלתי ניתנת לאבחנה כי היא בעלת סודיות מושלמת.

מ.ש.ל.☺

3. **צ"ל:** לכל פולינום $p\left(n\right)$ ולכל פונקציה זניחה $\nu\left(n\right)$ מתקיים כי $p\left(n\right)\cdot\nu\left(n\right)$ זניחה

הוכחה:
יהי $q\left(n\right)$ פולינום,

נשים לב כי $p(n)\cdot q(n)$ הוא פולינום (מכפלת פולינומים היא פולינום)
נשים לב כי $\nu(n)$ זניחה ולכן קיים $N\in\mathbb{N}$ כך שלכל $n\geq N$ מתקיים

$$0\leq\nu(n)\leq\frac{1}{p(n)\cdot q(n)}\Rightarrow\boxed{p(n)\cdot\nu(n)\leq\frac{1}{q(n)}}$$

כלומר הראנו שלכל פולינום $q(n)$ קיים $N\in\mathbb{N}$ כך שלכל $n\geq N$ מתקיים

$$p(n)\cdot\nu(n)\leq\frac{1}{q(n)}$$

ולכן מההגדרה מתקיים כי $p(n)\cdot\nu(n)$ זניחה

מ.ש.ל.☺

4. **צ"ל:** קיים D לא פולינומי כך ש־ $\left|\Pr_{s\leftarrow\{0,1\}^n}\left[D\left(G\left(s\right)\right)=1\right]-\Pr_{r\leftarrow\{0,1\}^{l(n)}}\left[D\left(r\right)=1\right]\right|\geq\frac{1}{2}$
הוכחה:
יהי G PRG.
יהי $r\in\{0,1\}^{l(n)}$ קלט, נגדיר D באופן הבא:

(א) החזר 1 אם קיים $s\in\{0,1\}^n$ כך ש־ $r=G(s)$
(ב) אחרת תחזיר 0

נשים לב כי D צריך לבדוק 2^n אפשרויות שונות ל־ s בשביל להחזיר 1 או 0, ולכן D רץ בזמן אקפוננציאלי.
בנוסף לכך, תחילה נשים לב כי $\left|\{G(s)\mid s\in\{0,1\}^n\}\right|\leq2^n$ כי לכל פונקציה מתקיים שגודל התמונה שלה קטן או גודל תחום ההגדרה ולכן $\left|\{G(s)\mid s\in\{0,1\}^n\}\right|\leq\left|\{0,1\}^n\right|=2^n$
בנוסף לכך נשים לב כי $\underset{r\leftarrow\{0,1\}^{l(n)}}{\mathbb{P}}\left[\exists s'\in\{0,1\}^n\text{ s.t. }r=G(s')\right]$ זה בדיוק מה הסיכוי לבחור איבר מהתמונה של G מכל האיברים ב־ $\{0,1\}^{l(n)}$, כלומר:

$$\underset{r\leftarrow\{0,1\}^{l(n)}}{\mathbb{P}}\left(\exists s'\in\{0,1\}^n\text{ s.t. }r=G(s')\right)=\frac{\left|\{G(s)\mid s\in\{0,1\}^n\}\right|}{\left|\{0,1\}^{l(n)}\right|}$$

עתה נשתמש ב2 האבחנות האלה ונקבל:

$$\begin{aligned}
&\left|\underset{s\leftarrow\{0,1\}^n}{\Pr}\left[D\left(G(s)\right)=1\right]-\underset{r\leftarrow\{0,1\}^{l(n)}}{\Pr}\left[D(r)=1\right]\right|\\
=&\left|\underset{s\leftarrow\{0,1\}^n}{\Pr}\left[\exists s'\in\{0,1\}^n\text{ s.t. }G(s)=G(s')\right]-\underset{r\leftarrow\{0,1\}^{l(n)}}{\Pr}\left[\exists s'\in\{0,1\}^n\text{ s.t. }r=G(s')\right]\right|\\
=&\left|1-\underset{r\leftarrow\{0,1\}^{l(n)}}{\Pr}\left[\exists s'\in\{0,1\}^n\text{ s.t. }r=G(s')\right]\right|\\
\overset{\star}{=}&1-\underset{r\leftarrow\{0,1\}^{l(n)}}{\Pr}\left[\exists s'\in\{0,1\}^n\text{ s.t. }r=G(s')\right]=1-\frac{\left|\{G(s)\mid s\in\{0,1\}^n\}\right|}{\left|\{0,1\}^{l(n)}\right|}\\
=&1-\frac{\left|\{G(s)\mid s\in\{0,1\}^n\}\right|}{2^{l(n)}}\geq1-\frac{2^n}{2^{l(n)}}\overset{l(n)\geq n+1}{\geq}1-\frac{2^n}{2^{n+1}}=1-\frac{1}{2}=\frac{1}{2}
\end{aligned}$$

נשים לב כי $\star$ מתקיים כי $\Pr_{r\leftarrow\{0,1\}^{l(n)}}\left[\exists s'\in\{0,1\}^n\text{ s.t. }r=G(s')\right]\leq1$ (נכון כי הסתברות) ולכן אפשר להוריד ערך מוחלט

מ.ש.ל.☺

5. **צ"ל:** קיים PRG כך ש- $H\left(0^n\right)=0^{2n}$ ו- H מגדיל את גודל הקלט פי 2

הוכחה:

נגדיר

$$\boxed{H\left(s\right)\stackrel{\text{def}}{=}G\left(s\right)\oplus G\left(0^n\right)}$$

נשים לב כי $G\left(s\right),G\left(0^n\right)$ שניהם באורך $2n$ ולכן הקסור שלהם הוא באורך $2n$, ולכן H אכן מגדיל את אורך הקלט פי 2.
בנוסף לכך, נשים לב ש- G הוא PRG ולכן הוא PPT, ולכן הפעלתו פעמיים זה גם PPT וקסור עליהם הוא גם פולינומי, ולכן נקבל כי H הוא גם PPT.
עתה נשים לב כי

$$H\left(0^n\right)=G\left(0^n\right)\oplus G\left(0^n\right)=0^{2n}$$

עתה נניח בשלילה שקיים אלגוריתם $\mathcal{A}$ שהוא PPT ופולינום $p\left(\cdot\right)$ שמקיימים

$$\left|\Pr_{s\leftarrow\{0,1\}^n}\left[\mathcal{A}\left(H\left(s\right)\right)=1\right]-\Pr_{r\leftarrow\{0,1\}^{2n}}\left[\mathcal{A}\left(r\right)=1\right]\right|\geq\frac{1}{p\left(n\right)}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$,
נגדיר אלגוריתם D באופן הבא:

(א) נקבל קלט $z\in\{0,1\}^{2n}$ ונחזיר $\mathcal{A}\left(z\oplus G\left(0^n\right)\right)$

נשים לב כי עבור $r\in\{0,1\}^{2n}$ מתקיים ש- $r\oplus G\left(0^n\right)$ מפולג באופן אחיד (כי $G\left(0^n\right)$ הוא קבוע) ולכן מתקיים

$$\Pr_{r\leftarrow\{0,1\}^{2n}}\left[\mathcal{A}\left(r\oplus G\left(0^n\right)\right)=1\right]\stackrel{\star}{=}\Pr_{r\leftarrow\{0,1\}^{2n}}\left[\mathcal{A}\left(r\right)=1\right]$$

נשים לב ש- D הוא PPT בגלל ש- A הוא PPT וגם מתקיים

$$\begin{aligned}
&\left|\Pr_{s\leftarrow\{0,1\}^n}\left[D\left(G\left(s\right)\right)=1\right]-\Pr_{r\leftarrow\{0,1\}^{2n}}\left[D\left(r\right)=1\right]\right|\\
=&\left|\Pr_{s\leftarrow\{0,1\}^n}\left[\mathcal{A}\left(G\left(s\right)\oplus G\left(0^n\right)\right)=1\right]-\Pr_{r\leftarrow\{0,1\}^{2n}}\left[\mathcal{A}\left(r\oplus G\left(0^n\right)\right)=1\right]\right|\\
\stackrel{\text{def}}{=}&\left|\Pr_{s\leftarrow\{0,1\}^n}\left[\mathcal{A}\left(H\left(s\right)\right)=1\right]-\Pr_{r\leftarrow\{0,1\}^{2n}}\left[\mathcal{A}\left(r\oplus G\left(0^n\right)\right)=1\right]\right|\\
\stackrel{\star}{=}&\left|\Pr_{s\leftarrow\{0,1\}^n}\left[\mathcal{A}\left(H\left(s\right)\right)=1\right]-\Pr_{r\leftarrow\{0,1\}^{2n}}\left[\mathcal{A}\left(r\right)=1\right]\right|\geq\frac{1}{p\left(n\right)}
\end{aligned}$$

עבור אינסוף ערכים של $n\in\mathbb{N}$, קיבלנו סתירה לכך ש- G הוא PRG,
ולכן נקבל כי H הוא PPT וגם לכל אלגוריתם PPT שנסמנו $\mathcal{A}$ קיימת פונקציה זניחה $\nu\left(\cdot\right)$ כך ש

$$\left|\Pr_{s\leftarrow\{0,1\}^n}\left[\mathcal{A}\left(H\left(s\right)\right)=1\right]-\Pr_{r\leftarrow\{0,1\}^{2n}}\left[\mathcal{A}\left(r\right)=1\right]\right|<\nu\left(n\right)$$

כלומר H הוא PRG שמכפיל את גודל הקלט וגם $H\left(0^n\right)=0^{2n}$

מ.ש.ל.☺