# פתרון תרגיל מספר 3־ מבוא לקריפטוגרפיה ואבטחת תוכנה

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

2022 במאי 18

#### ו. פתרון:

 $t=F_{k}\left(m_{1}
ight)\oplus\cdots\oplus F_{k}\left(m_{d}
ight)$  עם Mac Secure א) אייל: סכימה  $\Pi$  היא לא

:נגדיר יריב  ${\cal A}$  לסכימה  $\Pi$  באופן הבא

$$1^n$$
 נקבל פרמטר בטיחות .i

$$m=1^n||\underbrace{0^n||\dots||0^n}_{d-1 \text{ times}}$$
 , $m_0=\underbrace{0^n||\dots||0^n}_{d-1 \text{ times}}||1^n$  .ii

$$t = \operatorname{Mac}_k\left(m_0\right)$$
 נחשב את .iii

$$(m,t)$$
 נחזיר.iv

נשים לב שי אוא PPT שהוא שהוא כי כי רוב הריצה כי רוב הוא אוא לב שי לב כי נשים לב כי

$$\operatorname{Mac}_{k}\left(m\right) = F_{k}\left(1^{n}\right) \oplus \underbrace{F_{k}\left(0^{n}\right) \oplus \cdots \oplus F_{k}\left(0^{n}\right)}_{d-1 \text{ times}} = \underbrace{F_{k}\left(0^{n}\right) \oplus \cdots \oplus F_{k}\left(0^{n}\right)}_{d-1 \text{ times}} \oplus F_{k}\left(1^{n}\right) = \operatorname{Mac}_{k}\left(m_{0}\right) = t$$

, אור ערקע (
$$m, \mathrm{Mac}_k(m)$$
) אולכן אין אור ערקע ( $m, \mathrm{Mac}_k(m)$ ) אולכן אולכן אור אור אולכן אור אולכן אולכן אולכן אולכן אור אולכן אור אולכן אולכן

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}\left(n\right)=1\right)=1$$

כך ש $p\left(n
ight)=1$  כלומר הראנו שקיים יריב  $\mathcal{A}$  ופולינום

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,\mathcal{A}}(n) = 1\right) \ge \frac{1}{p(n)}$$

 $n \in \mathbb{N}$  לכל

כנדרש, כנדרש  $\Pi$  מההגדרה, כנדרש הוא  $\Pi$ 

מ.ש.ל.א.©

 $t=F_{k}\left(\left\langle 1\right
angle \left|\left|m_{1}
ight
angle \oplus\cdots\oplus F_{k}\left(\left\langle d
ight
angle \left|\left|m_{d}
ight
angle 
ight.$ עם  $\Pi$  איי שני סכימה  $\Pi$  היא לא איי שלי מכימה  $\Pi$  היא לא הוכחה:

:נגדיר יריב  $\mathcal A$  לסכימה  $\Pi$  באופן הבא

$$1^n$$
 נקבל פרמטר בטיחות.i

$$m^*=1^{rac{n}{2}}||0^{rac{n}{2}}$$
 , $m_0=0^{rac{n}{2}}||0^{rac{n}{2}},m_1=0^{rac{n}{2}}||1^{rac{n}{2}},m_2=1^{rac{n}{2}}||1^{rac{n}{2}}$  .ii

$$t_{0} = \operatorname{Mac}_{k}\left(m_{0}\right), t_{1} = \operatorname{Mac}_{k}\left(m_{1}\right), t_{2} = \operatorname{Mac}_{k}\left(m_{2}\right)$$
 .iii. נחשב את

$$(m^*, t_0 \oplus t_1 \oplus t_2)$$
 .iv

נשים לב שי  $\mathcal{A}$  הוא PPT כי רוב הריצה היא הריצה היא שהוא  $\operatorname{Mac}_k$  שהוא רב כי PPT הוא

$$\begin{split} &t_{0} \oplus t_{1} \oplus t_{2} = \operatorname{Mac}_{k}\left(m_{0}\right) \oplus \operatorname{Mac}_{k}\left(m_{1}\right) \oplus \operatorname{Mac}_{k}\left(m_{2}\right) \\ &= \left[F_{k}\left(\left\langle 1\right\rangle || 0^{\frac{n}{2}}\right) \oplus F_{k}\left(\left\langle 2\right\rangle || 0^{\frac{n}{2}}\right)\right] \oplus \left[F_{k}\left(\left\langle 1\right\rangle || 0^{\frac{n}{2}}\right) \oplus F_{k}\left(\left\langle 2\right\rangle || 1^{\frac{n}{2}}\right)\right] \oplus \left[F_{k}\left(\left\langle 1\right\rangle || 1^{\frac{n}{2}}\right) \oplus F_{k}\left(\left\langle 1\right\rangle || 1^{\frac{n}{2}}\right)\right] \\ &= \left[F_{k}\left(\left\langle 1\right\rangle || 0^{\frac{n}{2}}\right) \oplus F_{k}\left(\left\langle 1\right\rangle || 0^{\frac{n}{2}}\right)\right] \oplus \left[F_{k}\left(\left\langle 2\right\rangle || 0^{\frac{n}{2}}\right) \oplus F_{k}\left(\left\langle 1\right\rangle || 1^{\frac{n}{2}}\right)\right] \oplus \left[F_{k}\left(\left\langle 2\right\rangle || 1^{\frac{n}{2}}\right)\right] \\ &= 0^{n} \oplus \left[F_{k}\left(\left\langle 1\right\rangle || 1^{\frac{n}{2}}\right) \oplus F_{k}\left(\left\langle 2\right\rangle || 0^{\frac{n}{2}}\right)\right] \oplus 0^{n} = \operatorname{Mac}_{k}\left(m^{*}\right) \end{split}$$

,  $1=\mathrm{Vrfy}_k\left(m,\mathrm{Mac}_k\left(m
ight)
ight)=\mathrm{Vrfy}_k\left(m,t_0\oplus t_1\oplus t_2
ight)$  ולכן ,  $m\notin\{m_0,m_1,m_2\}=Q$  הניסוי מתקיים כי  $q\notin\{m_0,m_1,m_2\}=Q$  וגם מתקיים כי

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,A}(n)=1\right)=1$$

 $n \in \mathbb{N}$  לכל

כך ש כך  $p\left(n\right)=1$  ופולינום אקיים יריב שקיים כלומר הראנו

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

, $n \in \mathbb{N}$  לכל

כנדרש, כנדרש  $\operatorname{Mac}$  Secure כלומר  $\Pi$ 

מ.ש.ל.ב.☺

 $t=F_{k}\left(r
ight)\oplus F_{k}\left(m
ight)$  עם Mac Secure א"ל: סכימה  $\Pi$  היא לא

:נגדיר יריב  ${\cal A}$  לסכימה  $\Pi$  באופן הבא

 $1^n$  נקבל פרמטר בטיחות i.

 $(0^n,(0^n,0^n))$  .ii

נשים לב ש־ PPT וגם נשים לב כי PPT וגם נשים לב כי רוב הריצה היא

$$\operatorname{Vrfy}_{k}\left(m = 0^{n}, (r = 0^{n}, t = 0^{n})\right) = \begin{cases} 1 & 0^{n} = F_{k}\left(0^{n}\right) \oplus F_{k}\left(0^{n}\right) \\ 0 & else \end{cases} = \begin{cases} 1 & 0^{n} = 0^{n} \\ 0 & else \end{cases} = 1$$

רגם מנצח אולכן ,m 
otin Q = Q, ולכן המיד מנצח ולכן ,m 
otin Q = Q, ולכן וגם מתקיים כי

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,\mathcal{A}}(n)=1\right)=1$$

, $n\in\mathbb{N}$  לכל

כך ש $p\left(n\right)=1$  כלומר הראנו שקיים יריב  $\mathcal{A}$  ופולינום

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

, $n \in \mathbb{N}$  לכל

מההגדרה, כנדרש  $\operatorname{Mac}$  Secure כלומר  $\Pi$ 

מ.ש.ל.ג.©

Mac Secure מר 2 סכימות שאחת מהן מר Mac Secure  $\Pi$  2. צ"ל: ניתן ליצר הוכחה:

נגדיר סכמה  $\Pi$  באופן הבא:

$$\left(\operatorname{Mac}_{1,k_{1}}\left(m\right),\operatorname{Mac}_{2,k_{2}}\left(m\right)\right)$$
 נבו  $\left(\operatorname{Mac}_{k_{1}\mid\mid k_{2}}\left(m\right)\right)$  נבו  $\left(\operatorname{Mac}_{k_{1}\mid\mid k_{2}}\left(m\right)\right)$ 

$$\left(\operatorname{Vrfy}_{1,k_1}\left(m,t_1\right)=1\right)\wedge\left(\operatorname{Vrfy}_{2,k_2}\left(m,t_2\right)=1\right)$$
 מט :  $\operatorname{Vrfy}_{k_1\mid\mid k_2}\left(m,\left(t_1,t_2\right)\right)$  (מ)

,Mac Secure נשים לב שהכל ועתה נוכיח כי היא אירוף של 2 אימותים נכונים, ועתה נוכיח כי חPPTונטים לב שהכל נניח בשלילה ש־ חהיא לא Mac Secure כלומר קיים יריב PPT שהוא דריב שהיא לא היא לא שירים אלים לומר קיים יריב א

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,\mathcal{A}}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

 $n \in \mathbb{N}$  לאינסוף ערכים של

( $\Pi_2$  'כל ההוכחה סימטרית (כל היא Mac Secure נניח בלי הכלליות כי הכלליות כי וזהה ל־

נגדיר יריב  $\operatorname{Mac}_{1,k}$  אימות פונקצית עם פונקנ $\Pi_1$ ל־ ל

- $1^n$  נקבל פרמטר בטיחות (א)
  - $k_2 \leftarrow \operatorname{Gen}_2\left(1^n\right)$  (ב)
- $(\operatorname{Mac}_{1,k}\left(m\right),\operatorname{Mac}_{2,k_{2}}\left(m\right))$  את נחזיר את לאימות, שלו m ולכל בקשה שלו  $\mathcal{A}\left(1^{n}\right)$  את נריץ את
  - $(m^*,(t_1,t_2))$  ב־  ${\cal A}$  בי התשובה את (ד)
    - $(m^*,t_1)$  נחזיר (ה)

PPT נשים לב ש־ D הוא PPT כי רוב ריצתו היא הרצת D ו־ D מספר פולינומי של פעמים והם PPT כי רוב ריצתו היא הרצת D לכן הריצה של D תחזיר D, לכן הריצה של D לריצה מסוימת ב־ D לריצה מחוימת ב־ D מול D מול

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi_{1},D}\left(n\right)=1\right) \geq \mathbb{P}\left(\operatorname{MacForge}_{\Pi,\mathcal{A}}\left(n\right)=1\right) \geq \frac{1}{p\left(n\right)}$$

 $n\in\mathbb{N}$  לאינסוף ערכים של

כך ש<br/>ד $p\left(\cdot\right)$ ופולינום PPTשהוא יריב יריב שקיים הראנו כלומר כלומר יריב

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi_{1},D}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

, $\operatorname{Mac}$  Secure לאינסוף ערכים של  $n\in\mathbb{N}$ , בסתירה לכך שר לאינסוף ערכים של אינסוף היא  $\operatorname{Mac}$  Secure כלומר נקבל כי  $\Pi$ 

מ.ש.ל.©

# 3. פתרון:

colision resistant hash family איל:  $\hat{\mathcal{H}}$  היא

הוכחה:

,colision resistant hash family נניח בשלילה ש־  $\hat{\mathcal{H}}$  היא לא ככומר בשלילה ש־  $p\left(\cdot\right)$  כך ש־ כלומר קיים  $\mathcal{L}$  שהוא PT ופולינום

$$\mathbb{P}\left(\operatorname{HashColl}_{\hat{\mathcal{H}},\mathcal{A}}(n) = 1\right) \ge \frac{1}{p(n)}$$

, $n\in\mathbb{N}$  לאינסוף ערכים של גדיר ערכים לדD באופן נגדיר יריב ל

s ומפתח ומפתח .i

(x||b,x'||b') ונשמור את התוצאה ב־  $\mathcal{A}(1^n,s)$  וניץ את. ii.

(x,x') נחזיר. iii

.PPT נשים לב ש־ D הוא PPT כי A הוא

(x,x') נסמן את התשובה של D ב־(x||b,x'||b') ב־A היא

נניח ש־ $\mathcal{A}$  ניצח בניסוי  $Hash\ \mathrm{Coll}$  מול  $\hat{\mathcal{H}}$ , כלומר  $\hat{\mathcal{H}}_s(x'||b')=\hat{H}_s(x'||b')$ , נשים לב כי

$$H_{s}(x)||b = \hat{H}_{s}(x||b) = \hat{H}_{s}(x'||b') = H_{s}(x')||b'|$$

$$\Rightarrow b = b', H_{s}(x') = H_{s}(x)$$

נשים לב כי  $H_s\left(x'
ight)=H_s\left(x
ight)$  וגם x
eq x' וגם לב כי x|b=b' זה ניצחון ולכן מהיות לב כי  $x|b\neq x'|b'$  $\mathcal{H}$  מול Hash Coll מול  $\mathcal{H}$ , כלומר מול Hash Coll כלומר נקבל כי

$$\mathbb{P}\left(\mathrm{HashColl}_{\mathcal{H},D}\left(n\right)=1\right) \geq \mathbb{P}\left(\mathrm{HashColl}_{\hat{\mathcal{H}},\mathcal{A}}\left(n\right)=1\right) \geq \frac{1}{p\left(n\right)}$$

 $n\in\mathbb{N}$  לאינסוף ערכים של

כד ש־  $p\left(\cdot\right)$  ופולינום PPT שהוא לינום יריב יריב סלומר הראנו

$$\mathbb{P}\left(\mathrm{HashColl}_{\mathcal{H},D}\left(n\right)=1\right) \geq \frac{1}{p\left(n\right)}$$

,colision resilant hash family לאינסוף ערכים של  $n\in\mathbb{N}$ , בסתירה לכך שי $\mathcal{H}$  היא נדרש, colision resistant hash family  $\mathcal{H}$  ולכן נקבל כי

מ.ש.ל.א.©

colision resistant hash family ב"ל:  $\mathcal{W}$  היא לא $\mathcal{W}$  היא לא

,colision resistant hash family  $\mathcal{H}$  תהי

, נעשה את הבניית עזר שנעשתה בסעיף הקודם ונגדיר  $\hat{\mathcal{H}}$  כמו שהוגדר בסעיף הקודם כלומר לכל  $\hat{H}_s(x)$   $||b=\hat{H}_s(x)||b$  מתקיים  $s\in\{0,1\}^n$  ,  $b\in\{0,1\}$  ,  $x\in\{0,1\}^*$  עתה נסתכל על  $\mathcal{H}$  מעל למשפחת הפונקציות  $\hat{\mathcal{H}}$  מתקיים  $s\in\{0,1\}^n$  ,  $b\in\{0,1\}$  מתקיים לב כי לכל  $t\in\{0,1\}^n$  ,  $t\in\{0,1\}$ 

$$W_s(x||b) = \underbrace{H_s(x)||b}_{\text{n-1 left most bits}} = \underbrace{H_s(x)}_{\text{n-1 left most bits}}$$

- s ומפתח ומפתח .i
  - $(0^n||0,0^n||1)$  החזר. ii

נשים לב ש $M_s\left(0^n||0
ight)=W_s\left(0^n||1
ight)$  נישים לב ש $M_s\left(0^n||0
ight)=W_s\left(0^n||1
ight)$  נישים לב ש $M_s\left(0^n||0
ight)=W_s\left(0^n||1
ight)$  נישים לב ש  $n\in\mathbb{N}$  לכל  $\mathbb{P}\left(\mathrm{HashColl}_{\mathcal{W},\mathcal{A}}\left(n
ight)=1\right)=1$  לכל Hash Coll כלומר הראנו שקיים יריב  $\mathcal{A}$  ופולינום  $p\left(n\right)=1$  כך ש

$$\mathbb{P}\left(\mathrm{HashColl}_{\mathcal{W},\mathcal{A}}\left(n\right)=1\right) \geq \frac{1}{p\left(n\right)}$$

 $n \in \mathbb{N}$  לכל

כנדרש, כנדרה, מההגדרה, colision resistant hash family כלומר  ${\mathcal W}$  הוא לא

מ.ש.ל.ב.©

## Mac Secure **נ"ל:** Π היא

הוכחה:

כך ש־  $p\left(\cdot\right)$  ופולינום PPT שהוא היים יריב Mac Secure נניח בשלילה ש־  $\Pi$  היא לא

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,\mathcal{A}}(n) = 1\right) \ge \frac{1}{p(n)}$$

 $n\in\mathbb{N}$  לאינסוף ערכים של

:נגדיר יריב ל $\mathcal O$  שנסמנו ב־ עם גישה לאורקל שנסמנו ב־ שנסמנו ב־ ל

- $1^n$  נקבל פרמטר בטיחות (א)
  - $k_2 \leftarrow \left\{0,1\right\}^n$  ב) (ב)
- - $(m^*,t^*)$  ב־  $\mathcal{A}$  בי (ד)
  - 0 אחרת  $t^{*}=\mathcal{O}\left(m^{*}
    ight)\oplus F_{k_{2}}\left(\mathcal{O}\left(m^{*}
    ight)
    ight)$  וגם  $m^{*}
    otin Q$  אחרת ונחזיר  $t^{*}$

Q נשים לב ש־ D הוא PPT כי הוא רק מריץ את A, ניגש לאורקל מספר פולינומי של פעמים ובודק שייכות של איבר ל־ שמכילה מספר פולינומי של איברים.

ולכן Mac Forge מסמלץ לי מסמלץ לי אז D אז  $\mathcal{O}=F_k$  נשים לב שאם

$$\mathbb{P}_{k_1 \leftarrow \{0,1\}^n} \left( D^{F_{k_1}(\cdot)} \left( 1^n \right) = 1 \right) = \mathbb{P} \left( \text{MacForge}_{\Pi, \mathcal{A}} \left( n \right) = 1 \right)$$

נשים לב שאם אחיד ובלתי תלוי בשאר מתקיים כי  $f\left(m^*\right)$  הוא מתפלג באופן אחיד ובלתי תלוי בשאר הערכים, וגם  $\mathcal{A}$  החילה מתקיים ש־ $Q=f\leftarrow Func_{n o n}$  ולכן הסיכוי של  $\mathcal{A}$  לנצח בשביל ש־ $f\left(m^*\right)$  ולכן הסיכוי של  $f\left(m^*\right)$  ולכן הסיכוי של  $f\left(m^*\right)$  נכון ולכן במקרה זה הוא בדיוק הסיכוי לנחש את  $f\left(m^*\right)$  נכון ולכן

$$\mathbb{P}_{f \leftarrow Func_{n \to n}} \left( D^{f(\cdot)} \left( 1^n \right) = 1 \right) = \frac{1}{2^n}$$

, $n\in\mathbb{N}$  לכל  $\frac{1}{p(n)}-\frac{1}{2^n}\geq \frac{1}{q(n)}$  המקיים  $q\left(n\right)$  לכל לכל ושים לב שקיים פולינום ולכו נקבל כי

$$\left| \mathbb{P}_{k_1 \leftarrow \{0,1\}^n} \left( D^{F_{k_1}(\cdot)} \left( 1^n \right) = 1 \right) - \mathbb{P}_{f \leftarrow Func_{n \to n}} \left( D^{f(\cdot)} \left( 1^n \right) = 1 \right) \right| \ge \frac{1}{p(n)} - \frac{1}{2^n} \ge \frac{1}{q(n)}$$

 $n\in\mathbb{N}$  לאינסוף ערכים של

כך ש $q\left(n\right)=1$ ופולינום Dיריב ירים שקיים הראנו

$$\left| \mathbb{P}_{k_1 \leftarrow \{0,1\}^n} \left( D^{F_{k_1}(\cdot)} \left( 1^n \right) = 1 \right) - \mathbb{P}_{f \leftarrow Func_{n \to n}} \left( D^{f(\cdot)} \left( 1^n \right) = 1 \right) \right| \ge \frac{1}{q(n)}$$

PRF אינסוף ערכים של  $n\in\mathbb{N}$ , בסתירה לכך שי

כנדרש , $\operatorname{Mac}$  Secure כלומר  $\Pi$ 

מ.ש.ל.©

# 5. **פתרון:**

left-most bit leakage resilent Mac secure א) ב"ל:  $\Pi$  היא

הוכחה

,left-most bit leakage resilent Mac secure נניח היא לא  $\Pi$  היא לא פניח בשלילה ש־ חיריב  $p\left(\cdot\right)$  ופולינום רריב PT שהוא שהוא ררים יריב  $p\left(\cdot\right)$ 

$$\mathbb{P}\left(\operatorname{MacForgeBitLeakage}_{\Pi,\mathcal{A}}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

 $n \in \mathbb{N}$  לאינסוף ערכים של

יבאופן הבא  $\operatorname{Mac}_k$  באופן יצירת אימותים עם אלגוריתם לסכמה  $\Pi$ 

- $1^n$  נקבל פרמטר בטיחות .i
  - $b \leftarrow \{0,1\}$  .ii. נגריל.
- $(m^*,t^*)$  בקשה את ונשמור את את ונשמור את נחזיר את התשובה ב'  $\mathcal{A}\left(1^n,b\right)$  ולכל בקשה שלו ווני. נריץ את
  - $(m^*, t^*)$  גחזיר את .iv

 $\mathcal{P}PT$  נשים לב ש־  $\mathcal{A}$  שהוא רק מריץ הוא רק כי הוא PPT הוא D

נשים לב שבמקרה והגרלנו b שהוא באמת הביט השמאלי ביותר של המפתח, אנחנו בניסוי מסמלצים ל־  $\mathcal{A}$  את הניסוי Mac Forge Bit Leakage

$$\begin{split} & \mathbb{P}\left(\operatorname{MacForge}_{\Pi,D}\left(n\right)=1\right) \\ & \geq \mathbb{P}\left(\operatorname{guessed\ correctly\ last\ bit}\right) \cdot \mathbb{P}\left(\operatorname{MacForgeBitLeakage}_{\Pi,\mathcal{A}}\left(n\right)=1\right) \\ & = \frac{1}{2} \cdot \mathbb{P}\left(\operatorname{MacForgeBitLeakage}_{\Pi,\mathcal{A}}\left(n\right)=1\right) \geq \frac{1}{2 \cdot n\left(n\right)} \end{split}$$

 $n\in\mathbb{N}$  לאינסוף ערכים של

כל שר  $q\left(\cdot\right)$  ופולינום PPT שהוא שקיים יריב שקיים כלומר הראנו

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,D}\left(n\right)=1\right)\geq\frac{1}{q\left(n\right)}$$

,Mac Secure לאינסוף ערכים של  $n\in\mathbb{N}$ , בסתירה לכך ש־  $\Pi$  היא ולכן ערכים של לאינסוף ערכים של פולר. ולכן נקבל כי  $\Pi$  היא

מ.ש.ל.א.☺

left-half bit leakage resilient Mac secure ב) צ"ל: להגדיר

#### הוכחה:

באופן הבא:  $\Pi$  וסכמה  $\Pi$  ביחס ליריב Mac Forge Left half leakage נגדיר ניסוי עזר

- $1^n$  נקבל פרמטר בטיחות .i
- $|k_L| = |k_R|$  כאשר  $k = k_L ||k_R|$  ונסמן ונסמן  $k \leftarrow \operatorname{Gen}\left(1^n\right)$  .ii
- Q ולכל בקשה שלו שלו ברשימה . $\mathrm{Mac}_k\left(m
  ight)$  את נחזיר לו את הבקשות שלו ברשימה אוני. נריץ  $\mathcal{A}\left(1^n,k_L
  ight)$ 
  - $(m^*,t^*)$  ב־  $\mathcal{A}$  בי .iv
  - $\operatorname{Vrfy}_k\left(m^*,t^*\right)=1$  נחזיר 1 אם"ם  $m^*\notin Q$  נחזיר .v

 $u\left(\cdot\right)$  אם אניחה פונקציה אניחה PPT אם לכל יריב אוleft-half bit leakage resilient Mac secure איז  $\Pi$  כך ש־

$$\mathbb{P}\left(\operatorname{MacForgeLeftHalfLeakage}_{\Pi,\mathcal{A}}\left(n\right)=1\right)<\nu\left(n\right)$$

 $n \in \mathbb{N}$  לכל

 $\mathcal{A}\left(1^n,k_R
ight)$  את נגדיר ניסוי מאר באופן את Mac Forge Right half leakage מאר באופן דומה נגדיר ניסוי את Mac Forge Right half leakage resilient Mac secure נאמר ש־  $\Pi$  היא דומה אימר ש־ ווימת פונקציה אניחה מיחה איז דיימת פונקציה אניחה על יריב  $\mathcal{A}$  שריימת פונקציה היא דיימת פונקציה אניחה על יריב ער יריב ער פונקציה אניחה ביימת פונקציה הוא ביימת פונקציה ביימת ביימת פונקציה ביימת פונקציה ביימת פונקציה ביימת פונקציה ביימת ביימת פונקציה ביימת ביימת פונקציה ביימת ביימת פונקציה ביימת פונקציה

$$\mathbb{P}\left(\operatorname{MacForgeRightHalfLeakage}_{\Pi,\mathcal{A}}(n)=1\right)<\nu\left(n\right)$$

 $n \in \mathbb{N}$  לכל

מ.ש.ל.ב.©

 $_{
m left-half}$  bit leakage resilient Mac secure ג) איימת  $\Pi'$  שהיא לא $\Pi'$ 

#### הוכחה:

,Mac Secure סכמה שהיא דו  $\Pi=\langle \mathrm{Gen,Mac,Vrfy} 
angle$  נגדיר  $\Pi'$  באופן הבא:

k||k| נחשיר ונחזיר  $k \leftarrow \operatorname{Gen}(1^n)$  נחשב : $\operatorname{Gen}'(1^n)$  .i

 $\operatorname{Mac}_{k}\left(m\right)$  נחזיר:  $\operatorname{Mac}_{k\mid\mid k}^{\prime}\left(m\right)$  .ii

 $\operatorname{Vrfy}_{k}\left(m,t\right)$  נחזיר :  $\operatorname{Vrfy}_{k||k}^{\prime}\left(m,t\right)$  .iii

 $\operatorname{Vrfy}_{k||k}'\left(m,\operatorname{Mac}_{k||k}'\left(m
ight)
ight)=\operatorname{Vrfy}_{k||k}'\left(m,t
ight)=\operatorname{Vrfy}_{k}\left(m,t
ight)=\operatorname{Mac}_{k||k}'\left(m
ight)=\operatorname{Mac}_{k}\left(m
ight)=\operatorname{Mac}_{k}\left(m
ight)$  ולכן  $\operatorname{Mac}_{k||k}'\left(m
ight)=\operatorname{Mac}_{k}\left(m
ight)=\operatorname{Mac}_{k}\left(m
ight)=1$  ,  $\operatorname{Vrfy}_{k}\left(m,\operatorname{Mac}_{k}\left(m
ight)\right)=1$ 

עתה יהי  $\mathcal{A}$  יריב שהוא PPT, לכן קיימת פונקציה זניחה  $\mathcal{A}$  יריב שהוא

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,\mathcal{A}}(n) = 1\right) < \nu(n)$$

 $n \in \mathbb{N}$  לכל

נשים לב שמבחינת  $\Pi,\Pi'$  אהות ולירת האימותים של פונקציות ולכן

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi',\mathcal{A}}\left(n\right)=1\right)=\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}\left(n\right)=1\right)<\nu\left(n\right)$$

, $n\in\mathbb{N}$  לכל

כך ש־ עריב אניחה פונקציה פונקציה אוא ריב שהוא א פרומר לכל איריב א שהוא א ריב א פרומר לכל יריב א שהוא א ריב א

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi',\mathcal{A}}\left(n\right)=1\right)<\nu\left(n\right)$$

 $n \in \mathbb{N}$  לכל

.Mac Secure כלומר  $\Pi'$ 

,left-half bit leakage resilient Mac secure עתה נוכיח ש־  $\Pi'$  שר נוכיח של נגדיר יריב D באופן הבא:

 $k_L$  וחלק שמאלי של וחלק בטיחות וחלק בטיחות .i

 $(0^n,\operatorname{Mac}_{k_L}(0^n))$  .ii .ii

 $\operatorname{Vrfy}_{k_L\mid\mid k_L}\left(0^n,\operatorname{Mac}_{k_L}\left(0^n\right)\right)=0$ וגם  $\emptyset^n\notin\emptyset=Q$  וגם נשים לב עי  $\operatorname{PPT}$  הוא  $\operatorname{Mac}_{k_L}\left(0^n,\operatorname{Mac}_{k_L}\left(0^n,\operatorname{Mac}_{k_L}\left(0^n\right)\right)=1$  ,  $\operatorname{Vrfy}_{k_L}\left(0^n,\operatorname{Mac}_{k_L}\left(0^n\right)\right)=1$ 

כלומר אמיד מנצח בניסוי אותר כלומר תמיד מנצח כלומר D

$$\mathbb{P}\left(\operatorname{MacForgeLeftHalfLeakage}_{\Pi',D}\left(n\right)=1\right)=1$$

 $n \in \mathbb{N}$  לכל

כך ש כך  $p\left(n\right)=1$  כלומר הראנו שקיים יריב לירים פלומר הראנו

$$\mathbb{P}\left(\operatorname{MacForgeLeftHalfLeakage}_{\Pi',D}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

, $n\in\mathbb{N}$  לכל

מההגדרה, כנדרש left-half bit leakage resilient Mac secure כלומר  $\Pi'$ 

מ.ש.ל.ג.©

### 6. פתרון:

\_right-half bit leakage resilient Mac secure א) צ"ל:  $\Pi'$  ב"ל:

הוכחה:

,right-half bit leakage resilient Mac secure נניח היא ח' נניח בשלילה ש<br/>ר $\Pi'$  היא שהיא רבים כלומר כלומר אווים ארוא אווי ארוא PT שהוא יריב <br/>  $\mathcal{P}$  פרומר היים יריב א

$$\mathbb{P}\left(\operatorname{MacForgeRightHalfLeakage}_{\Pi',\mathcal{A}}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

 $n\in\mathbb{N}$  לאינסוף ערכים של

נגדיר יריב  $\operatorname{Mac}_k$  באופן אלגוריתם אלגורית עם  $\Pi$  לסכמה ל

 $1^n$  נקבל פרמטר בטיחות .i

$$k_R \leftarrow \{0,1\}^n$$
 נגריל.ii

Q ב־  $m\oplus k_R$  נשמור את כל הבקשות  $m\oplus k_R$  נחזיר את וווי. נריץ את הריץ את ולכל בקשה שלו A ( $1^n,k_R$ ) ווווי. נריץ את

 $(m^*,t^*)$  ב־  $\mathcal{A}$  בי .iv

 $(m^*\oplus k_R,t^*)$  את .v

נשים לב ש־ פולינומי של מחבר את  $\mathcal{A}$  את מריץ את א פעמים. PPT הוא D בשים לב ש־

 ${
m Mac}$  Forge עתה נשים לב ש־ D מסמלץ ל־

 $(m^*\oplus k_R,t^*)$  נסמן הרצה של  ${\cal A}$  ב־ $(m^*,t^*)$  ושל

 ${
m Vrfy}_{k_L}\left(m^*\oplus k_R,t^*
ight)=1$  מול  $\Pi'$  אם"ם Mac Forge Right Half Leakage וגם נשים לב ש־  $m^*\oplus k_R 
otin Q = \{m_0\oplus k_R, m_1\oplus k_R, \ldots, m_l\oplus k_R\}$  וגם  $\mathrm{Vrfy}_{k_L} \ (m^*\oplus k_R, t^*) = 1$  אם"ם  $m^*
otin Q = \{m_0, m_1, \ldots, m_l\}$  $\Pi$  מול  $Mac\ Forge$  מול מנצח מנצח מנצח מנצח מנצח אם

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,D}\left(n\right)=1\right)=\mathbb{P}\left(\operatorname{MacForgeRightHalfLeakage}_{\Pi',\mathcal{A}}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

 $n\in\mathbb{N}$  לאינסוף ערכים של

כלומר קיים יריב  $p\left(\cdot\right)$  שהוא PPT ופולינום יריב כלומר

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,D}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

, $\operatorname{Mac}$  Secure לאינסוף ערכים של  $n\in\mathbb{N}$ , בסתירה לכך שי כנדרש, right-half bit leakage resilient Mac secure ולכן  $\Pi'$ 

מ.ש.ל.א.©

 $_{
m left-half}$  bit leakage resilient Mac secure ב) אייל:  $\Pi'$  היא לא בהכרח

### הוכחה:

, $\operatorname{Mac}$  Secure סכמה שהיא  $\Pi = \langle \operatorname{Gen}, \operatorname{Mac}, \operatorname{Vrfy} \rangle$  תהי נגדיר  $\Pi_1$  באופן הבא:

 $k \leftarrow \operatorname{Gen}(1^n)$  נחשב : $\operatorname{Gen}_1(1^n)$  .i

 $(\operatorname{Mac}_{k}(m), m)$  נחזיר:  $\operatorname{Mac}_{1,k}(m)$  .ii

 $\operatorname{Vrfy}_{k}\left(m,t_{1}\right)$  נחזיר :  $\operatorname{Vrfy}_{1,k}\left(m,\left(t_{1},t_{2}\right)\right)$  .iii

, $\operatorname{Mac}$  Secure תחילה נוכיח ש־  $\Pi_1$ 

, $\operatorname{Mac}$  Secure נניח בשלילה ש־  $\Pi_1$  היא לא

כך ש<br/>ד $p\left(\cdot\right)$ ופולינום PPTשהוא שהוא ליים כלומר כלומר כלומר

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi_{1},\mathcal{A}}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

 $n\in\mathbb{N}$  לאינסוף ערכים של

נגדיר יריב  $\operatorname{Mac}_k$  באופן הבא: עם אלגוריתם יציתר אימותים  $\Pi$  ל־

- $1^n$  נקבל פרמטר בטיחות .i
- $(\operatorname{Mac}_k(m), m)$  נריץ את  $\mathcal{A}(1^n)$  ולכל בקשה שלו  $\mathcal{A}(1^n)$  ולכל. ii
  - $(m^*,(t_1^*,t_2^*))$  ב־  $\mathcal{A}$  בי .iii
    - $(m^*, t_1^*)$  נחזיר. iv

נשים. מספר פולינומי של פעמים.  $\operatorname{Mac}_k$  ושל  $\operatorname{PPT}$  כי הוא רוב ריצתו היא הרצה של פעמים.  $(m^*,(t_1^*,t_2^*))$  ב־  $\mathcal{A}$  של את התוצאה של

1= נשים לב ש־  $Mac\ {
m Forge}$  וגם  $Mac\ {
m Forge}$  מול  $Mac\ {
m Forge}$  נשים לב ש־ Aמול  $\Pi$ , כלומר  $\operatorname{Mac}$  Forge אם"ם D ניצח אם"ם  $m^* \notin Q$  וגם  $\operatorname{Vrfy}_k(m^*,t_1^*)$ 

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,D}\left(n\right)=1\right)=\mathbb{P}\left(\operatorname{MacForge}_{\Pi_{1},\mathcal{A}}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

 $n\in\mathbb{N}$  לאינסוף ערכים של

כלומר קיים יריב D שהוא PPT ופולינום יריב כלומר קיים

$$\mathbb{P}\left(\operatorname{MacForge}_{\Pi,D}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

, $\operatorname{Mac}$  Secure לאינסוף ערכים של  $n\in\mathbb{N}$ , בסתירה לכך שי

.Mac Secure לכן קיבלנו כי  $\Pi_1$  היא

 $\Pi_1$  ביחס לסכמה  $\Pi'$  ביחי לבניית עזר שהוגדרה בתרגיל על הבניית עזר שהוגדרה בתרגיל לבניית  $\Pi'$  ווכיח ש־  $\Pi'$  היא לא.left-half bit leakage resilient Mac secure נוכיח ש

נגדיר יריב  $\mathcal{A}'$  לסכמה  $\Pi'$  באופן הבא:

 $k_L$  בי שנסמנו מפתח של וחלק שמאלי וחלק בי ווחלק בי .i

את חזרה אזי נקבל אזי עבור  $m=0^n$ , אזי נקבל ווֹ. .ii

$$\operatorname{Mac}_{k_{L}}^{\prime}\left(0^{n}\right)\overset{\operatorname{def}}{=}\operatorname{Mac}_{1,k_{L}}\left(0^{n}\oplus k_{R}\right)=\left(\operatorname{Mac}_{k_{L}}\left(0^{n}\oplus k_{R}\right),0^{n}\oplus k_{R}\right)=\left(\operatorname{Mac}_{k_{L}}\left(0^{n}\oplus k_{R}\right),k_{R}\right)$$

 $(t_1,k_R)$  נשמור את התוצאה ב

 $\left(1^n,\operatorname{Mac}_{k_L}'\left(1^n\oplus k_R
ight)
ight)$  .iii .iii

נשים לב ש־  $\mathcal{A}'$  הוא PPT כי הוא רק ניגש ל־  $\mathrm{Mac}'_{k_L}$  פעמיים, והאלגוריתם ההוא בעצמו פולינומי. נסמן את התוצאה של  $\mathcal{A}'$  ב־ ר  $(1^n,\mathrm{Mac}'_{k_L}\,(1^n\oplus k_R))$ , עתה נשים לב ש־  $1^n\notin\{0^n\}=Q$  וגם

$$\operatorname{Vrfy}_{k_L}'\left(1^n,\operatorname{Mac}_{k_L}'\left(1^n\oplus k_R\right)\right)=\operatorname{Vrfy}_{1,k_L}\left(1^n,\operatorname{Mac}_{k_L}'\left(1^n\oplus k_R\right)\right)=\operatorname{Vrfy}_{1,k_L}\left(1^n,\operatorname{Mac}_{1,k_L}'\left(1^n\oplus k_R\right)\right)=1$$

ולכן Mac Forge Left Half Leakage כלומר  $\mathcal{A}'$  תמיד מנצח בניסוי

$$\mathbb{P}\left(\operatorname{MacForgeLeftHalfLeakage}_{\Pi'} _{A'}(n) = 1\right) = 1$$

 $n \in \mathbb{N}$  לכל

כלומר הראנו שקיים יריב  $\mathcal{A}$  ופולינום  $p\left(n
ight)=1$  כד ש

$$\mathbb{P}\left(\mathsf{MacForgeLeftHalfLeakage}_{\Pi',\mathcal{A}'}\left(n\right)=1\right)\geq\frac{1}{p\left(n\right)}$$

, $n \in \mathbb{N}$  לכל

כנדרש, כנדרה, מההגדרה, left-half bit leakage resilient Mac secure כלומר  $\Pi$ 

מ.ש.ל.ב.©