

2. ג'יג'ילט'ה יונגן ויכר - וילג נק'ה

7KJ07 13
313584401

in file

MAC → מיל' (בְּלִי מִזְבֵּחַ) י' כ' ס' ג' ו' ח' ו' ש' ו' ת' ו' ע' ו' ת' ו' ע' ו' ת'

הינה הינה π , $\text{MAC} \rightarrow \text{node}$ ו- node יוציאו
 node יוציאו PPT ו- node יוציאו A ו- node יוציאו B

$$\Pr[\text{MacForge}_{\mathcal{R}, A}(n) = 1] \leq V(n)$$

结论， $m = m_1 \parallel \dots \parallel m_j$ 时有 $\mu(m) = \mu(m_1) + \dots + \mu(m_j)$ (1)

: Given α_i , $i \in \{1, \dots, d\}$ by $m_i \in \{0, 1\}^n$

$$t = f_K(m_1) \oplus \cdots \oplus f_K(m_d)$$

FIGURE 2. LOGICAL FORM

רְמִים (רְמִים) ~~רְמִים~~ סֵלֶת שָׁמֶן גַּמְצָה וְלִבְנָה: גַּמְצָה:

newpm n \in N SfE p, PPT, A 271

הנומינטיב A מיל ז'ב) (1ⁿ ז'ניבר ז'ניבר נס)

think for app A

$$m = 0^n || 0^n || \dots || 0^n || 1^n$$

m^* works in (1B) A, but fails

since m where ℓ web unsigned rule

$$m^* = 0^n || 0^n || 0^n || \dots || 0^n, \text{ fails, } (\text{not } \sim \text{signed})$$

$t^* = t$ works, m is signed for rule
using only XOR operation, \neg , \wedge , \vee

t^* , \neg is sufficient

m^* doesn't work for \sim signed for U's

using \neg , \wedge , \vee K doesn't work

$$m \neq m^* \text{ since, } \text{Vrfy}_k(m^*, t^*) = 1$$

$\Pr[\text{Mac forge}_{\mathcal{A}, k}(n) = 1] = 1$ whenever f_k is

, \neg , \wedge , \vee , \neg , \wedge , \vee

$$, m = m_1 || \dots || m_d \text{ works for } (2)$$

$$, i \in \{1, \dots, d\} \text{ for } m_i \in \{0, 1\}^{n/2}$$

$$t = f_k((1) || m_1) || \dots || f_k((d) || m_d); \text{ (so) not}$$

2/8

• $\int_{\Omega} f_j \rightarrow \text{MAC} \rightarrow \text{mosf}(\cdot)$

الطبخ العربي

רכישת מילויים נספחים (PPT, A)

$\Pr[\text{MaxFolgenZ, } A(n) = 1] = 1$ nach ^{12/13} für $n \in \mathbb{N}$ S. 52

(הארץ גוֹיִם, כָּל נַעֲמֵנָה אֶפְרַיִם
- וְאֶתְבָּשָׂג בְּנֵי-יִשְׂרָאֵל -)

ב-1^ר מינימום גודל ו/or קפ"ד A גודל גורם

, 0^n : מילים הולכות ונעלמות במקומות שונים א

MINIMUM 1278 mls from 1ⁿ stage (1971) 1198 pds

$t_{1,1} \parallel t_{1,2}$; $\exists j : t_{0,1} \parallel t_{0,2}$; $\exists i$

רְבָעִים , כַּיְלָה נָמָת לְבִזְבֵּחַ מִלְגָנָת

$$\frac{n \cdot d}{2} \quad \text{Ug} \quad t_{0,1}, t_{0,2}, t_{1,1}, t_{1,2}$$

בנין נס, גראן א. (טיגר) ניקולאiev

min $\gamma \gamma$ wif $m^k = 1^{\frac{n}{2}} \parallel 0^{\frac{n}{2}}$ nleq n?

$$t^* = t_{1,1} \parallel t_{0,2}$$

Codice (che se c'è) nel quale si trova

3 (g)

וניהר כי $\nexists (m^*, t^*) \in \mathcal{M} \times \mathcal{T}$ כך ש $Vrf_{\mathcal{F}_k}(m^*, t^*) = 1$

ולא $m^* \neq 1^n$ וגם $m^* \neq 0^n$

לפיכך $\Pr[\text{MacForger}_{\mathcal{F}, A}(n) = 1] = 1$ נובע מכך ש

בנוסף לכך $m \in \{0, 1\}^n$ וקיים $r \in \{0, 1\}^n$ בזאת כי

קיים (r, t) ב \mathcal{G} כך ש $r \in \{0, 1\}^n$

$$t = f_k(r) \oplus f_k(m)$$

לפיכך r מוגדר MAC-הו של m

בנוסף לכך r יתגלה כMAC-הו של m

ולא ניתן לשבור את ה-PPT

$\Pr[\text{MacForger}_{\mathcal{F}, A}(n) = 1] = 1$ נובע מכך ש

קיים $r^* \in \{0, 1\}^n$ וקיים $t^* \in \mathcal{T}$ כך ש

$Vrf_{\mathcal{F}_k}(m^*, t^*) = 1$ נובע מכך ש

$m^* = 0^n$ וקיים $r^* \in \{0, 1\}^n$ ב \mathcal{G} כך ש

$$(r^*, t^*) = (0^n, 0^n)$$

4 ו'

new row $n \in \mathbb{N}$ $\text{for } i \in \mathcal{S} \text{ are}$

$n \in \mathbb{N}$ $\text{for } i \in \mathcal{S}, f_{ik}(m) \oplus f_k(m) = 0^n$

min. \mathcal{S} in (r^*, t^*) (same row)

is k max. one, m^* always 1)

, $Vrfy_k(m^*, (r^*, t^*)) = 1 : 1 \dots ?$, never 0

the m^* - e row in table, etc

and, max. min. \mathcal{S} we get via for

apply self with m^* we get if \mathcal{S}

: $n \in \mathbb{N}$ for some new \mathcal{S}

, $\Pr[\text{MacForge}_{\mathcal{R}, A}(n) = 1] = 1$

new \mathcal{S} , and in all \mathcal{S} profit

5 sig

$\Pi_1 = (\text{Gen}_1, \text{Mac}_1, \text{Vrfy}_1)$ וריאנט Π של

$\Pi_2 = (\text{Gen}_2, \text{Mac}_2, \text{Vrfy}_2)$

לפיה Π_2 הוא Π_1 עם MAC_2 במקום MAC_1

הנובות הדרושים ל MAC_2 מושפעות מ MAC_1

מוגדר MAC_2 כ MAC_1 בז'ר MAC_1 ו MAC_2 מושפעת מ MAC_1

ולפיה MAC_2 מושפעת מ MAC_1 ו MAC_2 מושפעת מ MAC_1

ולפיה Π_2 מושפעת מ Π_1 , ו Π_1 מושפעת מ Π_2

ולפיה Π_2 מושפעת מ Π_1

לפיה $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ מושפעת מ Π_1

ולפיה Π מושפעת מ Π_2 מוגדר Gen \oplus

$\text{K}_1 \leftarrow \text{Gen}(1^n)$ אם ולו K_1 מושפעת מ Π_1

$\text{K}_2 \leftarrow \text{Gen}_2(1^n)$

$\text{K} = (\text{K}_1, \text{K}_2)$ $\{ \text{B} \}$ מושפעת מ Π_1

ולפיה Mac מושפעת מ Π_1 מוגדר Mac \oplus

$\text{t}_1 \leftarrow \text{Mac}_1(\text{K}_1, \text{m})$ מושפעת מ Π_1 מוגדר t_1

$\text{t}_2 \leftarrow \text{Mac}_2(\text{K}_2, \text{m})$

$t = (t_1, t_2)$ \wedge $N(k)$ \Rightarrow $\exists k_1, k_2$

$\forall k_1, k_2, k = (k_1, k_2) \wedge \exists m \text{ s.t. } \text{Vrfy } \oplus$

$1 \text{ sign} , t = (t_1, t_2) \text{ then } \exists m \text{ s.t. } m$

, $\text{Vrfy}_1(k_1, m, t_1) = 1 \wedge \text{Vrfy}_2(k_2, m, t_2) \wedge \text{some}$

$\rightarrow 0 \text{ sign } \wedge \exists m$

$\exists k_1, k_2 \text{ s.t. } \exists m \text{ s.t. } \exists n \text{ s.t. } \text{Vrfy}_1(k_1, m, t_1) \wedge \text{Vrfy}_2(k_2, m, t_2)$

$\exists k_1, k_2 \text{ s.t. } \exists m \text{ s.t. } \exists n \text{ s.t. } \text{Vrfy}_1(k_1, m, t_1) \wedge \text{Vrfy}_2(k_2, m, t_2)$

$\exists k_1, k_2 \text{ s.t. } \exists m \text{ s.t. } \exists n \text{ s.t. } \text{Vrfy}_1(k_1, m, t_1) \wedge \text{Vrfy}_2(k_2, m, t_2)$

$\exists k_1, k_2 \text{ s.t. } \exists m \text{ s.t. } \exists n \text{ s.t. } \text{Vrfy}_1(k_1, m, t_1) \wedge \text{Vrfy}_2(k_2, m, t_2)$

$\exists k_1, k_2 \text{ s.t. } \exists m \text{ s.t. } \exists n \text{ s.t. } \text{Vrfy}_1(k_1, m, t_1) \wedge \text{Vrfy}_2(k_2, m, t_2)$

$\exists k_1, k_2 \text{ s.t. } \exists m \text{ s.t. } \exists n \text{ s.t. } \text{Vrfy}_1(k_1, m, t_1) \wedge \text{Vrfy}_2(k_2, m, t_2)$

$\exists k_1, k_2 \text{ s.t. } \exists m \text{ s.t. } \exists n \text{ s.t. } \text{Vrfy}_1(k_1, m, t_1) \wedge \text{Vrfy}_2(k_2, m, t_2)$

$\exists k_1, k_2 \text{ s.t. } \exists m \text{ s.t. } \exists n \text{ s.t. } \text{Vrfy}_1(k_1, m, t_1) \wedge \text{Vrfy}_2(k_2, m, t_2)$

$\exists k_1, k_2 \text{ s.t. } \exists m \text{ s.t. } \exists n \text{ s.t. } \text{Vrfy}_1(k_1, m, t_1) \wedge \text{Vrfy}_2(k_2, m, t_2)$

$\Pr[\text{MacForge}_{k_1, k_2}(h) = 1] > \frac{1}{p_m}$

$\neq \frac{1}{p_m}$

Die Spur alle, B versteckt ist(?) und
, Mordgut, B(b) und Spur alle, A1 muss

$k_2 \leftarrow \text{Gen}_2(1^n)$, $1^n \xrightarrow{\text{MFG}} G_{\text{MFG}}$, $B \vdash \neg A \wedge f_1$, $R_2 \vdash \neg A \wedge f_2$

ו- **A** ב- **B**, מ- **C** ו- **D** -

$\beta - e$ k₂ and line 18, $t_2 \in Mac_2(k_2, h)$
 198 ~ A-f 1301, p¹⁸ ~ 2317 ~ { }
 . $t = (t_1, t_2)$ ~ N(0,1)

Gibit liegt bei ~10 A-e auf -

we know that \mathcal{B} , $(m^*, (t_1^*, t_2^*))$

, (m^t, t_1^*) ; if for (PPT and PFR) m_3^t

• MacFarlane, A (n) ionic Se, A-f

In the B-e model with k_1 rel., for τ
 $\text{Verf}((k_1, k_2), m^*, (t_1^*, t_2^*)) = 18 \text{ in } \mathbb{R}^N \text{ as } \lambda \rightarrow 1.02$

now we prove that $\Pr[\text{MachForger}_{A_1, B_1}(n) = 1] \geq \frac{1}{2}$

if m is chosen such that $\epsilon_{B_1} > \epsilon_A$

, m is chosen such that $\epsilon_{B_1} > \epsilon_A$

$n \in \mathbb{N}$ be some value such that $\epsilon_{B_1} > \epsilon_A$

is enough to prove

$$\Pr[\text{MachForger}_{A_1, B_1}(n) = 1] \geq$$

$$\geq \Pr[\text{MachForger}_{A_1}(n) = 1] > \frac{1}{p(n)}$$

since $\epsilon_{B_1} > \epsilon_A$

• since R_1 is safe now

R_2 must be safe if R_1 is safe



so R_1 is safe

הנחתה היא \hat{H} ו- $\hat{A}(h) = 1$ ב-1/3 ה███

בנחתה \hat{H} ו- $\hat{A}(h) = 1$ ב-1/3 ה███

PPT, A יוציא כיבוי גלובלי - מילוי גלובלי ו-
פונקציית גלובלי יוציא כיבוי גלובלי ו-
כיבוי גלובלי נסיבתני כיבוי גלובלי ו-

$$\Pr[\text{Hash}(\text{Col}_{\hat{H}, \hat{A}}(h)) = 1] > \frac{1}{p(n)}$$

לפונקציית גלובלי $A \rightarrow$ אוסף D , PPT
לפונקציית גלובלי $H_S(X)$
 $(S \in \{0, 1\}^n)$

$S = \text{Gen}(1^n)$ ו- $f_{S, n}$, 1^n מינימום א-רנדומלי -
 $A \rightarrow$ פונקציית גלובלי

$$x' = x || b$$

~~לפונקציית גלובלי~~ $y \in D$, $y \neq x$
 $y = y' || b'$

~~לפונקציית גלובלי~~ $y', x \in D$ -

לפונקציית גלובלי $D - e$ מושג
 $\text{Hash}(\text{Col}_{\hat{H}, \hat{A}}(n))$ מושג בפונקציית גלובלי

$y' || b' - 1$ $x || b$ מושג א-רנדומלי, ו-

$$H_S(x) || b = H_S(y) || b' \Leftrightarrow \hat{H}_S(y || b') = \hat{H}_S(x || b)$$

$$\Leftrightarrow b' = b \wedge H_S(x) = H_S(y)$$

10 (w)

$x \parallel b \neq y \parallel b'$ \Rightarrow $\hat{H}_S(x \parallel b) = \hat{H}_S(y \parallel b')$ \rightarrow $\text{if } b \neq b' \text{ then } \hat{H}_S(x \parallel b) \neq \hat{H}_S(y \parallel b')$

$x \neq y$ \Rightarrow $b = b'$ \Rightarrow $\hat{H}_S(x) = \hat{H}_S(y)$ \rightarrow $\text{if } b = b' \text{ then } \hat{H}_S(x) = \hat{H}_S(y)$

$\therefore x \neq y \Rightarrow \hat{H}_S(x) = \hat{H}_S(y) \Leftarrow$

$\hat{H}_S(x \parallel b) = \hat{H}_S(y \parallel b')$ \rightarrow $\text{prob. of } b \neq b'$ \rightarrow $x \neq y$ \rightarrow $x \parallel b \neq y \parallel b'$ \Rightarrow $\hat{H}_S(x) \neq \hat{H}_S(y)$

$\text{HashCol}_{A, A}^{\wedge}(h) = 1 \Leftarrow \hat{H}_S(x) = \hat{H}_S(y)$

$\text{HashCol}_{H, D}^{\wedge}(h) = 1 \Leftarrow$

$\text{new row } n \in \mathbb{N}$ is full

$P[\text{HashCol}_{H, D}^{\wedge}(h) = 1] \geq P[\text{HashCol}_{A, A}^{\wedge}(m) = 1]$

$n \in \mathbb{N}$ \Rightarrow $\text{new row } \xrightarrow{\text{if } h \text{ is full}} \text{new row } h$

$P[\text{HashCol}_{H, D}^{\wedge}(h) = 1] > \frac{1}{P(n)}$

$\text{new row } h \text{ is full} \rightarrow$
 $\text{new row } h \text{ is full} \rightarrow$

11/18

, $x \in \{0,1\}^{*-1}$; $s \in \{0,1\}^n$ für (2) sie

$\sim \text{exp}(n-1) \rightarrow \text{number of } W_S(X) \text{ in } k)$
 $\cdot H_S(X) \text{ is the sum of squares}$

↪ Bsp. 1) Es soll nun gezeigt werden, dass $W = (\text{Gen}, W)$ ein Kollektiv ist.

zur H₂O und zur D₂O wird mehr H⁺ konzentriert als S_{CO₂}, B_n bei NEIN falle raus

$$Hs : \{0,1\}^* \rightarrow \{0,1\}^{n-1}$$

1887-1891 H. M. Miller et al.

$H_S : \{0,1\}^k \rightarrow \{0,1\}^n$ sei $S \subseteq \{0,1\}^n$ so si $n \in \mathbb{N}$ für
einen $b \in \{0,1\}^n$ -! $x \in \{0,1\}^k$ für $\neg S$

$$H_5(x||b) := H_5'(x) || b$$

الله يحيى الله ربنا رب العالمين

$w_s(x) \underset{x \in \{0,1\}^n}{\text{def}} x \in \{0,1\}^n$ if $s \in \{0,1\}^n$

you get, $H_S(x)$ be a single value $n-1$
 regions $b \in \{0, 1\}$ -! $x \in \{0, 1\}^n$ for \in

$$\cdot W_S(X||b) = H_S'(X)$$

: $X \in \{0,1\}^*$ 5P, prob

$$W_S(X||0) = H_S'(X) = W_S(X||1)$$

: 8 A 2.71 9.3711

$\exists n \forall S \in \{0,1\}^n$ \exists 1^n (S) prob

$\rightarrow X||0 \neq X||1$ wegen 8.51 $\rightarrow X||0, X||1$

: prob, $W_S(X||0) = W_S(X||1) \approx 1$

$$P(\text{HashCol}_{W,A}(n)=1) = 1$$

ausf. wie $\sim 1/2^n$ sieht W 

$\sim 1/2^n \cup 1 - 1/2^n$

using $\sim 1/2^n$ \rightarrow $\sim 1/2^n$ \rightarrow if we

NONP UK, NRG \rightarrow wie sieht es aus
wahrscheinlichkeit P(n) \rightarrow 1/2^n, PPT, A 2.91
wegen $n \in \mathbb{N}$ 2078 \rightarrow 1/2^n

$$\cdot P[\text{MacForge}_{R,A}(n)=1] > \frac{1}{P(n)}$$

: 8 D $\sim 1/2^n$ 2.71

: Spurkennung, 1^n \rightarrow NRG \rightarrow wie sieht es aus
 $Q \in \{f, f_k\}$

13.6.8

$f \leftarrow \text{func}_{n,n} - 1$ zum poln $K_1 \leftarrow \{0,1\}^n$

zum poln $K_2 \leftarrow \{0,1\}^n$ nach $\text{rel}(P, M)$
 $m \in K_2$ für A mit $P_2(m)$

mit exp , $m \in \{0,1\}^n$ A ist def. gp (3)

$t_2 := 2 \| f_{k_2}(z) A - P \circ \varphi \circ \Sigma := O(m)$

(m^*, t^*) nicht neu A ist gp (4)
 $t^* = O(m^*)$ exp

$t^* = 2^* \| f_{k_2}(z^*) \text{rel } 1 \text{ und } (5)$
 $O(25n)$ nicht

$Q = f_{k_1}$ nicht ~~gp~~ eingefügt \checkmark

D, A ist $m \in \{0,1\}^n$ def. gp Σ

poln φ über φ , $f_{k_1}(m) \| f_{k_2}(f_{k_1}(m)) \circ \varphi$

$\text{MacForger}_{D,A}(h) \rightarrow D$ mit $A - P$ nicht

1. nach oben D nicht φ $\circ \varphi$



$$P(D^{f_{k_1}(1)}(m)=1) = P[\text{MacForger}_{D,A}(h)=1] > \frac{1}{P(h)}$$

$n \in \mathbb{N}$ die erste $2 \cdot 2^n$ freie w

$f \in \text{Func}_{n,n}$ \quad $\text{Satz } O = f \text{ ist } \otimes$
 (1) $\exists A \quad \text{K} \text{ ist } f_{k_1}(f(m^*)) \neq f_{k_2}(f(m^*))$
 $\quad \quad \quad \text{z.B. } (m^*, t^*) \text{ raus}$

$[t^* = f(m^*) \mid \forall k_2 (f(m^*)) \wedge m^* \notin Q] \Leftrightarrow D^{f_{k_1}(\cdot)}(1^n) = 1$
 $\quad \quad \quad \text{wahrsch. ein } A \text{ mit } f_{k_1} \text{ ist } 1^n$

$P(z^* = f(m^*)) = \frac{1}{2^n} \quad \text{S.K., } z^* \in \{0,1\}^n$

$\quad \quad \quad \text{z.B. pols } \text{w.p. } f \in \text{Func}_{n,n} \text{ ist}$
 $f(m^*) \in \{0,1\}^n \text{ d.h. } m^* \notin Q \text{ ist}$
 $f(m) \in \{0,1\}^n \text{ ist } \text{w.p. } f(m) \in \{0,1\}^n$
 $\quad \quad \quad \text{ist } m \in Q \quad \text{w.p.}$
 $\quad \quad \quad \text{z.B. } n \in \mathbb{N} \text{ ist}$

$P[D^{f_{k_1}}(1^n) = 1] = P[f(m^*) \mid \forall k_2 (f(m^*)) \wedge m^* \notin Q]$
 $f \in \text{Func}_{n,n} \quad f \in \text{Func}_{n,n}$

$= P[z^* = f(m^*)] = \frac{1}{2^n}$
 $z^* \in \{0,1\}^n$
 $f \in \text{Func}_{n,n}$

Is fix?

מונען $N \in \mathbb{N}$ ו δ ממשי ו ρ

$$|P[D^{f_{k_1}(\cdot)}(1^n) = 1] - P[D^{f(\cdot)}(1^m) = 1]| =$$
$$\forall i \in \{0, 1\}^n \quad f \leftarrow \text{Func}_{n, m}$$

$$= |P[D^{f_{k_1}(\cdot)}(1^n) = 1] - \frac{1}{2^n}| \geq \frac{1}{p(m)} - \frac{1}{2^n} \geq \frac{1}{2p(m)}$$

$N \in \mathbb{N}$ ו ρ ממשי ו δ ממשי $\frac{1}{2^{n+1}} < \rho$
 $n > N$ ו $\delta < \rho$

$$\frac{1}{p(m)} - \frac{1}{2p(m)} = \frac{1}{p(m)} \left(1 - \frac{1}{2}\right) = \frac{1}{2p(m)} > \frac{1}{2^n} \Leftrightarrow$$

$$\Leftrightarrow \frac{1}{p(m)} > \frac{1}{2^{n+1}} \Leftrightarrow \frac{1}{p(m)} - \frac{1}{2^n} > \frac{1}{2p(m)}$$

• PRF \Rightarrow f - אטום וריאנט

אטום וריאנט $(1 : S)$ שפה

טיפוס טריביאלי ותפקיד MAC מודולריטי

ל. k_1 , k_2 , m ו ρ סינטטיים $(k_1, k_2) \in \mathcal{K}$ ו $m \in \text{Gen}(1^n)$ מודולריטי

new sig, PPT, A new sig resp; 25k
 : new new new or stark worse p, $P(n)$

$$\cdot P\{\text{MacForge}_B[t \text{Leakage}_{R,A}(h) = 1]\} > \frac{1}{P(h)}$$

for all, PPT, A' new worse new 15k
 : R inner enc

: $\forall b \in \{0,1\}^n$ new good found

$$\cdot b \leftarrow \{0,1\} \quad \text{new pair } \{b\} \quad (1)$$

b has in Gf for A nice find (2)

: m , $m \in \{0,1\}^n$, A resp BP (3)

$$\cdot t := \text{Mac}_k(m)$$

(m^*, t^*) good 13.3 nice now A re $\gamma_{\{b\}}$ (4)

$$\cdot (m^*, t^*) \text{ good}$$

: good nice pair

$$MF_{R,A'}(h) := \text{MacForger}_{R,A'}(h),$$

$$P_1 := P[b \neq k_1] \cdot P[MF_{R,A'}(h) = 1 \mid b \neq k_1] =$$

$$= \frac{1}{2} P[MF_{R,A'}(h) = 1 \mid b \neq k_1],$$

$$\begin{aligned}
 p_2 &:= P[b=k_1] \cdot P[MF_{R,A^c}(h)=1 \mid b=k_1] = \\
 &= \frac{1}{2} P[MF_{R,A^c}(h)=1 \mid b=k_1] = \\
 &= \frac{1}{2} \cdot P[\text{MacForgeBitLeak}_{A^c}(h)=1] \geq \frac{1}{2} \cdot \frac{1}{P(h)} \downarrow \\
 &\quad \text{siehe oben}
 \end{aligned}$$

○ Zwei arbeiten zusammen
 zeigen $n \in \mathbb{N}$ von f_R ist f_R^n

$$P[MF_{R,A^c}(h)=1] = p_1 + p_2 \geq p_2 > \frac{1}{2P(h)} \downarrow$$

siehe oben

und die RC ist sichere

: MAC kann nur 125 bits

$$RC = (\text{Gen}, \text{Mac}, \text{Vrfy})$$

unterteilt in drei Teile

A benötigt für : ohne den keiner

region, $\ell(\cdot)$ used to , PPT

$$\Pr[\text{MacForgeLeftHalfBitsLeakage}_{R,A}(h) = 1] \leq \frac{1}{P(h)}$$

! Major error , given $s_p \in \mathbb{N}$ for

$\text{MacForgeLeftHalfBitsLeakage}_{R,A}(h)$

for pair $\text{MacForge}_{R,A}(h)$ major error

$A \in \{0,1\}^n$ $\text{MacForge}_{R,A}(h)$ outputs s_p

, $\sim_{\mathcal{A}^*(h)} \text{Gen}(1^n)$ (\mathcal{A})

and \mathcal{A} $\in \{0,1\}^n$ major error

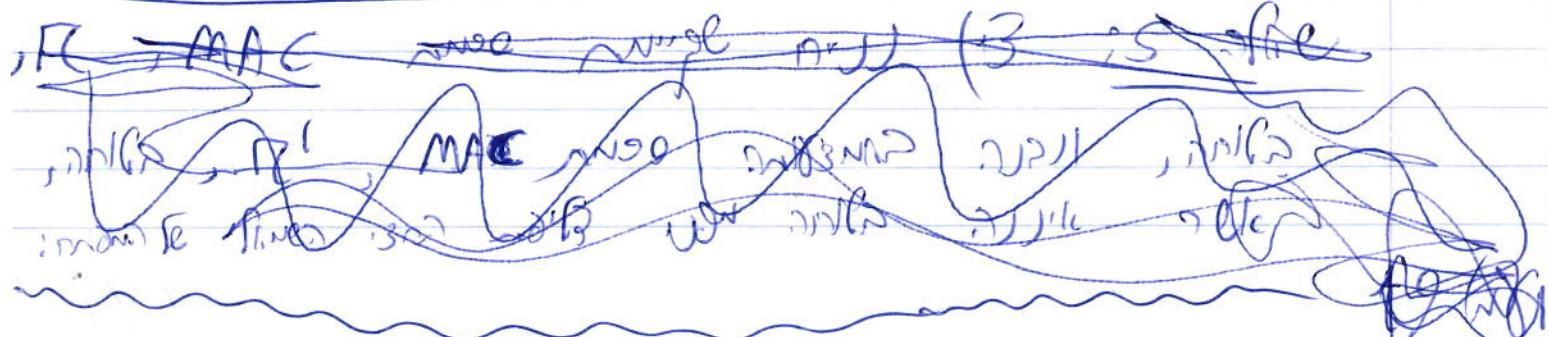
major $\in \{0,1\}^n$ and $\underline{\neq} 1^n$ $\sim_{\mathcal{A}^*(h)}$

major output major , $1 \leftarrow \text{Gen}(1^n)$

(\mathcal{A} major $\sim_{\mathcal{A}^*(h)}$ same output)

major output $\text{Gen}(1^n)$ major output

major \in 1^n



\mathcal{R} - MAC and verify $\mathcal{R} \models \text{MAC}$

and \mathcal{R}' , $\mathcal{R}' = (\text{Mac}', \text{Gen}', \text{Vrfy}')$

$\mathcal{R}' = (\text{Mac}', \text{Gen}', \text{Vrfy}')$, \mathcal{R}' - MAC and

sound (since \mathcal{R}) \mathcal{R}' is sound, \mathcal{R}' is secure, \mathcal{R}' is \mathcal{R}

sound \mathcal{R}' is secure

; 1^n given \mathcal{R}' is Gen' \oplus

. $l := |\mathbb{K}|$ then $k \leftarrow \text{Gen}(1^n)$

, $k = k_1 || k_2$ given \mathcal{R}' is Mac' \oplus

. $m \in \{0,1\}^*$ given \mathcal{R}'

$\text{Mac}'_{k_1 || k_2}(m) := \text{Mac}_{k_1}(m)$

, $k = k_1 || k_2$ given \mathcal{R}' is Vrfy' \oplus

. $t^* \in \{0,1\}^*$ given $m^* \in \{0,1\}^*$ given \mathcal{R}'

$\text{Vrfy}'_{k_1 || k_2}(m^*, t^*) = \text{Vrfy}_{k_1}(m^*, t^*)$

with \mathcal{R}' sound \mathcal{R}' is secure

, PPT, A given t^* to \mathcal{R}' given \mathcal{R}' $\vdash p(n)$ new \mathcal{R}'

20 WY

newer nell le neue zeit

$$\cdot P(\text{MacForge}_{R,A}(n) = 1) \geq \frac{1}{P(n)}$$

: Vrfj' map, 25%

$$\text{MacForge}_{R,A}(n) = 1 \Rightarrow \text{MacForge}_{R,A'}(n) = 1$$

: neue nell le neue zeit p*i*

$$P(\text{MacForge}_{R,A'}(n) = 1) \geq P(\text{MacForge}_{R,A}(n) = 1)$$

$$> \frac{1}{P(n)}$$



: R mit f_{pk} und kA A' von }
, 1^n (G) und p*i* }
1^n f_{pk} A mit f_{pk}(A)
Mac_R(m) >= A für m ∈ {0,1}^* und f_{pk}(m)
mit (m^{*}, t^{*}) geant, dann A = e(y) >= 1
· (m^{*}, t^{*}) passt }
}

Mac_{R||0,1}(m) = Mac_R(m) : neu mit m ∈ {0,1}^* f_{pk}
mit (m^{*}, t^{*}) geant A = e(y) und A' = f_{pk}(A)

~ with respect to A' and MacForgers, A (m)

- INSTR upon $A-e$ with respect to j

→ now we can get two sets $\oplus - \ominus$

which will be called α and β
and be shown (3n) ~~as~~ $\alpha\beta$

2nd step give plan, repeat 251

$$k_L = k - 1^n \quad (\text{if}) \quad \text{middle D}$$

gives step size, $k' = k_{10} \leftarrow \text{GCD}(k, n)$

$$\text{Mac}_{k10^l}(0^n) = \text{Mac}_k(0^n)$$

• 1 more result $(0^n, \text{Mac}_k(0^n))$ exists

$R = (Gen, Mac, Vrfy)$ on $(1 \leq 6)$ where

$\text{mig} \rightarrow R' \cup f(R)$ mig mig mig

, mig mig mig mig mig mig

$\{f_i \sim \mathbb{Z}_2^n \mid \text{if } i \in \mathbb{Z}_2^n : K_R$

$\text{mig} \geq p(n) \text{ mig}, \text{PPT}, A$

$\text{mig} \text{ mig} \text{ mig}$

$$\Pr[\text{MacForgeRH Bits Leakage}_{R', A}(h) = 1] > \frac{1}{p(n)}$$

R mig mig , PPT , A' mig mig
 $: k_L \leftarrow Gen(1^n) \text{ mig}$

$, 1^n \text{ mig}$

$K_R \leftarrow \{0, 1\}^n \text{ mig}$

$. K_R \text{ mig}$ m mig A mig f_R (2)

$\text{mig}, A \in \{0, 1\}^n \text{ mig}$ (3)

$$t := \text{Mac}_{k_L}(m \oplus K_R)$$

$. t \text{ mig}$

$\text{mig}, (m^*, t^*) \text{ mig}$ $A - e \text{ mig}$ (4)

$$. (m^* \oplus K_R, t^*)$$

23/08/23

pair $(f_{\text{hash}}, \text{PPT})$ must be A'
soundness review

MacForge RH Bits Leakage_{R, A}(h)

A - f

$m^* \oplus K_R \neq m \oplus K_R$ is a m^* from review

g response Verfy' \sim_{PRG} of

Verfy_{K_L}($m^* \oplus K_R, t^*$) = 1 \Leftrightarrow

Verfy_K(m^*, t^*) = 1

is enough to show that Proj. is a PPT

$P[\text{MacForge}_{R, A'}(h) = 1] =$

$= P[\text{MacForge RH Bits Leakage}_{R, A}(h) = 1] > \frac{1}{P(h)}$

which R need to be sound

$\mathcal{R} = (\text{Gen}, \text{Mac}, \text{Vrfy})_{\text{NIZK}}$ (2:16) the

and with zero

, $\mathcal{R}_2 = (\text{Gen}_2, \text{Mac}_2, \text{Vrfy}_2)$ 2:2

, $m \in \{0,1\}^n$ such $K \leftarrow \text{Gen}(1^n)$ private key

$\text{Mac}_K(m) = \text{Mac}_K(m) || m$

such that $\mathcal{R}_2 \subseteq \text{NIZK}$

{(h, m) s.t. there exists a w

private key, $P(h)$ public, PPT, A

; $n \in \mathbb{N}$ w.r.t. $\text{Pf}_{\mathcal{R}_2}$

$\Pr[\text{MacForge}_{\mathcal{R}_2, A}(h) = 1] \geq \frac{1}{p(n)}$

; 1ⁿ GPK private, PPT, A' and DPK

. 1ⁿ for A and f₂(m)

and GPK, m, A be sign GPK (2

$\text{Mac}_K(m) || m$ is w.r.t. A and $\text{Mac}_K(m)$

, $(m^*, t^* || m^*)$ given A and B

. (m^*, t^*) used

25' NY

ans? A -> F for pol P7 and A'

MacForge_{R2,A(h)} ; never make broken
if you open A never break

$$f^* = \text{Mac}_R(m^*)$$

never open A' negl

never open A' negl

$\forall n \in \mathbb{N}$, if you open A, open A - e

negl

$$\Pr[\text{MacForge}_{R,A,h}(n) = 1] \geq$$

$$\geq \Pr[\text{MacForge}_{R_2,A,h}(n) = 1] > \frac{\epsilon}{P(n)}$$

and \cap some job done

~~MacForge_{R2}~~, $\cap R_2$ vs

difficult to do
original tour, needs two or less

\mathcal{R} 2nd \mathcal{R}_2 \rightarrow

7.8 70% if $\mathcal{R}' \cup \mathcal{R}_2$ \approx

and so (level 3) and P

: PPT, ① 20, 23)

: I^n (P part)

: $\int_{\mathcal{R}'} 0^n$ approx 0% 78% \approx 0% (1)

$\text{Mac}_{K_L}(0^n) = \text{Mac}_{K_L}(0^n \oplus K_R) / |0^n \oplus K_R| =$

$\text{Mac}_{K_L}(K_R) / |K_R|$

~~K_L is 1% K_R will bring it to 0.2~~

$\text{Mac}_{K_L}(I^n \oplus K_R) \approx 0.5%$ due to D part

$m^* = I^n$ need (m^*, f^*) 7.5%

$f^* = \text{Mac}_{K_L}(I^n \oplus K_R) / |I^n \oplus K_R| - \frac{1}{9}$

$K_L \rightarrow K_R$ about 7%, PPT due to D, best

: P, $I^n \oplus K_R \neq 0^n \oplus K_R$: negl, 72% if yes

, 1 approx 10% often 0 $\Leftarrow I^n \oplus K_R \neq Q$

. and only I^n need P 72% 78%