2021 CYBERSECURITY : THE FOUNDATION OF DIGITAL REFORM

“ ”

ԓh fl Ố ᴸ Ợ á

ᶻ ẹ̆ ㇒ Ḡ ɯ\ ẹ̆ ỗ

g, ч‘ Ţ ά p ɨ ~ ɹ Λ [OBJ] Ш Φ ≈ و

Facebook ⅛ 3 ≠ ɨ ω3 ǎ Ł Ɑ [1]

Instagram ⅛ 3 ω ʌ ص9500 ǎ Ł Ɑ

Ƀ Ţ ɹ ω ʌ ص400 ǎ Ł Ɑ q‘ [2]

ɣ Ǐ ~ ⅛ 3 ω32 ǎ g, Ɑ q‘ [2]

g ч ɣ g Ị = Ụ ∫ ﻱ ك ٧ ا ڑ ۷

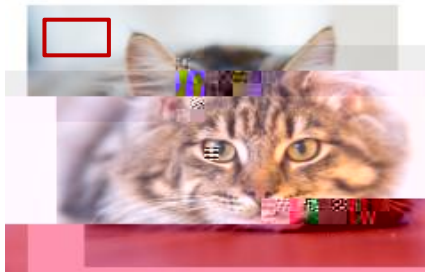
...

...

Clearview AI ʒ ᴎ ỉ ﻝ Facebook YouTube ⊐ Venmo ч ķ п ∧ ص30 ă g ᑕ _ á

OBJ _ ሀ ᵛ̈ ﻝ ﻝ Ỉ ﻝ ﻝ ƥ = ω ʒ ˇ ` OBJ ừ ̀ Ţ ώ ﻝ 600 Ķ _ ڤ Φ ɾ

g ■ ỷ ẹ OBJ g, ч Ѵ ˙ ʻH ɾ . g, ч ڭ ٧ ⌠ ᵢ OBJ l ɒ



g, ч ˋ 1

´ ‰ 5 ⅄

ŭ 5 ⅄ ‹ ‘

g, ч È Ẇ ı ά

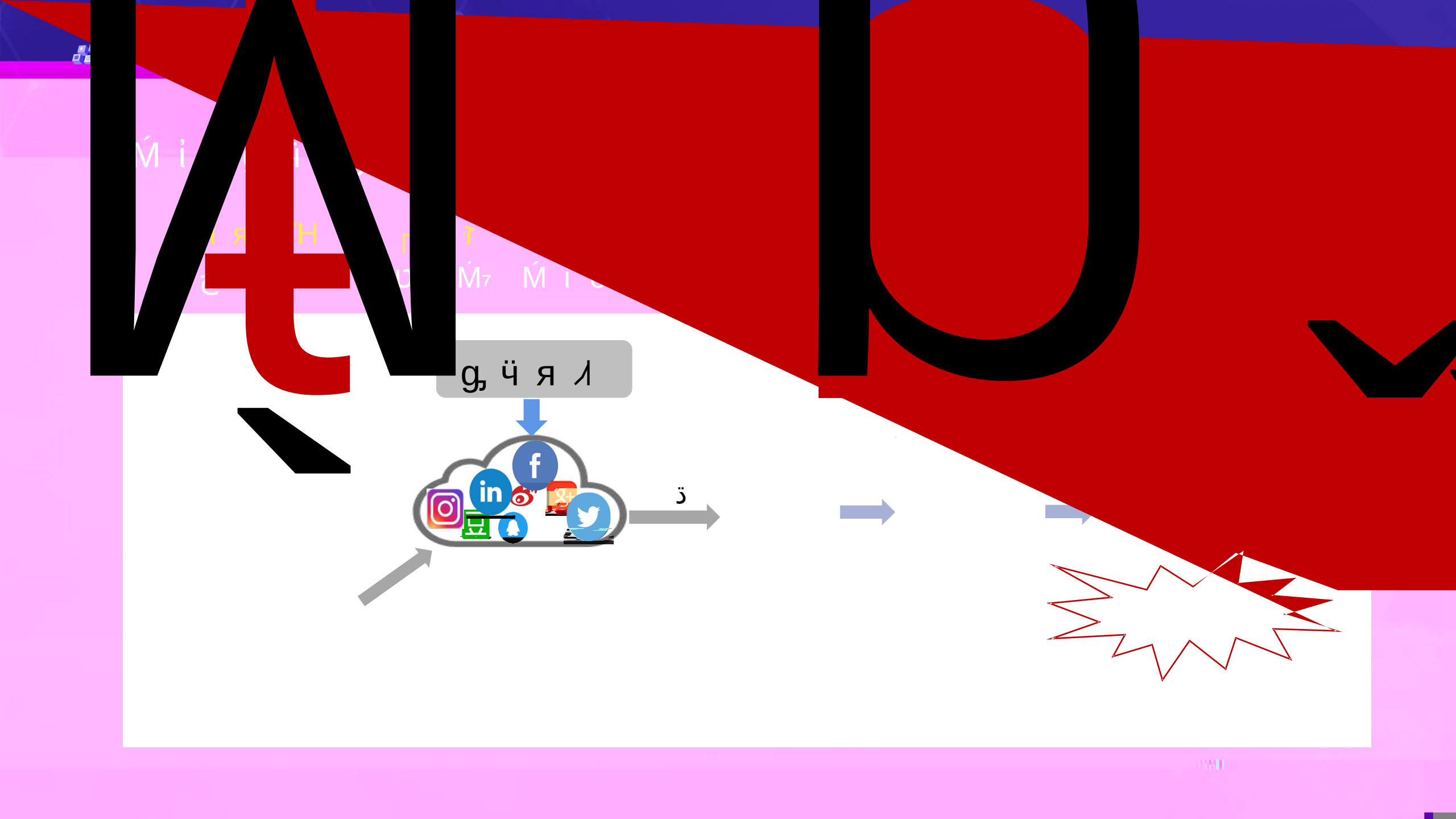
Ά ₌ R ㄣ R ¯ OBJ ■ ỷ ¯ ㄨ ㄨ ㄟ ı ᶎ ¸ OBJ

g, ч ₅ Ʊ ώ п ⌈ OBJ Ụ

D Ά ₌ ɾ ڭ ٧ ĭ OBJ ㄨ ₩ ㄣ ∫ ㄇ ʻH

ḅ ŭ ₩ ㄣ ⊃ ; ˇ ԁ ṇ | ˈ ı g DNNs OBJ

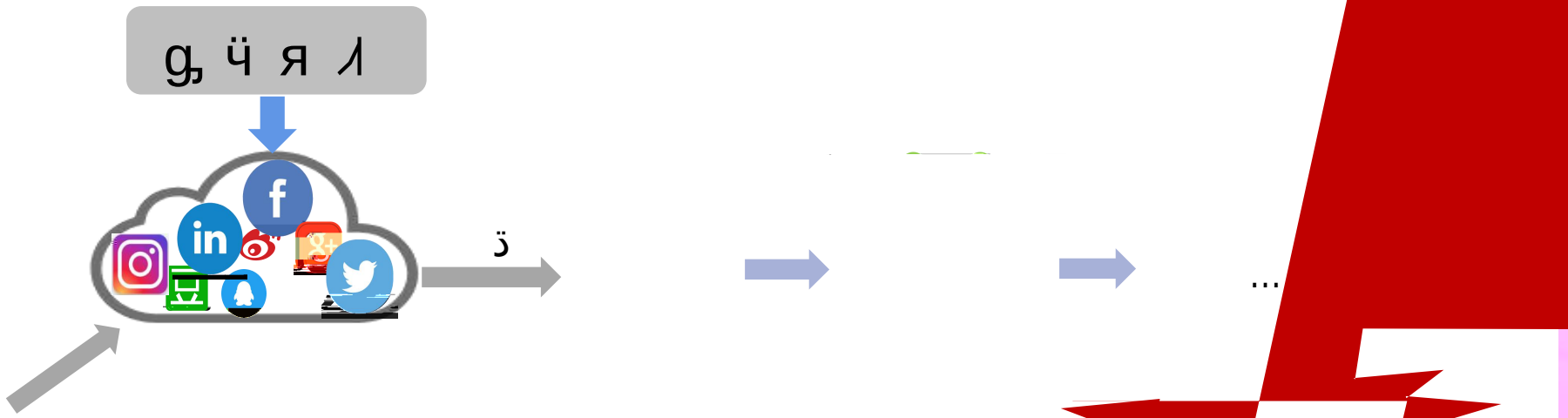
g, ч Ѵ ˙ ₩ ʒ



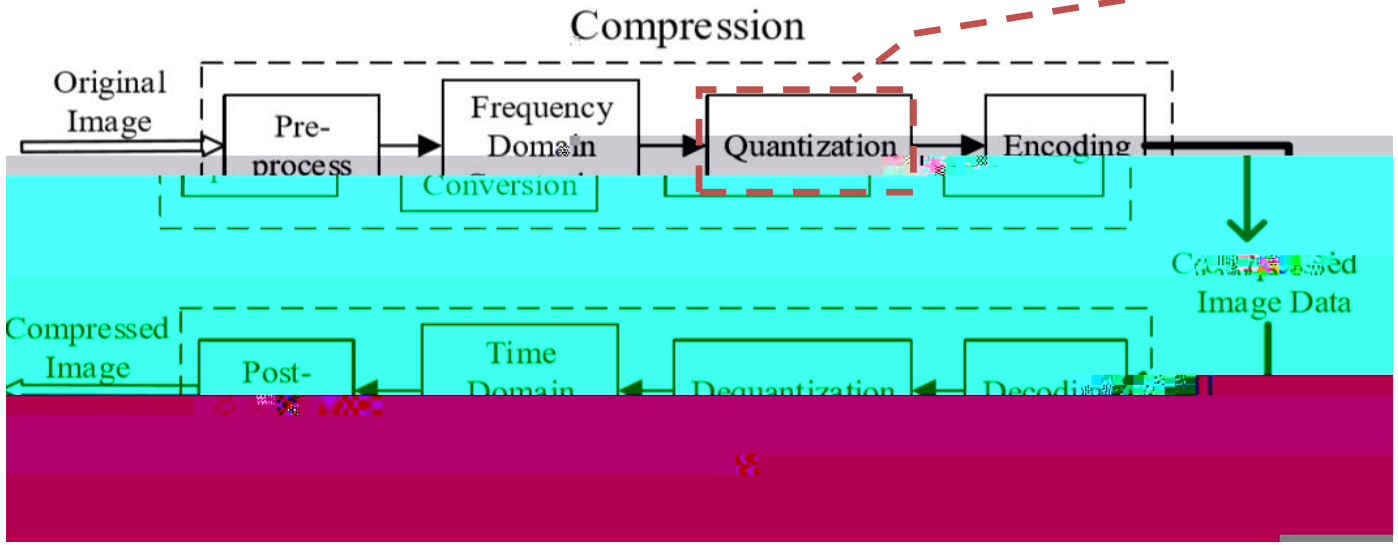
Ḿ ḭ ớ ḡ ч ﻝ ص ۊ ‟Ω я ﻝ ª ˜ ¸ ⊃Ḿ ḭ ớ

ḡ ч я ﻝ Ḥ ẍ ┌ Ẓ ŧ ˜ Ẉ ᴶ ⁋ ` ﻝ ڼ ° ◊ ⁼ ώ ڎ ڈ ڑ ۊ ' Ꞇ ĵ

_ ڎ [OBJ]Ḿ ḭ ớ ӈ ᴗ Ṁ₇ Ḿ ḭ ớ ḡ ч ¸ ۊ



g, ч я л \ | OBJ ı ỉ ễ ` ~ Ṁ7 ğ ı ắ i я л OBJ Ḿ i ớ g, ч



õ ¨Ω я л OBJ ا ص ١

Є ʒ OBJ g, ч я л Ά | ĩ g

ʒ ỷ OBJ Ḿ i ớ g, ч ı ắ \ | Л ķ

~ Ẉ J OBJ я л Ά Ã ĩ ₅ ḧ OBJ ắ

ф, Ḿ л OBJ | Ḿ i ʒ ớ

g, ч я л \ | [OBJ] ı ĭ ð ˙ ~ Ṁ7 ǯ ı ă i я л[OBJ]Ḿ i ớ g, ч

; Ḿ g, ч ˙ 1 ₩ ʒ [Seong et al. 2017]
; Ḿ ´ ‰ 5 ₩ ʒ [Liu et al. 2017]
; Ḿ ŭ ₩ ʒ [Shawn et al. 2020]

JPEG [Richard et al. 2017]

پ ¨ ı ĭ[OBJ]JPEG я л \ | 6 ı ĭ ė Ã

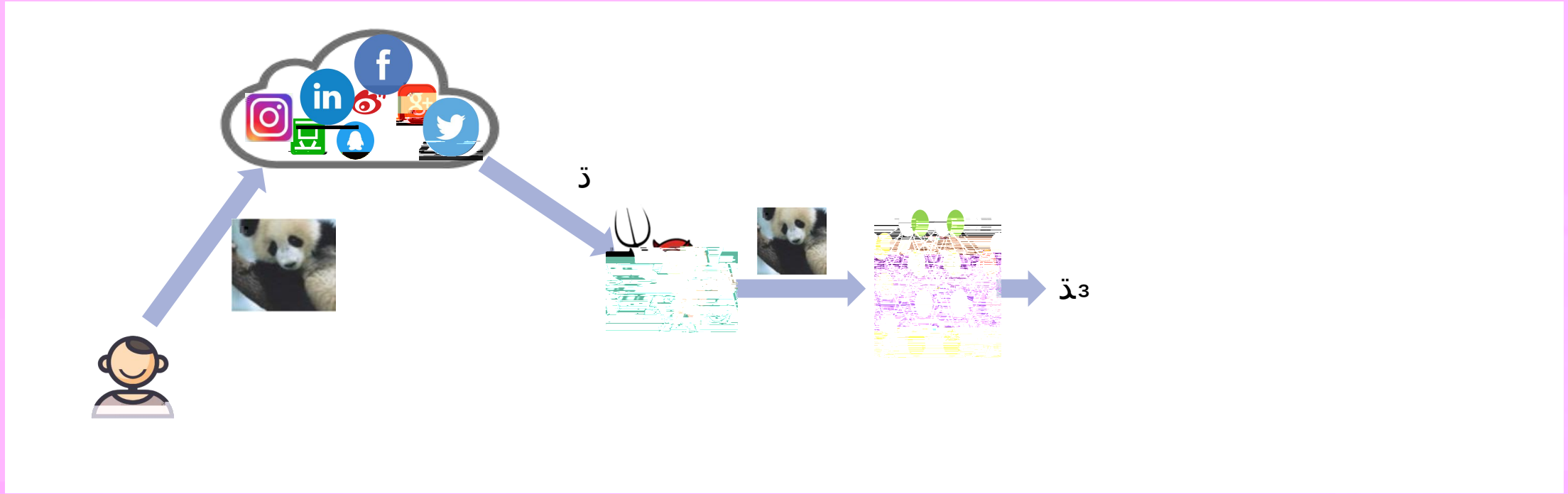
ļ ∂ JPEG я л \ | ˀ ʜ v Ѽ ș

ώ ϒ ἰ я ㄴ Ḿ ἰ ό ℊ ч ɨ ἄ Ά ϱ ϰ˜ ⸗ ㄴ ℊ ч ڭ ϒ ΐ

ʿ Ḿ ἰ ό ℊ ч ئ Ṁ ᾠ` ἃ n ệ ڃ ئ ڭ ϒ Ụ

Ḿ ἰ ό ℊ ч ъ ɬ ἰ я ㄴ ό ɜ ª ŋ ʻY Ъ Ḿ ἰ ό

ڰ ɾ ª ˜ Ψ ᴶ ъ ῶ ἰ ʿ ˜ я ㄴ ˝ ڰ Ḿ ἰ ό



ώ ϒ ί я ㄴ Ḿ ί ό ℊ ч ı ǎ Ά ђ ϰ ˜ ㄴ ㄴ ℊ ч ڭ ϒ ΐ

˜ Ẉ ᴊ я ㄴ Ά Ã ΐ ₅ ḣ

ŋ ΐ ‰ ´ я ㄴ ∖ | ҙ Ầ

Ḿ ǎ ᾽ ب ΐ “ س ¨ ”

ˡ ί я ㄴ ∖ | ⊐ g ₃ ů Ḿ ί

¯ ı ǎ ∖ | Ⅎ ķ

~ Ẉ ᴶ ﴾Ꮒ ό و

“ ”

ٹ ٬A Ḿ ~ Ẉ ᴶ پ ٹ ﴾я ﻝ Ά Ã ᵑ ٬A~ я ﻝ ٧ | ȝ ̓ ԋ v ٬Ω

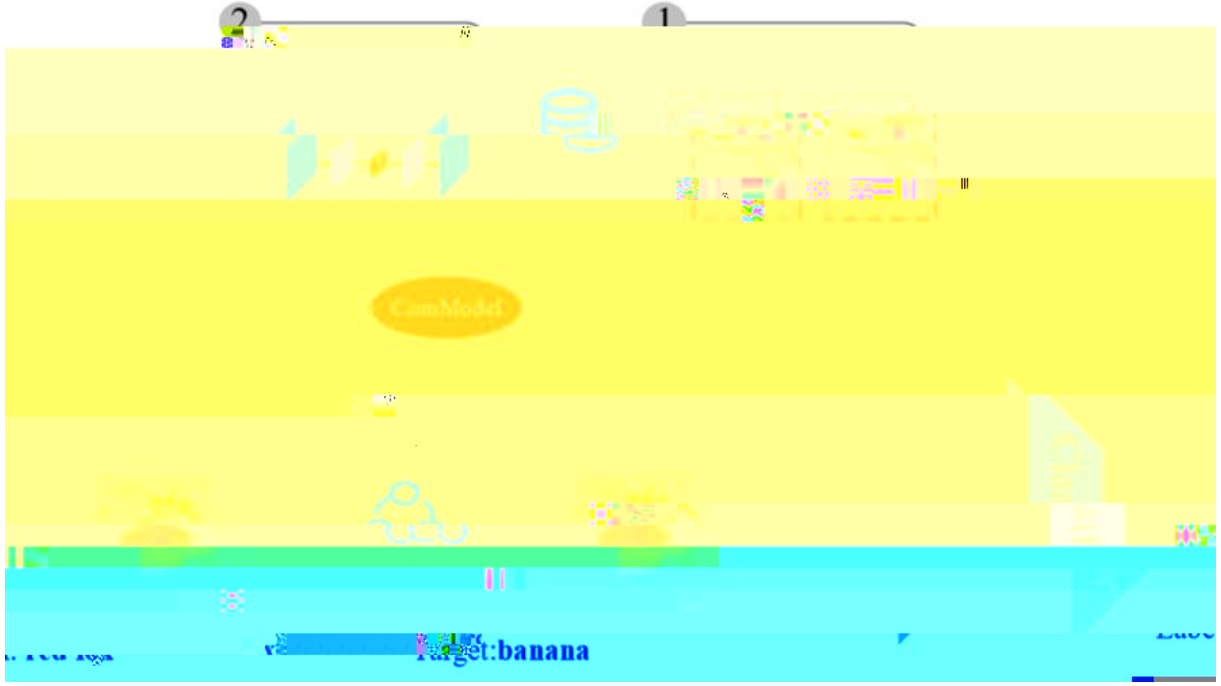
- ˋ g ӵ ᵎ q* Ẃ ⊨ ɳ

ώ g ⍲ H J H - - H H H H

■ ỷ¨ ﻝ ﻝ ﻵ ᵽ ᵹ ᵾ ³ ښ ﻟ T ﻝ ⊓ ệ ầ[OBJ]ᾧ '

Ф ш g ﾊ H J. H OBJ я л ė ₩ ʒ - ɾ ⊃ Ḋ ɡ ч я л ɡ ч Ѽ Ѿ Ѽ ѽ ѕ л ę я л ∖ | OBJ ė ė Ã

g я л ė ₩ ʒ ѽ ف א õ Ḿ ì ¯ ı ă ∖ | ı ă ì я л Ḿ ì ó ɡ ч



ѽ ѕ

ʒ n п ⊃ Ḋ ɡ ч ⁼ я л ɡ ч OBJ Ѽ Ѿ ѽ

ѕ л Ф ш OBJ

₩ ʒ ę b ҷ Ѽ ⊃ ɡ я л ɡ

ѽ ف א õ ∖

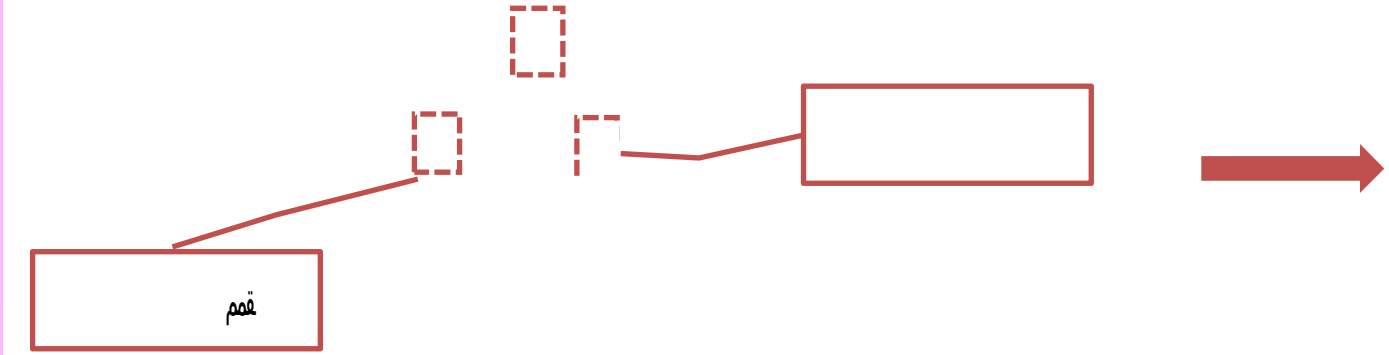
| ı ă ì я л OBJ Ḿ ì ó ɡ ч

2021 WEST L
CYBERSECURITY CONFE
西湖论剑 · 网络安全

´ ‰ ɯ Ą Ḿ i ¯ OBJ i я л ό

ً ḧ ᵇ Ḿ i ¯ ئ Ṁ₩ ȝ ڑ ڃ ئ OBJ ⌋ '

ḧ ᵇ Ḿ i ¯ ئ Ṁ₩ ȝ ڑ "Y ḧ OBJ ⌋ '



´ ‰ ɯ Ă Ḿ ì ¯ OBJ ì я ʌ ó r

g FGSM[1], BIM[2], MIM[3] OBJ ∂ ɹ ộ ỳ ∂ ɹ ì я ʌ Ḿ ì ¯ ҏ ´

‰

$$\arg\min_r ||r||_p$$

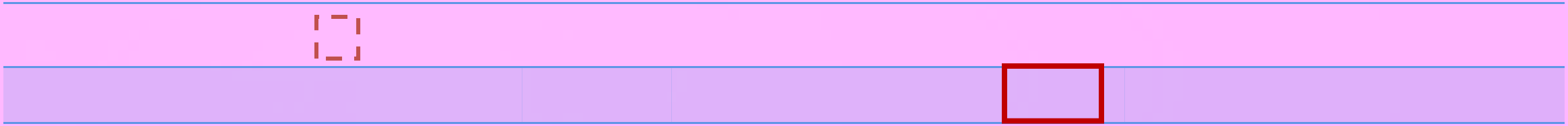
$$r = sign\left(\nabla_x \mathcal{L}\left(C\left(ComModel(x;\theta)\right), t\right)\right),$$

$$x_{t+1} = clip\left(x_t - \alpha \cdot r_t\right), x_0 = x$$

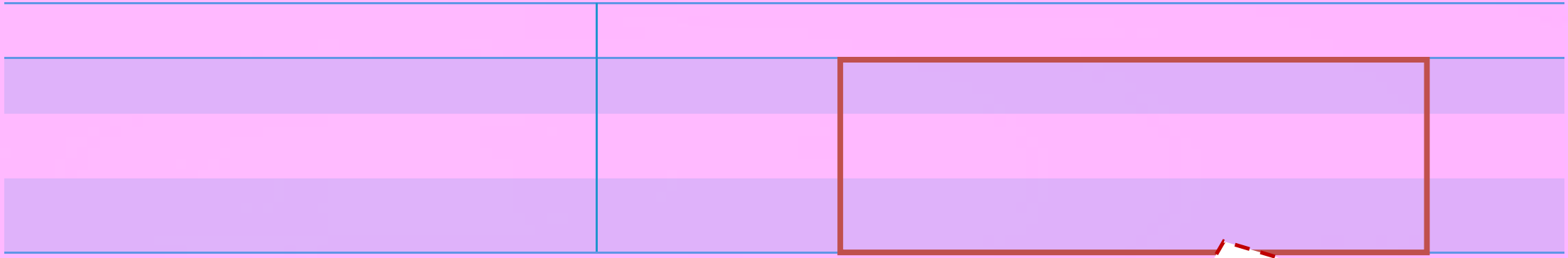
$$x_{t+1} = sign\left(m_t + \nabla_x \mathcal{L}\left(C\left(ComModel(x_t;\theta)\right), t\right)\right)$$

$$x_{t+1} = clip\left(x_t - \alpha \cdot r_t\right), x_0 = x, m_0 = 0.$$

ˇ Ω ˜ Ω ˛ Ч ă ŕ ă ŕ ă ŕ



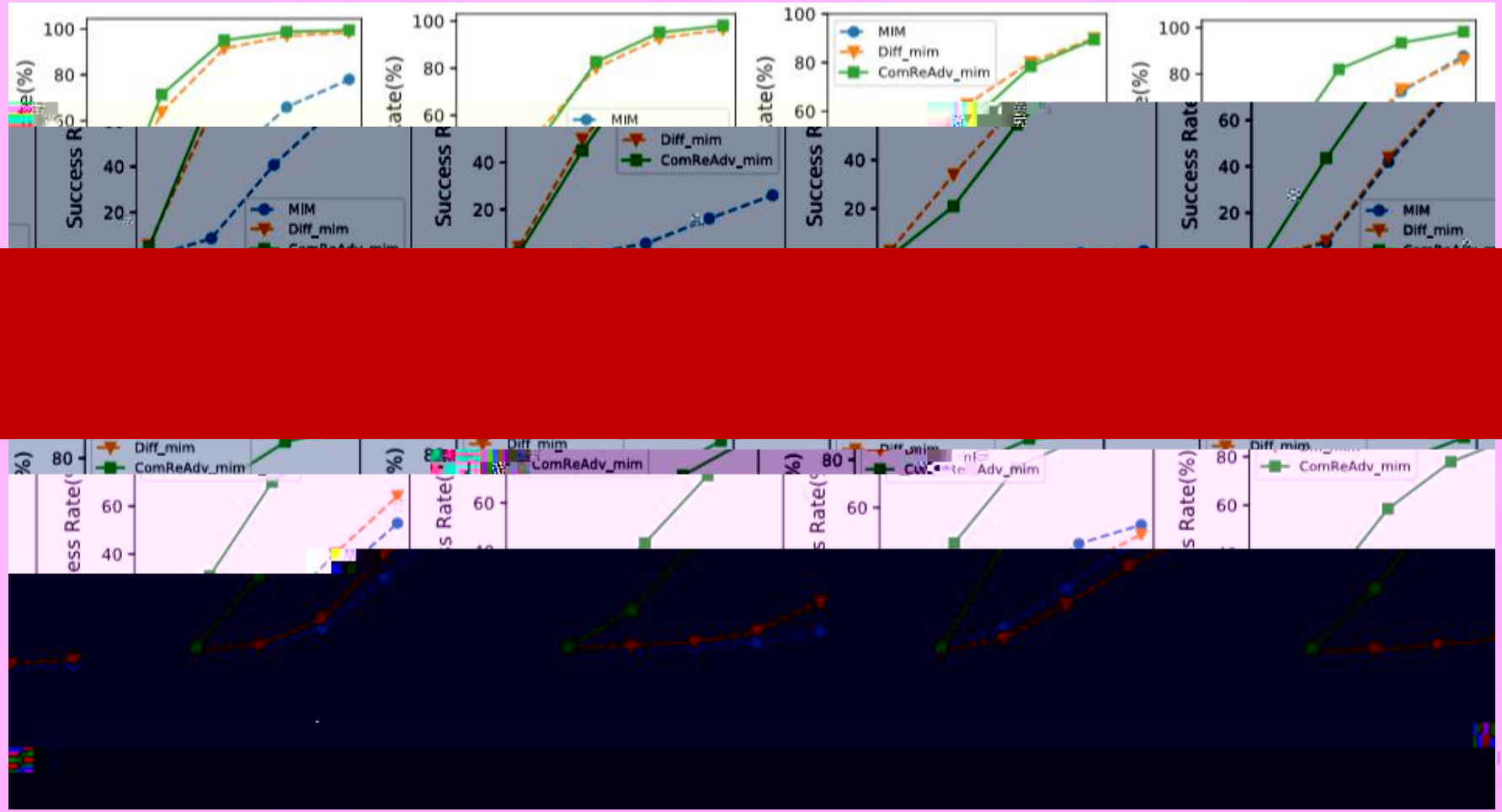
ComModel d

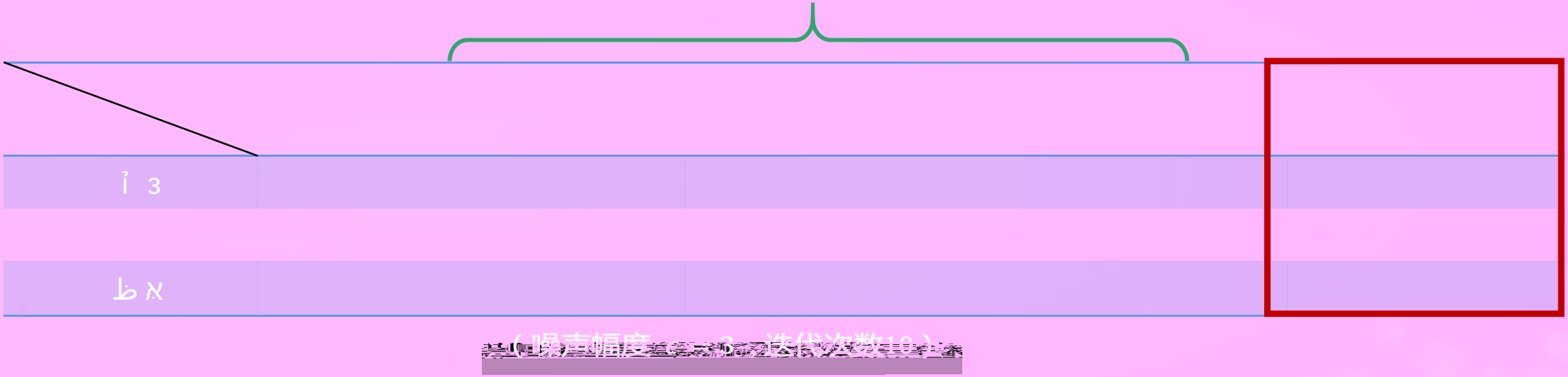


（噪声幅度ϵ =5, 迭代次数10）

ω ¨ Ḅ[OBJ]ώ` ώ '

⊃ Ḋ Ấ¦ ¡ я ⊿ Ấ¦ Ấ¦




ĺ 3
א ظ

2021 WEST LAKE CYBERSECURITY CONFERENCE
西湖论剑·网络安全大会

2021 CYBERSECURITY : THE FOUNDATION OF DIGITAL REFORM

¨Ė ȷ ˜ ^ ḥ▬o ˙ ° g