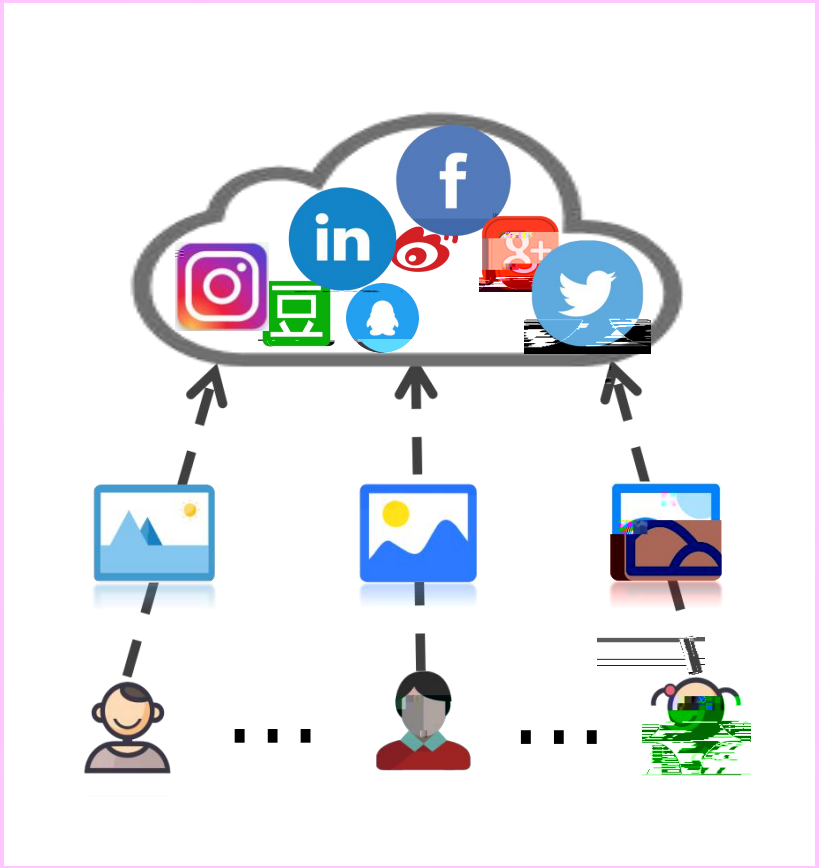
2021 CYBERSECURITY :
THE FOUNDATION OF DIGITAL REFORM

“ ”

ɥ fl Ố ᴸ Ợ ά

ᶻ ẹ̊ ㇷ Ḡ ɯ ᛊ ẹ̊ ᵬ

g, ч‘ Ţ ά ¯p ɻ ˜ ⅄ Λ [OBJ] ╚ Φ ≈ و



Facebook ⅛ ³ ⁼ ɻ ω3 ǎ Ł Ɑ [1]

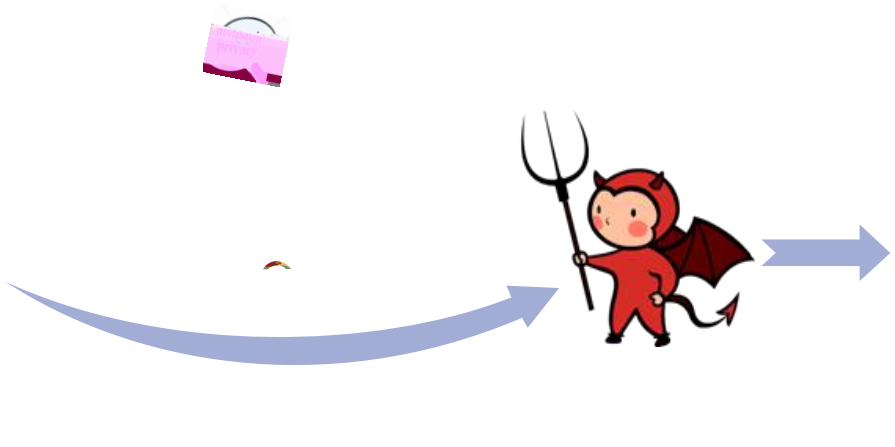
Instagram ⅛ ³ ω ʌ ص9500 ǎ Ł Ɑ

Þ Ţ ⅄ ω ʌ ص400 ǎ Ł Ɑ q‘ [2]

ɣ Ĭ ˜ ⅛ ³ ω32 ǎ g, Ɑ q‘ [2]

g ч ɣ g Ī Ụ ʃ ڭ ۷ ا ڑ ۂ





...

...

Clearview AI ʒ ᴎ ǐ ɹ Facebook YouTube ⊐ Venmo ч ķ п ʌ ص30 ǎ g ᑕ _ á

OBJ _ ሀ ⅋ ۷ ʌ Í ۷ ʌ ƥ = ω ʒ ˇ ` OBJ ừ T ώ ʌ 600 Ķ _ ڤ Φ ŕ

g ■ ỷ ẹ OBJ g, ч Ỿ ˙ Ή ɾ . g, ч ڎ ٧ ∫ ᵢ OBJ l ɒ



g, ч ‘ 1



´ ‰ 5 ⅄



ὄ 5 ⅄ ‘ ‘



g, ч È Ẇ ı ά

Ά ₌ R ㄣ R ¯ OBJ ■ ỷ ¯ ㄥ ㄥ ㄟ ı ƶ ¡ OBJ

g, ч ₅ Ʊ ώ ח ¯ OBJ Ụ

D Ά ₌ ɾ ڎ ٧ ï OBJ ㄥ ₩ ㄣ ∫ ת Ή

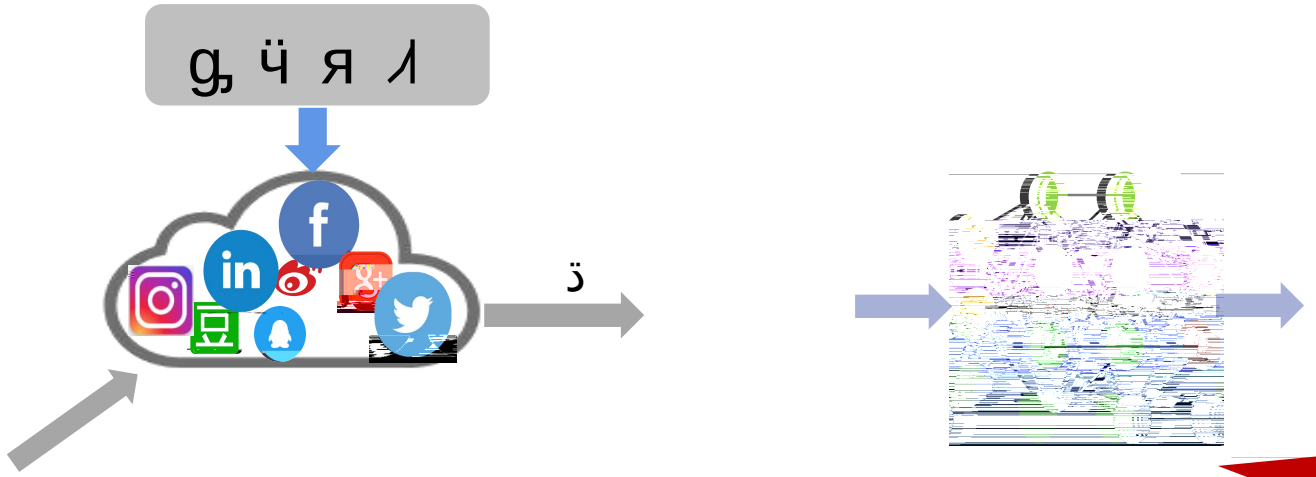
þ ὄ ₩ ㄣ ⊃ ; ˇ ԁ ή | ٬ g DNNs OBJ

g, ч Ỿ ˙ ₩ ʒ

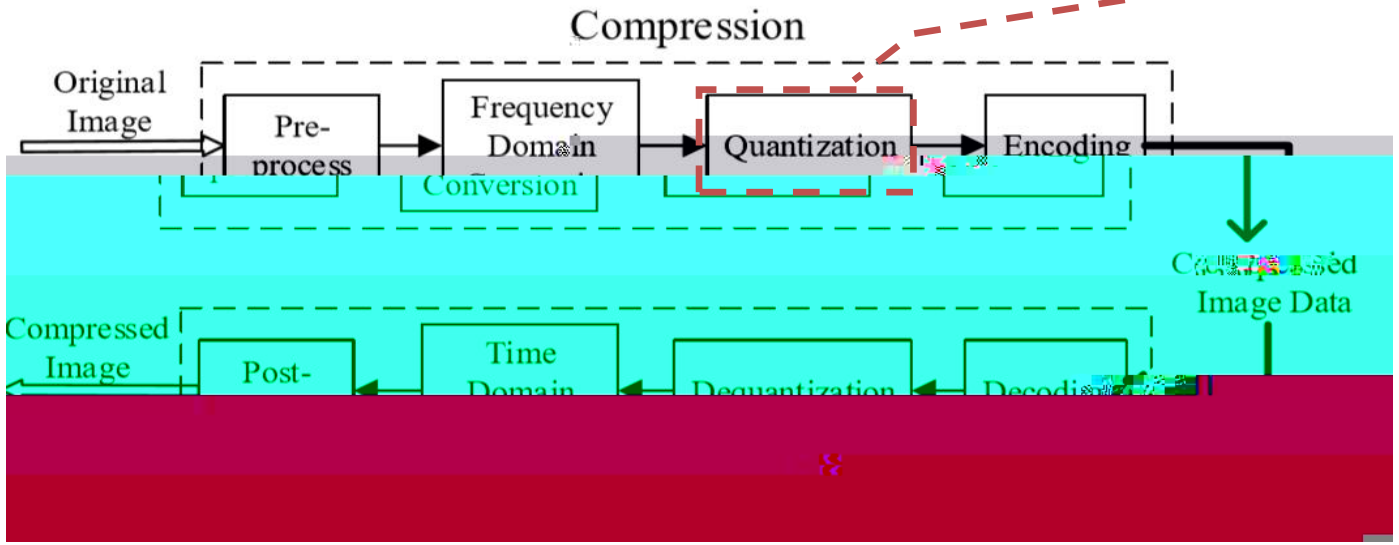


Ḿ ḭ ớ ḡ ч ﻝ ص õ ̈Ω я ﻝ ª ˜ ¸ ⊃Ḿ ḭ ớ

ḡ ч я ﻝ ̓H ẍ ┌ Ẓ ŕ ˜ Ẉ ᴶ ˠ ` ﻝ ڼ ° ◊ ⁼ ώ ڪ ڷ ڈ ۊ ' ᴛ ț́
_ ż OBJ Ḿ ḭ ớ ṋ ᴜ Ṁ₇ Ḿ ḭ ớ ḡ ч ¸ ۊ



g, ч я л \ | [OBJ] ' ỉ ã ` ~ Ṁ7 ǧ ·ı ă ì я л[OBJ]Ḿ ì 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 ì ớ g, ч ·ı ă \ | Л ķ

~ Ẉ J [OBJ]я л Ά Ã ĩ ₅ ḧ [OBJ]ắ

ḥ, Ḿ л[OBJ]| Ḿ ì ʒ ớ

g, ч я л ∖ | [OBJ] ı ĭ ð ˙ ˜ Ṁ₇ ǯ ı ă ĭ я л [OBJ] Ḿ ĭ ớ g, ч

¡ Ḿ g, ч ˋ ı ₩ ȝ [Seong et al. 2017]

¡ Ḿ ´ ‰ ₅ ₩ ȝ [Liu et al. 2017]

¡ Ḿ ŭ ∀ ¸ ₩ ȝ [Shawn et al. 2020]

JPEG [Richard et al. 2017]

پ ¨ ı ĭ [OBJ] JPEG я л ∖ | ₆ ı ĭ ė Ã

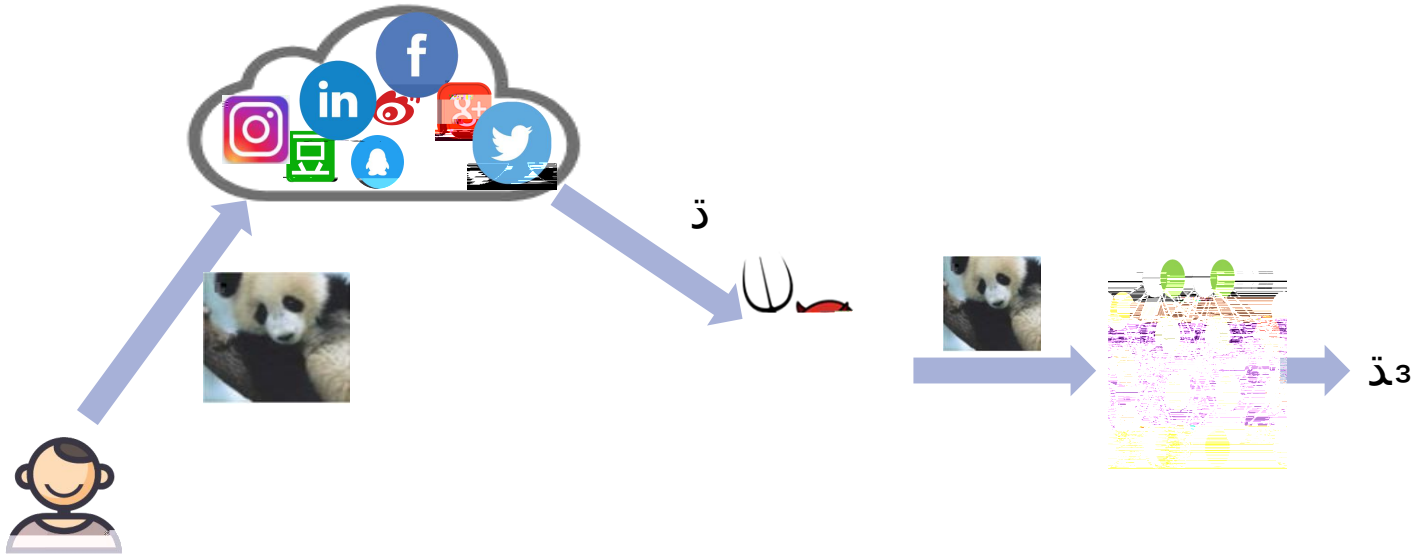
ļ ∂ JPEG я л ∖ | ˀ ʜ v Ѽ ș

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

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 ʹ Y Ъ Ḿ ἰ ό

گ ɾ ª ˜ Ψ J ъ ω̃ ἰ ˈ ˜ я ㄴ ˝ گ Ḿ ἰ ό



ώ¸ Ϟ ỉ я ㄴ[illegible]Ḿ ỉ ό ℊ ч ı ắ Ắ† ḫ ϰ˜ ㄴ ㅅ [illegible]ℊ ч ڈ ϒ ï

~ Ẉ ᴊ [illegible] я ㄴ Ắ Ã ĩ ₅ ḧ [illegible]

ŋ ĩ ‰´ [illegible] я ㄴ ৲ | ҙ Ầ

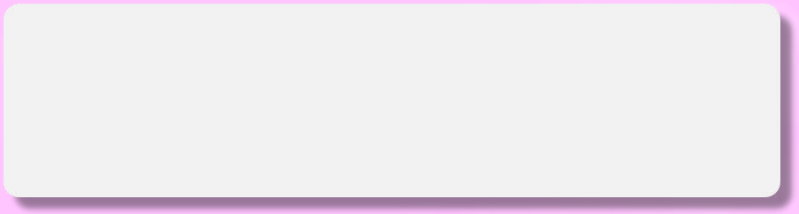
Ḿ ắ ᵽ ب ĩ “ س ¨ ” [illegible]

ı ỉ [illegible] я ㄴ ৲ | ⊐ g ₃ ỷ [illegible] Ḿ ỉ

¯ ı ắ ৲ | Ⅎ ķ







~ Ẉ ᴶ [OBJ]Ꮒ ό و

“ ”

ٹ ‘A Ḿ ~ Ẉ ᴶ پ ٹ [OBJ]я ﻝ Ά Ã ή ‘A~ я ﻝ ١ | ȝ ‘ Ꮒ v ‘Ω

- ‘ ℊ ч ᅵ q* Ẃ ⊧ ɳ

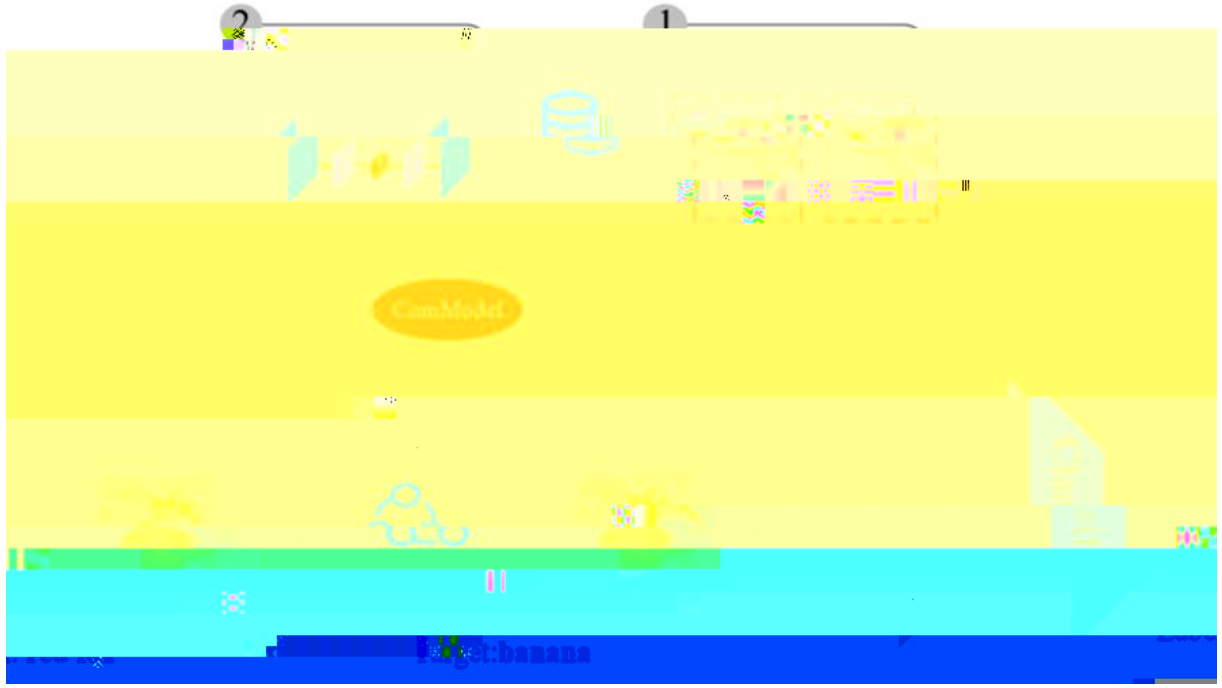
ώ¸ g ⅄ H J H - - H H H H

■ ỷ¨ ﻝ ﻝ ﻥ ᵽ ᵹ ч ³ ښ ﻟ ̰ ﻝ ⊓ ệ ầ[OBJ]ᾧ '

Ф ш ɡ ʌ̣ ⁼ н ȷ. н ОВЈ я л ė ₩ ʒ ˍ ɾ ⊃ Ḋ ɡ ц ч я л ɡ ц ч Ѽ Ѽ

ѣ ѡ л ę я л ∖ | ОВЈ ė ė Ã

ɡ я л ė ₩ ʒ ѽ ф א õ Ḿ ỉ ¯ ı ă ∖ | ı ă ỉ я л Ḿ ỉ ó ɡ ц



ѽ ѕ

ɜ n п ⊃ Ḋ ɡ ц ч ⁼ я л ɡ ц ч ОВЈ Ѽ Ѽ ѣ

ѡ л ф ш ОВЈ

₩ ʒ ę þ ҷ Ѽ ⊃ ɡ ˙ я л ɡ

ѽ ф א õ ∖

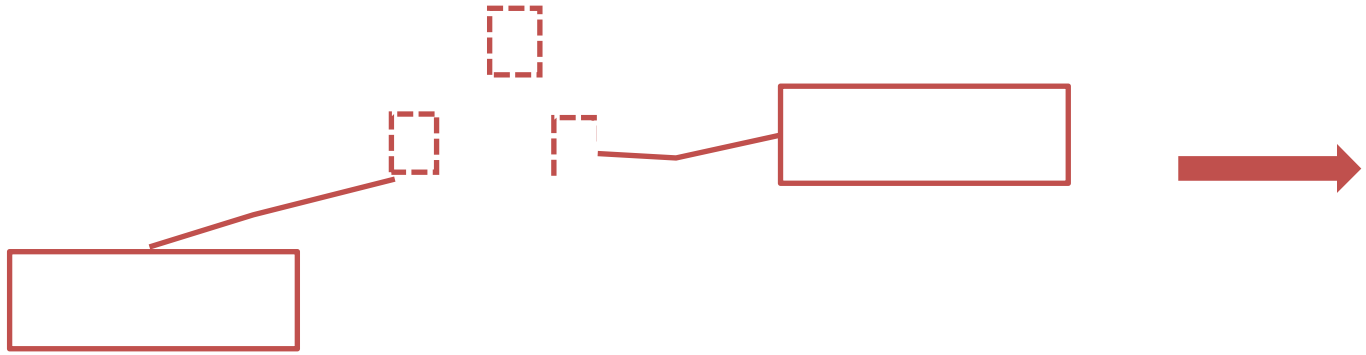
| ı ă ỉ я л ОВЈ Ḿ ỉ ó ɡ ц

2021 WEST

´ ‰ ɯ Ą Ḿ i ¯ OBJ i я ʎ ό

ˬ 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

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

‰

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





ˇ Ω ˜ Ω ˌ ʜ ʊ ǎ g ч ʊ ǎ ɾ ʊ ʌ ǎ ɾ ⫫

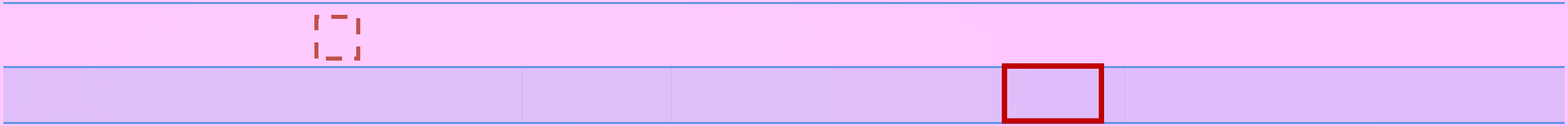
； ǎ ɾ ɔ -

ק ʜ

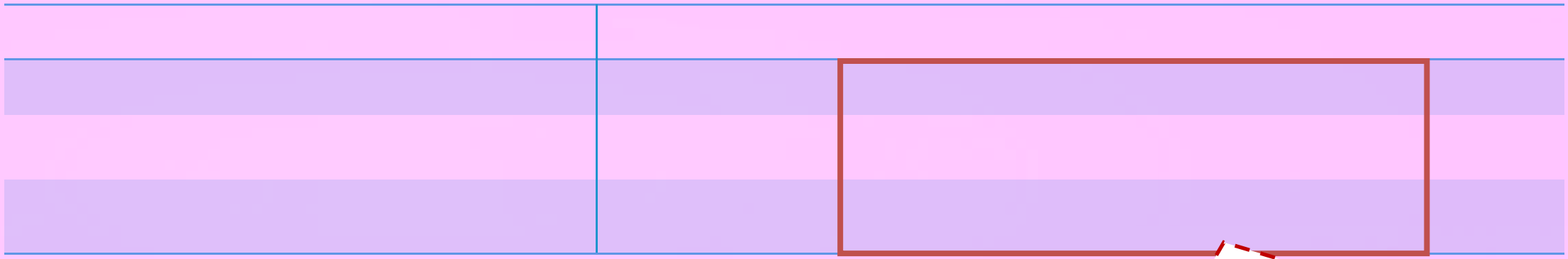
ʊ ɸ ɻ

ʂ ˇ ⫫ ；

ˇ ŋ ˜ Ẉ ɹ ⫫ ； ǐ ɜ ɻ א



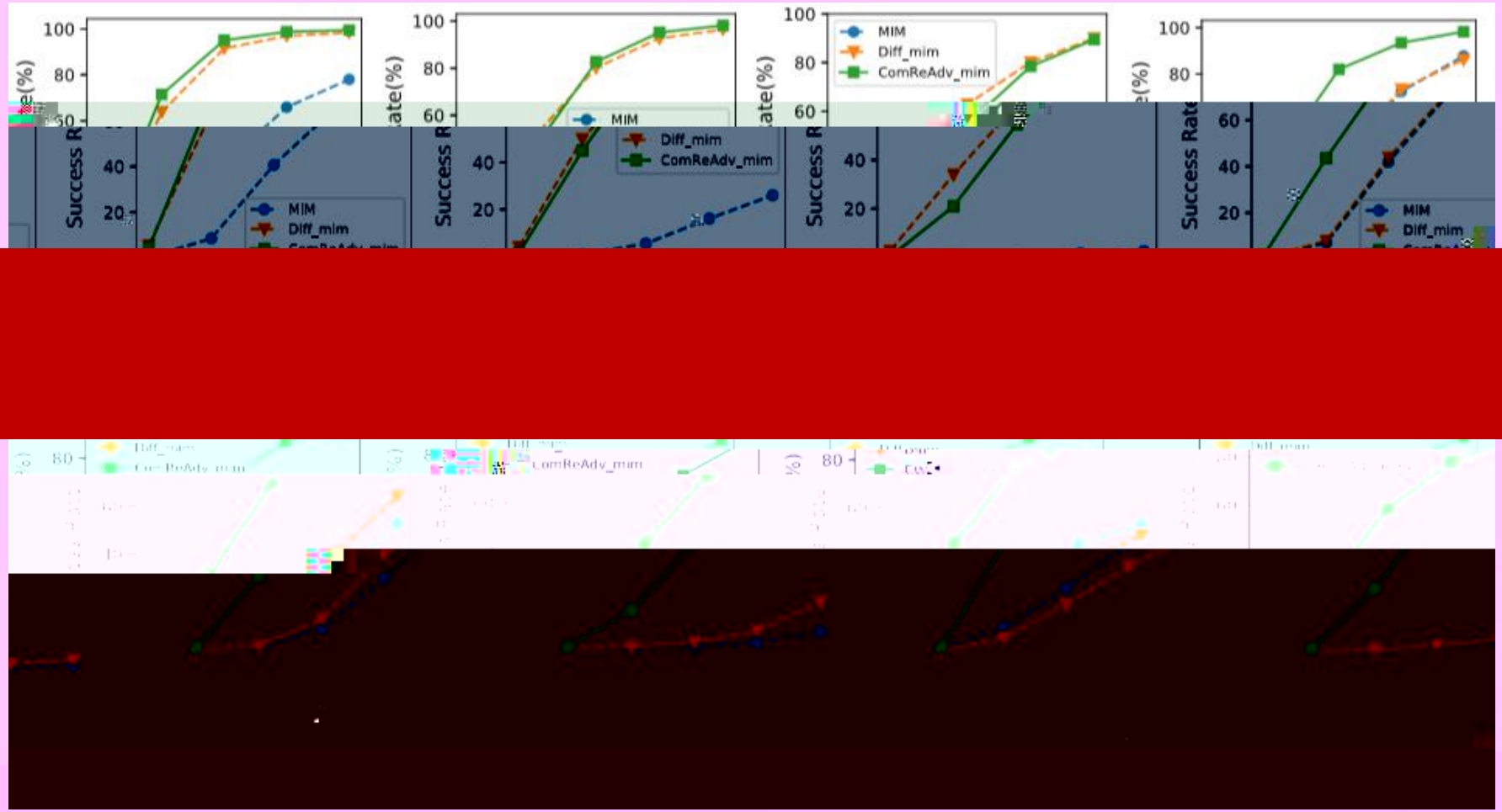
ComModel d

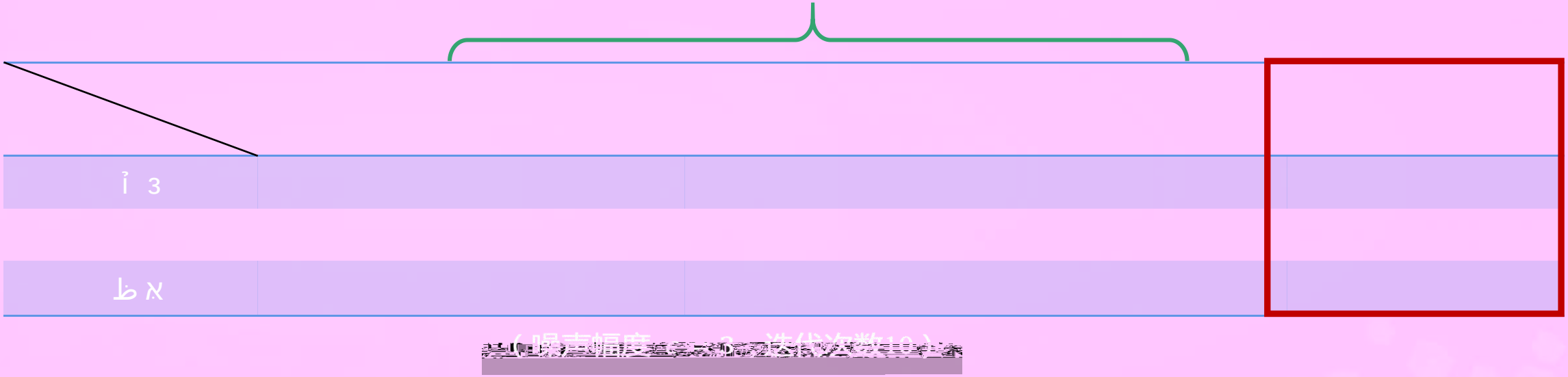


（噪声幅度ϵ =5，迭代次数10）

ω ¨ Ḅ[OBJ]ώ` ώ '

⊃ Ḋ Ấ ỉ я ㅅ 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



″Ę J ˜ ^ ḥ▬o ˙ ° g