1. ..... 1
2. Ð ..... 1
3. ..... 1
4. ..... 1
5. ..... 2
6. ..... 3

Ð ɯ GB/T 39786-2021 ê Ḥ ŋ Ḥ Ì ɛ̀ GM/T 0115-2021 ê Ḥ Ì Ḥ ’ ₮ ᵀ Â

Ð ɢ ȁ Ḥ ⅞ ȁ ȁ ǐ Â

1) GB/T 39786-2021 ê Ḥ ŋ Ḥ Ì

2) GM/T 0115-2021 ê Ḥ Ì

Ð Ǐ ʎ ↕ . ᵀ ↕ ‘

1) ɛ̀ ˜ Ð ʳ ’

2) GB/T 39786-2021 ɛ̀ GM/T 0115-2021’

3) : ą ’ ≢ : ą ˛ / ˚ ج / Ⱶ’

4) п ᾠ ضي ɛ̀ Ḥ ŋ ȁ ɛ̀ ŋ Â

ǟ GM/T 0115-2021˘ ↕ ɛ̂ ˆ ˆ ɑ . ᵀ ‘

ą ˆ *Cryptography **D**eployment effectiveness*˜ ˘ ʅ ȁ

ą ˘ ʏ Ḥ ŋ ˘ ʟ ȁ ȁ ɛ̀ ƀ ˜ ʅ

Ḡ ’

/ ˛ ˆ *Cryptography **A**lgorithm/Technique compliance*˜ ˘ Ḥ

Ţ ą ʅ ˛ ȁ ɛ̀ ˜ ɯ ‰ ȁ ʒ ‰ ˜

˘ Ḥ Ţ ą ʅ ˜ ɯ ‰ ɛ̀ ʒ ‰ ɯ

‰ Â

ŋˆ ***K**ey management security*˜ ˘ ŋ ث ʟ ʅ ŋ˘

G ᵒᵒ ج/ ⊢ ʅ ŋ Â

ˆ 1˜ ᴵ̥ . ᵀ ↕

Ţ˘ *i* ɑ ŋ *j* ᴵ˝Ḥ *k* $T_{i,j,k}$˘ ỉ .

ᵀ $S_{i,j,k}$ ŗ {0, 0.25, 0.5,1}˘ ỉ Ţ 0 ƀ ˛ ˘ 1 ˛ ˘ ỉ № ˛ Â $S_{i,j,k}$

ŭ ṿ №≢ 1 Â غ ᴵ̥ ŋ ᴵ ⊢ ⊥ غ ᴵ ᵒᵒ ج ⊥

ƀ ᴵ E Â

ƀ ᴵ̥ ɑ . ᵀ Â

ˆ 2˜ ᴵ˝Ḥ . ᵀ ↕

Ţ˘ *i* ɑ ŋ . ŭ

˘ Ӈ 2 ʟ ŋ ˘ ⁘ № ṿ `E ΐ ʳ ɥ ʽ

r . ᵀ S ɥ 100 №˘ ↕ ∞ Ḥ ᵛᵘ GB/T 39786-2021

’ *S* ʏ ɢ 100 № ȁ Ъ ʏ ɢ ṿ˘ ғ ᵀ ǖ ˘ ↕ ∞ Ḥ

ᵛᵘ GB/T 39786-2021 ’ Ɂ ↕˘ ∞ Ḥ Ъ ᵛᵘ GB/T 39786-2021

Â

1 .

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | *D* | *A* | *K* | | $S_{i,j,k}$ |
| | | | | | |

**2**

| | ŋ̊ *i* | ŋ | ɬ ʷḤ ʷ *j* | ɬ ʷḤ | ŋ ˆ $w_i$ ˜ | $w_{i,j}$ | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | W̄ | Ʉ | [illegible] | ضم |
| | 1 | غ ŋ | ˆ 1˜ | M ≢ | 10 | 0.4 | 0.7 | 1 | 1 |
| | | | ˆ 2˜ | Ʊ̃ | | 0.4 | 0.4 | 0.7 | 0.7 |
| | | | ˆ 3˜ | Ʊ̃ | | / | / | 0.7 | 0.7 |
| | | | ˆ 1˜ | M ≢ | | 0.4 | 0.7 | 1 | 1 |
| | 2 | غ ŋ Ḥ | | | 20 | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | ˆ 1˜ | | м ≠ | | 0.4 | 0.7 | 1 | 1 |

4 ġ ŋ 30

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | ŋ β ¬ 2 | | | | | |
| | | | | ˜ | | | | | |
| | | | ˆ 5˜ | β ¬ 2 Ḡ<br>L غ<br>L | | 0.7 | | | |