Metaphor as Semantic Encryption:
Zero Knowledge Proof Using *Dream of the Red Chamber* as an Example

Lian, Zihe Zhao, Ayizuorehe
AI Thrust, Info Hub, HKUST(GZ)
xlian289@connect.hkust-gz.edu.cn

Agenda

Motivation
- Crisis in digital creativity

Methodology
- Similarity between metaphor and ciphertext
- Combine Zero-knowledge proofs (ZKP) with system

Implementation
- An example of *Dream of the Red Chamber*
- Encryption and decryption of prophecies
- Constraint system generation

Results
- Zero knowledge proof process
- Circuit performance

Applications

Unlocking creation

Dual Crisis in Digital Creativity

- Encryption: Traditional methods secure content, but not creative value - texts “naked” during evaluation
- Validation: Subjective judgments; no way to prove value without revealing content

Copyright & Research

- Piracy Risk: Share drafts → stolen
- Exclusion: Non - experts can't verify credibility

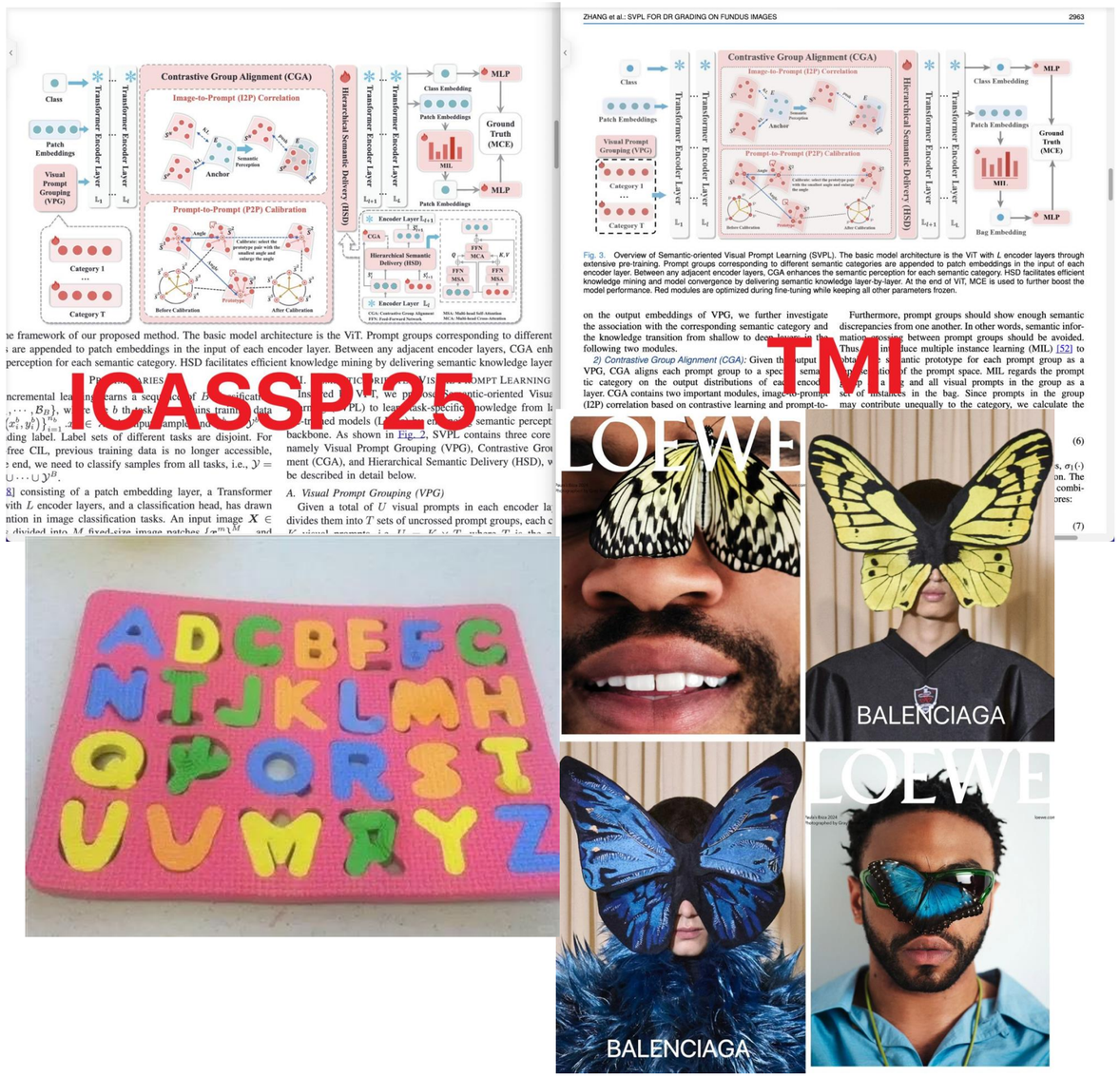
Eg.

Subjective Dream of the Red Chamber version checks

- Secure IP
- Quantify creativity
- Build trust across domains

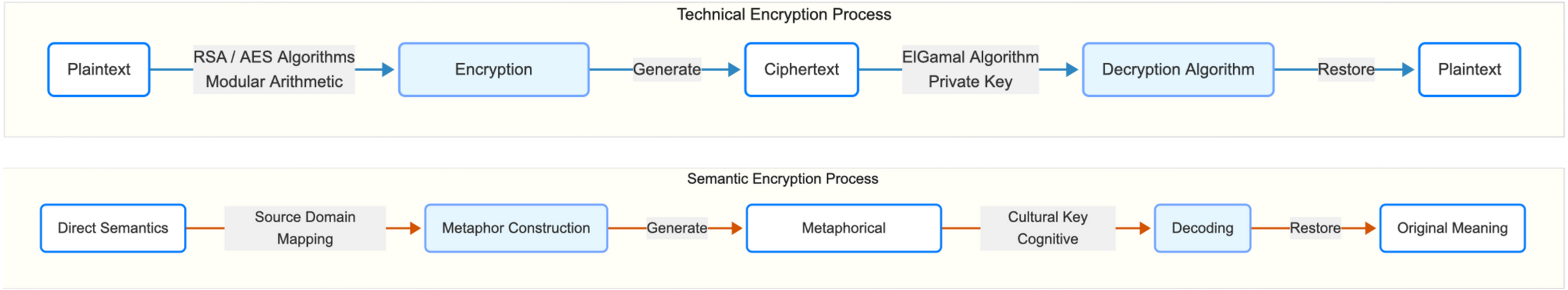
The Game - Changing Solution

- Metaphor - ZKP Integration



Similarity between metaphor and ciphertext

Cryptography and metaphor share a three-stage information transformation structure of **"plaintext - ciphertext - decryption":**



- Origin：Homesickness
- Encode：Via imagery/metaphor
- Metaphor：Moon & Longing
- Decode：With context & culture
- Restore：Back to homesickness

- Info Conversion：
  - Plaintext - Metaphor Orig Semantics;
  - Encrypt - Semantic Encode;
  - Ciphertext - Metaphor Text;
  - Decrypt - Semantic Decode
- Uncertainty：Key Space Variability vs. Interpretive Ambiguity
- Domain Diff：Mathematical Operations vs. Cognitive - Linguistic Processes

Zero-knowledge proofs (ZKP) & metaphor

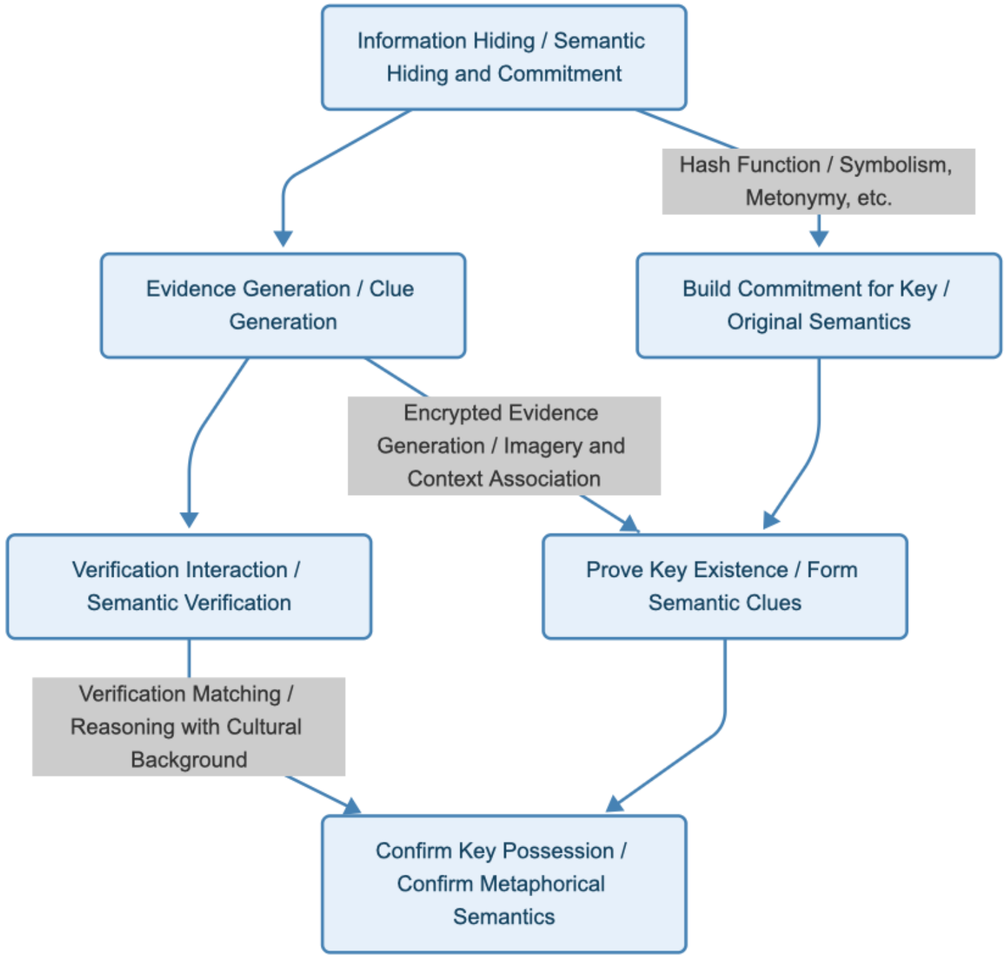
Zero - Knowledge Proofs (ZKP) Basics

- Definition: Do not disclose plaintext, only prove that 'I know' certain information.

- Key Elements:
  - Prover generates proof(zk-SNARKs/R1CS circuits and polynomial commitments)
  - The verifier checks whether the proof is valid(elliptic curve pairings and hash-based challenges)
  - The information itself is not exposed(cryptographic commitments)

ZKP in Metaphor:

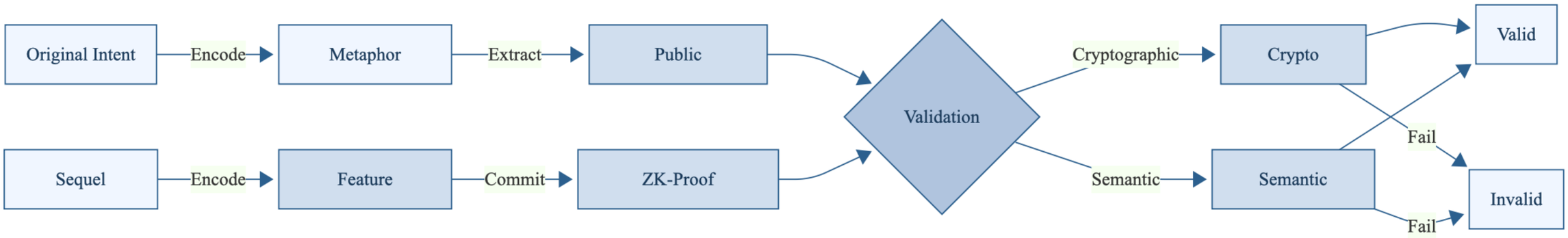
- Just as ZKP protects digital secrets, metaphors protect the original semantic meaning of a message.



An example of *Dream of the Red Chamber*

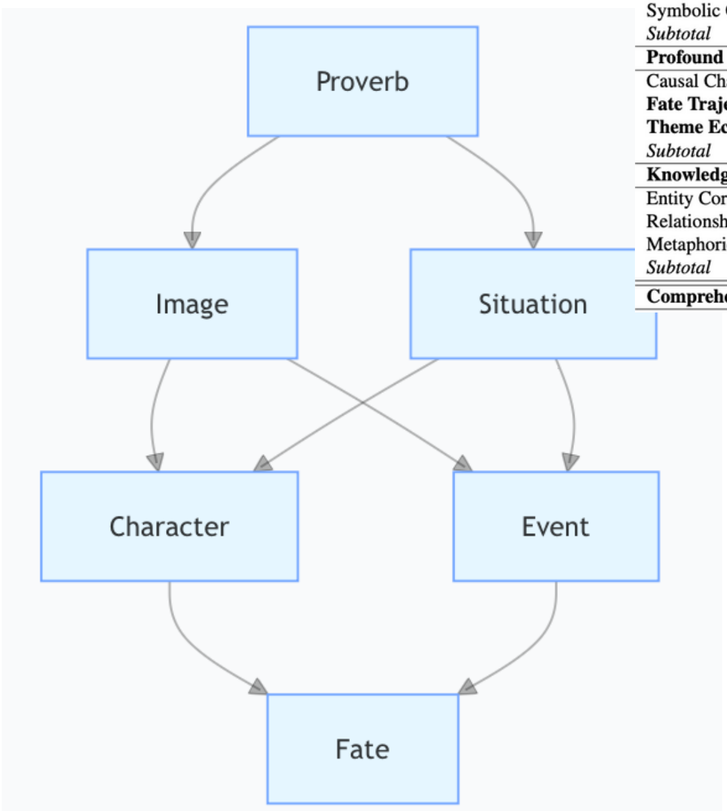
- The authorship of the last 40 chapters has been debated for centuries(Chenggao version VS Guiyou version).
- We hope to design a system that can **both protect text privacy and verify logical authentication.**
- Use NLP to extract text features and analyze the semantic consistency.
- Use ZKP to implement privacy protection verification.

ZKP Concept	*Dream of the Red Chamber* Scenario Correspondence
Plaintext	True Ending Ideas of Latter 40 Chapters, the fate of the main characters
Ciphertext	Prophecies (Portraits, Poems, Foreshadowing) in First 80 Chapters
Prover	Creator/Holder of Latter 40 Chapters' Version
Verifier	Redology Researchers, Readers, Automated Verification System
Commitment	Logical Mapping Declaration of Latter 40 Chapters' Version to Prophecies
Proof	Corresponding Plot Segments in the Version and Their Analysis

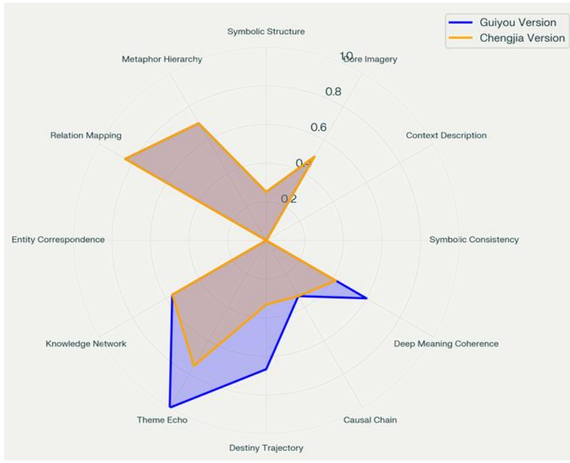


Encryption of prophecies

e.g. The class metaphor/prophecy in "金簪雪里埋" - "gold hairpin buried in snow"



Analysis Dimension	Guixiu Version	Chengjia Version	Difference
Symbolic Structure Matching Degree			
Core Image Correspondence	0.500	0.500	0.000
Situation Description Matching	0.002	0.002	0.000
Symbolic Connotation Consistency	0.000	0.000	0.000
Subtotal	*0.251*	*0.251*	*0.000*
Profound Meaning Coherence			
Causal Chain Completeness	0.333	0.333	0.000
Fate Trajectory Consistency	**0.667**	**0.333**	**0.334**
Theme Echo Degree	**1.000**	**0.750**	**0.250**
Subtotal	*0.600*	*0.417*	*0.183*
Knowledge Network Mapping Degree			
Entity Correspondence Degree	0.000	0.000	0.000
Relationship Mapping Degree	0.844	0.844	0.000
Metaphorical Hierarchy Degree	0.700	0.700	0.000
Subtotal	*0.562*	*0.562*	*0.000*
Comprehensive Score	**0.453**	**0.379**	**0.073**



Decryption of prophecies

Expand the dataset to include all core prophecies

人物	谶语原文	谶语类型	程高本实现	癸酉本实现	情感匹配度(程)	情感匹配度(癸)	情节复杂度(程)	情节复杂度(癸)	主题深度(程)	主题深度(癸)
林黛玉	两株枯木，木上悬着一围玉带	诗谶	焚诗稿泪尽病逝	误杀小红后自缢	0.85	0.92	0.8	0.9	0.82	0.88
薛宝钗	一堆雪，雪下一股金簪	物象谶	独守空闺	贪污被发配	0.82	0.89	0.75	0.85	0.78	0.85
贾元春	虎兕相逢大梦归	政治谶	疯症病逝	被乱刀砍死	0.8	0.95	0.7	0.92	0.75	0.9
史湘云	湘江水逝楚云飞	命运谶	守寡终老	沦为乞丐重逢宝玉	0.78	0.88	0.72	0.88	0.8	0.86
贾宝玉	出家为僧	行为谶	出家为僧	跳海自尽被救	0.85	0.9	0.78	0.85	0.82	0.88
李纨	桃李春风结子完	命运谶	教子成才	封官后病逝	0.75	0.82	0.7	0.8	0.75	0.82
王熙凤	机关算尽太聪明	性格谶	积劳成疾	狱中自缢	0.88	0.92	0.85	0.9	0.82	0.88
妙玉	欲洁何曾洁	讽刺谶	被掳下落不明	沦为妓女	0.82	0.9	0.75	0.85	0.8	0.88
贾探春	千里东风一梦遥	政治谶	远嫁他乡	和亲岛国	0.78	0.85	0.72	0.82	0.75	0.85
贾惜春	独卧青灯古佛旁	宗教谶	出家修行	拒认刘姥姥	0.8	0.85	0.75	0.8	0.78	0.82
贾迎春	一载赴黄粱	婚姻谶	忧郁而死	被毒打致死	0.75	0.88	0.7	0.85	0.72	0.82
巧姐	巧得遇恩人	救赎谶	嫁农家	被卖青楼后获救	0.82	0.9	0.78	0.88	0.8	0.85

谶语id		情节上下文	情节摘要	关键词	人物关联	情感倾向	类型
玉带林中挂	谶语原文	林黛玉判词配画"两株枯木，木上悬着一围玉带"（第五回）					诗谶
	程高本续	黛玉因宝玉成婚消息悲痛过度，焚诗稿后泪尽病逝（第97回）	临终前焚毁诗稿，紫鹃守候，宝玉未能见最后一面	焚稿、泪尽、病榻	紫鹃（贴身侍女）、贾母（默许婚事）、王熙凤（调包计策划）	凄美哀婉	诗谶+行为谶
	癸酉本续	贾府遭强盗入侵后，林黛玉承担起管理园中剩余人员的重任。鸳鸯向林黛玉献上贾蓉令牌，诬陷小红与贼寇勾结。黛玉误信谗言，命人将小红打死。事后知被骗，悔恨难当。（第97回）	黛玉悔恨交加，加之被贾蔷贾菱下药，携绳来到柳叶渚，将宝玉所赠旧帕藏入柳树洞。在槐树下自缢而亡。死前得知自己是绛珠仙草转世，一生泪已还尽。后被安排掌管朝暗司等职。	自缢、误杀、泪尽、绛珠草、柳叶渚	宝玉(痴情恋人)、鸳鸯(谮言者)、小红(冤死者)、紫鹃(忠仆)	悲剧性，误解导致自责，泪尽而终	图谶+政治谶
金簪雪里埋	谶语原文	薛宝钗判词配画"一堆雪，雪下一股金簪"（第五回）					诗谶
	程高本续	宝钗与宝玉成婚后，宝玉出家，宝钗独守空闺（第120回）	宝钗独守蘅芜苑，屋内陈设如雪洞，守寡至终老。虽有荣华富贵，却终是孤独凄凉，形同守活寡	元春选入宫中后身居高位，后因疯症病逝（第95回）	薛姨妈（病逝前托孤）、莺儿（贴身丫鬟）、贾兰（科举中举后探望）	隐忍的悲凉	物象谶
	癸酉本续	宝玉离家后,薛宝钗嫁给贾雨村。雨村官场腐败,夫妻二人因贪污被查,最终被发配到东北边疆充军行役。	在风雪窗荒之地,宝钗一病不起,临终埋怨雨村,感叹自己命运多舛,因无冷香丸调治,不久死去,葬在雪地中。"真是人生难料,世事无常。"	雨村之妻、充军东北、雪中埋骨、冷香丸、命舛	贾雨村、莺儿	功利主义反噬，怨恨、悔恨、无奈	政治谶+物象谶

Table 1: Overall Version Comparison Analysis

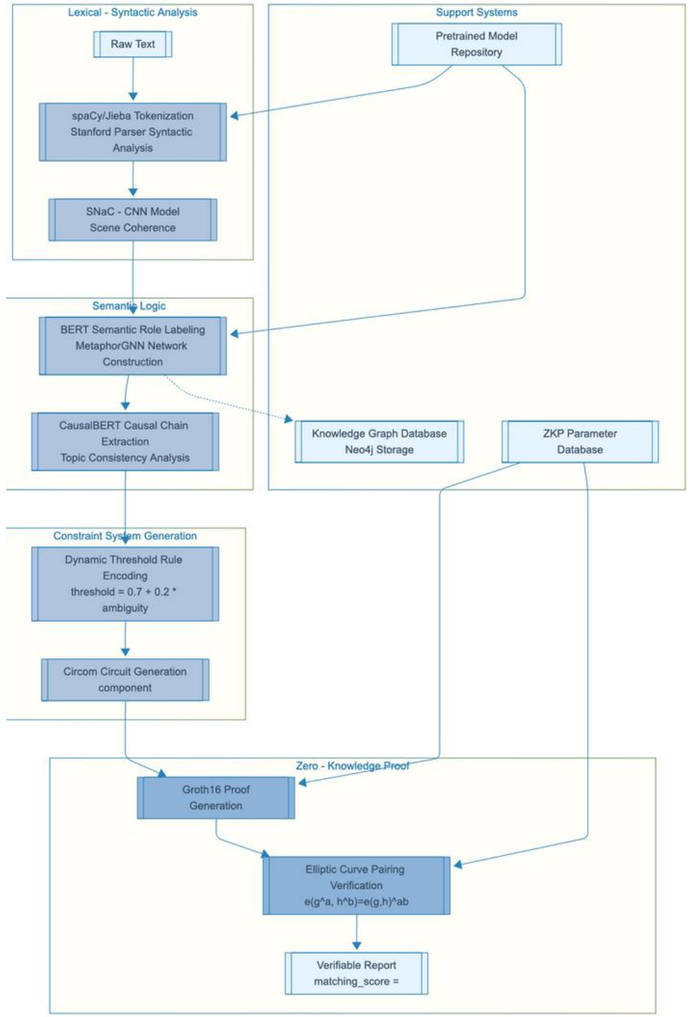
Dimension	Weight	Geng Cheng	Gui You	Difference
Symbolic Structure	0.4	0.61 (±0.20)	0.69 (±0.09)	+0.08
Semantic Coherence	0.4	0.66 (±0.21)	0.73 (±0.05)	+0.07
Knowledge Network	0.2	0.67 (±0.22)	0.73 (±0.07)	+0.07
Weighted Average	1.0	0.65 (±0.21)	0.72 (±0.07)	+0.07

Table 2: Detailed Dimension Analysis

Sub-dimension	Weight	Geng Cheng	Gui You	Difference
Symbolic Structure (0.4)				
Core Imagery	0.16	0.65 (±0.18)	0.72 (±0.08)	+0.07
Visual Alignment	0.12	0.60 (±0.22)	0.68 (±0.10)	+0.08
Text Interpretation	0.12	0.58 (±0.20)	0.67 (±0.09)	+0.09
Semantic Coherence (0.4)				
Causal Chain	0.16	0.68 (±0.19)	0.74 (±0.06)	+0.06
Fate Trajectory	0.12	0.65 (±0.22)	0.72 (±0.05)	+0.07
Theme Resonance	0.12	0.65 (±0.22)	0.73 (±0.04)	+0.08
Knowledge Network (0.2)				
Entity Mapping	0.08	0.68 (±0.21)	0.74 (±0.07)	+0.06
Relation Mapping	0.08	0.66 (±0.23)	0.72 (±0.07)	+0.06
Metaphor Analysis	0.04	0.67 (±0.22)	0.73 (±0.07)	+0.06

Table 3: Statistical Analysis of Version Performance

Statistical Measure	Symbolic	Semantic	Knowledge	Overall
Mean Score	0.65	0.70	0.70	0.68
Standard Deviation	±0.15	±0.13	±0.15	±0.14
Maximum Score	0.73	0.77	0.77	0.76
Minimum Score	0.00	0.00	0.00	0.00
Score Range	0.73	0.77	0.77	0.76



Constraint system generation

Prophecy Ambiguity and Threshold Calculation

$$\text{Ambiguity}(p) = \text{Base} + \text{Length Factor} + \text{Imagery Factor} + \text{Abstraction Factor} + \text{Contrast Factor}$$
$$\text{Adjusted Threshold}(p) = \max(0.3, \text{Base Threshold} - \text{Ambiguity}(p))$$

Based on each prophecy

- dynamically generate its ambiguity data to determine the threshold
- threshold = 0.7 + 0.2 * ambiguity

Ambiguity Calculation Example: "Yu Dai Lin Zhong (

Factor	**Value**
Base ambiguity	0.20
Short text (3 characters)	+0.15
Rich imagery (jade belt, forest)	+0.16
High abstraction	+0.15
Contrasting image description	+0.24
High ambiguity prophecy trait	+0.10
Total Ambiguity	**0.80**
Base threshold	0.70
Adjusted threshold (0.70 - 0.80)	-0.10
Final threshold (minimum bound)	**0.30**

Variable	Description	Value
w_1	Constant	1
w_2	Base Ambiguity	0.20
w_3	Short Text Bonus	0.15
w_4	Rich Imagery Bonus	0.16
w_5	Abstract Bonus	0.15
w_6	Contrasting Image Bonus	0.24
w_7	High Ambiguity Bonus	0.10
w_8	Total Ambiguity	0.80
w_9	Base Threshold	0.70
w_{10}	Adjusted Threshold	-0.10
w_{11}	Final Threshold	0.30

Formulating R1CS Constraints

For each constraint: $(\mathbf{A} \cdot \mathbf{w}) \times (\mathbf{B} \cdot \mathbf{w}) = \mathbf{C} \cdot \mathbf{w}$

Constraint 1: Total Ambiguity

Vector	Variable Coefficients										
	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}	w_{11}
A	1	0	0	0	0	0	0	0	0	0	0
B	0	1	1	1	1	1	1	0	0	0	0
C	0	0	0	0	0	0	0	1	0	0	0

Table 2: Total Ambiguity Constraint Matrix

Constraint 2: Threshold Adjustment

Vector	Variable Coefficients										
	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}	w_{11}
A	1	0	0	0	0	0	0	0	0	0	0
B	0	0	0	0	0	0	0	-1	1	0	0
C	0	0	0	0	0	0	0	0	0	1	0

Table 3: Threshold Adjustment Constraint Matrix

Verification Results

ID	Ambiguity	Threshold	CG	GY	Better
P1	0.80	0.30	0.71	0.74	GY
P2	0.80	0.30	0.71	0.73	GY
P3	0.80	0.30	0.71	0.74	GY

Table 4: Verification Results Summary

Zero knowledge proof process

R1CS to QAP Transformation

$$Z_i(x) = \prod_{j=1, j\neq i}^{m} \frac{x - r_j}{r_i - r_j}$$

$$A_i(x) = \sum_{j=1}^{m} a_{j,i} \cdot Z_j(x)$$

$$B_i(x) = \sum_{j=1}^{m} b_{j,i} \cdot Z_j(x)$$

$$C_i(x) = \sum_{j=1}^{m} c_{j,i} \cdot Z_j(x)$$

- Z_i (x) is a Lagrange basic polynomial, which is equal to 1 at a specific point and 0 at other points
- A_i (x), B_i (x), and C_i (x) are polynomials obtained through matrix transformation

Table 4: Verification Results for All Prophecies

Prophecy No.	Ambiguity	Threshold	Chenggao Score	Guiyou Score	Chenggao Pass	Guiyou Pass	Better Version
1	0.80	0.30	0.71	0.74	Yes	Yes	Guiyou
2	0.80	0.30	0.71	0.73	Yes	Yes	Guiyou
3	0.80	0.30	0.71	0.74	Yes	Yes	Guiyou
4	0.75	0.30	0.71	0.70	Yes	Yes	Chenggao
5	0.70	0.30	0.71	0.72	Yes	Yes	Guiyou
6	0.65	0.30	0.72	0.70	Yes	Yes	Chenggao
7	0.80	0.30	0.71	0.71	Yes	Yes	Equal
8	0.55	0.30	0.72	0.73	Yes	Yes	Guiyou
9	0.80	0.30	0.67	0.72	Yes	Yes	Guiyou
10	0.61	0.30	0.00	0.71	No	Yes	Guiyou
11	0.71	0.30	0.71	0.71	Yes	Yes	Equal

QAP Polynomial System

$$P(x) = \left(\sum_{i=0}^{n} w_i \cdot A_i(x)\right) \cdot \left(\sum_{i=0}^{n} w_i \cdot B_i(x)\right) - \left(\sum_{i=0}^{n} w_i \cdot C_i(x)\right)$$

$$Z(x) = \prod_{i=1}^{m} (x - r_i)$$

$$H(x) = \frac{P(x)}{Z(x)}$$

- P (x) represents the validation polynomial, which checks whether the R1CS constraint is satisfied
- Z (x) is a vanishing polynomial, equal to 0 at all constraint points
- H (x) is a quotient polynomial, and the constraint is only satisfied when P (x) can be divided by Z (x)

Trusted Setup and Key Generation

$$\tau \leftarrow \mathbb{F}_p$$

$$\{\tau^i\}_{i\in[d]} \leftarrow \{\tau, \tau^2, \tau^3, \ldots, \tau^d\}$$

$$\text{pk} = \{g^{\tau^k}, \{g^{A_i(\tau)\cdot\tau^k}, g^{B_i(\tau)\cdot\tau^k}, g^{C_i(\tau)\cdot\tau^k}\}_{i\in[n]}\}_{k\in[d-1]}$$

$$\text{vk} = \{g^{\tau^k}\}_{k\in\{0,d\}}, \{g^{A_i(\tau)}, g^{B_i(\tau)}, g^{C_i(\tau)}\}_{i\in I_p}$$

Proof Generation Process

Zero-Knowledge Proof Generation and Verification

Prover	Verifier
Public Inputs: prophecyId, ambiguity, threshold	
1. Calculate witness values • Compute all ambiguity factors • Determine intermediate results 2. Compute polynomials • Transform constraints to polynomials • Evaluate at secret point τ 3. Hide values using secret • Apply elliptic curve operations • Create the four proof elements	1. Receive the proof • Obtain the four elliptic curve points • Extract public outputs 2. Verify using pairing • Apply bilinear pairing operation • Check if equation holds 3. Accept or reject • If pairing check passes: Accept • Otherwise: Reject
Proof: $\pi = (g^{A(\tau)}, g^{B(\tau)}, g^{C(\tau)}, g^{H(\tau)})$	

Circuit performance and results

Performance data of the system processing prophecies

- Generate once, verify multiple times

Table 3: ZKP Performance Metrics for All Prophecies

Prophecy	Proof Size	Proving Time	Verification Time	Memory Usage	R1CS Size
1	1.1 KB	2.3s	0.05s	76 MB	8
2	1.1 KB	2.2s	0.05s	76 MB	8
3	1.1 KB	2.3s	0.05s	76 MB	8
4	1.1 KB	2.3s	0.05s	76 MB	8
5	1.1 KB	2.2s	0.05s	76 MB	8
6	1.1 KB	2.3s	0.05s	76 MB	8
7	1.1 KB	2.3s	0.05s	76 MB	8
8	1.1 KB	2.2s	0.05s	76 MB	8
9	1.1 KB	2.3s	0.05s	76 MB	8
10	1.1 KB	2.3s	0.05s	76 MB	8
11	1.1 KB	2.2s	0.05s	76 MB	8

Verification Equation

$$e(g^{A(\tau)}, g^{B(\tau)}) = e(g, g^{C(\tau)}) \cdot e(g^{H(\tau)}, g^{Z(\tau)})$$

Verification job:

- Just calculate whether this equation holds or not

No need for raw data:

- validators do not need to know any private computing details

Prophecy ID	Ambiguity (Public)	Threshold (Public)	Version Comparison CG vs GY	Result
P1	0.80	0.30	0.71 vs 0.74	Guiyou Better
P2	0.80	0.30	0.71 vs 0.73	Guiyou Better
P3	0.80	0.30	0.71 vs 0.74	Guiyou Better
P4	0.75	0.30	0.71 vs 0.70	Chenggao Better
P5	0.70	0.30	0.71 vs 0.72	Guiyou Better
P6	0.65	0.30	0.72 vs 0.70	Chenggao Better
P7	0.80	0.30	0.71 vs 0.71	Equal
P8	0.55	0.30	0.72 vs 0.73	Guiyou Better
P9	0.80	0.30	0.67 vs 0.72	Guiyou Better
P10	0.61	0.30	0.00 vs 0.71	Guiyou Better
P11	0.71	0.30	0.71 vs 0.71	Equal

Table 1: Prophecy Comparison Results (Cryptographically Verified via ZKP)

Prophecy	Proof Status	Proof Hash (Truncated)	Constraints
P1	✓ VALID	0x7a2b...e91c	Satisfied
P2	✓ VALID	0x6c3f...512d	Satisfied
P3	✓ VALID	0x9e7d...f38a	Satisfied
P4	✓ VALID	0x5d1e...c47b	Satisfied
P5	✓ VALID	0x4a8c...d23f	Satisfied
P6	✓ VALID	0x3b2a...918e	Satisfied
P7	✓ VALID	0x8f6d...320c	Satisfied
P8	✓ VALID	0x2e5b...746d	Satisfied
P9	✓ VALID	0x1c7a...592e	Satisfied
P10	✓ VALID	0x0d4c...b19f	Satisfied
P11	✓ VALID	0xab3e...729d	Satisfied

Table 2: Proof Verification Status

Metric	Count	Percentage
Guiyou Version Superior	7	63.6%
Chenggao Version Superior	2	18.2%
Equal Performance	2	18.2%
Failed Threshold (CG)	1	9.1%
Failed Threshold (GY)	0	0.0%

Table 3: Statistical Analysis of Verification Results

Further applications

Cultural Heritage Preservation

- Validates provenance of historical texts without exposing fragile or sacred original materials.
- Measure feasibility and restoration.

Commercial Bidding

- Define evaluation factors for bids.
- Ensure fairness and choose suitable bids.

Criminal Investigation

- Assess clues with the model.
- Analyze reliability and relevance. Verify clues privately like the model does, aiding investigations.

Blockchain Transactions

- Verify transactions without disclosing sensitive info like amounts and identities, ensuring security and preventing fraud.

Thanks for your listening
Q&A

Lian, Zihe Zhao, Ayizuorehe
AI Thrust, Info Hub, HKUST(GZ)
xlian289@connect.hkust-gz.edu.cn