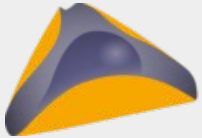


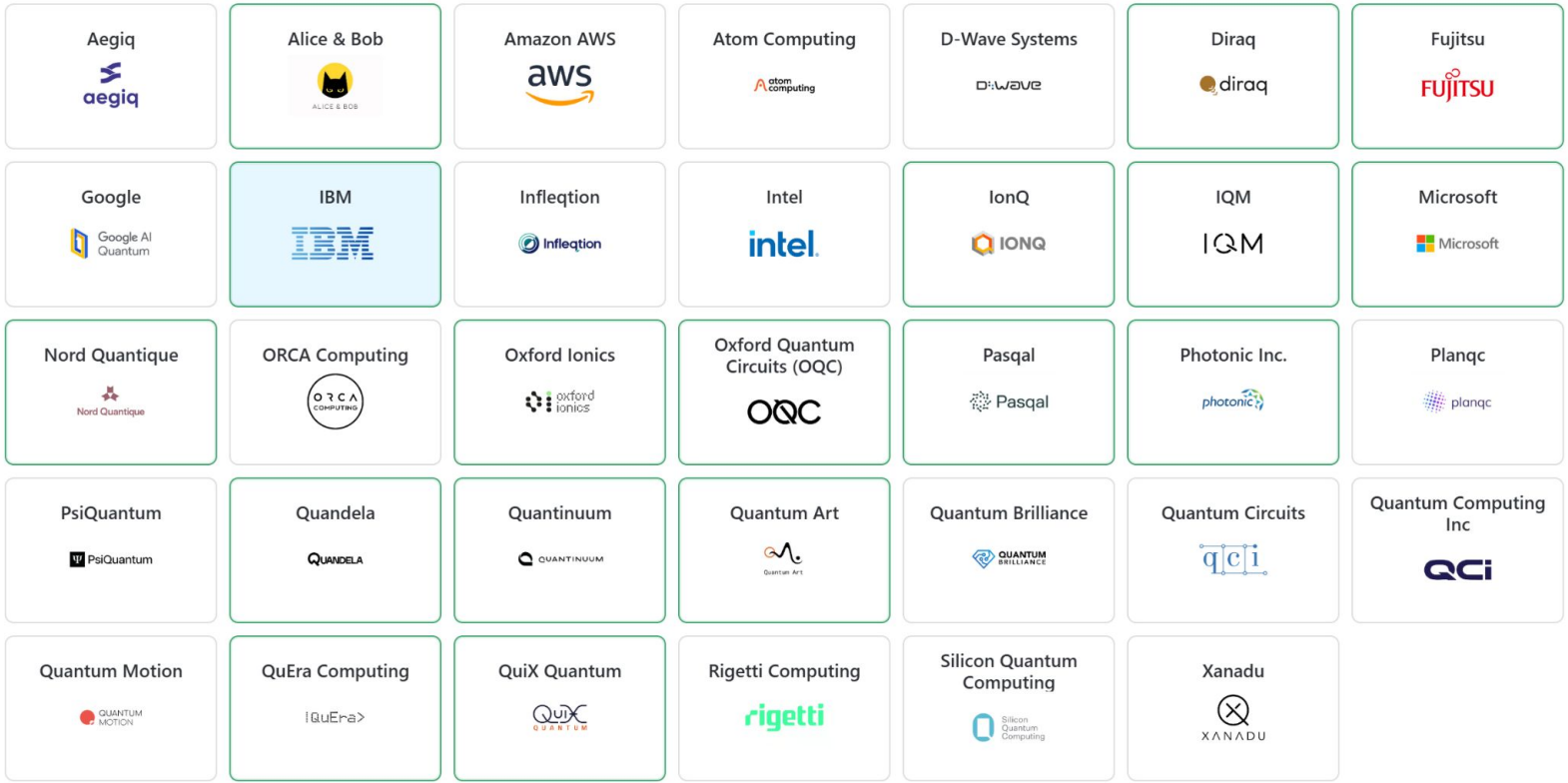
MASTER IN COMPUTER SCIENCE

Dynamic CBOM

A Survey of Cryptographic Bill of Materials Generation and a Runtime Proof-of-Concept

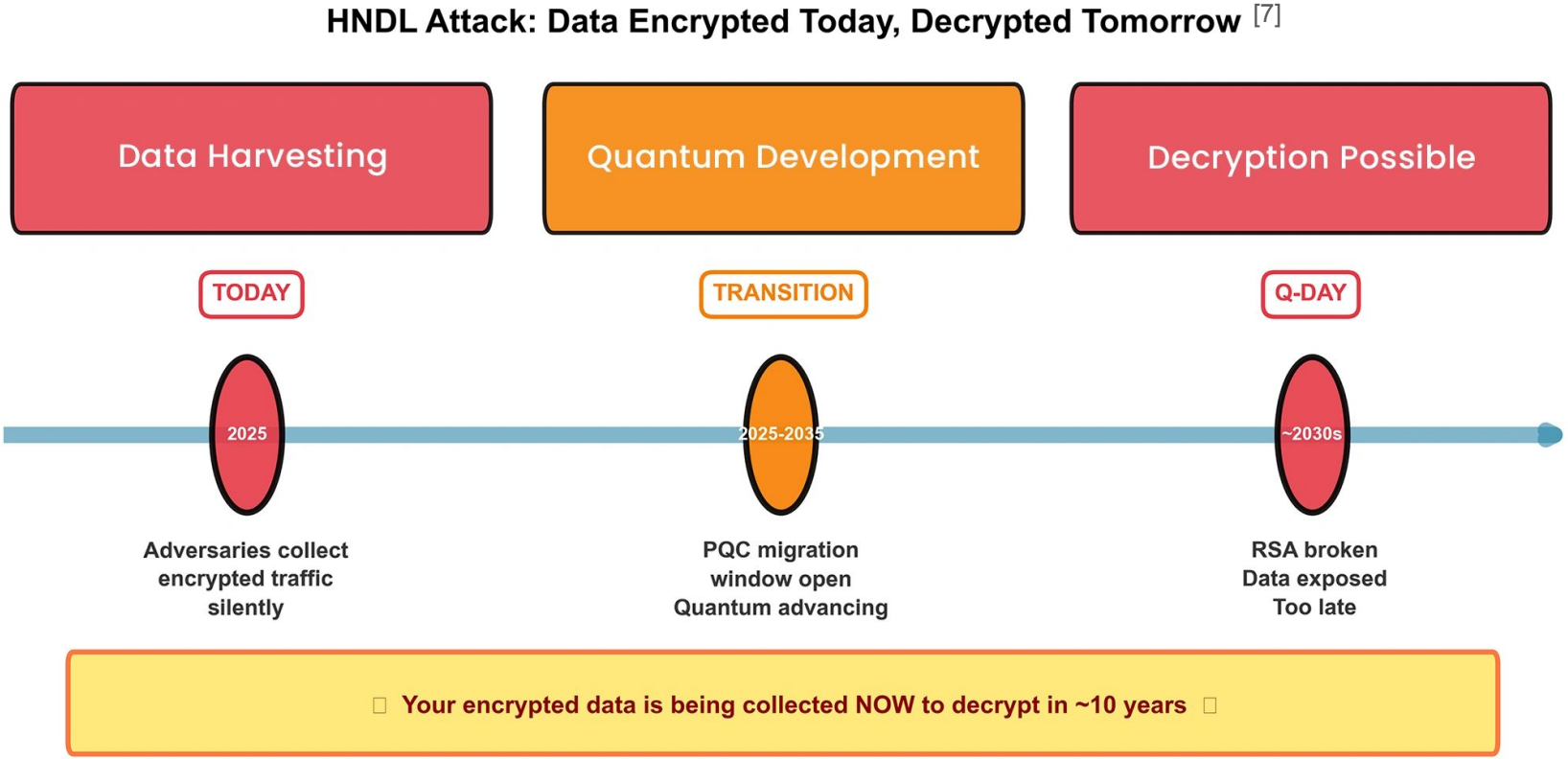
Master Thesis by William Dan

Quantum Roadmap of Large Corps.



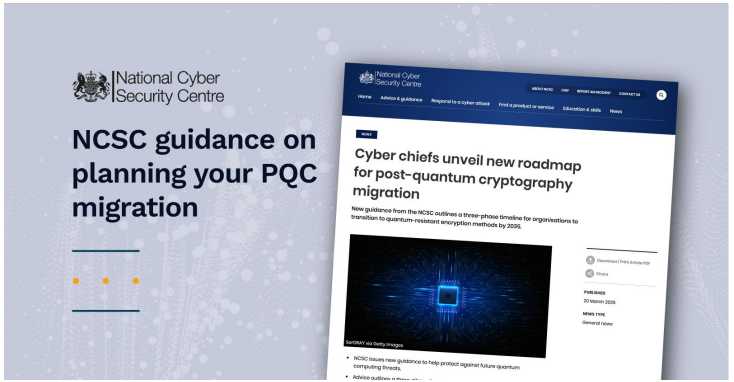
[6]

Harvest-Now-Decrypt-Later Attack

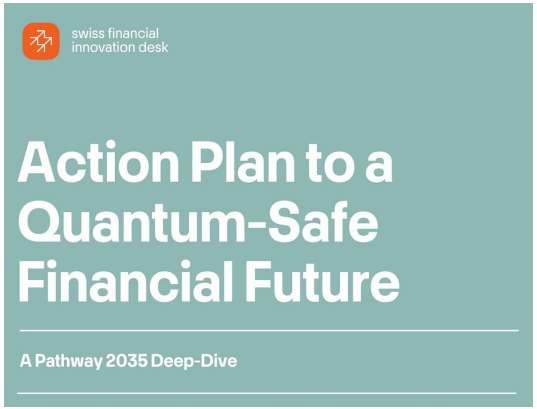


The Urgency to Quantum Migration

[1]



[2]



[3]

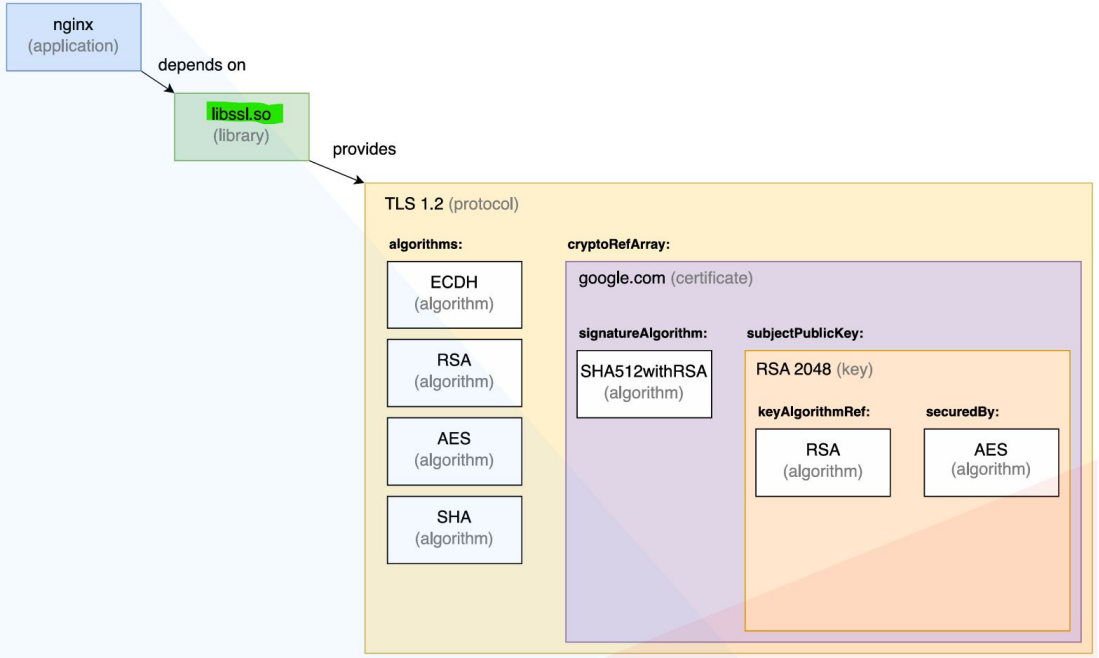
[4]

Senate bill orders White House to create post-quantum cybersecurity roadmap to protect federal systems

AUGUST 04, 2025

[5]

CycloneDX CBOM Standard




```
{
  "name": "RSA-PKCS1-1.5-SHA-512-2048",
  "type": "cryptographic-asset",
  "cryptoProperties": {
    "assetType": "algorithm",
    "algorithmProperties": {
      "algorithmFamily": "RSASSA-PKCS1",
      "primitive": "signature",
      "parameterSetIdentifier": "512",
      "executionEnvironment": "software-plain-ram",
      "implementationPlatform": "x86_64",
      "certificationLevel": [ "none" ],
      "cryptoFunctions": [ "sign", "verify" ],
      "nistQuantumSecurityLevel": 0
    },
    "oid": "1.2.840.113549.1.1.13"
  }
}
```

Research Questions

Research Question 1

Which generation techniques have already been used in current CBOM generator implementation?

CBOM Generation Techniques

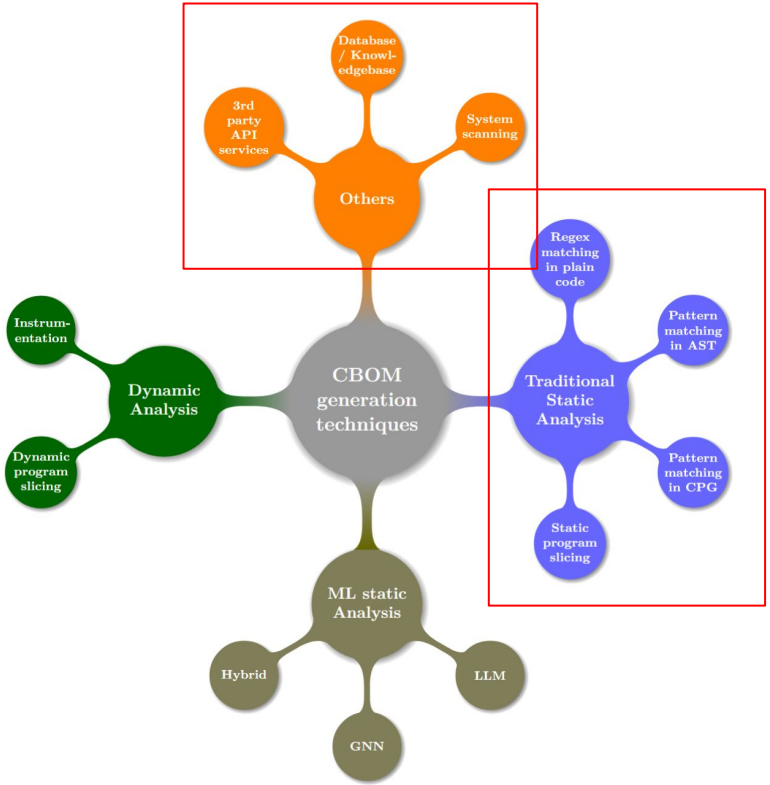


Figure 3.2: Categories of CBOM Generation Techniques

Table 3.1: CBOM Generators vs. generation techniques (tick = technique used by tool).

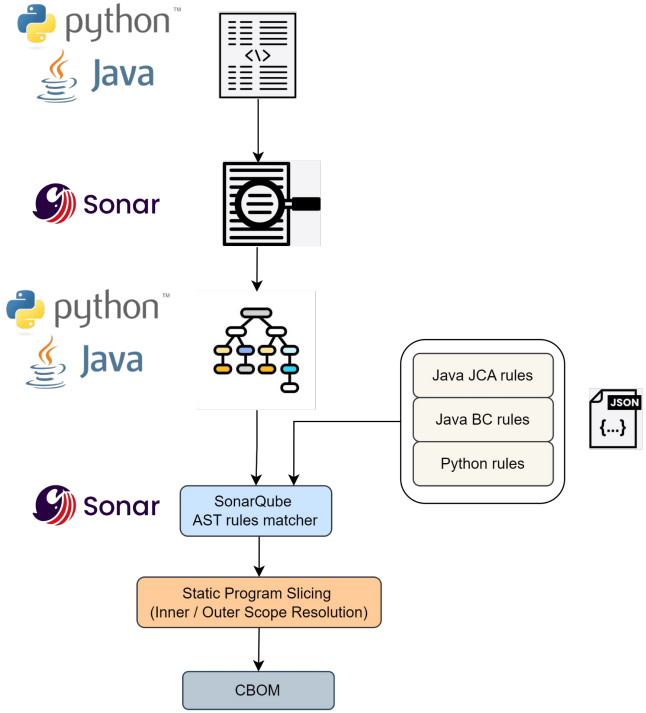
	Static analysis				Dynamic analysis		ML			Others		
Tool	Regex	AST	CPG	Program slicing	Instrumentation	Program slicing	LLM	GNN	Hybrid	System scanning	API Service	Knowledgebase
`cdxgen`* [49]	✓		✓	✓							✓	✓
`CBOMkit`* [67]		✓		✓						✓	✓	✓
`cryptobom-forge` [25]			✓								✓	✓
`CBOM-tool` [80]	✓											✓
`cbom-action` [16]			✓								✓	✓
`cbom-generator` [20]	✓									✓		✓
`crypto-bom-scanner` [100]			✓								✓	✓
`CBOM-Lens` [23]	✓									✓		✓
`qramm-cryptoscan` [109]	✓											✓
`qramm-cryptodeps` [21]	✓											✓

* Primary focus tools in our analysis.

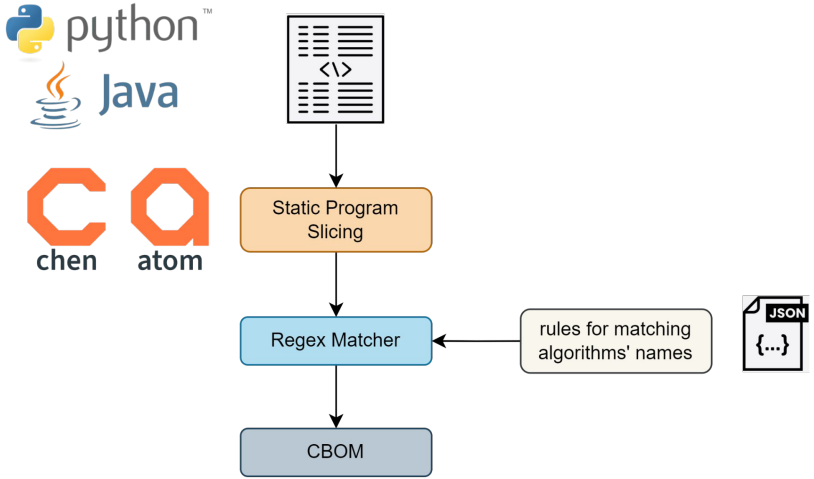
abbrev:

- Regex = Regex matching in plain code
- AST = Pattern matching in AST
- CPG = Pattern matching in CPG
- API Service = 3rd party API Services
- Knowledgebase = Database / Knowledgebase

How Techniques Used inside Tools



CBOMkit Sonar Cryptography Workflow



Cdxgen Workflow

Research Questions

Research Question 2

Which techniques can be potentially used in the future CBOM generator?

CBOM Generation Techniques

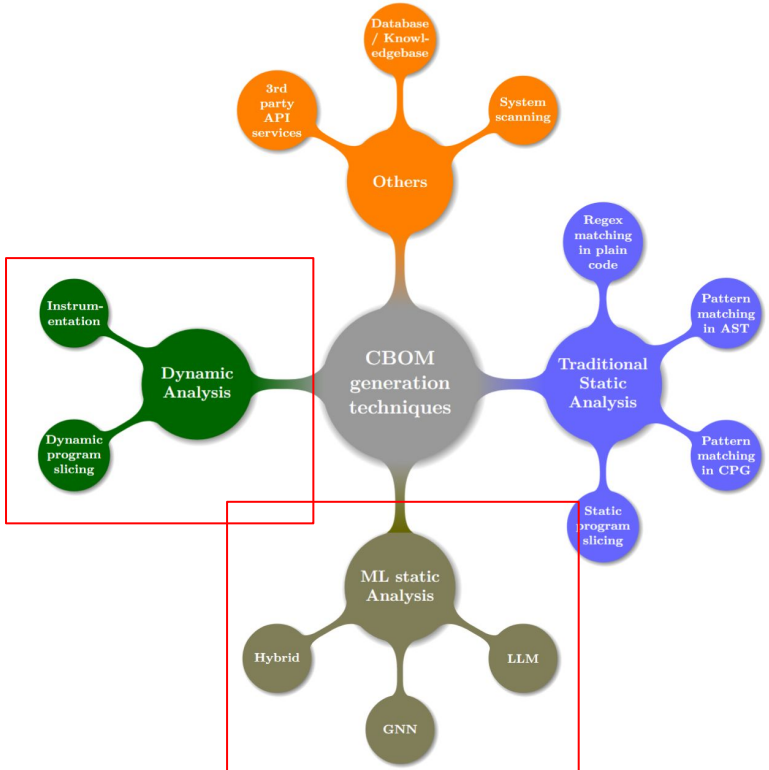


Figure 3.2: Categories of CBOM Generation Techniques

Table 3.1: CBOM Generators vs. generation techniques (tick = technique used by tool).

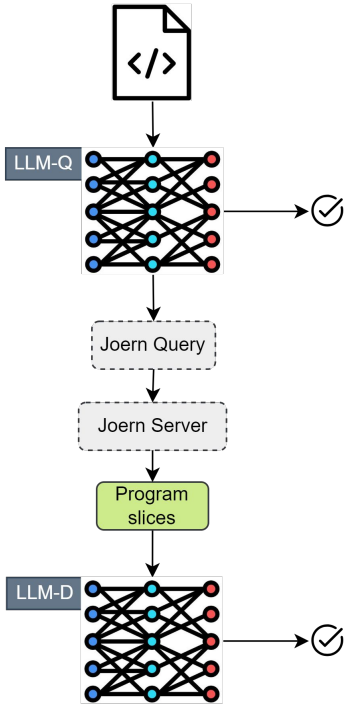
	Static analysis				Dynamic analysis		ML			Others		
Tool	Regex	AST	CPG	Program slicing	Instrumentation	Program slicing	LLM	GNN	Hybrid	System scanning	API Service	Knowledgebase
`cdxgen`* [49]	✓		✓	✓							✓	✓
`CBOMkit`* [67]		✓		✓						✓	✓	✓
`cryptobom-forge` [25]			✓								✓	✓
`CBOM-tool` [80]	✓											✓
`cbom-action` [16]			✓								✓	✓
`cbom-generator` [20]	✓									✓		✓
`crypto-bom-scanner` [100]			✓								✓	✓
`CBOM-Lens` [23]	✓									✓		✓
`qramm-cryptoscan` [109]	✓											✓
`qramm-cryptodeps` [21]	✓											✓

* Primary focus tools in our analysis.

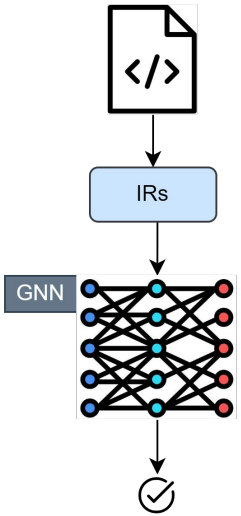
abbrev:

- Regex = Regex matching in plain code
- AST = Pattern matching in AST
- CPG = Pattern matching in CPG
- API Service = 3rd party API Services
- Knowledgebase = Database / Knowledgebase

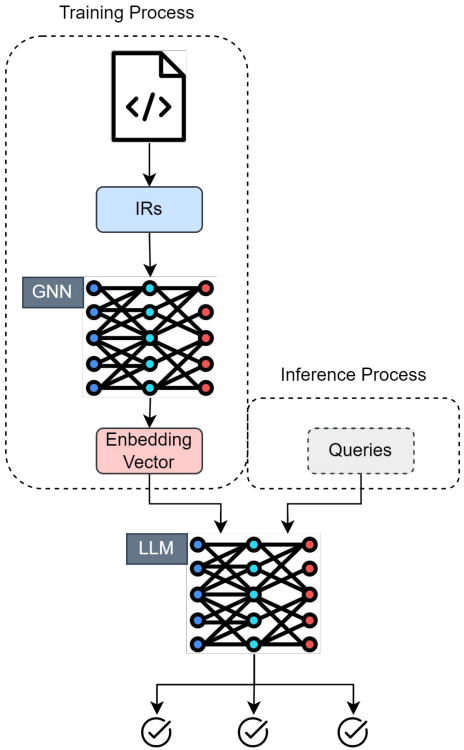
ML Static Analysis on Vulnerability Detection



LLM approach



GNN approach



Hybrid approach

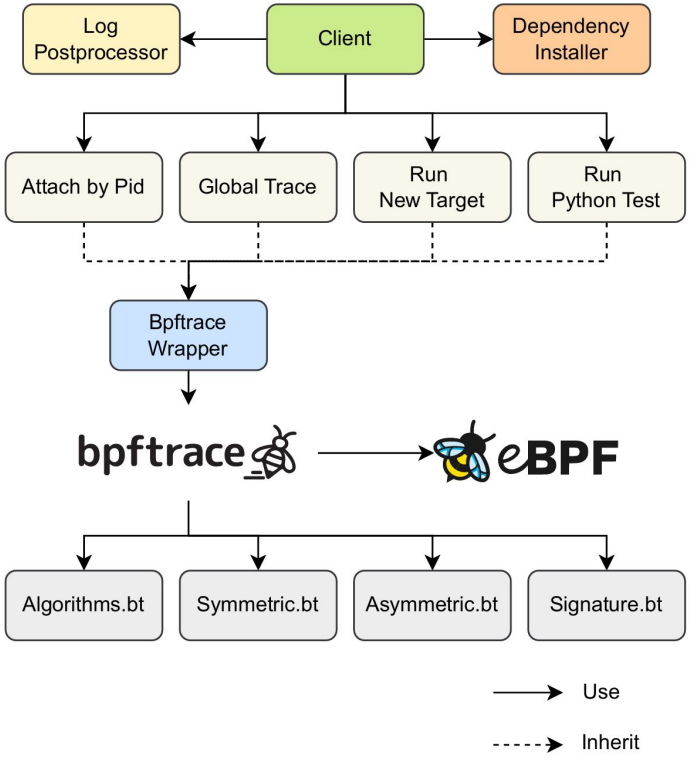
Research Questions

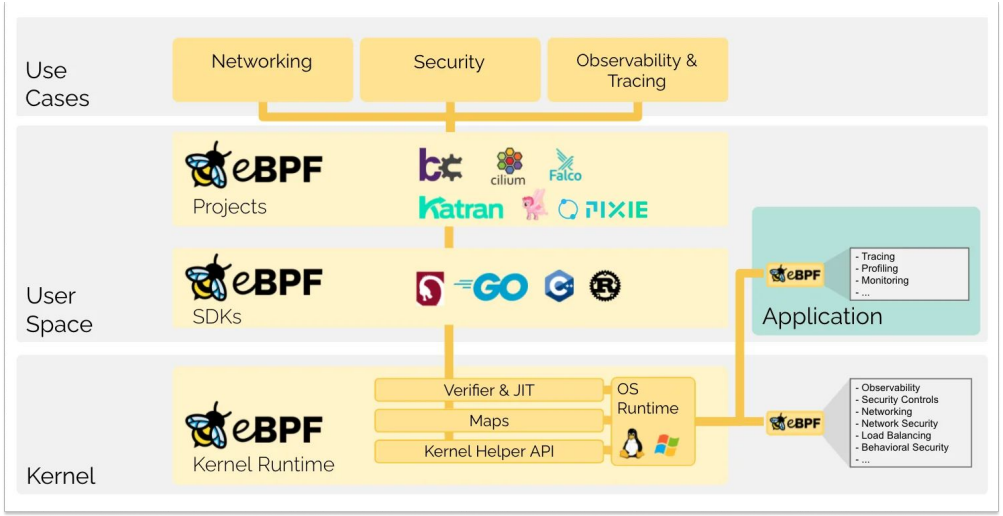
MASTER IN COMPUTER SCIENCE

Research Question 3

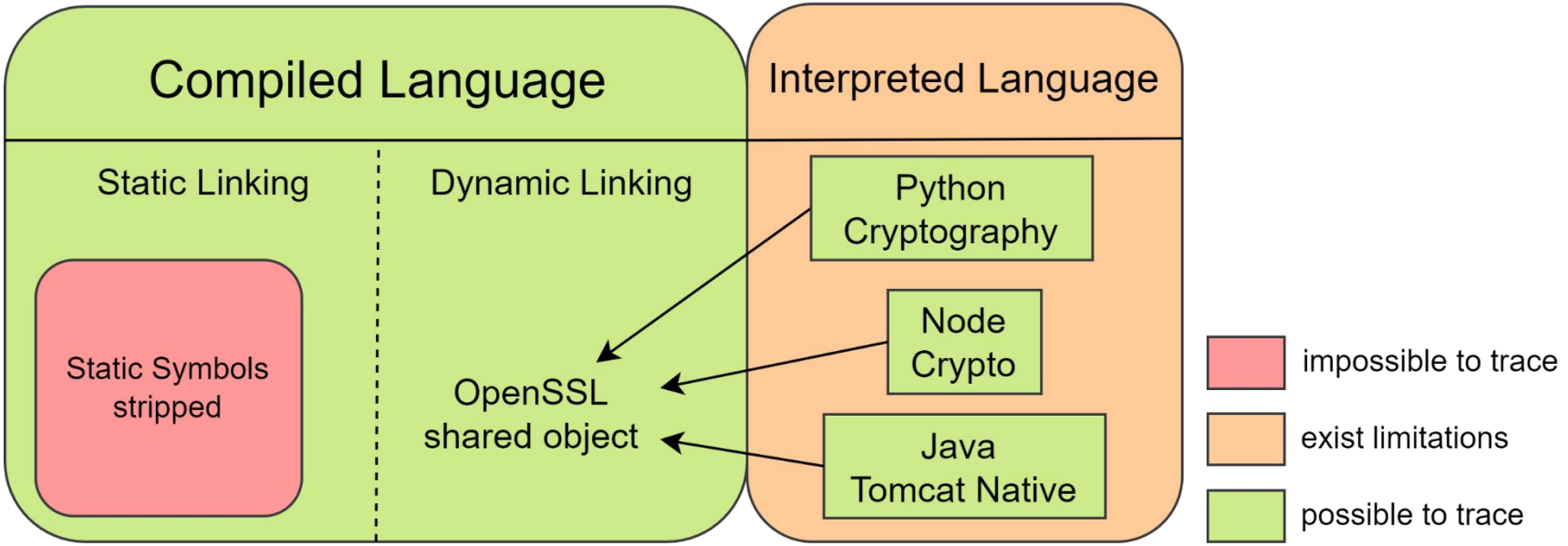
To what extent can we improve the current implementation by introducing new techniques?

Dynamic CBOM Architecture

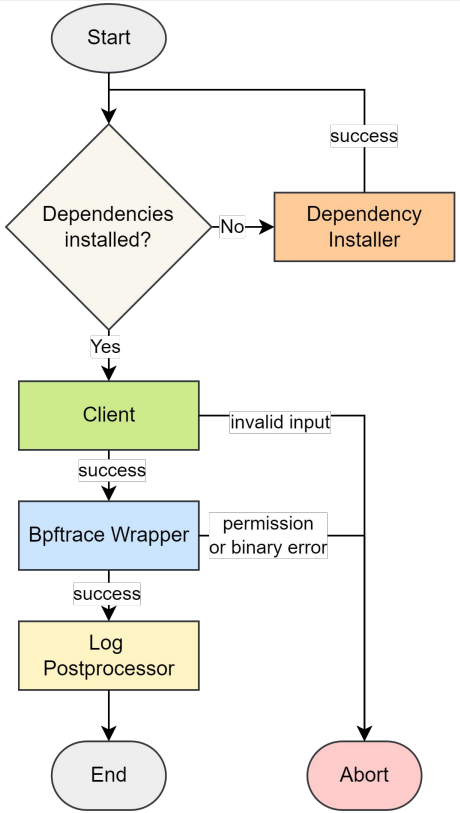


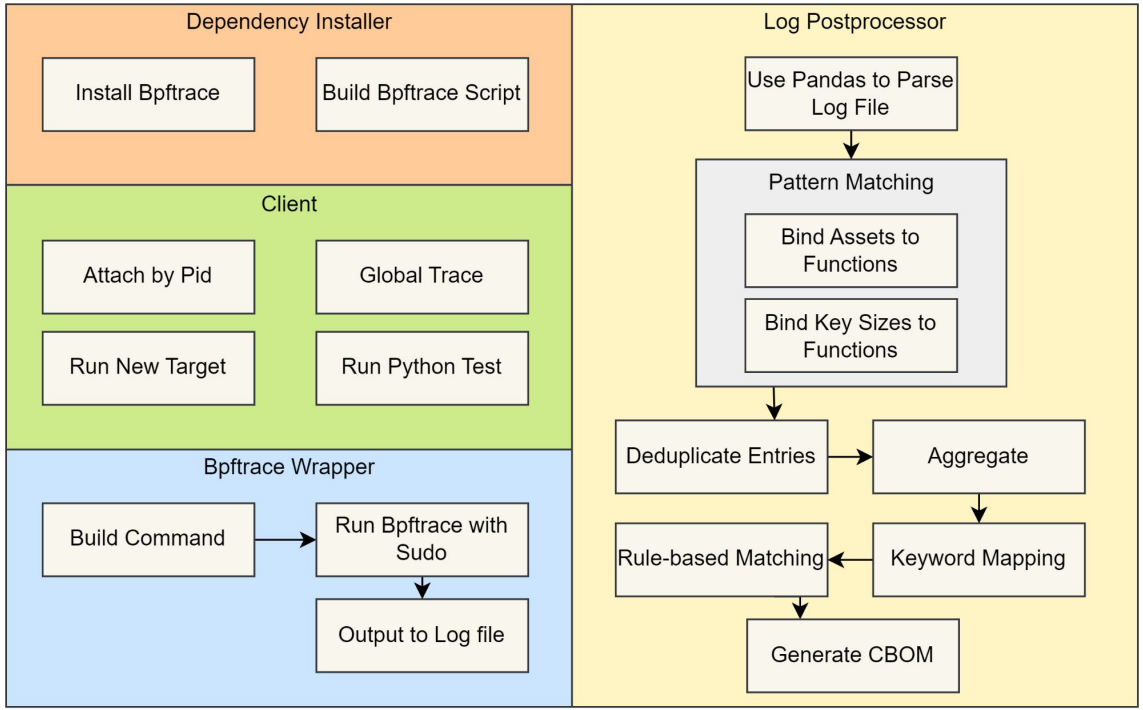


The Theoretic Scope of Dynamic CBOM

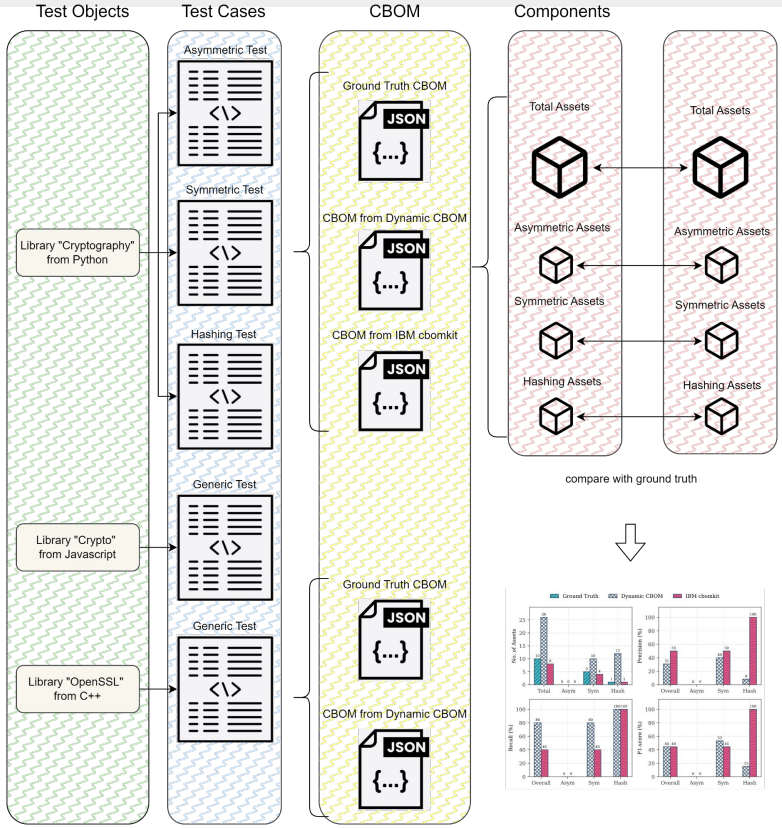


Implementation Details





Evaluation Design



Algorithm 1 CBOM Evaluation Method

Require: Ground truth assets $G = \{g_i\}_{i=1..n}$, target assets $T = \{t_j\}_{j=1..m}$, threshold $\tau \in [0, 1]$
Ensure: Matches M (GT $\rightarrow$ Target or $\varnothing$) and metrics P, R, F_1

function SIM(g, t)
  $s_{\text{name}} \leftarrow$ FUZZYTOKENSORT(`name`(g), `name`(t)) ▷ normalized to $[0, 1]$
  $s_{\text{prim}} \leftarrow \mathbb{1}[\texttt{primitive}(g) = \texttt{primitive}(t)]$
  return $0.5\, s_{\text{name}} + 0.5\, s_{\text{prim}}$
end function
procedure CBOMMATCH(G, T, τ)
  $S \leftarrow \mathbf{0}^{n \times m}$ ▷ similarity matrix
  for $i \leftarrow 1$ **to** n **do**
    for $j \leftarrow 1$ **to** m **do**
      $S[i, j] \leftarrow$ SIM(g_i, t_j)
    end for
  end for
  $C \leftarrow 1 - S$ ▷ cost matrix
  $\mathcal{A} \leftarrow$ HUNGARIANASSIGN(C) ▷ assigned pairs (i, j)
  $M \leftarrow [\,]$; $U \leftarrow \emptyset$ ▷ U: target indices used by accepted matches
  for all $(i, j) \in \mathcal{A}$ **do**
    if $S[i, j] \geq \tau$ **then**
      APPEND(M, (g_i.`bom-ref` $\rightarrow$ t_j.`bom-ref`, $S[i, j]$))
      $U \leftarrow U \cup \{j\}$
    else
      APPEND(M, (g_i.`bom-ref` $\rightarrow \varnothing$, $S[i, j]$)) ▷ below threshold $\Rightarrow$ FN
    end if
  end for
  $TP \leftarrow |\{x \in M \mid x \text{ maps to non-}\varnothing\}|$
  $FP \leftarrow m - |U|$ ▷ unmatched target assets
  $FN \leftarrow n - TP$
  $P \leftarrow \frac{TP}{TP+FP}$
  $R \leftarrow \frac{TP}{TP+FN}$
  $F_1 \leftarrow \frac{2PR}{P+R}$
  return M, P, R, F_1
end procedure

Result

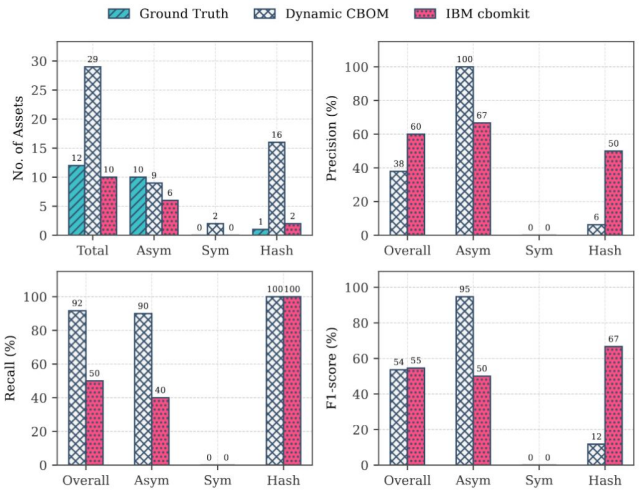


Figure 5.2: Asymmetric Test Result Comparison

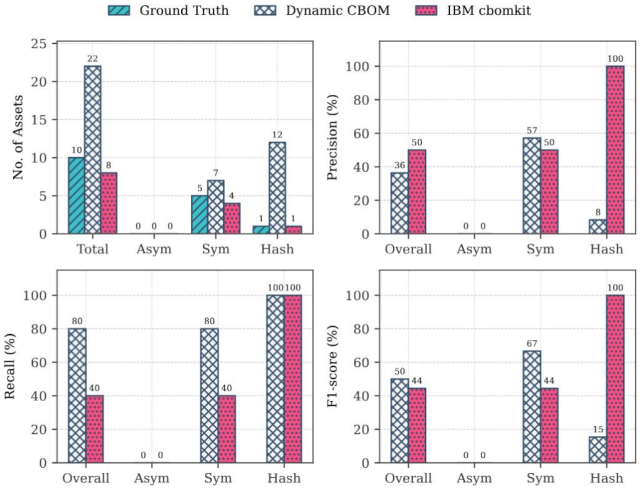


Figure 5.4: Symmetric Test Result Comparison

(a) Ground Truth (b) Dynamic CBOM (c) IBM cbomkit

Figure 5.3: Wordcloud of Asymmetric Test

(a) Ground Truth (b) Dynamic CBOM (c) IBM cbomkit

Figure 5.5: Wordcloud of Symmetric Test

Result

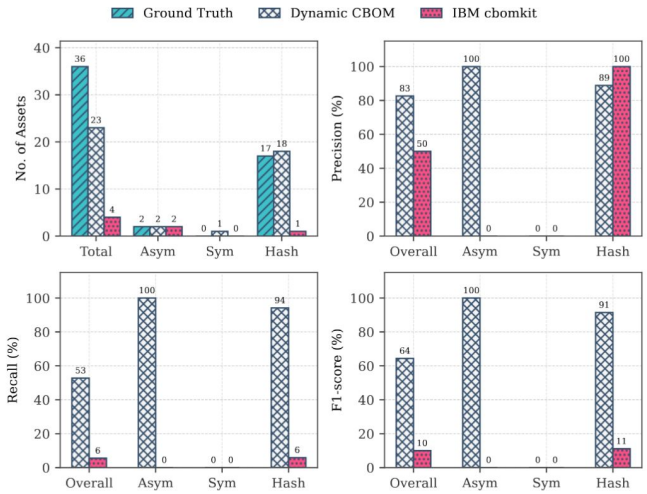


Figure 5.6: Hashing Test Result Comparison

(a) Ground Truth (b) Dynamic CBOM (c) IBM cbomkit

Figure 5.7: Wordcloud of Hashing Test

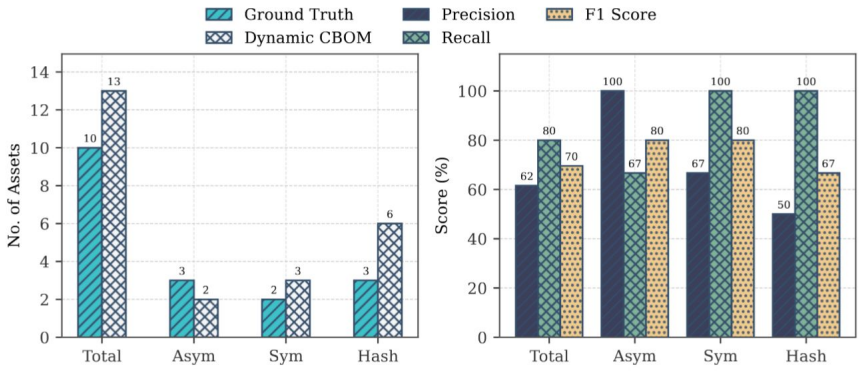


Figure 5.8: Javascript Test Result from Dynamic CBOM

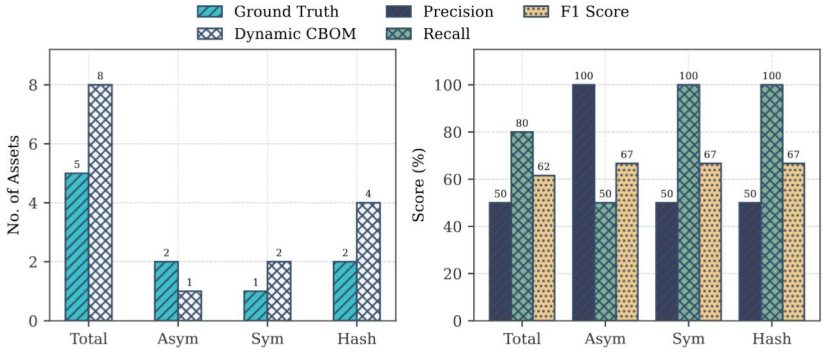


Figure 5.9: C++ Test Result from Dynamic CBOM

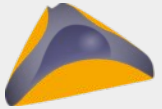
Final Project

Code is open source

Available on:

https://github.com/SEG-UNIBE/DynamicCBOM

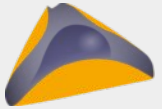
Limitations



MASTER IN COMPUTER SCIENCE

- Ad-hoc Test Bias
- Limited Covered Components (Symmetric, Asymmetric, Hash Algorithm)
- Limited Covered Library (OpenSSL)

Future Work



MASTER IN COMPUTER SCIENCE

- Combine Dynamic CBOM as a supplementation to static generation tool
- Develop other dynamic generation tools such as Java Bytebuddy to cover more languages
- Develop Ground Truth Dataset
- Develop a reusable Knowledgebase for rule-based detection
- Develop ML generation tool
- Improve current CycloneDX CBOM Standard

References

[1] M. Stubbs, “2035: Japan’s NCO sets the timeline for quantum security,” PQShield. Accessed: Jan. 05, 2026. [Online]. Available: https://pqshield.com/2035-japans-nco-sets-the-timeline-for-quantum-security/

[2] M. Abdel-Kareem, “UK’s NCSC Sets 2035 Deadline for National Migration to Post-Quantum Cryptography,” Quantum Computing Report. Accessed: Jan. 05, 2026. [Online]. Available: https://quantumcomputingreport.com/uks-ncsc-sets-2035-deadline-for-national-migration-to-post-quantum-cryptography/

[3] Swiss Financial Innovation Desk (FIND), Action Plan to a Quantum-Safe Financial Future.pdf. Accessed: Jan. 05, 2026. [Online].

[4] “中国移动研究院发布《应对量子威胁：SIM体系抗量子密 码迁移白皮 书》- 中国移动 — C114通信网.” Accessed: Jan. 05, 2026. [Online]. Available: https://www.c114.com.cn/news/118/a1291472.html

[5] A. Ribeiro, “Senate bill orders White House to create post-quantum cybersecurity roadmap to protect federal systems,” Industrial Cyber. Accessed: Jan. 05, 2026. [Online]. Available: https://industrialcyber.co/regulation-standards-and-compliance/senate-bill-orders-white-house-to-create-post-quantum-cybersecurity-roadmap-to-protect-federal-systems/

References

[6] Marin and M. Ivezic, “Quantum Hardware Companies and Roadmaps Comparison,” PostQuantum - Quantum Computing, Quantum Security, PQC. Accessed: Dec. 24, 2025. [Online]. Available: https://postquantum.com/quantum-computing-roadmaps-2025/

[7] “The Quantum Threat Is Already Here: We Just Can’t See It Yet,” United States Cybersecurity Magazine. Accessed: Jan. 05, 2026. [Online]. Available: https://www.uscybersecurity.net/csmag/the-quantum-threat-is-already-here-we-just-cant-see-it-yet/