RUB CASA Securing the Digital Society

Chair for Software Security

Hallucinating Certificates

Differential Testing of TLS Certificate Validation Using Generative Language Models

Talha Paracha[1] Kyle Posluns[2] Kevin Borgolte[1] Martina Lindorfer[3] David Choffnes[2]

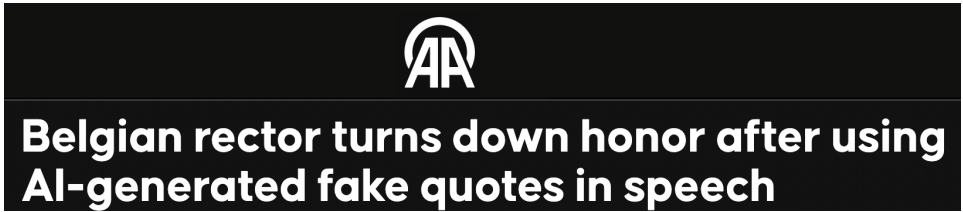
[1]Ruhr University Bochum [2]Northeastern University [3]TU Wien

48th International Conference on Software Engineering
Rio de Janeiro, Brazil
April 15, 2026

Language Models & Hallucinations

Hallucinating Certificates
Paracha et al.

Lawyer caught using AI-generated false citations in court case penalised in Australian first



Transport Layer Security (TLS)

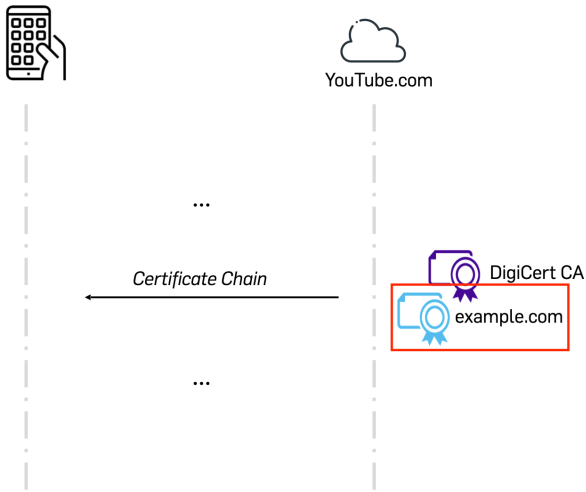
Transport Layer Security (TLS)
Certificate Validation

...

Certificate Chain

...

Transport Layer Security (TLS)
Certificate Validation



Transport Layer Security (TLS)
Certificate Validation

...

Certificate Chain

...

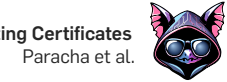
Transport Layer Security (TLS)
Certificate Validation

...

Certificate Chain

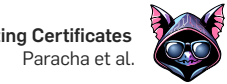
...

Sample TLS Certificate (PEM Encoded)



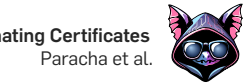
```
-----BEGIN CERTIFICATE-----
MIIFYjCCBEqgAwIBAgIQd70NbNs2+RrqIQ/E8FjTDTANBgkqhkiG9w0BAQsFADBX
MQswCQYDVQQGEwJCRTEZMBcGA1UEChMQR2xvYmFsU2lnbiBudi1zYTEQMA4GA1UE
CxMHUm9vdCBDQTEbMBkGA1UEAxMSR2xvYmFsU2lnbiBSb290IENBMB4XDTIwMDYx
........
9U5pCZEt4Wi4wStz6dTZ/CLANx8LZh1J7QJVj2fhMtfTJr9w4z30Z209fOU0iOMy
+qduBmpvvYuR7hZL6Dupszfnw0Skfths18dG9ZKb59UhvmaSGZRVbNQpsg3BZlvi
d0lIKO2d1xozclOzgjXPYovJJIultzkMu34qQb9Sz/yilrbCgj8=
-----END CERTIFICATE-----
```

Sample TLS Certificate (Decoded)



```
Certificate:
 Data:
  Version: 3 (0x2)
  Serial Number:
   77:bd:0d:6c:db:36:f9:1a:ea:21:0f:c4:f0:58:d3:0d
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign CA
  Validity
   Not Before: Jun 19 00:00:42 2020 GMT
   Not After : Jan 28 00:00:42 2028 GMT
  Subject: C=US, O=Google Trust Services LLC, CN=GTS Root R1
  Subject Public Key Info:
   Public Key Algorithm: rsaEncryption
....
```

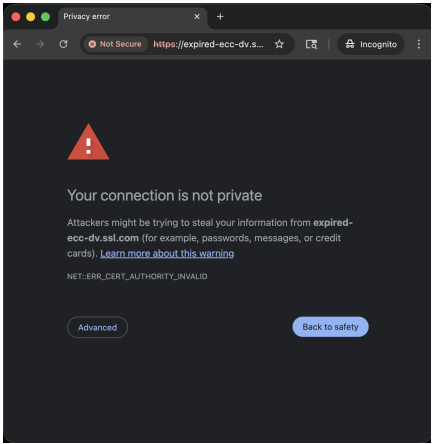
Sample TLS Certificate (Decoded)



```
...
 X509v3 extensions:
  X509v3 Key Usage: critical
  Digital Signature, Certificate Sign, CRL Sign
  X509v3 Basic Constraints: critical
  CA:TRUE
  X509v3 Subject Key Identifier:
   E4:AF:2B:26:71:1A:2B:48:27:85:2F:52:66:2C:EF:F0:89:13:71:3E
  X509v3 Authority Key Identifier:
   60:7B:66:1A:45:0D:97:CA:89:50:2F:7D:04:CD:34:A8:FF:FC:FD:4B
  Authority Information Access:
   OCSP - URI:http://ocsp.pki.goog/gsr1
   CA Issuers - URI:http://pki.goog/gsr1/gsr1.crt
....
```

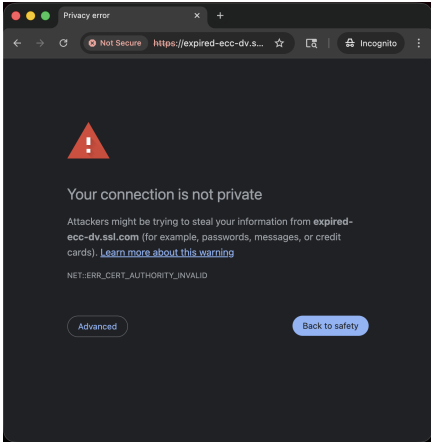
Challenges in Certificate Validation

Challenges in Certificate Validation



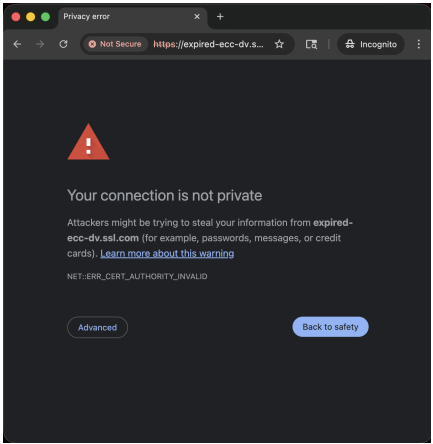
- Certificate validation can neither fail-open (accept ambiguous certificates), nor fail-close (reject ambiguous certificates)

Challenges in Certificate Validation



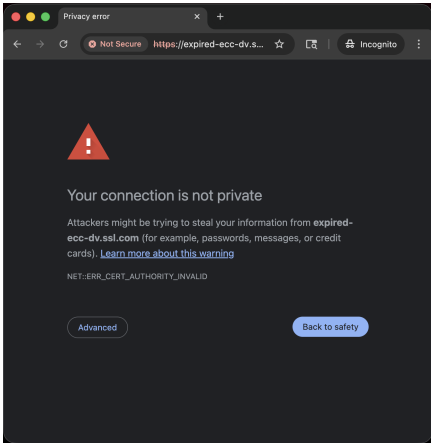
- Certificate validation can neither fail-open (accept ambiguous certificates), nor fail-close (reject ambiguous certificates)
- Validation software susceptible to programming bugs

Challenges in Certificate Validation



- Certificate validation can neither fail-open (accept ambiguous certificates), nor fail-close (reject ambiguous certificates)
- Validation software susceptible to programming bugs
- Protocol RFCs are ambiguous

Challenges in Certificate Validation

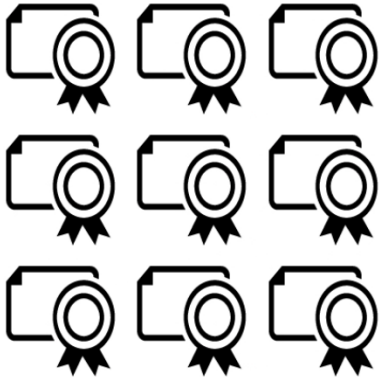


- Certificate validation can neither fail-open (accept ambiguous certificates), nor fail-close (reject ambiguous certificates)
- Validation software susceptible to programming bugs
- Protocol RFCs are ambiguous

Comprehensive testing is essential

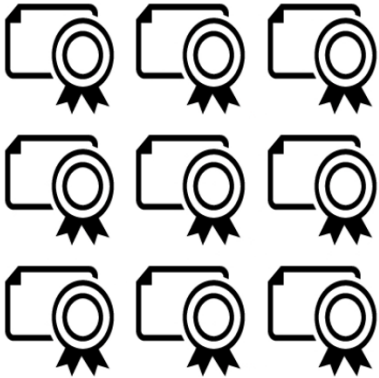
Testing TLS Certificate Validation

Use Real World Certificates



Testing TLS Certificate Validation

Use Real World Certificates



Issue

Edge cases are rare...

Testing TLS Certificate Validation

Frankencerts: Use Mutated Certificates (2014)

Testing TLS Certificate Validation

Frankencerts: Use Mutated Certificates (2014)

Issue

Mutations tend to make certificates invalid...

Testing TLS Certificate Validation

Transcert: Use Code Coverage (2023)

Nie, Pengbo, et al. “Coverage-directed Differential Testing of X.509 Certificate Validation in SSL/TLS Implementations”

Testing TLS Certificate Validation

Transcert: Use Code Coverage (2023)

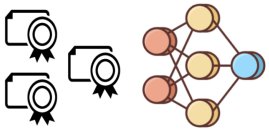
Issue

Certificate generation is slow and cannot be parallelized...

Nie, Pengbo, et al. "Coverage-directed Differential Testing of X.509 Certificate Validation in SSL/TLS Implementations"

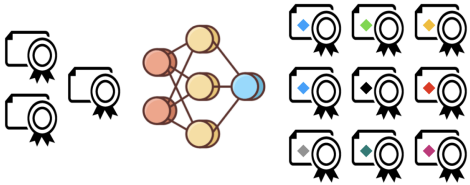
Testing TLS Certificate Validation

MLCerts: Use Language Models (Our Approach)



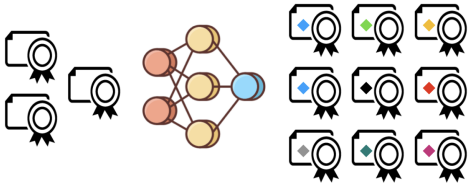
Testing TLS Certificate Validation

MLCerts: Use Language Models (Our Approach)



Testing TLS Certificate Validation

MLCerts: Use Language Models (Our Approach)

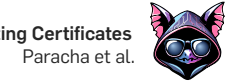


Features

- Can learn a quasi grammar
- Can be parallelized

Testing TLS Certificate Validation

MLCerts and Model Hallucinations



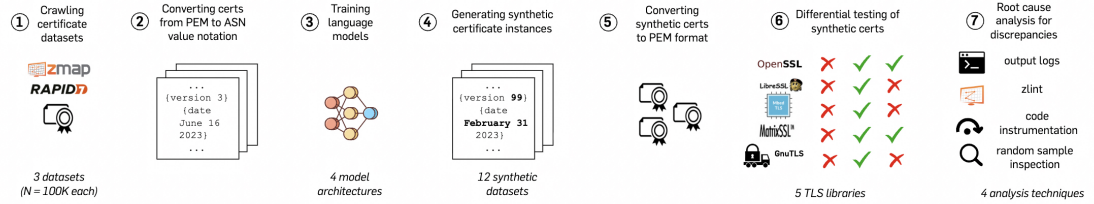
Prompt: How many ‘r’ characters appear in the word “strawberry”

Answer: There are two ‘r’ characters in the word “strawberry”

Insight

Syntactically correct, semantically invalid outputs can help software testing

Methodology



Methodology
Step 1: Training Datasets

3 datasets
(N = 100K each)

Methodology
Step 1: Training Datasets

3 datasets
(N = 100K each)

Insight

Multiple datasets to learn different certificate features

Methodology
Step 1: Training Datasets

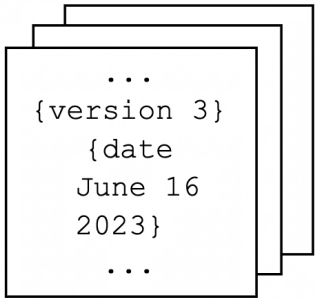
3 datasets
(N = 100K each)

Insight

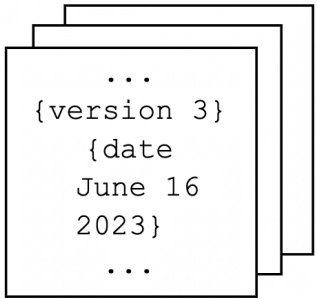
Multiple datasets to learn different certificate features

- IPv4, Modern, and Balanced datasets
- N = 100K certificates per dataset

Methodology
Step 2: Model Inputs



Methodology
Step 2: Model Inputs

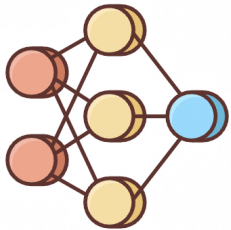


Insight

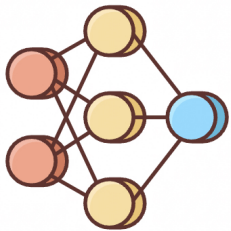
TLS certificates can be represented in a verbose textual notation.

- PyCrate to convert certificates from PEM to ASN.1 value notation.

Methodology
Step 3: Language Models



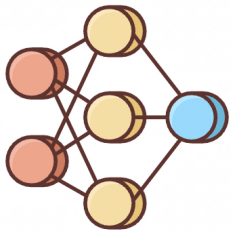
Methodology
Step 3: Language Models



Insight

Unclear if large language models (LLMs) would help or hurt testing

Methodology
Step 3: Language Models

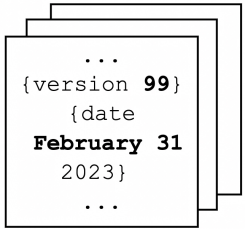


Insight

Unclear if large language models (LLMs) would help or hurt testing

- Use RNNs and GPTs
  - RNN-Small (1 mil. parameters)
  - RNN-Medium (10 mil. parameters)
  - GPT-Finetuned (125 mil. parameters)
  - GPT (125 mil. parameters)

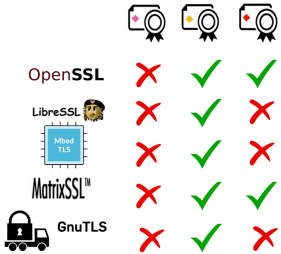
Methodology
Step 4: Generate Synthetic Certificates



12 synthetic datasets

Methodology
Step 5: Convert into PEM format

Methodology
Step 6: Differential Testing



5 TLS libraries

Methodology
Step 7: Discrepancy Analysis

output logs

zlint

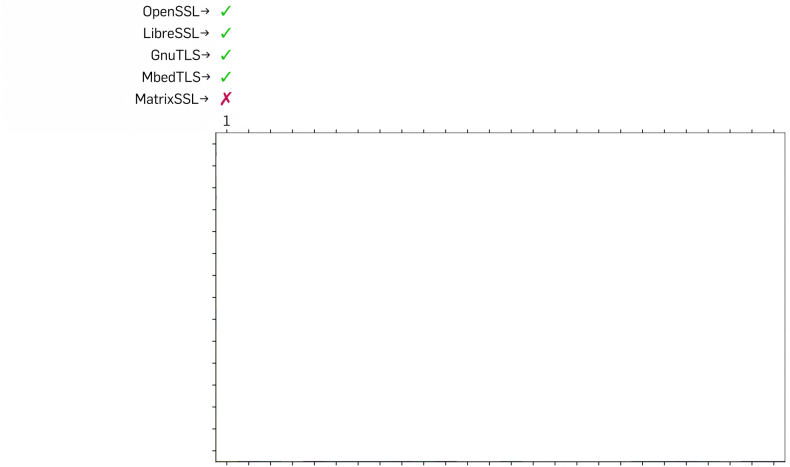
code instrumentation

random sample inspection

4 analysis techniques

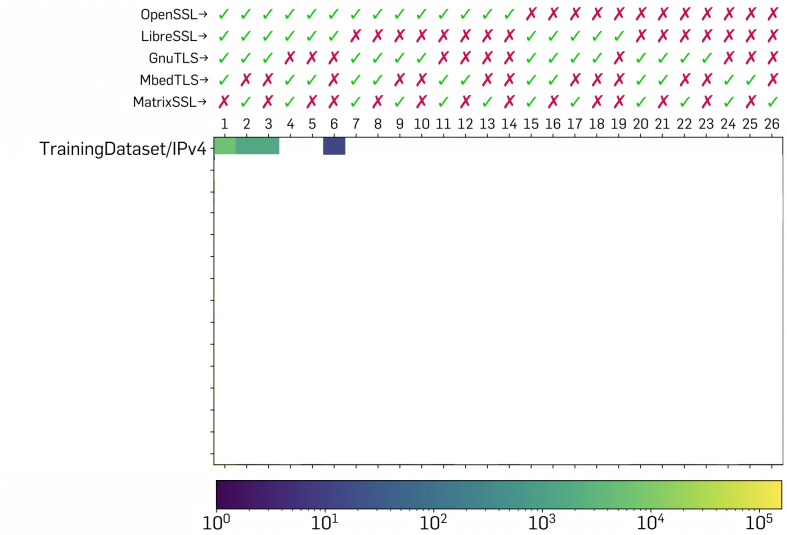
MLCerts Finds Unique Discrepancies

MLCerts Finds Unique Discrepancies



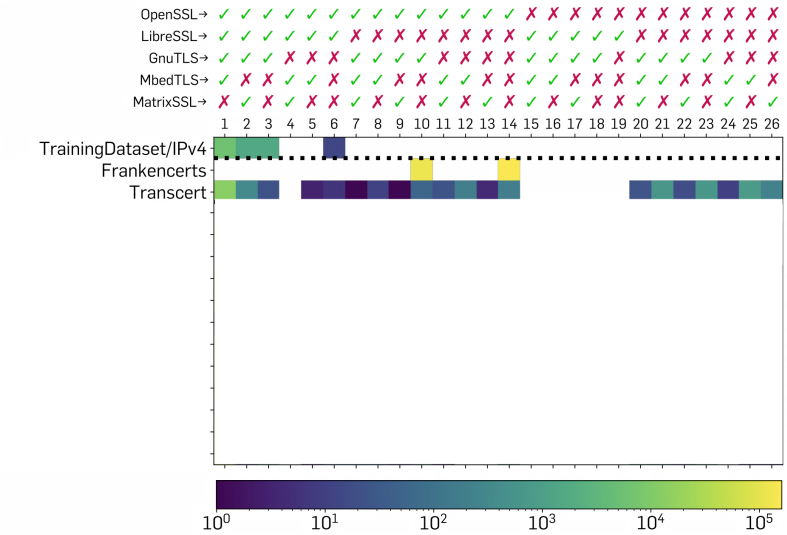
MLCerts Finds Unique Discrepancies

MLCerts Finds Unique Discrepancies

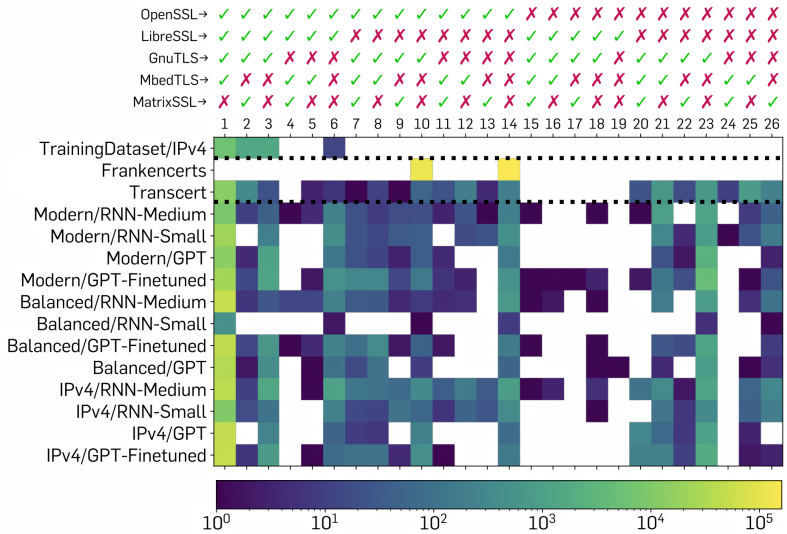


MLCerts Finds Unique Discrepancies

Hallucinating Certificates
Paracha et al.

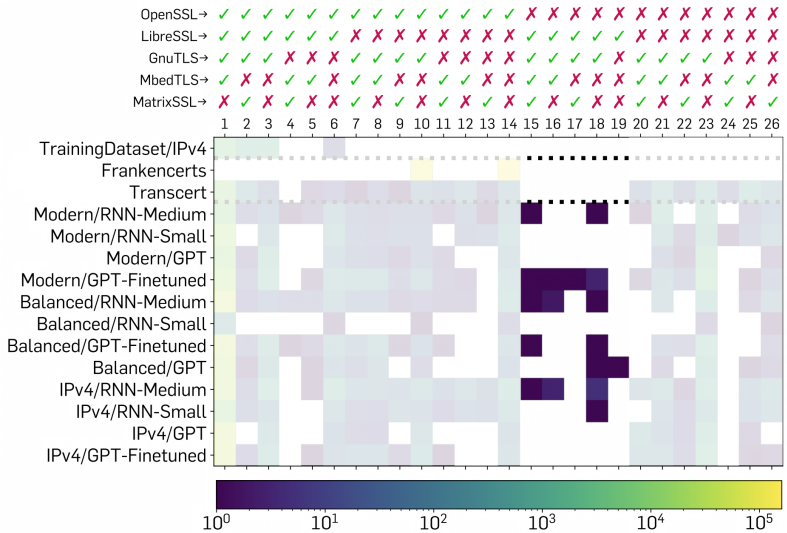


MLCerts Finds Unique Discrepancies

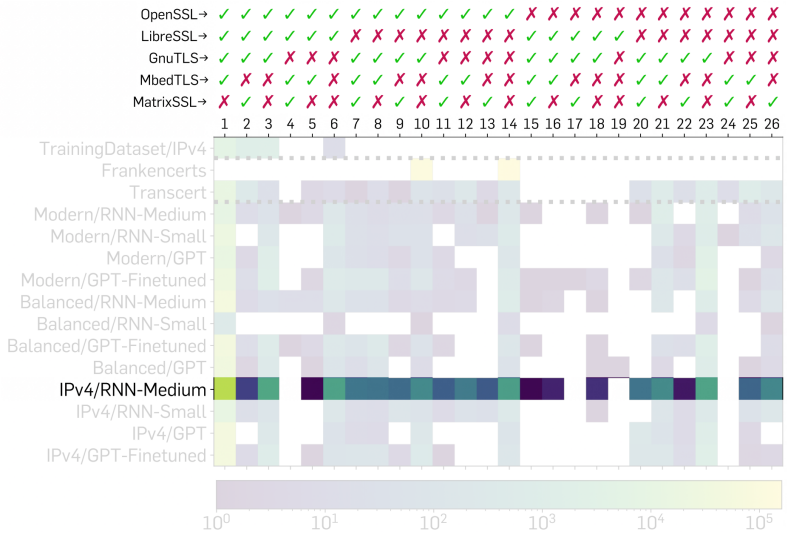


MLCerts Finds Unique Discrepancies

Hallucinating Certificates
Paracha et al.

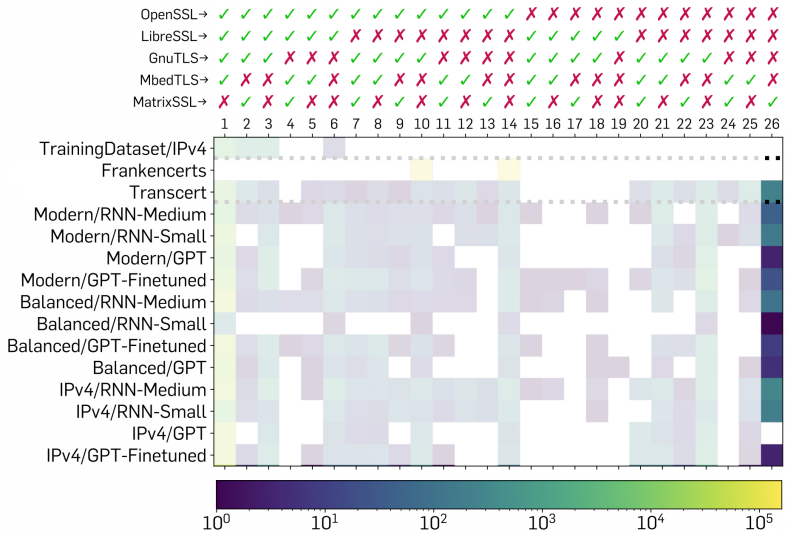


MLCerts Finds Unique Discrepancies



MLCerts Finds Unique Discrepancies

Hallucinating Certificates
Paracha et al.

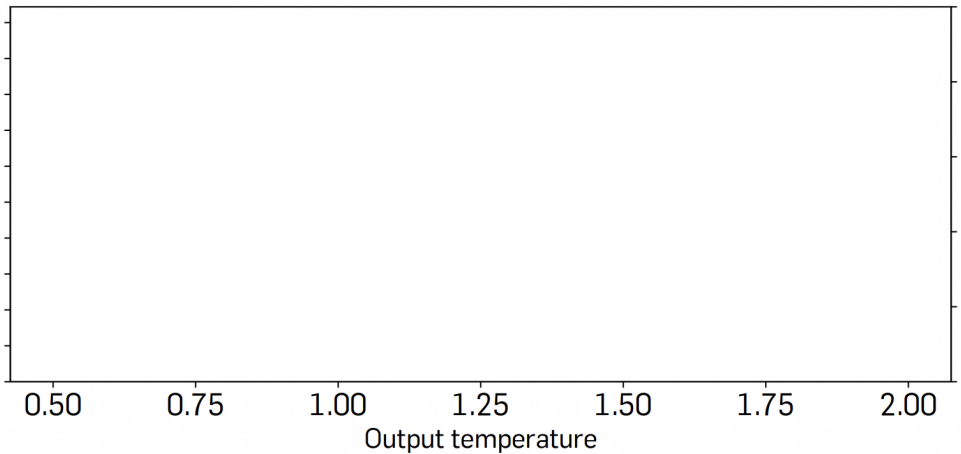


Model Hallucinations Are Useful

Hallucinating Certificates
Paracha et al.

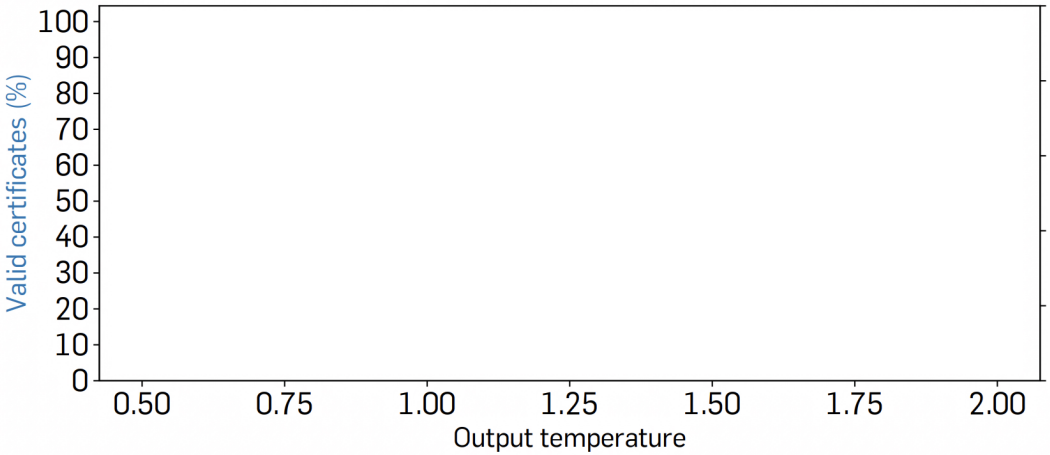
Model Hallucinations Are Useful

Hallucinating Certificates
Paracha et al.



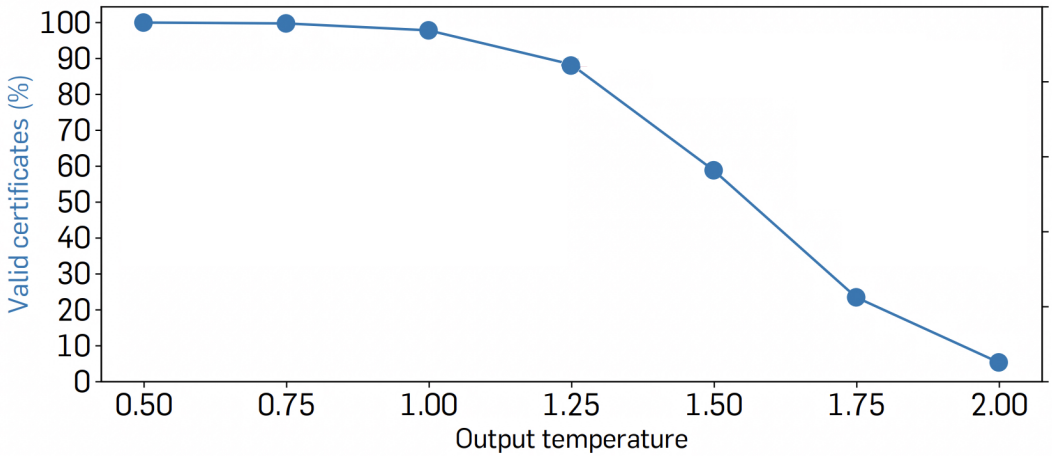
Model Hallucinations Are Useful

Hallucinating Certificates
Paracha et al.



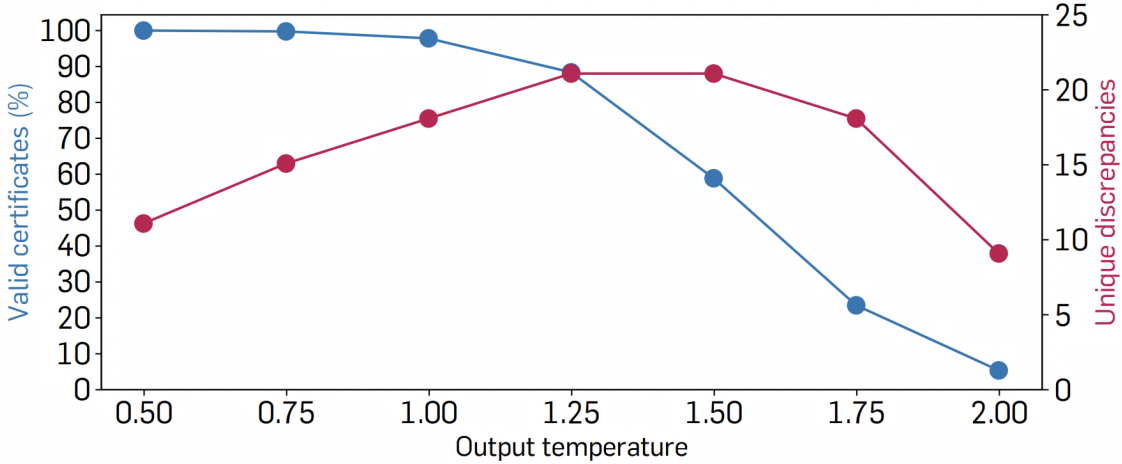
Model Hallucinations Are Useful

Hallucinating Certificates
Paracha et al.

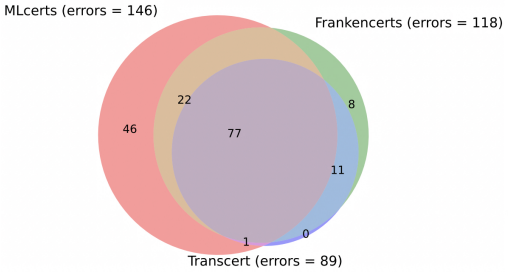


Model Hallucinations Are Useful

Hallucinating Certificates
Paracha et al.

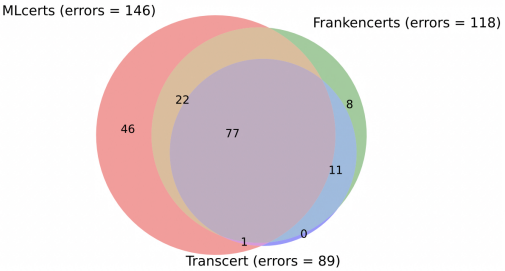


MLCerts Finds New Bugs



- Unique ZLint errors triggered by MLCerts

MLCerts Finds New Bugs



- Unique ZLint errors triggered by MLCerts
- Bugs in certificates with invalid dates:
  - Expiry date as *February 31st*
  - Leap seconds in time value: *YYMMDDHHMM**60***, instead of *YYMMDDHHMM**[0-59]***

Takeaways

- Language models can learn an input representation suitable for testing
- Large models are not necessary
- Need to “guide” the models towards producing diverse testcases

Paper and artifacts:

`softsec.link/icse26.mlcerts`

Funded by

DFG Deutsche Forschungsgemeinschaft
German Research Foundation

CASA
Securing the Digital Society

NSF

WWTF
Vienna Science and Technology Fund