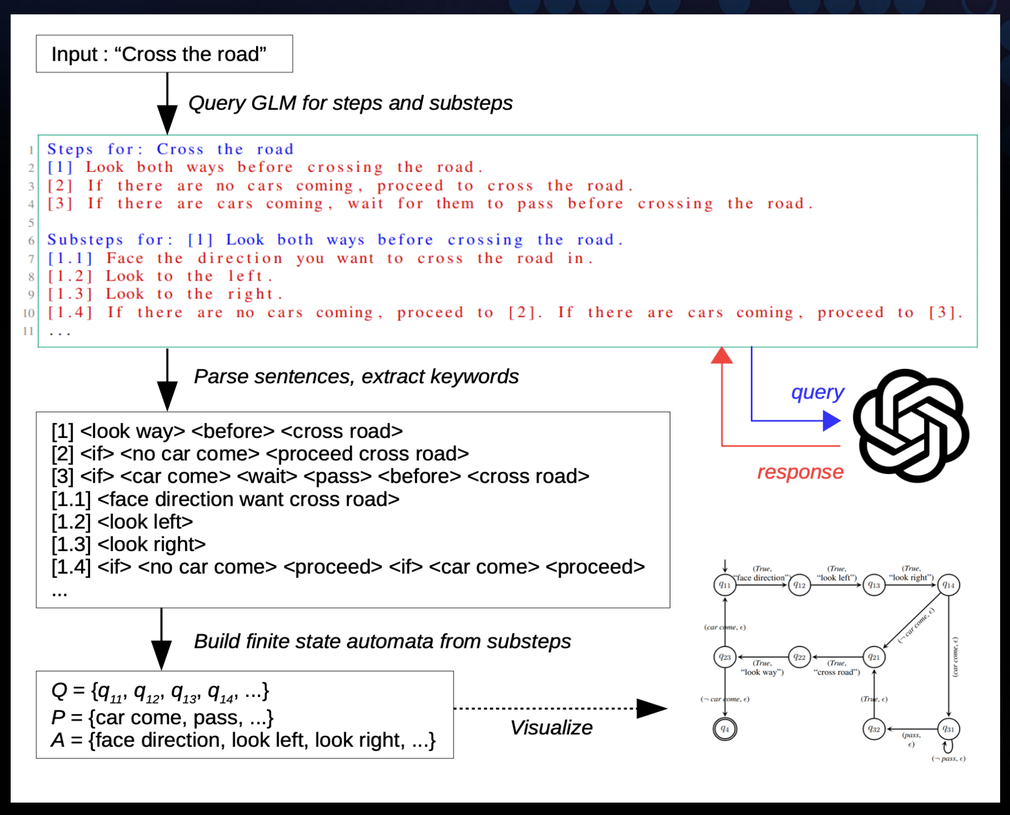
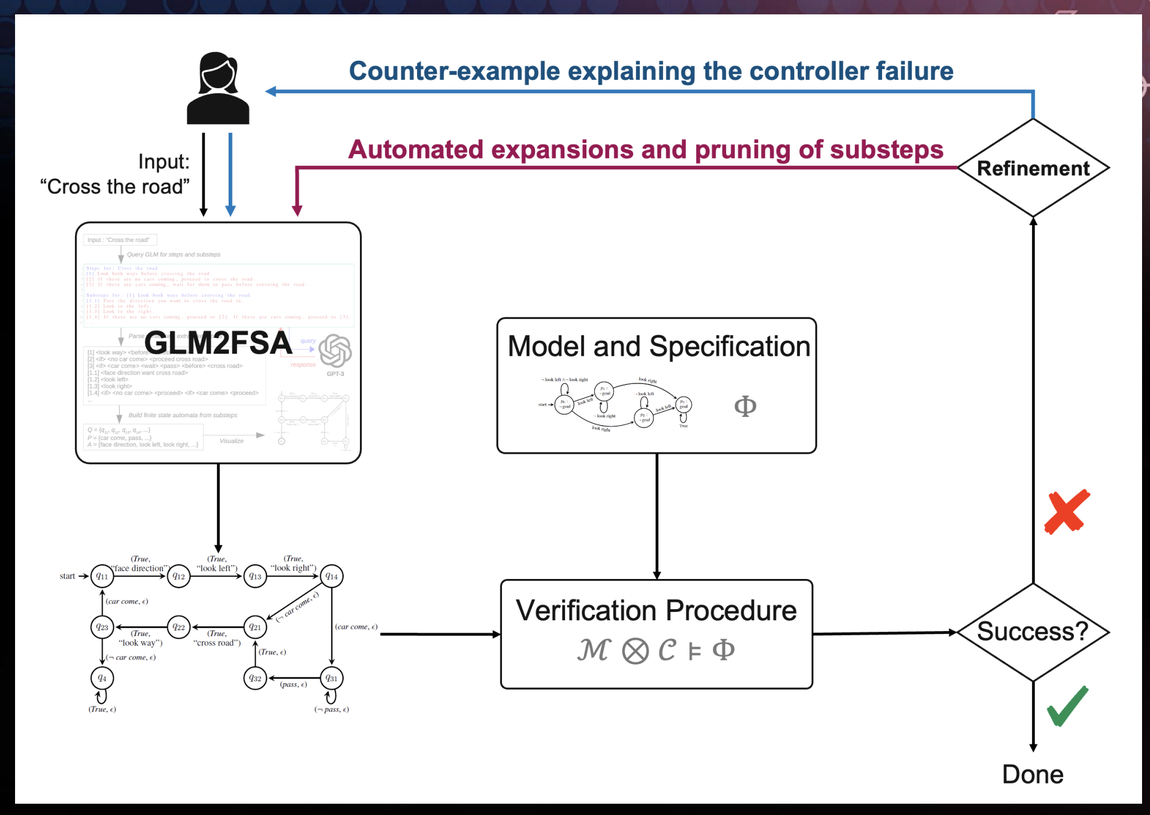
From Generative Pre-Trained Models To Verifiable Protocols for Security and Privacy Preservation

Ufuk Topcu, The University of Texas at Austin





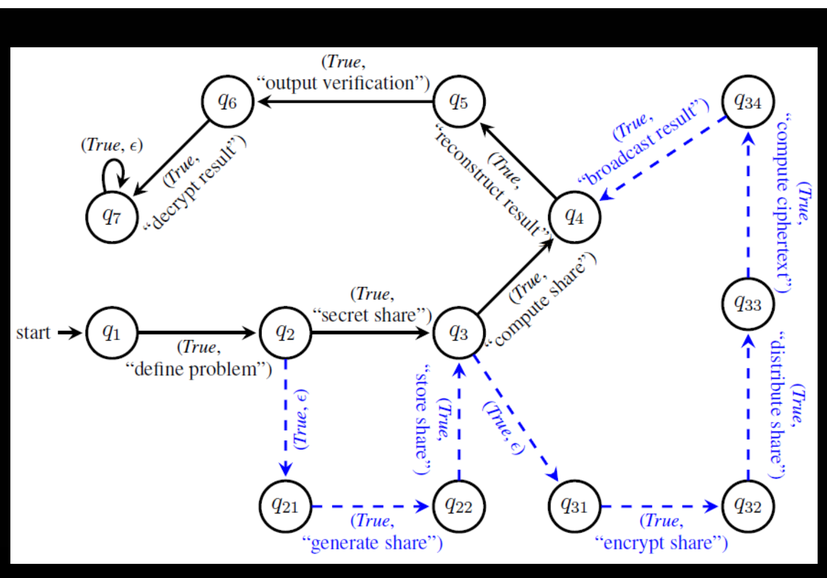
- Investigate the suitability of recently developed techniques in the intersection of pre-trained generative models and formal methods for synthesizing verifiable strategies for sequential decision-making.
- Demonstrate the utility in examples of protocols for preserving security and/or privacy.
- Refinement (automated or human-in-the-loop) guided by the outcome of verification

Secure multi-party computation

```
Steps for: secure multi-party computation
[1] Define problem and inputs.
[2] Secret sharing of inputs.
[3] Compute secret shares.
[4] Reconstruct the final result.
[5] Output verification.
[6] Decrypt the final result.

Substeps for: [2] Secret sharing of inputs.
[2.1] Generate random secret shares.
[2.2] Securely store secret shares.

Substeps for: [3] Compute secret shares.
[3.1] Encrypt secret share.
[3.2] Distribute encrypted shares.
[3.3] Compute ciphertext.
[3.4] Broadcast result.
```

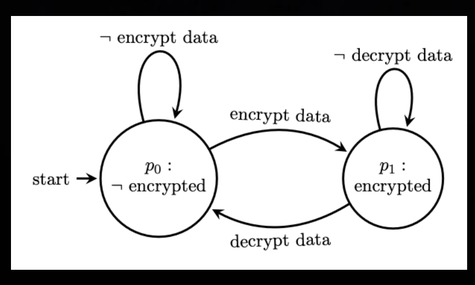


Connecting to a virtual private network

```
Steps for: Connecting to a virtual private network
[1] Establishing a connection.
[2] Encrypting data.
[3] Routing through the VPN server.
[4] Receiving data back.
```

after the initial query

$$\phi = \square(\text{ encrypted } \rightarrow \Diamond \text{ decrypt data }).$$



Verification: The initial automaton does not act “decrypt data” when the data is encrypted.

```
Refine the following steps to ensure "eventually decrypt data":
[1] Establishing a connection.
[2] Encrypting data.
[3] Routing through the VPN server.
[4] Receiving data back.

[1] Establishing a connection.
[2] Encrypting data.
[3] Routing through the VPN server.
[4] Receiving and decrypting data.
```

Final automaton after several refinement steps.