

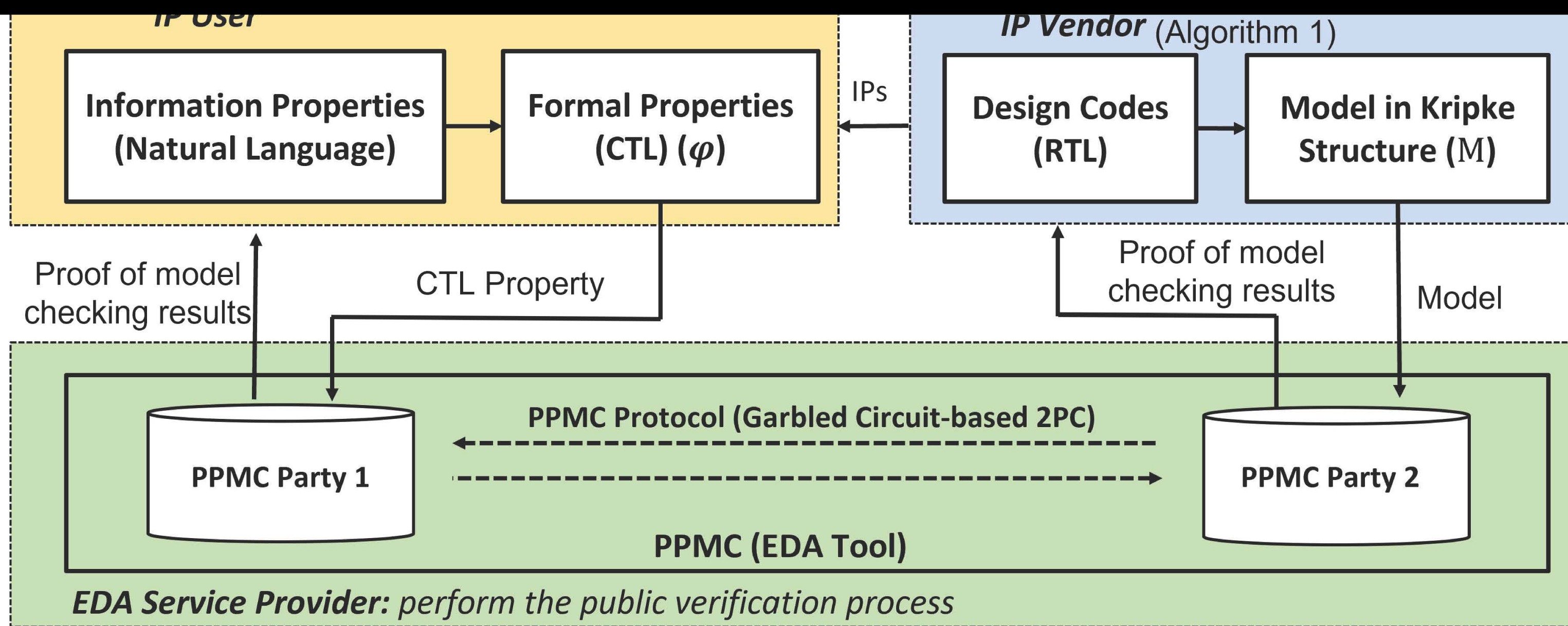


Figure 1. Zero trust verification framework for IP user, IP vendor, and EDA service provider.

Privacy Preserving Model Checking

1. Garbled circuit-based two-party secure computation with oblivious transfer-based secret exchange.
2. IP vendor (garbler) privately inputs transition and label matrices of $\mathcal{M}$.
3. IP user (evaluator) privately inputs φ and publicly declares $m = |\varphi|$.
4. Parties interactively execute m rounds of protocol to perform CTL model checking.
5. Output bit is disclosed to IP vendor (and optionally IP user and coordinating EDA SP).

$$\text{PPMC}(\mathcal{M}, \varphi) = b \in \{0, 1\} \text{ s.t. } b = 1 \iff \mathcal{M} \models \varphi.$$

References

- [1] S. Judson, N. Luo, T. Antonopoulos, and R. Piskac, "Privacy Preserving CTL Model Checking through Oblivious Graph Algorithms," in Proceedings of the 19th Workshop on Privacy in the Electronic Society (WPES@CCS), 2020.

b02	45	8	18.01 s	<code>assert property (U==1 -> stato==B);</code>
b01	63	10	44.01 s	<code>assert property (OVERFLW==1 -> ##2 (OVERFLW==0));</code>
RS232-T600	75	5	2.84 s	<code>cover property (ena);</code>
prep3	83	8	276.82 s	<code>assert property (next_out == 8'h20 -> ##1 (next_out == 8'h11 next_out = 8'h30));</code>
crc_ip	156	5	2.91 s	<code>cover property (write);</code>
apb_slave	240	3	1.20 s	<code>cover property (write_en);</code>
uart	495	7	9.48 s	<code>cover property (!received -> ##[0:\$]received);</code>
uart	495	7	23.35 s	<code>assert property (error -> ##1 reset);</code>
xtea	4638	15	18.81 s	<code>cover property (label);</code>

Table 1. Evaluation results of our zero trust verification framework.

Conclusion

- Propose zero trust framework for 3PIP/COTS IP verification, that addresses the limitations of the IEEE 1735 standard's threat model.
- Apply the Privacy-Preserving Model Checking (PPMC) tool of Judson *et al.* [1] in our framework to protect IP designs and assertion.
- Convert RTL IP (soft IP) designs into Kripke structures, as an input to PPMC.
- Validate our proposed framework by evaluating our tool on various open-source IP cores and security properties.

Acknowledge

This work was supported by the National Science Foundation(CCF-2019310) and the Office of Naval Research of the United States Department of Defense through an NDSEG Fellowship.

