B36B9F576B79F4A1	**Title**	**Conspectus 12022 Q4**
F9BBB15D357DAD56	**Subtitle**	**Chronical - IV**
1E1C8CDC0245CCB7	**Author**	**Recursion Ninja**
E37E0439E53122FA	**Date**	**12022+355 Wednesday, December 21**
C61E2BEBB09AF5EC	**Word Count**	**718 (ERT 3 min)**
CF9E678A82CCD86C	**Code Lines**	**0**
37D8F7A92947599D		
518A0B0BE44E849D	**Formats**	**.adoc .epub .html .markdown .txt**

Quarter 4: Autumnal Equinox to Winter Solstice

Doctoral Program

The unequivocally predominant accomplishment this quarter was finishing my first semester at The Graduate School and University Center of the City University of New York (GC - CUNY). Completing the *four* courses comprising 13 credits which I was enrolled in this semester was quite time consuming. However, the end of term projects and papers yielded some new avenues of research. I have begun reflecting with Professor Sergei Artemov on the foundational mathematics problem of proving an axiomatic system's consistency within the system. Additionally, I have started work with my doctoral advisor, Professor Subash Shankar, along with Professor Jun LI in applying program synthesis in deriving bit-manipulation techniques to remove control flow by utilizing abstractions from coding theory. I am excited to learn where these avenues of inquiry lead over the coming months.

TreeKEM Formal Verification

After the completion of my master's thesis on formal verification of TreeKEM via explicit model checking, I have continued refining the model encoding and performance tuning the verification strategy. The results of this endeavor have been manifold.

- The model's state vector length has been (roughly) reduced from 200 to 60 bytes.
- The utilization of bit-manipulation techniques to remove control flow within the model encoding reduced the state-space by one order of magnitude and, unsurprisingly, noticeably shortened the verification time.
- An abstraction was applied which allowed removing the T parameter from the model, permitting verification of LTL properties for any number of communica-

tion epochs, rather that only verify for a number of communication epochs up to the fixed bound T.
Overall space requirements have been reduced by multiple orders of magnitude.
Overall time of verification has been reduced by multiple orders of magnitude.

I am in the process of completing a manuscript for publication in 2023 detailing the techniques utilized to make verification tractable. The manuscript will include the results of verifying TreeKEM and the relationship of the results to prior work. For those individuals using secure group messaging platforms which utilize the TreeKEM protocol, the take away the impending manuscript is that *forward secrecy* and *post-compromise security* are security guarantees we can continue to enjoy for the foreseeable future.