Plano de Trabalho de Conclusão de Curso
Uma formalização da tradução da lógica intuicionista para a lógica modal S4

Elian Gustavo Chorny Babireski – elian.babireski@gmail.com
Karina Girardi Roggia – karina.roggia@udesc.br (*orientadora*)
Paulo Henrique Torrens – paulotorrens@gnu.org (*coorientador*)

Turma 2024/2 – Joinville/SC

23 de agosto de 2024

Resumo

As lógicas modais consistem em um conjunto de extensões da lógica clássica que contam com a adição de um ou mais operadores, chamados modalidades, que qualificam sentenças. Uma lógica modal com particular interesse à computação é o sistema **S4**, uma vez que a metalinguagem de Moggi que modela noções de computação em linguagens de programação por meio de mônadas pode ser traduzida a esse sistema. Ademais, existem correspondências entre a tradução da lógica intuicionista ao sistema modal **S4** com traduções *continuation-passing style* (CPS) usadas em compiladores. Este trabalho busca formalizar a derivação das sentenças $\mathbf{T}_\Diamond$ e $\mathbf{4}_\Diamond$ no sistema **S4** – uma vez que estas correspondem às tranformações naturais monádicas –, bem como formalizar duas traduções da lógica intuicionista para o sistema **S4** da lógica modal e demonstrar a equivalência entre elas. Todas as fomalizações serão feitas no assistente de provas Coq.

Palavras-chave: Coq, lógica intuicionista, lógica modal, S4, tradução de lógicas.

1 Introdução e justificativa

As lógicas modais consistem em um conjunto de extensões da lógica clássica que contam com a adição de um ou mais operadores, chamados modalidades, que qualificam sentenças. No caso do sistema **S4**, são adicionados as modalidades de necessidade ($\Box$) e possibilidade ($\Diamond$) em conjunto a regra da necessitação[1] e os axiomas **K**: $\Box(A \to B) \to \Box A \to \Box B$, **T**: $\Box A \to A$ e **4**: $\Box A \to \Box\Box A$ [Troelstra and Schwichtenberg 2000]. Ademais, pode-se derivar nesse sistema, por meio da dualidade entre as modalidades[2], sentenças duais aos axiomas **T** e **4**, sendo elas $\mathbf{T}_\Diamond$: $A \to \Diamond A$ e $\mathbf{4}_\Diamond$: $\Diamond\Diamond A \to \Diamond A$, respectivamente [Zach 2019].

As mônadas ganharam destaque na área de linguagens de programação desde que [Moggi 1991] formalizou uma metalinguagem que faz uso dessas estruturas para modelar noções de computação –

[1] $\dfrac{A}{\Box A}$

[2] $\Box A \equiv \neg\Diamond\neg A$

como parcialidade, não-determinismo, exceções e continuações – de uma maneira puramente funcional. Pode-se notar uma grande semelhança entre as sentenças $\mathbf{T}_\Diamond$ e $\mathbf{4}_\Diamond$ e as transformações naturais monádicas $\boldsymbol{\eta}$: $1_C \to T$ e $\boldsymbol{\mu}$: $T^2 \to T$, respectivamente. Nesse sentido, [Pfenning and Davies 2001] demonstraram que se pode traduzir essa metalinguagem para o sistema **S4** da lógica modal, pelo qual se torna interessante analisar esse sistema como uma linguagem de programação sob a ótica do isomorfismo de Curry-Howard.

[Troelstra and Schwichtenberg 2000] apresentam duas traduções equivalentes da lógica intuicionista para o sistema **S4** da lógica modal, sendo um deles correspondente a uma abordagem *call-by-name* e outra a um abordagem *call-by-value*. Tais traduções possuem grande similaridade com as traduções da lógica intuicionista para a lógica linear definidas por [Girard 1987]. Essas traduções equivalem à tradução por negação dupla que, por sua vez, equivalem à traduções de *continuation-passing style* (CPS) em compiladores por meio do isomorfismo de Curry-Howard [Reynolds 1993], o que torna esse tema interessante no ponto de vista de compilação.

Durante grande parte da história, provas lógicas e matemáticas eram validadas manualmente pela comunidade acadêmica, o que muitas vezes – a depender do tamanho e complexidade da prova – se mostrava ser um trabalho complexo e sujeito a erros.

Este trabalho será uma continuação do desenvolvimento da biblioteca de lógica modal no assistente de provas Coq feito em [Silveira 2020] e posteriormente expandido de forma a permitir a fusão de lógicas modais em [Nunes 2023]. Uma formalização similar de traduções de lógicas foi feito em [Sehnem 2023], porém, neste caso, das lógicas clássica e intuicionista para a lógica linear.

2 Objetivos

Objetivo geral: Formalização no assistente de provas Coq das traduções da lógica intuicionista para o sistema **S4** da lógica modal apresentados em [Troelstra and Schwichtenberg 2000], bem como provar a derivabilidade das sentenças $\mathbf{T}_\Diamond$ e $\mathbf{4}_\Diamond$ no sistema.

Objetivos específicos:

- Fornecer uma introdução à criptografia e seus tipos;
- Apresentar os conceitos de reticulados e suas aplicações na criptografia;
- Especificar e compreender os problemas SVP e CVP envolvendo reticulados;
- Apresentar o esquema LWE e suas variações;
- Apresentar o algoritmo Kyber e seu funcionamento;
- Apresentar o método NTT para otimização de multiplicação entre polinômios; e
- Efetuar uma implementação simples do algoritmo Kyber.

3 Metodologia

Este trabalho será dividido em duas partes, a primeira com a fundamentação teórica dos assuntos indicados e escrita de texto acessível a estudantes de graduação para consulta e estudos introdutórios à criptografia pós-quântica. Na segunda parte será realizada a implementação dos algoritmos e estudo de caso.

4 Cronograma proposto

Para a realização dos objetivos citados acima, o trabalho foi dividido nas seguintes etapas:

1. Pesquisa bibliográfica sobre criptografia;
2. Pesquisa bibliográfica sobre reticulados;
3. Pesquisa bibliografica sobre aplicações de reticulados na criptografia;
4. Estudo sobre os problemas SVP e CVP;
5. Estudo sobre o esquema LWE e derivados;
6. Estudo sobre o método NTT para multiplicação de polinômios;
7. Implementação do algoritmo Kyber; e
8. Estudo comparativo entre os algoritmos pós-quânticos e os atualmente utilizados.

Atividades	Meses									
	Fevereiro		Março		Abril		Maio		Junho	
1			■							
2				■	■					
3				■	■					
4						■	■	■		
5						■	■	■		
6									■	■

	Julho		Agosto		Setembro		Outubro		Novembro	
7	■	■	■	■	■	■	■	■	■	
8								■	■	■

5 Linha e grupo de pesquisa

O trabalho faz parte das atividades do Grupo de Pesquisa em fundamentos da Computação (FUNÇÃO).

6 Forma de acompanhamento/orientação

O acompanhamento das atividades desenvolvidas será realizada em reuniões semanais, presenciais ou via *chat*, com até uma hora de duração. Também serão utilizados correio eletrônico e outros recursos para, caso necessário, orientação ao longo da semana. A adição de novos encontros pode vir a ser necessária de acordo com o desenvolvimento do trabalho. Os artefatos produzidos pelo orientado serão disponibilizados à orientadora em ambientes de acesso mútuo para acompanhamento contínuo.

Referências

[Girard 1987] Girard, J.-Y. (1987). Linear logic. *Theoretical Computer Science*, 50.

[Moggi 1991] Moggi, E. (1991). Notions of computation and monads. *Information and Computation*, 93.

[Nunes 2023] Nunes, M. A. (2023). Fusão de lógicas modais no assistentes de provas Coq. Dissertação (Bacharelado), Universidade do Estado de Santa Catarina.

[Pfenning and Davies 2001] Pfenning, F. and Davies, R. (2001). A judgmental reconstruction of modal logic. *Mathematical Structures in Computer Science*, 11.

[Reynolds 1993] Reynolds, J. C. (1993). The discoveries of continuations. *LISP and Symbolic Computation*.

[Sehnem 2023] Sehnem, A. J. (2023). Formalização da tradução das lógicas clássicas e intuicionista para a lógica linear em Coq. Dissertação (Bacharelado), Universidade do Estado de Santa Catarina.

[Silveira 2020] Silveira, A. A. d. (2020). Implementação de uma biblioteca de lógica modal em Coq. Dissertação (Bacharelado), Universidade do Estado de Santa Catarina.

[Troelstra and Schwichtenberg 2000] Troelstra, A. S. and Schwichtenberg, H. (2000). *Basic Proof Theory*. Cambridge Tracts in Theoretical Computer Science 43. Cambridge University Press, 2nd edition.

[Zach 2019] Zach, R. (2019). Boxes and diamonds: an open introduction to modal logic.

Karina Girardi Roggia	***Elian Gustavo Chorny Babireski***
Orientadora	**Discente**