UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CÂMPUS TOLEDO
COTSI - CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET

JOÃO PEDRO RODRIGUES LEITE

SEGURANÇA EM COMUNICAÇÕES PÓS-QUÂNTICAS

PROPOSTA DE TRABALHO DE CONCLUSÃO DE CURSO

TOLEDO
2024

JOÃO PEDRO RODRIGUES LEITE

SEGURANÇA EM COMUNICAÇÕES PÓS-QUÂNTICAS

Proposta de Trabalho de Conclusão de Curso de graduação, apresentado à disciplina de Trabalho de Conclusão de Curso 1, do COTSI - Curso de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná - UTFPR - Câmpus Toledo, como requisito parcial para a obtenção do título de Tecnólogo em Sistemas para Internet.

Orientador: prof. Dr. Fábio Engel de Camargo

TOLEDO
2024

1 PROPOSTA DE TRABALHO DE CONCLUSÃO DE CURSO

1.1 TÍTULO

O título desta proposta de conclusão de curso (TCC) é "Segurança em comunicações pós-quânticas".

1.2 MODALIDADE DO TRABALHO

A presente proposta de TCC enquadra-se na categoria de trabalho científico aplicado.

1.3 ÁREA DO TRABALHO

Esta proposta de TCC está inserida na área de segurança da informação, especificamente na criptografia pós-quântica. Esta é uma subárea emergente que aborda a criação e implementação de métodos de criptografia que possam resistir aos ataques de computadores quânticos, os quais têm potencial para quebrar os esquemas criptográficos convencionais atualmente em uso. À medida que a computação quântica evolui e se aproxima de uma aplicação prática, o desenvolvimento de estratégias de criptografia que possam garantir a segurança das comunicações digitais contra tais ameaças torna-se crucial.

1.4 RESUMO

Esta proposta de trabalho de conclusão de curso(TCC) aborda a crescente preocupação na área da segurança da informação em relação à possível ameaça representada pelos computadores quânticos à criptografia convencional. Com o avanço da pesquisa e desenvolvimento de tecnologia quântica, torna-se evidente que algoritmos de criptografia atualmente considerados seguros podem ser quebrados de forma eficiente por esses dispositivos revolucionários. Diante desse cenário, surge a necessidade de identificar e apresentar novas técnicas criptográficas resistentes aos ataques quânticos. Há a necessidade de garantir a segurança das comunicações digitais em um futuro onde os computadores quânticos podem comprometer a eficácia dos algoritmos convencionais. Além disso, é discutido o desafio do "Store Now, Decrypt Later"(SNDL), no qual os dados são armazenados aguardando um momento futuro para serem decifrados. Pesquisas sobre trabalhos relacionados serão realizados de modo a identificar e apresentar os algoritmos relevantes e seus fundamentos. Espera-se que com esse trabalho haja uma conscientização da ameaça e dos problemas enfrentados na segurança da informação com a iminente chegada dos computadores quânticos.

2 DESCRIÇÃO DA PROPOSTA

2.1 INTRODUÇÃO

Nos últimos anos, avanços consideráveis na pesquisa e desenvolvimento de tecnologia quântica têm levantado questões sobre a segurança dos sistemas de criptografia convencional. O poder de processamento das informações dos computadores quânticos, por realizarem operações em paralelo, representa uma ameaça significativa à criptografia convencional utilizada atualmente para proteger dados sensíveis em comunicações digitais.

Diante desse cenário, surge o problema central abordado neste trabalho: a necessidade urgente de garantir a segurança das comunicações digitais devido a potencial capacidade dos computadores quânticos de quebrar algoritmos de criptografia convencionais de forma eficiente. Além disso, é crucial abordar também o desafio do "Store Now, Decrypt Later"(SNDL), onde os dados são armazenados aguardando um momento futuro para serem decifrados, em um contexto onde a chegada dos computadores quânticos torna a segurança convencional vulnerável.

A segurança das comunicações digitais é essencial para a proteção da privacidade, integridade e autenticidade das informações. Diante da iminente chegada dos computadores quânticos, a busca por soluções criptográficas pós-quânticas torna-se uma necessidade urgente, visando garantir a segurança dos dados em um ambiente de ameaças em constante evolução.

O principal desafio deste projeto consiste na identificação e apresentação das novas técnicas criptográficas capazes de resistir aos potenciais ataques quânticos, e na compreensão dos fundamentos teóricos subjacentes a essas técnicas. A complexidade dos algoritmos de criptografia pós-quântica apresenta um desafio significativo, exigindo um entendimento profundo de conceitos matemáticos e computacionais.

Este trabalho pretende contribuir para uma maior compreensão dos desafios e soluções na área da segurança da informação em um contexto pós-quântico. Ao identificar e apresentar os algoritmos de criptografia pós-quântica existentes, espera-se fornecer uma conscientização em relação à importância da proteção das comunicações digitais em um ambiente de ameaças em constante evolução.

2.2 OBJETIVOS

A seguir são apresentados os objetivos geral e específicos que regem esta proposta.

2.2.1 Objetivo Geral

O objetivo geral deste trabalho de TCC é estudar as soluções de criptografia pós-quântica disponíveis para assegurar a segurança das comunicações digitais frente aos desafios impostos pela computação quântica. Este estudo visa o entendimento das tecnologias criptográ-

ficas que são projetadas para serem resilientes contra os métodos de quebra que computadores quânticos podem oferecer, uma vez que se tornem operacionais. Para tanto, o trabalho focará na revisão e apresentação dos algoritmos de criptografia pós-quântica mais relevantes e nos princípios que garantem sua eficiência. O trabalho pretende abordar algoritmos já estabelecidos e também, possivelmente, aqueles ainda em desenvolvimento, proporcionando uma visão ampla do estado atual da criptografia pós-quântica e suas potenciais aplicações práticas para proteger informações críticas em um futuro próximo.

2.2.2 Objetivos Específicos

Os objetivos específicos desta proposta de TCC incluem:

- Identificar e catalogar os principais algoritmos de criptografia pós-quântica que estão atualmente em uso ou em fase de desenvolvimento, descrevendo suas bases teóricas, características e contextos de aplicação.
- Identificar as principais técnicas empregadas pelos algoritmos de criptografia pós-quântica.
- Comparar os algoritmos de criptografia pós-quântica entre si em termos de complexidade computacional, robustez e praticabilidade, utilizando critérios de avaliação para determinar suas vantagens e limitações.
- Apresentar os impactos práticos da implementação de criptografia pós-quântica em sistemas de informação existentes, considerando aspectos como custos, interoperabilidade e necessidades de adaptação tecnológica.
- Elaborar recomendações para desenvolvedores web, tendo em visto as deficiências nos atuais algoritmos de criptografia, frente a potenciais aplicações práticas de computadores quânticos.

2.3 JUSTIFICATIVA

Consiste na apresentação, de forma clara, objetiva e rica em detalhes, das razões de ordem teórica ou prática que justificam a realização do trabalho proposto. A justificativa deve indicar:

- A relevância do problema a ser investigado.

- As contribuições que o trabalho pode trazer, no sentido de proporcionar respostas aos problemas propostos.

- O estágio de desenvolvimento dos conhecimentos referentes ao tema.

- A possibilidade de sugerir modificações no âmbito da realidade proposta pelo tema.

(substitua este texto pela justificativa do trabalho)

2.4 REFERÊNCIAL TEÓRICO

Uma vez formulado o problema a ser atacado, é preciso se inteirar do que já foi feito, dito e discutido sobre ele. Isso se chama "estado da arte". Pode ser que a dúvida, que está

motivando a pesquisa, já tenha sido respondida de alguma maneira por alguém. Por isso, é preciso aprofundar o conhecimento sobre a questão, antes de dar prosseguimento ao projeto.

Essa etapa também recebe o nome de revisão bibliográfica, quando são estudados os trabalhos que se situam na circunvizinhança do problema, trabalhos que versam sobre problemas similares.

Vê-se aí por que a revisão bibliográfica é importante. De um lado, ela deve comprovar que o pesquisador não está querendo realizar algo que já foi feito, de outro lado, ela ajuda a encaminhar o passo seguinte da pesquisa, a justificativa, quer dizer, a argumentação sobre a relevância do trabalho.

Para a proposta de TCC deve ser descrito, de maneira breve, alguns (sugestão de 2 (dois) a 3 (três)) trabalhos correlatos, converse com seu orientador para citar os mais relevantes do tema abordado. Pode ser seguido a seguinte sugestão de parágrafos/tópicos:

P1. Descrição do trabalho 1

P2. Descrição do trabalho 2

P3. Descrição do trabalho 3

P4. Discussão dos trabalhos mencionados destacando porque eles são importantes para o trabalho proposto.

Para utilização de citações atente ao tipo de citação que se deseja usar. As citações são classificadas em indeireta e direta, podem ser longas ou curtas.

Uma citação indireta é a transcrição, com suas próprias palavras, das idéias de um autor, mantendo-se o sentido original. A citação indireta é a maneira que o pesquisador tem de ler, compreender e gerar conhecimento a partir do conhecimento de outros autores. Quanto à chamada da referência, ela pode ser feita de duas maneiras distintas, conforme o nome do(s) autor(es) façam parte do seu texto ou não. Exemplo de chamada fazendo parte do texto:

Enquanto Maturana e Varela (2003) defendem uma epistemologia baseada na biologia. Para os autores, é necessário rever ....

A chamada de referência foi feita com o comando `\citeonline{chave}`, que produzirá a formatação correta.

A segunda forma de fazer uma chamada de referência deve ser utilizada quando se quer evitar uma interrupção na sequência do texto, o que poderia, eventualmente, prejudicar a leitura. Assim, a citação é feita e imediatamente após a obra referenciada deve ser colocada entre parênteses. Porém, neste caso específico, o nome do autor deve vir em caixa alta, seguido do ano da publicação. Exemplo de chamada não fazendo parte do texto:

Há defensores da epistemologia baseada na biologia que argumentam em favor da necessidade de ... (MATURANA; VARELA, 2003).

Nesse caso a chamada de referência deve ser feita com o comando `\cite{chave}`, que produzirá a formatação correta.

Uma citação direta é a transcrição ou cópia de um parágrafo, de uma frase, de parte dela ou de uma expressão, usando exatamente as mesmas palavras adotadas pelo autor do trabalho consultado.

Quanto à chamada da referência, ela pode ser feita de qualquer das duas maneiras, assim como nas nas citações indiretas, conforme o nome do(s) autor(es) façam parte do texto ou não. Há duas maneiras distintas de se fazer uma citação direta, conforme o trecho citado seja longo ou curto.

Quando o trecho citado é longo (4 ou mais linhas) deve-se usar um parágrafo específico para a citação, na forma de um texto recuado (4 cm da margem esquerda), com tamanho de letra menor e espaçamento entrelinhas simples. Exemplo de citação longa:

> Desse modo, opera-se uma ruptura decisiva entre a reflexividade filosófica, isto é a possibilidade do sujeito de pensar e de refletir, e a objetividade científica. Encontramo-nos num ponto em que o conhecimento científico está sem consciência. Sem consciência moral, sem consciência reflexiva e também subjetiva. Cada vez mais o desenvolvimento extraordinário do conhecimento científico vai tornar menos praticável a própria possibilidade de reflexão do sujeito sobre a sua pesquisa (SILVA; SOUZA, 2000, p. 28).

Para fazer a citação longa deve-se utilizar os seguintes comandos:

```
\begin{citacao}
<texto da citacao>
\end{citacao}
```

No exemplo acima, para a chamada da referência o comando `\cite[p.~28]{Silva2000}` foi utilizado, visto que os nomes dos autores não são parte do trecho citado. É necessário também indicar o número da página da obra citada que contém o trecho citado.

Quando o trecho citado é curto (3 ou menos linhas) ele deve inserido diretamente no texto entre aspas. Exemplos de citação curta:

A epistemologia baseada na biologia parte do princípio de que "assumo que não posso fazer referência a entidades independentes de mim para construir meu explicar"(MATURANA; VARELA, 2003, p. 35).

A epistemologia baseada na biologia de Maturana e Varela (2003, p. 35) parte do princípio de que "assumo que não posso fazer referência a entidades independentes de mim para construir meu explicar".

Outros exemplos de comandos para as chamadas de referências e o resultado produzido por estes são:

Maturana e Varela (2003) `\citeonline{Maturana2003}`
Barbosa et al. (2004) `\citeonline{Barbosa2004}`
(SILVA; SOUZA, 2000, p. 28) `\cite[p.~28]{Silva2000}`
Silva e Souza (2000, p. 33) `\citeonline[p.~33]{v}`
(MATURANA; VARELA, 2003, p. 35) `\cite[p.~35]{Maturana2003}`
Maturana e Varela (2003, p. 35) `\citeonline[p.~35]{Maturana2003}`
(BARBOSA et al., 2004; MATURANA; VARELA, 2003) `\cite{Barbosa2004,Maturana2003}`

Em relação as referências, a bibliografia é feita no padrão BibTEX. As referências são colocadas em um arquivo separado. Neste template as referências são armazenadas no arquivo "base-referencias.bib".

Existem diversas categorias documentos e materiais componentes da bibliografia. A classe abnTEX define as seguintes categorias (entradas):

```
@book
@inbook
@article
@phdthesis
@mastersthesis
@monography
@techreport
@manual
@proceedings
@inproceedings
@journalpart
@booklet
@patent
@unpublished
@misc
```

Cada categoria (entrada) é formatada pelo pacote abnTeX2 e Araujo (2014b) de uma forma específica. Para maiores detalhes, refira-se a abnTeX2 e Araujo (2014b), abnTeX2 e Araujo (2014a), Araujo e abnTeX2 (2014).

2.4.1 DIFERENCIAL TECNOLÓGICO

O diferencial teórico é uma complementação do tópico discussão da seção estado da arte, onde será evidenciado qual o diferencial do trabalho perante os demais correlatos já existentes. Deve-se destacar os seguintes itens:

Diferencial do trabalho proposto perante produtos concorrentes ou semelhantes;

Vantagens que os possíveis usuários terão ao usar o trabalho a ser desenvolvido;
Destacar inovação tecnológica, por exemplo, uso de novas tecnologias e vantagens;
(substitua este texto pelo diferencial tecnológico do trabalho)

2.5 MATERIAIS E MÉTODOS

Na seção de procedimentos metodológicos ou metodologia (ver qual o nome mais adequado ao trabalho) deve ser descrito sucintamente o procedimentos metodológicos para a execução do projeto ressaltando como os objetivos serão alcançados.

Em geral, a seção descreve os procedimentos usados para resolver o problema atacado. Pode ser estruturada em tópicos, onde cada tópico representa um subproduto do objetivo geral.

No caso de desenvolvimento de sistemas deve-se descrever a metodologia a ser utilizada, por exemplo Scrum, eXtreme Programming, RUP, etc.

Também pode ser descritos técnicas de desenvolvimento de software como por exemplo TDD, BDD, SPA, etc.

Coloque todos os materiais que serão utilizados. Exemplos: computadores, equipamentos de redes, licenças de software, etc. Também deverá ser colocado se os recursos estarão disponíveis. A universidade não comprará os recursos, portanto a responsabilidade de comprar algo será do aluno.

(substitua este texto pelo de recursos necessários do trabalho)

(substitua este texto pelo de procedimentos metodológicos/metodologia do trabalho)

Materiais Necessários: computador, equipamentos com capacidade de processamento adequada para a análise de dados e simulação de algoritmos, se necessário. Softwares específicos para simulação criptográfica, se aplicável.

Método: Revisão Bibliográfica: revisão de literatura para identificar e catalogar os algoritmos de criptografia pós-quântica disponíveis. Fontes incluirão artigos acadêmicos, teses, relatórios de conferências e publicações de padrões internacionais. Bancos de dados como IEEE Xplore, SpringerLink, Scopus, e Google Scholar serão utilizados para esta pesquisa.

2.6 RESULTADOS ESPERADOS

Descrever quais os resultados esperados com a execução do trabalho.

2.7 CRONOGRAMA

O planejamento do trabalho que será desenvolvido pelo aluno, ao longo do período letivo, está descrito no cronograma da Quadro 1. Neste cronograma constam todas as atividades com seus respectivos prazos para o cumprimento.

Quadro 1 – Cronograma de Atividades.

Atividades	**Mar**	**Abr**	**Mai**	**Jun**	**Jul**	**Ago**	**Set**	**Out**	**Nov**	**Dez**
1. Revisão dos apontamentos da banca										
2. Revisão bibliográfica										
3. Redação do projeto de TCC			X	X						
4. Defesa do projeto de TCC					X					
5. Escrita da Monografia de TCC						X	X	X		
6. Elaboração da apresentação final								X	X	
7. Defesa final do TCC									X	

2.8 CONCLUSÃO/CONSIDERAÇÕES FINAIS

Na seção de Conclusão ou Considerações Finais (ver qual o nome mais adequado ao trabalho) o acadêmico deve descrever:

Como espera alcançar os objetivos propostos;

Destacar as dificuldades encontradas e previstas;

Fazer o fechamento do trabalho destacando sua importância.

(substitua este texto pelo de estado da arte do trabalho)

Referências

ABNTEX2; ARAUJO, L. C. **A classe abntex2**: Documentos técnicos e científicos brasileiros compatíveis com as normas abnt. [S.l.], 2014. 46 p. Disponível em: <http://abntex2.googlecode.com/>. Acesso em: 12 de setembro de 2014. Citado na página 6.

ABNTEX2; ARAUJO, L. C. **O pacote abntex2cite**: Estilos bibliográficos compatíveis com a abnt nbr 6023. [S.l.], 2014. 91 p. Disponível em: <http://abntex2.googlecode.com/>. Acesso em: 12 de setembro de 2014. Citado na página 6.

ARAUJO, L. C.; ABNTEX2. **O pacote abntex2cite**: Tópicos específicos da abnt nbr 10520:2002 e o estilo bibliográfico alfabético (sistema autor-data). [S.l.], 2014. 23 p. Disponível em: <http://abntex2.googlecode.com/>. Acesso em: 12 de setembro de 2014. Citado na página 6.

BARBOSA, C. et al. **Testando a utilização de "et al."**. 2. ed. Cidade: Editora, 2004. Citado na página 6.

MATURANA, H. R.; VARELA, F. J. **A Árvore do Conhecimento**: as bases biológicas da compreensão humana. 3. ed. São Paulo: Editora Palas Athena, 2003. Citado 3 vezes nas páginas 4, 5 e 6.

SILVA, J.; SOUZA, J. a. L. **A Inteligência da Complexidade**. São Paulo: Editora Petrópolis, 2000. Citado 2 vezes nas páginas 5 e 6.