UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Gustavo Zambonin

ESQUEMAS DE ASSINATURA DIGITAL BASEADOS EM FUNÇÕES DE RESUMO CRIPTOGRÁFICAS

Florianópolis

2017

Gustavo Zambonin

ESQUEMAS DE ASSINATURA DIGITAL BASEADOS EM FUNÇÕES DE RESUMO CRIPTOGRÁFICAS

Monografia submetida ao Programa de Graduação em Ciência da Computação para a obtenção do Grau de Bacharel em Ciência da Computação.
Orientador: Prof. Dr. Ricardo Felipe Custódio
Coorientador: Prof. Dr. Daniel Panario

Florianópolis

2017

FOLHA DE APROVAÇÃO DE PROPOSTA DE TCC

Acadêmico(s)	Gustavo Zambonin
Título do trabalho	Esquemas de assinatura digital baseados em funções de resumo criptográficas
Curso	Ciência da Computação/INE/UFSC
Área de Concentração	Matemática da Computação

Instruções para preenchimento pelo ORIENTADOR DO TRABALHO:

- Para cada critério avaliado, assinale um X na coluna SIM apenas se considerado aprovado. Caso contrário, indique as alterações necessárias na coluna Observação.

Critérios	Aprovado				Observação
	Sim	Parcial	Não	Não se aplica	
1. O trabalho é adequado para um TCC no CCO/SIN (relevância / abrangência)?					
2. O título do trabalho é adequado?					
3. O tema de pesquisa está claramente descrito?					
4. O problema/hipóteses de pesquisa do trabalho está claramente identificado?					
5. A relevância da pesquisa é justificada?					
6. Os objetivos descrevem completa e claramente o que se pretende alcançar neste trabalho?					
7. É definido o método a ser adotado no trabalho? O método condiz com os objetivos e é adequado para um TCC?					
8. Foi definido um cronograma coerente com o método definido (indicando todas as atividades) e com as datas das entregas (p.ex. Projeto I, II, Defesa)?					
9. Foram identificados custos relativos à execução deste trabalho (se houver)? Haverá financiamento para estes custos?					
10. Foram identificados todos os envolvidos neste trabalho?					
11. As formas de comunicação foram definidas (ex.: horários para orientação)?					
12. Riscos potenciais que podem causar desvios do plano foram identificados?					
13. Caso o TCC envolva a produção de um software ou outro tipo de produto e seja desenvolvido também como uma atividade realizada numa empresa ou laboratório, consta da proposta uma declaração (Anexo 3) de ciência e concordância com a entrega do código fonte e/ou documentação produzidos?					

Avaliação	☐ **Aprovado**		☐ **Não Aprovado**
Professor Responsável	Ricardo Felipe Custódio	12/06/2017	

RESUMO

Algoritmos utilizados em esquemas de assinatura digital atualmente, como RSA e ECDSA, têm sua segurança baseada em calcular a fatoração de números muito grandes ou logaritmos discretos. Este tipo de cômputo pode ser realizado por um computador quântico suficientemente poderoso, utilizando algoritmos já conhecidos (e.g. algoritmo de Shor). Deste modo, para manter o ecossistema de assinaturas digitais continuamente seguro, é necessário oferecer alternativas pós-quânticas, ou seja, resistentes a computadores quânticos. Este trabalho busca apresentar esquemas baseados apenas em funções de resumo criptográficas, cuja segurança baseia-se apenas na resistência à colisão da função escolhida, com o objetivo de mostrar que a construção de esquemas de assinatura seguros independe de problemas considerados difíceis em teoria de números ou álgebra, levando em conta apenas algoritmos quânticos, como o algoritmo de Grover. Ademais, apresentam-se soluções para alguns problemas deste tipo de esquema, como o tamanho e possibilidade de reutilização das chaves pública e privada, assim como uma variada gama de algoritmos com estas características, particularmente os baseados em árvores de Merkle e variantes do esquema Winternitz.

Palavras-chave: criptografia, Merkle, assinatura digital, pós-quântico

SUMÁRIO

1 INTRODUÇÃO

Funções de resumo criptográficas são essenciais em diversas aplicações de segurança da informação, como códigos de autenticação de mensagens (MACs), identificação de arquivos a partir de uma ''impressão digital'' única, detecção de perda de informações em uma transmissão volátil etc., e têm uso disseminado em esquemas de assinatura digital, os quais são o foco deste trabalho. Uma característica relevante destes é a possibilidade da demonstração matemática da autenticidade de uma mensagem transmitida entre entidades, sejam estas confiáveis ou não, utilizando as funções citadas anteriormente, para que seja estabelecida uma comunicação segura.

A maior parte dos esquemas de assinatura digital, na prática, utilizam criptossistemas de chave pública baseados em problemas de teoria de números – fatoração de inteiros, logaritmo discreto – que, atualmente, não podem ser computados em tempo polinomial (ou seja, seu tempo de execução é limitado por uma expressão polinomial relacionada com o tamanho da entrada do algoritmo). Entretanto, utilizando-se de um computador quântico, tais problemas podem ser resolvidos em tempo polinomial (SHOR, 1997).

A criptografia *pós-quântica* encarrega-se de buscar algoritmos criptográficos cuja complexidade independe de problemas futuramente solucionáveis em teoria de números. Como visto em (MERKLE, 1989), um criptossistema de chaves públicas pode ser definido de forma independente da função de resumo criptográfica utilizada, assim possibilitando a exploração de diversas combinações, cujos elementos essenciais (e.g. árvores de Merkle) não influenciam na segurança do esquema.

Neste trabalho, utilizamos funções de resumo criptográficas para a construção de esquemas de assinatura digital, considerados seguros se e somente as funções forem resistentes à colisão (a inviabilidade computacional de encontrar duas mensagens distintas que, submetidas à mesma função, retornam a mesma saída), tornando os requisitos de segurança mínimos para os esquemas.

1.1 OBJETIVOS

Objetivo geral. Apresentar um estudo detalhado sobre esquemas de assinatura digital baseados em funções de resumo criptográficas, partindo de esquemas de assinatura única (LAMPORT, 1979), observando o refinamento destes, até o estado da arte, onde não é necessário saber quantas assinaturas foram geradas anteriormente (BERNSTEIN et al., 2015), bem como imple-

mentações em linguagem de alto nível para a fácil compreensão destes esquemas.

Objetivos específicos. Descrever os esquemas de assinatura digital única Lamport-Diffie e Winternitz; descrever os esquemas de assinatura digital baseado em árvores de Merkle – *Merkle Signature Scheme*, *eXtended Merkle Signature Scheme*; implementar os esquemas supracitados; comparar o desempenho destes algoritmos entre si, utilizando funções de resumo criptográficas e parâmetros internos aos algoritmos distintos, onde aplicável.

Escopo do trabalho. Não se aplica ao conteúdo deste trabalho a análise profunda de provas de segurança definidas por um modelo adversarial teórico – ou seja, demonstrar que um atacante deve resolver um problema muito difícil para tornar o algoritmo inseguro, bem como algoritmos de criptografia pós-quânticos baseados em outras estruturas matemáticas (reticulados, teoria de códigos etc.) ou algoritmos clássicos (RSA, DSA, ECDSA etc.).

Critérios de aceitação. Estudo e implementação de pelo menos dois esquemas de assinatura digital única (Lamport-Diffie, Winternitz), a estrutura de dados chamada de árvore de Merkle e um esquema de assinatura digital composto da união destes elementos, como o XMSS (BUCHMANN; DAHMEN; HüLSING, 2011).

Entregas do projeto. Relatórios referentes às disciplinas de Trabalho de Conclusão de Curso do INE/UFSC, incluindo monografia completa ao final da disciplina de Trabalho de Conclusão de Curso II, bem como implementação documentada em linguagem de programação de alto nível dos esquemas descritos no trabalho.

Restrições e premissas. Espera-se reunir com os orientadores, de forma periódica, para a discussão dos resultados obtidos e a definição dos passos seguintes. As restrições consistem na finalização do projeto até o prazo de entrega final da disciplina de Trabalho de Conclusão de Curso II do INE/UFSC, utilização de software livre e de código aberto, normatização dos documentos referentes ao projeto de acordo com órgãos especializados (ABNT, BU/UFSC) e disponibilização de artigos e livros pagos e/ou gratuitos referentes aos esquemas abordados.

1.2 PROCEDIMENTOS METODOLÓGICOS

O trabalho será desenvolvido utilizando a infraestrutura e recursos do Laboratório de Segurança em Computação (LabSEC/UFSC), onde será estudada bibliografia referente aos temas abordados nesta pesquisa buscando encontrar as vantagens e desvantagens entre cada um dos esquemas de assinatura digital escolhidos, bem como observar seu desempenho e tamanho de elementos como par de chaves e assinatura, ao utilizar funções de resumo criptográficas distintas em implementações produzidas ou fornecidas.

2 CRONOGRAMA

Etapas	Meses – 2017					
	jul.	**ago.**	**set.**	**out.**	**nov.**	**dez.**
Fundamentação teórica						
Revisão do estado da arte						
Desenvolvimento do TCC						
Implementação						
Relatório de TCC I						

Etapas	Meses – 2018					
	jan.	**fev.**	**mar.**	**abr.**	**mai.**	**jun.**
Ajustes na implementação						
Redação da monografia						
Ajustes na monografia						
Relatório de TCC II						
Defesa pública						
Ajustes finais do TCC						

3 CUSTOS

Item	Quantidade	Valor unitário (R$)	Valor Total (R$)
Material permanente			
Computador	1	R$ 3.000,00	R$ 3.000,00
Internet	1	R$ 1.000,00	R$ 1.000,00
Artigos	10	R$ 90,00	R$ 900,00
Livros	2	R$ 200,00	R$ 400,00
Material de consumo			
Alimentação	264	R$ 10,00	R$ 2.640,00
CDs/DVDs	4	R$ 2,00	R$ 8,00
Outros recursos e serviços			
Impressões	200	R$ 1,00	R$ 200,00

4 RECURSOS HUMANOS

Nome	Função
Gustavo Zambonin	Autor
Ricardo F. Custódio	Orientador
Daniel Panario	Coorientador
Renato Cislaghi	Coordenador de projetos
A definir	Membro(s) da banca

5 COMUNICAÇÃO

O que precisa ser comunicado	Por quem	Para quem	Melhor forma de comunicação	Quando e com que frequência
Enviar plano de projeto	Autor	Orientador, coorientador, coordenador de projetos	Sistema de TCC	Única vez, até dia 12/06/2017
Entrega de relatório de TCC I	Autor	Orientador, coorientador, coordenador de projetos, membro(s) da banca	Sistema de TCC	Única vez, ao final do semestre 2017/2
Entrega de relatório de TCC II	Autor	Orientador, coorientador, coordenador de projetos, membros(s) da banca	Sistema de TCC	Única vez, em meados do semestre 2018/1
Defesa do TCC	Autor	Orientador, coorientador, coordenador de projetos, membro(s) da banca	Pessoalmente	Única vez, em meados do semestre 2018/1
Entrega final da monografia	Autor	Orientador, coorientador, coordenador de projetos, membro(s) da banca	Sistema de TCC	Única vez, após a defesa, antes do término de 2018/1
Reuniões de acompanhamento da pesquisa	Autor	Orientador, coorientador	Pessoalmente, webconferência	Quinzenalmente
Monitoramento do projeto	Autor	Orientador, coorientador	E-mail	Esporadicamente
Convite de membro(s) da banca	Autor	A definir	Sistema de TCC	Única vez, em meados do semestre 2017/2

6 RISCOS

Risco	Proba-bilidade	Impacto	Priori-dade	Estratégia de resposta	Ações de prevenção
Paralisação de transporte público	Média	Médio	Baixa	Transportar-se à Universidade utilizando meios alternativos	Combinar transporte alternativo
Paralisação de servidores públicos	Muito baixa	Alto	Média	Produzir monografia e pesquisa utilizando recursos pessoais	Não se aplica
Problemas de saúde	Baixa	Alto	Alta	Tratamento médico das condições identificadas	Diminuição do fator de exposição em caso de doenças com fator ambiental, e exames para verificar condições genéticas
Perda de dados	Muito baixa	Alto	Média	Recuperar cópia de segurança	Cópias de segurança periódicas do material produzido
Queima de equipa-mento(s) eletrô-nico(s)	Muito baixa	Alto	Média	Comprar novo(s) equipamento(s)	Evitar utilização do(s) equipamento(s) em más condições de tempo ou por períodos muito prolongados

REFERÊNCIAS

BERNSTEIN, D. J. et al. SPHINCS: Practical stateless hash-based signatures. In: OSWALD, E.; FISCHLIN, M. (Ed.). **Advances in Cryptology – EUROCRYPT 2015**. [s.n.], 2015. (Lecture Notes in Computer Science, v. 9056), p. 368–397. Disponível em: <https://eprint.iacr.org/2014/795>.

BUCHMANN, J.; DAHMEN, E.; HüLSING, A. XMSS - a practical forward secure signature scheme based on minimal security assumptions. In: YANG, B.-Y. (Ed.). **Post-Quantum Cryptography**. [s.n.], 2011. (Lecture Notes in Computer Science, v. 7071), p. 117–129. Disponível em: <https://eprint.iacr.org/2011/484>.

LAMPORT, L. **Constructing digital signatures from a one-way function**. [S.l.], out. 1979. Disponível em: <https://www.microsoft.com/en-us-/research/publication/constructing-digital-signatures-one-way-function/>.

MERKLE, R. C. A certified digital signature. In: BRASSARD, G. (Ed.). **Advances in Cryptology – CRYPTO '89**. [S.l.: s.n.], 1989. (Lecture Notes in Computer Science, v. 435), p. 218–238.

SHOR, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM Journal on Computing**, v. 26, n. 5, p. 1484–1509, out. 1997. Disponível em: <https://arxiv.org/abs/quant-ph/9508027v2>.