Avaliação de esquemas pós-quânticos de assinatura baseada em atributos

Érico Rolim , Marco Henriques
{e170610@dac.unicamp.br, maah@unicamp.br}

Departamento de Engenharia de Computação e Automação (DCA)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (Unicamp)
Campinas, SP, Brasil

Resumo – Esquemas de assinaturas baseadas em atributos (attribute-based signatures — ABS) utilizando curvas elípticas já foram muito estudados, com múltiplas implementações validadas. Entretanto, não se pode dizer o mesmo sobre esquemas baseados em reticulados, apesar das principais propostas de esquemas pós-quânticos se basearem neles. Isso torna necessário o estudo mais profundo do uso de reticulados nesse tipo de esquema. Esse trabalho busca implementá-los de forma eficiente, ao mesmo tempo que avalia o nivel de segurança que oferecem.

Palavras-chave – post-quantum lattice attribute signature

1. Introdução

1.1. Assinaturas baseadas em atributos

Assinaturas baeadas em atributos são uma classe de construção criptográfica com propriedades interessantes de proteção de privacidade. Permitem a criação de assinaturas onde o foco é nos atributos do indivíduo que gerou a assinatura, sem reveler a identidade desse indivíduo [4]. Atributos podem ser de vários tipos, como o fato do indivíduo ser aluno de um determinado curso ou instituição, ou pertencer a uma certa classe trabalhadora em uma empresa. Normalmente, esses atributos são fornecidos e certificados por uma entidade central.

Há, ainda, aplicações menos óbvias da tecnologia, como em frotas de veículos que se comunicam para transmitir informações sobre movimento e condições de vias [1]: uma entidade central distribui identidades para todos os veículos, e eles podem se comunicar sem revelar sua identidade por completo para outros veículos.

O mecanismo básico de operação da assinatura baseada em atributos é o mesmo, independentemente dos detalhes do esquema criptográfico de cada proposta. Há quatro etapas distintas [3]:

- Setup (configurar): a entidade gera sua chave secreta e define quantos (e talvez quais) atributos serão suportados
- Extract (extrair): a entidade cria uma chave para um certo indíviduo, correspondente aos atributos possuídos pelo indivíduo
- Sign (assinar): o indíviduo cria uma mensagem, e a assina com sua chave; dependendo do esquema criptográfico utilizado, pode ser possível não assinar a mensagem com todos os atributos possuídos pelo indivíduo
- Verify (verificar): um terceiro verifica a mensagem e a assinatura, confirmando que foi assinada por alguém com certos atributos, mas sem saber a identidade desse indivíduo

1.2. Criptografia pós-quântica

Ocorreram muitos avanços em computação quântica nos últimos anos, levando a uma preocupação no mundo da criptografia: os esquemas criptográficos modernos (baseados em grandes números primos e curvas elípticas), se atacados por um computador quântico suficientemente poderoso, podem ser quebrados. Isso levou ao estudo de algoritmos e construções que não tenham as mesmas fraquezas [2].

Entretanto, esquemas de assinaturas baseadas em atributos, em sua maioria, utilizam emparelhamento de curvas elípticas [5]. Dos poucos esquemas utilizando reticulados, e, portanto, possivelmente resistentes a ataques de um computador quântico, não encontramos implementações concretas ou avaliações claras de suas propriedades de segurança ou eficiência.

2. Proposta

A proposta desse trabalho de conclusão de curso, portanto, é avaliar múltiplos aspectos dos esquemas de assinaturas baseadas em atributos presentes em artigos publicados nos últimos anos. As características que serão avaliadas são explicadas abaixo:

- Eficiência: uso de recursos computacionais e tamanho dos artefatos gerados (chaves e assinaturas)
- Segurança: qual o nível equivalente de segurança garantido pela prova de segurança do esquema

Para isso, será necessário implementar os esquemas descritos nos artigos encontrados, uma vez que nenhum conta com implementações públicas dos esquemas criptográficos.

O trabalho começará com uma avaliação mais profunda do esquema explicado em [3], que já foi implementado, com algumas mudanças, no repositório `https://github.com/regras/labs`, por um ex-aluno da FEEC.

Agradecimentos

Agradeço o grupo de estudo ReGrAS, liderado pelo professor Marco Henriques, pelas discussões e apresentações sobre criptografia pós-quântica.

Agradeço minha família por todo apoio e incentivo.

Referências

[1] Hui Cui, Robert H Deng, and Guilin Wang. An attribute-based framework for secure communications in vehicular ad hoc networks. *IEEE/ACM Transactions on Networking*, 27(2):721–733, 2019.

[2] Taniya Hasija, KR Ramkumar, Amanpreet Kaur, Sudesh Mittal, and Bhupendra Singh. A survey on nist selected third round candidates for post quantum cryptography. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)*, pages 737–743. IEEE, 2022.

[3] Xie Jia, Hu Yupu, Gao Juntao, Gao Wen, and Li Xuelian. Attribute-based signatures on lattices. *The Journal of China Universities of Posts and Telecommunications*, 23(4):83–90, 2016.

[4] Hemanta K Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-based signatures. In *Cryptographers' track at the RSA conference*, pages 376–392. Springer, 2011.

[5] Prince Silas Kwesi Oberko, Victor-Hillary Kofi Setornyo Obeng, Hu Xiong, and Saru Kumari. A survey on attribute-based signatures. *Journal of Systems Architecture*, page 102396, 2022.