Proposta de TCC - Criptografia Pós-Quântica Baseada em Códigos Corretores de Erros

Gervásio Protásio dos Santos Neto - NUSP: 7990996

11 de abril de 2016

Orientador: Prof. Dr. Routo Terada

Instituto de Matemática e Estatística - IME USP
Rua do Matão 1010
05311-970 Cidade Universitária, São Paulo - SP

1 Introdução

Atualmente, os padrões de encriptação mais populares no mundo são o RSA [R L78] e criptossistemas baseados em curvas elípticas (em inglês: Elliptic Curves Criptossystems, ou **ECC**) [Mil86].

A segurança destes modelos basea-se no **Problema do Logarítmo Discreto** [Ter00], que de forma generalizada consiste em, dado um grupo abeliano G e $g, s \in G$, calcular $t \in \mathbb{N}$ tal que

$$s = g^t$$

.

No caso do RSA o grupo G é o grupo multiplicativo de $\mathbb{Z}_n$, onde n é o produto de dois primos. Para ECCs o grupo consiste de uma curva elíptica sobre um Corpo de Galois de característica 2, munida de operações sobre os pontos e um ponto no infinito.

Acredita-se que resolver o PLD em computadores clássicos é difícil [Ter00]. Não existe atualmente nenhum algoritmo polinomial para sua resolução.

Contudo, em 1994, Peter Shor propôs um algoritmo quântico que era capaz de resolver o PLD em tempo polinomial [Sho97]. Se computadores quânticos vierem a se tornar viáveis e comercialmente disponíveis, o Algoritmo de Shor pode ser utilizado para facilmente descobrir as chaves secretas de sistemas que usam curvas elípticas ou RSA.

1.1 Criptografia Pós-Quântica

Conforme tornou-se claro que os métodos mais populares de segurança estariam ameaçados por possíveis avanços tecnológicos em Computação Quântica, a comunidade de segurança começou linhas de pesquisa em algoritmos criptográficos que não dependem do Problema do Logaritmo Discreto, a chamada *criptografia pós-quântica*.

Enquanto há diversas propostas para possíveis novos padrões de segurança pós-quântica, como por exemplo sistemas baseados em sistemas de variáveis multinomiais [Buc+04] ou sistemas baseados em hash [Mer79], uma das propostas mais promissora parece ser a de sistemas baseado em códigos corretores de erros [Aug+15].

1.2 Códigos Corretores de Erros

Códigos corretores de erro são formas de assegurar que mensagens transmitidas por canais propensos a erro podem ser lidas ao chegar no seu destino [Van12]. Eles consistem essencialmente em introduzir redundâncias na mensagem de tal forma que o receptor da mensagem consegue checar o padrão das redundâncias, detectando e corrigindo até um número pré-estabelecido de erros.

De forma mais formal, temos que se A é o alfabeto de nossas mensagens, que podemos assumir ter comprimento m, temos uma função de codificação $f : A^m \to \mathbf{C} \subset A^n$, $n > m$, que leva mensagens para o espaço dos códigos.

$\mathbf{C} \subset A^n$ que será o nosso *código*. Quando recebemos uma mensagem y, sabemos que ela contém um erro, com certeza, se $y \notin \mathbf{C}$. Para corrigir os erros de y, a traduzimos como x onde:

$$x = \arg_{z \in \mathbf{C}} \min d(z, y) \ ,$$

onde $d(\cdot, \cdot)$ é a *distância de Hamming*. O número de erros que um dado código $\mathbf{C}$ consegue corrigir depende da menor distância entre dois de seus elementos.

Seja:

$$d = min\{d(x, y) : x, y \in \mathbf{C}\}$$

Então $\mathbf{C}$ é capaz de detectar até $d - 1$ e corrigir até $\kappa = \lfloor \frac{d-1}{2} \rfloor$ erros.

Existem diversas famílias de códigos corretores de erros, que diferem entre si tanto na função de codificação f quanto nas distâncias mínimas d que se consegue obter.

Para criptografia, a família de códigos mais relevante são os **Códigos de Goppa** [Gop70]. Ela possui bons algorimos para codificar e decodificar, além de ser possível provar cotas inferiores para suas distâncias mínimas.

1.3 Criptografia de McEliece

A criptografia de McEliece foi desenvolvida em 1978 [McE78] e utiliza códigos de Goppa para transmissão segura de mensagens. Nela, a chave secreta é um código de Goppa, que tem fácil decodificação, capaz de corrigir t erros. A partir dele, produz-se um código que será *difícil* de decodificar e servirá como chave secreta.

A encriptação consiste essencialmente em transformar a mensagem a ser transmitida para o espaço dos Códigos de Goppa e introduzir t erros. Para decriptar a mensagem, aplica-se o código corretor de erros para se recuperar a mensagem sem erros e recupera-se a mensagem que gerou o código.

A segurança do sistema se baseia em dois fatores [Mis13]:

1. Realizar a decodificação de um código linear genérico é NP-difícil [BMV78]
2. Deve ser difícil distinguir a representação do código presente na chave pública de ruído.

Apesar de ser mais rápido que criptossistemas baseados no PLD, o criptossistema de McEliece não recebeu muita atenção até que começasse o interesse em possíveis alternativas pós-quânticas ao RSA. Esta reação tem dois motivos:

1. Comparadas às chaves do RSA, as do criptossistema de McEliece são muito longas. Por exemplo, para conseguir 80-bits de segurança o RSA precisa de uma chave de 1024 bits, contra os mais de 460 mil bits necessários no criptossistema de McEliece.[Mis13]

2. Códigos corretores de erros e Criptografia têm propósitos intrinsecamente opostos. Enquanto Criptografia se preocupa em obfuscar informação e transmitir mensagens que não podem ser lidas por partes externas, a correção de erros existe para que a integridade da mensagem seja preservada e informação não seja perdida. Essa oposição das áreas gerou ceticismo em relação a um criptossistema que utilizava correção de erros.

1.4 Tentativas de melhora do Criptossistema de McEliece

Devido ao tamanho proibitivo das chaves do Criptossistema de McEliece, diversas tentativas de redução foram feitas. Algumas tentaram trocar a família de códigos corretores de erros utilizadas, contudo em geral isto levou à introdução de inseguranças no esquema criptográfico. [Mis13]

No trabalho serão as abordagens descritas em [Mis13] e [Mis+13] que visam encurtar o tamanho das chaves enquanto preservando a segurança do sistema e ainda permitir uma análise melhor da segurança da chave-pública, reduzindo o problema de distinção da chave por ruído a um problema melhor estabelecido em Teoria dos Códigos.

As abordagens consistem tanto em manter códigos de Goppa, mas utilizando uma variante que permite resultados melhores; quanto em os trocar por códigos baseados em grafos que preservam a segurança do algoritmo.

2 Objetivos

A seguir, descrevemos o que se espera realizar neste trabalho.

2.1 Formalização Matemática

Para compreender tanto o Criptossistema de McEliece quanto as modificações propostas por Misoczki et al. é necessário primeiro entender a Teoria de Códigos Corretores de Erros e Teoria Algébrica dos Códigos.

Como o próprio nome indica, Teoria Algébrica dos Códigos é baseada em resultados de Álgebra Abstrata, principalmente Teoria dos Corpos e Teoria dos Grupos. Torna-se portanto necessário revisar os principais resultados destas áreas para ter um bom entendimento de códigos algébricos.

Há excelentes livros tanto no tópico de Álgebra Abstrata quanto na Teoria de Códigos Algébrica. Um exemplo de referência que oferece ampla base nos dois tópicos é [Van12].

Os códigos corretores de erros baseados em grafos utilizados em [Mis13] e [Mis+13] são pouco explorados na literatura clássica sobre códigos corretores de erros, então para seu entendimento pretende-se usar a investigação feita em [Mis13].

Por fim, julga-se necessário ter noção dos fundamentos da computação quântica para entender os ataques e defesas feitas aos criptossistemas pós-quânticos baseados em códigos. Novamente, a bibliografia disponível é ampla, mas acreditamos que [AB09] e [KSV02] serão introdutores úteis.

2.2 Compreensão do Criptossistema Clássico e das modificações possíveis

A parte central do trabalho é analisar e entender como funciona o criptossitema de McEliece em sua formulação clássica, bem como entender a modificações e aperfeicoamentos descritos em [Mis13].

2.3 Estudo de Ataques

Um criptossitema só se prova útil depois de ter resistido a diversos ataques.

Não se conhece nenhum ataque quântico que é eficaz contra criptossistemas baseados em códigos de Goppa. Contudo, é necessário entender os ataques mal sucedidos para que se possa compreender porque essa classe de algoritmos criptográficos é útil, bem como se tornar ciente de possíveis aspectos que podem ser melhorados.

Em [BLP08] encontramos uma boa fonte para esse estudo.

2.4 Comparação de Performance

É interessante ver como a performance do esquema de encriptação clássico proposto por McEliece se compara às do criptossistema modificado prosposto em [Mis13].

Para tal, nos propomos a implementar em uma linguagem de alto nível ambos os criptossitemas e compará-los nas seguintes métricas:

1. Tamanho das chaves
2. Tempo para codificação da mensagems
3. Tempo de encriptação
4. Tempo de decriptação

3 Cronograma

Com base nas atividades descritas na seção anterior, podemos quebrar a realização do trabalho nas seguintes etapas:

1. Revisão de assuntos de álgebra abstrata
2. Familiarização com códigos corretores de erros
3. Familizarização com computação quântica
4. Estudo do criptossistema de McEliece Clássico
5. Estudo das modificações propostas por Misoczki et al.
6. Estudo dos ataques
7. Implementação dos sistemas e comparação das performances
8. Escrita da monografia
9. Montar pôster e apresentação

E montamos o seguinte cronograma:

Tabela 1: Cronograma ideal

	mar	abr	maio	jun	jul	ago	set	out	nov
1	x	x	x						
2	x	x	x						
3	x	x	x						
4		x	x	x					
5		x	x	x					
6				x	x				
7					x	x			
8							x	x	x
9							x	x	x

Referências

[AB09] Sanjeev Arora e Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[Aug+15] Daniel Augot et al. "Initial recommendations of long-term secure post-quantum systems". Em: *Availab le at pqcrypto. eu. org/docs/initial-recommendations. pdf* (2015).

[BLP08] Daniel J Bernstein, Tanja Lange e Christiane Peters. "Attacking and defending the McEliece cryptosystem". Em: *Post-Quantum Cryptography*. Springer, 2008, pp. 31–46.

[BMV78] Elwyn R Berlekamp, Robert J McEliece e Henk CA Van Tilborg. "On the inherent intractability of certain coding problems". Em: *IEEE Transactions on Information Theory* 24.3 (1978), pp. 384–386.

[Buc+04] Johannes A Buchmann et al. "Post-Quantum Signatures." Em: *IACR Cryptology ePrint Archive* 2004 (2004), p. 297.

[Gop70] Valerii Denisovich Goppa. "A new class of linear correcting codes". Em: *Problemy Peredachi Informatsii* 6.3 (1970), pp. 24–30.

[KSV02] Alexei Yu Kitaev, Alexander Shen e Mikhail N Vyalyi. *Classical and quantum computation*. Vol. 47. American Mathematical Society Providence, 2002.

[McE78] R. J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Em: *Deep Space Network Progress Report* 44 (1978), pp. 114–116.

[Mer79] Ralph Merkle. "Security, authentication and public-key systems - A certified digital signature." Tese de doutorado. Stanford University, 1979.

[Mil86] V.S. Miller. "Use of elliptic curves in cryptography". Em: *Advances in Cryptology (CRYPTO85)* (1986), pp. 417–426.

[Mis+13] Rafael Misoczki et al. "MDPC-McEliece: New McEliece variants from moderate density parity-check codes". Em: *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*. IEEE. 2013, pp. 2069–2073.

[Mis13] Rafael Misoczki. "Two Approaches for Achieving Efficient Code-Based Cryptosystems". Tese de doutorado. Université Pierre et Marie Curie-Paris VI, 2013.

[R L78] L. M. Adleman R. L. Rivest A. Shamir. "A method for obtaining digital signatures and public-key cryptosystems". Em: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[Sho97] P. W. Shor. "Polynomial Time Algorithms for prime factorization and discrete logarithms on a quantum computer." Em: *SIAM Journal on Computing* 26.5 (1997), pp. 1481–1509.

[Ter00] Routo Terada. *Segurança de dados: criptografia em redes de computador*. Editora Blucher, 2000.

[Van12] Jacobus Hendricus Van Lint. *Introduction to coding theory*. Vol. 86. Springer Science & Business Media, 2012.