Criptografia Pós-Quântica e Teoria dos Códigos

André Jucovsky Bianchi
Departamento de Ciência da Computação
Instituto de Matemática e Estatística
Universidade de São Paulo
ajb@ime.usp.br

***Resumo*—O desenvolvimento teórico e prático de sistemas computacionais quânticos representa uma ameaça a sistema criptográficos cujos problemas computacionalmente difíceis associados são baseados em determinadas estruturas algébricas. Sistemas populares como o RSA e problemas bastante estudados como criptografia baseada em curvas elípticas têm sua segurança quebrada pelos algoritmos quânticos de fatoração e de logaritmo discreto de Shor. Este artigo descreve brevemente alguns conceitos fundamentais da criptografia Pós-Quântica para em seguida introduzir os sistemas criptográficos de McEliece e Niederreiter, resistentes a ataques baseados na técnica de amostragem quântica de Fourier, como é o caso do algoritmo de Shor. Ao final, comentamos diversas publicações com propostas de melhoria ou extensão destes sistemas criptográficos, evidenciando algumas linhas de esutdo da Criptografia Pós-Quântica.**

I. Introdução

Os avanços dos anos 60 e 70 na área de complexidade computacional trouxeram a possibilidade de basear sistemas criptográficos em problemas computacionalmente difíceis. Neste contexto, ao longo do desenvolvimento da criptografia moderna foram propostos novos modelos de segurança utilizando estes problemas como ingredientes, substituindo assim a ideia de segurança perfeita pela restrição mais fraca de que seja apenas ineficiente extrair informações sobre o texto original a partir do texto cifrado sem o conhecimento da chave criptográfica. Este relaxamento permitiu o desenvolvimento de diversos sistemas criptográficos eficientes com chaves substancialmente menores que nos algoritmos clássicos.

Problemas NP-completos, por serem representantes de uma classe de problemas para os quais há forte evidência de intratabilidade, seriam candidatos imediatos a servirem de base para sistemas criptográficos, não fosse por alguns detalhes. É frequente encontrar problemas NP-completos cujo caso médio não é intratável e, frequentemente, a própria computação de instâncias intratáveis é, ela mesma, intratável. Desta forma, a atenção dos desenvolvedores de criptossistemas se voltou naquele momento para problemas menos difíceis porém com complexidade suficientemente alta, ou seja, problemas cujo cálculo de um caso médio é eficiente, mas para os quais encontrar a solução do caso médio é supostamente intratável. É este o caso, por exemplo, dos protocolos Diffie-Hellman para troca de chaves (1976) e RSA (1978) para criptografia de chave pública, ambos baseados no problema do logaritmo discreto.

Este cenário mudou bruscamente em 1994 com o advento dos algoritmos de Shor para fatoração e logaritmo discreto em tempo polinomial utilizando um computador quântico. A partir daí, o desenvolvimento da Computação Quântica contribuiu em duas direções para a criptografia. Por um lado, a Computação Quântica forneceu ferramental teórico para a caracterização da segurança de novos sistemas criptográficos beaseados em Física Quântica, área que podemos chamar de Criptografia Quântica. Por outro lado, a possibilidade de resolver em tempo polinomial (utilizando um computador quântico) problemas nas quais muitos sistemas criptográficos atuais estão baseados motiva o desenvolvimento da criptografia *Pós-Quântica*: aquela criptografia que trata dos sistemas que não são quebrados com o advento do computador quântico e seu arsenal de algoritmos, entre eles os de Shor.

Na próxima seção, apresentaremos uma breve introdução à criptografia Pós-Quântica. Em seguida, apresentaremos os sistemas criptográficos de McEliece e Niederreiter, sugeridos no final dos anos 70 e provados somente em 2011 serem resistentes a ataques como os que quebram a maioria dos sistemas criptográficos atuais supondo a existência de computadores quânticos grandes o suficiente. Finalmente, discutiremos algumas propostas de melhorias e aplicações destes criptossistemas, contextualizando seu estudo atual.

A. Criptografia Pós-Quântica

Em 1994, Peter Shor desenvolveu algoritmos para computar eficientemente a fatoração em primos e o logaritmo discreto utilizando um computador quântico [12]. Estes algoritmos são baseados em um processo chamado Quantum Fourier Sampling (QFS), que consiste em utilizar o paralelismo quântico para a computação rápida da transformada discreta de Fourier de funções limitadas em $\mathbb{Z}^n$ e em seguida realizar a medição dos resultados.

Os problemas resolvidos por tais algoritmos são na realidade instâncias de um problema mais geral chamado

Hidden Subgroup Problem (HSP). O HSP é definido informalmente da seguinte forma: dado um grupo e uma função que é constante e distinta em coclasses de algum subgrupo desconhecido, encontre um conjunto de geradores deste subgrupo. Em outras palavras, uma função constante e distinta em coclasses de um subgrupo é uma função periódica, e encontrar o subgrupo pode ser compreendido como encontrar o período desta função. Desta forma, não é de surpreender que a utilização de técnicas baseadas na Transformada de Fourier possam ajudar a resolver este problema. De fato, quando o grupo subjacente é finito e abeliano, a técnica QFS leva à solução do HSP.

Assim, há evidência suficiente para supor que problemas computacionalmente difíceis baseados em grupos abelianos podem ser resolvido por instâncias adaptadas do algoritmo de Shor utilizando as técnicas acima mencionadas. Então, alguns problemas utilizados com bastante frequência na criptografia moderna são, na verdade, "Pré-Quânticos", pois não resistem ao advento do computador quântico. Exemplos de problemas Pré-Quânticos são os já mencionados problemas da fatoração em primos e do logaritmo discreto, além de outros como curvas elípticas, homomorfismos algébricos, entre outros [3].

Desta forma, a pesquisa para o desenvolvimento da criptografia Pós-Quântica possui como foco a busca por sistemas criptográficos baseados em problemas algébricos construídos sobre grupos não-abelianos, provas de segurança para estes esquemas e propostas práticas com parâmetros de tamanho razoável que garantam bons níveis de segurança.

Este artigo trata de sistemas criptográficos baseados em códigos corretores de erros, para os quais há provas de que não são afetados pelas técnicas baseadas no algoritmo de Shor. Mas, além destes, há também sistemas para os quais não se conhece ataques quânticos, além de haver evidência de que sejam resistem aos ataques descritos acima, como é o caso de sistemas baseados em reticulados ou em sistemas de equações multivariadas quadráticas.

Este texto tem como objetivo apresentar os principais conceitos envolvidos na criptografia baseada em teoria dos códigos corretores de erros, apresentados pela primeira vez por McEliece em 1979, e seus desenvolvimentos recentes com o interesse crescente em problemas Pós-Quânticos. Publicado apenas um ano após o sistema RSA, a proposta de McEliece para sistemas baseados em teoria dos códigos não teve tanta atenção quanto outros. Por motivos de interesse prático e comercial, o RSA ganhou inicialmente bastante aceitação e se tornou um dos padrões mais utilizados na criptografia moderna. Hoje se mostra necessário revisitar ideias antigas para recuperar e desenvolver sistemas interessantes que foram deixados para trás.

Na próxima seção, descreveremos brevemente a teoria envolvida na criptografia baseada em códigos corretores de erros para em seguida apresentar alguns desenvolvimentos recentes destas ideias.

II. Criptossistemas Pós-Quânticos baseados em códigos corretores de erros

Os estudos na área da teoria da informação, iniciada principalmente por Claude Shannon no final dos anos 40, permitiram o desenvolvimento da teoria dos códigos, que consiste principalmente em duas grandes frentes: codificação da fonte (compressão) e codificação do canal (correção de erros). Richard Hamming foi pioneiro nesta área e em 1950 inventou o primeiro código corretor de erros, chamado de código de Hamming $(4, 7)$. Informalmente, a ideia é transmitir, junto com a informação desejada (neste caso 4 bits), uma certa quantidade de informação redundante (totalizando, neste caso, 7 bits) que permita a recuperação dos dados originais na eventualidade de serem introduzidos erros ao longo de um canal de comunicação ruidoso.

Quase três décadas depois, muito da teoria básica desenvolvida para códigos corretores de erros já havia sido compilada em forma de livro por McEliece [8], quando este publicou, em 1978, reduções polinomiais de problemas NP-completos para problemas simples de códigos corretores de erros [1]. Assim, com forte evidência de intratabilidade de alguns problemas baseados em teoria dos códigos, abriu-se caminho para a criação de novos criptossistemas que mais tarde seriam revisitados por sua característica Pós-Quântica, então desconhecida.

A seguir, apresentaremos algumas definições básicas para a compreensão do uso dos códigos corretores de erros para criptografia. Em seguida, apresentaremos os sistemas criptográficos de chave pública de McEliece e de Niederreiter, variantes de um mesmo tema sobre códigos corretores de erros, e que mais tarde foram provados serem equivalentes para uma certa escolha adequada de parâmetros [6].

A. Códigos corretores de erros

Definição 1. *Um $(n, k)-$**código linear** sobre um corpo finito $\mathbf{F}_q$ é um subespaço $k-$dimensional de um espaço linear $n-$dimensional $\mathbf{F}_q^n$. Dizemos que n é o* comprimento *do código, e que k é sua* dimensão*.*

Dependendo da estrutura algébrica do corpo utilizado para sua construção, cada código possuirá uma determinada capacidade de correção de erros. Para ter uma ideia mais clara do processo de correção de erros, introduzimos mais duas definições para em seguida complementar com um exemplo.

Definição 2. *Seja C um $(n, k)-$código linear sobre $\mathbf{F}_q$. Uma matriz G cujo espaço gerado pelas linhas*

seja igual a C é chamada de ***matriz geradora*** *de C. Reciprocamente, se G é uma matriz com valores em $\mathbf{F}_q$, o espaço gerado por suas linhas é chamado de* ***código gerado por*** *G.*

Definição 3. *Uma* ***palavra de código*** *de um $(n,k)-$código linear C é um vetor $n-$dimensional pertencente a C.*

Exemplo 1. *Seja C_1 um $(7,4)-$ código linear com a seguinte matriz geradora:*

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Este código é chamado de Código de Hamming.

Um $(n,k)-$código linear possui q^k palavras de código, de forma que pode comunicar q^k mensagens diferentes. A codificação de uma $k-$tupla $u = (u_1, \ldots, u_k)$ consiste no mapeamento através da combinação linear das linhas da matriz G geradora do código, da seguinte forma:

$$u \to uG$$

Assim, utilizando o código do exemplo 1, é possível mapear vetores quaisquer de dimensão 4 em vetores de dimensão 7 que pertencem ao código, através da multiplicação de vetor por matriz da forma descrita acima.

A recuperação da mensagem original através da palavra de código é feita através da utilização de uma *matriz de paridade* associada ao código. Para um determinado $(n,k)-$código linear C, uma *verificação de paridade* é uma equação da forma

$$a_1x_1 + \cdots + a_nx_n = 0$$

que é satisfeita para todo $x = (x_1, \ldots, x_n) \in C$. O conjunto de todos os vetores $a = (a_1, \ldots, a_n)$ para os quais a equação acima é satisfeita para todo $x \in C$ é também um subespaço vetorial de $\mathbf{F}_q^n$, chamado *código dual de C* e denotado por $C^\perp$. É possível mostrar que $C^\perp$ é um $(n, n-k)-$código linear sobre $\mathbf{F}_q$, de forma que uma matriz de paridade para C pode ser definida como uma matriz geradora de $C^\perp$. Ou, equivalentemente:

Definição 4. *Seja C um $(n,k)-$código linear sobre $\mathbf{F}_q$. A matriz H com a propriedade de que $Hx^T = 0$ se e só se $x \in C$ é chamada de* ***matriz de verificação de paridade para*** *C.*

Supondo que os alfabetos das mensagens enviadas e recebidas por um certo canal ruidoso sejam os mesmos, se uma certa palavra de código $x = (x_1, \ldots, x_n) \in \mathbf{F}_q^n$ é enviada, então a palavra recebida $y = (y_1, \ldots, y_n)$ também pertence a $\mathbf{F}_q^n$. A diferença $z = y - x$ é chamada de *padrão de erros* introduzido pelo canal na transmissão da mensagem, de forma que se $z_i \neq 0$ então dizemos que ocorreu um erro na posição i da palavra de código.

A decodificação é realizada através da utilização da matriz de verificação de paridade H, da forma descrita a seguir. Para todo x transmitido, vale que $Hx^T = 0$, de forma que se $z \neq 0$ então é muito provável que $Hy^T \neq 0$. O vetor $s = Hy^T$ é chamado de *síndrome*, e tem a característica de que seu valor depende apenas do padrão de erros introduzido no canal, e não depende da palavra de código transmitida, pois:

$$\begin{aligned} s = Hy^T &= H(x+z)^T \\ &= Hx^T + Hz^T = Hz^T. \end{aligned} \tag{II.1}$$

No contexto de correção de erros, o interesse está em recuperar o valor da palavra transmitida x. Mas, se for possível inferir z a partir de Hy^T, então basta fazer $x = y - z$ para obter a mensagem original. Em geral, existem diversas escolhas possíveis para z a partir de uma certa síndrome, e a inferência de qual foi o padrão de erros inserido é baseada em estatísticas do canal e propriedades algébricas dos corpos utilizados.

Para terminar esta seção, enunciamos formalmente os problemas de decodificação de síndromes q-árias que embasam os criptossistemas que serão apresentados. Para isto, utilizamos a noção de *peso de Hamming* de um vetor, definido a seguir.

Definição 5. *O* ***peso de Hamming*** *de um vetor x é o número de coordenadas não nulas de x, denotado por $wt(x)$.*

Problema 1. *O problema da decodificação de síndromes q-árias (qSD)*

- ***Entrada:*** *H uma matriz $r \times n$ de verificação de paridade sobre $\mathbf{F}_q$, $s \in \mathbf{F}_q^r$ e um inteiro $\omega > 0$.*
- ***Saída:*** *Uma palavra de código $x \in \mathbf{F}_q^n$ tal que $wt(x) \leq \omega$ e $Hx^T = s^T$.*

Uma outra forma de enunciar o problema pode ser vista a seguir.

Problema 2. *O problema geral da decodificação de síndromes q-árias (G-SD)*

- ***Entrada:*** *G uma matriz $n \times k$ geradora de um $(n,k)-$código linear sobre $\mathbf{F}_q$, $y \in \mathbf{F}_q^n$ e um inteiro $\omega > 0$.*
- ***Saída:*** *Uma palavra de código $x \in \mathbf{F}_q^n$ e um padrão de erros $e \in \mathbf{F}_q^k$ tais que $wt(e) \leq \omega$ e e $xG + e = y$.*

Esta forma do enunciado do problema é exatamente o problema NP-completo utilizado no criptossistema proposto por McEliece em 1978, que veremos na próxima seção.

B. O criptossistema de McEliece

O criptossistema de McEliece [7] utiliza um $(n, k)-$código linear binário C construído selecionando-se aleatoriamente um polinômio irredutível de grau t sobre $\mathbf{F_{2^m}}$. A possibilidade de construção de um sistema criptográfico está baseada no fato de que para cada polinômio deste tipo existe um código de comprimento 2^m e dimensão $k \geq n - tm$ eficientemente decodificável e capaz de corrigir um padrão de erros com peso menor ou igual a t.

Sistema 1. *Criptossistema de McEliece*

Sejam G uma matriz $k \times n$ geradora do código C, S qualquer matriz $k \times k$ não singular e P qualquer matriz de permutação $n \times n$. O criptossistema de McEliece é definido da seguinte forma:

- ***Chave privada:*** *G, S e P, como descritas acima.*
- ***Chave pública:*** *$G' = SGP$ e t.*
- ***Mensagens:*** *vetores x de k bits sobre $\mathbf{F}_2$.*
- ***Encriptação:*** *O texto cifrado é $y = xG' + e$, sendo que e é um vetor de erros aleatório sobre $\mathbf{F}_q^n$ com $wt(e) = t$.*
- ***Decriptação:*** *Como $y = xSGP + e$, então $yP^{-1} = (xS)G + eP^{-1}$. Assim, podemos utilizar um algoritmo rápido de decodificação para C para "corrigir" o erro eP^{-1}, de forma a obter xS e finalmente x.*

É interessante notar que o sistema é facilmente implementável tanto em software quanto em hardware, pois se baseia em operações elementares de álgebra linear como multiplicação de vetor por matriz. Em seu artigo original, McEliece não chega a fazer uma análise completa da segurança do sistema, mas comenta que utilizando-se $n = 1024$, $k = 524$ e $t = 50$, a probabilidade da decodificação correta de um vetor aleatório sem o conhecimento da chave privada é de cerca de 2^{-215}.

C. O criptossistema de Niederreiter

O criptossistema de Niederreiter utiliza a ideia de matriz de verificação de paridade, e também é baseado em códigos de Goppa, mas agora sobre $\mathbf{F}_q$[10].

Sistema 2. *Criptossistema de Niederreiter*

Sejam H uma matriz $(n-k) \times n$ de verificação de paridade para um código C, M uma matriz $(n-k) \times (n-k)$ não singular qualquer, e P uma matriz $n \times n$ de permutação, todas sobre $\mathbf{F}_q$. O criptossistema de Niederreiter é definido da seguinte forma:

- ***Chave privada:*** *H, M e P, como descritas acima.*
- ***Chave pública:*** *$H^* = MHP$ e t.*
- ***Mensagens:*** *vetores y de n bits sobre $\mathbf{F}_q$ com peso t.*
- ***Encriptação:*** *O texto cifrado é $z = y(H^*)^T$, com dimensão $(n-k)$.*
- ***Decriptação:*** *Como $z = y(MHP)^T$, então $z(M^T)^{-1} = (yP^T)H^T$. Assim, podemos utilizar um algoritmo rápido de decodificação para C para encontrar yP^T, e finalmente y.*

Como já mencionamos anteriormente, os dois criptossistemas apresentados são equivalentes. Na próxima seção, discutiremos algumas implementações.

III. Desenvolvimento e implementações

Uma vez proposto um criptossistema, o interesse de pesquisadores da área costuma determinar os rumos da investigação sobre sua segurança e praticidade. Por motivos históricos, comerciais e práticos, os sistemas propostos por McEliece e Niederreiter no final dos anos 70 não tiveram tanta atenção quanto outros sistemas desenvolvidos na mesma época.

Apenas recentemente, com o desenvolvimento da Criptografia Pós-Quântica, estes sistemas voltaram a receber maior atenção. Em 1994, Li et al. mostraram a equivalência dos dois sistemas [6] sem citar as descobertas de Shor do mesmo ano (publicadas de fato somente três anos mais tarde) e suas implicações na área de criptografia. Nos anos seguintes, a pesquisa se intensificou sobre estas propostas na busca de sistemas resistentes a ataques quânticos conhecidos.

Foi somente no ano da publicação do presente texto (2011) que Dinh et al. mostraram que, de fato, os criptossistemas acima descritos, baseados em códigos corretores de erros, são resistentes a ataques do tipo QSP, descrito na introdução [5].

Nesta seção, veremos alguns avanços nas propostas de implementação dos sistemas descritos na seção anterior. O que buscamos aqui é tanto ilustrar os diferentes aspectos envolvidos na segurança de um criptossistema, quanto evidenciar de que forma a motivação "Pós-Quântica" tem contribuído para o desenvolvimento das pesquisas sobre os criptossistemas de McEliece e Niederreiter.

A. Segurança semântica

O conceito de segurança semântica em um certo sistema criptográfico de chaves públicas pode ser compreendido informalmente como a dificuldade de obter informações sobre o texto original a partir do texto cifrado. Em outras palavras, deve ser computacionalmente difícil distinguir o texto cifrado de um texto escolhido aleatoriamente com distribuição de probabilidade constante sobre as letras do alfabeto em questão.

Acontece que os sistemas McEliece e Niederreiter não são seguros contra a modalidade de ataques chamada de *Chosen Plaintext Attacks*, nas quais o atacante tem a possibilidade de associar um texto cifrado a uma mensagem original escolhida a dedo. Considerando, por exemplo, o sistema McEliece, se um atacante possui

acesso a um certo texto cifrado y que sabe ser a versão criptografada de uma de duas mensagens x_1 ou x_2, então ele pode computar $x_1G + y$ e verificar se o peso do resultado é igual ao valor público t. Desta forma, a informação obtida pode, com alta probabilidade, quebrar o sistema.

Em 2008, Nojima et al. provaram que a concatenação do texto original com uma palavra aleatória de um certo tamanho mínimo antes da encriptação é condição suficiente para garantir a segurança semântica dos sistemas, contanto que os problemas da decodificação de síndromes e da obtenção do código original após a permutação das matrizes geradora e de verificação de paridade sejam realmente difíceis[11].

Ao fim do artigo é proposta a utilização de códigos lineares com $n = 4096$ e $k = 2560$ e a introdução de $t = 128$ erros para a codificação de mensagens de tamanho igual a 512 bits e nível de segurança de 131 bits, aproximadamente.

B. Melhorando os ataques e a segurança dos sistemas

Um dos melhores ataques conhecidos para os sistemas McEliece e Niederreiter é chamado de Information-Set Decoding (ISD). O ataque de Stern é uma variante deste ataque, que busca encontrar uma palavra de código de tamanho pequeno, o que é suficiente para a decodificação de um código linear, e consequentemente também é suficiente para quebrar os sistemas da forma que foram propostos.

Em um artigo de 2008, Bernstein et al. apresentaram uma variante mais poderosa do ataque de Stern que utiliza escolhas mais cuidadosas ao longo do algoritmo de forma a chegar mais rápido na resposta desejada [2]. Com este novo ataque, eles demonstram que é possível quebrar o sistema com os parâmetros originalmente propostos utilizando um computador desktop comum em 1400 dias (em comparação a 7 milhões e 400 mil dias para o ataque anterior).

Com o novo ataque, os autores sugerem novos valores para os parâmetros do sistema, aumentando o tamanho das palavras de código e o número de erros introduzidos através de novas técnicas de decodificação. Para um nível de segurança de 256 bits, eles propõem a utilização de $(6624, 5129)-$códigos lineares com a introdução de $t = 117$ erros, resultando em chaves públicas de cerca de 7,6 Mbits.

C. Encurtando as chaves

Ao mesmo tempo que a complexidade dos algoritmos de encriptação e decriptação (com o conhecimento das chaves) é mais baixa do que em sistemas baseados nos problemas da fatoração e do logaritmo discreto, os sistemas baseados em códigos corretores de erros possuem chaves bem maiores do que os algoritmos mais comumente utilizados. Muitas propostas foram feitas para diminuição do tamanho das chaves sem comprometimento da segurança do sistema, como por exemplo a utilização de códigos pouco densos, quasi-cíclicos e outros, o que permite uma certa economia na representação das matrizes utilizadas por conta de sua estrutura.

Em 2009, Misoczki et al. [9] propuseram a utilização de códigos de Goppa quasi-diádicos, que resultam em chaves menores em um fator de $\tilde{O}(n)$ em relação às chaves propostas originalmente, conseguindo inclusive manter o fator de correção de erros intacto, diferentemente do que ocorreu em propostas anteriores de diminuição do tamanho das chaves.

Os autores mostram que o problema da decodificação de síndromes quasi-diádicas é equivalente ao QSD, e portanto NP-completo. As operações de geração de código, codificação e decodificação também têm sua complexidade reduzida para $O(n \log n)$ e é proposta a utilização de $(8192, 4096)-$códigos lineares de Goppa, com introdução de $t = 256$ erros e chaves de 65 Kbits para um nível de segurança 256 bits.

D. Side channel attacks

Ataques que exploram características das implementações dos criptossistemas são chamados de *side channel attacks*, ou "ataques de canais colaterais". Variáveis como tempo de processamento, consumo de energia ou utilização de memória podem ser utilizadas para obter informação relevante sobre o texto original sem ter acesso às chaves criptográficas.

Um artigo de Strenzke et al. de 2008 apresenta em detalhes um ataque de temporização sobre o grau do polinômio localizador de erros, utilizado no passo de correção de erros do algoritmo de decriptação [13]. Através da manipulação dos textos cifrados, um oponente pode acompanhar o tempo de decifração e obter informações sobre o padrão de erros inserido na mensagem. A proposta de medida de precaução é aumentar o grau dos polinômios artificialmente sempre que eles forem menores do que um certo valor.

Também são apresentados, com menos detalhes, ataques que se baseiam na análise da utilização de memória e consumo de energia, assim como possíveis medidas preventivas. A conclusão é que, assim como outros sistemas, os sistemas McEliece e Niederreiter também são vulneráveis a ataqueis por canais colaterais e necessitam de estudo minucioso para viabilizar sua utilização prática.

E. Esquemas de identificação

Os esquemas criptográficas construídos a partir de problemas relacionados à teoria dos códigos não se limitam

a infraestruturas de chave-pública somente. É possível utilizar variações das mesmas construções para o desenvolvimento de esquemas de assinatura, indentificação, entre outros.

Um exemplo de esquema de identificação que utiliza provas com conhecimento zero baseadas nos problemas de decodificação de síndromes q-árias foi publicado em 2010 por Cayrel et al.[4]. Os autores apresentam uma variação, sobre alfabetos $q-$ários, de um outro esquema publicado anteriormente construído sobre códigos binários. O sistema proposto possui valores de parâmetros bem menores para um nível de segurança equivalente.

Para um nível de segurança de 128 bits, os autores propõem 16 rodadas do algoritmo de identificação construído sobre um $(n, k)-$código linear sobre $\mathbf{F}_{256}$ com $n = 208$, $k = 104$ e chave privada com peso de Hamming igual a 75. Neste contexto, a informação pública do sistema ocupa pouco menos que 87 Kbits, porém a identificação pública ocupa apenas 832 bits e chave privada 1664 bits. A comunicação entre as partes é de cerca de 48 Kbits.

Com isto concluímos a apresentação de uma amostra das propostas e estudos relacionados aos sistemas apresentados, todos motivados pela característica Pós-Quântica dos sistemas baseados em códigos corretores de erros. Na próxima seção faremos uma breve discussão do que foi apresentado para então concluir este relatório.

IV. Discussão e conclusão

Como vimos, as características Pós-Quânticas dos problemas baseados em teoria dos códigos motivam hoje diversos estudos sobre os sistemas McEliece e Niederreiter. A escolha cuidadosa das estruturas e manipulações algébricas e dos parâmetros de cada sistema é fundamental e diversas direções podem ser exploradas com o objetivos de melhorar o desempenho ou a segurança dos sistemas.

Vimos, na seção anterior, propostas de (1) estabelecimento da segurança semântica dos sistemas, (2) melhoria de alguns tipos de ataque com o objetivo de refinar a escolha dos parâmetros e assim aumentar a segurança dos sistemas, (3) encurtamento de chaves e outros parâmetros, (4) ataques baseados em implementações físicas dos sistemas, e (5) esquemas com outros objetivos que não somente a proteção de informação trafegada em canais públicos. Isto dá uma ideia da vastidão de possibilidades que têm de ser investigadas para que haja consenso na utilização de um certo algoritmo em detrimento de outros.

O campo da criptografia Pós-Quântica é terreno fértil para novos estudos. É interessante notar que uma parte significativa das pesquisas atuais trate de de problemas e algoritmos que tiveram pouca atenção por muito tempo.

A computação quântica ainda é uma área recente e pode ser que no futuro apareçam algoritmos que resolverão os problemas da teoria de códigos corretores de erros de forma eficiente em computadores quânticos. Por outro lado, já se completam quase duas décadas desde a primeira aparição do algoritmo de Shor, e deste então não se tem notícias de outros algoritmos quânticos tão poderosos em termos de criptanálise. Qualquer que seja o resultado, o processo de investigação é fundamental para validar ou refutar propostas de novos criptossistemas.

Referências

[1] E R Berlekamp, R J Mceliece, and H C A Van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24, 1978.

[2] Daniel Bernstein, Tanja Lange, and Christiane Peters. Attacking and defending the mceliece cryptosystem. In *Post-Quantum Cryptography*, volume 5299 of *Lecture Notes in Computer Science*, pages 31–46. 2008.

[3] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. *Post Quantum Cryptography*. Springer Publishing Company, Incorporated, 1st edition, 2008.

[4] Pierre-Louis Cayrel, Pascal Véron, and Sidi Mohamed El Yousfi Alaoui. A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. In *Selected Areas in Cryptography*, pages 171–186, 2010.

[5] Hang Dinh, Cristopher Moore, and Alexander Russell. Mceliece and niederreiter cryptosystems that resist quantum fourier sampling attacks. In *CRYPTO*, pages 761–779, 2011.

[6] Yuan Xing Li, Robert H. Deng, and Xin mei Wang. On the equivalence of mceliece's and niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, 1994.

[7] R J Mceliece. A public-key cryptosystem based on algebraic coding theory. *DSN progress report*, 42(44):114–116, 1978.

[8] Robert J. Mceliece. *The Theory of Information and Coding*, volume 3 of *Enciclopedia of Mathematics: Probability*. 1977.

[9] Rafael Misoczki and Paulo S. Barreto. Selected areas in cryptography. chapter Compact McEliece Keys from Goppa Codes, pages 376–392. 2009.

[10] H Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[11] Ryo Nojima, Hideki Imai, Kazukuni Kobara, and Kirill Morozov. Semantic security for the mceliece cryptosystem without random oracles. *Des. Codes Cryptography*, 49(1-3):289–305, 2008.

[12] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Computing*, pages 1484–1509, 1997.

[13] Falko Strenzke, Erik Tews, H. Molter, Raphael Overbeck, and Abdulhadi Shoufan. Side channels in the mceliece pkc. In *Post-Quantum Cryptography*, volume 5299 of *Lecture Notes in Computer Science*, pages 216–229. 2008.