Proposta de Minicurso para a SBSeg 2016

Criptografia Pós-Quântica Baseada em Códigos Corretores de Erros

Gervásio Santos
IME-USP
gervasio@ime.usp.br

Routo Terada
IME-USP
rt@ime.usp.br

Thales Paiva
IME-USP
tpaiva@ime.usp.br

27 de junho de 2016

Sumário

1 Dados Gerais

1.1 Objetivo e Justificativa

Nosso objetivo é apresentar duas variantes do esquema de McEliece [McEliece, 1978], propostas por Misoczki em sua tese de doutorado [Misoczki, 2013], tratando com cuidado da teoria necessária para a sua compreensão. O esquema de chave pública de McEliece foi o primeiro baseado em códigos corretores de erros, e também o primeiro a usar um procedimento aleatório no processo de encriptação [Menezes et al., 1996]. Tanto a encriptação quanto a decriptação são computacionalmente mais eficientes que as respectivas de outros criptossistemas baseados no problema do logaritmo discreto. Apesar disso, o tamanho da chave pública entre centenas e milhares de quilobytes faz com que esse sistema seja pouco utilizado.

Depois de anos sem atenção, o esquema de McEliece passa a ser estudado pois, ao contrário do RSA [R. L. Rivest, 1978] e das Curvas Elípticas [Miller, 1986], esse sistema resiste a ataques quânticos baseados no algoritmo de Peter Shor [Shor, 1997]. Com os principais algoritmos de chave pública em uso ficando cada vez mais vulneráveis com os avanços em computação quântica, justificam-se as buscas por algoritmos criptográficos resistentes a ataques quânticos, dando origem à área chamada Criptografia Pós-Quântica.

Uma das linhas de pesquisa em criptografia pós-quântica é diminuir o tamanho das chaves originais do esquema de McEliece através da escolha adequada da família de códigos associada. Originalmente, McEliece sugeriu o uso de códigos de Goppa binários e irredutíveis, que resultam em grandes chaves. Algumas outras famílias de códigos foram propostas, como as dos códigos BCH quase cíclicos [Gaborit, 2005], alternantes quase cíclicos [Berger et al., 2009], e códigos LDPC [Shokrollahi et al., 2000]. Apesar de obterem uma boa redução do comprimento da chave, as duas primeiras foram mostradas inseguras alguns anos depois [Otmani et al., 2010, Faugere et al., 2010], e os próprios autores da terceira proposta explicam por que ela é vulnerável.

Duas propostas de famílias de códigos associadas ao esquema de McEliece, que obtêm chave pública compacta, e não mostradas inseguras, foram feitas por Misoczki em sua tese de doutorado [Misoczki, 2013]. A primeira é a dos Códigos de Goppa quase p-ádicos, e a segunda é a dos códigos com matriz de verificação de paridade de densidade moderada (MDPC).

Em 2013, no XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Barreto, Biasi, Piazza, e Dahab, apresentaram um minicurso introdutório sobre criptografia pós-quântica [Barreto et al., 2013]. Nesse minicurso, dentre os vários aspectos de criptografia pós-quântica, são apresentados superficialmente os esquemas de criptografia baseados em códigos corretores de erros na seção 2.4. Então, em relação a esse texto, nossa proposta é aprofundar essa seção.

1.2 Tratamento dado ao tema

Nosso tratamento será fundamentalmente teórico, mas apoiado por código em SageMath [Stein et al., 2008], desenvolvido pelos autores, que será disponibilizado num repositório online.

Para que se possa entender o esquema de McEliece, são essenciais alguns resultados de álgebra e teoria de códigos. Assim, nas primeiras seções fazemos uma revisão desses conceitos. E depois, introduzimos os códigos de Goppa, seus algoritmos de codificação e decodificação, com as suas devidas demonstrações.

Com todos os pré-requisitos já preenchidos, definimos o criptossistema de McEliece, e fazemos a sua redução de segurança. Mostramos os tamanhos das chaves e comparamos com as repectivas do RSA e de curvas elípticas, para um mesmo nível de segurança.

Apresentamos em uma seção a proposta dos códigos de Goppa quase p-ádicos, para diminuir as chaves. Duas seções são dedicadas à apresentação de famílias de códigos sem estrutura algébrica, os LDPC e os MDPC. Os LDPC são provados como inseguros, e mostramos como os códigos MDPC possuem algumas vantagens dos LDPC, mas se mantêm seguros contra ataques algébricos.

Finalmente, uma seção de conclusão mostra as comparações entre os códigos apresentados, com relação à complexidade das operações de codificação e decodificação. Também comparamos os criptossistemas apresentados com o RSA e curvas elípticas com relação ao tamanho das chaves, segurança esperada, e complexidade das operações de encriptação e decriptação.

1.3 Perfil dos alunos

Estudantes de Ciência da Computação com conhecimentos básicos de álgebra e estudantes de Matemática com familiaridade com algoritmos e Complexidade.

2 Estrutura prevista do texto

A estrutura prevista e os números esperados de páginas em cada seção são dados a seguir.

1 Introdução (5 páginas)
2 Preliminares (12 páginas)
  2.1 Corpos Finitos
  2.2 Códigos Lineares
3 Códigos de Goppa (10 páginas)
  3.1 Definição
  3.2 Resultados
  3.3 Codificação
  3.4 Decodificação
4 Criptossistema de McEliece (6 páginas)
  4.1 Definição
  4.2 Redução de segurança
  4.3 Sobre a segurança do esquema
5 Códigos de Goppa quase p-ádicos (11 páginas)
  5.1 Definição
  5.2 Codificação
  5.3 Decodificação
  5.4 Ataque e Defesa
6 Códigos LDPC (5 páginas)
  6.1 Definições
  6.2 Codificação e Decodificação
  6.3 Fraquezas e Vulnerabilidades
7 Códigos MDPC (7 páginas)
  7.1 Definição
  7.2 Codificação e Decodificação
  7.3 Resultados
8 Conclusão (3 páginas)

Total aproximado de páginas: 59 páginas

3 Resumo e bibliografia de cada seção

3.1 Introdução

Será introduzido o conceito de criptografia pós-quântica, justificando a sua importância, e citando alguns dos sistemas existentes [Bernstein et al., 2009]. Então, fazemos uma introdução informal sobre os códigos corretores de erros, e mostramos como a Criptografia pode fazer uso deles.

3.2 Preliminares

São apresentados os fundamentos matemáticos necessários para o entendimento dos algoritmos e teoremas relacionados ao Criptossistema de McEliece. Para cada área apresentaremos as principais definições e teoremas, bem como provas selecionadas para os mais importantes. Nos baseamos principalmente em [Fraleigh, 2003] para a parte de Corpos Finitos, e [Van Lint, 2012] para a de Teoria de Códigos. A divisão da seção é dada a seguir.

1 Teoria de Corpos Finitos (6 páginas)
2 Códigos Lineares (6 páginas)

3.3 Códigos de Goppa

É apresentada a família dos códigos lineares de Goppa [Goppa, 1970], e mostrados os principais resultados sobre, seguindo a exposição em [Engelbert et al., 2007]. Primeiro apresentamos códigos gerais, mas nos aprofundamos em códigos de Goppa binários e irredutíveis. Mostramos os algoritmos de codificação e decodificação, demonstrando a sua corretude, e discutimos aspectos de implementação [Biswas and Sendrier, 2008]. A divisão da seção é dada a seguir.

1 Definição (3 páginas)
2 Resultados (3 páginas)
3 Codificação (1 página)
4 Decodificação (3 páginas)

3.4 Criptossistema de McEliece

Nesta seção, será introduzido o esquema criptográfico de chave pública proposto por McEliece [McEliece, 1978]. Nossa exposição será baseada em [Bernstein et al., 2009, Bernstein et al., 2008], e discutimos detalhes práticos de implementação. Mostramos a sua redução de segurança [Berlekamp et al., 1978] e fazemos uma pequena análise de sua sua segurança, nos baseando nos trabalhos [Bernstein et al., 2008] [Canteaut and Sendrier, 1998]. A divisão da seção é dada a seguir.

1 Definição (2 páginas)
2 Redução de segurança (2 páginas)
3 Sobre a segurança do esquema (2 páginas)

3.5 Códigos de Goppa quase p-ádicos

É apresentada a classe dos Códigos de Goppa quase p-ádicos para a redução de chave pública no criptossistema de McEliece [Misoczki, 2013] [Misoczki and Barreto, 2009]. Mostramos a sua definição e explicitamos como contruí-los. A exposição seguirá a de [Misoczki, 2013]. Citamos o ataque por criptanálise algébrica [Faugere et al., 2010], e mostramos a sugestão de defesa contra esse ataque. Consideramos aspectos de implementação [Heyse, 2011]. A divisão da seção é dada a seguir.

1 Definição (3 páginas)
2 Codificação (1 página)
3 Decodificação (2 páginas)
4 Ataque e Defesa (5 páginas)

3.6 Códigos LDPC

É apresentada a classe dos códigos lineares cujas matrizes de verificação de paridade têm baixa densidade (*Low Density Parity Check Matrix*). Apresentamos a interpretação desses códigos como grafos esparsos e seus algoritmos de codificação e decodificação seguindo as apresentações em [Gallager, 1962] [Misoczki, 2013]. Ao final, mostramos as vulnerabilidades criptográficas dessa família [Shokrollahi et al., 2000]. A divisão da seção é dada a seguir.

1 Definições (1 página)
2 Codificação e Decodificação (2 páginas)
3 Vulnerabilidades (2 páginas)

3.7 Códigos MDPC

São apresentados os códigos lineares cuja matriz de verificação de paridade tem densidade moderada (*Moderate Density Parity Check Matrix*) [Misoczki et al., 2013] e os comparamos com os códigos LDPC. Mostramos como códigos MDPC não sofrem da mesma vulnerabilidade que os LDPC, e discutimos por que parecem ser uma alternativa melhor do que os códigos de Goppa, já que não têm estrutura algébrica. Explicamos como seu uso no esquema de McEliece permite chaves bastante reduzidas, competitivas com as do RSA. A apresentação segue [Misoczki et al., 2013] e [Misoczki, 2013]. Consideramos detalhes de implementação [Maurich et al., 2015].

1 Definição (2 páginas)
2 Codificação e Decodificação (1 página)
3 Resultados (4 páginas)

4 Biografias dos Autores

4.1 Routo Terada

Possui graduação em Engenharia Elétrica Eletrônica pela Universidade de São Paulo (1970), mestrado em Matemática Aplicada pela Universidade de São Paulo (1975) e doutorado em Ciência da Computação - University of Wisconsin - Madison (1979). Atualmente é professor titular da Universidade de São Paulo, avaliador de artigos do International Journal of Information Security e do Journal of the Brazilian Computer Society. Tem experiência na área de Ciência da Computação, com ênfase em Criptografia, atuando principalmente nos seguintes temas: segurança de dados, criptografia, algoritmos, criptossistemas e mathematical morphology.

4.2 Thales Paiva (Apresentador)

Mestrando em Ciência da Computação pelo Instituto de Matemática e Estatística da Universidade de São Paulo sob a orientação do Professor Routo Terada. Bacharel em Ciência da Computação pelo mesmo instituto. Tem interesse nas áreas de Teoria de Informação, Criptografia, Teoria de Códigos, e Teoria de Complexidade.

4.3 Gervásio Santos (Apresentador)

Graduando em Ciência da Computação pelo Instituto de Matemática e Estatística da Universidade de São Paulo. Foi aluno de inciação científica na área de Criptografia e Teoria dos Números sob a orientação do Professor Routo Terada. Tem interesse nas áreas de Criptografia, Teoria de Códigos, Álgebra Abstrata, e Teoria da Complexidade.

Referências

[Barreto et al., 2013] Barreto, P. S., Biasi, F. P., Dahab, R., César, J., Pereira, G. C., and Ricardini, J. E. (2013). Introdução à criptografia pós-quântica. *Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais—SBSeg*.

[Berger et al., 2009] Berger, T. P., Cayrel, P.-L., Gaborit, P., and Otmani, A. (2009). Reducing key length of the mceliece cryptosystem. In *Progress in Cryptology–AFRICACRYPT 2009*, pages 77–97. Springer.

[Berlekamp et al., 1978] Berlekamp, E. R., McEliece, R. J., and Van Tilborg, H. C. (1978). On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386.

[Bernstein et al., 2009] Bernstein, D. J., Buchmann, J., and Dahmen, E. (2009). *Post-quantum cryptography*. Springer Science & Business Media.

[Bernstein et al., 2008] Bernstein, D. J., Lange, T., and Peters, C. (2008). Attacking and defending the mceliece cryptosystem. In *Post-Quantum Cryptography*, pages 31–46. Springer.

[Biswas and Sendrier, 2008] Biswas, B. and Sendrier, N. (2008). Mceliece cryptosystem implementation: Theory and practice. In *Post-Quantum Cryptography*, pages 47–62. Springer.

[Canteaut and Sendrier, 1998] Canteaut, A. and Sendrier, N. (1998). Cryptanalysis of the original mceliece cryptosystem. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 187–199. Springer.

[Engelbert et al., 2007] Engelbert, D., Overbeck, R., and Schmidt, A. (2007). A summary of mceliece-type cryptosystems and their security. *J. Mathematical Cryptology*, 1(2):151–199.

[Faugere et al., 2010] Faugere, J.-C., Otmani, A., Perret, L., and Tillich, J.-P. (2010). Algebraic cryptanalysis of mceliece variants with compact keys. In *Advances in Cryptology–Eurocrypt 2010*, pages 279–298. Springer.

[Fraleigh, 2003] Fraleigh, J. B. (2003). *A first course in abstract algebra*. Pearson Education India.

[Gaborit, 2005] Gaborit, P. (2005). Shorter keys for code based cryptography. In *Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)*, pages 81–91.

[Gallager, 1962] Gallager, R. (1962). Low-density parity-check codes. *IRE Transactions on information theory*, 8(1):21–28.

[Goppa, 1970] Goppa, V. D. (1970). A new class of linear correcting codes. *Problemy Peredachi Informatsii*, 6(3):24–30.

[Heyse, 2011] Heyse, S. (2011). Implementation of mceliece based on quasi-dyadic goppa codes for embedded devices. In *International Workshop on Post-Quantum Cryptography*, pages 143–162. Springer.

[Maurich et al., 2015] Maurich, I. V., Oder, T., and Güneysu, T. (2015). Implementing qc-mdpc mceliece encryption. *ACM Transactions on Embedded Computing Systems (TECS)*, 14(3):44.

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

[Menezes et al., 1996] Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

[Miller, 1986] Miller, V. (1986). Use of elliptic curves in cryptography. *Advances in Cryptology (CRYPTO85)*, pages 417–426.

[Misoczki, 2013] Misoczki, R. (2013). *Two Approaches for Achieving Efficient Code-Based Cryptosystems*. PhD thesis, Université Pierre et Marie Curie-Paris VI.

[Misoczki and Barreto, 2009] Misoczki, R. and Barreto, P. S. (2009). Compact mceliece keys from goppa codes. In *Selected Areas in Cryptography*, pages 376–392. Springer.

[Misoczki et al., 2013] Misoczki, R., Tillich, J.-P., Sendrier, N., and Barreto, P. S. (2013). Mdpc-mceliece: New mceliece variants from moderate density parity-check codes. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2069–2073. IEEE.

[Otmani et al., 2010] Otmani, A., Tillich, J.-P., and Dallot, L. (2010). Cryptanalysis of two mceliece cryptosystems based on quasi-cyclic codes. *Mathematics in Computer Science*, 3(2):129–140.

[R. L. Rivest, 1978] R. L. Rivest, A. Shamir, L. M. A. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

[Shokrollahi et al., 2000] Shokrollahi, A., Monico, C., and Rosenthal, J. (2000). Using low density parity check codes in the mceliece cryptosystem. In *IEEE International Symposium on Information Theory (ISIT 2000)*, page 215.

[Shor, 1997] Shor, P. W. (1997). Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1481–1509.

[Stein et al., 2008] Stein, W. et al. (2008). Sage: Open source mathematical software. *7 December 2009*.

[Van Lint, 2012] Van Lint, J. H. (2012). *Introduction to coding theory*, volume 86. Springer Science & Business Media.