Secure and efficient software implementation of QC-MDPC code-based cryptography

Antonio Guimarães [1] Diego Aranha [2] Edson Borin [1]

[1]University of Campinas

[2]Aarhus University

Abstract. The emergence of quantum computers is pushing an unprecedented transition in the public key cryptography field. Conventional algorithms, mostly represented by elliptic curves and RSA, are vulnerable to attacks using quantum computers and need, therefore, to be replaced. Cryptosystems based on error-correcting codes are considered some of the most promising candidates to replace them for encryption schemes. Among the code families, QC-MDPC codes achieve the smallest key sizes while maintaining the desired security properties. Their performance, however, still needs to be greatly improved to reach a competitive level. In this work, we focus on optimizing the performance of QC-MDPC code-based cryptosystems through improvements concerning both their implementations and algorithms. We first present a new enhanced version of QcBits' key encapsulation mechanism, which is a constant time implementation of the Niederreiter cryptosystem using QC-MDPC codes. In this version, we updated the implementation parameters to meet the 128-bit quantum security level, replaced some of the core algorithms avoiding slower instructions, vectorized the entire code using the AVX 512 instruction set extension and introduced some other minor improvements. Comparing with the current state-of-the-art implementation for QC-MDPC codes, the BIKE implementation, our code performs 1.9 times faster when decrypting messages. We then optimize the performance of QC-MDPC code-based cryptosystems through the insertion of a configurable failure rate in their arithmetic procedures. We present constant time algorithms with a configurable failure rate for multiplication and inversion over binary polynomials, the two most expensive subroutines used in QC-MDPC implementations. Using a failure rate negligible compared to the security level (2^{-128}), our multiplication is 2 times faster than the one used in the NTL library on sparse polynomials and 1.6 times faster than a naive constant-time sparse polynomial multiplication. Our inversion algorithm, based on the inversion algorithm of Wu et al., is 2 times faster than the original and 12 times faster than the inversion algorithm of Itoh and Tsujii using the same modulus polynomial ($x^{32749} - 1$). By inserting these algorithms in our enhanced version of QcBits, we were able to achieve a speedup of 1.9 on the key generation and up to 1.4 on the decryption time. Comparing with BIKE, our final version of QcBits performs the uniform decryption 2.7 times faster. Moreover, the techniques presented in this work can also be applied to BIKE, opening new possibilities for further improvements.

Resumo. A expectativa do surgimento de computadores quânticos impulsiona uma transição sem precedentes na área de criptografia de chave pública. Algoritmos convencionais, representados principalmente por criptografia baseada em curvas elípticas e pelo RSA,são vulneráveis a ataques utilizando computadores quânticos e, portanto, precisarão ser substituídos. Cripto sistemas baseados em códigos corretores de erros são considerados alguns dos candidatos mais promissores para substituí-los em esquemas de encriptação.Entre as famílias de códigos, os códigos QC-MDPC alcançam os menores tamanhos de chave, enquanto mantêm as propriedades de segurança desejadas. Seu desempenho,no entanto, ainda precisa ser melhorado para atingir um nível competitivo.Este trabalho tem ênfase na otimização do desempenho dos cripto sistemas baseados em código QC-MDPC através de melhorias em suas implementações e algoritmos. Primeiramente, é apresentada uma nova versão aprimorada do mecanismo de encapsulamento de chaves da QcBits, uma implementação em tempo constante do Cripto sistema Niederreiter utilizando códigos QC-MDPC. Nesta versão, os parâmetros da implementação foram atualizados para atender ao nível de segurança quântica de 128 bits, alguns dos principais algoritmos foram substituídos para evitar o uso de instruções mais lentas, o código foi inteiramente vetorizado utilizando o conjunto de instruções AVX 512 e outras pequenas melhorias foram introduzidas. Comparando com o atual estado-da-arte para códigos QC-MDPC, a implementação BIKE, a implementação apresentada neste trabalho executa 1,9 vezes mais rápido ao decriptar mensagens.Em seguida, foca-se na otimização de desempenho dos sistemas criptográficos baseados em códigos QC-MDPC por meio da inserção de uma taxa de falhas configurável em seus procedimentos aritméticos. São apresentados algoritmos com execução em tempo constante que aceitam uma taxa de falhas configurável para multiplicação e inversão sobre polinômios binários, as duas subrotinas mais caras utilizadas nas implementações QC-MDPC. Usando uma taxa de falhas negligível comparada ao nível de segurança (2^{-128}), a multiplicação é 2 vezes mais rápida que a multiplicação utilizada pela biblioteca NTL em polinômios esparsos e 1,6 vezes mais rápida que uma multiplicação polinomial esparsa ingênua em tempo constante. O algoritmo de inversão, baseado no algoritmo deWuet al., é 2 vezes mais rápido que o original e 12 vezes mais rápido que o algoritmo de inversão de Itoh e Tsujii utilizando o mesmo polinômio de módulo ($x^{32749} - 1$). Ao inserir esses algoritmos na versão aprimorada da QcBits, atingiu-se uma aceleração de 1,9na geração de chaves e de até 1,4 na decriptação.Comparando com a BIKE, a versão final da QcBits apresentada neste trabalho executa a decriptação uniforme 2,7 vezes mais rápida. Além disso, as técnicas aqui apresentadas também podem ser aplicadas à BIKE, abrindo novas possibilidades de melhorias para cripto sistemas QC-MDPC.