
From: BIDOUX Loic <loic.bidoux@worldline.com>
Sent: Friday, December 14, 2018 11:05 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: RQC

Dear all,

We have conducted a study on the resistance of RQC to timing attacks which is available at <http://pqc-rqc.org/doc/rqc-constantTime.pdf>

Abstract: This paper studies the resistance of the code-based encryption scheme RQC to timing attacks. We describe two chosen ciphertext timing attacks that relies on a correlation between the weight of the error to be decoded and the running time of Gabidulin code's decoding. These attacks are of theoretical interest as they outperform the best known algorithm to solve the rank syndrome decoding problem in term of complexity. Nevertheless, they are quite impracticable in real situations as they require a huge number of requests to a timing oracle. We also provide a constant-time algorithm for the decoding of Gabidulin codes that prevent these attacks without any performance cost for honest users.

An additional implementation including the aforementioned algorithm will be added later. This implementation should be seen as the first step of an effort to provide a constant time version of RQC.

Sincerely,
The RQC team

!!!*****

"Ce message et les pièces jointes sont confidentiels et réservés à l'usage exclusif de ses destinataires. Il peut également être protégé par le secret professionnel. Si vous recevez ce message par erreur, merci d'en avvertir immédiatement l'expéditeur et de le détruire. L'intégrité du message ne pouvant être assurée sur Internet, la responsabilité de Worldline ne pourra être recherchée quant au contenu de ce message. Bien que les meilleurs efforts soient faits pour maintenir cette transmission exempte de tout virus, l'expéditeur ne donne aucune garantie à cet égard et sa responsabilité ne saurait être recherchée pour tout dommage résultant d'un virus transmis.

This e-mail and the documents attached are confidential and intended solely for the addressee; it may also be privileged. If you receive this e-mail in error, please notify the sender immediately and destroy it. As its integrity cannot be secured on the Internet, the Worldline liability cannot be triggered for the message content. Although the sender endeavours to maintain a computer virus-free network, the sender does not warrant that this transmission is virus-free and will not be liable for any damages resulting from any virus transmitted.!!!"