
| | |
|---|---|
| **Evento** | Salão UFRGS 2018: SIC - XXX SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS |
| **Ano** | 2018 |
| **Local** | Campus do Vale - UFRGS |
| **Título** | Sistema de criptografia Matsumoto-Imai |
| **Autor** | BRUNO PERIN BENEDETTI |
| **Orientador** | JULIANE GOLUBINSKI CAPAVERDE |

Título: Sistema de criptografia Matsumoto-Imai
Autor: Bruno Perin Benedetti
Orientadora: Juliane Golubinski Capaverde
Instituição de Origem: Universidade Federal do Rio Grande do Sul (UFRGS)

A imensa maioria dos sistemas de criptografia utilizados na atualidade são baseados na dificuldade de se fatorar inteiros, porém com a existência de um computador quântico, essa dificuldade será superada. Então os pesquisadores começaram a buscar outras dificuldades computacionais para basearem seus sistemas, dificuldades que ainda não foram superadas nem por algoritmos quânticos, a dificuldade que iremos focar será na de se encontrar soluções para sistemas de equações polinomiais multivariadas.

Dentre os sistemas de criptografia baseados nessa dificuldade, os notórios têm sua base no sistema de criptografia Matsumoto-Imai. Será então apresentado o funcionamento desse sistema, assim como sua importância. E por fim, demonstraremos através de um ataque sobre ele, o porquê dele ser obsoleto, por mais que nele se baseiem os sistemas de criptografia (por hora) bem sucedidos.