330 **TÉCNICAS DE PROTEÇÃO DE DADOS CRIPTOGRAFADOS.** *Aquiles Macedo Dias, Ricardo Augusto da Luz Reis (orient.)* (UFRGS).

Sistemas de criptografia estão se tornando cada vez mais importantes e presentes no nosso dia-a-dia. A criptografia permite que as pessoas tenham no mundo eletrônico a segurança do mundo real, permitindo a realização de negócios eletronicamente sem preocupações com fraudes ou enganos. Todo dia centenas de milhares de pessoas interagem eletronicamente, seja através de e-mail, comunicação de redes com segurança, comércio eletrônico, caixa automático, entre outros. O constante crescimento de informações transmitidas eletronicamente tem levado a um aumento na utilização da criptografia. Ao mesmo tempo em que algoritmos de criptografia são desenvolvidos, técnicas para a quebra desses têm sido estudadas com o objetivo de obter as informações confidenciais que estão contidas nesses serviços. Os principais tipos de ataques a circuitos de criptografia são: 1. Side channels - que se baseiam em leakages (non-invasive/passive). 2. Fault attacks - que modificam o funcionamento do dispositivo. Algumas técnicas têm sido apresentadas com o objetivo de proteger os circuitos de criptografia contra esses ataques. Técnicas de proteção desses circuitos de criptografia foram desenvolvidas em vários níveis de abstração. O trabalho em desenvolvimento consiste em investigar métodos de proteção de circuitos ao nível de layout.