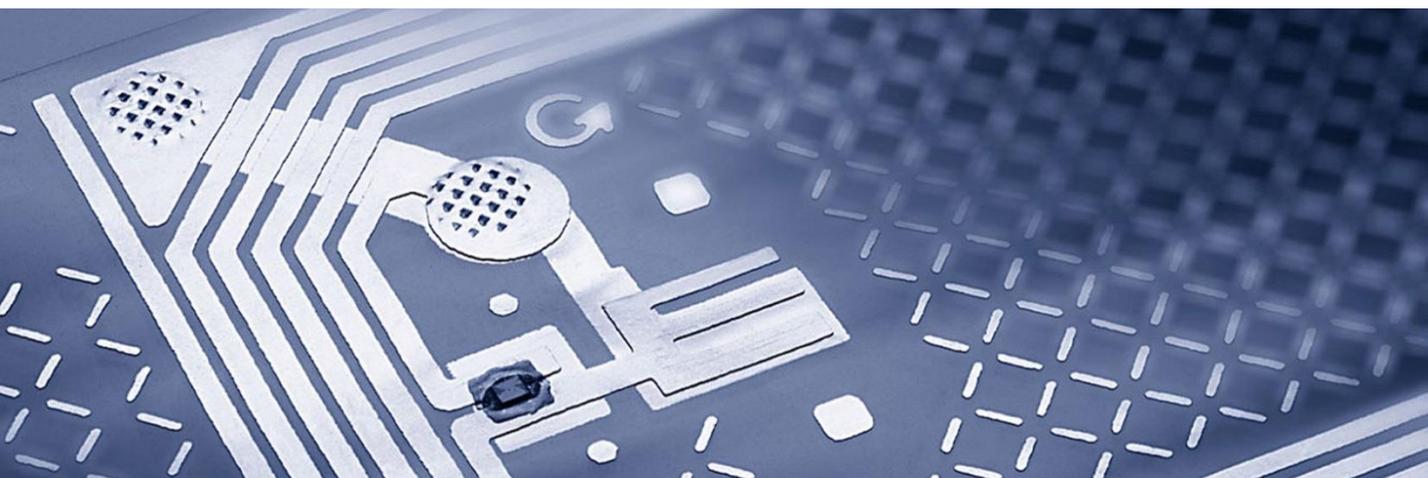


Dispositivo para Autenticação de RFID's



Pesquisadores da Unicamp desenvolveram um PUF (Physical Unclonable Function) capaz de autenticar de maneira segura e barata dispositivos com consumo de potência crítico, como os RFID's. Além do PUF, foi desenvolvido um método de captura para identificação e um circuito integrado para implementação, do PUF.

Pode ser aplicada em:

- Autenticação de dispositivos **RFID** e energy harvesting
- Autenticação de dispositivos móveis e portáteis, e smartcards
- Geração de chaves para sistemas criptográficos

Os diferenciais desta tecnologia são:

- Menor área de silício, com quantidade de hardware 5 vezes menor do que o Arbiter PUF (APUF)
- Menor custo para RFID's com PUF
- Menor consumo de potência comparado ao APUF
- Menor número de desafios para a autenticação comparado ao APUF (comunicação mais curta)
- Diminuição de erros de reconhecimento por ter maior imprevisibilidade de respostas.

STATUS DA PATENTE

Pedido de patente de invenção depositado junto ao INPI.

CÓDIGO INTERNO

697_AUTENTICACAO

MAIS INFORMAÇÕES:

parcerias@inova.unicamp.br

Tel: (19) 3521.2607 / 2612

(19) 3521.5012 / 2552

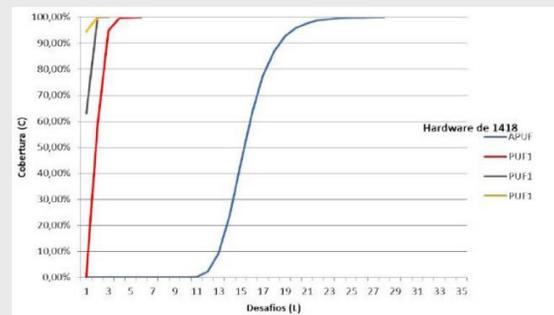


Autenticação de dispositivos através de PUF (Physical Unclonable Function)

A autenticação de dispositivos através de métodos criptográficos possui aplicação limitada, pois demandam muita energia e área de circuito, não sendo facilmente aplicáveis em dispositivos *power harvesting* e RFID. O PUF (*Physical Unclonable Functions*) é uma solução. Funciona como uma impressão digital para dispositivos eletrônicos e é capaz de levar a outro patamar a segurança no uso de dispositivos eletrônicos. O PUF possui baixo gasto de potência para fazer a autenticação e apresentam diversas vantagens em relação à segurança, tornando improvável a falsificação do RFID e altamente seguro seu método de autenticação.

O custo de RFID's é muito sensível à área de circuito o que muitas vezes inviabiliza seu uso mais intensivo. Nessa direção pesquisadores da Unicamp desenvolveram um PUF que além de possuir desempenho superior à modelos comerciais, possui **reduzida área e gasto de potência**, sendo ainda mais apto para aplicação em RFID's.

Foi comprovado experimentalmente que o PUF desenvolvido utiliza 5 vezes menos hardware e necessita de menos pares de desafio-resposta para a autenticação (gráfico). Além disso o PUF proposto apresenta para um aumento de hardware linear um aumento exponencial da imprevisibilidade das respostas diminuindo as chances de erros de reconhecimento.



Esse gráfico demonstra que o APUF (em azul) precisa de maior número de desafios do que o PUF da presente tecnologia para a autenticação. (Hardware de 1418 transistores)

Pesquisador Responsável:

Mário Lúcio Côrtes

Possui graduação em Engenharia Eletrônica pelo Instituto Tecnológico de Aeronáutica (1973), mestrado em Engenharia Elétrica pela Universidade de São Paulo (1980) e doutorado em Electrical Engineering - Stanford University (1987). Trabalhou na Fundação Centro de Pesquisa e Desenvolvimento em Telecomunicações como pesquisador e gerente de qualidade no período 1987 a 2010. Professor Associado do Instituto de Computação da Universidade Estadual de Campinas, com ingresso em 1991. Tem experiência na área de Ciência da Computação, com ênfase em Arquitetura de Sistemas de Computação, atuando principalmente nos seguintes temas: engenharia de software, projeto e teste de circuitos VLSI e arquitetura de computadores.



A equipe responsável pela invenção é composta por: Mário Lúcio Côrtes, Guido Costa Souza de Araújo e Marcelo Fontes Santana.