

Trabalhos curtos aceitos na trilha principal SBSeg 2018

A Receipt-Free i-Voting System Based on Blind Signatures and Anonymous IDs

Charles Figueredo de Barros (UFSJR - Brazil), Diego Freire Pimenta (UFSJR - Brazil)

Preservando a Privacidade na Internet das Coisas com Pseudônimos Usando SDN

Antônio Janael Pinheiro (UFPE - Brazil), Caio Burgardt (UFPE - Brazil), Divanilson Campelo (UFPE - Brazil)

White Box Implementations of Dedicated Ciphers on the ARM NEON Architecture

Ricardo Dahab (UNICAMP - Brazil), Julio Hernandez (UNICAMP - Brazil), Félix Rodrigues (UNICAMP - Brazil), Hayato Fujii (UNICAMP - Brazil), Giuliano Sider (UNICAMP - Brazil), Ana Clara Zoppi Serpa (UNICAMP - Brazil)

Proposta de implementação do algoritmo SHA-256 em Hardware

Carlos Eduardo Santos Júnior (EBSERH-UFRN - Brazil), Marcelo A. C. Fernandes (UFRN - DCA - Brazil)

Implementation of the SHA-3 family using AVX512 instructions

Roberto Filho (UNICAMP - Brazil), Julio Hernandez (UNICAMP - Brazil)

Avaliação de mecanismos de consenso para blockchains em busca de nova estratégia mais eficiente e segura

Yoshitomi Maehara Aliaga (UNICAMP - Brazil), Marco Aurelio Amaral Henriques (FEEC - Unicamp - Brazil), Antônio Lucena (Unicamp - Brazil), Victor Leal (University of Campinas - Brazil)

Privacy-preserving recommendations for Online Social Networks using Trusted Execution Environments

Luiz Celso Gomes Jr (UTFPR - Brazil), Guilmour Rossi (UTFPR - Brazil), Keiko Fonseca (UTFPR - Brazil), Marcelo Rosa (UTFPR - Brazil)

Finite Field Arithmetic Using AVX-512 For Isogeny-Based Cryptography

Gabriell Orisaka (UNICAMP - Brazil), Julio Hernandez (UNICAMP - Brazil), Diego Aranha (Aarhus University - Denmark)



SBSeg2018

XVIII SIMPÓSIO BRASILEIRO
EM SEGURANÇA DA INFORMAÇÃO
E DE SISTEMAS COMPUTACIONAIS
22 a 25 de Outubro | Natal | RN

2-Isogenies Between Elliptic Curves in Hesse Model

João Paulo da Silva (UNICAMP - Brazil), Ricardo Dahab (UNICAMP - Brazil), Julio Hernandez (UNICAMP - Brazil)

Securing IoT Apps with Fine-grained Control of Information Flows

Davino Junior (UFPE - Brazil), Kiev Gama (CIn-UFPE - Brazil), Atul Prakash (University of Michigan, Ann Arbor - USA)

Estudo preliminar da adoção de assinaturas baseadas em hash no blockchain do Bitcoin

Antônio Lucena (Unicamp - Brazil), Marco Aurelio Amaral Henriques (FEEC - Unicamp - Brazil)

Avaliação do custo/benefício da adoção de autômatos celulares na geração de números pseudoaleatórios do Linux

Sílvia Magossi (Unicamp - Brazil), Marco Aurelio Amaral Henriques (FEEC - Unicamp - Brazil)

On the Use of New Blockchain-based Technologies for Securely Distributing Data

Gustavo Alves (UFRN - Brazil), Thais Vasconcelos Batista (UFRN - Brazil), Everton Cavalcante (UFRN - Brazil)

Secure Cloud Processing for Smart Meters Using Intel SGX

MARCOS VINICIUS ARAUJO (UFRJ - Brazil), Charles Prado (Inmetro - Brazil), Luiz Fernando Rust da Costa Carmo (Inmetro - Brazil), Alvaro Rincon (UFRJ - Brazil), Claudio Farias (NCE/UFRJ - Brazil)

DmzVisor: um Firewall para a Segurança de Zona Desmilitarizada Corporativa em Redes Definidas por Software

Ygor de Sena (UFRPE - Brazil), Valson da Silva Pereira (UFRPE - Brazil)

An Adaptive Anti-DDoS System for IP Service Provider Backbones

Alberto Rodrigues (UFF - Brazil), Fábio dos Santos (UFF - Brazil), Marcos Oliveira (UFF - Brazil), Natalia Fernandes (UFF - Brazil)

Realização



Patrocínio

