CONCURSO PARA ATRIBUIÇÃO DE BOLSA(s)

Cargo/posição/bolsa:

Referência:	AE2018-0344 (INESC TEC LA - HASLAB)
	INESC TEC - Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência
Cargo/posição/bolsa:	Investigação (BI)
Localidade:	HASLab, Departamento Informática, Campus de Gualtar, Universidade do Minho, Braga
Área científica:	Genérica: COMPUTER SCIENCE
	Específica:

Resumo do anúncio:

O INESC TEC abre concurso para a atribuição de 1 Bolsa(s) de Investigação para Mestre .

Projeto:	INESC TEC - EEA/50014 (POCI-01-0145-FEDER-006961)
Orientador Científico:	José Manuel Valença
Duração da bolsa:	de 2019-01-01 a 2019-12-31 (12)
Local de trabalho:	HASLab, Departamento Informática, Campus de Gualtar, Universidade do Minho, Braga

Texto do anúncio:

Área de trabalho: Criptografia

Descrição do Trabalho: Um objetivo é descrever uma generalização da c. linear nessa com diagramas comutativos, vendo que condições são necessárias para obter segurança. Também se pode analisar o comportamento das cifras do ponto de vista computacional: a noção de hashes aleatórios liga a complexidade computacional com as propriedades de unidirecionalidade que caracterizam as funções de hash criptograficamente seguras. Outro objetivo é avaliar a exequibilidade de ligar este tipo de análise a cifras simétricos.

Objetivos: Generalizar a c. linear, utilizando matrizes de difusão. Pôr este ataque numa framework de diagramas comutativos que já engloba alguns dos ataques clássicos, e ver se daqui surgem direções para novos possíveis ataques. Modelar dois tipos de falhas das cifras: leaking da chave, e leaking do plaintext. Analisar (com oráculos) a relação entre a (in)segurança da primitiva com o oráculo verificar (ou não) uma propriedade designada de "lowness".

Habilitações académicas:	Mestrado em Engenharia Informática
Requisitos mínimos:	Mestrado em Engenharia Informática
Fatores de preferência:	Sólidos conhecimentos de algebra, matemática discrete. Experiência com programação em C e Python. Experiência prévia na análise de construções criptográficas.
Valor mensal da bolsa:	€ 980,00 (Mestrado) conforme tabela de valores das bolsas atribuídas diretamente pela FCT , pago por transferência bancária, podendo o bolseiro auferir remunerações adicionais, pelo envolvimento em contratos ou projectos complementares que contribuam para o plano de trabalhos (Artºs 12º e 13º do Regulamento de Bolsas INESC TEC e Anexo II) em conformidade com o nº4 do Artº 5º do Estatuto do Bolseiro - Lei Nº 40/2004, de 18 de Agosto, até um limite máximo de 50% do valor mensal da bolsa.

Duração do Projeto:	-
Entidade Financiadora:	Financiado por Fundos FEDER através do Programa Operacional Competitividade e Internacionalização - COMPETE 2020 e por Fundos Nacionais (PIDDAC) através da FCT/MCTES, no âmbito do projeto POCI-01-0145-FEDER-006961 .

A contratação será regida pelo estipulado na legislação em vigor relativa ao Estatuto do Bolseiro de Investigação , aprovado pela Lei nº 40/2004, de 18 de Agosto, alterado e republicado pelo Decreto-Lei nº 202/2012, de 27 de agosto e alterado pelo Decreto-Lei nº 233/2012, de 29 de outubro e pela Lei nº 12/2013, de 29 de janeiro, e Decreto-Lei nº 89/2013 de 9 de julho, bem como pelo Regulamento de Bolsas INESC TEC , aprovado pela Fundação para a Ciência e a Tecnologia em 12 de janeiro de 2011 e pelo Regulamento de Bolsas de Investigação da FCT em vigor .

Para mais informações consultar o Regulamento de Bolsas INESC TEC e respetivos anexos em www.inesctec.pt/bolsas

Métodos de avaliação: Avaliação curricular baseada nos critérios referidos no Art.º 7º do Regulamento de Bolsas INESC TEC e incluirá entrevista individual na fase final do processo de seleção, com a respetiva valoração 80 % avaliação curricular (50 % Curriculum, 15 % Domínios científicos e 15 % Experiência) e 20 % Entrevista .Só serão chamados para a entrevista os candidatos que obtiverem no mínimo 70% na avaliação curricular (CV + Domínio Científico + Experiência).

Júri de Seleção:	Presidente do Júri: Prof. José Manuel Valença ; Vogal: Prof. José Bacelar Almeida ; Vogal: Prof. Alcino Cunha ;
Notificação dos resultados:	Os resultados do processo de seleção serão divulgados aos interessados por correio eletrónico, nos termos referidos no Artº 8º do Regulamento de Bolsas INESC TEC .
Período de candidatura:	De 2018-11-21 a 2018-12-04
Submissão candidaturas:	Preenchimento de formulário eletrónico em www.inesctec.pt na secção SEJA NOSSO COLABORADOR , anexando Curriculum Vitae, certificado de habilitações ou outros documentos comprovativos relevantes para a apreciação final.

COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional FCT Fundação para a Ciência e a Tecnologia