

# **FSE 2012 best papers**

**Anne Canteaut**

INRIA (France) and DTU (Denmark)

20 March 2012

## Three best papers

- *Improved Rebound Attack on the Finalist Grøstl*  
by Jérémy Jean, María Naya-Plasencia and Thomas Peyrin.
- *New attacks on Keccak-224 and Keccak-256*  
by Itai Dinur, Orr Dunkelman and Adi Shamir.
- *Recursive Diffusion Layers for Block Ciphers and Hash Functions*  
by Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala and Pouyan Sepehrdad.

will receive a solicitation from the editor-in-chief of the *Journal of Cryptology* to submit an extended version of their paper.