



Cost IC1306 CryptoAction

Aim: promotion of movement of ideas and people between European research centers

Participants: anyone from one of the 30 COST countries

Research meetings before Eurocrypt (Sunday April 26) in Sofia

- protocol analysis
- implementation and formal verification
- authenticated encryption

Free but registration is required

A limited number of stipends available **Deadline: March 11 (tomorrow)**



Cost Action IC1306

Working Group 3: Implementation and Verification

Two presentation/discussion sessions covering:

- **Efficient implementation of quasi-practical crypto.**
- **Side-channel attacks: recent developments and theory vs practice.**

Organizer: Manuel Barbosa (mbb@di.uminho.pt)

Working Group 4: Cryptographic primitives

- **Presentations/discussions on recent results on AE and Caesar**
- **Cryptanalysis work in small groups on some CAESAR candidates**

Organizer: Anne Canteaut (anne.canteaut@inria.fr)



Short-Term Scientific Missions

For PhD students and postdocs from a home institution in a COST participating country to a host institution in another COST participating country

- **Duration:** 5 days - 90 days
- **Financial support:** 60-90 Euros / day + 300 Euros for travel

<http://cryptoaction.eu>