

# Research Group Summary

UK Open Rights Group  
European e-Voting Activism Workshop  
Sharing & Learning across Europe

Joe Kiniry  
8 February 2007



# Background and Perspective

- ✧ Systems Research Group
  - ✧ founded by Prof. Paddy Nixon, Dr. Simon Dobson, and Dr. Joe Kiniry in Oct, 2004 and has now grown to just over 40 researchers
  - ✧ SRG postdoc Dr. Lorcan Coyle (with Dr. Donal Doyle, led by Prof. Pádraig Cunningham, now at UCD) twice performed the black-box testing of the PowerVote system for the CEV
  - ✧ my primary research in *applied formal methods*
    - ✧ heavy focus on shipping FLOSS systems with strong formal foundation that help developers



# Background

- ✧ KSR led by Dr. Joseph Kiniry (Ph.D. Caltech)
  - ✧ correctness and security research, development, and consulting for ~15yrs
- ✧ some previous work in security R&D
  - ✧ reverse-engineering various smart card protocols, filesystems, programs, and security systems
  - ✧ verification of deployed commercial smart card-based software systems (mainly major financial institutions)



# Current Work

- ✧ P.I. of Mobius: E.U. FP6 IST FET project
  - ✧ type- and logic-based verification of COTS concurrent software (Java VM) with proof-carrying code
- ✧ P.I. of Lero: the Irish Software Engineering Research Centre
  - ✧ formal methods in model-driven architectures within software product lines for automobile industry



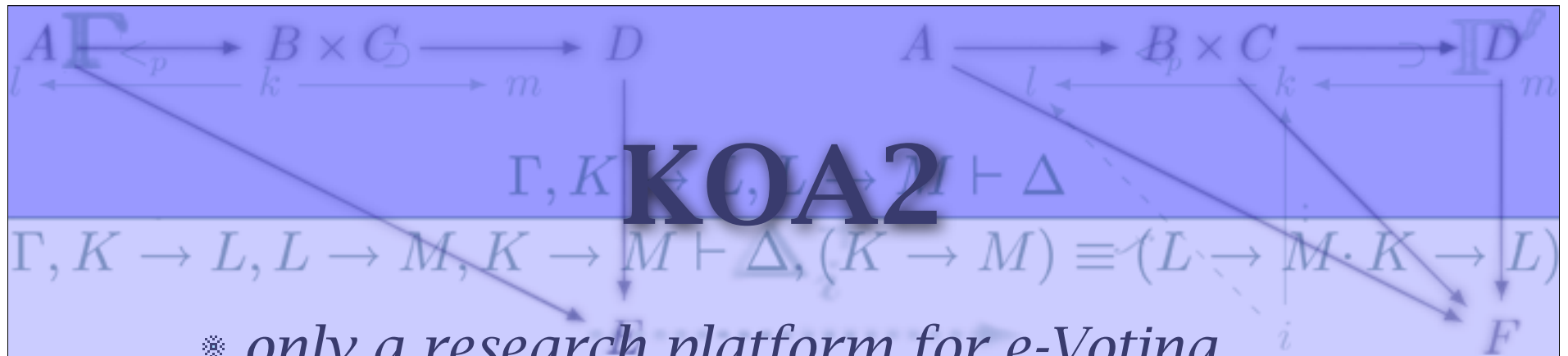
# e-Voting in NL

- ✧ mapped, probed, and attacked KOA beta
- ✧ led security evaluation of KOA
- ✧ author of CEV-like report to Parliament
- ✧ co-lead of formal methods-based development of a new tally system for KOA
- ✧ helped convince NL government to release KOA under GPL
  - ✧ all above work with Prof. Bart Jacobs, Dr. Martijn Oostdijk, Dr. Engelbert Hubbers, and Dr. Cees-Bart Breunesse

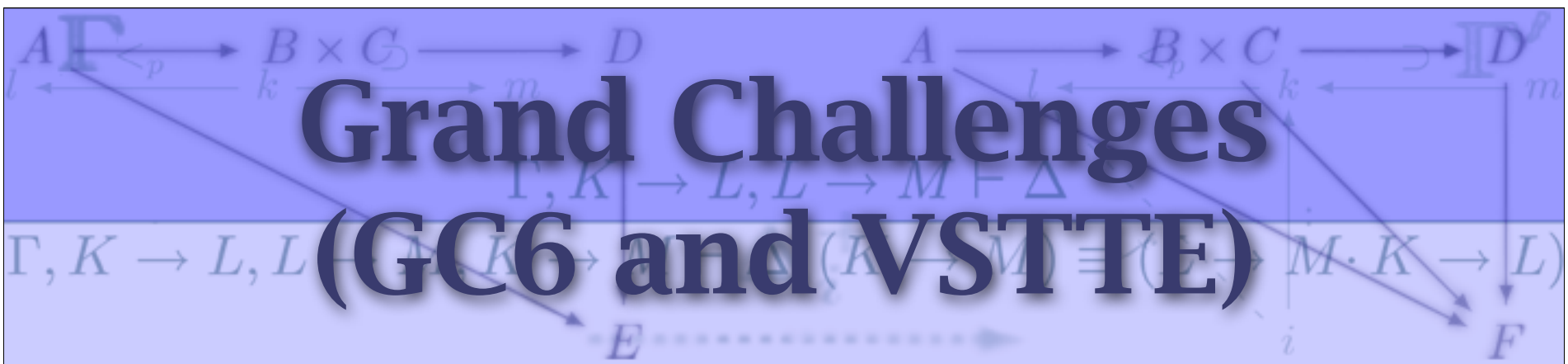


# e-Voting in IE

- ✧ asked to participate in Irish CEV in 2004, then uninvited because I would not budge
- ✧ asked to participate in IE corporate bid on verification of PowerVote software
- ✧ reverse engineered of “missing” KOA parts (with Alan Morkan)
- ✧ critical post mortem of NL tally software (with Fintan Fairmichael)
- ✧ formal specification of IE vote counting system (using JML and ESC/Java2 and implementation underway using DBC (with Dermot Cochran and Patrick Tierney)



- ✧ *only a research platform for e-Voting*
- ✧ now runs on an entirely FLOSS foundation
- ✧ nearly all documentation translated from Dutch to English
- ✧ many parts of the system now have formal specifications
- ✧ vote setup, execution, and tally being refactored into pluggable modules
- ✧ first non-NL module is IE system under dev



# Grand Challenges (GC6 and VSTTE)

- ✧ have been working within the verification community to excite them about e-Voting
- ✧ e-Voting has been adopted as one of four key case studies in GC6 initiative
  - ✧ researchers are interested in more than encryption and verification, they wish to model and reason about *entire process*
- ✧ am lobbying the same should be done for a new E.U. FP7 proposal underway