REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
06/30/2010	Final Technical Report	01 Mar 2006 - 31 Dec 2009

4. TITLE AND SUBTITLE
Probabilistic Models and Interoperability, Pervasive Computing and Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N00014-06-1-0284

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Michael W. Mislove

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Tulane University - Uptown
6823 St. Charles Ave.
New Orleans, LA 70118

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research
Reg Admin Atlanta - N66020
100 Alabama St., SW Suite 4R15
Atlanta, GA 30303-3104

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Reports and publications are publicly available with no restrictions.

13. SUPPLEMENTARY NOTES
None

20111128001

14. ABSTRACT
The research supported under this grant has two main focuses: first, modeling security protocols, and second, devising new domain-theoretic models for probabilistic phenomena. In the first area, we developed a new approach to modeling probabilistic input/output automata, originally devised by Canetti, Lynch, Segala et al, and new applications of these automata in security, specifically to the area of anonymity. In the second area, we devised new models combining probability and nondeterminism, and used this approach to provide an alternative development of the indexed valuations of Daniele Varacca. An important application of this is the development of the only known CCC supporting probabilistic choice.

15. SUBJECT TERMS
Crypto-protocols, probabilistic automata, domain theory, Cartesian closed category

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Michael W. Mislove
U	U	U	UU		19b. TELEPHONE NUMBER *(Include area code)* (504) 862-3441

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATE COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33315-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report. e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

ONR Final Technical Report
Award #N00014-06-1-0284
3/1/06 - 12/31/09
"Probabilistic Models and Interoperability, Pervasive Computing and Security"

NAME OF PI: Michael Mislove

UNIVERSITY/Contractor:
Tulane University

TITLE OF PROJECT: Probabilistic Models and Interoperability, Pervasive Computing and Security

GRANT/CONTRACT/WORK REQUEST NUMBER:
N00014-99-1-0150

1. Papers published in referred journals (TITLE; JOURNAL):

1) Discrete random variables over domains, Theoretical Computer Science **380** (2007), pp. 181--198
2) Monoids over domains, Mathematical Structures for Computer Science **16** (2006), pp. 255--277.

2. Papers published in conference proceedings (TITLE; JOURNAL):

1) Testing semantics: Connecting processes and logics, Proceedings AMAST 2006, LNCS **4019** (2006), pp. 308--322
2) On combining probability and nondeterminism, ENTCS **162** (2006), pp. 261--265

3. Books or Book chapters published (TITLE; AUTHORS/EDITORS; PUBLISHER):

1) Labeled Markov processes as generalized stochastic processes, in: Computation, Meaning and Logic, Articles Dedicated to Gordon Plotkin, ENTCS **172** (2007), pp. 459--478

4. Proceedings Edited (TITLE; AUTHORS/EDITORS; PUBLISHER):

1) Proceedings of MFPS 25, ENTCS **249** (2009), with S. Abramsky and C. Palamidessi
2) Proceedings of MFPS 24, ENTCS **218** (2008), with A. Bauer
3) Proceedings of Clifford Lectures and MFPS 18, Theoretical Computer Science **357** (2006), with S. Artemov.
4) Proceedings of MFPS 22, ENTCS **158** (2006), with S. Brookes.
5) Proceedings of MFPS 21, ENTCS **155** (2006), with M. Escardo and A. Jung

5. Patents (ANNOTATE EACH WITH FILED OR GRANTED):

None

8. Presentations (INVITED):

1) Random bits of noise, MFPS 25, Oxford, UK, May, 2009
2) Modeling security with PIOAs, Protocol eXchange Meeting, NPS, Monterey, CA, January, 2009
3) Task Probabilistic Input/Output Automata as domains, Fourth FCC Workshop, CMU, June,

2008

4) Probabilistic Input/Output Automata as domains, Oxford University, Oxford, UK, November, 2007
5) Probabilistic Input/Output Automata as Domains, LIX, Ecole Polytechnique, November, 2007
6) Domains and random variables, Conference on Emerging Trends in Concurrency, November, 2007
7) Domains and random variables, Conference Honoring Peter Collins and G. M. Reed, University of Oxford, August, 2006

8. Presentations (CONTRIBUTED):

1) New Orleans After Katrina, MFPS 24, University of Genoa, Italy, May, 2006.

8. **Summary of Research Accomplishments:**

The research supported under this grant has two main focuses: first, modeling security protocols, and second, devising new domain-theoretic models for probabilistic phenomena. In the first area, work was undertaken to provide a better understanding of the use of *probabilistic input/output automata* as models for crypto-protocols. This approach, originally devised by Ran Canetti, Nancy Lynch and Roberto Segala, among others, provides a novel mechanism for analyzing crypto-protocols, including reasoning about the cryptographic primitives used to achieve security. However, the approach is arcane and difficult to understand. In our work, we have been developing a domain-based approach to constructing and analyzing such automata. We have made significant progress in unraveling the structure of these as models for security, and we also have devised new applications of them to the area of anonymity. The results of this work is partly reflected in the publications and presentations listed above, but the most significant advances have only recently been achieved. For this reason, this work continues under current grant funding.

The second area of research focused on models for probability, and in particular how to present probabilistic models that also supported the incremental approach typical of domain models of computational processes. Our work here is included in the papers on monoids over domains and the one on domain models for discrete random variables. Both of these papers were inspired by work of Daniele Varacca, who devised a model of probability-like processes that obeyed certain categorical laws that made them more amenable to systematic analysis. Our work gave a new approach to devising Varacca's models, using domain theory, an approach that clarifies the structure of the models. In addition, the discrete random variables paper gives the only known model that combines probability and nondeterminism in a Cartesian closed category.

Another facet of the work was on labeled Markov processes, reported in the conference paper 8) above, in which the earlier work on probability and nondeterminism was picked up again in the context of labeled Markov processes. The main result shows how the labeled Markov process theory gives rise to an operational model for a simple process calculus which extends Milner's CCS with probabilistic choice, and in which this operational model qua bisimulation relation has the earlier domain-theoretic model for nondeterminism and probabilistic choice as a fully abstract denotational model.

The final aspect of research to report on this contract is reported in the book chapter on labeled Markov processes as generalized stochastic processes. The main result of that work is a duality theory for these processes, which allows for a better understanding of their structure and their behavior.

7. Honors (Presidential YIP, elections to Fellow status in major scientific society; appointed editor of scientific journal, elected NAS/NAE/IOM, awarded medal by scientific society, Chairman of scientific meeting, etc): 1) Listed in *Who's Who in America, Who's Who in Science and Engineering.* 2) Named Pendergraft Herbert Buchanan Professor, Tulane University, 2006 – 3) Honored with Special Session on the occasion of my 65th birthday, MFPS 25, May, 2006
8. Number of graduate students: 3
9. Number of Post-doctoral students: 1
10. Number of undergraduate students supported: 0
11. Number of under-represented members by group: 0