

# Clinton Bowen

<https://www.torrho.com>  
Clinton.Bowen@gmail.com | 818.687.1941

## EDUCATION

### CAL STATE NORTHRIDGE

MASTERS IN APPLIED MATHEMATICS  
August 2015

BS IN APPLIED MATHEMATICS  
May 2010

## LINKS

 LinkedIn

## SOFTWARE

### LANGUAGES

C  
C++  
C#  
Java  
LaTeX  
Mathematica  
Matlab  
Python  
SQL (MySQL, PostgreSQL, SQLite)  
R

### FRAMEWORKS & LIBRARIES

.NET  
Sage Python  
SciPy  
RSA BSAFE  
Gurobi  
CPLEX  
Django (and GeoDjango)  
PeachFuzz  
American Fuzzy Lop

### DEVELOPMENT OPERATIONS

IC-Agile Certified Professional  
Secure Development Lifecycle  
Practitioner  
DOD Secret Clearance

## SKILLS

### CRYPTOGRAPHY + CYBER-SEC

Engineering Standards  
SME on FIPS 140 to 202 • Cyber-Security  
Framework • SME on Special Publications  
800 Series • RFCs • CNSSPs • DODAF

### SYSTEM ENGINEERING

GPS  
Subject Matter Expert (SME) on C/A and  
CNAV

## EXPERIENCE

### THE MITRE CORPORATION | SENIOR CYBER SECURITY ENGINEER

April 2015 – Present | El Segundo, CA

- Static Analysis Continuous Integration Platform
  - Currently developing a KLEE symbolic execution plug-in for Jenkins CI (Java, Python, C)
  - Extending plug-in development for Summer 2016 to build multiple plug-ins for free open source static analysis tools
- Cyber Command and Control System Software Development
  - Continuing the ongoing development of an operational and infrastructure analysis tool (Ruby, SQL)
- Source Code Vulnerability Review for GPS
  - Provided security assessment to military user equipment C source code with Fortify
  - Performed a FOSS analysis on two military user equipment code bases with Palamida
- System engineering consulting on the modernization effort AEP Ground Segment
  - Gathering technical assessments from various organizations to perform data exchanges via AEP
- Consulting on Key Management Concept of Operations for OCX Ground Segment
  - Providing guidance to sponsor and contract for NSA Type 1 cryptographic key management

### BOOZ ALLEN HAMILTON ENGINEERING SERVICES, LLC |

TECHNOLOGIST

June 2010 – April 2015 | El Segundo, CA

- Directing weekly technical meetings between a team of software developers and clients for project management
  - Capture customer input into software development and system engineering requirements and tasks
  - Provide schedule and progress of software development & system engineering tasks and backlog items
  - Illustrate and present system designs and constraints to customers in DOD Architectural Framework formats
  - Prioritize software development tasks for software development team
- Provides mentorship for software development interns
  - Issue tasks for interns
  - Provide guidance for completion of tasks

## COURSEWORK

### GRADUATE

Markov Chains  
Measure Theory  
Partial Differential Equations (PDEs)  
Regression Analysis  
Functional Analysis  
Point Set Topology  
Numerical Methods for Interpolation  
Numerical Methods for PDEs  
Mathematical Modeling

### COURSERA

Discrete Optimization (2014)  
Linear and Discrete Optimization (2014)  
Cryptography I (2016)  
Cryptography II (2017)

### MOOC

Code-Based Cryptography (2016)

### BLACK HAT 2014

C and C++ Source Code Auditing  
Application Security for Developers  
and Attackers

### IACR

Workshop on EasyCrypt (2015)  
School on Securing Cryptographic Algorithms and Devices (2015)  
Real World Crypto (2016)  
WhibOx (2016)  
Real World Crypto (2017)

## INTERESTS

### CRYPTO + PL

Authenticated Encryption  
Permutation Cryptography  
Programming Synthesis  
Formal Verification  
SMT Solvers  
Symbolic Execution

### OPTIMIZATION

Portfolio Theory  
Scheduling Problems  
Sequencing Problems

## BOOZ ALLEN HAMILTON ENGINEERING SERVICES, LLC |

### TECHNOLOGIST

#### Continued...

- Provided cryptographic analysis for a GPS CNAV project
  - Identified feasible cryptographic solutions
  - Assisted in drafting a cryptographic protocol for authentication of associated data and high level overview of key management
  - Consulted and developed software for prototyping the cryptographic concept
- Designed a SOAP software architecture for GPS SAASM Mission Planning System
- Designed C# framework, ATLAS, for internal use within the Booz Allen Hamilton Advanced Research and Development office
- Designed, developed, & tested a MATLAB Reed-Solomon error correction code library without the MATLAB Communication Toolbox
  - Allows for arbitrary  $(n, k)$  code encoded using Galois fields
  - Uses a Berlekamp-Welch decoding scheme
- Developed & demonstrated a cryptographic use case using SHA-3 based algorithms in embedded C software for a PIC24HJ12GP201I Controller
- Built and demonstrated Zig-bee 802.15.4 wireless data transfer software in C to potential business partners
- Designed, developed, & tested a random number generation test suite in C# based on NIST SP800-21
  - Performs a bank of statistical confidence interval tests to assure randomness of data for hardware random number generators
- Developed & tested C/C# cryptographic (ECDSA & SHA-2) software for a software GPS receiver
  - Implemented fast Galois addition over elliptic curves
  - Tested for cryptographic algorithm validity and security measures.
- Designed, developed, & tested message optimization software for GPS L2C and L5 signals in python
  - Designed a periodic graph which models feasible message sequences
  - Linear inequalities were derived from the L2C and L5 constraints using the periodic graph
  - Message sequencing results we derived using linear programming
- Modeled, developed, & tested message packing software for GPS C/A signal in python
  - Software was given an a set of messages; using a bin packing problem solver implemented using linear programming, messages were packed into C/A
- Corrected NIST test vectors for SHA-2 based digital signature algorithms
- Contributed the 'K' in SHAKE for NIST FIPS-202
- Designed and prototyped a cradle to grave management system for NIST compliant cryptographic keys that met NIST SP800-53 SC-12 (1) and (2)
- Drafted CONOPS documents for cryptographic systems
- Drafted command and control software operator manuals
- Drafted key management plans and non-standard key handling agreements for cryptography systems

## RESEARCH

### **REALIZATION OF SIMPLY CONNECTED POLYGONAL LINKAGES AND RECOGNITION OF UNIT DISK CONTACT TREES** | SPRINGER

VERLAG, LECTURE NOTES IN COMPUTER SCIENCE, SEPTEMBER 2015

### **LIE GROUPS, HOMOGENEOUS MANIFOLDS, AND COMPLEX PROJECTIVE SPACES** | Co-AUTHORED WITH MAYRA MORAN AND

ATOUR BEAN, MAY 2009

Partially funded by NSF Grant DMS-0502258

## PRESENTATIONS

- 2015 Optimizations on Message Sequencing in CNAV GPS
- 2014 Permutation and Construction Library:  
A Library for Permutation Based Cryptography
- 2014 What the Heck is Fuzz-Testing?
- 2014 BlackHat, DEFCON, SHA-3, & DIAC: The Summer Conferences
- 2014 Configuration Management within Booz Allen Hamilton  
and an Introduction to C# ATLAS
- 2014 Message Optimization over L2C and L5
- 2013 Error Correction Codes over Finite Fields
- 2012 Mission Planning Optimization
- 2010 Reed Solomon Error Correction Codes

## MISCELLANEOUS SOFTWARE DEVELOPMENT

### **SOFTWARE DEVELOPMENT IN ACADEMIA** August 2007 – May 2015 | Cal State Northridge

- Developed a python script to generate random trees using Markov chains
- Developed R scripts to perform multi-regression analysis (ANOVA,  $R^2$ , principle component analysis) on car data to model miles per gallon
- Developed R scripts for bootstrapping limited samples to develop statistical tests over the sampling distribution
- Developed a MATLAB application which was able to identify individuals from their voice using partial differential equations
- Used C++ OpenCV to identify text in Arabic and English from a digital images. Application was used for an unmanned air vehicle project
  - Used Canny algorithm, splines, and Hausdorff distance measurements to estimate characters in Arabic and English
- Developed a python application to optimize resource scheduling management software using evolution algorithms
- Modeled Joukowski air foils (aircraft wing and lift) as a system of partial differential equations in Mathematica
- Modeled growth and decay of animal and bacteria populations as a system of partial differential equations in Mathematica

### **PERSONAL SOFTWARE DEVELOPMENT** June 2004 – Present

- Currently developing an open source, formally verified, symbolically tested, library for standardized cryptographic permutations and constructions
  - Using LLVM KLEE based platforms for symbolic testing
  - Permutations slated for inclusion are Keccak and any permutation that is selected for the second round of the authenticated encryption associated data algorithm competition, CAESAR.
- Developed python code for interpolating stochastic differential equations for use in modern portfolio theory and management
- Web development in Drupal CMS (version 4,5, and 6)