

JAKE MASSIMO

Ph.D Student - Cyber Security

Royal Holloway, University of London

jake.massimo.2015@rhul.ac.uk \diamond <https://www.massi.moe>

EDUCATION

Royal Holloway, University of London, England

2015 - Current

Doctor Of Philosophy (Ph.D.), Cyber Security. Advisor, Prof. Kenneth Paterson.

University of Exeter, England

2014 - 2015

Master's Degree (MMath), Mathematics, 1st Class. Advisor, Prof. Nigel Byott.

Dissertation topic: Factorisation Algorithms.

University of Exeter, England

2011 - 2014

Bachelor of Science (BSc), Mathematics, 1st Class.

RESEARCH INTERESTS

Algorithmic and computational number theory: primality testing, factorisation, finite field mathematics, Carmichael numbers. Applications of the above in cryptography: public-key cryptography, Diffie-Hellman key exchange, real-world implementations (OpenSSL, GNU GMP, mathematical software and TLS), cryptanalysis.

PUBLICATIONS

1. Martin R. Albrecht, Jake Massimo, Kenneth G. Paterson and Juraž Somorovsky. Prime and Prejudice: Primality Testing Under Adversarial Conditions. 2018 ACM SIGSAC Conference on Computer and Communications Security 2018 Oct 15 (pp. 281-298). ACM. *Best Paper Award Finalist*.

<https://eprint.iacr.org/2018/749>

This work provides a systematic analysis of primality testing under adversarial conditions, where the numbers being tested for primality are not generated randomly, but instead provided by a possibly malicious party. We study a broad range of cryptographic libraries and assess their performance in this adversarial setting. As examples of our findings, we are able to construct 2048-bit composites that are declared prime with probability $1/16$ by OpenSSL's primality testing in its default configuration; the advertised performance is 2^{-80} . We can also construct 1024-bit composites that *always* pass the primality testing routine in GNU GMP when configured with the recommended minimum number of rounds. And, for a number of libraries (Cryptlib, LibTomCrypt, JavaScript Big Number, WolfSSL), we can construct composites that *always* pass the supplied primality tests.

2. Steven Galbraith, Jake Massimo and Kenneth G. Paterson. Safety in Numbers: On the Need for Robust Diffie-Hellman Parameter Validation. In submission 2018.

We consider the problem of constructing Diffie-Hellman (DH) parameters which pass standard approaches to parameter validation but for which the Discrete Logarithm Problem (DLP) is relatively easy to solve. We consider both the finite field setting and the elliptic curve setting. For finite fields, we show how to construct DH parameters (p, q, g) for the strong prime setting in which $p = 2q + 1$ is prime, q is smooth but fools random-base Miller-Rabin primality testing with some reasonable probability, and g is of order $q \bmod p$. In the elliptic curve case, we use an algorithm of Bröker and Steenhoven to construct an elliptic curve E over a finite field \mathbb{F}_p having a specified number of points n . We are able to select n of the form $h \cdot q$ such that h is a small co-factor, q is smooth but fools random-base Miller-Rabin primality testing with some reasonable probability, and E has a point of order q .

COMMON VULNERABILITIES AND EXPOSURES (CVE)

CVE-2018-4398 <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4398>

Issued for the security update to macOS Mojave 10.14.1 and iOS 12.1 for exposing a vulnerability in which an attacker may be able to exploit a weakness in the Miller-Rabin primality test to incorrectly identify prime numbers.

EXPERIENCE

Royal Holloway, University of London

Student Ambassador

June 2017

London, UK

I have participated in the “Exploring Mathematics” program as a student ambassador. This is an outreach event in which Royal Holloway showcases the study of Mathematics at university level to A-level students across London. My role included helping students participate in small workshops in which they solved short mathematical puzzles and providing an account of my experiences at university.

University Of Exeter

Mathematics Tutor

September 2013 - September 2015

Exeter, UK

- While studying at Exeter I was also employed as a paid tutor. In the third year of my degree I tutored first year BSc Mathematics students in four different core modules. This involved guidance through worked question sheets and giving explanations of some material to small groups. The reason I initially signed up to take part in this was to get an idea of what it would be like to be a lecturer teaching university level material. I enjoyed tutoring so much, that I became a tutor again in the fourth year of study, this time tutoring second year BSc Mathematics students which I found even more rewarding as the level of complexity increased.

AUXILIARY ACTIVITIES

Industry Exposure

June 2016

Royal Holloway, University of London

London, UK

- The Centre for Doctoral Training (CDT) program at Royal Holloway gave me the opportunity to attend several trips to industry partners and the opportunity to participate in several workshops. Industry visits included external outings to Thales and KPMG. Both entailed a brief overview of the company itself, followed by the participation in some short tasks and challenges in small groups. The workshops included topics on: cyber security insurance, banking and payment infrastructure and practical experience working hands on with industry IPsec hardware.

Summer School

June 2017

Real-World Crypto and Privacy

Šibenik Croatia

- In June 2017 I attended the 4 day summer school on real-world crypto and privacy in Šibenik Croatia. The summer school provides a host of introductory lectures on various topics, including: cryptography for the Internet, recent developments in symmetric key cryptography, security proofs in cryptography, wireless security, cryptography for systems security, software and hardware security and privacy enhancing technologies. I also published a small blog post on the ISG's news page summarising the event and my experience.

Reading Groups

June 2017

Royal Holloway, University of London

London, UK

- In addition to the CDT activities mentioned above I also took part in participation of several reading groups. I kept up ongoing attendance of the student ran Introduction to Modern Cryptography reading group as well as the Yet Another Crypto Reading Group (YACRG) ran by the department.

I presented a session myself in YACRG, on the paper “Measuring small subgroup attacks against Diffie-Hellman” <https://eprint.iacr.org/2016/995>.

TALKS

- *Prime and Prejudice: Primality Testing Under Adversarial Conditions*, 12th December 2016, 27th HP Colloquium on Information Security, ISG RHUL, London, UK. (20 minutes).
- *Prime and Prejudice: Primality Testing Under Adversarial Conditions*, 26th April 2017, ISG RHUL CDT Showcase, London UK (20 minutes).
- *Prime and Prejudice: Primality Testing Under Adversarial Conditions*, 15 – 19th October 2018, ACM CCS 2018, Toronto, Canada (20 minutes).

OTHER SKILLS

Computing	Python - 7 years extensive experience and knowledge of standard mathematic and scientific packages with considerable usage of SAGE. C - 3 years experience, knowledge of arbitrary-precision arithmetic libraries such as OpenSSL and GNU GMP and many libraries offering cryptographic functionality. Basic knowledge of Java, GoLang, C++, R. Proficient use of Word, PowerPoint and LaTeX throughout PhD project.
Sports	Swam for Exeter University Swimming team in 2012 - 2014. Also represented Exeter University at British Universities and Colleges Sport (BUCS) for Surfing 2011 - 2015.
Languages	Native English speaker.
Driving	Full, clean UK driving license.