JAKE MASSIMO

Ph.D Student - Cyber Security
Royal Holloway, University of London
jake.massimo.2015@rhul.ac.uk ◇ 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, prime number generation, factorisation, finite field mathematics, Carmichael numbers. Applications of the above in cryptography: public-key cryptography, Diffie-Hellman key exchange, RSA, Digital Certificates. Real-world implementations and cryptographic library analysis (OpenSSL, GNU GMP, mathematical software), cryptanalysis, TLS.

PUBLICATIONS

1. Martin R. Albrecht, Jake Massimo, Kenneth G. Paterson and Juraj 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. Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography. 2019.
   https://eprint.iacr.org/2019/032

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 mod p. In the elliptic curve case, we use an algorithm of Bröker and Stevenhagen 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.

3. Jake Massimo and Kenneth G. Paterson. A Performant, Misuse-Resistant API for Primality Testing. To appear in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, CCS 2020, Orlando, USA, November 9-13, 2020, ACM.* `https://eprint.iacr.org/2020/065`

In this work we set out to design a performant primality test that provides strong security guarantees across all use cases and that has the simplest possible API. We examine different options for the core of our test, describing four different candidate primality tests and analysing them theoretically and experimentally. We then evaluate the performance of the chosen test in the use case of prime generation and discuss how our proposed test was fully adopted by the developers of OpenSSL through a new API and primality test scheduled for release in OpenSSL 3.0 (2020).

COMMON VULNERABILITIES AND EXPOSURES (CVE)

CVE-2018-4398

My work uncovered a vulnerability in the primality testing procedure of Apple's crypto library. This issue was classified as high severity by NIST and affected versions prior to iOS 12.1, macOS Mojave 10.14.1, tvOS 12.1, watchOS 5.1, iTunes 12.9.1, iCloud for Windows 7.8. See the section *CoreCrypto* of Apple's security update `https://support.apple.com/en-gb/HT209192` and NIST's vulnerability page `https://nvd.nist.gov/vuln/detail/CVE-2018-4398` for more information.

OPEN SOURCE CODE CONTRIBUTIONS

OpenSSL Working with Kurt Roeckx of the OpenSSL team, my research has been used to guide the implementation and renovation of the primality testing procedures in OpenSSL. This work has achieved both a stricter guarantee of security and and an improvement of efficiency. The suggestions made by my work were adopted with only minor modifications: the forthcoming OpenSSL 3.0 (scheduled for release in Q4 of 2020) will include our simplified API for primality testing, and the OpenSSL codebase has been updated to use it almost everywhere (the exception is prime generation, which uses the old API in order to avoid redundant trial division). Moreover, OpenSSL will now always use our suggested primality test (64 rounds of Miller-Rabin) on all inputs up to 2048 bits, and 128 rounds of Miller-Rabin on larger inputs. This represents the first major reform of the primality testing code in OpenSSL for more than 20 years. Some of the code development can be seen at: `https://github.com/openssl/openssl/pull/9272` and a full release is expected in OpenSSL 3.0.

I have also authored smaller contributions to OpenSSL surrounding parts of the primality testing and prime generation procedure seen in the merge at:
`https://github.com/openssl/openssl/commit/2500c093aa1e9c90c11c415053c0a27a00661d0d`.

Apple, Bouncy Castle, Botan and WolfSSL During the work of *Prime and Prejudice* (2018), we reached out to all cryptographic libraries that were effected by our work. This resulted in working with the developers and security teams of Apple, Bouncy Castle, Botan (`https://github.com/randombit/botan/pull/1636`) and WolfSSL (`https://github.com/wolfSSL/wolfssl/pull/1665`) to advise and propose solutions.

EXPERIENCE AND INTERNSHIPS

Amazon Web Services (AWS) May-October 2019
Applied Scientist Intern *Seattle, Washington, USA*

- During 5 months of the my final year as a PhD student, I undertook an internship at Amazon Web Services (AWS) in Seattle, USA. I was part of the Crypto Algorithms team at AWS who specialise in providing general guidance on cryptographic solutions for Amazon products and service features.

Working as an applied scientist in AWS, I was given the opportunity to expand my skill set of working with applied cryptography, mathematics and computational number theory and apply it within a new framework of tools provided by AWS. For example, taking my existing knowledge of coding and working with cryptographic libraries in C and elevating this to next level, by creating software and production level code that is implemented using tools such as AWS Lambda functions and reading and writing to S3 file storage. I was given the opportunity to work on problems for which a clear path to a solution was not known, and this allowed me to both refine some of my existing skills, as well as learn new ones.

This also gave me the opportunity to bridge the gap in between working in a highly theoretical setting of PhD study, with working in a business environment and producing work with a high level of robustness and development acumen. This included creating detailed design documents for my work, providing in-depth code documentation and extensive testing procedures. I was also given the opportunity to sharpen my skills in working on a project as a team. This meant having regular discussions about the reasoning behind design choices, equating against alternative methods and having the output (be it code or documentation) reviewed and assessed.

I am most excited about collaborating with other great academics and engineers, to work on solving practical problems that have an impact on the security of millions of customers across the world. Working with AWS gave me an opportunity to learn from the industry experts in my team and across the organization as they work on both the implementation and research in information security and cryptography at a scale that is industry leading.

Royal Holloway, University of London June 2017 - Current
Student Ambassador *London, UK*

- I have participated in the "Exploring Mathematics" and "Royal Holloway Science Fair" programs as a student ambassador. These are outreach events in which Royal Holloway showcases the study of Mathematics and cryptography at university level to students from primary school to A-level age 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 September 2013 - September 2015
Mathematics Tutor *Exeter, UK*

- While studying at Exeter I was 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 Royal Holloway, University of London
June 2016 *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 Real-World Crypto and Privacy
June 2017 *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 Royal Holloway, University of London
2017-2019 *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

- *Primality Testing in Cryptographic Applications*, 16 – 18th December 2019, St Annes College, University of Oxford, 17th IMA International Conference on Cryptography and Coding (20 minutes).
- *Safety in Numbers: On the Need for Robust Diffie-Hellman Parameter Validation. Public-Key Cryptography*, 14 – 17th April 2019, IACR PKC 2019, Beijing, China (30 minutes).
- *Prime and Prejudice: Primality Testing Under Adversarial Conditions*, 12th November 2018, Mozilla Security Research Summit, London UK (15 minutes).
- *Prime and Prejudice: Primality Testing Under Adversarial Conditions*, 15 – 19th October 2018, ACM CCS 2018, Toronto, Canada (25 minutes). (Available at: `https://www.youtube.com/watch?v=OohldLXyVpc`)
- *Prime and Prejudice: Primality Testing Under Adversarial Conditions*, 12th December 2016, 27th HP Colloquium on Information Security, ISG RHUL, London, UK. (20 minutes).

OTHER SKILLS

Computing Python - 8 years extensive experience and knowledge of standard mathematic and scientific packages with considerable usage of SAGE.
C - 4 years experience, knowledge of arbitrary-precision arithmetic libraries such as OpenSSL, GNU GMP and many libraries offering cryptographic functionality.
Basic knowledge of Java, GoLang, C++, R.
Experience with developing using AWS services, such as AWS Lambda, ECR, ECS, S3, EC2.
Proficient use of Word, PowerPoint, Adobe Photoshop and LaTeX.

Sports Represented Exeter University at the British Universities and Colleges Sport (BUCS) competition for Exeter Universit Surf team 2011 - 2015 and Exeter University Swimming team in 2012 - 2014.

Website `https://massi.moe`
GitHub `https://github.com/JBeatz`
Google Scholar `https://scholar.google.com/citations?user=MbwY1twAAAAJ`
Languages Native English speaker.
Driving Full, clean UK driving license.