Valid Proof: Understanding the Politics of Public-Key Cryptography

Robert Pantalone, Social and Political Thought
Acadia University, Canada
robertpantalone@acadiau.ca

Abstract

This paper considers the political implications of the public-key cryptosystems which secure communication over popular messaging programs such as WhatsApp, and underwrite the blockchain infrastructures of cryptocurrencies like Bitcoin. While the distribution of privacy and security through access to cryptography has been a salient topic in academic and public discourse, less has been written about cryptographic mechanisms themselves. Public-key cryptography makes use of a mathematical concept called the one-way function. One-way functions are assumed to be easy to compute in one direction, but difficult to reverse. However, one-way functions have an unusual relationship to validity: they rely on conjectures about computing which have not been proven. This property is considered in relationship to Michel Foucault's concept of the unthought to suggest that it reflects the condition of the modern episteme. This takes on a political dimension in the uncertain conditions of cryptographic design, where national security interests often lead to the restriction of research. Furthermore, cryptographers must design systems which are resistant to both external adversaries as well as malicious users. Cryptosystems must therefore be designed against the users who they nominally protect. The confluence of epistemic uncertainty and practical insecurity makes distrust endemic in cryptographic research. This outlook enacts a logic of suspicion at the level of its design; as applications based on cryptography attain wider circulation, this will have increasing social effects.

The politics of cryptography is typically framed as a debate about the extent to which personal privacy must be balanced with collective security. By encrypting a message, one can protect themselves against surveillance; however, encrypted messages may not be accessible to law enforcement apparatuses even when valid search warrants are issued. As a result, access to encryption technologies is framed as a zero-sum game: there can be either security or privacy, but not both. Although encryption has been a salient topic for academic and public discourse, efforts to legislate cryptosystem design reveal that this is an equally relevant issue. In the United Kingdom, for instance, section 253 of the 2015 Investigatory Powers Act allows for the government to issue notices which compel service providers to redesign their encryption protocols to comply with surveillance warrants (Open Technology Institute, 2017: 5). The political importance of these mechanisms will only grow as variations of public-key cryptography become increasingly commonplace on popular messaging programs such as WhatsApp, in evidentiary mechanisms like digital signatures, or cryptocurrencies such as Bitcoin. This paper departs from the privacy-security framework to analyse how the mechanisms of contemporary cryptography reflect the political practices of the security apparatuses which make use of encryption technologies. There is a parallel effort in both projects to manage the risk of uncertainty. Highlighting this connection explains cryptography's relevance for security politics and provides a basis for analysing emergent applications of encryption processes.

The Mechanisms of Public-key Cryptography

Contemporary cryptography uses a public-key encryption scheme with pairs of keys – one private and one public – to allow users to communicate securely. Although anyone may use a public-key to encrypt a message, the message can only be decrypted by reversing this process using the information contained in the private-key. There is therefore no need to distribute shared keys over secure channels as with earlier symmetric methods. The two keys are linked by mathematical processes which are easy to compute, but infeasible to reverse; it is therefore exceedingly difficult to find the private-key based on the public one. These mechanisms, called one-way functions, were brought to wider attention in 1976 by Whitfield Diffie and Martin Hellman in their germinal paper, 'New Directions in Cryptography'. Responding to the need for both privacy and authentication in communication over open-channels, such as radio waves, where transmissions can be easily intercepted or falsely planted, Diffie and Hellman (1976) propose using one-way problems to send messages securely even if the data are transmitted over public channels.

Although Diffie and Hellman use a code compiler as an illustrative example of a one-way function, their paper does not offer a practical scheme for public-key cryptography. The first openly-published public-key cryptosystem would be developed by American researchers Ron Rivest, Adi Shamir, and Leonard Adelman two years later in 1978. As befits the secretive nature of the discipline, it was later revealed that British researchers employed at the Government Communications Headquarters (GCHQ) developed the very same scheme in 1973 (Levy, 1999). The method itself is both devilishly simple and fiendishly difficult. The Americans suggest that multiplying two large prime numbers (at least 100-digits long) can act as a one-way function. Because it is trivial to perform the multiplication – it could be done with pen and paper – but exceedingly difficult to find the factors of the resulting product without knowing them in advance, the product can be published as a public-key and the primes can be used as a private-key (Rivest, Shamir and Adelman, 1978). This process (now referred to by its inventors' initials, RSA) became a cryptographic standard and remains in use.

The importance of one-way functions for modern cryptography cannot be overstated. In addition to providing secret communication, one-way functions are also used to authenticate transmissions. For these digital signature schemes, a sender uses their private-key to generate information that can be verified though use of their public-key; this validates their message because it would be infeasible to replicate the process and forge the message without knowing the private-key (Sako, 2011). One-way functions are also used for pseudorandom number generators which increase cryptographic strength by preventing predictable key choices (Ha Stad et al., 1999). Finally, they can be used as hash functions which output a string of bits of a fixed size from an input string of an arbitrary length (Naor and Yung, 1989: 34). Hashing a message compresses it and thereby reduces the computing burden required to encrypt it. In sum, the one-way function is both the theoretical basis of modern cryptography and critically important for its practical implementation.

The Validity of the One-way Function

While cryptosystems ostensibly offer a demonstrable means for security, an examination of the principles upon which they are based reveals that this is not so clearly the case. Mathematically speaking, one-way functions are operations which are thought to have asymmetrical computational demands: they are easy to perform in one direction, but are infeasible – meaning they require impractical computational effort – to invert (Robshaw, 2011). These form the basis of many cryptographic primitives from which more complicated cryptosystems are constructed (Kalinski, 1999: 92). If the difficult element of a one-way function (called a hard-core predicate) can be identified, then it may be used to design cryptosystems which are considered more provably secure (Goldreich and Levin, 1989). Finding and discovering one-way functions remains an important research focus in cryptography. In spite of this, one-way functions are not proven. Although RSA, for example, has been the subject of intense research to define best practice, its strength is the absence of a known algorithm for factoring large composite numbers (Boyer and Moore, 1984: 182). One-way functions exist as unverifiable conjectures and therefore exemplify the search for difficult or intractable problems, which, according to Claude Shannon, the godfather of information theory and pioneer of cryptography, distinguishes the field (Shannon, 1949: 704).

This has complicated the notion of proof in the discipline of cryptology. In mathematics, a proof is traditionally a rigorous argument that can be verified by a human and deductively validates a logical relationship (Krantz, 2010: 242). Within computing, however, proof means that the theoretical model of a computer system aligns with its enacted design, regardless of whether the underlying assumptions are true or if the design is adequate (MacKenzie, 1995: 48). This is verified mechanically by automated theorem-testing programs that determine whether the propositions are valid under the specified conditions; however, these programs themselves have not been entirely formally verified (MacKenzie, 1995: 51). Because of these limitations, proof becomes a problem insofar as it increases the dependability of a system through automatic mathematical investigation to manage the risk that there may be unknown complications (MacKenzie, 2004: 8). As there is always some degree of doubt, proof is never absolute or exhaustive; rather, it is probabilistic. Validity is constructed through successive but limited verifications that diminish uncertainty. The development of provable security in cryptography similarly relies on mechanical proof. Rigid step-wise protocols have been developed to standardize the requirements of cryptographic design as a guarantee of security (Sprenger and Basin, 2010). But because one-way functions are unproven, their reliability can only be tested indirectly, which requires making further assumptions (Dent, 2006). The result is called a refinement paradox: attempts to develop demonstrably secure systems cannot evaluate that quality directly (Alur, Černý and Zdancewic, 2006). Consequently, although mechanical proof enhances the validity of existing systems, it also compounds the underlying problem by adding propositions. As a result,

cryptographers are in the unenviable position of designing secure systems from indemonstrable propositions; the possibility of errors can be mitigated but not entirely eliminated.
In public-key cryptography, validity is not only a problem of managing uncertainty to ensure that a system works. Counterintuitively, it is the limitations of computing and the unknown properties of the one-way function that make cryptography possible. Indeed, if research showed that one-way functions were reversible, they would no longer be useful. Mathematician and computer theorist Oded Goldreich reveals how this presents a fundamental challenge for secure design. His treatise, Foundations of Cryptography, is unique in cryptographic discourse because it eschews the development of new systems in favour of formalizing the core principles of cryptography. The basic problem is that while 'one-way functions are the very minimum needed for doing most sorts of cryptography […] our current state of understanding of efficient computation does not allow us to prove that one-way functions exist' (Goldreich, 2001: xiv). The contradiction at the heart of cryptography, then, is that the inability to resolve whether one-way functions are directional is both the condition and limitation of their usefulness.

This is not an idle concern because uncertainties are vulnerabilities. The safest assumption in designing a cryptosystem is to assume that an adversary has effectively unlimited capabilities (Goldreich, 2001: 22). In a separate meditation on the relationship between proof and cryptography, Goldreich stresses the need to make minimal assumptions about the validity of one-way function to ensure that analyses are sufficiently rigorous. He summarizes the dilemma which the discipline faces, writing: 'intuition invoked in time of need (as any feeling that arises in time of distress) is to be suspected, certainly not trusted. For sure, such intuition can serve as a basis for knowledge, and things are even worse in cryptography' because there is always a presumption of adversarial behaviour, and therefore cause for concern (Goldreich, 2006: 12). Designing cryptography requires being suspicious of knowledge because the lack of definitive deductive proof may be exploited in an attack. Goldreich thus reveals the confluence between epistemic validity and political security in cryptography: uncertainty is tantamount to risk.

Proof as an Epistemic Problem

The paradoxical status of the one-way function in cryptography can be more fully understood if its validity is seen as part of a larger epistemic problem. Indeed, one-way functions have not always been cryptographic: in their earlier formulation by William Stanley Jevons, they are treated as a broader class of logical problems whose irreversibility is of general importance (Jevons, 1877: 121–196). Accordingly, the one-way function intersects with the broader question of how valid knowledge develops in the face of the unprovable. In an essay examining the bases of modern science, Martin Heidegger shows that the limit of thought is also the condition of knowledge. This is exemplified by mathematics. Returning to the term's Greek roots, mathēsis (learning) and mathēmata (what is learnable), Heidegger suggests that mathematics is 'coming to know actually and to the very foundations what we already know' (2008: 275). Mathematics is thus a practice of self-investigation. This reflexive practice gives birth to experimentation in modern science which establishes axioms as the standard of knowledge. Although this liberates thought by making everything subject to evaluation, it also imposes 'a binding with obligations that are self-imposed' (Heidegger, 2008: 291). In mathematics, 'thinking thinks itself' by both questioning and enacting limits (Heidegger, 2008: 302). Heidegger's characterization of mathematics continues in the discipline of cryptography which must perpetually re-examine its propositions according to the programs of mechanical proof.

Michel Foucault's archaeology of modern thought, The Order of Things, connects the concept of the limit with the unknown. For Foucault, mathēsis in Classical thought refers to a qualitative science of order that seeks to establish a continuity of knowledge (Foucault, 1994: 56). However, mathēsis also articulates a transition toward the modern episteme because it makes possible empirical disciplines which do not conform to an a priori order, for example a divine design, but instead refer only to their internal cohesion (Foucault, 1994: 243). This restructures knowledge: as mathēsis becomes dissociated from a universal order, there is no longer a given coherence between objects and their representations. Instead, all knowledge is made in relation to the thinking subject who, Foucault argues, occupies an 'ambiguous position as an object of knowledge and as a subject that knows' (1994: 312). The result is that empirical knowledge is always incomplete because it is 'a fundamental finitude which rests on nothing but its own existence as fact' (Foucault, 1994: 315). This analytic of finitude is not a stable arrangement because the thinking subject is always aware of the finitude of their thought. There is an obligation to unceasingly question knowledge so as to affirm its validity. Modern thought must continually confront its limit – the impossibility of absolute certainty – to retain its concrete form. Consequently, the modern cogito encounters what Foucault terms the unthought: 'an irreducible, an insuperable exteriority' which exceeds it but is nevertheless integral to its thinking (1994: 324). The unthought is neither the opposite of thought nor its negation. It is, rather, the indispensable condition of the thinking subject's relentless reflexivity and that which it can never overcome. Foucault's analysis reveals that the central dilemma of cryptography is also that of the modern episteme. One-way functions' resistance to deductive proof is not an aberration, but a manifestation of how thought encounters its finitude in the form of an unthinkable but necessary exterior. Contemporary public-key cryptography can be characterized as what Foucault calls a science of the unconscious, which is directed not 'toward that which is below consciousness', but instead 'towards that which, outside of man, makes it possible to know with a positive knowledge, that which is given to or eludes his consciousness' (Foucault, 1994: 378). In this regard, public-key cryptography constitutes an effort to generate stability from conditions of epistemic uncertainty. The unprovable nature of one-way functions does not foreclose the possibility of security, but instead demands a set of epistemic practices, for example the use of mechanical proofs, which work within the finitude of computing knowledge. Out of this indeterminacy, cryptographers produce standards from which theoretical apparatuses and practical applications arise. There is, however, no possibility of certain proof on account of the underlying epistemic uncertainty. As a result, all cryptographic developments are by necessity subject to persistent suspicion which indefinitely endeavours to secure itself.

Cryptography as a Political Technology

The goal of analysing the disparity between valid mathematical proof and working cryptographic design is neither to reveal a disciplinary deficiency nor to resolve the discrepancy between the two. Rather, triangulating the gap between the theory and practice of public-key cryptography reveals that the question of security is not confined to how encryption technologies are used, but also linked to their epistemic mechanisms. If these functions are seen as inherently political rather than neutral, then it is possible to understand why these technologies are important for practices of security without recourse to familiar and reductive narratives about the rise of electronic communication in a networked society. Encryption technologies make possible secret communication. These are political relations because, as Georg Simmel argues, secrets must be 'to a certain extent recognized by the other' and as such serve to distinguish between members of a group and outsiders (1906: 462). As part of digital communication, cryptography forms part of what Alex Galloway terms protocol. Protocols, for instance the TCP/IP standards through which the Internet operates, enable flexible connection between many networked nodes, but only under the absolute and rigidly coded rules (Galloway, 2006: 8). As a result, protocols are political because they modulate and manage the flow of information according to their programming; they govern relationships by creating the occasion for action within the confines of encoded possibilities.

Cryptography is therefore a means of managing political relations. Technology theorist Jean-François Blanchette affirms this is the case. In one of the few political considerations of public-key cryptography, he observes that 'cryptography is code created with the sole purpose of regulating behavior. Cryptographic technologies are specifically designed to provide confidentiality, authentication, anonymity, accountability – in short to implement the locks and keys of cyberspace architecture' (Blanchette, 2012: 95). Encryption technologies do not replace existing institutions but become integrated with them. For instance, digital signatures gain evidentiary value through their association with state bureaucracies and actors like notaries public (Blanchette, 2012: 156). However, cryptography also reflects an overriding desire to avoid relying on any trusted third party by implementing systems which offer security on the basis of mathematical proof alone (Blanchette, 2012: 40). Public-key cryptography is seen as a way of validating information even when those who provide it cannot be trusted. For example, encryption technologies guarantee security independently from the promises of national security apparatuses, which may try to control or censor them (Blanchette, 2012: 38). They must also be resistant to tampering from users who might try to falsify information (Blanchette, 2012: 80). Public-key cryptography must therefore be designed against attackers as well as against abuse by those who it nominally protects. As a result, efforts to mitigate uncertainty at the level of computing are paralleled by political practices which work to reduce risk by treating any user as an adversary who might exploit a weakness. As Foucault observes in a lecture, 'the primary, implacable law of both modern governmentality and historical science [is] that man henceforth has to live in an indefinite time' (2007: 356). Political theorist Michael Dillon extends this convergence, arguing that modern security constitutes a political analytic of finitude because it perpetually governs lives that will necessarily end (2011: 782). In the absence of an extra-historical standard by which to judge political decisions or which promises a coming salvation, 'finite regimes of government and rule have indefinitely to secure themselves against the realization of their very own finitude' (Dillon, 2015: 37). More than that, everything which politics seeks to secure is 'dangerous because, in its very know-ability, which is to say its governability, everything also proliferates ungovernably' as all knowledge is implicated with the unthought which by definition cannot be fully contained (Dillon, 2015: 39). The very task of politics in an analytic of finitude is managing uncertainty and endlessly securing the validity of that venture. Thus the epistemic mistrust of mathematical proof is doubled as a political maxim in which nothing can be fully assured and therefore everything must be securitized anew. Public-key cryptography is of contemporary importance because it resonates with this political project. Although encryption technologies are deployed as a response to endemic suspicion and pervasive risk, these mechanisms of public-key cryptography reproduce a logic of security which enacts the same mistrust it is meant to overcome.

References

Alur, R., Černý, P. and Zdancewic, S. (2006) Preserving secrecy under refinement, *Lecture Notes in Computer Science: Automata, Languages and Programming*, 4052, 107–118.

Blanchette, J. (2012) *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*, MIT Press, Cambridge, MA.

Boyer, R. and Strother Moore, J. (1984) Proof checking the RSA: Public key encryption algorithm, *The American Mathematical Monthly*, 91(3), 181–189.

Dent, A. (2006) Fundamental problems in provable security and cryptography, *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 364, 3215–3230.

Diffie, W. and Hellman, M. (1976) New directions in cryptography, *IEEE Transactions on Information Theory*, 22(6), 644–654.

Dillon, M. (2011) Specters of biopolitics: Finitude, eschaton, and katechon, *South Atlantic Quarterly*, 110(3), 780–792.

Dillon, M. (2015) *Biopolitics of Security: A Political Analytic of Finitude*, Routledge, New York.

Foucault, M. (1994) *The Order of Things: An Archaeology of the Human Sciences*, Vintage Books, New York.

Foucault, M. (2007) *Security, Territory, Population: Lectures at the Collège de France*, 1977–1978, M. Senellart, ed., G. Burchell, trans., Picador, New York.

Galloway, A. (2006) *Protocol: How Control Exists After Decentralization*, MIT Press: Cambridge, MA.

Goldreich, O. (2001) *Foundations of Cryptography: Basic Tools*, Cambridge University Press, Cambridge.

Goldreich, O. (2006) On post-modern cryptography, *IACR Cryptology EPrint Archive*, 461, 1–12.

Goldreich, O. and Levin, L. (1989) A hard-core predicate for all one-way functions, Paper presented at the Twenty-First Annual ACM Symposium on Theory of Computing, 14–17 May 1989, New York.

Ha Stad, J., Impagliazzo, R., Levin, L. and Luby, M. (1999) A pseudorandom generator from any one-way function, *SIAM Journal on Computing*, 28(4), 1364–1396.

Heidegger, M. (2008) Modern science, metaphysics, and mathematics, in D. Farrell Krell, ed., *Basic Writings*, Harper Perennial Modern Thought, New York, pp. 271–305.

Jevons, W. (1877) *The Principles of Science: A Treatise on Logic and Scientific Method*, Macmillan, London.

Kalinski, B. (1999) Emerging standards for public-key cryptography, in I. Bjerre Damgård, ed., *Lectures on Data Security Modern Cryptology in Theory and Practice*, Springer-Verlag, Berlin, pp. 87–104.

Krantz, S. (2010) The history and concept of mathematical proof, in V. Lundsgaard Hansen and J. Gray, eds., *History of Mathematics*, Encyclopedia of Life Support Systems Publishers, United Kingdom, 239–268.

Levy, S. (1999) The open secret, *WIRED*, accessed at: **https://www.wired.com/1999/04/crypto/** (10 March 2018).

MacKenzie, D. (1995) The automation of proof: A historical and sociological exploration, IEEE Annals of the History of Computing, 17(3), 7–29.

Mackenzie, D. (2004) *Mechanizing Proof: Computing, Risk, and Trust*, MIT Press, Cambridge, MA.

Naor, M. and Yung, M. (1989) Universal one-way hash functions and their cryptographic applications, Paper presented at Twenty-First Annual ACM Symposium on Theory of Computing, 14–17 May 1989, New York.

Open Technology Institute (2017) *Deciphering the European Encryption Debate: United Kingdom*, New America, Washington, D.C.

Rivest, R., Shamir A. and Adleman L. (1978) A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, 21(2), 120–126.

Robshaw, M. (2011) One-way function, in H. van Tilborg and S. Jajodia, eds., *Encyclopedia of Cryptography and Security*, Springer Reference, New York, pp. 887–888.

Sako, K. (2011) Digital signature schemes I, in H. van Tilborg and S. Jajodia, eds., *Encyclopedia of Cryptography and Security*, Springer Reference, New York, pp. 343–344.

Shannon, C. (1949) Communication theory of secrecy systems, *Bell Labs Technical Journal*, 28(4), 656–715.

Simmel, G. (1906) The sociology of secrecy and of secret societies, *American Journal of Sociology*, 11(4), 441–498.

Sprenger, C. and Basin, D. (2010) Developing security protocols by refinement, Paper presented at Seventeenth ACM Conference on Computer and Communications Security, 4–8 October, Chicago, IL.