IST-Africa 2017 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2017
ISBN: 978-1-905824-57-1

Blockchain as an Enabler for Public mHealth Solutions in South Africa

Martin WEISS[1], Adèle BOTHA[2,] Marlien HERSELMAN[3], Glaudina LOOTS[4]
[1]South African Medical Research Council, P.O. Box 19070, Cape Town, 7505, South Africa, & Jembi Health Systems NPC, 382 Main Rd, Tokai, Cape Town, South Africa
Tel: +27 21 701 0939, Email: martin.weiss@jembi.org
[2, 3]CSIR Meraka, P.O. Box 395, Pretoria, 0001, South Africa & School of Computing, Unisa, Florida, 0001, South Africa
Tel: +27 12 841 3065, Email: [2]abotha@csir.co.za, [3]mherselman@csir.co.za
[4]Department of Science and Technology, Private Bag X894, Pretoria, 0001, South Africa
Tel:+27 21 469 5020, Email:glaudina.loots@dst.gov.za

Abstract: Blockchain technology underpins a radical rethink of information privacy, confidentiality, security and integrity. As a decentralised ledger of transactions across a peer-to-peer network, the need for a central third party intermediate verification authority is disrupted. To unlock the potential for mHealth, the need for authentication and verified access to often sensitive data, specialised services and transfer of value need to be realised. This paper interrogates current processes and aims to make a case for Blockchain technology as an improved security model that has the potential to lower the *cost of trust* and an alternative to managing the burden of proof. This is particularly relevant for mHealth that, by its nature, is often a distributed endeavour involving the goal-orientated collaboration of a number of stakeholders.

Keywords: Blockchain, mHealth, security infrastructure

1. Introduction

The Normative Health Standards [1] and eHealth strategy [2] define the security, monitoring and auditing requirements for health information at an enterprise level – connecting clinics through an information exchange system to national public health services. This is however, not the case for mHealth, an emerging and substantially important subset of eHealth, with its own unique challenges [3, 4].

One of the mHealth challenges not addressed is that of the security infrastructure, and as a result, mHealth providers implement *ad hoc* or home grown security solutions that are generally outside their domain of expertise [4]. In addition, misinterpretation of security requirements has seen mobile applications offering different levels of security, sometimes compromising patient confidentiality. These factors have resulted in an ecosystem riddled with disparate security solutions and offering conflicting levels of security across different mobile applications [5].

A parallel can be drawn in the formal banking environment, where only as recently as 2005, did a sufficient level of trust between banking institutes result in an inter-operative environment where electronic transfers between banks as well as between bank clients and their banks were possible [6]. This inter-operability still required transaction brokers to translate transactions from one banks' security protocol into another banks' security protocol; each bank retaining ownership of their clients' records and privacy. With this architecture however, a client is beholden to a certain bank for all their banking requirements on a banking account.

Disruptive technology [7] is the form of Blockchain [8], has underpinned a radical approach to payment mechanisms in the form of Bitcoin [9] – a virtual cash currency that does not require a central bank to manage an account. Bitcoin provides clients with a mechanism to pay-for and receive virtual cash that is both anonymized (to a certain degree) as well as secure. Secure in the sense that it can be verified as authentic, but still with some of the risks associated with real cash.

The underlying security technology of Blockchain is not particularly novel or new and has been used in cryptography and authentication of data for at least the past 15 years) [10, 11]. However, what Blockchain does introduce are the concepts of *provenance* and *distributed ledgers*; providing a solution to what has stalled the implementation of virtual cash [12, 13]. These main advantages (with regards security infrastructure) allows for the preservation of transaction history – being able to trace back any transaction to its genesis, and secondly to provide irrefutable proof of:

- the authenticity of a transaction's participants,
- any transaction values,
- the time and date of the transaction, as well as
- its unique position in a digital ledger.

In addition, Blockchain introduced the notion of distributed ledgers hosted on multiple sites around the world with no single server being a dominant element in any of the transactions. The distributed ledgers implies no central control, clearing house or single point of failure [8]. In Bitcoin, anyone is able to establish a ledger site, and compete with other ledger sites in creating ledgers (transaction blocks) – allowing for the democratization of the virtual cash – not owned, controlled or managed by any single entity [8]. For the financial world and internet payment world, this is truly revolutionary and responsible for creating both challenges and opportunities for current financial and solution providers [8, 14].

Because of these unique features, Blockchain is now being considered for circumstances where provenance and irrefutable traceability are required [15]. These include financial services, management of legal contracts, traceability of title deeds and other deeds of sales, digital identity, digital art, intellectual property, notary services, supply change management and medical prescription management [9, 15, 16]. Examples of practical implementations include *PassportParking* [17], *Slock.it* [18] and *Bitland* [19].

PassportParking [17] is a North Carolina based company that provides parking lot management services utilizing blockchain. The main advantage being the almost zero merchant processing fees that are usually associated with payments. Slock.it [18] has its headquarters in Mittweida, Germany and provides blockchain enabled door locks as well as electric vehicle recharge sockets. These *Slock.it* locks and sockets transact through blockchain with a mobile application, granting the user limited access to the service (access to a hotel room for example). *Bitland* [19], a non-profit real estate company based in Ghana, will be providing title deed registration and tracking as well as authentication services for the Ghanaian Land Commission using blockchain technology.

As Blockchain is well-documented [20] and its source code is in the public domain [21, 22], solutions such as in the examples above are able to be developed and deployed licence and royalty free [23].

This paper builds on the argument that blockchain provides a security infrastructure that is capable of addressing most situations where transactions between two parties need to be recorded securely and irrefutably**.** Abstracting this argument to current mHealth solutions, a case is made that highlights the benefits that blockchain could bring to mHealth security. The reset of the paper is outlined as follows. Section 2 overviews the methodology and poses the research question. Section 3 provides a high level overview of some of the applications of security in mHealth and highlights its limitations. Section 4 explores

potential benefits to mHealth in implementing blockchain and Section 5 concludes with some relevant aspects to consider going forward.

2. Methodology

For the purpose of this paper a scoping review was used to determine the current state of research on blockchain in mHealth towards supporting the argument that blockchain provides a security infrastructure that is capable of addressing most situations where transactions between two parties need to be recorded securely and irrefutably. This study is confined to the study of the current state and limitations of security infrastructure in public mHealth applications only, excluding personal health and private health applications.

This method is supported by Grant and Booth [24] and Davis, et al. [25] for when a researcher has to establish the current state of research in a particular subject area. Colquhoun, et al. [26] define a scoping review as "a form of knowledge synthesis that addresses an exploratory research question aimed at mapping key concepts, types of evidence, and gaps in research related to a defined area or field by systematically searching, selecting, and synthesizing existing knowledge". Davis, et al. [25] clarify that *non- research material* could also contribute to scoping reviews making the method suitable for emerging research areas that are often practice based. Moreover, Arksey and O'Malley [27] and Armstrong, et al. [28] highlight the following reasons for conducting a scoping literature review. A scoping literature review allows the researcher to [27, 28]:

- examine the extent, range and nature of the research activity;
- determine the value of undertaking a full systematic review;
- summarise and disseminate research findings; and
- identify research gaps in the existing literature.

A scoping review was deemed appropriate as the extent, range and nature of research activity around blockchain and implementation would be explored. The scoping included the following databases: ACM digital library, IEEE Xplore, Scopus, ScienceDirect and Pubmed. Harzing's publish or perish software was also used to identify highly cited studies which were not indexed in the databases. Using the Harzing's Publish or Perish software [29], the key words were included in the *All of the words* section, The *Year of Publication* section was between 2000 and 2016. Manual searches for relevant literature was also conducted to identify academic and non-academic publications. The search was conducted in September 2016.

This section provides a high level overview of some of the applications of security in mHealth, touching on the current state of four aspects of mHealth security relevant to the South African Public Health domain:

- the current legal framework,
- current public mHealth implementations,
- state of technology, and
- current ability to audit and evaluate security solutions.

These are argued in the context of how patient information is acquired, stored and processed prior to interfacing to any eHealth enterprise infrastructure. Issues such as the sharing of information between health care providers to optimize patient outcomes therefore are not deemed relevant in the discussion on how mHealth security is implemented.

The discussion below highlights the legal requirements around personal information that is set to regulate the processing of this information. Although currently a South African issue, it is in line with international best practice and has relevance to international practitioners. The *current implementations* section looks at how these legal requirements would impact on broad categories of mobile applications and services. The *state of*

technology section overviews the current mHealth implementations in South Africa and their compliance to the legal obligations. Lastly in the *current ability to audit and evaluate security solutions section,* the auditability of the information transactions as responsibility of NDOH in the South African context is noted.

Current legal framework

November 2013 saw the South African Protection of Personal Information Act (POPI) [30, 31] being adopted by parliament to regulate the processing of personal information. This act further defines the term *processing* as anything done with the personal information, including collection, usage, storage, dissemination, modification or destruction. Accountability for the protection as well as processing of personal information is defined as being held by that of the *responsible party*. This implicates any public or private body or person which, alone or in conjunction with others, determines the purpose of and means for processing personal information. In the context of this paper, the *responsible party,* having the obligation for public health information security, is therefore the South African National Department of Health [32].

Some of the obligations for the NDOH under POPI act [30, 31]are to :

- only collect information that is needed for a specific purpose;
- apply reasonable security measures to protect the information;
- ensure the information is relevant and up to date;
- only hold as much information as needed, for as long as needed; and
- allow the subject of the information access upon request.

POPI [30, 31], originally published on the 26 November 2013[30] has recently been signed into law by the President of South Africa on the 19 November 2016. A grace period of one year is provided for in the act for responsible parties to ensure compliance. As POPI [30, 31] offers a higher level of personal data protection, it therefore supersedes other requirements such as the Companies Act [33]. The *Act No. 4 of 2013: Protection of Personal Information Act* [30] also makes provision for defining Codes of Conduct that guide, in this case for health care practitioners, on the processing of personal information. Within the South African context, the NDOH is to be held responsible for the security of mHealth related applications within public health care.

Implementations

The mHealth development environment in South Africa is described as dynamic and set to grow [34]. HealthEnabled [35] identified 125 mHealth applications available on various mobile app stores for download to Android based devices. These applications can be broadly cast into one of three categories:

- *On-board application*, such as informative and health guides. These applications do not require any personal information to process and therefore no patient information is gathered directly. There is therefore no privacy or confidentiality requirements imposed on this type of mobile application and are not impacted by the POPI Act [30, 31];
- *Interactive connected applications and services*, such as surveys and questionnaires. Surveys and questionnaires typically require either the user to complete a questionnaire on a mobile application, or a facilitator to capture user responses and enter these responses on a mobile application. The main aim of the application or service is the collection and processing of data and is impacted by the POPI Act [30, 31]; and
- *Extended or connected applications or use*, such as screening or diagnostic point of care sensors connected (or paired) to a mobile device. These are typically either operated by the recipient of the treatment or may be administered by a facilitator. These applications collect data and are impacted by the POPI Act [30, 31].

An in-depth review of the specific security levels offered by each one of these category of applications or services is a formidable task and beyond the scope of this paper. Suffice to say that each service or application's development team would have their own strategies and understanding of what security in mHealth entails, and who the accountable entity is. mHealth applications and services within the South African public and private health context will need a security infrastructure that is compliant with POPI [30, 31].

State of technology

The eHealth Strategy of South Africa [2] elucidates the top priorities of the South African National Department of Health. With relation to mobile health, it is stated that "*Mobile technology has provided an opportunity to revolutionise healthcare, especially in countries like South Africa that have the challenges of providing care in deep rural settings but also have a thriving telecommunications market."*

Two of the top ten priorities namely *Applications and tools to support Healthcare Delivery*, and the *Monitoring and Evaluation of the eHealth Strategy* could make use of mobile devices and applications [2]. The National Health Normative Standards Framework (HNSF)[1] lays out the architecture, systems interoperability and standards for public health systems is South Africa on an enterprise level. It includes details of the methods and structures required to store patient information securely, however, this prescription does not extend to mHealth security architecture. Corporate and private sector IT solution providers have addressed similar interoperability issues as experienced in mHealth, and have developed *Enterprise Mobility Management Platforms* [36] that are specifically geared towards managing large fleets of mobile devices for corporates and private sector enterprises. Unlike enterprise security infrastructure and management for servers, routers and desktop PCs, mobile devices are substantially different both in their physical area of operation and in the way they operate, requiring a different set of management and security criteria [36, 37]. In addition, corporate security risk concerns are less around personal privacy or confidentially issues [38, 39] and typically centres on protecting corporate information that is accessed from mobile devices [38].

The National mHealth strategy document of 2015 [40] identifies the top priorities for mHealth implementation, and although interoperability is mentioned, no discussion further than the National Health Normative Standards Framework [41] is available. The fragmented silo'd nature of mHealth implementations have resulted in multiple transaction platforms that are inflexible and difficult to [42] audit.

Current ability to audit and evaluate security solutions

In Bruce Schneier's article Security in the Real World: How to Evaluate Security Technology [43], he refers to forensics as *a big deal.* Schneier [43] argues the "[we] need more mechanisms for evidence gathering, and trusted evidence gathering, in computer systems." As an internationally recognized cryptography and security expert, he [44-46], claims that, although seemingly simple to create, security infrastructure is complex and difficult to test. He reasons that through peer review and hacking attempts to break security, the flaws that emerge within a security infrastructure can be identified and that, arguably, the longer a security infrastructure is being attacked in the public domain, the more secure it becomes. It follows that using a security infrastructure that already exists in the public domain is preferable than attempting to create and evaluate new security protocols and algorithms. It would therefore not be feasible to create and evaluate security infrastructures for every mHealth application that is being developed.

In both the NDOH mHealth strategy of 2015 [40] as well as the eHealth strategy [2], reference is made to the evaluation of security solutions. In the National Health Normative Standards Framework [41] systems architecture of eHealth, *security and auditing* is

describes as a federated service. This implies a centralized service should provide auditing and security services to the eHealth infrastructure.

For public mHealth mobile services and applications to comply with this architecture, it would therefore be necessary for a centralized security service to be able to manage the security infrastructure required on the mobile devices used to implement the mHealth services. The challenge faced in integrating public mHealth applications and services are apparent from the uniquely mobile device management criteria and protocol requirements that are very different for public mHealth as compared to those related to enterprise security. It would therefore be extremely complex and costly to attempt to crowbar enterprise security onto mHealth applications.

A common security architecture will be required for public mHealth applications. This architecture will be substantially different to enterprise mobile security architecture and that whatever form this public mHealth security architecture takes, it needs to be interoperable with the federated eHealth security infrastructure.

3. Potential benefits to South African public mHealth in implementing Blockchain

For Bitcoin implementers, Blockchain technology has provided technology that allows service providers to deliver [8]:

- Secure peer to peer transactions with no need for a trusted third party.
- Digital signatures to safeguard content and thus the integrity of the data
- Transactional chains that store history of ownership providing auditability
- Blockchain that hold transactional order to prove authenticity of transactions.

Implementing blockchain as a security infrastructure could therefore be a viable alternative to the NDOH in fulfilling their fiduciary obligations around, POPI [30, 31], both in the processing of personal information (for example, as blockchain provides traceability, the ability for the NDOH to prove that a patient has accepted a particular version of the terms and conditions of an application is now possible, the encryption of patient information as well as the capturing of the unique identity number of the healthcare worker administering the service) as well as being able to audit security infrastructure as implemented by disparate development teams.

Lessons learnt in the current implementation of Bitcoin need to be investigated. Although substantially different (public health does not require competing ledger-servers on the public network, as public health ledger-servers will be ring-fenced), there may be relevance in understanding those implementation issues and applying them to a public health scenario.

As a practitioner based endeavour, best practices implementation frameworks and guidelines are still being formulated as blockchain is being implemented in different domains.

Additional benefits to the development community includes access to a common open source framework or toolbox on which to build and implement security into their mHealth applications, reference code and reference applications, as well as a seamless compliance to NDOH security requirements.

4. Conclusions

The eHealth architecture caters for security on an enterprise level; however, the requirements to implement mHealth security are fundamentally different and require an alternative framework to deliver secure information.

From the above argument, enterprise mobile security platforms have been successfully implemented in private corporate security solutions, however these do not bode well for a public mHealth solution where mobile bandwidth and mobile data usage are constrained.

Further research has shown that the fragmented and silo'd nature of public mHealth implementations have resulted in multiple transaction platforms that are inflexible, difficult to audit and costly to maintain [42].

Although not a panacea for implementing POPI [30, 31], Blockchain is a well-supported, tried and tested open source security solution that can be rapidly adopted by developers to provide a scaffold for compliance to POPI [30, 31]requirements. On the other hand, self-developed security frameworks often are not secure, complex to audit and result in high risk and costly implementation for the NDOH. By providing the development community with reference code, reference applications and software development toolboxes and libraries, the adoption of such a security framework should lead to a far more integrated and compliance network of mobile applications for public mHealth. Blockchain has the potential to manage the burden of proof for the NDOH by providing the required security necessary to allow compliance with POPI [30, 31] for public mHealth, with the added benefits of provenance and information irrefutability - straight out of the box.

Acknowledgement
Jembi Health Systems for sponsoring participation at IST-Africa 2017 Conference.

References

[1] NDoH and CSIR, "South African National Health Normative Standards Framework for Interoperability in eHealth," in *Government Gazette Version (Government Notice 314, Government Gazette 37583)*, ed. South Africa: South African National Department of Health and Council for Scientific and Industrial Research (CSIR GWDMS Number: 240074), 2014.

[2] NDoH, "eHealth Strategy South Africa 2012," N. D. o. Health, Ed., ed. Pretoria, 2012.

[3] W. Nilsen, S. Kumar, A. Shar, C. Varoquiers, T. Wiley, W. T. Riley*, et al.*, "Advancing the science of mHealth," *Journal of health communication,* vol. 17, pp. 5-10, 2012.

[4] N. Vithanwattana, G. Mapp, and C. George, "mHealth-Investigating an Information Security Framework for mHealth Data: Challenges and Possible Solutions," in *Intelligent Environments (IE), 2016 12th International Conference on*, 2016, pp. 258-261.

[5] M. Plachkinova, S. Andrés, and S. Chatterjee, "A Taxonomy of mHealth Apps--Security and Privacy Concerns," in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, 2015, pp. 3187-3196.

[6] S. Y. Yousafzai, J. G. Pallister, and G. R. Foxall, "A proposed model of e-trust for electronic banking," *Technovation,* vol. 23, pp. 847-860, 2003.

[7] C. Markides, "Disruptive innovation: In need of better theory," *Journal of product innovation management,* vol. 23, pp. 19-25, 2006.

[8] A. M. Antonopoulos, "Mastering bitcoin," 2014.

[9] M. Pilkington, "Blockchain technology: principles and applications," *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar,* 2016.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 21, pp. 120-126, 1978.

[11] D. Eastlake 3rd and T. Hansen, "US secure hash algorithms (SHA and HMAC-SHA)," 2070-1721, 2006.

[12] M. Mainelli and M. Smith, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," *The Journal of Financial Perspectives,* vol. 3, pp. 38-69, 2015.

[13] T. Swanson, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems," ed: R3, Tech. Rep., 6 Apr. 2015.[Online]. Available: http://www. ofnumbers. com/2015/04/06/consensus-as-a-service-a-briefreport-on-the-emergence-of-permissioned-distributed-ledger-systems, 2015.

[14] B. Geva, *The law of electronic funds transfers*: LexisNexis, 2015.

[15] M. Swan, *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc.", 2015.

[16] H. M. Kim and M. Laskowski, "Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance," 2016.

[17] A. Kay and A. Goldberg, "Personal Dynamic Media," *IEEE Computer,* vol. 10, pp. 31-41, 1977.
[18] A. C. Kay, "A personal computer for children of all ages," in *Proceedings of ACM National Conference*, ed Boston: Association of Computing Machinery, 1972.
[19] D. F. P. Keefe, amp, and Z. A., "Annotated bibliography of ubiquitous computing evaluations," 2003.
[20] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," ed, 2008.
[21] D. Keegan, *The Future of Learning: From eLearning to mLearning*: Hagen, Zentrales Institut für Fernstudienforschung, FernUniversität, 2002.
[22] K. Keenoy, *SeLeNe – Preliminary Report:Learning Objects, Meta-Data and Standards*, 2003.
[23] K. R. Lakhani and E. von Hippel, "How open source software works: "free" user-to-user assistance," *Research Policy,* vol. 32, pp. 923-943, 6// 2003.
[24] M. J. Grant and A. Booth, "A typology of reviews: an analysis of 14 review types and associated methodologies," *Health Information & Libraries Journal,* vol. 26, pp. 91-108, 2009.
[25] K. Davis, N. Drey, and D. Gould, "What are scoping studies? A review of the nursing literature," *International journal of nursing studies,* vol. 46, pp. 1386-1400, 2009.
[26] H. L. Colquhoun, D. Levac, K. K. O'Brien, S. Straus, A. C. Tricco, L. Perrier*, et al.*, "Scoping reviews: time for clarity in definition, methods, and reporting," *Journal of clinical epidemiology,* vol. 67, pp. 1291-1294, 2014.
[27] H. Arksey and L. O'Malley, "Scoping studies: towards a methodological framework," *International journal of social research methodology,* vol. 8, pp. 19-32, 2005.
[28] R. Armstrong, B. J. Hall, J. Doyle, and E. Waters, "'Scoping the scope'of a cochrane review," *Journal of Public Health,* vol. 33, pp. 147-150, 2011.
[29] A.-W. Harzing, *The publish or perish book*: Tarma software research Melbourne, 2010.
[30] "Act No. 4 of 2013: Protection of Personal Information Act, 2013," vol. 581, ed. Cape Town, 2013.
[31] L. Kennedy and S. D, "Text Messaging in Practice," J. D. B. G. S. M. S. S. C. Attewell, Ed., ed. London: Learning and Skills Development Agency, 2003.
[32] L. Kennedy and D. Sugden, "Text Messaging in Practice," in *Mlearn 2003 Conference on Learning with Mobile Devices*, London, 2003.
[33] G. J. Rossouw, A. Van der Watt, and D. M. Rossouw, "Corporate governance in South Africa," *Journal of Business ethics,* vol. 37, pp. 289-302, 2002.
[34] Botha and Booi, "The current state of mHealth intervention strategies and implementation in South Africa," presented at the IST AFrica, Durban, South Africa, 2016.
[35] HealthEnabled, "Integrating life-saving digital health solutions into large scale health systems," CSIR, Ed., ed. Presentation made at CSIR: HealthEnabled, 2015.
[36] K. Rhee, W. Jeon, and D. Won, "Security requirements of a mobile device management system," *International Journal of Security and Its Applications,* vol. 6, pp. 353-358, 2012.
[37] T. E. Danford and S. K. Batchu, "Virtual instance architecture for mobile device management systems," ed: Google Patents, 2011.
[38] A. Scarfo, "New security perspectives around BYOD," in *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on*, 2012, pp. 446-451.
[39] K. W. Miller, J. M. Voas, and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," *It Professional,* vol. 14, pp. 53-55, 2012.
[40] N. D. o. Health, "mHealth Strategy 2015 - 2019," D. o. Health, Ed., ed: Department of Health, 2015.
[41] "National Health Normative Standards Framework for Interoperability in eHealth in South Africa," vol. 586, D. o. H. M. Institute, Ed., ed: SA Government printing works, 2014.
[42] A. Botha, M. Herselman, and D. Kotze, "mHealth and Wellness Innovation Ecosystem," in *Strateties , Approaches and Experences: Towards building a South African Digital Health Innovation Ecosystem*, ed Pretoria, South Africa: CSIR Meraka, 2016.
[43] B. Schneier, "Security in the real world: How to evaluate security technology," *Computer security journal,* vol. 15, pp. 1-14, 1999.
[44] (2016, 15 December 2016). *Bruce Schneier*. Available: https://en.wikipedia.org/wiki/Bruce_Schneier
[45] B. Schneier, *Secrets and lies: digital security in a networked world*: John Wiley & Sons, 2011.
[46] N. Ferguson and B. Schneier, *Practical cryptography* vol. 23: Wiley New York, 2003.