Privacy, compliance and the cloud

Chris Mitchell

Information Security Group, Royal Holloway, University of London
me@chrismitchell.net

Abstract Use of the cloud clearly brings with it major privacy concerns. Whilst a range of technical solutions, including use of one of the many variants of homomorphic encryption, potentially enable these concerns to be addressed, in practice such complex privacy enhancing technologies are not widely used. Instead, cloud users, including both individuals and organisations, rely in practice on contractual agreements to help ensure that Personally Identifiable Information (PII) stored in the cloud is handled appropriately. This contractual approach builds on *compliance*, a widely used notion in information security. Specifically, cloud service providers obtain certification of compliance to appropriate security standards and guidelines, notably the ISO/IEC 27000 series, to prove they provide a secure service. To provide privacy guarantees, a standard, ISO/IEC 27018:2014, has recently been published specifically aimed at enabling cloud service vendors to show compliance with regulations and laws governing the handling of PII. This is just the first in an emerging series of standards providing guidelines on cloud security and privacy, as well as more general PII handling in IT systems. This paper reviews the state of the art in such standards, and also looks forward to areas where further standards and guidelines are needed, including discussing the issues that they need to address.

1 Introduction

Almost by definition storing and processing data in the cloud bring major security and privacy concerns, over and above those that apply in any environment where sensitive data is processed. That is, except in the case of a private cloud, owned and operated by the data owner, use of the cloud involves passing control over that data to the organisation providing the cloud service.

From the privacy perspective, a key issue is how PII is handled by the cloud service provider. Indeed, in many jurisdictions the client of the cloud service will have legal responsibilities governing the handling of PII, and these responsibilities

will extend to ensuring that the PII is handled appropriately by any cloud service provider.

To make the nature of these responsibilities a little clearer, we introduce some terminology (all taken from ISO/IEC 29100, [14]). *Personally identifiable information (PII)* is 'any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal'. A *PII principal* is a 'natural person to whom the personally identifiable information (PII) relates'. A *PII controller* is a 'privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing PII other than natural persons who use data for personal purposes'. A *PII processor* is a 'privacy stakeholder that processes PII on behalf of and in accordance with the instructions of a PII controller'. Using this terminology, the PII controller has legal responsibilities governing the processing of the PII it controls, and these extend to ensuring that any PII processors it appoints (such as cloud service providers) process PII in accordance with the law.

There is a range of ways in which a PII controller could try to meet its obligations regarding the protection of PII. One approach would be to avoid any use of the cloud, and retain control of all PII storage and processing 'in house'. However, as has been widely discussed, many advantages arise from the use of the cloud, and so we take it as read for the purposes of this chapter that the PII controller wishes to transfer PII to a cloud provider for storage and processing. In this context, one approach would be to encrypt all PII before transfer to the cloud, and to only decrypt it when it is retrieved from the cloud. However, with conventional encryption techniques, this would prevent the cloud provider doing anything but storing the data, which again limits the usefulness of the cloud. A more sophisticated encryption technique known as *homomorphic encryption* seeks to solve this problem (see, for example, [21]). An encryption technique that is homomorphic with respect to the operator $\circ$ is one which has the property that, for a given key K, the encryption function E satisfies $E(x \circ y) = E(x) \circ E(y)$, for all x and y. Schemes have been devised that are homomorphic for a range of operation types, the goal being to find a scheme which is homomorphic with respect to a set of operations capturing the types of processing likely to be required of a cloud provider. This would then enable the cloud provider to process the data in encrypted form, i.e. so that the cloud provider is able to process data but learns nothing about the data being processed. However, despite huge progress in developing schemes of this type in recent years, the available algorithms remain too computationally complex for routine deployment. This means that, in practice, we must find non-technical means to protect remotely processed PII, which leads to the compliance approach, i.e. where the PII controller seeks to be assured about the deployed security measures and privacy practices of the cloud PII processor.

In this chapter we look at how standards are being developed covering the potentially complex relationship between the PII controller and the PII processor. More specifically, how can PII controllers know whether or not PII processors

will handle PII appropriately, how can PII processors ensure that they meet their obligations to PII controllers, and how can standards help with this?

The remainder of the chapter is organised as follows. In the next section we review the compliance approach, and existing standards directed specifically at PII processing issues. This is followed by an examination of standards currently being developed in this area. Before concluding we look briefly at possible future topics for standardisation in this key area.

2 Compliance – the state of the art

We start by discussing what we mean here by compliance. This necessitates taking a somewhat broader perspective of security management before we return to looking at cloud security and privacy issues in particular. The compliance approach we refer to here is essentially an approach to security management that involves setting up a standards-compliant security management system, and then being audited against compliance with the standards. If the audit is successful, the resulting certification can be used to give third parties confidence that security management is being performed in accordance with accepted norms and practices, as well, of course, as giving the organisation itself confidence that its security management is in accordance with the state of the art.

Such a compliance approach is widely adopted across industry, commerce and government. The main advantage of such an approach is that it disseminates good practice, and encourages the universal adoption of an agreed baseline for IT security. The main disadvantage, as has been widely documented in the literature (see, for example, [5], [20]), is that it encourages a slavish box-ticking approach to security, where minimal safeguards are put in place without appropriate ongoing management and organisation-wide buy-in. However, it could be argued that most of the criticisms are not of the approach itself, but of the way it is implemented, and that organisations which do not implement the standardised approach well would not implement any other approach to security very well either. It is certainly the case that without careful and considered adoption, any approach to IT security will fail, whether it is the compliance-led approach or some other ad hoc scheme. In any event, to a first approximation the compliance approach is the only show in town: it is what we have and it is what is being implemented, and hence it is worth taking very seriously (and enhancing, wherever possible).

The leading contender for such a standards-based approach is based on the ISO/IEC 27000 series of standards. According to ISO/IEC 27000, [9], an *Information Security Management System (ISMS)* consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve

business objectives. It is based upon a risk assessment and the organisation's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS'. As well as defining the concept of an ISMS, ISO/IEC 27000 [9] provides a comprehensive set of related terminology.

In doing so, ISO/IEC 27000 provides the foundation for ISO/IEC 27001, [10], the heart of the ISO/IEC 27000 series. According to its scope statement, ISO/IEC 27001 'specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of the organisation. … [It] also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements … are generic and are intended to be applicable to all organisations, regardless of type, size or nature'. In other words, ISO/IEC 27001 describes what is needed to create and operate an ISMS.

Application of ISO/IEC 27001 is supported by perhaps the best known of these standards, namely ISO/IEC 27002, [11]. ISO/IEC 27002 provides a catalogue of *security controls*, i.e. measures that can be implemented by an organisation to address identified security risks, and associated implementation guidance. This comprehensive set of controls has a long history and has been revised and expanded over time – with origins in a British standard (BS 7799, [1], which became BS 7799-1, [2]) first published in the mid-1990s. In passing we note that ISO/IEC 27001 is also derived from a British standard, namely BS 7799-2, [3], [4].

The controls in ISO/IEC 27002 are organised into 14 categories, covering topics such as information security policies (clause 5), human resource security (clause 7), asset management (clause 8), access control (clause 9), supplier relationships (clause 15), and compliance (clause 18). Within each clause a number of control objectives are defined; there are a total of 35 such objectives. For example, clause 18.1, entitled *Compliance with legal and contractual requirements*, gives the objective 'To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security objectives'. Under each objective are one or more detailed controls, typically with extensive accompanying implementation guidance, which can be deployed to help meet the objective. There are over 100 such controls, ranging from *Monitoring and review of supplier services* ('Organisations should regularly monitor, review and audit supplier service delivery': clause 15.1.2) to *Regulation of cryptographic controls* ('Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations': clause 18.1.5).

The set of controls in ISO/IEC 27002 is intended as a guide to the designers of an ISMS. That is, it is certainly not mandated for any organisation using the ISO/IEC 27001 approach to adopt all the controls given in ISO/IEC 27002; indeed the intention is that the risk analysis performed as part of setting up the ISMS should consider the appropriateness of the controls in the catalogue, and adopt

(only) those that are necessary to address the identified risks. Nevertheless, many of the controls are so fundamental that it is hard to imagine IT systems which do not need their adoption to ensure reasonable levels of security.

Returning to the focus on privacy, it merits note that one of the controls in ISO/IEC 27002 (in clause 18.1.4) is entitled *Privacy and protection of personally identifiable information*, and specifies that 'Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable'. The associated implementation guidance is very general, starting by stating that 'An organization's data policy for privacy and protection of personally identifiable information should be developed and implemented. This policy should be communicated to all persons involved in the processing of personally identifiable information'. It goes on to discuss the need for a privacy policy and also the potential need for a nominated officer in an organisation to manage privacy issues.

This leads naturally to a discussion of ISO//IEC 27018, [13]. This standard is focussed specifically on PII protection when it is processed in the cloud – more specifically when the processing is performed by a public cloud service provider. It provides a set of controls, supplementing ISO/IEC 27002, aimed at cloud service providers who act as PII processors on behalf of a PII controller. That is, the main focus of the standard is not those cloud service providers which act as PII controllers, although the controls in ISO/IEC 27018 will almost certainly apply to such entities (as well as many other controls besides, e.g. as given in the emerging standards ISO/IEC 27017 and ISO/IEC 29151 – see below).

The idea behind ISO/IEC 27018 is that a cloud service provider can have its ISMS audited using the ISO/IEC 27001 system, where the auditor will verify that the risk management process and subsequent ISMS implementation has properly taken into account the supplementary set of controls in ISO/IEC 27018. The certification resulting can then be used to both inform prospective users of the privacy-respecting properties of the cloud service, and also become part of the relevant contractual arrangements when the cloud service is used. It is hoped that this will greatly simplify the task of the PII controller when selecting a cloud service provider.

The set of controls in the standard was derived from a range of sources. Prior to producing the first draft of ISO/IEC 27018, an extensive analysis was performed of existing law relating to the third party processing of PII. The main result of this analysis was a set of 70 controls, which were documented in the original proposal to start work on the standard, published in November 2011, [16]. Only those not already covered in ISO/IEC 27002 were included in the subsequent working drafts of the standard. In July 2012, the European Union published an important review of cloud computing privacy issues, [6]. This was carefully analysed, along with other published opinions, and used to derive a number of additional controls which were included in the second working draft of December 2012, [17]. During 2013 additional input was received from a number of parties, and used to shape the final document published in 2014, [13].

The scope of ISO/IEC 27018 was kept deliberately tight for two main reasons. Firstly, those of us responsible for its development believed it was important to try to publish the standard quickly, and limiting the scope makes rapid progress much simpler. Secondly, the focus of the standard, namely cloud service providers processing PII on behalf of the PII controller, was believed to be particularly important, and hence focussing on this subject made practical sense. Both these motivations appear to have been borne out by experience – the interval between the new work item proposal and publication of a completed standard was a little over 30 months, which is virtually as short a period as is possible within ISO/IEC SC 27, and the standard has rapidly become a 'best seller', at least in the context of ISO/IEC[1]!

Of course ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27018 are only four of a major series of standards known collectively as the 27000 series. Some standards in the series seek to expand upon particular topics addressed within ISO/IEC 27001, including:

- ISO/IEC 27003: *Implementation guidance*, giving more details on the implementation of an ISMS;
- ISO/IEC 27004: *Measurement*, covering security metrics;
- ISO/IEC 27005: *Information security risk management*; and
- ISO/IEC 27006: *Requirements for bodies providing audit and certification of information security management systems*, setting out how certification of ISMSs against ISO/IEC 27001 should be carried out.

Other 27000 series standards, like ISO/IEC 27018, act as a supplement to ISO/IEC 27002, providing an additional set of controls and accompanying guidance for a specific application domain, including:

- ISO/IEC 27011: *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

Note that all these standards are available for purchase from ISO (www.iso.org), IEC (www.iec.ch), and also from national standards organisations such as BSI in the UK (www.bsigroup.com).

Whilst mentioning existing standards of relevance to privacy in the cloud, brief mention should also be given to ISO/IEC 29100, [14], the *Privacy framework*. This standard was published back in 2011, and provides a set of eleven privacy principles (Consent and choice; Purpose legitimacy and specification; Collection limitation; Data minimisation; Use, retention and disclosure limitation; Accuracy and quality; Openness, transparency and notice; Individual participation and access; Accountability; Information security; and Privacy compliance). These principles were used to inform and motivate the supplementary control set given in

[1] For example, ISO/IEC 27018 was listed at number 7 in the April 2015 list of best-selling ISO standards, as published by the Singapore standards organisation – see http://www.singaporestandardseshop.sg/ISOStandards/BestSellingISOStandards.aspx (checked on 9th June 2015).

ISO/IEC 27018. Indeed, the ISO/IEC 27018 supplementary controls are organised according to the eleven privacy principles.

3 Compliance – emerging standards

ISO/IEC 27018 was published in mid-2014. Two other standards directly relevant to cloud privacy, and with somewhat larger scopes, are currently under development. Both ISO/IEC 27017 and ISO/EC 29151, like ISO/IEC 27018, aim to provide a set of controls and associated implementation guidance aimed to supplement those given in ISO/IEC 27002 for a specific application domain. In some sense both of these emerging standards have the focus of ISO/IEC 27018 as a subset.

ISO/IEC 27017, which is nearing completion (as of mid-2015 it was at the Final Draft International Standard stage, [12], the last stage before publication), aims to enhance the set of controls in ISO/IEC 27002 to cover all the security and privacy aspects of operating a cloud service. As stated in the introduction, it 'provides guidelines supporting the implementation of information security controls for cloud service customers and cloud service providers. Many of the guidelines guide the cloud service providers to assist the cloud service customers in implementing the controls, and guide the cloud service customers to implement such controls. Selection of appropriate information security controls, and the application of the implementation guidance provided, will depend on a risk assessment as well as any legal, contractual, regulatory or other cloud-sector specific information security requirements'.

The current draft of ISO/IEC 27017, [12], is, as one might expect, much larger than ISO/IEC 27018; indeed, it is something like half the length of ISO/IEC 27002 itself. It incorporates controls and guidance derived from a wide range of sources including standards and reports from Australia, Hong Kong, the US (including NIST), Singapore, the Cloud Security Alliance, ENISA and ISACA. It looks set to be published in late 2015 or early 2016.

A somewhat complementary focus applies to the development of ISO/IEC 29151, which as of mid-2015 has just reached the committee draft stage, [15]. ISO/IEC 29151 aims to document controls relevant to the protection of PII no matter where it is stored and which entity acts as the PII processor or controller. As it states in the introduction 'The number of organisations processing PII is increasing, as is the amount of PII that these organisations deal with. At the same time, the societal expectation for the protection of PII and the security of data relating to the individuals is also increasing. A number of countries are augmenting their laws to address the increased number of high profile breaches. As the number of PII breaches increase, organisations controlling or processing PII, including smaller newcomers (e.g. small and medium enterprises (SMEs)) will increasingly need guidance on how they should protect PII in order to reduce the risk of priva-

cy breaches occurring, and to reduce the impact of breaches on the organisation and on the individuals concerned. This document provides such guidance'.

The current draft is again an extensive document, and builds on a wide variety of sources. At the current rate of development, publication is likely no earlier than 2017.

We conclude by providing in Table 1 a summary of the current and emerging standards of relevance to privacy compliance in the cloud.

Table 1. Summary of cloud-privacy-relevant ISO/IEC standards

Standard	Title and scope
ISO/IEC 27000:2014	*Information security management systems – Overview and vocabulary*
	Sets the scene for the ISO/IEC 27000 series
ISO/IEC 27001:2013	*Information security management systems – Requirements*
	Defines general principles for an information security management system, including how an ISMS should be established and run – it is the foundation of the ISO/IEC 27000 series of standards
ISO/IEC 27002:2013	*Information security management systems – Code of practice for information security controls*
	Provides a catalogue of generally applicable security controls, to be used as part of an ISMS as defined in ISO/IEC 27001
ISO/IEC FDIS 27017 (2015)	*Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
	Provides supplementary information for ISO/IEC 27002 controls and a set of new controls aimed specifically at the cloud (a superset of ISO/IEC 27018)
ISO/IEC 27018:2014	*Code of practice for protection of PII in public clouds acting as PII processors*
	Provides supplementary information for ISO/IEC 27002 controls and a set of new controls aimed specifically at cloud providers processing PII on behalf of a PII controller
ISO/IEC 29100	*Privacy framework*
	Lays down a general set of privacy principles for information storage and processing
ISO/IEC CD 29151 (2015)	*Code of practice for PII protection*
	Provides supplementary information for ISO/IEC 27002 controls and a set of new controls aimed at all processing and storage of PII (a superset of ISO/IEC 27018)

4 Compliance – future work

Even when ISO/IEC 27017 and ISO/IEC 29151 are completed and in use, the work on standards governing cloud privacy will not come to an end. Apart from anything else, all the standards we have discussed are subject to a continuing process of review and, where necessary, improvement. There are also further areas where standards guidance is needed.

One such area is that of data de-identification, i.e. the processing of PII so that it is no longer linked to a particular individual. Organisations processing PII, including cloud service providers, are required to comply with the applicable privacy-enforcing regulations and laws, which often prevents processing of personal data for purposes other than those for which the data was originally collected. Data de-identification techniques (e.g. pseudonymisation or anonymisation) are widely used as a way of enabling the re-use of large data sets to extract otherwise hidden information (so called *big data*) without endangering user privacy. Such an approach is viable since in many cases the value of processing is maintained even if PII principals are no longer identifiable, directly or indirectly, either by the organisation alone as PII controller or in collaboration with any other party. Additionally, it may be permissible for an organisation to process data for purposes other than those for which the PII principals had given their consent, as long as the data has been rendered into a form in which identification of the PII principals is no longer reasonably feasible, taking into account the state of the art and the organisation's context. That is, de-identification techniques are tools that may enable the wide range of potential benefits arising from data processing to be maintained, whilst respecting privacy regulations and laws.

However, such data de-identification techniques need to be used with great care, not least because of the risk of data re-identification, in which, using contextual or other information, the data can be linked back to an individual. Organisations proposing to use de-identification must therefore carefully define the de-identification measures that are appropriate in their context in order to ensure results that are sufficiently robust given the risks of re-identification. As such it will be extremely helpful to end user organisations, notably the many cloud service providers holding large data sets containing PII, to provide a detailed and practical description of these techniques, including their strengths and weaknesses.

This is an increasingly pressing issue since, in organisations of many types, the amount of data created and potentially being used continues to increase, as do the capabilities of data analytics. Furthermore, the state of the art shows (see, for example, [19]) that achieving robustness in de-identification processes is far from trivial. There is thus a need for a standard that will help organisations in defining and reviewing their processes according to the state of the art and their environment, including their regulatory context. Such a standard would also enable organisations to build trust with a variety of stakeholders (including PII principals,

customers, and data protection agencies) and to establish a common language for transparency regarding their processes.

At its May 2015 meeting in Kuching, WG 5 of ISO/IEC JTC 1/SC 27 (the standards committee responsible for ISO/IEC 27018 and ISO/IEC 29151) agreed to issue a new work item proposal, [18], to create a standard covering data de-identification techniques to address this growing need. The proposed standard will provide information to organisations which aim to use de-identification techniques, with the goal of creating awareness of typical characteristics to consider and to help them avoid common pitfalls.

The new work item proposal, [18], has an attached preliminary working draft, which draws extensively on a recent Article 29 Working Party report, [7]. Apart from a comprehensive set of definitions of terminology, intended to enable unambiguous discussions of de-identification, the new standard is expected to contain clauses covering the usability of de-identified data, the risks of re-identification, techniques for pseudonymisation, and techniques for achieving and metrics for measuring anonymisation. It will also draw on an existing health-sector-specific ISO technical specification on pseudonymisation [8].

5 How effective is the compliance model?

As already discussed, the compliance model has been widely criticised, not least for encouraging a 'box-ticking mentality'. However, without doubt ISO/IEC 27002 (and its predecessors) has done much to inform organisations of the fundamental techniques of information security management. For better or worse it would appear that use of the 27000 series standards is considered as a fundamental part of security management for almost every large organisation, at least in the western world.

One could reasonably ask critics of the compliance approach whether they would rather employ a cloud service provider which has verified that its security and privacy practices conform to the state of the art or one which has not. It seems hard to argue in favour of the latter. Indeed, the author is not aware of any research calling for routine security management measures to be abandoned; instead, what seems to be needed are better ways of managing the human side of security management. The compliance approach is still evolving, and there is clearly no cause for complacency. Ultimately there is no replacement for good management practices, both within IT and more broadly, and the 27000 series standards are just one part of the overall information security solution.

6 Concluding remarks

We have attempted to review both recently published and emerging international standards of relevance to privacy, and in particular PII protection, in the cloud. ISO/IEC 27018 has made a significant in the short period since it was published, and will be joined in the near future by ISO/IEC 27017, and, later on, by ISO/IEC 29151. In the longer term future, it is hoped that we will see the development of detailed guidance on de-identification techniques, enabling greater confidence that data collected through the provision of cloud services is used for greater societal benefit in ways which respect end user privacy.

References

[1] BS 7799:1995, *Code of practice for information security management*.
[2] BS 7799-1:1999, *Information security management – Part 1: Code of practice for information security management*.
[3] BS 7799-2:1999, *Information security management – Part 2: Specification for information security management systems*.
[4] BS 7799-2:2002, *Information security management systems – Specification with guidance for use*.
[5] B. Duncan and M. Whittington, *Reflecting on whether checklists can tick the box for cloud security*. In: *Proc. of 2014 IEEE 6th International Conference on Cloud Computing Technology and Science*, IEEE (2014) pp.805-810.
[6] European Union, Article 29 Working Party, *Opinion 05/2012 on Cloud Computing*, adopted July 2012.
[7] European Union, Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, April 2014.
[8] ISO/TS 25237:2008, *Health informatics – Pseudonymization*.
[9] ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
[10] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.
[11] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.
[12] ISO/IEC FDIS 27017 *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*, July 2015.
[13] ISO/IEC 27018:2014, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.
[14] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.
[15] ISO.IEC 1st CD 29151, *Information technology – Security techniques – Code of practice for personally identifiable information protection*, June 2015.
[16] ISO/IEC JTC 1/SC 27 N10550, *Proposal for a new work item on Code of practice for data protection controls for public cloud computing services*, November 2011.
[17] ISO/IEC JTC 1/SC 27 N11742, 2nd WD 27018, *Information technology — Security techniques — Code of practice for data protection controls for public cloud computing services*, December 2012.
[18] ISO/IEC JTC 1/SC 27 N15297, *Proposal for a new work item on Privacy enhancing data de-identification techniques*, June 2015.

[19] S. Ji, W. Li, N. Z. Gong, P. Mittal and R. Beyah, *On your social network de-anonymizability: Quantification and large scale evaluation with seed knowledge*. In: Proc. NDSS '15, Internet Society, 2015.
[20] J. Kwon and M. E. Johnson, *Proactive versus reactive security investments in the healthcare sector*. MIS Quarterly 38 (2014) pp.451-471.
[21] M van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, *Fully homomorphic encryption over the integers*. In: Proc. Eurocrypt 2010, Springer LNCS 6110 (2010) pp.24-43.