PRISMACLOUD preprint of:

T. Lorünser, S. Krenn., Ch. Striecks, **Th. Länger** 2017 Agile Cryptographic Solutions for the Cloud. In e & i Elektrotechnik und Informationstechnik, September 2017, ISSN: 0932-383X (printed version) ISSN: 1613-7620 (electronic version) (2017)

# Agile Cryptographic Solutions for the Cloud

Thomas LORÜNSER[a], Stephan KRENN[a],
Christoph STRIECKS[a], Thomas LÄNGER[b]

[a] *AIT Austrian Institute of Technology GmbH, Center for Digital Safety and Security, Austria*
[b] *University of Lausanne, Department of Information Systems, Switzerland*

## Zusammenfassung

Mit einem Jahresumsatz im Bereich von 150 Milliarden US Dollar ist Cloud Computing heute der am schnellsten wachsende Sektor im Bereich Informationstechnologien. Doch die Grundlage von Cloud Computing, welches auf dem Outsourcing von Daten und Verarbeitungen beruht, bringt naturgemäß Probleme für die Informationssicherheit und Privatsphäre mit sich. Obwohl die kryptografische Forschung in den letzten Jahren signifikante Fortschritte gemacht hat und im Bereich Cloud Computing eine ganze Reihe von innovativen, anwendbaren Verfahren zur Verfügung stellt, werden diese nicht in nennenswertem Umfang praktisch eingesetzt. Wir werden in dem vorliegenden Artikel die größten Hindernisse analysieren, die einer weiten Verbreitung von kryptografischen Verfahren in Cloud Services im Wege stehen, und aufzeigen, wie dem mittels organisationeller und prozeduraler Methoden entgegengewirkt werden kann. Zum Abschluss möchten wir einige dieser neuartigen Verfahren vorstellen, und aufzeigen, was deren Einsatz zu einem wirkungsvollen Schutz von End-User-Daten beitragen kann.

Schlüsselwörter: Cloud Computing, Kryptografie, Security, Privacy

## Summary

Cloud computing, with its estimated market size of 150 billion USD annual turnover, is one of the major growth areas in information and communication technologies today. As a paradigm building on outsourcing of storage and processing, cloud computing suffers from intrinsic security and privacy problems. But cryptographic research has made substantial progress over the last years and provides today a portfolio of mature cryptographic primitives and protocols suitable for addressing several of these problems in an effective and efficient way. Nevertheless, today's reality shows that there exists a gap between what is possible and what is actually available in the cloud. We will present a detailed analysis of inhibitors and roadblocks standing in the way of an extensive deployment of cryptographic protection to cloud services, and how organizational and procedural measures may support the practical deployment of cryptography. We conclude our article with an overview of novel cryptographic schemes and their potential for protection of end-user data during storage and processing in the cloud, once they will become widely available.

Keywords: cloud computing, cryptography, gap analysis, end-user security, end-user privacy.

## 1. Introduction

Cloud computing is a state-of-the-art paradigm for the delivery of IT resources and mainly builds on the concept of IT outsourcing, which has intrinsic security and privacy problems. Cryptography is considered a viable technology to deliver the best protection possible in third-party infrastructures. However, today's most widely used cryptographic solutions are not suitable for direct adoption in the cloud. Clouds are very dynamic environments also supporting new ways of collaboration, requiring manipulation, sharing, and processing of data in a very agile way. Therefore, new cryptographic methods are needed to protect data under these conditions and to enable new security enhanced services. Today cryptography is mostly used to protect the data in transit from and to the cloud, or for user authentication, but not for the protection of data inside the cloud infrastructure.

However, in the scientific world, a large body of work on new cryptographic primitives has been proposed. Many new primitives were studied, and we have access to a large repository of novel technologies already mature enough to be integrated in cloud scenarios with only little research and development effort required. Nevertheless, we do not see real adoption of these technologies in the cloud market and it is not obvious why the adoption is hampered.

In this article, we provide an anamnesis of the current use of cryptography to mitigate or reduce most of the prevailing security and privacy risks in cloud services. In Section 2 we analyze the gap between what is possible and what is currently deployed and try to explain why that is the case. In Section 3, we present strategies we identified and developed to overcome the problem in our ongoing research projects. In Section 4, we present some crypto schemes of interest for the CSC (cloud service customer) and cloud service provider (CSP) and identify challenges to successfully bring them to market. We briefly conclude in Section 5.

## 2. Inhibitors of Cryptography in the Cloud

In this section, we present an analysis of possible roadblocks for the adoption of modern cryptography in cloud computing and present our hypotheses, as why there is a gap between what is possible and what is currently used. These hypotheses are based on our experience from various collaborative research projects in the domain of applied cryptography in the cloud.

### 2.1. Complexity and Insufficient Specifications in the Literature

In our opinion, a major reason why practitioners often do not pick cryptographic protocols is the high complexity of the implementation process itself, which again has two main challenges. First, it requires substantial domain-specific precise knowledge in the field of cryptography to be able to translate the specification provided in a cryptographic publication into a specification that a software engineer can use. This includes not only the correct choice of parameters such as key sizes, but also the ability to resolve abstract notations used by theoreticians, which are often very compact and hide lots of the concrete complexity from the reader. The second challenge is that the secure implementation of cryptographic applications requires substantially more experience and knowledge from a software engineer than other less security sensitive implementation tasks. Besides the correct implementation of the specification per se, also non-standards aspects like side-channel security (to protect, e.g., against timing attacks) need to be considered. Overall, this makes the secure, sound, and efficient realization of cryptographic protocols published in literature a time-consuming, expensive and potentially error-prone task.

An additional challenge is given by the fact that despite rigorous and formal protocol specifications and proofs, the real-world deployment of cryptographic primitives often remains unclear because of a gap between the idealized world used by theoreticians and the real world. For instance, issues like key distribution or also the ubiquitous access to certain parameters or common reference strings is often assumed in theory, but in practice, it often remains unclear how the honest generation and authenticity of such common input can be verified if needed.

### 2.2. Requirements Engineering

Although it is common practice to motivate cryptographic research with real-world applications, even in theoretical research, this kind of motivation is often rather artificial and does not map well to real-world problems. Specifically, the motivation aims at convincing other cryptographers rather than practitioners. Therefore, the gap between cryptographic theory and practice used to be huge. The smart grid domain is a good example for this. A huge amount of protocols with all kind of advanced features has been proposed in literature, but when asking domain specialists, almost none of these solutions are fit for real world use cases because neither the needs of the operators nor the legal framework are considered.

However, in the recent years, events such as the annual “Real-World Cryptography Symposium” – where mostly practically efficient cryptography is presented – try to aim at the early adoption of well-researched cryptography for practical applications. Furthermore, since the Snowden revelations, awareness even on the theoretical side is raised to participate in social, economic, and political debates [Rog15]. This is a first initiative to bring together theoreticians as well as practitioners but still not enough to ensure prosper exchange between these communities.

### 2.3. Market Aspects and Differentiators

Currently, we see only little commercial interest in comprehensive practical usage of cryptography in the cloud. The lack of good security and privacy practice in general is often caused by its missing visibility. The used technology is mostly transparent to users and in the ideal case “just works”. In addition, if products are upgraded or hardened with cryptography, there is normally no gain in functionality that is visible to a user, hence, the added value is hard to grasp.

Furthermore, the reason why the best suited cryptographic solutions are often not used in applications is often missing awareness on the technology side due to a lack of communication between researchers, developers, security professionals, and end users. For developers and architects it is not easy to understand what could be possible and which solutions really have practical relevance. Some demonstrators and easy accessible software tools would be a good starting point to improve this communication. Specifically, open-source software and hardware could be an enabler in this respect.

Cryptographic protection from provider related threats does in many situations also mean excluding the provider itself from access to plaintext data. This can potentially have a large impact on provider-business models, especially in the consumer market where free services are standard nowadays. Providers would no longer be able to exploit user data nor promote additional services based on that data, which should be a no-go anyhow in the business-to-business segment. Moreover, missing standards and certifications make it hard for business customers to compare offerings and to understand or promote the added values. It also makes it hard for the provider to monetize the increased effort.

## 3. Promoters of Cryptography Usage in the Cloud

In the following, we propose solutions and methodologies, as well as necessary environmental conditions identified to foster and support a more widespread use of cryptography in cloud-based applications, i.e., to improve the protection of data throughout its life cycle in modern ICT systems.

## 3.1. Service and Tool Based Approach

From our collaboration with industry we learned that providing readymade cryptographic software and hardware tools to system developers is a key for actual adoption. Furthermore, the tools should also be easily configurable and usable without cryptographic knowledge. If tools are too basic in their functionality, the probability for misconfiguration and wrong usage is extremely high, therefore, the tools should have an easy to understand application programming interface with only a limited set of options and, ideally, already come preconfigured for most typical application scenarios.

In some cases it is even important to provide tools for code generation, e.g., like demonstrated in EU FP7 project CACE (Computer Aided Cryptography Engineering): among others, developed tools for automatically translating abstract specifications of zero-knowledge proofs into concrete protocols and documentation [ABB+12,ABB+10].

For cloud computing, this concept can even be put further. The tools can even be integrated in ready-made security enhanced cloud (micro-)services to make it even easier for developers to integrate them into applications. Thus, we can further reduce the knowledge required for system architects and developers and, therefore, significantly lower the entry bar for integration of cryptography into applications. This concept is due to the trend of modularization and (micro-)service-oriented architectures driven by cloud technologies.

In order to systematically address the problem of multidisciplinarity and the broad range of skills required, we proposed a new 4-tier architecture for the development of cryptographic cloud-based applications [LSL+16]. The architecture encapsulates expert knowledge required for theoretical cryptography, implementation of cryptography, as well as tools and services development into layers and define interfaces between them. These interfaces have an equivalent with the natural interfaces found between disciplines involved in bringing novel cryptographic techniques to practice, e.g., the mathematics is completely encapsulated and, thus, hidden from the software experts, enabling them to leverage results in an easy and secure way.

## 3.2. Standardisation and Compliance to Regulation

Although standardisation of security controls and services, or the underlying cryptography mechanisms can be a tedious process, it provides multiple opportunities for an accelerated uptake of cryptographic cloud solutions. Standards for clouds exist on different layers and levels, and there are several standardisation organisations active in this field, most notably the International Organization of Standardisation (ISO) that together with the International Electrotechnical Commission (IEC) formed the Joint Technical Committee 1 (JTC1), active in two sub-committees in cloud standardisation: SC38 and SC27. On a global level, there is also the International Telecommunication Union ITU, an agency of the United Nations active in cloud standardisation. On a European level, there are mainly the European Telecommunications Standards Institute ETSI and European Committee for Standardization CEN/CENELEC active in that field. Other important European actors, who are not exactly standardisation organisations but nevertheless setting important reference, are the European Union Agency for Network and Information Security ENISA, the EuroCloud consortium, and in the field of cloud privacy the European Data Protection Board EDPB. There is also a plethora of other interest groups and consortia actively trying to influence standardisation while the big market dominators, e.g., Amazon and Google, are setting “de facto” standards by propagating their proper solutions.

Low-level standards of interest for us are basic standards for cryptographic primitives, like ISO/IEC 19592 for the secret-sharing primitive. Such standards codify and disseminate a state of the art and help avoid proprietary cryptography. They provide a level playing field for competitors and support increased security and privacy by defining “sound cryptography”. Basic standards define ontologies, concepts, and reference architectures, and in particular, standards for portability and interoperability can bring more and better choices for the end user. Standards for cloud service level agreements (SLAs), as the ISO/IEC 19086 series, help end users to establish comprehensive and fair contracts with cloud providers and make cloud services comparable. High-level standards define capabilities of cloud services for different domains, like e.g. for eHealth (see, e.g., the http://www.eStandards-project.eu homepage, accessed 1.8.2017) and other e-domains. Compliance to such high-level standards supports the emergence of new markets and builds confidence among cloud users (end users, service providers).

The upcoming European General Data Protection Regulation GDPR will likely also have a major influence on cryptography usage in the cloud. From May 2018 on, it will govern the rights to the protection of personal data for roughly 500 million citizens of the European Union. The GDPR will impose strict regulation not only on the data controllers, but also on the processors, i.e., the cloud providers who will have to tightly protect their customers' data or face significant fines in case of a breach. This will certainly provide additional motivation for cloud providers to deploy cryptography to their cloud offerings, and adherence to established standards will provide them better cryptography, and also a justification of diligent protection, in case a breach happens despite cryptographic protection.

### 3.3. Security and Privacy Patterns

Another issue of importance with regard to usability is, that different stakeholder groups are involved in the design and implementation of cloud-based applications, and they need to be able to communicate requirements and capabilities across disjunctive domains of expertise. In our case of cryptographically secured cloud applications, there are end users, application designers, cloud service designers, and the cryptographic tools designers as well as cryptographers who need to share a common understanding. The tools designers and the cloud service designers need to understand the requirements of the end users, while the cloud service designers need to understand the capabilities of the cryptographic tools so that they employ them in a correct way in the cloud services they design. These complex requirements can efficiently be addressed by using design patterns, and specifically cloud security and privacy design patterns, as well as human computer interaction (HCI) patterns.

Design patterns are a means to codify expert knowledge and requirements in a way that the information remains accessible across domains of involved actors. In information technologies, the concept was initially applied in software architecture, where object oriented design and re-usability requires efficient communication of complex issues across different domains. Later on, the concept was used for the specification of security and privacy patterns in general, and for the specification of cloud security and privacy patterns in particular, e.g., in [LPG16]. [FKP+10] contains a catalogue of specific, practically tested user interfaces for complex security and privacy technologies in the form of HCI patterns. All these design patterns have in common that they are defined across a set of categories and characterizations in natural language. Such categories give a *summary description*, describe the *context* (where the pattern is applicable), list *intentions* (end user values, or in case of security patterns, security properties covered), state the *problem* (empirical background, range of manifestations), present a *solution* (how a general arrangement of elements may solve the problem), list *known uses* of the pattern etc. These are the most common categories used in a pattern description, while the actual categories may vary in different pattern catalogues.

## 4. Cryptographic Schemes for Fast Adoption

In this section, we focus on most promising candidates for integration in commercial cloud offerings or even on top of them as an additional security layer. These technologies have also been selected by the two EU-funded Horizon 2020 research projects PRISMACLOUD and CREDENTIAL[1]. Many more technologies can be found in the literature for all kinds of task, e.g. searchable encryption, verifiable

[1] https://prismacloud.eu; https://credential.eu (both accessed 1.8.2017)

computing or oblivious RAM, to just name a few of them, but these are out of scope for the current analysis.

Furthermore, we focus on technologies targeting data at rest, data in use, and particular privacy enhancing technologies. Protecting data in move in point-to-point communication channels can be considered as a solved problem.

## 4.1. Secret Sharing

Secret sharing [Bla79, Sha79] in its very pure form is more an encoding technique than an encryption scheme. The basic idea of secret sharing is the distribution of trust. A (*k*,*n*)-scheme provides two main algorithms, one takes a message as input and generates *n* fragments – so called shares – whereby *k* of them are needed to reconstruct the plaintext. Security of shared messages is then established by storing the fragments on different servers or trust zones.

*Applications*: Secret sharing is well suited to increase security and availability in cloud-storage applications [LHS15]. If shares of data can be stored in different trust zones, security is increased for data breaches of single shares. Moreover, because *k*-out-of-*n* threshold schemes can be used, the availability can also be increased and data can be protected from data loss, too. Ideally, multiple providers are used to disperse the data.

*Challenges*: There exist completely different security models, which are often hard to understand. Although some forms of secret-sharing schemes provide even information-theoretic security, i.e., they are considered to be secure against very strong adversaries, this property is only guaranteed by the non-collusion assumption, i.e. that the providers holding the single shares do not maliciously cooperate. Unfortunately, this assumption is hard to grasp and to guarantee, and very different to the well-established model of private and public-key cryptography. Nevertheless, secret sharing and information dispersal are versatile encoding methods, adding additional security, increasing availability and resiliency in many scenarios with features such as batch-verifiability [KLS17]. Standardization is ongoing and first drafts are already available which we expect, will give a further push to the adoption.

## 4.2. Attribute-Based Encryption

Attribute-Based Encryption (ABE) [GPS+06] is a cryptographic encryption primitive, capable of enforcing attribute-based access control (ABAC) solely on a cryptographic level. Previous solutions suffered from the drawback that encryption schemes were equipped with software-enforced ABAC systems—which requires significant trust in the security guarantees of the software implementations. In the most basic form, ABE assigns attributes, e.g., “Scientist”, “Engineer”, and “AIT”, to users. In this sense, ciphertexts can be created with respect to some access policy, e.g., (“Scientist” .and. “AIT”) .or. “Engineer” which loosely speaking means that any scientist working at AIT or any engineer can access the plain text while at the same time no scientist not working at AIT is able to decrypt.

*Applications*: The ABE primitive has huge potential in cloud computing, mobile, and IoT where one does not want to rely on software-based ABAC mechanisms. For example, in the cloud computing scenario, encrypted data sharing can easily be done with ABE where the data to be shared is encrypted according to some policy and no software-based access control is needed.

*Challenges*: ABE is a very active field of research with several publications on very mature and expressive ABE systems available today [GVW15]. Unfortunately, ABE is less used in real-world scenarios and, in particular, no standardization activities have been carried out so far. Currently, the European Telecommunication Standards Institute (ETSI) is addressing this issue and has established a specialist task force to draft a protocol specification on ABE.

## 4.3. Proxy Re-Encryption

Proxy Re-Encryption (PRE) [BBS98] is a cryptographic primitive, which involves a semi-trusted proxy, which gets empowered by a legitimate recipient (delegate) of a ciphertext to re-encrypt it for a different receiver (delegatee). This primitive can be seen as an extension of public-key encryption that allows for delegating decryption rights of ciphertexts via a semi-trusted proxy to other parties. More concretely, the semi-trusted proxy is capable of translating ciphertexts under the delegator's public key into ciphertexts under delegatees' public keys using so-called re-encryption keys. Thereby, the proxy need not learn any information about the underlying plaintexts.

*Application*: PRE is for example very useful in encrypted e-mail forwarding or storage-based data sharing and has been subject of significant research. Specifically for cloud-based data sharing, PRE is a very promising candidate. In a typical scenario, the message can be encrypted under the own public key and stored on a remote server, which can be a public cloud service. Decryption rights are then given by generating re-encryption keys for the remote server. Hence, the remote server is able to translate the ciphertext to the public key of the delegate, which then is able to decrypt.

*Challenges*: PRE has already extensively been considered for the above scenario, however, current security definitions are not compatible with the standard data-sharing scenario in dynamic groups. In particular, the established security model allows schemes which enable a receiver of a re-encrypted ciphertext to be able to decrypt all re-encryptable ciphertext which clearly puts shared encrypted data at risk once access is revoked (by deleting the re-encryption key). Thus, further research is required to close the gap in the security model of PRE and, furthermore, additional forward-secure variants of PRE need to be proposed, which also protect from key leakage at the remote server.

## 4.4. Redactable and Sanitizable Signatures

Redactable Signature Schemes (RSS) [JMS+02] and sanitizable Signature Schemes (SSS) [ACN+05] are digital signature schemes allowing for controlled modification by a potentially semi-trusted third party. This is a quite counterintuitive idea, and contrary to standard digital signatures which become invalid as soon as a single bit on the protected message is changed. In the case of RSS and SSS, the authenticity of subsequently modified content is preserved. In a nutshell, SSSs allow a designated third party, named the sanitizer, to change, i.e., sanitize, signer-chosen parts of a signed message while RSSs allow to censor, i.e., redact, parts of a signed message.

*Applications*: Although this concept seems rather non-intuitive, there are many real-life use cases where support for subsequent alterations by external parties are valuable, especially when personal or sensitive data is handled on remote parties or clouds. RSS thus supports privacy preserving data minimization by blacking out specific information of a signed dataset, non-essential for a specific purpose, without destroying the authenticity of the remaining (not blacked out) data.

*Challenges*: A lot of progress has been achieved on a technical level and many open problems have been solved. The main problems of adoption are: missing legal framework and standards supporting policies; complexity needs to be reduced; clear new use cases with new features and usage patterns need to be defined.

## 4.5. Attribute-Based Credential Systems

Privacy-enhancing attribute-based credential systems (also ABCs or anonymous credentials) [CKL+15] are a cryptographic primitive enabling user-centric identity management. ABCs are cryptographically well established and allow for strong user authentication, while still respecting user privacy and giving users full control over the data that is revealed. In a basic ABC system, a user receives a credential from an issuer, certifying certain information such as name or date of birth. Later, when the user wants to authenticate towards a service provider, he/she can decide which information to reveal or to keep private. This can be done in a way guaranteeing to the user that no two actions can be linked, even by maliciously colluding service providers and issuers.

*Applications*: The importance of such data minimization techniques has been recognized by the European Commission and the US government. Although a large body of research has been put into ABCs and mature implementations exist in industrial products, e.g. IBM's Identity Mixer and Microsoft's U-Prove, they never have been widely adopted.

*Challenges*: One main challenge is the cloudification of ABCs for easier access independent of devices and locations. While preservation of the same privacy is not possible in the cloud, a reasonable trade-off should be found to unleash the potential of data minimization. Unfortunately, up to date, all known ABC systems require access to all attributes in the clear at the time of proving possession of a credential to a third party. This makes it hard for privacy-preserving identity management systems as a service, as the user still needs specific key material and/or dedicated software locally, e.g., on a mobile device. Furthermore, the user is required to be online. The idea is to propose a new cloud-based ABC system where a dedicated cloud service (a so-called “cloud wallet”) can present unlinkable and authenticated possession of user credentials to a third-party without accessing the attributes in the clear. This would enable new privacy-preserving applications of ABCs in the cloud.

## 5. Conclusion and Outlook

In this article, we identified several challenges and inhibitors standing in the way of an adoption of cryptographic techniques for increased end user security and privacy protection in the cloud. A gap exists between existing, mature results of cryptography research and the practical application of these results in cloud services. In the H2020 projects PRISMACLOUD and CREDENTIAL we are counting on several promoters to improve this situation with a positive outcome for the end user. We are using security and privacy patterns to make the technologies accessible by a broad audience, including cloud service developers, cloud providers, and prospective end users. Especially cloud providers may find how they can comply with legal requirements, as e.g. demanded by the upcoming European General Data Protection Regulation, and end users can see what they may ask for from cloud service providers. Introducing technologies into ISO standards is another opportunity to make these technologies known and to increase the trust in their security and privacy providing capabilities. As regards practical application, we will provide a software toolkit and several reference cloud service implementations, the capabilities of which we will demonstrate in three use cases from the domains of eHealth, eGovernment, and Smart Cities.

## Acknowledgement

This work has been done in projects that have received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 644962 (PRISMACLOUD) and no 653454 (CREDENTIAL).

## References

[ABB+10] J. B. Almeida, E. Bangerter, M. Barbosa, Stephan Krenn, A.-R. Sadeghi, T. Schneider. *A Certifying Compiler for Zero-Knowledge Proofs of Knowledge Based on Sigma-Protocols*. ESORICS 2010: 151-167.

[ABB+12] J. B. Almeida, M. Barbosa, E. Bangerter, G. Barthe, S. Krenn, S. Zanella Béguelin. *Full Proof Cryptography: Verifiable Compilation of Efficient Zero-Knowledge Protocols*. ACM CCS 2012: 488-500.

[ACN+05] G. Ateniese, D. H. Chou, B. de Medeiros, G. Tsudik. *Sanitizable Signatures*. ESORICS 2005: 159-177.

[Bla79] G. R. Blakley. *Safeguarding cryptographic keys*. Proceedings of the National Computer Conference 48: 313-317 (1979).

[BBS98] M. Blaze, G. Bleumer, M. Strauss. *Divertible Protocols and Atomic Proxy Cryptography*. EUROCRYPT 1998: 127-144.

[CKL+15] J. Camenisch, S. Krenn, A. Lehmann, G. L. Mikkelsen, G. Neven, M. Ø. Pedersen: Formal Treatment of Privacy-Enhancing Credential Systems. SAC 2015: 3-24

[EC12] European Commission. *European Cloud Computing Strategy: Unleashing the Potential of Cloud Computing in Europe.* COM(2012) 529 final.

[FKP+10] S. Fischer-Hübner, C. Köffel, J.-S. Pettersson, P. Wolkerstorfer, C. Graf, L.-E. Holtz, U. König, H. Hedbom und B. Kellermann, *FP7 Project PrimeLife D4.1.3 - HCI Pattern Collection, Version 2;* available at http://primelife.ercim.eu/results/documents/ (accessed 1.8.2017) , 2010

[GPS+06] V. Goyal, O. Pandey, A. Sahai, B. Waters: *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*. ACM CCS 2006: 89-98.

[GVW15] S. Gorbunov, V. Vaikuntanathan, H. Wee. *Attribute-Based Encryption for Circuits*. J. ACM 62(6): 45:1-45:33 (2015).

[JMS+02] R. Johnson, D. Molnar, D. Song, D. Wagner. *Homomorphic signature schemes*. In CT-RSA 2002: 244-262.

[KLS17] S. Krenn, T. Lorünser, C. Striecks. *Batch-Verifiable Secret Sharing with Unconditional Privacy*. ICISSP 2017: 303-311.

[LSL+16] T. Lorünser, D. Slamanig, T. Länger, H. C. Pöhls. *PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services*. ARES 2016: 733–741.

[LHS15] T. Lorünser, A. Happe, D. Slamanig. *ARCHISTAR: Towards Secure and Robust Cloud Based Data Sharing*. CloudCom 2015: 371–378.

[LPG16] T. Länger, H. C. Pöhls, S. Ghernaouti. *Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds.* APF 2016: 115-132.

[Rog15] P. Rogaway. *The moral character of cryptographic work*. Cryptology ePrint Archive, Report 2015/1162. 2015.

[Sha79] A. Shamir. *How to Share a Secret*. Commun. ACM 22(11): 612-613 (1979).