Journal of Advances in Science and Technology
Vol. II, Issue, I, August-2011, ISSN 2230-9659

Data Security in cloud computing

Pradeep. K. Deshmukh

Asst. Professor, Computer Engg. Dept. Rajashree Shau College of Engineering Pune India

Abstract: **Cloud computing sees a technical and cultural shift of computing service provision from being provided locally to being provided remotely, and en masse, by third-party service providers. Data that was once housed under the security domain of the service user has now been placed under the protection of the service provider. Users have lost control over the protection of their data: No longer is our data kept under our own watchful eyes.**

This thesis investigates how Predicate Based Encryption (PBE) could be leveraged within the Cloud to protect data. PBE is a novel family of asymmetric encryption schemes in which decryption of a cipher-text is dependent upon a set of attributes satisfying a certain predicate, allowing for selective fine-grained access control to be specified over cipher-texts.

It is argued that obfuscation of one's data is not enough when seeking to protect data. The control of how one's data is used and the trust afforded to service providers is equally as important. To this end, three archetypal scenarios are described that illustrate ways in which service users could specify precisely with whom they wish to share their data, for what purpose, and for how long. Furthermore, two additional scenarios are presented that would allow a service provider to facilitate keyword search over encrypted data using expressive queries supporting conjunction and disjunction of terms.

----------♦----------

CONCLUSION

Cloud Computing embodies the as-a-Service paradigm and allows for services to be provided en masse to consumers. The problems associated with the use of cloud based services can be summarised by the unknown risk profile (see Section 3.8) and unknown expectation of privacy—see Section 3.9.2. When service users push data to the cloud they need to rely upon Cloud Service Providers (CSPs) adhering to their remit, and doing so dutifully. However, when looking to build solutions to protect data in the cloud it is important to remember that for the service user the CSP can be trusted, albeit at arm's length—see Section 6.3. The threat models presented in Chapter 4 illustrate that threats to data occur both in the domain of the service user and the domain of the CSP. Traditional privacy models are too user-centric and CSP-fearing when trying to address the problem of protecting data—see Section 6.2. A privacy model centred around Kafka's The Trial helps to address this problem, this privacy model indicates that when protecting one's data one should also have control over its use rather than solely preventing its collection: CSPs and service users need to work together.

Predicate Based Encryption (PBE) presents an interesting and also novel family of asymmetric encryption schemes. PBE combines Attribute Based Access Control (ABAC) with asymmetric encryption, allowing for a single-encrypt or/multi-decrypt or environment to be realised using a single scheme. Replicating such functionality using more traditional techniques requires a more complex approach—see Section 10.2. Even so, PBE is inherently more flexible, data can be encrypted for a decrypting entity prior to the creation of the decrypting entity's decryption key: The precise list of decrypting entities need not be known a priori. Such novelty lies with the cryptographic keys—see Section 10.1. Cryptographic keys are not just numbers, there is no one-to-one pairing of encryption and decryption keys, and encryption and decryption keys are created separately from each other.

Though understanding the operation and potential use of PBE schemes was not inherently difficult it was not trivial either. Understanding the means through which PBE schemes can be constructed also proved to be a somewhat tedious affair. Unfortunately with PBE, a disproportionate amount of time was spent searching for, and collating, information from different sources; different papers begat different schemes which in turn begat different terminology. However, these efforts were not without dividends, by learning more about PBE scheme construction, various issues surrounding cryptographic keys were identified and addressed. For instance, blinding values prevent decrypting entities from combining their decryption keys—see Section 8.6.2. The inclusion of numerical attributes also presents an underlying hidden cost (see Section 10.5.3), which together with key revocation techniques will increase the space needed to store decryption keys—see Section 10.5.6. Furthermore,

by looking at different schemes a means to categorise the different PBE schemes emerged from such schemes' emergent properties.

Similarly, describing PBE's use as part of a crypto-system was also a necessary evil, it establishednot only how PBE schemes could be deployed (see Section 9.8) but also points of contention within such deployment. Of which the most notable issues were those surrounding key manage ment such as constructing, issuing and revocation. Furthermore, the use of PBE identified three different modes of operation that describe the three different ways in which PBE schemes can be leveraged within an crpyto-system—see Section 9.8. When combined with the cloud setting, two different sets of scenarios emerged based upon whether the service user's or CSP's data was to be protected.

PBE schemes can be used to protect service user's data in three different scenarios: Scenario I saw the inclusion of PBE within a service; Scenario II saw the provision of PBE as-a-Service ; and Scenario V saw PBE being deployed by the user themselves. In each of these three scenarios PBE can be used by service users to specify precisely with whom they wish to share their data, for what purpose, and for how long. Although Scenario V may be a privacy zealot's ideal choice—they are in full control—its practical feasibility has yet to be determined; the ability for service users' to act competently as a Key Authority is still unclear. The remaining two scenarios, on the other hand, do appear to be more promising. However, these scenarios in themselves do present a dilemma between usability and the guarantees made over end-to-end security—see Section 12.3.

When looking to protect CSP's data, PBE can facilitate keyword search with complex queries over encrypted data: Scenario III by the CSP; and in Scenario IV by a service user. This use of PBE is rather interesting in that the focus of these scenarios is on the CSP and not service user, and is most certainly worthy of further investigation.

The use of PBE within the cloud appears to be concentrated at both the PaaS and SaaS service layers. Though some may be surprised at PBE's lack of use at the IaaS layer, this was not totally unexpected. The primary interaction between a service user and CSP at this level is over managing virtual machines: Not much else happens.

As previously mentioned, comprehending the field of PBE was made more difficult due to the inherently heterogeneous nature of the schemes studied. As such this thesis also sought to provide readers with a decent starting point over PBE schemes and also their use within crypto-systems. However, towards the end of this investigation a plethora of papers have been released addressing PBE in terms of its description and use within a cryptographic system. From Boneh, Sahai and Waters [BSW10], PBE can now be seen under the guise of Functional Based Encryption (FBE), here Boneh, Sahai and Waters provides a coherent, and authoritative, definition towards PBE together with a categorisation of the different FBE schemes. Interestingly the categorisation presented is similar to that presented within this thesis—see Section 7.3. Furthermore, Akinyele, Lehmann et al. [AL+10] utilises PBE to secure medical records, and Bobba, Fatemieh et al. [BF+10] utilises PBE to for secure messaging. Both these solutions show real-life uses of PBE schemes and as part of a cryptographic system. In fact the solutions presented in Bobba, Fatemieh et al. [BF+10] and Akinyele, Lehmann et al. [AL+10] would both correspond to Scenario I.

FURTHER RESEARCH

Several avenues for further research are discussed. Addressing Predicate Based Signing, Distributed Attribute Based Encryption, Use Case development and practical feasibility.

ATTRIBUTE BASED SIGNING

PBE schemes provide assurances towards the confidentiality of data. They do not provide as surances towards the authenticity of the data. To provide such assurances digital signature schemes are required. Attribute Based Signing (ABS) is an adaptation of Attribute Based Encryption (ABE) for the purposes of providing guarantees towards the provenance of the signed data, and moreover towards the anonymity of the signer [MPR10]. Within ABS schemes the digital signature indicates that the signer can satisfy the given predicate and hence has attested to the message—provenance. Furthermore, the precise set of attributes used by the signer is not revealed—signer anonymity. Such a signature scheme has several practical uses. Maji, Prabhakaran and Rsulek [MPR10] discusses the use of ABS schemes for attribute-based authentication, trust negotiation, and the leaking of secrets. Future research would seek to investigate:

- The feasibility of such schemes.
- How such schemes can be leveraged in general: What do they allow for? and What do they bring? and finally
- How these schemes can be used within the Cloud.

DECENTRALIZING THE KEY AUTHORITY

The Key Authority is responsible for the management of attributes, attribute definition, and also over attribute assignment to entities. However, these attributes naturally originate from different sources and as such they will also be managed by different authorities. For example, within a university setting students, and information concerning students, are handled by various administrative departments[1]. Matriculation is typically performed by a central administrative body, while more degree programme specific aspects (e.g. advising) are handled at a faculty level, and also further on a per school/department basis. There may not be one central body that collates and is able to verify the attributes/access policies that are to be assigned to the student. The ability for a single Attribute Authority and Decryption Authority to administer over a 'global' attribute universe is made more difficult. Distributed Attribute Based Encryption (DABE), also known as Multi-Authority ABE, is an adaptation of Ciphertext-Policy-ABE that delegates the management of attributes and the creation of decryption keys to other individual attribute authorities [LC+10; MKE09; Cha07]. Future work will be to investigate:

- The feasibility of such schemes.

  How these schemes can be incorporated within the existing description for the use of PBE within a crypto-system

- Following from the previous point, how this new description of the crypto-system affects the scenarios governing its use within the Cloud.

CRYPTOGRAPHIC KEYS

Chapter 8 discussed the different techniques that can be used to construct a Linear Secret Sharing Scheme (LSSS) from boolean formula. These techniques fell into two categories: access tree oriented, or based upon MSPs. It is also known that these different techniques will have some affect upon the composition, namely that of efficiency, of the constructed LSSS. Future investigations should include the comparison of these different techniques looking at how the constructed LSSSs affect: storage requirements, encryption and decryption efficiency. A similar avenue for further investigation is concerned with key revocation. With Key-Policy schemes it is the Key Authority (KA) that is responsible for the specification and construction of policy rules. These policies can be combined to construct other policy rules, creating a hierarchy of policy rules. Can this be used to facilitate key revocation within Key-Policy schemes?

USE CASE DEVELOPMENT

The description of how PBE can be used within a crypto-system (given in Chapter 9) does not address fully how other security issues/guarantees such as authenticity and non-repudiation can be assured. This is necessary when discussing the distribution of cryptographic keys and the sending of messages. Area of future work can be the provision of a 'complete description' of a crypto-system that makes used of PBE. Following on from this, another area of investigation will be to look at how such a complete description affects the different scenarios given in Chapter 11. Moreover, these scenarios have been described rather generically and have used 'guiding examples' to aid in their description. An area of future work would be to develop these scenarios further providing more concrete examples of their use.

PRACTICAL CONSIDERATIONS

This thesis has primarily been concerned with the theoretical considerations and implications over PBE and the Cloud. Following on from the future work suggested Section 14.5, an obvious next step is to investigate various practical aspects of the use of PBE such as its implementation, deployment and Quality of Service (QoS). Areas of interest that should be addressed include: • The effect that access policy composition, especially concerning numerical comparisons, has upon the performance of the encryption, decryption and key generation functions.

• The QoS measurements and guarantees that can be made, aside from function efficiency, over PBE.

• The effect that access policy composition has upon, if any, the size of cipher-text produced.

• The representation (encoding) of access policies/rules and list of attributes.

• Existing standards and technologies that should be leveraged or adhered to.

• The construction of a means through which policy rule administration, for both users and CSPs, can be achieved.

BIBLIOGRAPHY

ACCESS CONTROL

Ravi S. Sandhu, Edward J. Coyne et al. 'Role-Based Access Control Models'. In: Computer 29.2 (1996), pp. 38–47. issn: 0018-9162. doi: http://doi.ieeecomputersociety.org/10.1109/2.485845.

R S Sandhu and P Samarati. 'Access Control: Principle and Practice'. In: IEEE COmmunications Magazine 32.9 (Sept. 1994), pp. 40–48.

Eric Yuan and Jin Tong. 'Attributed Based Access Control (ABAC) for Web Services'. In: Proceedings of the IEEE International Conference on Web Services. ICWS '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 561–569.isbn:0-7695-2409-5.doi:http://dx.doi.org/10.1109/ICWS.2005.25. url:http://dx.doi.org/10.1109/ICWS.2005.25.

CLOUD COMPUTING

Michael Armbrust, Armando Fox et al. Above the Clouds: A Berkeley View of Cloud Computing. Tech. rep. UCB/EECS-2009-28. Electrical Engineering and Computer Sciences, University of California at Berkeley, Feb. 2009. url: http : / / www . eecs . berkeley . edu / Pubs / TechRpts / 2009 / EECS -2009-28.html.

G. Alp´ar, J.-H. Hoepman and J. Siljee. 'The Identity Crisis. Security, Privacy and Usability Issues in Identity Management'. In: ArXiv e-prints (Jan.2011). arXiv:1101.0427 [cs.CR].

Ken Birman, Gregory Chockler and Robbert van Renesse. 'Toward a cloud computing research agenda'. In: SIGACT News 40.2 (2009), pp. 68–80.issn: 0163-5700. doi: http://doi.acm.org/10.1145/1556154.1556172.

Philippa J. Broadfoot and Andrew P. Martin. A Critical Survey of Grid Security Requirements and Technologies. Tech. rep. PRG-RR-03-15. Wolf-son Building Oarks Road Oxford OX1 3QD: Oxford University Computing Laboratory, 2003. url: http://www.comlab.ox.ac.uk/files/930/RR-03-15.ps.gz.

Monica Chew, Dirk Balfanz and Ben Laurie. '(Under)mining Privacy in Social Networks'. In: Proceedings of the 2008 IEEE Symposium on Security and Privacy Workshop: Web 2.0 Security and Privacy - W2SP 2008. Publish Online. 2008. url: http://w2spconf.com/2008/papers/s3p2.pdf.

Flavin Cristian. 'Understanding fault-tolerant distributed systems'. In: Common. ACM 34.2 (1991), pp. 56–78. issn: 0001-0782. doi: http:// doi.acm.org/10.1145/102792.102801.

Gabriele D'Angelo, Fabio Vitali and Stefano Zacchirolo. 'Content Cloacking: Preserving Privacy with Google Docs and other Web Applications'. To appear in the 25th Symposium On Applied Computing (SAC'10), March 22-26, 2010, Sierre Switzerland. Mar. 2010.

Cloud Computing: Benefits, risks and recommendations for information security. Tech. rep. European Network and Information Security Agency (ENISA), 2009 url: http : / / www . enisa . europa . eu / act / rm / files / deliverables/cloud-computing-risk-assessment.

Ian Foster. 'The Anatomy of the Grid: Enabling Scalable Virtual Organizations'. In: Euro-Par 2001 Parallel Processing (2001), pp. 1–4. url: http://dx.doi.org/10.1007/3-540-44681-8_1.

[GTF08]

Saikat Guha, Kevin Tang and Paul Francis. 'NOYB: privacy in online social networks'. In: WOSP '08: Proceedings of the first workshop on Online social networks. Seattle, WA, USA: ACM, 2008, pp. 49–54. isbn: 978-1-60558-182- 8. doi: http://doi.acm.org/10.1145/1397735.1397747.

[Hay08]

Brian Hayes. 'Cloud computing'. In: Commun. ACM 51.7 (2008), pp. 9–11. issn: 0001-0782. doi: http://doi.acm.org/10.1145/1364782.1364786. url: http://portal.acm.org/citation.cfm?doid=1364782.1364786.

[HM+05]

Ragib Hasan, Suvda Myagmar et al. 'Toward a threat model for storage systems'. In: StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and survivability. Fairfax, VA, USA: ACM, 2005, pp. 94–102. isbn: 1-59593-233-X. doi: http://doi.acm.org/10.1145/1103780. 1103795.

[HS+10]

Dan Hubbard, Michael Sutton et al. Top Threats to Cloud Computing v1.0 Tech. rep. v1.0 Cloud Security Alliance, Mar. 2010. url: http://www. cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[JGL08]

Meiko Jensen, Nils Gruschka and Norbert Luttenberger. 'The Impact of Flooding Attacks on Network-based Services'. In: ARES '08: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. Washington, DC, USA: IEEE Computer Society, 2008, pp. 509–513. isbn: 978-0-7695-3102-1. doi: http://dx.doi.org/10.1109/ARES. 2008.16.

[JM09]

Carter Jernigan and Behram F.T. Mistree. 'Gaydar: Facebook friendships expose sexual orientation'. In: First

Monday14.10 (Oct. 2009). [Online]. url: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302.

[JS09]

Meiko Jensen and Jorg Schwenk. 'The Accountability Problem of Flooding Attacks in Service-Oriented Architectures'. In: Availability, Reliability and Security, International Conference on 0 (2009), pp. 25–32. doi: http://doi.ieeecomputersociety.org/10.1109/ARES.2009.11.

[JS+09]

Meiko Jensen, Jorg Schwenk et al. 'On Technical Security Issues in Cloud Computing'. In: Cloud Computing, IEEE International Conference on 0 (2009), pp. 109–116. doi:http://doi.ieeecomputersociety.org/10.1109/CLOUD.2009.60.

[KD+09]

Graham Kirby, Alan Dearle et al. An Approach to Ad hoc Cloud Computing. Tech. rep. St Andrews Cloud Computing Initiative, School of Computer Science, University of St Andrews, Feb. 2009. url: http://arxiv.org/abs/1002.4738.

[MA05]

Michael McIntosh and Paula Austel. 'XML signature element wrapping at-tacks and countermeasures'. In: SWS '05: Proceedings of the 2005 workshop on Secure web services. Fairfax, VA, USA: ACM, 2005, pp. 20–27. isbn: 1-59593-234-8. doi: http://doi.acm.org/10.1145/1103022.1103026.

[MKL09]

Tim Mather, Subra Kumaraswamy and Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risk and Compliance. Editor Mike Loukides. O'Reilly, 2009.

[MP09]

Miranda Mowbray and Siani Pearson. 'A client-based privacy manager for cloud computing'. In: COMSWARE '09: Proceedings of the Fourth Inter-national ICST Conference on COMmunication System softWAre and mid-dlewaRE. Dublin, Ireland: ACM, 2009, pp. 1–8. isbn: 978-1-60558-353-2. doi: http://doi.acm.org/10.1145/1621890.1621897.

[NR05]

Syed Naqvi and Michel Riguidel. 'Threat Model for Grid Security Services'. In: Advances in Grid Computing - EGC 2005. Ed. by Peter M. A. Sloot, Alfons G. Hoekstra et al. Vol. 3470. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2005, pp. 1048–1055. doi: 10.1007/11508380_107.url:http://dx.doi.org/10.1007/11508380 107.

[NS09]

Arvind Narayanan and Vitaly Shmatikov. 'De-anonymizing Social Net-works'. In: Security and Privacy, IEEE Symposium on 0 (2009), pp. 173–187. issn: 1081-6011. doi:http://doi.ieeecomputersociety.org/10.1109/SP.2009.22.

[NW+09]

Daniel Nurmi, Rich Wolski et al. 'The Eucalyptus Open-Source Cloud-Computing System'. In: CCGRID '09: Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid. Washington, DC, USA: IEEE Computer Society, 2009, pp. 124–131. isbn: 978-0-7695-3622-4. doi: http://dx.doi.org/10.1109/CCGRID.2009.93.

[Pea09]

Siani Pearson. 'Taking account of privacy when designing cloud computing services'. In: CLOUD '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. Washington, DC, USA: IEEE Computer Society, 2009, pp. 44–52. isbn: 978-1-4244-3713-9. doi: http://dx.doi.org/10.1109/CLOUD.2009.5071532.

[RT+09]

Thomas Ristenpart, Eran Tromer et al. 'Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds'. In: 16th ACM Conference on Computer and Communications Security CCS'09. Nov. 2009.

[Vou08]

Mladen A. Vouk. 'Cloud Computing — Issues, Research and Implement-ations'. In: Journal of Computing and Information Technology 16 (2008), pp. 235–246. doi: 10.2498/cit.1001391. url: http://cit.srce.unizg.hr/index.php/CIT/article/view/1674/1378.

[VRM+09]

Luis M. Vaquero, Luis Rodero-Merino et al. 'A break in the clouds: towards a cloud definition'. In: SIGCOMM Comput. Commun. Rev. 39.1 (2009), pp. 50–55. issn: 0146-4833. doi: http://doi.acm.org/10.1145/1496091.1496100.

[WH+10]

Gilbert Wondracek, Thorsten Holz et al. 'A Practical Attack to De-anonymize Social Network Users'. In: Security and Privacy, IEEE Symposium on 0 (2010), pp. 223–238. issn: 1081-6011. doi: http://doi .ieeecomputersociety.org/10.1109/SP.2010.21.

LEGAL PERSPECTIVES

[Con08]

Chris Connolly. 'The US Safe Harbor - Fact or Fiction?' In: Privacy Laws&Business International 96 (Dec. 2008). url: http://www.galexia. com/public/research/articles/research_articles-pa07.html.

[Cou09]

David A. Couillard. 'Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing'. In: Min-nesota Law Review 93 (June 2009), pp. 2205–2238.

[JLG08]

Paul T. Jaeger, Jimmy Lin and Justin M. Grimes. 'Cloud Computing and Information Policy: Computing in a Policy Cloud?' In: Journal of Information Technology & Politics 5.3 (2008), pp. 269–283. url: http://www. informaworld.com/10.1080/19331680802425479.

[Nis04]

Helen Nissenbaum. 'Privacy as Contextual Integrity'. In: Washington Law Review 79.1 (2004). url: http://ssrn.com/abstract=534622.

[SEC-2002-196]

The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. English. Commission Staff Working Document SEC (2002) 196. Commission of the European Communities. url: http: / / ec . europa . eu / justice home / fsj / privacy / docs / adequacy / sec -2002-196/sec-2002-196_en.pdf.

[SEC-2004-1323]

The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce English. Commission Staff Working Document SEC (2004) 1323. Commission of the European Communities. url: http//ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf.

[Sol07]

Daniel J. Solove. ''I've got nothing to hide' and Other Misunderstandings of Privacy'. In: San Diego Law Review 44 (2007). GWU Law School Public Law Research Paper No. 289, pp. 745–772. url: http://ssrn.com/abstract=998565.

MISC TOPICS ON CRYPTOGRAPHY

[AL02]

Carlisle Adams and Steve Lloyd. Understanding PKI: Concepts, Standards, and Deployment Considerations. 2nd. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2002. isbn: 0672323915.

[Bei96]

Amos Beimel. 'Secure Schemes for Secret Sharing and Key Distribution'. PhD thesis. Israel Institute of Technology, 1996.

[BL88]

Josh Benaloh and Jerry Leichter. 'Generalized Secret Sharing and Monotone Functions'. In: Advances in Cryptology —CRYPTO'88 (1988), pp. 27–35. url: http://dx.doi.org/10.1007/0-387-34799-2_3.

[BR08]

Mihir Bellare and Phillip Rogaway. 'Code-Based Game-Playing Proofs and the Security of Triple Encryption'. Cryptology ePrint Archive, Report 2004/331. Version: 20081129:034148. 2008. url: http://eprint.iacr.org/2004/331.

[BW07]

Dan Boneh and Brent Waters. 'Conjunctive, Subset, and Range Queries on Encrypted Data'. In: Theory of Cryptography. Ed. by Salil Vadhan. Vol. 4392. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2007, pp. 535–554. doi: 10.1007/978- 3- 540- 70936- 7 29. url: http://dx.doi.org/10.1007/978-3-540-70936-7_29.

[Den06]

Alexander W Dent. 'Fundamental problems in provable security and cryptography'. In: Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 364.1849 (2006), pp. 3215–3230. doi:10. 1098 / rsta . 2006 . 1895. eprint:http://rsta.royalsocietypublishing . org / content / 364 /1849/3215.full.pdf+html.url:http://rsta.royalsocietypublishing.org/content/364/ 1849/3215.abstract.

[ElG85]

T. ElGamal. 'A public key cryptosystem and a signature scheme based on discrete logarithms'. In: IEEE Transactions on Information Theory. 31 (1985). Could not find PDF, pp. 469–472.

[GMW86]

Oded Goldreich, Silvio Micali and Avi Wigderson. 'Proofs that yield nothing but their validity and a methodology of cryptographic protocol design'. In: Foundations of Computer Science, Annual IEEE Symposium on 0 (1986), pp. 174–187. issn: 0272-5428. doi: http ://doi .ieeecomputersociety.org/10.1109/SFCS.1986.47.

[Kan08]

Murat Kantarcioglu. 'A Survey of Privacy-Preserving Methods Across Horizontally Partitioned Data'. In: Privacy-Preserving Data Mining. Ed. By Ahmed K. Elmagarmid, Amit P. Sheth et al. Vol. 34. Advances in Database Systems. Springer US, 2008, pp. 313–335. isbn: 978-0-387-70992-5. url: http://dx.doi.org/10.1007/978-0-387-70992-5_13.

[KW93]

M Karchmer and A Widgerson. 'On Span Programs'. In: Proceedings of the Eighth Annual Structure in Complexity Theory Conference, 1993. IEEE Computer Society, June 1993, pp. 102–111. doi: 10.1109/SCT.1993.3365 36.

[LC10]

Zhen Liu and Zhenfu Cao. 'On Efficiently Transferring the Linear Secret Sharing Scheme Matrix in Ciphertext-Policy Attribute-Based Encryption'. Cryptology ePrint Archive, Report 2010/374. 2010. url: http://eprint.iacr.org/2010/374.

[RSA78]

R. L. Rivest, A. Shamir and L. Adleman. 'A method for obtaining digital signatures and public-key cryptosystems'. In: Commun. ACM 21.2 (1978), pp. 120–126. issn: 0001-0782. doi: http://doi.acm.org/10.1145/359340.359342.

[Sha79]

Adi Shamir. 'How to share a secret'. In: Commun. ACM22.11 (1979), pp. 612–613. issn: 0001-0782. doi: http://doi.acm.org/10.1145/35916 8.359176.

[Sti04]

Douglas Stinson. 'A Polemic on Notions of Cryptographic Security'. July 2004. url:http://www.cacr.math.uwaterloo.ca/~dstinson/papers/polemic.pdf.

GUIDES TO PAIRING BASED CRYPTOGRAPHY

[Bon07]

Dan Boneh. 'A Brief Look at Pairings Based Cryptography'. In: Foundations of Computer Science, Annual IEEE Symposium on 0 (2007), pp. 19–26. issn: 0272-5428. doi: http://doi.ieeecomputersociety.org/10.1109/FOCS.2007.51.

[DBS04]

Ratna Dutta, Rana Barua and Palash Sarkar. 'Pairing-Based Cryptographic Protocols : A Survey'. Cryptology ePrint Archive. Version 20040624:121914. 2004. url: http://eprint.iacr.org/2004/064.

[Men09]

Alfred Menezes. 'Recent Trends in Cryptography'. In: ed. by Ignacio Luengo. Vol. 477. American Mathematical Society and Real Sociedad Matem´atica Espa˜nola, 2009. Chap. An Introduction to Pairing-Based Cryptography, pp. 47–65.

PREDICATE BASED CRYPTOGRAPHY

[AL+10]

Joseph A. Akinyele, Christoph U. Lehmann et al. 'Self-Protecting Electronic Medical Records Using Attribute-Based Encryption'. Cryptology ePrint Archive, Report 2010/565. Version 20101118:220821. 2010. url: http://eprint.iacr.org/2010/565.

[BBG05]

Dan Boneh, Xavier Boyrn and Eu-Jin Goh. 'Hierarchical identity based encryption with constant size ciphertext'. In: Lecture Notes in Computer Science 3494 (2005). Anglais, p. 17.

[BDC+04]

Dan Boneh, Giovanni Di Crescenzo et al. 'Public Key Encryption with Keyword Search'. In: Advances in Cryptology - EUROCRYPT 2004 3027/2004 (2004), pp. 506–522. url: http://www.springerlink.com/content/0hafhrbbvt2l7vn3.

[BF01]

Dan Boneh and Matt Franklin. 'Identity-Based Encryption from the Weil Pairing'. In: Advances in Cryptology — CRYPTO 2001 2139/2001 (2001), pp. 213–229. doi: 10.1007/3-540-44647-8_13.

[BF+10]

Rakesh Bobba, Omid Fatemieh et al. 'Attribute-Based Messaging: Access Control and Confidentiality'. In: ACM Trans. Inf. Syst. Secur. 13 (4 Dec. 2010), 31:1–31:35. issn: 1094-9224.
doi:http://doi.acm.org/10.1145/1880022.1880025.
url:http://doi.acm.org/10.1145/1880022.1880025.

[BKP10]

Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran. 'Attribute Sets: A Practically Motivated Enhancement to Attribute-Based Encryption'. In: Computer Security — ESORICS 2009 (2010), pp. 587–604. url:http://dx.doi.org/10.1007/978-3-642-04444-1_36.