Gen data

Data-Driven
Genomic
Computing

Cryptographic Techniques - D61

Draft contributed by

Arcangelo Castiglione, Paolo D'Arco, Alfredo De Santis,
Roberto De Prisco, Barbara Masucci, Ivan Visconti.

Dipartimento di Informatica
Via Giovanni Paolo II, 132
I-84084, Fisciano (SA)
University of Salerno, Italy

Abstract

This deliverable surveys the cryptographic techniques which have been object of investigation in the first year of the GenData project. The document is structured in sections. Each section is divided in two parts: in the first, it provides a description of the cryptographic primitive or technique, a brief overview of the state-of-the-art, and its relevance or applicability to secure genomic computing; in the second, it outlines the findings that have been obtained and the open research lines.

1 Cryptographic Access Control

1.1 Problem and State-of-Art

The access control management ensures that only authorized users are given access to certain resources. In particular, with respect to their respective powers and responsibilities, users are typically organized into hierarchies composed by several disjoint classes (*security classes*). A hierarchy arises from the fact that some users might have more access rights than others. A user with access privileges for a given class gains access to the objects stored in that class as well as to all the descendant ones in the hierarchy. Hierarchical structures are widely employed in many different application areas, including database management systems, computer networks, operating systems, military and government communications. The problem of key management for such hierarchies consists in assigning a key to each class of the hierarchy in such a way that the keys for descendant classes can be obtained efficiently from users belonging to classes at a higher level in the hierarchy.

The use of cryptographic techniques to address the problem of key management in hierarchical structures has been first considered by Akl and Taylor [1], who proposed a *hierarchical key assignment scheme* where each class is assigned a key that can be used, along with some public information generated by a trusted authority, to compute the key assigned to any class lower down in the hierarchy. Subsequently, many researchers have proposed schemes offering different trade-offs in terms of the amount of public and private information and the complexity of key derivation (e.g., [24, 16, 18, 25, 22, 26, 39, 10, 34, 5, 30, 3, 2, 12, 13, 33, 14]). Many other proposals either support more general access control policies [40, 23, 27, 29] or satisfy additional time-dependent constraints [36, 11, 17, 41, 6, 38, 37, 31, 32, 7]. Despite the large number of proposed schemes, many of them lack a formal security proof and have been shown to be insecure against *collusive attacks* [43, 42, 35, 6, 28], whereby two or more classes collude to compute a key to which they are not entitled.

Atallah et al. [2] first addressed the problem of formalizing security requirements for hierarchical key assignment schemes and proposed two different notions: security against *key recovery* and with respect to *key indistinguishability.* Informally speaking, the former captures the notion that an adversary should not be able to compute a key to which it should not have access, while in the latter, the adversary should not even be able to distinguish between the real key and a random string of the same length.

Different constructions satisfying the above defined notions of security have been proposed in [6, 30, 4, 12, 13, 33, 32, 7, 14]. In particular, De Santis et al. [30, 33] proposed two different constructions satisfying security with respect to key indistinguishability: the first one, which is based on symmetric encryption schemes, is simpler than the one proposed in [2], requires a single computational assumption, and offers more efficient procedures for key derivation and key updates; the second one, which is based on a public-key broadcast encryption scheme, allows to obtain a hierarchical key assignment scheme offering constant private information and public information linear in the number of classes. D'Arco et al. [12, 13] analyzed the Akl-Taylor scheme according to the notions proposed in [2] and showed how to choose the public parameters in order to get instances of the scheme which are secure against key recovery under the RSA assumption. Moreover, they showed how to turn the Akl-Taylor scheme in a construction offering security with respect to key indistinguishability; however such a scheme, is less efficient than the constructions proposed in [2, 30, 33]. Finally, Ateniese et al. [6, 7] extended the model proposed in [2] to schemes satisfying additional time-dependent constraints and proposed two different constructions offering security with respect to key indistinguishability. Other constructions for time-dependent schemes, offering different trade-offs in terms of amount of public and private information and complexity of key derivation, were shown in [31, 32].

Recently, Freire et al. [15] proposed new security notions for hierarchical key assignment schemes. Such notions, called security against *strong key recovery* and security with respect to *strong key indistinguishability*, provide the adversary with additional compromise capability, thus representing a strengthening of the model provided in [2]. Finally, in [15] the authors showed that the notions of security against key recovery and against strong key recovery *are separated*, i.e., there exist schemes that are secure against key recovery but which are not secure against strong key recovery. On the other hand, they did not clarify the relations between the notions of security with respect to key indistinguishability and with respect to strong key indistinguishability.

In addition, it is important to emphasize that given the ever increasing diffusion of data outsourcing, which allows to exploit external services for the distribution of resources, a significant research effort has been also devoted to the management of access control in such context [19, 20, 21].

Genomic data are highly sensitive and for this reason they could be abused. Therefore, the access to such data should be protected and ensured by implementing proper control policies, which are in agreement with the national laws concerning the access to personal data, as well as with the constraints imposed by insurance companies. It is easy to point out that Cryptographic Access Control is the natural solution for implementing the aforementioned policies.

1.2 Findings

Genomic data management defines a sort of "*multi-domain environment*", in which there are different cooperating entities, each of them with different interests, responsibilities and tasks to perform. It is important to emphasize that a particular entity, depending on the context and the role which it assumes, may have different roles towards another given entity to which it intends to access. Informally speaking, an entity can take on several tasks, and according to the role assumed it may have different access rights. On the other hand, a certain security class can provide the same entity with different access rights, according to the tasks performed by the latter in such particular context at that particular time. Clearly, at a given time an entity may need to take simultaneously all of its different tasks.

Therefore, besides the conventional hierarchical access, it can be useful, or sometimes necessary, to allow the access to the key of a specific security class to some particular sets of users, which have specific access credentials. In addition, it is essential to assess the relations between the several security notions proposed in the state of the art.

We first proposed a novel access control model which provides the user with the minimum permissions possible, in order to access a specific resource or to carry out a given task. This model enables to prevent the abuse of permission, defines alternative methods to gain such permission and allows separation of duties. The model also enables collaboration among set of users for gaining specific permissions, defining the way in which such collaboration takes place [45, 44]. In addition, we formally defined a hierarchical key assignment scheme which implements such a novel access control model, and in particular we provided a construction for that scheme, denoted as the *Shared Encryption Based Construction* (*SEBC*). The proposed construction uses as building blocks a *symmetric encryption scheme* and a *perfect secret sharing scheme*. Moreover, we showed how the security property of the proposed construction relies on the ones of the underlying encryption scheme and secret sharing scheme. In particular, we showed that the proposed construction is provably secure with respect to *key indistinguishability* [45, 44].

Furthermore, we explored the relations between all security notions for hierarchical key assignment schemes, by clarifying implications and separations occurring between such notions. In particular, we showed that security with respect to strong key indistinguishability is *not stronger* than the one with respect to key indistinguishability, thus establishing the equivalence between such two security notions [46]. In addition, we showed a similar result in the *unconditionally secure setting* [9]. Finally, we also showed how to construct a hierarchical key assignment scheme which is secure against strong key recovery, starting from any scheme which guarantees security against key recovery [46].

References

[1] Selim G. Akl and Peter D. Taylor. Cryptographic Solution to a Problem of Access Control in a Hierarchy. *ACM Trans. Comput. Syst.*, 1(3):239–248, 1983.

[2] Mikhail J. Atallah, Marina Blanton, Nelly Fazio, and Keith B. Frikken. Dynamic and Efficient Key Management for Access Hierarchies. *ACM Trans. Inf. Syst. Secur.*, 12(3), 2009.

[3] Mikhail J. Atallah, Marina Blanton, and Keith B. Frikken. Key Management for Non-Tree Access Hierarchies. In David F. Ferraiolo and Indrakshi Ray, editors, *SACMAT 2006,11th ACM Symposium on Access Control Models and Technologies, Lake Tahoe, California, USA, June 7-9, 2006, Proceedings*, pages 11–18. ACM, 2006.

[4] Mikhail J. Atallah, Marina Blanton, and Keith B. Frikken. Incorporating Temporal Capabilities in Existing Key Management Schemes. In Joachim Biskup and Javier Lopez, editors, *Computer Security - ESORICS 2007, 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24-26, 2007, Proceedings*, volume 4734 of *Lecture Notes in Computer Science*, pages 515–530. Springer, 2007.

[5] Mikhail J. Atallah, Keith B. Frikken, and Marina Blanton. Dynamic and Efficient Key Management for Access Hierarchies. In Vijay Atluri, Catherine Meadows, and Ari Juels, editors, *Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS 2005, Alexandria, VA, USA, November 7-11, 2005*, pages 190–202. ACM, 2005.

[6] Giuseppe Ateniese, Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Provably-Secure Time-Bound Hierarchical Key Assignment Schemes. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006*, pages 288–297. ACM, 2006.

[7] Giuseppe Ateniese, Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Provably-Secure Time-Bound Hierarchical Key Assignment Schemes. *J. Cryptology*, 25(2):243–270, 2012.

[8] Elisa Bertino, Ning Shang, and Samuel S. Wagstaff Jr. An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting. *IEEE Trans. Dependable Sec. Comput.*, 5(2):65–70, 2008.

[9] M. Cafaro, R. Civino, and B. Masucci. On the Equivalence of Two Security Notions for Hierarchical Key Assignment Schemes in the Unconditional Setting. *IEEE Trans. Dependable Sec. Comput.*, 2014.

[10] Tzer-Shyong Chen and Yu-Fang Chung. Hierarchical Access Control Based on Chinese Remainder Theorem and Symmetric Algorithm. *Computers & Security*, 21(6):565–570, 2002.

[11] Hung-Yu Chien. Efficient Time-Bound Hierarchical Key Assignment Scheme. *IEEE Trans. Knowl. Data Eng.*, 16(10):1301–1304, 2004.

[12] Paolo D'Arco, Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Security and Tradeoffs of the Akl-Taylor Scheme and Its Variants. In Rastislav Královic and Damian Niwinski, editors, *Mathematical Foundations of Computer Science 2009, 34th International Symposium, MFCS 2009, Novy Smokovec, High Tatras, Slovakia, August 24-28, 2009. Proceedings*, volume 5734 of *Lecture Notes in Computer Science*, pages 247–257. Springer, 2009.

[13] Paolo D'Arco, Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Variations on a theme by Akl and Taylor: Security and Tradeoffs. *Theor. Comput. Sci.*, 411(1):213–227, 2010.

[14] Eduarda S. V. Freire and Kenneth G. Paterson. Provably Secure Key Assignment Schemes from Factoring. In Udaya Parampalli and Philip Hawkes, editors, *Information Security and Privacy - 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings*, volume 6812 of *Lecture Notes in Computer Science*, pages 292–309. Springer, 2011.

[15] Eduarda S. V. Freire, Kenneth G. Paterson, and Bertram Poettering. Simple, Efficient and Strongly KI-Secure Hierarchical Key Assignment Schemes. In Ed Dawson, editor, *Topics in Cryptology - CT-RSA 2013 - The Cryptographers' Track at the RSA Conference 2013, San Francisco,CA, USA, February 25-March 1, 2013. Proceedings*, volume 7779 of *Lecture Notes in Computer Science*, pages 101–114. Springer, 2013.

[16] Lein Harn and Hung-Yu Lin. A Cryptographic Key Generation Scheme for Multilevel Data Security. *Computers & Security*, 9(6):539–546, 1990.

[17] Hui-Feng Huang and Chin-Chen Chang. A New Cryptographic Key Assignment Scheme with Time-Constraint Access Control in a Hierarchy. *Computer Standards & Interfaces*, 26(3):159–166, 2004.

[18] H.T. Liaw, S.J. Wang, and C.L. Lei. A Dynamic Cryptographic Key Assignment Scheme in a Tree Structure. *Computers & Mathematics with Applications*, 25(6):109 – 114, 1993.

[19] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, G. Livraga, S. Paraboschi, and P. Samarati, "Enforcing dynamic write privileges in data outsourcing," *Computers & security*, vol. 39, pp. 47–63, 2013.

[20] S. D. C. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Encryption policies for regulating access to outsourced data," *ACM Transactions on Database Systems (TODS)*, vol. 35, no. 2, p. 12, 2010.

[21] S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, “Over-encryption: management of access control evolution on outsourced data,” in *Proceedings of the 33rd international conference on Very large data bases*. VLDB endowment, 2007, pp. 123–134.

[22] Chu-Hsing Lin. Dynamic Key Management Schemes for Access Control in a Hierarchy. *Computer Communications*, 20(15):1381 – 1385, 1997.

[23] Iuon-Chang Lin, Min-Shiang Hwang, and Chin-Chen Chang. A New Key Assignment Scheme for Enforcing Complicated Access Control Policies in Hierarchy. *Future Generation Computer Systems*, 19(4):457 – 462, 2003. Selected papers from the IEEE/ACM International Symposium on Cluster Computing and the Grid, Berlin-Brandenburg Academy of Sciences and Humanities, Berlin, Germany, 21-24 May 2002.

[24] Stephen J. MacKinnon, Peter D. Taylor, Henk Meijer, and Selim G. Akl. An Optimal Algorithm for Assigning Cryptographic Keys to Control Access in a Hierarchy. *IEEE Trans. Computers*, 34(9):797–802, 1985.

[25] Hwang Min-Shiang. A Cryptographic Key Assignment Scheme in a Hierarchy for Access Control. *Math. Comput. Model.*, 26(2):27–31, July 1997.

[26] Ravi S. Sandhu. Cryptographic Implementation of a Tree Hierarchy for Access Control. *Inf. Process. Lett.*, 27(2):95–98, 1988.

[27] Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Cryptographic Key Assignment Schemes for Any Access Control Policy. *Inf. Process. Lett.*, 92(4):199–205, 2004.

[28] Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Enforcing the Security of a Time-Bound Hierarchical Key Assignment Scheme. *Inf. Sci.*, 176(12):1684–1694, 2006.

[29] Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Unconditionally Secure Key Assignment Schemes. *Discrete Applied Mathematics*, 154(2):234–252, 2006.

[30] Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Efficient Provably-Secure Hierarchical Key Assignment Schemes. In Ludek Kucera and Antonín Kucera, editors, *Mathematical Foundations of Computer Science 2007, 32nd International Symposium, MFCS 2007, Ceský Krumlov, Czech Republic, August 26-31, 2007, Proceedings*, volume 4708 of *Lecture Notes in Computer Science*, pages 371–382. Springer, 2007.

[31] Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes. In Volkmar Lotz and Bhavani M. Thuraisingham, editors, *SACMAT 2007, 12th ACM Symposium on Access Control Models and Technologies, Sophia Antipolis, France, June 20-22, 2007, Proceedings*, pages 133–138. ACM, 2007.

[32] Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes. *Theor. Comput. Sci.*, 407(1-3):213–230, 2008.

[33] Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Efficient Provably-Secure Hierarchical Key Assignment Schemes. *Theor. Comput. Sci.*, 412(41):5684–5699, 2011.

[34] Victor R. L. Shen and Tzer-Shyong Chen. A Novel Key Management Scheme Based on Discrete Logarithms and Polynomial Interpolations. *Computers & Security*, 21(2):164–171, 2002.

[35] Qiang Tang and Chris J. Mitchell. Comments On a Cryptographic Key Assignment Scheme. *Computer Standards & Interfaces*, 27(3):323–326, 2005.

[36] Wen-Guey Tzeng. A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy. *IEEE Trans. Knowl. Data Eng.*, 14(1):182–188, 2002.

[37] Wen-Guey Tzeng. A Secure System for Data Access Based on Anonymous Authentication and Time-Dependent Hierarchical Keys. In Ferng-Ching Lin, Der-Tsai Lee, Bao-Shuh Paul Lin, Shiuhpyng Shieh, and Sushil Jajodia, editors, *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2006, Taipei, Taiwan, March 21-24, 2006*, pages 223–230. ACM, 2006.

[38] Shyh-Yih Wang and Chi-Sung Laih. Merging: An Efficient Solution for a Time-Bound Hierarchical Key Assignment Scheme. *IEEE Trans. Dependable Sec. Comput.*, 3(1):91–100, 2006.

[39] Tzong-Chen Wu and Chin-Chen Chang. Cryptographic Key Assignment Scheme for Hierarchical Access Control. *Comput. Syst. Sci. Eng.*, 16(1):25–28, 2001.

[40] J. Yeh, R. Chow, and R. Newman. A Key Assignment for Enforcing Access Control Policy Exceptions. In *Proc. of the International Symposium on Internet Technology*, pages 54–59, 1998.

[41] Jyh-haw Yeh. An RSA-based Time-Bound Hierarchical Key Assignment Scheme for Electronic Article Subscription. In Otthein Herzog, Hans-Jörg Schek, Norbert Fuhr, Abdur Chowdhury, and Wilfried Teiken, editors, *Proceedings of the 2005 ACM CIKM International Conference on Information and Knowledge Management, Bremen, Germany, October 31 - November 5, 2005*, pages 285–286. ACM, 2005.

[42] Xun Yi. Security of Chien's Efficient Time-Bound Hierarchical Key Assignment Scheme. *IEEE Trans. Knowl. Data Eng.*, 17(9):1298–1299, 2005.

[43] Xun Yi and Yiming Ye. Security of Tzeng's Time-Bound Key Assignment Scheme for Access Control in a Hierarchy. *IEEE Trans. Knowl. Data Eng.*, 15(4):1054–1055, 2003.

[44] A. Castiglione, A. D. Santis, and B. Masucci, Hierarchical and Shared Access Control, In submission.

[45] A. Castiglione, A. De Santis, and B. Masucci, "Hierarchical and Shared Key Assignment," in *17th International Conference on Network-Based Information Systems, NBIS 2014, IEEE*, 2014, pp. 263–270. [Online]. Available: `http://dx.doi.org/10.1109/NBiS.2014.106`

[46] A. Castiglione, A. D. Santis, and B. Masucci, "Key Indistinguishability vs. Strong Key Indistinguishability for Hierarchical Key Assignment Schemes," *IACR Cryptology ePrint Archive*, vol. 2014, p. 752, 2014. [Online]. Available: `http://eprint.iacr.org/2014/752`

2 Anonymous Primitives and Protocols

2.1 Problem and State-of-Art

In all its forms privacy has become a major issue in information technology. Several events of the last couple of years, in which secret and classified information has been disclosed, e.g., *Wikileaks* [23] or the *Snowden affair* [22], have shown that authorities have access to phone calls, e-mails and other communications far beyond constitutional bounds. Many nations, including those expressing the strongest protests in the name of user rights, collect intelligence on each other. Adversarial entities, for plenty of reasons, might trace or build a profile of movements, interests and, more generally, of user behaviors. Attacks of these types are a strong threat to the user freedom. People should be protected against these attacks made possible by the current methods of communication and of information processing.

On the other hand, it is immediate to realize that if in an adversarial world in which users are exposed to any kind of attacks, social aspects of privacy are important and worthy of investigation, user *personal* information protection is a priority. It is imperative to safeguard his sensitive data. As soon as genomic computing becomes a mass technology, tools for a secure implementations of computations and services are strongly needed to cope with any form of attacks which in this scenario might be also targeting classes of users.

It is therefore compelling to put forward methods for guaranteeing user privacy and protocols for anonymous computation and communication.

General notions and efficient methods for building privacy-preserving applications have been proposed in the past. Among them, the notion of *key-privacy* in public-key encryption [2] is an important feature a public-key encryption scheme may exhibit, which is helpful in building applications providing user anonymity, through which an adversary is unable to tell *which* public key has been used to compute a given ciphertext. Moreover, many privacy-preserving low-level cryptographic protocols, like secret sets and anonymous broadcast encryption, have been introduced.

Fifteen years ago, Molva and Tsudik [18] put forward the notion of *secret set* as a method to enhance user privacy. Loosely speaking, a secret set is a *representation* of a subset of users of a given universe such that *any* user of the universe can check whether he is or is not a member of the subset, *no one* can check if another user of the universe is or is not a member, and *no one* can determine the size of the subset. The last two properties should hold also against coalitions of users. The authors proposed some constructions and showed how secret sets can be useful to protect receivers' privacy in multicast communications, and against traffic analysis of mobile devices. Later on, De Santis and Masucci [10] provided a formal treatment of the notion. They defined unconditionally secure secret sets by using the language of information theory, showed lower bounds in terms of needed number of bits on user storage, on representation length of a secret set, and on the randomness needed to set up a scheme, and proved the bounds are tight. Moreover, they defined computationally secure secret sets in terms of *indistinguishability* of representations associated to different sets, and showed that such schemes exists if and only if semantically secure symmetric encryption exists. Micali et al. in [17] put forward the notion of *zero-knowledge set*, which is somehow related. A zero-knowledge set is a method through which a prover can construct a representation of a set of strings S of a given universe $\mathcal{U}$ such that, for any string $x \in \mathcal{U}$, he is able to prove non-interactively and in zero-knowledge whether $x \in S$ or $x \notin S$. In particular, the representation of S does not leak any other information about S, e.g., the size of S. The authors showed that zero-knowledge sets exist if the discrete logarithm problem is hard. Several papers have further focused on Micali et al.'s work, e.g., see [7, 5, 19, 6].

Broadcast Encryption schemes enable a center to deliver encrypted data to a large set of users, in such a way that only a privileged subset of them can decrypt the data. Applications for these schemes range from pay-tv to systems for delivering sensitive information stored on media like a CD/DVD. Broadcast encryption works as follows: during a set-up phase, every user receives a set of predefined keys. Then, at the beginning of each data transmission, the center sends a broadcast message enabling privileged users to compute a session key, by means of which, the encrypted data, that will be delivered later on, can be decrypted. In many content distribution systems it is important to both restrict access to content to authorized users and to protect *their identities*. Unfortunately, a broadcast encryption scheme *does not* guarantee any form of privacy for the set of recipients. Actually, in almost all existing constructions, the broadcast message contains an *explicit description* of the set of recipients, which is used by each recipient to identify the part of the broadcast message he/she is able to decrypt with the predefined keys received during the set-up phase, in order to retrieve the session key. In [4] the authors introduced *private broadcast encryption*. A private broadcast encryption scheme is exactly a mechanism to encrypt a broadcast message such that only authorized users can decrypt the message and read the content and, at the same time, the identities of the recipients are kept secret, even from each other. Such a notion has been further studied in [16], under the name of *anonymous broadcast encryption*.

2.2 Findings

By using the currently available knowledge and tools, developed during the last years, we have taken a further look at the key-privacy notion, at secret sets, focusing our attention on constructions in the public-key setting, and at anonymous broadcast encryption. Indeed, several issues were still open: key privacy was introduced as an additional property a secure encryption scheme might exhibit, but it was not clarified what kind of relation this notion has with security. With respect to secret sets, the authors of [18] proposed some constructions based on encryption schemes and the Chinese Remainder Theorem and suggested two important applications, but the treatment they provided was quite informal. Security reductions within a formal adversarial model were not provided. On the other hand, [10] provided a formal treatment, but in the computational case the authors looked mainly at the symmetric setting. Moreover, in both papers, no efficient construction hides the size of the set S, which is disclosed to the users. Regarding anonymous broadcast encryption, the authors of [4] gave a look at the current practice, by discussing a PGP implementation which supports private broadcast encryption and is secure against a *passive* adversary, proposed two new constructions which are secure against an *active* adversary, and discussed a useful application, i.e., how to realize encrypted file systems preserving user privacy. Later on, [16] revised the notion of private broadcast encryption, which was referred to as *anonymous broadcast encryption*, provided a strong security definition, an in-depth analysis of which tools are needed in order to achieve the definition, and general as well as concrete constructions. However, efficient constructions are still an open problem.

First of all, we showed that for robust encryption schemes key privacy under chosen ciphertext attack implies non-malleability and, hence, security under chosen ciphertext attacks. Such a result is of independent interest and helps to simplify the set of requirements that public key encryption schemes need to satisfy when stating and proving theorems. Then, we formally defined in the public key setting secret sets and anonymous broadcast encryption and showed an equivalence between them with respect to non-adaptive adversaries. More precisely, we first showed how to construct a secret set by using an anonymous broadcast encryption scheme. Later on, we showed how to construct an anonymous broadcast encryption scheme by using multiple times a secret set scheme. Finally, we revisited some of the constructions for secret sets of [18]. For each of them, we showed which security requirements set in the model the construction achieves, and under which computational assumptions. The security reductions, hence, *clarify* what is really needed to get certain security properties [8].

References

[1] M. Abdalla, M. Bellare, and G. Neven, *Robust Encryption*, Proc. of TCC 2010, LNCS, Vol. 5978, pp. 480-497, 2010.

[2] M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval, *Key-Privacy in Public-Key Encryption*, Proc. of Asiacrypt 2001, LNCS, Vol. 2248, pp. 566-582, 2001.

[3] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, *Relations among notions of security for public-key encryption schemes*, Proc. of Crypto 1998, LNCS, Vol. 1462, pp. 26-45, 1998.

[4] A. Barth, D. Boneh and B. Waters, *Privacy in Encrypted Content Distribution Using Private Broadcast Encryption*, Proc. of Financial Cryptography (FC 2006), LNCS, Vol. 4107, pp. 52-64, 2006.

[5] D. Catalano, Y. Dodis and I. Visconti, *Mercurial Commitments: Minimal Assumptions and Efficient Constructions*, Proc. of the third Theory of Cryptography Conference (TCC 06), LNCS Vol. 3876, pp. 120-144, 2006.

[6] D. Catalano, D. Fiore and M. Messina, *Zero-Knowledge Sets with Short Proofs*, Proc. of Eurocrypt 2008, LNCS, Vol. 4965, pp. 433-450, 2008.

[7] M. Chase, A. Healy, A. Lysyanskaya, T. Malkin and L. Rezin, *Mercurial Committments with applications to zero-knowkedge sets*, Proc. of Eurocrypt 2005, LNCS Vol. 3494, pp. 422-439, 2005

[8] P. D'Arco and A. De Santis, *Key Privacy and Anonymous Protocols*, Proc. of the IEEE 11th International Conference on Privacy, Security and Trust (PST2013), July 10-12, 2013. ISBN 978-1-4673-5839-2. Journal version accepted for publication in Theoretical Computer Science.

[9] D. Dolev, C. Dwork, and M. Naor, *Non-malleable cryptography*, SIAM Journal of Computing, Vol. 30, N. 2, pp. 391-437, 2000.

[10] A. De Santis and B. Masucci, *On Secret Set Schemes*, Inform. Process. Lett. 74 (2000) 243-251.

[11] A. Fiat and M. Naor, *Broadcast Encryption*, Advances in Cryptology - CRYPTO '93, LNCS, Vol. 773, pp. 480-491, 1994.

[12] G. Goldwasser and S. Micali, *Probabilistic Encryption*, Journal of Computer and System Sciences 28(2), 278-299 (1984).

[13] O. Goldreich, *Foundations of Cryptography: Volume II, Basic Applications*, Cambridge University Press, 2004.

[14] J. Hastad and M. Naslund, *The Security of all RSA and Discrete Log Bits*, Journal of ACM, Vol. 51, N. 2, 2004.

[15] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC Press, 2008.

[16] B. Libert, K. Paterson, and E. A. Quaglia, *Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model*, Proc. of the 15th International Conference on Practice and Theory in Public Key Cryptography (PKC 2012), LNCS, 2012, Vol. 7293, pp. 206-224, 2012, full version on the eprint archive, 476/2011.

[17] S. Micali, M. Rabin and J. Kilian, *Zero-Knowledge Sets*, Proc. of the 44th IEEE Symposium on Foundations of Computer Science (FOCS 2003).

[18] R. Molva and G. Tsudik, *Secret Sets and Applications*, Inform. Process. Lett. 65 (1998) 47-55.

[19] R. Xue, NH Li, JT Li, *Algebraic construction for zero-knowledge sets*, Journal of Computer Science and Technology 23(2): 166175 Mar. 2008

[20] K. Sako, *An auction protocol which hides bids of losers*, Proc. of the Third International Workshop on Theory and Practice of Public-Key Cryptography (PKC 2000), LNCS Vol. 1751, pp. 422-432, 2000.

[21] O. Solon, *Turkey's PM: social media is 'worst menace to society'*, http://www.wired.co.uk/news/archive/2013-06/03/turkey-social-media

[22] Wikipedia, Edward Snowden, http://en.wikipedia.org/wiki/Edward_Snowden

[23] Wikileaks, http://wikileaks.org/

3 Private Set Intersection

3.1 Problem and State-of-Art

The Private Set Intersection (PSI) problem, in a nutshell, concerns with two parties, each holding a set of inputs drawn from a ground set, that wish to jointly compute the intersection of their sets, without leaking *any* additional information [21]. In particular, cryptographic solutions to the PSI problem allow interaction between a server S and a client C, with respective private input sets $\mathcal{C} = \{c_1, \ldots, c_v\}$ and $\mathcal{S} = \{s_1, \ldots, s_w\}$, both drawn from the ground set $\mathcal{U}$. At the end of the interaction, C learns $\mathcal{S} \cap \mathcal{C}$ and $|\mathcal{S}|$, while S learns nothing beyond $|\mathcal{C}|$. Since its introduction, the PSI problem has received considerable attention from the cryptographic community due to its appealing, due to the usefulness of its solutions in more complex protocols and, especially, because of its nice real-life applications.

Freedman et al. [21] introduced the first PSI protocol based on oblivious polynomial evaluation (OPE). The key intuition is that elements in the client's private set can be represented as roots of a polynomial, i.e., $P(x) = \prod_{i=1}^{v}(x - c_i) = \sum_{i=1}^{v} a_i x^i$. Hence, leveraging any additively homomorphic encryption scheme (e.g., [32]) the encrypted polynomial is obliviously evaluated by S on each element of its data set. In particular, S computes $\{u_j\}_{j=1,\ldots,w} = \{E(r_j P(s_j) + s_j)\}_{j=1,\ldots,w}$ where $E()$ is the encryption function of the additively homomorphic encryption scheme and r_j is chosen at random. Clearly, if $s_j \in \mathcal{S} \cap \mathcal{C}$, then C learns s_j upon decryption of the corresponding ciphertext (i.e., u_j); otherwise C learns a random value. OPE-based PSI protocols have been extended in [28, 19, 16, 17] to support multiple parties and other set operations (e.g., union, element reduction, etc.).

Hazay et al. [25] proposed Oblivious Pseudo-Random Function (OPRF) [20] as an alternative primitive to achieve PSI. In [25], given a secret index k to a pseudo-random function family, S evaluates $\{u_j\}_{j=1,\ldots,w} = \{f_k(s_j)\}_{j=1,\ldots,w}$ and sends it to C. Later, C and S engage in v executions of the OPRF protocol where C is the receiver with private input $\mathcal{C}$ and S is the sender with private input k. As a result, C learns $\{f_k(c_i)\}_{i=1,\ldots,v}$ such that $c_i \in \mathcal{S} \cap \mathcal{C}$ if and only if $f_k(c_i) \in \{u_j\}_{j=1,\ldots,w}$. Improvements by using the same approach were provided in [23, 24].

Given $\mathcal{U}$ as the ground set where elements of $\mathcal{C}$ and $\mathcal{S}$ are drawn (i.e., $\mathcal{C}, \mathcal{S} \subseteq \mathcal{U}$), none of the above techniques prevents a client to run a PSI protocol on private input $\mathcal{C} \equiv \mathcal{U}$ in order to learn the elements in $\mathcal{S}$. To this end, Camenisch et al. extended PSI to *Certified Sets* [10], where a Trusted Third Party (TTP) ensures that private inputs are valid and binds them to each participant. The certification issue was also addressed in [13], where a related problem to PSI was considered. Moreover, the same extension, under a different name, *Authorised PSI*, was considered in [15], where protocols that use modular exponentiation, multiplication and hash evaluation were described.

Efficiency of the protocols on large data sets is an important practical issue, and it has been addressed in several papers in the last years. In [14] were proposed linear-complexity private set intersection protocols for malicious adversaries. Along the line of [30], to gain efficiency, Bloom filters have been applied in [27, 12]. The protocols proposed in [27] are elegant and one of the them is designed for an outsourced scenario. On the other hand, the protocols described in [12] and their optimizations suggested in [33] are currently, with respect to semi-honest adversaries, the most efficient available solutions on the market.

All of the above techniques reveal the size of the participants' sets. That is, C (resp. S) learns $|\mathcal{S}|$ (resp. $|\mathcal{C}|$), even if $\mathcal{S} \cap \mathcal{C} \equiv \emptyset$. To protect the size of private input sets, Ateniese et al. [1] proposed a so-called Size-Hiding PSI (SHI-PSI) protocol where C can privately learn $\mathcal{S} \cap \mathcal{C}$ without leaking the size of $\mathcal{C}$. Their scheme is based on RSA accumulators and the property that the RSA function is an unpredictable function. The authors proved its security against honest but curious adversaries in the Random Oracle Model (ROM).

Later on, general results on hiding the input-size in two party computation were given in [29]. Related works in which the input-size issue has been addressed are [5]

Genomic Computing strongly motivates the need for efficient protocols on large data sets: the user wants to protect the privacy of sensitive information coded in her genomic sequence, i.e., her set of secrets, but at the same time wishes to engage in private computations with other parties, in order to get some advantage, e.g., understand whether she has a predisposition to certain diseases or whether some medicines could be useful to improve her state of health, which could be revelead with a set intersection operation with a reference genomic pattern, i.e., the other set of secrets [2] and [4].

3.2 Findings

Building on top of [1], we have explored PSI protocols where parties hide the size of their private sets, under different security models. We have started looking at *unconditionally secure* SHI-PSI where *both* parties hide the size of their sets. In this context, we showed that SHI-PSI protocols where both the client and the server hide the size of their sets are not achievable, while this is possible for the authorized flavor of PSI, namely APSI.

Then we moved to computational security and showed that there exist an APSI protocol where both parties hide the size of their sets. Finally, we provided some explicit constructions for *one-sided* protocols, where only the client hides the size of her set. More precisely, we designed two protocols which are computationally secure under standard assumptions, and two very efficient protocols which are secure in the random oracle model [11]. The following table summarizes our findings.

Result	Model	Size-Hiding	Assumption	Efficiency	Rounds
Impossible	Client/Server	Two-side	None	×	×
Prot. 1	C/S with TTP	Two-side	None	*NO*	2
Prot. 2	Client/Server	Two-side	Standard Model	*NO*	2
Prot. 3	Client/Server	Two-side*	Standard Model	*YES*	2
Prot. 4	C/S with TTP	One-side	Standard Model	*YES*	1
Prot. 5	C/S with TTP	One-side	Standard Model	*YES*	2
Prot. 6	C/S with TTP	One-side	Random Oracle Model	*YES*	3
Prot. 7	C/S with TTP	One-side	Random Oracle Model	*YES*	1

* an upper bound on the sizes of both sets (client's and server's) is needed

References

[1] G. Ateniese, E. De Cristofaro, and G. Tsudik, *(If) Size Matters: Size-Hiding Private Set Intersection*, PKC 2011, LNCS, Vol. 6571, pp. 156-173, 2011.

[2] P. Baldi, R. Baronio, E. De Cristofaro, P. Gasti, and G. Tsudik, *Countering GATTACA: Efficient and Secure Testing of Fully-Sequenced Human Genomes* In CCS, 2011.

[3] M. Bellare and P. Rogaway, *The Exact Security of Digital Signatures - How to Sign with RSA and Rabin*, EUROCRYPT 1996, LNCS, Vol. 1070, pp. 399416, 1996.

[4] E. De Cristofaro, S. Faber, G. Tsudik, *Secure Genomic Testing with Size- and Position-Hiding Private Substring Matching*, WPES 13, 2013.

[5] M. Chase and I. Visconti, *Secure database commitments and universal arguments of quasi knowledge*, In CRYPTO, pp. 236254, 2012.

[6] J.L. Carter and M.N. Wegman, *Universal classes of hash functions*, Journal of Computer and System Sciences, Vol. 18, 143154, 1079.

[7] R. Cramer, *Introduction to Secure Computation*, Lectures on Data Security, LNCS, Vol. 1561, pp. 16-62, 1999.

[8] J. Camenisch, M. Kohlweiss and C. Soriente, *An Accumulator Based on Bilinear Maps and Efficient Revocation for Anonymous Credentials*, PKC 2009, LNCS, Vol. 5443, pp. 481-500, 2009.

[9] J. Camenisch and A. Lysyanskaya, *A Signature Scheme with Efficient Protocols*, SCN 2002, LNCS, Vol. 2576, pp., 268-289, 2003.

[10] J. Camenish and G. M. Zaverucha, *Private Intersection of Certified Sets*, FC 2009, LNCS, Vol. 5628, pp., 108-127, 2009.

[11] P. D'Arco, M. I. Gonzalez Vasco, A. L. Perez del Pozo, and C. Soriente *Size-Hiding in Private Set Intersection: Existential Results and Constructions* Proc. of the 5th International Conference on Cryptology (Africacrypt 2012). Lecture Notes in Computer Science, Vol. 7374, pp. 378-394, Springer Verlag, 2012. Journal version in progress.

[12] C. Dong, L. Chen, and Z. Wen, *When Private Set Intersection Meets Big Data: An Efficient and Scalable Protocol*, CCS13, pp. 789-800, 2013.

[13] E. De Cristofaro, S. Jarecki, J. Kim, G.Tsudik. *Privacy-Preserving Policy-Based Information Transfer.* Privacy Enhancing Technologies (PES09), LNCS, Vol. 5672, pp. 164184, 2009.

[14] E. De Cristofaro, J. Kim, and G. Tsudik, *Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model*, ASIACRYPT 2010, LNCS, Vol. 6477, pp. 213231, 2010.

[15] E. De Cristofaro and G. Tsudik, *Practical Private Set Intersection Protocols with Linear Complexity*, FC 2010, LNCS, Vol. 6052, pp. 143-159, 2010.

[16] D. Dachman-Soled, T. Malkin, M. Raykova and M. Yung, *Efficient Robust Private Set Intersection*, 7th International Conference on Applied Cryptography and Network Security (ACNS), Vol. , pp. 125-142, 2009.

[17] D. Dachman-Soled, T. Malkin, M. Raykova and M. Yung, *Secure Efficient Multiparty Computing of Multivariate Polynomials and Applications*, 9th International Conference on Applied Cryptography and Network Security (ACNS), Vol. , pp. 130-146, 2011.

[18] S. Even, O. Goldreich, and A. Lempel, *A Randomized Protocol for Signing Contracts*, Communications of the ACM, Volume 28, Issue 6, pp. 637-647, 1985.

[19] K. Frikken, *Privacy-Preserving Set Union*, ACNS 2007, Vol. , pp. 237-252, 2007.

[20] M. J. Freedman, Y. Ishai, B. Pinkas and O. Reingold, *Keyword Search and Oblivious Psudorandom Functions*, TCC 2005, LLNC, Vol. 3378, pp. 303-324, 2005.

[21] M. J. Freedman, K. Nissim, and B. Pinkas, *Efficient Private Matching and Set Intersection*, Eurocrypt 2004, LNCS, Vol. 3027, pp. 1-19, 2004.

[22] O. Goldreich, *Foundations of Cryptography - Volume II Basic Applications*, Cambridge Press, 2004.

[23] S. Jarecki, X. Liu. *Efficient oblivious pseudorandom function with ap- plications to adaptive OT and secure computation of set intersection*, TCC 2009, LNCS, Vol. 5444, pp. 577594, 2009.

[24] S. Jarecki, X. Liu. *Fast and Secure Computation of Set Intersection*, SCN 2010, LNCS 6280, pp. 418435, 2010.

[25] C. Hazay and Y. Lindell, *Efficient Protocols for Set Intersection and Pattern Matching with Security Against Covert Adversaries*, TCC 2008, LNCS, Vol. 4948, pp. 155 - 175, 2008.

[26] R. Impagliazzo and S. Rudich, *Limits on the provable consequences of one-way permutations*, Proc. of the 21st Annual ACM Symposium on Theory of Computing, pp. 44-61, Seattle, Washington, May 1989.

[27] F. Kerschbaum, *Outsourced Private Set Intersection Using Homomorphic Encryption*, ASIACCS 12, 2012.

[28] L. Kissner and D. Song, *Privacy-Preserving Set Operations*, Crypto 2005, LNCS, Vol. 3621, pp. 241-257, 2005.

[29] Y. Lindell, K. Nissim, and C. Orlandi, *Hiding the Input-Size in Secure Two-Party Computation*, ASIACRYPT 2013, LNCS, Vol. 8270, pp. 421440, 2013.

[30] R. Nojima, Y. Kadobayashi, *Cryptographically Secure Bloom-Filter*, Transactions on Data Privacy, Vol. 2, pp. 131139, 2009.

[31] M. Naor and O. Reingold, *Number-theoretic constructions of efficient pseudo-random functions*, Journal of the ACM, Vol. 51, No. 2, pp. 231-262, 2004.

[32] P. Pailler, *Public-key Cryptosystems based on composite degree residuosity classes*, Crypto 1999, LNCS, Vol. 1592, pp. 223-239, 1999.

[33] B. Pinkas, T. Schneider, M. Zohner, *On the Performance of Private Set Intersection.*

[34] M. Rabin, *How to exchange secrets by oblivious transfer*, Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[35] R. Rivest, *Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer*, unpublished manuscript, 11/8/1999 available at http://people.csail.mit.edu/rivest/publications.html

[36] D. R. Stinson, *Universal hash families and the leftover hash lemma, and applications to cryptography and computing*, J. Combin. Math. Combin. Comput. Vol. 42, 3-31, 2002.

4 Visual Cryptography

4.1 Problem and state-of-art

Visual cryptography is a special type of secret sharing in which the secret is an image and the shares are random-looking images printed on transparencies. The captivating peculiarity of this type of secret sharing is that the reconstruction of the secret is performed without any computational machinery: it is enough to superpose the shares (transparencies) in order to reconstruct the secret. Visual cryptography has been introduced independently by Naor and Shamir [24], who have used a deterministic framework, and by Kafri and Keren [20], who have used a probabilistic framework.

Roughly speaking, deterministic visual cryptography works as follows. A secret image, known by a trusted party called the *dealer*, has to be shared among a set of participants in such a way that some subsets of participants, called *qualified sets* are able to visually recover the images while others, called *forbidden sets*, do not have any information about the secret image. In order to share the image, the dealer creates a share for each participant. In a share each single pixel of the secret image is represented with a set of m, $m \geq 2$, pixels. Parameter m is the pixel expansion: the recovered secret image will be m times bigger than the original secret image. Limiting our discussion to black and white images, the shares are such that when we superpose shares of a qualified set of participants, among the m pixels that represent a secret pixels s, we will find at most ℓ black pixels if s is white and at least h black pixels if s is black, with $0 \leq \ell < h \leq m$. That is, in the recovered secret image, white secret pixels are reconstructed with at most ℓ black pixels out of m pixels, while black secret pixels are reconstructed with at least h black pixels. This difference makes up the *contrast*, which is a measure of the quality of the reconstructed image.

In the probabilistic framework, instead, there is no pixel expansion, that is to say, if we want still to use the parameter m, that we have $m = 1$. Clearly, with no pixel expansion, a secret pixel corresponds to one pixel in the reconstructed image, and obviously we will consider it white if the pixel is white and black if it is black. Using the thresholds ℓ and h, we have that for random grids we must use $\ell = 0$ and $h = 1$. It is not surprising that we cannot achieve such a reconstruction in a deterministic way. Indeed reconstruction in visual sharing based on random grids is guaranteed only with some probability: the *average light transmission* (white pixels) in the area of the reconstructed image that corresponds to the white area of the secret image is bigger than the average light transmission in the area of the reconstructed image that corresponds to the black area of the secret image. Such a difference makes up the contrast.

Usually one talks about *deterministic* visual cryptography to refer to the model introduced by Naor and Shamir and about *random grid* visual cryptography to refer to the model introduced by Kafri and Keren (a random grid is an image where each pixel is randomly chosen to be black or white with uniform probability).

Deterministic visual cryptography has been widely studied. Many papers have explored various aspects: minimal pixel expansion (e.g., [4, 5, 18]), optimal contrast (e.g., [22, 19, 8, 6]), general access structures (e.g., [1, 23]), perfect reconstruction of black pixels (e.g., [7, 27, 5]) color images (e.g. [11, 12, 17, 21, 28, 33]), and other issues (e.g. [3, 31, 32]). We remark that the above citations are not comprehensive. We refer the interested reader to [14] for more pointers to the literature.

The random grid model has recently received a lot of attention. Yang [30] introduced a model (called *probabilistic*) which is in fact equivalent to the random grid model of Kafri and Keren.

In the field of genomic computing visual cryptography might be used to protect private information that must be accessible only to specified subset of people (e.g., the patient and some specific doctors). Although such a goal can be achieved also through regular secret sharing, visual secret sharing is more suitable in the cases where the reconstruction has to happen without the use of a computing device (e.g., near the patient bed or in other places where a computer is not available).

4.2 Findings

We have studied the relation between the deterministic and the random grid model proving that they are essentially equivalent. Any scheme in the deterministic model can be transformed into an equivalent scheme in the random grid model and viceversa. This result is important because it allows not to duplicate research efforts. We have also provided new schemes for the case where the secret image is a black and white image and the shares are allowed to be color images. Another interesting point is that of using visual cryptography as a means for secure two-party computation. We have showed how to use physical shares to implement a well-known protocol for secure two-party computation. The *contrast* is a measure of the quality of the visual reconstruction of the secret image. Various measures of the contrast have been used to assess the goodness of visual cryptography schemes. We have characterized optimal schemes using an approach that is independent of the specific measure of contrast that is used and can be instantiated with such a measure.

References

[1] Ateniese G., Blundo C., De Santis A. and Stinson D. R. (1996) Visual cryptography for general access structures. Information and Computation, 129, pp. 86–106.

[2] Ateniese G., Blundo C., De Santis A. and Stinson D. R. Constructions and bounds for visual cryptography. Proceedings of ICALP 1996, LNCS 1099, pp. 416–428, 1996.

[3] Ateniese G., Blundo C., De Santis A. and Stinson D. R. Extended schemes for visual cryptography. *Theoretical Computer Science*, vol. 250, pp. 143–161, 2001.

[4] Blundo C., Cimato S. and De Santis A. Visual cryptography schemes with optimal pixel expansion. *Theoretical Computer Science*, vol. 369, pp. 169-182, 2006.

[5] Blundo C., De Bonis A. and De Santis A.. Improved schemes for Visual Cryptography. *Designs, Codes and Cryptography*, vol. 24, pp. 255-278, 2001.

[6] Blundo C., D'Arco P., De Santis A. and Stinson D. R. Contrast optimal threshold visual cryptography schemes. *SIAM J. on Discrete Mathematics*, vol. 16, pp. 224–261, 2003.

[7] Blundo C. and De Santis A. Visual cryptography schemes with perfect reconstruction of black pixels. *Journal for Computers & Graphics*, vol. 22, pp. 449–455, 1998.

[8] Blundo C., De Santis A. and Stinson D. R. On the contrast in visual cryptography schemes. *Journal of Cryptology*, vol. 12, pp. 261–289, 1999.

[9] Chen T.-H., Tsao K.-H. Visual secret sharing revisited. *Pattern Recognition*, vol. 42, pp. 2203–2217, 2009.

[10] Chen T.-H., Tsao K.-H. Threshold visual secret sharing by random grids. *The Journal of Systems and Software*, vol. 84, pp. 1197-1208, 2011.

[11] Cimato S., De Prisco R. and De Santis A., Colored visual cryptography without color darkening. *Theoretical Computer Science*, Vol. 374(1-3), pp. 261-276, 2007.

[12] Cimato S., De Prisco R. and De Santis A. Optimal colored threshold visual cryptography schemes. *Designs, Codes and Cryptography*, vol. 35, pp. 311–335, 2005.

[13] Cimato S., De Prisco R. and De Santis A. Probabilistic Visual Cryptography Schemes. *Comput. J.*, vol. 49(1), pp. 97–107, 2006.

[14] *Visual Cryptography and Secret Image Sharing*, Cimato S. and Yang C.-N. editors, CRC Press, Boca Raton, Florida, USA, ISBN 978-1-4398-3721-4, 2012.

[15] D'Arco P., De Prisco R., De Santis A. Measure-independent characterization of contrast optimal visual cryptography schemes. *Journal of Systems and Software* vol. 95 pp. 89-99, 2014.

[16] De Prisco R., De Santis A. On the Relation of Random Grid and Deterministic Visual Cryptography. *IEEE Transactions on Information Forensics and Security* Vol. 9(4), pp.653-665, 2014.

[17] De Prisco R. and De Santis A., Using Colors to Improve Visual Cryptography for Black and White Images, Proceedings of ICITS 2011, LNCS 6673, pp. 182–201, 2011.

[18] Eisen P.A. and Stinson D.R., Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels. *Designs, Cods and Cryptography*, vol. 25, pp. 15–61, 2002.

[19] Hofmeister T., Krause M. and Simon H. U., Contrast-optimal k out of n secret sharing schemes in Visual Cryptography. *Theoretical Computer Science*, 240, pp. 471–485, 2000.

[20] Kafri O. and Keren E., Encryption of pictures and shapes by random grids. *Optics Letters*, vol. 12, n. 6, pp. 377-379, 1987.

[21] Koga H. and Yamamoto H., Proposal of a Lattice-Based Visual Secret Sharing Scheme for Color and Gray-Scale Images. *IEICE Trans. on Fundamentals of Electronics, Communication and Computer Sciences*, Vol 81-A(6), pp. 1262–1269, 1998.

[22] Krause M. and Simon H. U. Determining the optimal contrast for secret sharing schemes in visual cryptography. *Combinatorics, Probability and Computing*, vol. 12, pp. 285–299, 2003.

[23] Lu S., Manchala D. and Ostrovsky R.. Visual cryptography on graphs. *J. Comb. Optim.*, vol 21, pp. 47–66, 2011.

[24] Naor M. and Shamir A. Visual cryptography. In Proceedings of Eurocrypt 94, LNCS 950, pp. 1–12, 1994.

[25] Shyu S.-J., Image encryption by random grids. *Pattern Recognition*, vol. 40, pp. 1014–1031, 2007.

[26] Shyu S.-J., Image encryption by multiple random grids. *Pattern Recognition*, vol. 42, pp. 1582–1596, 2009.

[27] Simon H.U., Perfect Reconstruction of Black Pixels Revisited. Proceedings of FCT 2005, LNCS 3623, pp. 221–232, 2005.

[28] Verheul E. R. and van Tilborg H. C. A. Constructions and properties of k out of n visual secret sharing schemes. *Designs, Codes, and Cryptography*, vol. 11, pp. 179–196, 1997.

[29] Wang R.-Z., Lan Y.-C., Lee Y.-K., Huang, Shyu S.-J., Chia T.-L., Incrementing visual cryptography using random grids. *Optics Communication*, vol. 283, pp. 4242–4249, 2010.

[30] Yang C-N. New Visual Secret Sharing Schemes using Probabilistic Method. *Pattern Recognition Letters*, vol. 25, pp. 481–494, 2004.

[31] Yang C-N. and Chen T-S. Size-adjustable visual secret sharing schemes. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E88-A, pp. 2471–2474, 2005.

[32] Yang C-N. and Chen T-S. Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion *Pattern Recognition Letters*, vol. 26, pp. 193–206, 2005.

[33] Yang C-N. and Laih C.-S. New colored visual secret sharing schemes. *Designs, Codes, and Cryptography*, vol. 20, pp. 325–335, 2000.

5 Private Proofs of Physical Properties

5.1 Problem and State-of-Art

The concepts of interactive proofs and zero knowledge are fundamental building blocks in Cryptography.

An *interactive proof system* [6] for a language L is a pair of interactive Turing machines (P, V), satisfying the requirements of *completeness* and *soundness.* Informally, completeness requires that for any $x \in L$, at the end of the interaction between P and V, where P has on input a valid witness for $x \in L$, V rejects with negligible probability. Soundness requires that for any $x \notin L$, for any computationally unbounded $\mathsf{P}^\star$, at the end of the interaction between $\mathsf{P}^\star$ and V, V accepts with negligible probability. When $\mathsf{P}^\star$ is only probabilistic polynomial-time, then we have an argument system.

An interactive proof system is *zero knowledge* if no information is leaked by P during the interaction with an adversarial verifier $\mathsf{V}^\star$. This security notion is formalized by requiring the existence of an expected polynomial-time machine named Simulator, that without having access to a witness is able to produce an output that is indistinguishable from the one of $\mathsf{V}^\star$ after an execution of the proof system with P.

We know that anything that can be proved efficiently can also be proved in a zero-knowledge manner [5]. Unfortunately, this feasibility result and all follow up papers do not help to prove physical properties. Considering the case of proving that two DNA fingerprints match, it is not clear at all whether previous work on zero-knowledge proofs can be helpful. More in general, it is not clear how to prove in zero knowledge that an object satisfies some physical properties.

Notice that genetic privacy in DNA profiling is nowadays a well known issue.

5.2 Findings

Very recently, Fisch et al. in [9] presented the first formal treatment of the notion of physical zero knowledge that is inspired to the notion of Universally Composability of [1].

They also constructed the first zero-knowledge protocol that allows a prover to convinces a verifier that the DNA profile of the prover does not match another known profile. The prover manages to convince the verifier without leaking any additional information about its DNA profile.

6 Hiding the Input-Size in *Any* 2-Party Computation

6.1 Problem and State-of-Art

The setting of secure 2-party computation considers two mutually distrustful parties that want to securely evaluate a function f. The result of [7] showed how to realize such a task even when a party can be corrupted.

For the same reasons already explained when discussing PSI, the input size of both players is revealed by the constructions of [7]. Therefore an important open question is whether there exist constructions of secure 2-party computation for all functions that allow to protect input privacy of a player. We stress that for generic functionalities, the notion of secure computation is the only known way to meaningfully capture security against arbitrarily malicious adversaries.

The previously discussed motivations for considering input-size hiding PSI in the context of genomic computing, also apply to the case of input-size hiding secure 2PC. The reason is that all progress on PSI is relevant only for the set intersection feature. For instance consider the variation of PSI where also elements of the sets that are similar enough are supposed to be given in output. Clearly a protocol for PSI becomes useless and a new input-size hiding protocol should be designed for such a new functionality. The need of constructing ad-hoc protocols each time the function chances is a major weakness that can seriously affect the attempt to introduce security features in genomic computing.

6.2 Findings

In a very recent work [2], we show how to obtain input-size hiding secure 2PC for any functionality, protecting therefore the input-size of one player in addition to the security obtained in [7]. We obtained this result by slightly modifying the definition of [7] and making use of recent progress in cryptography (i.e., fully homomorphic encryption [4], probabilistic checkable proofs of proximity [3], universal arguments of quasi knowledge [5]).

More in details, we give a definition that requires the player to essentially know a short representation of its input. Moreover the player must also know how to compute the output of the function by relying only on the input of the other player, and to its knowledge of the input corresponding to the short representation discussed above.

A natural question is whether the update of the definition is really needed to obtain such results. The answer is affirmative in the sense that another result proved in [2] shows that under the standard definition of [7], input-size hiding secure 2PC would imply a form of proofs of work that seems to be impossible to achieve under standard assumptions.

References

[1] R. Canetti, *Universally Composable Security: A New Paradigm for Cryptographic Protocols*, In *FOCS '01*, pp. 136–145. 2009.

[2] M. Chase, R. Ostrovsky and I. Visconti, *Input-Size Hiding Secure Computation and a New Ideal Model*, In submission.

[3] D. Dachman-Soled and Y. T. Kalai, *Securing Circuits against Constant-Rate Tampering*, In *CRYPTO '12*, pp. 553-551. 2012.

[4] C. Gentry, *Fully homomorphic encryption using ideal lattices*, In *STOC '09*, pp. 169–178. 2009.

[5] O. Goldreich, S. Micali, A. Wigderson, Avi, *Proofs that yield nothing but their validity.* Journal of the ACM 38 (3): 690728.

[6] S. Goldwasser, S. Micali, and C. Rackoff, *The knowledge complexity of interactive proof systems*, *SIAM Journal on Computing*, 18(1):186–208, 1989.

[7] O. Goldreich, S. Micali, and A. Wigderson. *How to play any mental game or a completeness theorem for protocols with honest majority.* In *STOC '87*, pp. 218–229. 1987.

[8] B. Fisch, D. Freund, M. Naor *How to Prove all NP-Statements in Zero-Knowledge, and a Methodology of Cryptographic Protocol Design* In *CRYPTO '86.*

[9] B. Fisch, D. Freund, M. Naor, *Physical Zero-Knowledge Proofs of Physical Properties*, In *CRYPTO '14.*