A quick overview of my research activity.
Abstracts of the papers published from 1999 to 2013

Paolo D’Arco

July 23, 2013

Hi! In the following pages I have collected the abstracts of the papers which, with my co-authors, I have published in my academic career until now. Conference versions are treated together with the corresponding journal versions, if they have been written and published. The abstracts are about Cryptography, apart a couple of them, which belong to the data security area.
Abstract: The growing need for user privacy protection has lead to the development of general notions and efficient tools for building privacy-preserving applications. Among them, the notion of key privacy in public-key encryption, which guarantees that an adversary is unable to tell with which public key a certain ciphertext has been produced, plays a key-role in the design of several anonymous protocols. Apparently, it seems to be unrelated to the security of the encrypted content, and it looks like just an additional property the encryption scheme can enjoy. In this paper we show that for a robust encryption scheme key privacy under chosen ciphertext attack implies non-malleability and, hence, security under chosen ciphertext attacks. Then, we look at two privacy-preserving protocols: secret sets and anonymous broadcast encryption. We prove that secret sets and anonymous broadcast are equivalent w.r.t. non-adaptive adversaries: the first can be used to design the second and vice versa. Finally, we revisit some previous constructions for secret sets, and we show the security properties they enjoy within a rigorously defined adversarial model.

Title: Towards tracing and revoking schemes secure against collusion and any form of secret information leakage.
Authors: Paolo D’Arco and Angel Perez del Pozo.

Abstract: Tracing and revoking schemes enable a center to deliver protected content to a subset of privileged users of a given universe. The main property these schemes enjoy is that traitors, who illegally help unauthorized users to set up a pirate decoder for gaining access to the protected content, can be identified and removed from the privileged subset. Historically traitors have been modeled as users who privately share their secret information with unauthorized users. However, in the Pirates 2.0 attack model, traitors collaborate in public and partially share their secret information with a certified guarantee of anonymity. Several classes of tracing and revoking schemes, like tree-based tracing and revoking schemes and code-based tracing schemes, are subject to such a new threat. In this paper we propose methods to cope with the Pirates 2.0 attack. We focus our attention on the class of tree-based schemes. We start by discussing some simple techniques, which can partially help to deal with the attack, and point out their limits. Then, looking through the literature, we recover some ideas, which can be used to strengthen tracing and revoking schemes. We also analyze the trade-off which can be obtained by applying these ideas to the schemes. Finally, we describe new hybrid schemes, obtained by mixing previous constructions, which can be used to face up the Pirates 2.0 attack.
Title: Size-Hiding in Private Set Intersection: Existential Results and Constructions.
Authors: Paolo D’Arco, Maria Isabel Gonzalez Vasco, Angel Luis Perez del Pozo, and Claudio Soriente

Abstract: In this paper we focus our attention on private set intersection. We show impossibility and existential results, and we provide some explicit constructions. More precisely, we start by looking at the case in which both parties, client and server, in securely computing the intersection, would like to hide the sizes of their sets of secrets, and we show that:

- It is impossible to realize an unconditionally secure size-hiding set intersection protocol.
- In a model where a TTP provides set up information to the two parties and disappears, unconditionally secure size-hiding set intersection is possible.
- There exist computationally secure size-hiding set intersection protocols.

Then, we provide some explicit constructions for one-sided protocols, where only the client gets the intersection and hides the size of her set of secrets. In the model with the TTP, we design two protocols which are computationally secure under standard assumptions, and two very efficient protocols which are secure in the random oracle model. We close the paper with some remarks and by pointing out several interesting open problems.

Title: An Almost-Optimal Forward-Private Rfid Mutual Authentication Protocol with Tag Control.
Author: P. D’Arco

Abstract: In this paper we propose an efficient forward-private RFID mutual authentication protocol. The protocol is secure under standard assumptions. It builds over a recent work, extends it to achieve mutual authentication, and improves it by introducing a resynchronization mechanism between tag and reader, through which the server-side computation from $O(N\omega)$ is reduced to $O(N + \omega)$, where $N$ is the total number of tags in the system, and $\omega$ is the maximum number of authentications each single tag can afford during its lifetime. Moreover, the protocol enables the server to control how many times a tag has been read by legitimate and fake readers.

Title: On Ultra-Lightweight RFID Authentication Protocols.
Authors: Paolo D’Arco and Alfredo De Santis.
Abstract: A recent research trend, motivated by the massive deployment of RFID technology, looks at cryptographic protocols for securing communication between entities in which some of the parties have very limited computing capabilities. In this paper we focus our attention on **SASI**, a new RFID authentication protocol, designed for providing **Strong Authentication** and **Strong Integrity**. **SASI** is a good representative of a family of RFID authentication protocols, referred to as Ultra-Lightweight RFID authentication protocols. These protocols, suitable for passive tags with limited computational power and storage, involve simple bitwise operations like **and**, **or**, **exclusive or**, modular addition, and cyclic shift operations. They are efficient, fit the hardware constraints, and can be seen as an example of the above research trend. However, the main concern is the real security of these protocols, which are often supported only by apparently reasonable and intuitive arguments. The contribution we provide with this work is the following: we start by showing some weaknesses in the **SASI** protocol and, then, we describe how such weaknesses, through a sequence of simple steps, can be used to compute in an efficient way all secret data used for the authentication process. Specifically, we describe three attacks: 1) a de-synchronisation attack, through which an adversary can break the synchronisation between the RFID reader and the tag; 2) an identity disclosure attack, through which an adversary can compute the identity of the tag; 3) a full disclosure attack, which enables an adversary to retrieve all secret data stored in the tag. Then, we present some experimental results, obtained by running several tests on an implementation of the protocol, in order to evaluate the performance of the proposed attacks, which confirm that the attacks are effective and efficient. It comes out that an active adversary by interacting with a tag more or less three-hundred times, makes the authentication protocol completely useless. Finally, we close the paper with some observations. The cryptoanalysis of **SASI** gets some new light on the ultra-lightweight approach, and can also serve as a warning to researchers working on the field and tempted to apply these techniques. Indeed, the results of this work, rise serious questions regarding the limits of the ultra-lightweight family of protocols, and on the benefits of these ad-hoc protocol design strategies and informal security analysis.

| Title: Variations on a Theme by Akl and Taylor: Security and Tradeoffs. 
| Authors: Paolo D’Arco, Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. 

Abstract: In 1983 Akl and Taylor [Cryptographic Solution to a Problem of Access Control in a Hierarchy, ACM Transactions on Computer Systems, 1(3), 239–248, 1983] first suggested the use of cryptographic techniques to enforce access control in hierarchical structures. Due to its simplicity and versatility, the scheme has been used, for more than twenty years, to implement access control in several different domains, including mobile agent environments and XML documents. However, despite of its use over time, the scheme has never been fully analyzed with respect to security and efficiency requirements. In this paper we provide new results on the Akl-Taylor scheme and its variants. More precisely:

- We provide a rigorous analysis of the Akl-Taylor scheme. We consider different key assignment strategies and prove that the corresponding schemes are secure against key recovery.
We show how to obtain different tradeoffs between the amount of public information and the number of steps required to perform key derivation in the proposed schemes.

We also look at the MacKinnon et al. and Harn and Lin schemes and prove they are secure against key recovery.

We describe an Akl-Taylor based key assignment scheme with time-dependent constraints and prove the scheme efficient, flexible and secure.

We propose a general construction, which is of independent interest, yielding a key assignment scheme offering security w.r.t. key indistinguishability, given any key assignment scheme which guarantees security against key recovery.

Finally, we show how to use our construction, along with our assignment strategies and tradeoffs, to obtain an Akl-Taylor scheme, secure w.r.t. key indistinguishability, requiring a constant amount of public information.

Title: Semi-Destructive Privacy in RFID Systems.
Authors: Paolo D’Arco, Alessandra Scafuro and Ivan Visconti.

Abstract: RFID is nowadays a pervasive technology, of interest for several research areas (e.g., sensor networks, algorithms, cryptography, hardware design) with different goals. A major challenge is the design of RFID-enabled systems which enjoy satisfying notions of security and privacy, and that can be executed by currently available low-cost RFID chips. In order to evaluate properties and weaknesses of RFID protocols, Vaudenay presented in [ASIACRYPT 2007] a general RFID security and privacy model that abstracts some previous works in a single, concise, and much more understandable framework. He introduced eight distinct notions of privacy, corresponding to adversaries of different strength, and proved some possibility and impossibility results for such privacy notions. However, some interesting problems as: 1) achieving stronger privacy using low-cost tags (i.e., tags that usually cannot perform public-key cryptography), 2) achieving stronger privacy in presence of side-channel attacks (e.g., DoS attacks, detection of the outputs of identification protocols), and 3) achieving stronger privacy under standard complexity-theoretic assumptions, are still left open. In this paper, we address the above problems and give two contributions. First of all we show that Vaudenay’s privacy notions are impossible to achieve in presence of DoS attacks. Therefore, we extend the model to better reflect the real-world scenario, where these attacks are easy to mount (e.g., by physically destroying/making inactive tags). More precisely, we refine Vaudenay’s privacy model to deal with DoS attacks, and introduce an additional privacy notion, referred to as semi-destructive privacy, which takes into account hardware features of some real-world tags. Then, we show an efficient RFID protocol that, by only using symmetric-key cryptography, satisfies the notion of semi-destructive privacy, under standard complexity-theoretic assumptions. This protocol is the main contribution of the work. Indeed, previous results either used public-key cryptography (too...
expensive according to current tags’ capabilities) or resorted to the existence of random oracles (a controversial assumption) or achieved some weak forms of privacy (e.g., against limited adversaries which cannot corrupt tags).

Title: Optimising SD and LSD in presence of non-uniform probabilities of revocation.
Authors: Paolo D’Arco and Alfredo De Santis.

Abstract: Some years ago two efficient broadcast encryption schemes for stateless receivers, referred to as SD (Subset Difference Method) and LSD (Layered Subset Difference Method), were proposed. They represent one of the most suitable solution to broadcast encryption. In this paper we focus on the following issue: both schemes assume uniform probabilities of revocation of the receivers. However, in some applications, such an assumption might not hold: receivers in a certain area, due to historical and legal reasons, can be considered trustworthy, while receivers from others might exhibit more adversarial behaviours. Can we modify SD and LSD to better fit settings in which the probabilities of revocation are non-uniform?

More precisely, we study how to optimise user key storage in the SD and LSD schemes in presence of non-uniform probabilities of revocation for the receivers. Indeed, we would like to give less keys to users with higher probability of revocation compared to trustworthy users. We point out that this leads to the construction of binary trees satisfying some optimality criteria.

We start our analysis revisiting a similar study, which aims at minimising user key storage in LKH schemes. It was shown that such a problem is related to the well-known optimal codeword length selection problem in information theory. We discuss the approach therein pursued, pointing out that a characterisation of the properties a key assignment for LKH schemes has to satisfy, does not hold. We provide a new characterisation and give a proof of it. Then, we show that also user key storage problems of SD and LSD are related to an interesting coding theory problem, referred to as source coding with Campbell’s penalties. Hence, we discuss existing solutions to the coding problem.

Title: On Unconditionally Secure Distributed Oblivious Transfer
Authors: Carlo Blundo, Paolo D’Arco, Alfredo De Santis and Douglas Stinson.

Abstract: This paper is about the Oblivious Transfer in the distributed model proposed by M. Naor and B. Pinkas. In this setting a Sender has n secrets and a Receiver is interested in one of them. During a set up phase, the Sender gives information about the secrets to m Servers. Afterwards, in a recovering phase, the Receiver can compute the secret she wishes by interacting with any k of them. More precisely, from the answers received she computes the secret in which she is interested but she gets no information on the others and, at the same time, any coalition of k – 1 Servers can neither compute any secret nor figure out which one the Receiver has recovered.

We present an analysis and new results holding for this model: lower bounds on the resources required to implement such a scheme (i.e., randomness, memory storage, communication complexity);
some impossibility results for one-round distributed oblivious transfer protocols; two polynomial-based constructions implementing 1-out-of-n distributed oblivious transfer, which generalize and strengthen the two constructions for 1-out-of-2 given by Naor and Pinkas; as well as new one-round and two-round distributed oblivious transfer protocols, both for threshold and general access structures on the set of Servers, which are optimal with respect to some of the given bounds. Most of these constructions are basically combinatorial in nature.

Title: On Self-healing Key Distribution Schemes.
Authors: Carlo Blundo, Paolo D’Arco, and Alfredo De Santis.

Abstract: Self-healing key distribution schemes allow group managers to broadcast session keys to large and dynamic groups of users over unreliable channels. Roughly speaking, even if during a certain session some broadcast messages are lost due to network faults, the self-healing property of the scheme enables each group member to recover the key from the broadcast messages he has received before and after that session. Such schemes are quite suitable in supporting secure communication in wireless networks and mobile wireless ad-hoc networks. Recent papers have focused on self-healing key distribution, and have provided definitions, stated in terms of the entropy function, and some constructions. The contribution of this paper is the following:

- We analyze current definitions of self-healing key distribution and, for two of them, we show that no protocol can achieve the definition.
- We show that a lower bound on the size of the broadcast message, previously derived, does not hold.
- We propose a new definition of self-healing key distribution, and we show that it can be achieved by concrete schemes.
- We give some lower bounds on the resources required for implementing such schemes i.e., user memory storage and communication complexity. We prove that the bounds are tight.

Title: Neural Network Techniques for Proactive Password Checking.
Authors: Angelo Ciaramella, Paolo D’Arco, Alfredo De Santis, Clemente Galdi, and Roberto Tagliaferri.
Abstract: This paper deals with the access control problem. We assume that valuable resources need to be protected against unauthorised users and that, to this aim, a password-based access control scheme is employed. Such an abstract scenario captures many applicative settings. The issue we focus our attention on is the following: password-based schemes provide a certain level of security as long as users choose good passwords, i.e., passwords hard to guess in a reasonable amount of time. In order to force the users to good choices, a proactive password checker can be implemented as a submodule of the access control scheme. Such a checker, any time the user chooses/changes his own password, decides on the fly whether to accept or refuse the new password, depending on its guessability. Hence, the question is: How can we get an effective and efficient proactive password checker? By means of neural networks and statistical related techniques, we answer the above question developing proactive password checkers. Through a series of experiments, we show that these checkers have very good performance: error rates are comparable to the ones of the best existing checkers, implemented on different principles and by using other methodologies, and memory requirements are better in several cases. It is the first time that the neural network technology is fully and successfully applied to designing proactive password checkers.

Title: Properties and Constraints of Cheating-Immune Secret Sharing Scheme.
Authors: Paolo D’Arco, Wataru Kishimoto, and Douglas Stinson.

Abstract: A secret sharing scheme is a cryptographic protocol by means of which a dealer shares a secret among a set of participants in such a way that it can be subsequently reconstructed by certain qualified subsets. The setting we consider is the following: in a first phase, the dealer gives in a secure way a piece of information, called a share, to each participant. Then, participants belonging to a qualified subset send in a secure way their shares to a trusted party, referred to as a combiner, who computes the secret and sends it back to the participants. Cheating-immune secret sharing schemes are secret sharing schemes in the above setting where dishonest participants, during the reconstruction phase, have no advantage in sending incorrect shares to the combiner (i.e., cheating) as compared to honest participants. More precisely, a coalition of dishonest participants, by using their correct shares and the incorrect secret supplied by the combiner, have no better chance in determining the true secret (that would have been reconstructed if they submitted correct shares) than an honest participant. In this paper we study properties and constraints of cheating-immune secret sharing schemes. We show that a perfect secret sharing scheme cannot be cheating-immune. Then, we prove an upper bound on the number of cheaters tolerated in such schemes. We also repair a previously proposed construction to realize cheating-immune secret sharing schemes. Finally, we discuss some open problems.

Title: A Unified Model for Unconditionally Secure Key Distribution.
Authors: Stelvio Cimato, Antonella Cresti, and Paolo D’Arco.
Abstract: A key distribution scheme is a method by means of which a trusted party distributes pieces of information among a set of users in such a way that each group of them can compute a common key for secure communication. In this paper we present a model for unconditionally secure key distribution schemes, i.e., schemes whose security is independent of the power of the adversary. We prove lower bounds on the amount of information the trusted party has to generate and each user has to keep secret in such schemes, and we show that some previous unconditionally secure models for key distribution fall in our model. As a consequence, the lower bounds given in the literature for these models can be seen as corollaries of our results. Hence, the main contribution of the paper consists in pointing out a sort of common structure underlying some apparently different key distribution techniques.

Title: Security of Public Key Cryptosystems based on Chebyshev Polynomials.
Authors: Pina Bergamo, Paolo D’Arco, Alfredo De Santis, and Ljupco Kocarev.

Abstract: Chebyshev polynomials have been recently proposed for designing public-key systems. Indeed, they enjoy some nice chaotic properties, which seem to be suitable for use in Cryptography. Moreover, they satisfy a semi-group property, which makes possible implementing a trapdoor mechanism. In this paper we study a public key cryptosystem based on such polynomials, which provides both encryption and digital signature. The cryptosystem works on real numbers and is quite efficient. Unfortunately, from our analysis it comes up that it is not secure. We describe an attack which permits to recover the corresponding plaintext from a given ciphertext. The same attack can be applied to produce forgeries if the cryptosystem is used for signing messages. Then, we point out that also other primitives, a Diffie-Hellman like key agreement scheme and an authentication scheme, designed along the same lines of the cryptosystem, are not secure due to the aforementioned attack. We close the paper by discussing the issues and the possibilities of constructing public key cryptosystems on real numbers.

Title: Analysis and Design of Distributed Key Distribution Centers.
Authors: Carlo Blundo and Paolo D’Arco.

Abstract: A Key Distribution Center of a network is a server who generates and distributes secret keys to groups of users for secure communication. A Distributed Key Distribution Center is a set of servers that jointly realizes a Key Distribution Center. In this paper we describe in terms of information theory a model for distributed key distribution centers, and we present lower bounds holding in the model for the main resources needed to set up and manage a distributed center, i.e., memory storage, randomness, and bandwidth. Then, we show that a previously proposed protocol
which uses a bidimensional extension of Shamir’s secret sharing scheme meets the bounds and it is, hence, optimal.

Title: Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures.
Authors: Carlo Blundo, Paolo D’Arco Vanesa Daza, and Carles Padró

Abstract: In this paper we investigate the issues concerning with the use of a single server across a network, the Key Distribution Center, to enable private communications within groups of users. After providing several motivations, showing the advantages related to the distribution of the task accomplished by this server, we describe a model for such a distribution, and present bounds on the amount of resources required in a real-world implementation: random bits, memory storage, and messages to be exchanged. Moreover, we introduce a linear algebraic approach to design optimal schemes distributing a Key Distribution Center and we point out that some previous constructions belong to the proposed framework.

Title: Design of Self-healing Key Distribution Schemes.
Authors: Carlo Blundo, Paolo D’Arco, Alfredo De Santis and Massimiliano Listo.

Abstract: A self-healing key distribution scheme enables dynamic groups of users of an unreliable network to establish group keys for secure communication. In such a scheme, a group manager, at the beginning of each session, in order to provide a key to each member of the group, sends packets over a broadcast channel. Every user, belonging to the group, computes the group key by using the packets and some private information. The group manager can start multiple sessions during a certain time-interval, by adding/removing users to/from the initial group. The main property of the scheme is that, if during a certain session some broadcasted packet gets lost, then users are still capable of recovering the group key for that session simply by using the packets they have received during a previous session and the packets they will receive at the beginning of a subsequent one, without requesting additional transmission from the group manager. Indeed, the only requirement that must be satisfied, in order for the user to recover the lost keys, is membership in the group both before and after the sessions in which the broadcast messages containing the keys are sent. This novel and appealing approach to key distribution is quite suitable in certain military applications and in several Internet-related settings, where high security requirements need to be satisfied. In this paper we continue the study of self-healing key distribution schemes, introduced by Staddon et al. We analyse some existing constructions: we show an attack that can be applied to one of these
constructions, in order to recover session keys, and two problems in another construction. Then, we present a new mechanism for implementing the self-healing approach, and we present an efficient construction which is optimal in terms of user memory storage. Finally, we extend the self-healing approach to key distribution, and we present a scheme which enables a user to recover from a single broadcast message all keys associated with sessions in which he is member of the communication group.

Title: Hyppocrates: A New Proactive Password Checker.
Authors: Carlo Blundo, Paolo D’Arco, Alfredo De Santis, and Clemente Galdi.

Abstract: In this paper we propose a new proactive password checker, a program which prevents the choice of easy-to-guess passwords. The checker uses a decision tree, constructed applying the Minimum Description Length Principle and a Pessimistic Pruning Technique. Experimental results show a substantial improvement in performances of this checker compared to previous proposals. Moreover, the whole software package we provide has a user-friendly interface, enabling the system administrator to configure an ad hoc password proactive checker, in order to satisfy certain policy requirements.

Title: The Key Establishment Problem
Authors: Carlo Blundo and Paolo D’Arco

Abstract: Key Establishment is one of the most intriguing, fascinating and deeply studied problems in Cryptography. In this paper we propose a brief excursus among ideas and techniques that during the last years have been applied in a variety of settings, in order to design suitable and often mathematically delightful protocols to solve this issue. The presentation uses a very simple language: it is basically an introduction to the subject. Hopefully, it is even self-contained. Formal proofs and details are omitted, but the interested reader can find them in the referred papers.

Title: Anonymous Group Communication for Mobile Networks.
Authors: Stelvio Cimato, Paolo D’Arco, and Ivan Visconti.

Abstract: In this paper we propose efficient schemes enabling groups of users of a mobile network to communicate anonymously with respect to an adversarial party (i.e., other users, network managers, and so on). Each user can start a group communication, and his identity, as well as the identities of the other members of the group, are not revealed even if several other parties of the system collude. We consider two network settings and, for each of them, we propose an efficient and secure scheme.
Title: Fault Tolerant and Distributed Broadcast Encryption.
Authors: Paolo D’Arco and Douglas Stinson.

Abstract: A broadcast encryption scheme enables a server to broadcast information in a secure way over an insecure channel to an arbitrary subset of privileged recipients. In a set-up phase, the server gives pre-defined keys to every user of the system, using secure point-to-point channels. Later on, it broadcasts an encrypted message along a broadcast channel, in such a way that only users in a privileged subset can decrypt it, by using the pre-defined keys received in set-up phase. Usually, the broadcast message contains a fresh session key, which can subsequently be used for secure broadcast transmission to the privileged set of recipients. In this paper we deal with two aspects of secure broadcast transmission: reliability and trust in the broadcaster. The first is a well-studied issue in communication over unreliable channels: packets can get lost and some redundancy is required to provide reliable communication. The second aspect concerns with the assumption that the broadcaster, who receives information for broadcasting from several entities, must be trusted. This issue has not previously been addressed in the broadcast transmission setting. We provide a motivating scenario in which the assumption does not hold and, for both problems, we review and extend some existing broadcast encryption schemes, in order to gain fault tolerance and to remove the need for trust in the broadcaster.

Title: A Ramp Model for Distributed Key Distribution Schemes.
Authors: Carlo Blundo, Paolo D’Arco, and Carles Padró

Abstract: A Key Distribution Center (KDC) of a network is a server enabling private communications within groups of users. The center provides the secret keys for encrypting and decrypting the messages. A Distributed Key Distribution Center (DKDC) is a set of servers that jointly realizes a Key Distribution Center. In this paper we introduce a ramp model for unconditionally secure Distributed Key Distribution Centers. In the ramp approach, the required resources (randomness, information storage, messages to be exchanged,...) can be reduced at the cost of a security degradation which depends on the size of the coalition of users who tries to break the scheme. We show lower bounds on the amount of information needed to setup and manage such a DKDC and describe a simple protocol meeting the bounds.

Title: Contrast Optimal Threshold Visual Cryptography Schemes.
Authors: Carlo Blundo, Paolo D’Arco, Alfredo De Santis, and Douglas R. Stinson.
Abstract: A $(k, n)$-threshold visual cryptography scheme (VCS) is a method to encode a secret image $SI$ into $n$ shadow images called shares such that any $k$ or more shares enable the “visual” recovery of the secret image. However, by inspecting less than $k$ shares one cannot gain any information on the secret image. The “visual” recovery consists of copying the shares onto transparencies and then stacking them. Any $k$ shares will reveal the secret image without any cryptographic computation. In this paper we analyze the contrast of the reconstructed image for a $(k, n)$-threshold VCS. We define a canonical form for a $(k, n)$-threshold VCS and provide a characterization of a $(k, n)$-threshold VCS. We completely characterize a contrast optimal $(n - 1, n)$-threshold VCS in canonical form. Moreover, for $n \geq 4$, we provide a contrast optimal $(3, n)$-threshold VCS in canonical form. We first describe a family of $(3, n)$-threshold VCS achieving various values of contrast and pixel expansion. Then we prove an upper bound on the contrast of any $(3, n)$-threshold VCS and show that a scheme in the described family has optimal contrast. Finally, for $k = 4, 5$ we present two schemes with contrast asymptotically equal to $1/64$ and $1/256$, respectively.

Title: On Unconditionally Secure Robust Distributed Key Distribution Centers.
Authors: Paolo D’Arco and Douglas Stinson.

Abstract: A Key Distribution Center enables secure communications among groups of users in a network by providing common keys that can be used with a symmetric encryption algorithm to encrypt and decrypt messages the users wish to send to each other. A Distributed Key Distribution Center is a set of servers of a network that jointly realize a Key Distribution Center. In this paper we propose an unconditionally secure scheme to set up a robust Distributed Key Distribution Center. Such a distributed center keeps working even if some minority of the servers malfunction or misbehave under the control of a mobile adversary. Our scheme for a distributed key distribution center is constructed using unconditionally secure proactive verifiable secret sharing schemes. We review the unconditionally secure verifiable secret sharing scheme described by Stinson and Wei, discuss a problem with the proactive version of that scheme, and present a modified version which is proactively secure.

Title: A t-Private k-Database Information Retrieval Scheme.
Authors: Carlo Blundo, Paolo D’Arco, and Alfredo De Santis.

Abstract: A private information retrieval scheme enables a user to privately recover an item from a public accessible database. In this paper we present a private information retrieval scheme for $k$ replicated databases. The scheme is information-theoretically secure against coalitions of databases of size $t \leq k - 1$. It improves the communication complexity of the scheme described in [Proc. of STOC99] for coalitions of size $\frac{k}{2} \leq t \leq k - 1$. 

13
Title: Paolo D’Arco and Douglas Stinson.  
Authors: Generalized Zig-zag Functions and Oblivious Transfer Reductions. 

Abstract: In this paper we show some efficient and unconditionally secure oblivious transfer reductions. Our main tool is a class of functions that generalizes the Zig-zag functions, introduced by Brassard, Crepéeau, and Sántha. We show necessary and sufficient conditions for the existence of such generalized functions, and some characterizations in terms of well known combinatorial structures. Moreover, we point out an interesting relation between these functions and ramp secret sharing schemes where each share is a single bit.

Title: Carlo Blundo, Paolo D’Arco, Antonio Giorgio Gaggia.  
Authors: A τ-restricted Key Agreement Scheme. 

Abstract: A one-restricted key agreement scheme is a method by which initially a trusted authority distributes private individual pieces of information to a set of users. Later, each member of any group of users of a given size, referred to as a conference, can compute a common key by exchanging messages over a broadcast channel all users have access to. Such schemes can be used to establish only one common key. In this paper we analyze τ-restricted key agreement schemes. Such schemes allow the computation of up to τ common keys for τ distinct conferences. For certain values of the parameters the scheme that we propose distributes less information than the trivial one obtained by considering τ copies of a one-restricted scheme.