Boolean Functions and Distance Bounding

Cédric Lauradoux

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Boolean Functions and Distance Bounding

Cédric Lauradoux

N° 7568

March 2011

Networks and Telecommunications

ISSN 0249-6399 ISRN INRIA/RR--7568--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
GRENOBLE - RHÔNE-ALPES

Boolean Functions and Distance Bounding

Cédric Lauradoux

Theme : Networks and Telecommunications
Networks, Systems and Services, Distributed Computing
Équipe-Projet SWING

Rapport de recherche n° 7568 — March 2011 — 10 pages

Abstract: Distance bounding protocols are a critical mechanism of wireless technologies such as RFID or ZigBee. They aim to enforce a stronger definition of authentication by preventing any kind of the relay attack, namely the distance fraud, the mafia fraud and the terrorist fraud. This paper aims to define the Boolean functions used in the distance bounding protocols based on the work of Hancke and Kuhn. Indeed, the choice of these functions has never been discussed despite the considerable literature. We define the criteria on the function needed to defeat each fraud.

Key-words: Distance bounding, man-in-the-middle, vectorial Boolean functions.

Centre de recherche INRIA Grenoble – Rhône-Alpes
655, avenue de l'Europe, 38334 Montbonnot Saint Ismier
Téléphone : +33 4 76 61 52 00 — Télécopie +33 4 76 61 52 52

Boolean Functions and Distance Bounding

Résumé : Les protocols de *distance bounding* sont très importants pour les technologies sans fil comme la RFID ou ZigBee. Ils permettent de réaliser une version forte de l'authentification résistant aux attaques par relais, plus exactement la fraude à la distance, la fraude mafieuse et la fraude terroriste. Ce rapport a pour objectif de définir les propriétés requises pour fonctions booléennes employées par ces protocols. En effet, le choix de ces fonctions n'a jamais été discuté malgré le nombre considérable de propositions pour le *distance bounding*. Nous définissons les critères requis pour contrer chaque type de fraude.

Mots-clés : Distance bounding, man-in-the-middle, fonctions Booléennes.

1 Introduction

Man in the middle attacks (MITM) are often reduced to a special case in the cryptographic literature. Indeed, it is always assumed that the adversary tampers with the execution of a cryptographic protocol. Desmedt *et al.* [1, 2] have shown that a MITM in which the adversary simply forwards the messages between two parties is sufficient to break the most advanced authentication protocols.

The first countermeasures to this class of MITM were given by Rivest and Shamir in "How to expose an eavesdropper" [3]. Early solutions were also devised by Desmedt *et al.* [1, 2] when the attacks first appeared but they cannot by applied in any context. Finally, distance bounding protocols were introduced by Brands and Chaum [4] as a solution for low-cost devices. Basically, a distance bounding protocol combines an authentication with the computation of an upper-bound on the distance between the two parties involved. This combination mitigates the possibility to mount relay attacks. The mechanism favored to measure the distance is the time of flight because it requires only one clock. More details and definitions can be found in [5].

The propositions of distance bounding protocol can be divided into two categories according to the need or not of a final signature to complete the authentication. This distinction between the protocols inspired by the results of Brands and Chaum [4] (presence of a signature) and those derived from Hancke and Kuhn [6] (no signature). This paper is dedicated to the latter categories, not meaning that our results do not apply to Brands and Chaum's protocol but rather to simplify the analysis. The core of any distance bounding protocols is an interactive phase in which Bob sends small challenges to Alice who answers shortly. The timing of each challenge/response is measured accurately to deduce an upper-bound on the distance. Each response is computed using a Boolean function f who takes as input, the challenge and some variables known only by Alice and Bob. At the end, Bob checks that each answer and its corresponding timing are consistent.

This work aims to understand how the response is computed and more precisely how the function f must be chosen to defeat the different frauds. The criteria to resist to the distance and mafia fraud are rather obvious for the readers familiar with Boolean functions. The main contribution of the paper is the criteria related to the terrorist fraud which capture nicely the problem we are facing. Our notations are compliant with the use of vectorial Boolean functions in the perspective of the development of the MIMO technology. Throughout the paper, the examples are given for Boolean functions for convenience.

The Section 2 contains the background related to vectorial Boolean functions. Our template protocol is described in Section 3. Section 4 deals with the distance fraud. Section 5 and Section 6 are respectively devoted to the mafia fraud and the terrorist fraud.

2 Notations

We denote by $\mathcal{B}_n^m$ the set of vectorial Boolean functions of n variables and m outputs such that n and m are two positive integers and $m \leq n$, $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

The truth table vector T_f of $f \in \mathcal{B}_n^m$ is written:

$$(f(\alpha_0), \cdots, f(\alpha_{2^n-1})),$$

where $\alpha_0, \cdots, \alpha_{2^n-1}$ are all the elements of $\mathbb{F}_2^n$ sorted by lexicographic order. The algebraic normal form (ANF) is also used to represent Boolean functions in a compressed notation. The Hamming weight $w_H(y)$ of binary vector $y = (y_0, \cdots, y_{m-1})$ of length m is the number of one in y: $\sum_{i=0}^{m-1} y_i$. The notation $y_i \in \mathbb{F}_2$ denotes the i-th coordinate of c

Definition 1 *Let U be a p-dimensional subspace of $\mathbb{F}_2^n$. The restriction of $f \in \mathcal{B}_n^m$ to U, denoted f_U is defined by $f_U(x) = f(x),\ \forall x \in U$.*

Throughout the paper, a element x belonging to $\mathbb{F}_2^n$ is decomposed as the vector $x = (c, s, k)$ with $c \in \mathbb{F}_2^{n_c}$, $s \in \mathbb{F}_2^{n_s}$, $k \in \mathbb{F}_2^{n_k}$ such that $n = n_1 + n_2 + n_3$. The restriction of f to the subspace U_c of dimension n_2+n_3 defined for $\forall c \in \mathbb{F}_2^{n_c}$ by:

$$U_c = \{(c, s, k) | c = cst,\ s \in \mathbb{F}_2^{n_s} \text{ and } k \in \mathbb{F}_2^{n_k}\},$$

is simply noted $f_c(x)$, $\forall x \in U_c$. Similarly, $f_{c,s}$ is the restriction of f to $U_{c,s}$, *i.e.* c and s are kept constant.

Definition 2 *A vectorial Boolean function f is said to be balanced if each elements of $\mathbb{F}_2^m$ appears 2^{n-m} times in the truth table vector T_f.*

The protocol considered between Alice and Bob is unilateral for its authentication part. Alice is a legitimate prover, Bob the verifier and Eve an adversary.

3 Template protocol

To support your hunt of the function f, we give a template distance bounding protocol. The protocol is depicted Fig. 1.

Prior to the execution of the protocol, Alice and Bob have agreed on a secret key K of $\ell \times n_c$ bits, on a vectorial Boolean function f and a pseudo-random function (PRF) g. The key is view has a vector $K = (k^0, k^1, \cdots, k^{\ell-1})$ with $k^j \in \mathbb{F}_2^{n_k}$, $\forall j \in [0, \ell-1]$. Then, our template protocol is composed of three steps.

1) Initialization – Alice and Bob exchange the nonces N_A and N_B. They use the function g to compute the a share internal state $S = (s^0, s^1, \cdots, s^{\ell-1})$, $s^j \in \mathbb{F}_2^{n_s}$, $\forall j \in [0, \ell-1]$. The state S can be the output of $g(K, N_A, N_B)$. It worth mentioning that the duration of the initialization phase is subject to important timing variations because the computational power of the prover can be limited and the computation of g can be time consuming.

2) Interactive phase – This phase consists in ℓ rounds. At each round, Bob picks randomly a challenge $c^j \in \mathbb{F}_2^{n_c}$ and sends it to Alice who receives $\hat{c}^j$. Alice computes:

$$r^j = f(\hat{c}^j, s^j, k^j). \tag{1}$$

This phase required a precise synchronization because Bob computes the time spent between the emission of the challenges c^j and the reception of the corresponding answer $\hat{r}^j$. This *Round Trip Time* (RTT) is denoted δ_j.

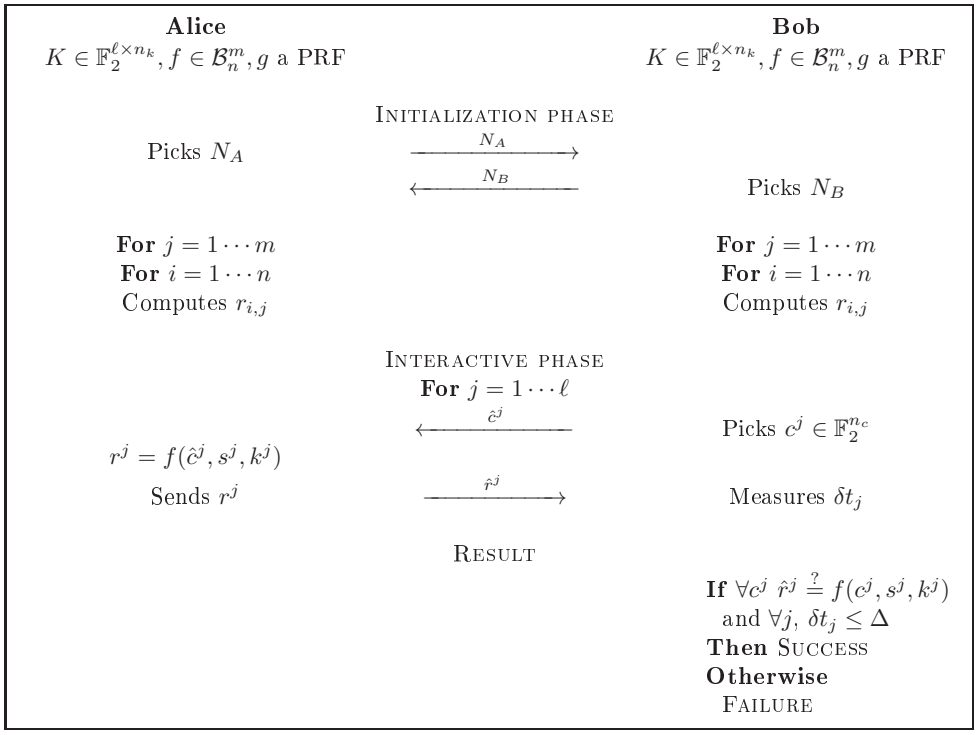

Figure 1: The template distance bounding protocol.

3) Result – Bob checks that each answer $\hat{r}_i$ received from Alice is correct, *i.e.* $\hat{r}^j = f(c^j, s^j, k^j)$ and that $\forall i, \ \delta_i \leq \Delta$ with Δ a given threshold. The time measuring method and the attacks related to this mechanism are not discussed in here. The precision of this measurement is critical with respect to the applications. The readers can consult the works [7, 8, 9] for more information on this subject.

The template protocol described in this section follows the principle defined by Hancke and Kuhn [6] except for two points.

Multi-channel communications – Alice and Bob are using MIMO radio systems over a half-duplex channel, *i.e.* they can transmit several bits simultaneously over different channels. It implies that $n_c > 1$ and $m > 1$. A similar hypothesis is made in [10] with MUSE-pHK in which symbols belonging to $\mathbb{F}_p$, $p > 2$ are transmitted by Alice and Bob. In the original works of Hancke and Kuhn [6], the values $n_c = 1$, $n = 3$ and $m = 1$ were considered for an usage in RFID. We also assume that the communications are noise-free.

Key insertion – The purpose of the protocol of Hancke and Kuhn [6] is to defeat the mafia fraud and the distance fraud. All the variables used as an input to the function f provided no information on the key ($n_k = 0$). it results that this protocol cannot defeat the terrorist fraud. As a consequence, the key shared by Alice and Bob must be directly used during the computation of f.

Bussard and Bagga [11] are to be credited for this idea. This particular problem is considered in Section 6.

In our protocol, all the rounds are independent. In what follows the round number j is often omitted for the variables c, s, k to simplify the notations.

Example 1 *The protocol proposed by Hancke and Kuhn [6] used the parameters* $n = 3, m = 1$, $n_k = 0$, $n_c = 1$ *and* $n_s = 2$. *The Boolean function* f *used is defined by:*

$$\forall c \in \mathbb{F}_2, s \in \mathbb{F}_2^2,\ f(c_0, s_0, s_1) = c_0 s_0 + c_0 s_1 + s_1.$$

We now consider how to the function f is chosen. Finding good vectorial Boolean function consists to find the appropriate restrictions of f that will capture a given attack.

4 Distance fraud

In a distance fraud, Alice attempts to lie on her distance to Bob. Such an attack is particularly critical for ankle monitor in criminal surveillance applications. The ankle monitor has to restrict the action of Alice. If she is not in the neighborhood of Bob and an alarm is triggered. If Alice can make believe Bob she is in the neighborhood while she is not: she can commit crimes.

To carry out a distance fraud, Alice can try to compensate the extra distance by answering Bob's challenges before they were sent. This strategy is known as the *early reply* in the literature. The ability of Alice to succeed the distance fraud depends on her capability to interact with the ankle monitor (the device used to execute the protocol). If the device is tampered resistant, then Alice is on her own. This is referred as the black-box model in the literature [5]. To defeat such an adversary, the function f must be chosen such that:

Property 1 *To defeat the distance fraud in the black-box model, the function* f *in the protocol* $\mathcal{P}$ *must be balanced.*

Any bias in the function provide an advantage to the adversary.

There is an way for Alice to succeed the early reply strategy. She can execute the interactive phase with our device prior to executing the interactive phase with Bob. She send $\hat{c} \in \mathbb{F}_2^{n_c}$ to the device and obtain $r = f(\hat{c}, s, k)$. This information can help Alice to choose an appropriate reply. This strategy is known as *pre-ask-then-early-reply*. If the function is not chosen properly and adversary can narrow down the possible answer and gain an advantage. The following property capture this strategy to model it into a criterion for f.

Property 2 *To maximize the resistance to the pre-ask-then-early-reply strategy in the black-box model, the function* f *must verified that:*

$$\forall c, s, k, \hat{c},\ f_U(c, s, k) \text{ is balanced with } U = \{(c, s, k) | f(\hat{c}, s, k) = r, \hat{c} = cst\}.$$

The other model for the relation between Alice and her device is known as the white-box. Alice can tamper with the execution of the algorithm to recover useful information. It means that Alice knows the internal value of the algorithm, *i.e.* s and k.

Property 3 *To maximize the resistance to the distance fraud in the white-box model, the function f must verified:*

$$\forall s, k,\ f_{s,k}(c, s, k) \text{ is balanced.}$$

Property 3 is the strongest one since we assume that Alice has accessed to the large amount of information.

Remark 1 *The reader familiar with the design of block-ciphers and especially s-boxes, may have remarked that we are not so far from the resiliency criterion (except for Property 2). Indeed, it applies on a subset of input variables of f not to all the variables. This makes the difference with resiliency.*

5 Mafia fraud

In the mafia fraud, an external adversary, Eve, is introduced and Alice is once again honest. To impersonate Alice and meet the timing constraints, Eve first relay the initialization phase. Then, she has two strategies, namely the *no-ask* strategy and the *pre-ask* strategy, to succeed the attack. In the no-ask strategy, Eve executes directly the interactive phase with Bob. She knows c which defines the appropriate restriction to work with.

Property 4 *To maximize the resistance to the no-ask strategy, the function f must verified:*

$$\forall c,\ f_c(c, s, k) \text{ is balanced.}$$

In the pre-ask strategy, Eve is allowed to execute the interactive phase with Alice prior to executing her own instance of the interactive phase with Bob. Eve sends $\hat{c}$ to Alice and obtain $r = f(\hat{c}, s, k)$. During the execution of the interactive phase with Bob, Eve receives c and attempts to answer. If $\hat{c} = c$, she replies r and wins the round. Otherwise, she is on her own if the function verifies the following property.

Property 5 *To maximize the resistance to the pre-ask strategy, the function f must verified:*

$$\forall c \neq \hat{c},\ I(f(c, s, k); f(\hat{c}, s, k)) = 0,$$

where I stands for the mutual information.

One may have noticed the fact that we never speak about the disclosure of the key during our analysis of the distance and mafia fraud. In fact, we can deal with these two frauds while considering $n_k = 0$. The problem of the key disclosure is related to the terrorist fraud.

6 Terrorist fraud

The terrorist fraud is a tricky business. The protocol designer has to deal with two adversaries. Indeed, Alice conspires with Eve to deceive Bob on the distance between them. Such a scenario occurs when Alice pays Eve for getting a perfect alibi to commit a crime. The terrorist fraud can be risky for Alice if Eve is able to (re)impersonate her afterward: Eve could commit crimes pretending

to be Alice. Hence, Alice agrees to carry out a terrorist fraud only if Eve is able to achieve a *one-time impersonation*. More precisely, we assume that Alice does not get involved in a terrorist fraud if Eve, by doing so, may gain some advantage for further attacks.

To prevent a malicious Alice from helping Eve, the secret key must be introduced as an input to f as an incentive not to cheat. Moreover, the secret of an honest Alice must not be exposed. The swiss knife to thwart this fraud is threshold cryptography.

Property 6 *To preven any key leakage during a terrorist fraud, the function f that $\forall c, s, k$:*

$$I(k; f(c,s,k)|c) = 0, \quad (2)$$
$$I(k; f(c,s,k)|c, \Phi_{\delta-1}(s)) = 0, \quad (3)$$
$$I(k; f(c,s,k)|c, \Phi_{\delta}(s)) = n_k, \quad (4)$$
$$I(k; f(c,s,k)|c, f(\hat{c},s,k)|\hat{c}) = 0, \quad (5)$$

where $\hat{c} \neq c$ and $\Phi_\delta(s)$ is any combination of δ coordinates of s.

Each equation of the previous property corresponds to a specific situation of our protocol. From this situation, Eve can extract some knowledge on the variables of the procotol.

EQUATION 2 – The first thing to check is if an eavesdropper can recover k from the challenge c and its corresponding answer $f(c, s, k)$.

EQUATION 3 and 4 – The concern of this equation is to determined how much information can be provided by Alice to Eve. Equation 3 and 4 describes a threshold scheme. Providing too much information to Eve must expose the key. The function f, k and the coordinates of s act as a system of shares in secret-sharing scheme.

EQUATION 5 – Eve can launch fault attack in order to recover the key. To mount this attack, she modifies the legitimate challenge c such that Alice receives $\hat{c}$ with $\hat{c} \neq c$. Alice sends $r = f(\hat{c}, s, k)$ to Bob. But Eve tampers with this answer and Bob received $\hat{r}$ chosen by Eve. If Eve knows if the result is correct or not, she knows $f(c, s, k)$, $f(\hat{c}, s, k)$ with $\hat{c} \neq c$. Then, she can try to recover k from this material. A variant of this attack was first presented in [12].

Example 2 *Let consider $f(c, s, k) = k_0 c_0 + s_0 + k_0$. This function has been proposed in the protocol of Reid et al. [13]. This function matches the criteria required for the mafia fraud. Let see if there are any information leakage on the key. It is easy to see that $I(k_0; f(c_0, s_0, k_0)|c_0) = 0$. Eve learns $s_0 + k_0$ if c_0 is equal to 0. Otherwise ($c_0 = 1$), Eve learns s_0. Equation 2 is verified. However, it also means that Equation 5 can not be satisfied. The fault attack provides to Eve e_0 ($f(1, s_0, k_0)$) and $s_0 + k_0$ ($f(0, s_0, k_0)$), so she can recover the key. Equation 3 and 4 are also not satisfied.*

7 Conclusion

Studying distance bounding protocols from the perspective of vectorial Boolean functions offers many new ideas apart from giving solutions to the terrorist fraud. In this paper, we consider that the function was fixed and known to the adversary. Following these hypothesis, we define the criteria on f. Protocols in which Alice and Bob agree on a random Boolean function at the beginning of the protocol may be valuable and interesting from a security point of view.

Changing the function f at each round could be also interesting but it should be done carefully since such a scheme may have a big impact on the accuracy of the timing procedure. A way to do so is to use a sequential circuit rather than a combinatorial circuit for the computation of the answers. By doing so, the function is virtually modified at each round without a significant impact on the timing accuracy. This approach was explored in [12, 14]. A theoretical comparison of these two strategies, combinatorial and sequential is yet to be done.

Acknowledgement

The author would like to thank all the members of the GSI group for the fruitful discussions on the many aspects of distance bounding protocols.

References

[1] Desmedt, Y., Goutier, C., Bengio, S.: Special Uses and Abuses of the Fiat-Shamir Passport Protocol. In: Advances in Cryptology – CRYPTO'87. Lecture Notes in Computer Science 293, Santa Barbara, CA, USA, Springer-Verlag (1988) 21–39

[2] Beth, T., Desmedt, Y.: Identification Tokens - or: Solving the Chess Grandmaster Problem. In: Advances in Cryptology – CRYPTO'90. Lecture Notes in Computer Science 537, Santa Barbara, CA, USA, Springer-Verlag (1990) 169–177

[3] Rivest, R.L., Shamir, A.: How to expose an eavesdropper. Communication of the ACM **27**(4) (1984) 393–394

[4] Brands, S., Chaum, D.: Distance-Bounding Protocols. In: Advances in Cryptology – EUROCRYPT'93. Lecture Notes in Computer Science 765, Lofthus, Norway, Springer-Verlag (1993) 344–359

[5] Avoine, G., Bingöl, M.A., Kardaş, S., Lauradoux, C., Martin, B.: A Framework for Analyzing RFID Distance Bounding Protocols. Journal of Computer Security – Special Issue on RFID System Security (2010) To appear.

[6] Hancke, G., Kuhn, M.: An RFID Distance Bounding Protocol. In: Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005, Athens, Greece, IEEE (2005)

[7] Hancke, G.P.: Practical Attacks on Proximity Identification Systems. In: IEEE Symposium on Security and Privacy - S&P 2006, Berkeley, California, USA, IEEE Computer Society (2006) 328–333

[8] Clulow, J., Hancke, G.P., Kuhn, M.G., Moore, T.: So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks. In: Security and Privacy in Ad-Hoc and Sensor Networks, Third European Workshop - ESAS 2006. Lecture Notes in Computer Science 4357, Hamburg, Germany, Springer Verlag (2006) 83–97

[9] Flury, M., Poturalski, M., Papadimitratos, P., Hubaux, J.P., LeBoudec, J.Y.: Effectiveness of Distance-Decreasing Attacks Against Impulse Radio Ranging. In: 3rd ACM Conference on Wireless Network Security - WiSec 2010, NJ, USA (2010)

[10] Avoine, G., Floerkemeier, C., Martin, B.: RFID Distance Bounding Multistate Enhancement. In: Proceedings of the 10th International Conference on Cryptology in India – Indocrypt 2009. Lecture Notes in Computer Science 5922, New Delhi, India, Springer-Verlag (2009) 290–307

[11] Bussard, L., Bagga, W.: Distance-bounding proof of knowledge to avoid real-time attacks. In Ryoichi, S., Sihan, Q., Eiji, O., eds.: Security and Privacy in the Age of Ubiquitous Computing. Volume 181 of IFIP International Federation for Information Processing., Chiba, Japan, Springer-Verlag (2005) 223–238

[12] Kim, C.H., Avoine, G., Koeune, F., Standaert, F.X., Pereira, O.: The Swiss-Knife RFID Distance Bounding Protocol. In: International Conference on Information Security and Cryptology – ICISC'08. Lecture Notes in Computer Science 5461, Seoul, Korea, Springer-Verlag (2008) 98–115

[13] Reid, J., Nieto, J.M.G., Tang, T., Senadji, B.: Detecting relay attacks with timing-based protocols. In: ACM symposium on Information, computer and communications security - ASIACCS '07, Singapore, ACM (2007) 204–213

[14] Kara, O., Kardaş, S., Bingöl, M.A., Avoine, G.: Optimal Security Limits of RFID Distance Bounding Protocols. In: Workshop on RFID Security – RFIDSec'10, Istanbul, Turkey (2010)

Centre de recherche INRIA Grenoble – Rhône-Alpes
655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399