Application

2015-03-31

2015-04628 **Thobaben, Ragnar** **NT-14**

Information about applicant

Name: Ragnar Thobaben

Doctorial degree: 2007-07-23

Birthdate: 19770707

Academic title: Docent

Gender: Male

Employer: Kungliga Tekniska högskolan

Administrating organisation: Kungliga Tekniska högskolan

Project site: Avdelningen för Kommunikationsteori

Information about application

Call name: Forskningsbidrag Stora utlysningen 2015 (Naturvetenskap och teknikvetenskap)

Type of grant: Projektbidrag

Focus: Fri

Subject area:

Project title (english): Sharing secrets

Project start: 2016-01-01

Project end: 2019-12-31

Review panel applied for: NT-14, NT-2, NT-13

Classification code: 20204. Telekommunikation, 20203. Kommunikationssystem

Keywords: Secure communication, Information theory, Coding theory

Funds applied for

Year:	2016	2017	2018	2019
Amount:	889,200	998,600	1,033,900	1,136,000

Descriptive data

Project info

Project title (Swedish)*

Att dela hemligheter

Project title (English)*

Sharing secrets

Abstract (English)*

The purpose of this project is to develop new fundamental secret sharing schemes and to study their applications to decentralized key distribution in wireless networks and authentication in biometric systems. We also provide new concepts for key generation from dynamic systems in networked control systems.

In our work, we consider four fundamental information theoretical models: the wiretap channel, the source model and the channel model for secret sharing, and the privacy amplification model. We employ recent results from coding theory to develop flexible secret sharing algorithms that show an asymptotically optimal performance, guarantee perfect security, enjoy a linear-time complexity, and are applicable to a wide range of application scenarios. We also use information theoretic bounds to determine factors that limit the finite-length performance of the studied key generation schemes. Furthermore, we develop a new model for secret key generation from dynamic systems, which enhances security in networked control systems. We extend our studies to this model and assess the performance of the developed theoretical concepts for realistic application scenarios like wireless key generation, biometric authentication, and networked control systems.

The research in this project is organized in three tasks. Task 1 is concerned with development and validation of novel coding solutions for secret sharing. Research in this task will be lead by one Ph.D. student (activity level 80%, newly recruited for the project) supported by a team of supervisors from the Communication Theory Department at KTH (including the applicant). Task 1 is subdivided into four subtasks: In Task 1.1 (Month 1-12) we focus on polar code designs. In Task 1.2 (Month 13-24), we explore the intersection between coding and computer science and construct invertible extractors from linear codes. In Task 1.3 (Month 25-48), we study solutions based on spatially coupled and protograph sparse-graph codes, whereas Task 1.4 (Month 13-48) is dedicated to the integration and validation of the provided solutions.

In Task 2 (Month 1-24), lead by the applicant (activity level 40%), we develop a new framework for secret key generation from dynamic systems. We start by transferring recent results on the secure degrees of freedom for wireless networks to the considered setup. One interesting aspect of this work is the utilization of helpers (e.g., jammers in a wireless context), which translate into additional actuators that perturb the plant in order to confuse the eavesdropper.

Task 3 (Month 25-48), also lead by the applicant, provides a theoretical finite block length analysis of the two main design concepts (separation versus joint design) and provides a comparison. We will use the frameworks developed by Polyanskiy, Kostina, and Verdu and their extensions. We will also use bounds derived by Hayashi to quantify the leakage in the non-asymptotic regime.

If successful, the project will have far-reaching impact: Theoretical concepts and feasible algorithms developed in this project will enable distributed, perfectly secure, and reliable key sharing for a large range of application scenarios like wireless networks, networked control systems, and biometric authentication systems. In this way, our results will contribute towards an improved security for such systems. Our contributions will also help to significantly reduce the security overhead since the framework provided in this project will allow us to replace complex asymmetric encryption (used, e.g., for authentication and privacy) by significantly less complex symmetric encryption schemes. This is especially relevant for securing machine-type communication or biometric systems, where devices are often limited in their computational capabilities. Finally, besides published research results, the main outcome of the project will be the graduation of one Ph.D. in the area of wireless communications and security.

Popular scientific description (Swedish)*

Säkerhet är en viktig egenskap för dagens och framtidens kommunikationssystem. För att garantera sekretess använder moderna kommunikationssystem sig av kryptering. Kryptering använder hemliga nycklar ("delade hemligheter") som bara är kända för sändaren och mottagaren. Men hur delar man hemligheter på ett säkert sätt? Och hur säkra är de befintliga krypteringsmetoderna?

Ur säkerhetssynpunkt lider moderna krypteringsmetoder av två svagheter:

(1) Kryptering utgår från att det finns ett säkert sätt att generera och fördela de hemliga nycklarna. Det innebär att ett kommunikationssystem är bara så säkert som sitt nyckelhanteringssystem. Det är ett problem i stora distribuerade system som t.ex. sensornätverk eller ad-hoc nätverk som kan sakna en permanent uppkoppling till en centraliserad infrastruktur samt till ett nyckelhanteringssystem. Under dessa förutsättningar är det svårt att upprätthålla säkerhet på lång sikt.

(2) Säkerhet i krypteringssystem som använder sig av ett så kallat par av offentliga och privata nycklar är baserad på matematiska problem som är svåra att lösa på begränsad tid. Det innebär att säkerheten är bara garanterad så länge det inte finns lösningar till det underliggande matematiska problemet. Så snart en lösning för problemet hittas upphör krypteringens säkerhet.

Syftet med det här projektet är att bidra med nya lösningar till en förbättrad säkerhet i moderna kommunikationssystem. Vi använder oss av koncept från informationsteori som garanterar båda ovillkorlig säkerhet och robusthet. Det vill säga, en utomstående som avlyssnar en pågående överföring kan inte dra några slutsatser om det överförda meddelandet medan den legitimerade mottagaren säkert och felfritt kan avkoda meddelandet.

De informationsteoretiska koncept som projektet bygger på är kända sedan länge. Men ändå finns det inga lösningar som kan uppnå den optimala prestandan under de högsta säkerhetskraven och som samtidigt är implementerbara i praktiska system. Nya resultat inom kodningsteorin visar att kodning är ett mäktigt verktyg som kan bidra till problemets lösning. Projektets mål är därför att utveckla nya kommunikationsalgoritmer som använder sig av kodningsteoretiska resultat för att garantera att information kan överföras säkert och robust. Våra lösningar kommer att prestera nära de teoretiska gränserna och de kommer att vara implementerbara i praktiska system. Kommunikationsalgoritmerna som utvecklas i det här projektet kommer vara viktiga ingredienser till nya nyckelhanteringssystem som signifikant ökar säkerheten t.ex. i distribuerade system.

Project period

Number of project years*

4

Calculated project time*

2016-01-01 - 2019-12-31

Classifications

Select a minimum of one and a maximum of three SCB-codes in order of priority.

Select the SCB-code in three levels and then click the lower plus-button to save your selection.

SCB-codes*	2. Teknik > 202. Elektroteknik och elektronik > 20204. Telekommunikation 2. Teknik > 202. Elektroteknik och elektronik > 20203. Kommunikationssystem

Enter a minimum of three, and up to five, short keywords that describe your project.

Keyword 1*

Secure communication

Keyword 2*

Information theory

Keyword 3*

Coding theory

Keyword 4

Keyword 5

Ethical considerations

Specify any ethical issues that the project (or equivalent) raises, and describe how they will be addressed in your research. Also indicate the specific considerations that might be relevant to your application.

Reporting of ethical considerations*

Inga etiska frågor är aktuella.

The project includes handling of personal data

No

The project includes animal experiments

No

Account of experiments on humans

No

Research plan

1 Purpose and Aims

The purpose of this project is to develop new fundamental secret sharing schemes and to study their applications in the context of decentralized key distribution in wireless networks and authentication in biometric systems. We also provide new concepts for key generation in networked control systems. Our solutions are derived from fundamental information theoretic models using modern coding techniques, enjoy linear-time complexity, and provide perfect (strong) secrecy.

Security features in current communication systems and biometric systems are based on symmetric and asymmetric encryption. Asymmetric schemes employ pairs of private secret keys and shared public keys. Asymmetric encryption is attractive since it enables flexible system designs. However, it is computationally demanding (e.g., the complexity of the RSA crypto system grows cubically with the number of encrypted bits). This leads to a severe security overhead, which is undesirable in general, and in particular, in applications like machine-type communication or biometric systems where often low-complexity battery-driven devices are employed. Symmetric schemes on the other hand are based on pre-shared secret keys. They are significantly less complex compared to asymmetric schemes (by a factor of 100-1000). However, the employed pre-shared keys need to be updated regularly, and a dedicated key distribution infrastructure is required. This is a major drawback: if the key distribution infrastructure is compromised, the updated keys will be compromised as well.

Secret sharing techniques provided in this project allow us to overcome the drawbacks mentioned above. First, our solutions help to solve the key distribution problem: Whenever communication partners have access to a common source of randomness (e.g., the wireless channel, biometric features, observations of a physical system) and the legitimate system has an advantage over the eavesdropper, perfectly secure secret sharing is possible. Secondly, if the perfectly secure shared secret is used for symmetric encryption, asymmetric encryption can be replaced by symmetric encryption, and the security overhead is significantly reduced thanks to the linear-time complexity of our solutions and the low complexity of symmetric cryptosystems.

In our work, we consider four fundamental models that have been studied in the information theory literature: the wiretap channel model, the source model and the channel model for secret sharing, and the privacy amplification model. The models are illustrated in Figure 1 and consider different scenarios in which two terminals, Alice and Bob, try to exchange a secret while keeping the eavesdropper, Eve, perfectly ignorant. The wiretap channel model in (a) considers communication over a broadcast channel where Eve overhears the transmission from Alice to Bob. The channel model for secret sharing in (b) extends the wiretap channel model by a public discussion channel. In the source model for secret sharing (c), Alice, Bob, and Eve each observe samples of three correlated sources. The shared randomness is exploited to agree on a shared secret by using public discussion. Finally, the privacy amplification model is similar to the source model except that Alice and Bob observe identical source samples. For each model, the goal is to maximize the number of securely communicated bits. If successful,

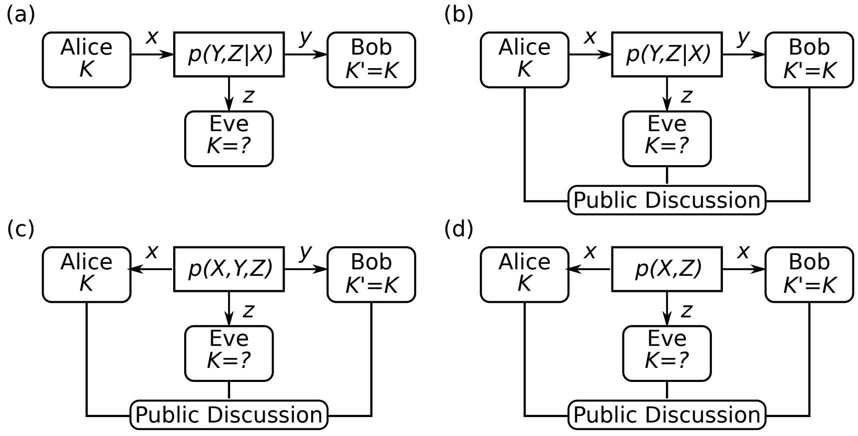

Figure 1: Wiretap channel (a), channel model for secret sharing (b), source model for secret sharing (c), and privacy amplification (d).

the shared secret can be used for symmetric secret key encryption or for authentication.

The considered models are selected to cover a wide range of application scenarios: The wiretap channel model in (a) is well suited to design secure forward communication strategies in wireless networks where the eavesdropper is part of the network. Similarly, the channel model for secret sharing in (b) is a powerful model for wireless secret key agreement and authentication. It is also applicable to other scenarios like networked control systems. For example, let the conditional probability mass function $p(Y, Z|X)$ describe Bob's and Eve's observations Y and Z, respectively, of the response of a dynamic system to a given (random) excitation X. Then, key generation in networked control systems is possible by utilizing the plant as a source of randomness that is hardly observable by an external attacker. To the best of our knowledge, this idea has not been studied elsewhere before. The source model in (c) can be employed for secret sharing over wireless channels by exploiting the reciprocity of the channel. In this case, noisy estimates of the channel response are used as correlated random sources. The source model can also be used to describe authentication in biometric systems. Here, the source X corresponds to a feature vector that is generated during the enrolment process (e.g., a finger print or an iris scan) and Y corresponds to a sample that is submitted for authentication. Access is granted if a secret key derived from X can be reconstructed from Y by using a public message. In this model, Eve's observation may correspond, e.g., to a correlated sample obtained from a relative. Finally, the privacy amplification model in (d) has lead to a powerful result that can be applied to all the previous scenarios to strengthen the results of any of the other models and to convert weakly secure communication strategies into strongly secure strategies.

Good progress has been made in developing optimal coding schemes for implementing the best known communication strategies for the four models. Mainly two approaches for achieving strong secrecy are known: schemes that treat security and reliability jointly through appropriate code design, and designs that separate reliability and security by employing coding to establish reliability and randomness extractors to achieve secrecy. However, existing coding solutions lack flexibility, which limits their applicability in practical scenarios, and require a secret random seed, which is asymptotically negligible but will reduce the effectiveness in a finite-length regime. Furthermore, the benefits and drawbacks of the two solution concepts in the finite block length regime are not well understood. It is therefore important to identify the limiting factors under finite-length constraints for both approaches in order to be able to decide in which scenarios separation and in which scenarios joint designs are beneficial.

To reach the purpose of this project (i.e., to provide new secret sharing mechanisms that are applicable to the considered scenarios described above), the aims of this proposal are to:

1. Develop flexible coding techniques with an asymptotically optimal performance that are applicable in a wide range of practical scenarios like wireless key generation, key generation in networked control systems, and biometric authentication;
2. Determine factors that limit the finite-length performance of key generation schemes and identify regimes in which separation based designs are optimal, and regimes in which joint designs are optimal;
3. Develop validation frameworks for assessing the performance of the developed theoretical concepts in realistic application scenarios like wireless key generation, key generation in networked control systems (*keys from dynamic systems*), and biometric authentication.

In doing this, this project will generate new theoretical concepts as well as novel feasible algorithms with excellent performance in practical applications. Compared to the state-of-the-art, our solutions will lead to an improved system security with a significantly reduced security overhead: Our solutions allow us to replace computationally demanding asymmetric encryption schemes with low-weight symmetric encryption that employs secret keys provided by our *decentralized* key sharing framework.

2 Survey of the Field

Communication algorithms and coding schemes developed in this project are based on fundamental information theoretic models and strategies. In the following, we summarize the most important theoretical results and give an overview over code design methods. Open issues are summarized in Section 2.3. A summary of own research results is provided in Section 2.4.

2.1 Information Theoretic Models and Tools

The four models that we introduced in Section 1 build the theoretical foundation of our work in this project. Here, we provide a short summary of directions in research that have emerged from these fundamental models. The summarized contributions provide inner and outer bounds on the achievable secrecy rate, i.e., the rate at which reliable and secure communication is possible. The inner bounds are of special interest for this project as they provide solution concepts that define the first step in the design of feasible communication algorithms.

Wiretap Channel The wiretap channel model (see Figure 1(a)) was introduced by Wyner in [1]. Wyner showed for the special case where the eavesdropper's channel (i.e., the channel between Alice and Eve in Figure 1(a)) is a degraded version of the main channel between Alice and Bob, that the secrecy capacity under weak secrecy constraint is strictly positive[1]. It can be achieved using a randomized coding scheme that is based on capacity-achieving codes. This result was generalized by Csiszár and Körner in [2], who showed that a positive secrecy capacity is obtained even if the eavedropper's channel is not degraded as long as the main channel is "less noisy" than the eavesdropper's channel. Wyner's and Csiszár and Körner's works have been extended in numerous ways[2]. Studies have considered, e.g., extensions to wireless channel models and multi-user scenarios.

Source and Channel Model for Secret Sharing Initial results on secret sharing were independently developed in [3] and [4]. Both contributions studied two different models of secret sharing: a channel model and a source model (see Figures 1(b) and (c)). Both papers [3, 4] provide inner and outer bounds on the secret key capacities of the models. In some special cases, the secret key capacity has been found. Different extensions of the source and the channel model for secret key sharing have been considered. For example, Khisti studied secret key rates for an extended model that combines the source and the channel model [5]. Secret key generation over rate-limited public channels is investigated in [6].

Privacy Amplification and Separation of Reliability and Secrecy The main point of criticism regarding information theoretic security is the fact that most works only provide weak secrecy such that asymptotically still an infinite amount of information may leak to the eavesdropper. However, as shown in [7], privacy amplification can be employed to convert a weakly secure communication scheme into a strongly secure scheme[3]. Here, strong secrecy is obtained if so-called extractors and universal-2 functions are employed. This result has an important implication on the design of secure communication algorithms: Reliability and secrecy can be treated separately. That is, in a first step, coding is applied to satisfy reliability requirements (reconciliation), and randomness extractors are used to establish secrecy (privacy amplification). The separation for key generation has recently been studied by Bloch in [8]. The result is that even though secrecy and reliability can be treated in two separate steps, both steps need to be matched with each other.

Strong Secrecy from Resolvability In [9], Bloch and Laneman show that wiretap codes that are based on capacity-achieving random codes are incapable of providing strong secrecy. As an alternative solution, Bloch and Laneman propose to construct communication strategies for strong secrecy by utilizing channel resolvability [10], which is defined as the lowest resolution rate of an input distribution of a channel that is required to closely approximate the output distribution that is induced by any other input distribution. The approach in [9] is to set up a coding scheme that controls the distribution at the output of the eavesdroppers's channel such that it is indistinguishable for different message realizations and hence conditionally indepen-

[1] We say that a communication scheme is weakly secure if the information leakage measured in terms of the information rate observed by an eavesdropper tends to zero asymptotically.

[2] According to the IEEE Explore database, the paper [2] has been cited more than 723 times.

[3] A communication scheme is strongly secure if the absolute mutual information or the variational distance observed by an eavesdropper tends to zero asymptotically.

dent of the transmitted message. It is interesting to note that the polar code construction [11] achieves strong secrecy in a similar way.

Performance Under Finite Length Constraints The majority of the contributions summarized so far provide asymptotic results that hold in the limit of infinite block length, and only little attention is paid to the finite block length regime. While in the asymptotic case the error probability and the leakage to the eavesdropper can be made arbitrarily small, the finite-length performance is characterized by a residual error probability and a residual information leakage. Both are functions of the block length. In this setup, the maximal coding rate that is achievable for a fixed block length, fixed error probability, and a fixed amount of leaked information becomes the fundamental limit of the channel under the given constraints. For transmission over point-to-point channels (without secrecy), the maximal finite block length coding rate $R^*(\epsilon, n)$, for a fixed error probability ϵ and block length n, has been studied by Polyanskiy and Verdu in [12]. The authors provide new inner and outer bounds leading to a tight approximation of the maximum rate $R^*(\epsilon, n)$. A similar framework has been derived by Kostina and Verdu in [13] to characterize the finite length rate-distortion function for the noisy source coding problem. In another line of work considering the non-asymptotic regime, Hayashi has provided bounds on the information leakage for the wiretap channel and for privacy amplification.

Applications The considered information theoretic models have mainly been discussed in a wireless communications context. However, also biometric authentication systems can be studied in a secret sharing framework. For example, key rates under realistic conditions have been studied in [14] considering ultra wideband systems, and the connection between biometric authentication systems and secret sharing has been discussed in [15] and references therein.

2.2 Coding for Wiretap Channels and Secret Sharing

Mainly two families of linear codes have been considered to implement the different secret sharing concepts: low-density parity-check (LDPC) codes [16] and polar codes [17].

Wiretap Codes Initial work by Thangaraj in [18] studied the design of irregular LDPC codes for the wiretap channel under the weak secrecy condition. Irregular low-density generator-matrix (LDGM) codes that achieve strong secrecy have been presented in [19]. Here, the authors connect the absolute information leakage to the error probability of the dual code under message-passing decoding and show that strong secrecy is obtained if the error probability decays faster than linear with increasing block length. A design of large-girth codes that satisfy this requirement is presented. Unfortunately, the design is not applicable to capacity achieving irregular codes. That is, the code design in [19] provides strong secrecy but it fails to achieve the secrecy capacity. It is interesting to note that nested LDPC code designs by the applicant (e.g., [RT4][4]) are also applicable to the wiretap channel. However, only weak secrecy would be achieved without further modifications.

The design of polar codes for degraded wiretap channels has been addressed in, e.g., [RT8] and [11, 20]. The code designs make use of a special property of the channel transformation that is used by the polar codes. For degraded channels, the sets of the so-called bad channels are nested such that secrecy can be obtained by transmitting information only through the bit channels that are simultaneously good for Bob and bad for Eve. In [11], this approach has been developed further to achieve strong secrecy. Unfortunately, for the construction in [11], reliability is only proven for error-free main channels. A workaround to resolve this issue has recently been presented in [21]. If a transmission is carried out over multiple blocks, every packet can provide a small fraction of additional frozen bits that are used for decoding the next packet. This requires however a small seed of secret bits that are shared among Alice and Bob. Then, if the number of packets becomes large, this scheme approaches the secrecy capacity.

Codes for Secret Sharing Coding solutions based on LDPC codes have been presented, e.g., in [22, 23, 24]. [22, 24] consider the channel model for secret sharing, and [23] considers the source model. All schemes implement the required distributed lossy source coding by

[4] References that are marked with ”RT” refer to publications listed in the publication list in Appendix C.

concatenating scalar quantizers with Slepian-Wolf coding. This becomes a limitation if rate constraints on the public discussion channel reduce the key rate, and none of the proposed schemes will be able to reach the optimal key rates. While [22, 23] apply a sequential design, [24] presents a joint approach to establish reliability and secrecy. Again optimal LDPC code designs by the applicant ([RT4, RT7]) are directly applicable under the assumptions of the papers [22, 23, 24] and allow for reaching the optimal performance under the given assumptions. However, to reach the optimal performance bounds, the overall design strategy from [22, 23, 24] needs to be changed. Task 1.3 in the work description is partly dedicated to address this.

Polar code designs for key agreement have been presented in [20, 25, 26]. Here, [20] provides a joint design which however only achieves weak secrecy. Strong secrecy is achieved in [25] and [26], where the authors in [25] apply a sequential design strategy (reconciliation and privacy amplification) while [26] addresses reliability and secrecy jointly. We note that polar code designs by the applicant presented in [RT6] are also applicable for secret sharing. However, similar to [20], only weak secrecy would be guaranteed.

Intersection of Coding and Cryptography Randomness extractors that are employed for privacy amplification are a cryptographic tool while code designs have their roots in communication engineering. Interestingly, there is a clear intersection between the two: As shown in [27], extractors can be constructed from polar codes, and in fact, the separate polar code design in [25] uses polar codes for privacy amplification. Furthermore, [28] identifies Reed-Solomon codes as suitable extractors for bit fixing sources.

2.3 Summary of Open Issues

Based on the survey above, we identify the following shortcomings of existing solutions:

1. Achieving the highest possible rate over the wiretap channel under the strong secrecy constraint with LDPC/LDGM codes remains an open issue. Furthermore, available LDPC/LDGM code designs for secret sharing are strictly suboptimal regardless whether weak or strong secrecy is considered.
2. Optimal code designs based on polar codes only provide a good performance for extremely large block lengths. This makes this class of coding schemes inflexible in practical applications like biometric systems, where rather short block lengths are required.
3. Strongly secure polar code designs require a perfectly secure random seed to be shared among Alice and Bob. The seed rate is asymptotically negligible; however, it reduces the effectiveness of the methods in a finite-length regime.
4. It is unclear which design approach (separation of reliability and security versus joint design) is beneficial under finite-length constraints. From other communication problems (e.g., separation of source and channel coding), it is known that sequential finite-length designs are prone to error propagation while joint designs are more robust. It is hence important to identify the factors that limit the performance of both strategies under finite-length constraints in order to be able to develop optimal practical secret sharing schemes.

2.4 Own Research

Some connections to previous research by the applicant have already been pointed out in the previous section. A more complete overview is given in the following. Previous research by the applicant was dedicated to joint source-channel coding, cooperative communications, information theoretic and physical layer security, and adaptive coding in wireless networks. Here, we provide a summary of relevant results on the design of coding schemes for cooperative communication schemes and adaptive codes. Preliminary results on information theoretic and physical layer security are summarized in Section 5.

Cooperative Communications and Relaying Our work has focused on the three-node relay channel. We have proposed distributed code designs for decode-and-forward relaying based on nested LDPC convolutional codes which achieve the best known rates for this model [RT4, RT25, RT32]. Nested polar codes achieving the capacity of the degraded decode-and-forward relay channel have been presented in [RT6]. In [RT35, RT42], we have developed transmission strategies for compress-and-forward relaying using joint source-channel coding ideas (see, e.g., [RT9, RT52]). Polar code constructions which achieve the highest possible rate under compress-and-forward relaying have been presented in [RT6, RT37].

Adaptive Coding In [RT7] we have developed a new family of rate-compatible LDPC convolutional codes with remarkable properties: All codes in the rate-compatible family are capacity achieving over the binary erasure channel, and the codes can be designed to realize any rational rate $R \in (0, 1)$. The good performance of the codes has been demonstrated in an ARQ framework [RT31] and a dynamic decode-and-forward setup [RT25].

3 Project Description

Overview The project is led by the applicant, and it is hosted by the Communication Theory Department, School of Electrical Engineering (EES), KTH, in Stockholm. The duration of the project is four years. Research in this project is performed by one Ph.D. student (activity level 80%), newly recruited for this project, and the applicant (activity level 40%). The applicant serves as main supervisor of the Ph.D. student. The project also involves Mikael Skoglund, Prof. in Communication Theory, EES, KTH as co-supervisor (not paid by the project), who brings in his expertise in information theory and security. The applicant has project management experience from EU/FP7 projects and has completed training worth 18 credit units in research supervision and teaching and learning in higher education.

Objectives To reach the goals stated in Section 1, we define the following objectives:

1. Provide new LDPC/LDGM code designs for the wiretap channel as well as the secret sharing models that closely approach the fundamental limits under *strong* secrecy;
2. Provide new polar code designs for the wiretap channel as well as the secret sharing models that closely approach the fundamental limits under *strong* secrecy, *without* requiring a pre-shared secret random seed;
3. For secure communication schemes that are based on the separation principle as well as for communication schemes that employ a joint design to achieve reliability and security, identify the factors that limit the finite-length performance;
4. Provide a novel framework for secret key generation from dynamic systems;
5. Validate the results of this project in context of relevant application scenarios.

A central objective of this project is to achieve strong secrecy. Even though strong secrecy is an asymptotic measure, it is also relevant in practice: Strongly secure code designs will outperform weakly secure designs due to code properties that are exploited for achieving strong secrecy. The resulting codes will be more reliable. Furthermore, strong secrecy is a standard requirement in cryptography: Results generated by this project will not be picked up by other research communities unless strong secrecy can asymptotically be shown.

Project Organization The research in this project is organized in three tasks: Task 1 is concerned with development and validation of novel coding solutions for secret sharing that allow us to overcome the shortcomings of existing approaches (see Section 2.3). Research in this task will be lead by the Ph.D. student supported by the team of supervisors. In Task 2, lead by the applicant, we develop a new framework for secret key generation from dynamic systems. This task will provide input to the validation framework used in Task 1. Task 3, also lead by the applicant, provides a theoretical finite block length analysis of the two main design concepts (separation versus joint design) and provides a comparison. The timing of the tasks is indicated in the following where we use the notation "M7" to refer to Month 7 of the project.

Task 1: Coding for Secrecy (M1-M48)

This task is divided into four sub tasks dealing with polar code designs (Task 1.1), constructions of randomness extractors from codes (Task 1.2), and LDPC code designs (Task 1.3). Task 1.4 foresees integration and validation of the developed techniques in relevant application scenarios. Task 1.1 is designed to let the involved student acquire the required background in coding and information theory while producing significant results at the same time. The results from Task 1.1 and Task 1.2 are expected to be summarized in the student's licentiate thesis.

Task 1.1: Polar Codes (M1-M12) In this task, our goal is to develop novel polar code designs that simultaneously guarantee strong secrecy and reliability at rates approaching the theoretical limits of the wiretap channel and the secret sharing models. In particular, we aim at overcoming the shortcomings of existing solutions: The work in [11] has already shown that by redefining the set of bad bit channels for the eavesdropper, strong secrecy is achieved; however, [11] fails to provably establish reliability. In [21, 26], this problem has been resolved by using a secret random seed and coding over multiple blocks. However, this solution is not applicable to, e.g., biometric authentication systems or communication systems with sporadic communication (e.g., sensor networks). In these scenarios, one-shot security is desired. In this task, we propose a new approach to achieve strong secrecy: We will utilize an additional design parameter of polar codes, the kernel of the generator matrix. As shown in [29], higher-dimensional kernels lead to improved rates of polarization such that the set of critical bit channels is reduced and reliability is improved. This is an approach that has not been applied to strengthen security before. We will furthermore reinvestigate the definitions of good and bad sets of bit channels for the eavesdropper and the designated receiver. We will develop this approach first for the wiretap channel model and then extend it to the lossy source coding problem that underlies the secret sharing problem when rate-limited public communication reduces the key rate. In this task, we will benefit from our experience in the design of polar codes for wiretap channels [RT8], relay channels [RT6, RT37], and coordination [RT29].

Task 1.2: Invertible Extractors from Codes (M13-M24) As pointed out in Section 2.2, extractors can be constructed from linear codes. The goal of this task is to explore this intersection of cryptography and communication engineering. In particular, we will construct invertible extractors from channel codes. Invertible extractors are of practical interest since they allow us to implement secure communication schemes with forward communication based on the separation principle. In brief, the inverse extractor[5] is used at the transmitter to generate a pseudo-random bit sequence that is transmitted over the channel by using standard capacity achieving code. After decoding, the receiver recovers the bit sequence and reconstructs the message by applying the extractor. In our design, we will make use of the fact that Reed-Solomon codes, which have been identified in [28] to be suitable extractors, are cyclic codes for which recursive encoders can be constructed from the parity check matrix. In a second step, we study the interrelation of the channel codes and the extractor and evaluate under which conditions strong secrecy is achieved. A first approach is to model decoding errors at the eavesdropper as realizations of a bit-fixing source which can then be characterized by the input-output weight-enumerating function of the employed code. In this way, we can connect the achievable key rate with properties of the employed channel code.

Task 1.3: Sparse-Graph Codes (M25-M48) Our goal is to develop novel LDPC and LDGM code designs that guarantee strong secrecy at rates close to the theoretic limits and to assess their performance for several wiretap channel and secret key sharing models. We take the result from [19] as a starting point and extend it to LDPC/LDGM code designs based on protographs like, e.g., repeat-accumulate and accumulate-repeat-accumulate codes (e.g., [30]), protograph-based LDPC convolutional codes (e.g., [31]), and spatially coupled LDPC codes [32]. Due to the properties of the considered codes (e.g., linear growth of the minimum distance, capacity achieving/approaching performance without requiring degree-2 variable nodes) we expect to be able to overcome the main weakness of [19], which is not applicable to capacity achieving sequences of irregular LDPC codes, and to provide new code constructions that provide strong secrecy for transmission over the wiretap channel at rates that closely approach the secrecy capacity. Here, we benefit from our previous results on the design of optimal structured LDPC convolutional codes in [RT4, RT7, RT18, RT25, RT31]. In a second step, we will extend our studies to secret sharing models with a special focus on rate constraints on the public discussion channel. This constraint is important, e.g., for the design of biometric systems since here the

[5] Note that the inverse extractor is not a unique function; it is a randomized function that selects bit sequences from the pre-image of the extractor uniformly at random.

public message corresponds to the credentials that are stored in the user data base. Under this model, the developed codes are used for lossy source coding employing belief-propagation guided decimation (BPGD) for encoding. BPGD encoding is in general difficult to analyze due to the decimation of the Tanner graph. However, good progress has recently been made in [33], where the authors show that spatially coupled LDGM ensembles achieve the rate-distortion bound. Here, we will extend the tools from [33] to nested code structures and study the performance of spatially coupled LDGM ensembles for secret-key generation.

Task 1.4: Integration and Validation (M13-M48) The goal of this task is to integrate the developed coding solutions provided by Task 1 into relevant application frameworks like, e.g., key generation in wireless networks, biometric authentication systems, and key generation schemes for networked control systems that are developed in Task 2, and to evaluate the performance of the developed algorithms under realistic constraints. The results in this task will be based on computer simulations and will hence complement the studies carried out in Task 3 where the finite-length performance is evaluated by means of theoretical tools. In the simulations we will mainly focus on code constructions that are known to perform well for short block length (e.g., protograph codes proposed in [30], non-binary polar code designs).

Task 2: Secret Keys from Dynamic Systems (M1-M24)

We consider a control system where sensors, actuators, and controllers are connected through a communication network. We assume that parts of the system like remote sensors are connected through a wireless network and difficult to access. In order to ensure system security (privacy and authenticity), symmetric key encryption is used due to limited capabilities of the devices. Our goal in this task is to develop a key generation protocol that employs the plant as source of randomness for key generation. We take a linear dynamic system as starting point for our study and develop a secret sharing protocol based on the channel model, where the excitation of the plant is interpreted as the channel input, the plant as the communication channel, and observations at the sensors as the channel output. Under this model and under the assumption that an external attacker has a degraded observation of the system state compared to the legitimate sensors, a secret key can be constructed. For example, if the system can be excited and observed (by the legitimate sensors) in the null space of the observations of the attacker, strongly secure keys can be generated since the output distribution observed by the eavesdropper is independent of the excitation. This strategy can be interpreted as constructing a resolvability code for the model of the dynamic system, and it has its origin in the multiple-antenna wiretap channel literature (see, e.g., [34]). In this task, we will develop the information theoretical framework for analyzing key sharing in this model and derive bounds on the achievable key rates under relevant constraints (e.g., stability, loss of utility during key generation, energy consumption). We start by transferring recent results on the secure degrees of freedom for wireless networks (see, e.g., [35]) to the considered setup. One interesting aspect of this work is the utilization of helpers (e.g., jammers in a wireless context), which translate into additional actuators that perturb the plant in order to increase the secrecy rate by additionally confusing the eavesdropper. The developed framework will later be used in Task 1.4 to assess the performance of the developed coding schemes.

Task 3: Finite-Length Performance (M25-M48)

The goal of this task is to identify the factors that limit the finite-length performance of secure communication schemes that are based on the separation principle as well as for communication schemes that employ a joint design to achieve reliability and security. We are interested in the question whether the performance of a sequential design suffers from error propagation due to concatenation of codes and extractors. In a first step, we analyze the sensitivity of source coding and decoding techniques, channel coding and decoding techniques, and extractors to fluctuations of the input distributions in order to quantify the impact of variations in the source distributions and variations of the channel for finite block length. By combining these results we will be able to give bounds on the performance of secure communication systems that employ a joint design or follow the separation principle. In our work we will use the frameworks developed by Polyanskiy, Kostina, and Verdu in [12, 13] and their extensions (e.g, [36]). We will also use bounds derived by Hayashi to quantify the leakage in the non-asymptotic regime.

Dissemination and Open Access Our results will be disseminated via papers in high-quality international (IEEE) conferences and journals. All publications will be published with open access. Both the lively exchange between the Communication Theory Lab and Ericsson Research in Stockholm and workshops organized by the ACCESS VR Linnaeus Centre will guarantee that results and ideas of this project will be presented to relevant Swedish industries.

4 Significance

If successful, the project will have far-reaching impact: Theoretical concepts and feasible algorithms developed in this project will enable distributed, perfectly secure, and reliable key sharing for a large range of application scenarios like wireless networks, networked control systems, and biometric authentication systems. In this way, our results will contribute towards an improved security for such systems. Our contributions will also help to significantly reduce the security overhead since the framework provided in this project will allow us to replace complex asymmetric encryption (used, e.g., for authentication and privacy) by significantly less complex symmetric encryption schemes. This is especially relevant for securing machine-type communication, where nodes are often limited in their computational capabilities. By addressing the open issues that were pointed out in this proposal, we expect furthermore to make significant contributions to open problems in theoretical research on information and coding theory and security. Finally, besides published research results, the main outcome of the project will be the graduation of one Ph.D. in the area of wireless communications and security. We emphasize the importance of providing the Stockholm area with well-qualified researchers in this field.

5 Preliminary Results

We have contributed to research on information theoretic security with the design of channel coding schemes for the wiretap channel under weak secrecy constraint. In particular, we have presented code constructions based on nested polar codes in [RT8] and based on LDPC codes in [RT5, RT47]. The code construction in [RT8] was developed independently of [11, 20], and it was among the first contributions that proved that polar codes asymptotically achieve the rate-equivocation region under weak secrecy constraint. In [RT5, RT36], we have furthermore developed a method to quantify the equivocation of the eavesdropper for nested LDPC codes in the asymptotic case. Examples provided in [RT5] show that even simple ensembles of regular LDPC codes achieve a very good performance if weak secrecy is considered. In recent work [RT11], we demonstrated that nested Reed-Solomon wiretap codes can be used to implement perfectly secure multiparty computation protocols.

6 International and National Collaboration

Through the ACCESS Linnaeus Center the applicant has collaborations with colleagues from, e.g., KTH's Signal Processing and Automatic Control Labs. Within Sweden the applicant has collaborations with the Universities of Linköping and Lund and Chalmers. Through European projects the applicant has collaborations with several European universities (e.g., Aalto University in Helsinki, NTNU in Trondheim, RWTH Aachen, TU Dresden, TU Munich, EURECOM, University of Rome, King's College London, University of Surrey, University of Valencia). The Communication Theory Lab has furthermore collaborations through, e.g., exchange of students and/or joint work with Stanford University, Princeton University, MIT, Georgia Tech.

References

[1] A.D. Wyner, "The wire-tap channel," *Bell System Tech. Journal*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[2] I. Csiszar and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. on Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[4] U.M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[5] A. Khisti, S.N. Diggavi, and G.W. Wornell, "Secret-key generation using correlated sources and channels,"

IEEE Trans. Inf. Theory, vol. 58, no. 2, pp. 652–670, Feb. 2012.

[6] I. Csiszar and P. Narayan, “Common randomness and secret key generation with a helper,” *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Feb. 2000.

[7] U. Maurer and S. Wolf, “Information-theoretic key agreement: From weak to strong secrecy for free,” in *Lecture Notes in Computer Science*. 2000, pp. 351–368, Springer-Verlag.

[8] R.A. Chou and M.R. Bloch, “Separation of reliability and secrecy in rate-limited secret-key generation,” *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4941–4957, Aug. 2014.

[9] M.R. Bloch and J.N. Laneman, “Strong secrecy from channel resolvability,” *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[10] T.S. Han and S. Verdu, “Approximation theory of output statistics,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, May 1993.

[11] H. Mahdavifar and A. Vardy, “Achieving the secrecy capacity of wiretap channels using polar codes,” *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[12] Y. Polyanskiy, H.V. Poor, and S. Verdu, “Channel coding rate in the finite blocklength regime,” *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[13] V. Kostina and S. Verdu, “Fixed-length lossy compression in the finite blocklength regime,” *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3309–3338, June 2012.

[14] R. Wilson, D. Tse, and R.A. Scholtz, “Channel identification: Secret sharing using reciprocity in ultrawideband channels,” *IEEE Trans. Inf. Forensics and Security*, vol. 2, no. 3, pp. 364–375, Sept. 2007.

[15] S. Rane, Ye Wang, S.C. Draper, and P. Ishwar, “Secure biometrics: Concepts, authentication architectures, and challenges,” *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 51–64, Sept. 2013.

[16] R. G. Gallager, *Low Density Parity Check Codes*, Cambridge, MA: MIT Press, 1963.

[17] E. Arikan, “Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels,” *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[18] A. Thangaraj, S. Dihidar, A.R. Calderbank, S.W. McLaughlin, and J.-M. Merolla, “Applications of LDPC codes to the wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[19] A. Subramanian, A. Thangaraj, M. Bloch, and S.W. McLaughlin, “Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes,” *IEEE Trans. Inf. Forensics & Security*, vol. 6, no. 3, pp. 585–594, 2011.

[20] O.O. Koyluoglu and H. El-Gamal, “Polar coding for secure transmission and key agreement,” *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 5, pp. 1472–1483, Oct. 2012.

[21] E. Sasoglu and A. Vardy, “A new polar coding scheme for strong security on wiretap channels,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2013.

[22] M. Bloch, A. Thangaraj, S.W. McLaughlin, and J.-M. Merolla, “LDPC-based secret key agreement over the Gaussian wiretap channel,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2006.

[23] X. Sun, X. Wu, C. Zhao, M. Jiang, and W. Xu, “Slepian-Wolf coding for reconciliation of physical layer secret keys,” in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, 2010.

[24] Chan Wong Wong, T.F. Wong, and J.M. Shea, “Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel,” *IEEE Trans. Inf. Forensics & Security*, vol. 6, no. 3, pp. 551–564, Sept 2011.

[25] J.M. Renes, R. Renner, and D. Sutter, “Efficient one-way secret-key agreement and private channel coding via polarization,” in *Advances in Cryptology-ASIACRYPT 2013*, pp. 194–213. Springer, 2013.

[26] R. A. Chou, M.R. Bloch, and E. Abbe, “Polar coding for secret-key generation,” *arXiv preprint arXiv:1305.4746v2*, Oct. 2013.

[27] E. Abbe, “Polarization and randomness extraction,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2011.

[28] M. Cheraghchi, F. Didier, and A. Shokrollahi, “Invertible extractors and wiretap protocols,” *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1254–1274, Feb 2012.

[29] S.B. Korada, E. Sasoglu, and R. Urbanke, “Polar codes: Characterization of exponent, bounds, and constructions,” *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6253–6264, Dec. 2010.

[30] D. Divsalar, S. Dollinar, C. R. Jones, and K. Andrews, “Capacity approaching protograph codes,” *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 6, pp. 876–888, Aug. 2009.

[31] M. Lentmaier, A. Sridharan, D. J. Costello, and K. S. Zigangirov, “Iterative decoding threshold analysis for LDPC convolutional codes,” *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 5274–5289, Oct. 2010.

[32] S. Kudekar, T. Richardson, and R.L. Urbanke, “Spatially coupled ensembles universally achieve capacity under belief propagation,” *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7761–7813, Dec. 2013.

[33] V. Aref, N. Macris, and M. Vuffray, “Approaching the rate-distortion limit with spatial coupling, belief propagation and decimation,” *arXiv preprint arXiv:1307.5210v2*, July 2013.

[34] A. Mukherjee and A.L. Swindlehurst, “Robust beamforming for security in MIMO wiretap channels with imperfect CSI,” *IEEE Trans. Signal Processing*, vol. 59, no. 1, pp. 351–361, Jan 2011.

[35] Jianwei Xie and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks,” *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, June 2014.

[36] V.Y.F. Tan, “Achievable second-order coding rates for the wiretap channel,” in *Proc. IEEE International Conference on Communication Systems (ICCS)*, 2012.

Interdisciplinarity

My application is interdisciplinary

□

An interdisciplinary research project is defined in this call for proposals as a project that can not be completed without knowledge, methods, terminology, data and researchers from more than one of the Swedish Research Councils subject areas; Medicine and health, Natural and engineering sciences, Humanities and social sciences and Educational sciences. If your research project is interdisciplinary according to this definition, you indicate and explain this here.

Click here for more information

Scientific report

Scientific report/Account for scientific activities of previous project

Budget and research resources

Project staff

Describe the staff that will be working in the project and the salary that is applied for in the project budget. Enter the full amount, not in thousands SEK.

Participating researchers that accept an invitation to participate in the application will be displayed automatically under Dedicated time for this project. Note that it will take a few minutes before the information is updated, and that it might be necessary for the project leader to close and reopen the form.

Dedicated time for this project

	Role in the project	Name	Percent of full time
1	Applicant	Ragnar Thobaben	40
2	PhD Student	TBA	80

Salaries including social fees

	Role in the project	Name	Percent of salary	2016	2017	2018	2019	Total
1	Applicant	Ragnar Thobaben	15	144,900	149,200	153,700	158,300	606,100
2	PhD Student	TBA	80	423,300	472,400	491,200	545,700	1,932,600
	Total			568,200	621,600	644,900	704,000	2,538,700

Other costs

Describe the other project costs for which you apply from the Swedish Research Council. Enter the full amount, not in thousands SEK.

Premises

	Type of premises	2016	2017	2018	2019	Total
1	Office Space	69,000	75,000	78,000	85,000	307,000
	Total	69,000	75,000	78,000	85,000	307,000

Running Costs

	Running Cost	Description	2016	2017	2018	2019	Total
1	Travel costs		20,000	60,000	60,000	60,000	200,000
2	Publication costs			15,000	15,000	30,000	60,000
	Total		20,000	75,000	75,000	90,000	260,000

Depreciation costs

	Depreciation cost	Description	2016	2017	2018	2019	Total
1	Computer Infrastructure	Laptop computers	24,000				24,000
	Total		24,000	0	0	0	24,000

Total project cost

Below you can see a summary of the costs in your budget, which are the costs that you apply for from the Swedish Research Council. Indirect costs are entered separately into the table.

Under Other costs you can enter which costs, aside from the ones you apply for from the Swedish Research Council, that the project includes. Add the full amounts, not in thousands of SEK.

The subtotal plus indirect costs are the total per year that you apply for.

Total budget

Specified costs	2016	2017	2018	2019	Total, applied	Other costs	Total cost
Salaries including social fees	568,200	621,600	644,900	704,000	2,538,700	1,010,000	3,548,700
Running costs	20,000	75,000	75,000	90,000	260,000		260,000
Depreciation costs	24,000	0	0	0	24,000		24,000
Premises	69,000	75,000	78,000	85,000	307,000	122,210	429,210
Subtotal	681,200	771,600	797,900	879,000	3,129,700	1,132,210	4,261,910
Indirect costs	208,000	227,000	236,000	257,000	928,000	369,356	1,297,356
Total project cost	889,200	998,600	1,033,900	1,136,000	4,057,700	1,501,566	5,559,266

Explanation of the proposed budget

Briefly justify each proposed cost in the stated budget.

Explanation of the proposed budget*

Salary Costs

Research in this project is planned for one Ph.D. student at activity level 80% and the applicant at activity level 40%. From VR, we seek for funding of 80% of one new Ph.D. student and 15% of one Associate Professor. The remaining 25% activity to reach a total activity of 40% is funded by KTH faculty funds and listed in the column "Annan kostdnad" in the table above (including the remaining costs for office space and overhead).

Office Space

The costs for office space are calculated at a fixed rate of 12.1% of the salary costs.

Travel Costs

The travel costs consider conference travels for the applicant and the involved PhD student. In order to make the results of the project visible, up to three travels per year to international high-quality IEEE conferences are expected (except for the first year).

Publication Costs

Publication costs include open access fees for journal publications.

Computer Infrastructure

Costs for computer infrastructure include the costs for two laptop computers scaled by the activity level of the applicant and the PhD student (20000 kr x 0.8 + 20000 kr x 0.4 = 24000 kr).

Indirect Costs

Indirect costs include KTH taxes (23.6% of salary costs), school taxes (6.28% of salary costs), and department taxes (6.68% of salary costs).

Other funding

Describe your other project funding for the project period (applied for or granted) aside from that which you apply for from the Swedish Research Council. Write the whole sum, not thousands of SEK.

Other funding for this project

	Funder	Applicant/project leader	Type of grant	Reg no or equiv.	2016	2017	2018	2019	Total
1	MSB	Henrik Sandberg	Center funding		4,000,000	4,000,000	4,000,000	4,000,000	16,000,00
	Total				4,000,000	4,000,000	4,000,000	4,000,000	16,000,00

CV and publications

CV

Curriculum Vitae Ragnar Thobaben

1 Higher Education Qualification

Dipl.-Ing.	2001	Christian Albrechts University, Kiel, Germany Electrical Engineering/Communications Engineering

2 Doctoral Degree

Dr.-Ing.	2007	Christian Albrechts University, Kiel, Germany Electrical Engineering/Communications Engineering Title: *Iterative Source-Channel Decoding for Variable-Length Codes* Advisor: Prof. Dr. Ulrich Heute

3 Postdoctoral Position

2006-2008	Communication Theory Lab, School of Electrical Engineering and ACCESS Linnaeus Center, KTH Royal Institute of Technology

4 Qualification Required for Appointment as a Docent

2013	Docent in Communication Theory

5 Current Position

2013-Present	Associate Professor (*lektor*) Communication Theory Lab, School of Electrical Engineering and ACCESS Linnaeus Center, KTH Royal Institute of Technology. Full-time employment with 80% research.

6 Previous Positions

2008-2013	Assistant Professor (*forskarassistent 2008-2010, bitr. lektor 2010-2013*) Communication Theory Lab, School of Electrical Engineering and ACCESS Linnaeus Center, KTH Royal Institute of Technology. Full-time employment with 80% research.
2006-2008	Postdoc Communication Theory Lab, School of Electrical Engineering and ACCESS Linnaeus Center, KTH Royal Institute of Technology.
2001-2006	Research and Teaching Assistant Institute for Circuits and Systems Theory, Christian Albrechts University, Kiel, Germany.

7 Interruptions in Research

Jan.-Aug. 2013	Parental leave (80% on leave)
Jan.-Aug. 2015	Parental leave (80% on leave)

8 Ph.D. Student Supervision (as Co-Advisor)

2007-2013	Zhongwei Si. Ph.D. Thesis: *Structured LDPC Convolutional Codes*, KTH, Jan. 2013. Main Supervisor: Mikael Skoglund
2007-2013	Ricardo Blasco Serrano. Ph.D. Thesis: *On Coordination and Compression in Networks*, KTH, Nov. 2013. Main Supervisor: Mikael Skoglund
2007-2014	Mattias Andersson. Ph.D. Thesis: *Coding and Transmission Strategies for Secrecy*, KTH, April 2014. Main Supervisor: Mikael Skoglund
2009-2014	Frederic Gabry. Ph.D. Thesis: *Secrecy in Cognitive Radio Networks*, KTH, Dec. 2014. Main Supervisor: Mikael Skoglund.
2009-Present	Leefke Dössel. Topic: *Anytime Coding.* Main Supervisor: Lars Rasmussen.

9 Other Information of Relevance to the Application

Main Research Grants

2015 TNG Postdoc Grant, "Fast nonlinear Fourier transform for multi-soliton transmission in optical fiber." Main applicant.

2010-2013 *Advanced Coexistence Technologies for Radio Optimisation in Licensed and Unlicensed Spectrum* (ACROPOLIS), EU/FP7 Network of Excellence. Co-applicant and responsible researcher at KTH.

2010-2012 *Quantitative Assessment of Secondary Spectrum Access* (QUASAR), EU/FP7, STREP. Co-applicant.

2008 *Combined Network and Channel Coding for Future Wireless Systems*, Wireless@KTH, seed project. PI.

Awards

2008 Faculty Award 2008 for the best Ph.D. thesis in engineering. Award for the best Ph.D. thesis in engineering in 2006/07. Christian Albrechts University, Kiel, Germany.

2001 VDE/VDI Prof. Dr. Werner Petersen Award. Award for excellent Diploma and Master's degree projects in Schleswig-Holstein in 2000/01. Christian Albrechts University, Kiel, Germany.

Review Assignments

Reviewer for numerous IEEE journals and conferences in the fields Information Theory, Communications, Wireless Communications, and Signal Processing (approx. 15 journal papers and 25 conference papers per year).

Thesis Committee

April 2008 Opponent at the Licentiate thesis defense of Mr. Daniel Puaca, Linköping University, Sweden. Thesis title: "Topics on Majority Logic Decoding." Supervisor: Danyo Danev.

June 2015 External referee at the Ph.D. thesis defense of Ms. Anne Wolf, TU Dresden, Germany. Thesis title: "Robust Optimization of Private Communication in Multi-Antenna Systems." Supervisor: Eduard A. Jorswieck.

Technical Program Committee (TPC) Member and Conference Organization

2015 IEEE SPAWC 2015, Stockholm, Sweden, June 2015. (Publicity Chair, Special-Session Organizer)

IEEE Globecom 2015 - Wireless Communications Symposium, San Diego, CA, USA, Dec. 2015. (TPC Member)

2014 IEEE Globecom 2014 - Wireless Communications Symposium, Austin, Texas, USA, Dec. 2014. (TPC Member)

Swedish Communication Technologies Workshop (Swe-CTW 2014), Västerås, Sweden, Jun. 2014. (Technical Program Chair)

2013 IEEE Vehicular Technology Conference (VTC-Spring 2013), Dresden, Germany, June 2013. (TPC Member)

2012 Swedish Communication Technologies Workshop (Swe-CTW 2012), Lund, Sweden, Oct. 2012. (TPC Member)

IEEE International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC 2012), Sydney, Australia, Sep. 2012. (TPC Member)

International Symposium on Wireless Communication Systems (ISWCS 2012), Paris, France, Aug. 2012. (TPC Member)

International Symposium on Turbo Codes & Iterative Information Processing, Gothenburg, Sweden, Aug. 2012. (Publicity Chair)

2011 IEEE Swedish Communication Technologies Workshop (Swe-CTW 2011), Stockholm, Sweden, Oct. 2011. (Publicity Chair)

Publication list

Publication List, April 2007 – Present

Citation data is based on **Google Scholar** database information (last update: 17 March, 2015). Self-citations by the applicant have been removed. Total number of citations in the considered period (without self-citations): 439.

1 Peer-Reviewed Original Articles

[RT1] L. Grosjean, L. K. Rasmussen, R. Thobaben, and M. Skoglund, "Systematic LDPC Convolutional Codes: Asymptotic and Finite-Length Anytime Properties," in *IEEE Transactions on Communications*, vol. 62, no. 12, 2014.

Number of citations: 1

[RT2] R. Blasco-Serrano, D. Zachariah, D. Sundman, R. Thobaben, and M. Skoglund, "A measurement rate-MSE tradeoff in compressive sensing through partial support recovery," in *IEEE Transactions on Signal Processing*, vol. 62, no. 8, Aug. 2014.

Number of citations: 1

[RT3] R. Blasco-Serrano, J. Lv, R. Thobaben, E. A. Jorswieck, and M. Skoglund, "Multi-antenna transmission for underlay and overlay cognitive radio with explicit message learning phase," *EURASIP Journal on Wireless Communications and Networking (JWCN)*, 2013:195.

Number of citations: -

[RT4] **(*)** Z. Si, R. Thobaben, and M. Skoglund, "Bilayer LDPC convolutional codes for decode-and-forward relaying," *IEEE Transactions on Communications*, vol. 61, no. 8, Aug. 2013.

Number of citations: 5

[RT5] **(*)** V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge type LDPC codes for the BEC wiretap channel," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1048–1064, Feb. 2013.

Number of citations: 13

[RT6] **(*)** R. Blasco-Serrano, R. Thobaben, M. Andersson, V. Rathi, and M. Skoglund, "Polar codes for cooperative relaying," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3263–3273, Nov. 2012.

Number of citations: 13

[RT7] **(*)** Z. Si, R. Thobaben, and M. Skoglund, "Rate-compatible LDPC convolutional codes achieving the capacity of the BEC," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 4021–4029, June 2012.

Number of citations: 6

[RT8] **(*)** M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Communications Letters*, vol. 14, no. 8, pp. 752–754, August 2010.

Number of citations: 62

[RT9] R. Thobaben and J. Kliewer, "An efficient variable-length code construction for iterative source-channel decoding," *IEEE Transactions on Communications*, vol. 57, no. 7, pp. 2005–2013, July 2009.

Number of citations: 7

2 Peer-Reviewed Conference Contributions

[RT10] Pin-Hsun Lin, F. Gabry, R. Thobaben, E. Jorswieck, M. Skoglund, "Multi-Phase Transmission for Secure Cognitive Radio Networks," in *Proc. IEEE International Conference on Communications (ICC)*, June 2015, London, UK.

Number of citations: -

[RT11] R. Thobaben, G. Dan, H. Sandberg, "Wiretap Codes for Secure Multi-Party Computation," in *Proc. IEEE Globecom 2014*, Dec. 2014, Austin, Tx, USA.

Number of citations: -

[RT12] Pin-Hsun Lin, F. Gabry, R. Thobaben, E. Jorswieck, M. Skoglund, "Clean relaying in cognitive radio networks with variational distance secrecy constraint," in *Proc. Globecom 2014*, Dec. 2014, Austin, Tx, USA.

Number of citations: -

[RT13] R. Blasco Serrano, R. Thobaben, and M. Skoglund, "Communication and Interference Coordination", *Information Theory and Applications Workshop (ITA) 2014*, San Diego, CA, USA, Feb. 2014.

Number of citations: -

[RT14] F. Naghibi, S. Salimi, R. Thobaben, and M. Skoglund, "The Lossless CEO Problem with Security Constraints," *Proc. International Symposium on Wireless Communication Systems 2013 (ISWCS 2013)*, Ilmenau, Germany, Aug. 2013.

Number of citations: 2

[RT15] R. Blasco-Serrano, D. Zachariah, D. Sundman, R. Thobaben, and M. Skoglund, "An achievable measurement rate-MSE tradeoff in compressive sensing through partial support recovery," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Vancouver, Canada, May 2013.

Number of citations: 3

[RT16] F. Gabry, S. Salimi, R. Thobaben, and M. Skoglund, "High SNR Performance of Amplify-and-Forward Relaying in Rayleigh Fading Wiretap Channels," in *Proc. 2013 Iran Workshop on Communication and Information Theory (IWCIT 2013)*, Tehran, Iran, May 2013.

Number of citations: 1

[RT17] F. Naghibi, R. Thobaben, S. Salimi, and M. Skoglund, "Layered LDPC convolutional codes for compression of correlated sources under adversarial attacks," in *Proc. International Symposium on Information Theory and its Applications (ISITA 2012)*, Honolulu, Hawaii, USA, Oct. 2012.

Number of citations: -

[RT18] Z. Si, R. Thobaben, M. Skoglund, and T.J. Oechtering, "Bidirectional broadcasting by using multi-edge type LDPC convolutional codes," in *Proc. International Symposium on Turbo Codes & Iterative Information Processing*, Gothenburg, Sweden, Aug. 2012.

Number of citations: 2

[RT19] J. Lv, R. Blasco-Serrano, E. A. Jorswieck, and R. Thobaben, "Linear precoding in MISO cognitive channels with causal primary message," in *Proc. International Symposium on Wireless Communication Systems 2012 (ISWCS 2012)*, Paris, France, Aug. 2012.

Number of citations: 2

[RT20] L. De Nardis, M.-G. Di Benedetto, D. Tassetto, S. Bovelli, A. Akhtar, O. Holland, and R. Thobaben, "Impact of mobility in cooperative spectrum sensing: theory vs. simulation," in *Proc. International Symposium on Wireless Communication Systems 2012 (ISWCS 2012)*, Paris, France, Aug. 2012.

Number of citations: 3

[RT21] F. Gabry, N. Li, N. Schrammar, M. Girnyk, E. Karipidis, R. Thobaben, L. K. Rasmussen, E. G. Larsson, and M. Skoglund, "Secure broadcasting in cooperative cognitive radio networks," in *Proc. Future Network & Mobile Summit 2012*, Berlin, Germany, July 2012.

Number of citations: 7

[RT22] R. Blasco-Serrano, J. Lv, R. Thobaben, E. A. Jorswieck, A. Kliks, and M. Skoglund, "Comparison of underlay and overlay spectrum sharing strategies in MISO cognitive channels," in Proc. *International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM 2012)*, Stockholm, Sweden, June 2012.

Number of citations: 5

[RT23] L. Dössel, L. K. Rassmussen, R. Thobaben, and M. Skoglund, "Anytime reliability of systematic LDPC convolutional codes" in *Proc. IEEE International Conference on Communications (ICC 2012)*, Ottawa, Canada, June 2012.

Number of citations: 6

[RT24] F. Gabry, N. Schrammar, M. A. Girnyk, N. Li, R. Thobaben, and L. K. Rasmussen, "Cooperation for secure broadcasting in cognitive radio networks," in *Proc. IEEE International Conference on Communications (ICC 2012)*, Ottawa, Canada, June 2012.

Number of citations: 9

[RT25] Z. Si, R. Thobaben, and M. Skoglund, "Dynamic decode-and-forward relaying with rate-compatible LDPC convolutional codes," in *Proc. International Symposium on Communications, Control and Signal Processing (ISCCSP 2012)*, invited paper, Rome, Italy, May 2012.

Number of citations: -

[RT26] J. Lv, R. Blasco-Serrano, E. A. Jorswieck, R. Thobaben, and A. Kliks, "Optimal beamforming in MISO cognitive channels with degraded message sets," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC 2012)*, Paris, France, April 2012.

Number of citations: 8

[RT27] J. Lv, E. A. Jorswieck, R. Blasco-Serrano, R. Thobaben, and A. Kliks, "Linear precoding in MISO cognitive channels with degraded message sets," in *Proc. International ITG Workshop on Smart Antennas 2012*, Dresden, Germany, March 2012.

Number of citations: 3

[RT28] A. Kliks, P. Sroka, J. Lv, R. Thobaben, E. A. Jorswieck, and R. Blasco-Serrano, "Crystallized rate regions in the secondary interference channels," in *Proc. International ITG Workshop on Smart Antennas 2012*, Dresden, Germany, March 2012.

Number of citations: 1

[RT29] R. Blasco-Serrano, R. Thobaben, and M. Skoglund, "Polar codes for coordination in cascade networks," in *Proc. International Zurich Seminar on Communications (IZS 2012)*, Zürich, Switzerland, March 2012.

Number of citations: 6

[RT30] F. Gabry, R. Thobaben, and M. Skoglund, “Cooperation for secrecy in presence of an active eavesdropper: a game-theoretic analysis,” in *Proc. IEEE International Symposium on Wireless Communication Systems (ISWCS 2011)*, Aachen, Germany, Nov. 2011.

Number of citations: 1

[RT31] Z. Si, M. Andersson, R. Thobaben, and M. Skoglund, “Rate-compatible LDPC convolutional codes for capacity-approaching hybrid ARQ,” *Proc. IEEE Information Theory Workshop (ITW 2011)*, Paraty, Brazil, Oct. 2011.

Number of citations: 5

[RT32] Z. Si, R. Thobaben, and M. Skoglund, “Bilayer LDPC convolutional codes for half-duplex relay channels,” in *Proc. IEEE International Symposium on Information Theory (ISIT 2011)*, St. Petersburg, Russia, August 2011.

Number of citations: 10

[RT33] F. Gabry, R. Thobaben, and M. Skoglund, “Outage performance and power allocation for decode-and-forward relaying and cooperative jamming for the wiretap channel,” in *Proc. IEEE International Conference on Communications (ICC 2011)*, Kyoto, Japan, June 2011.

Number of citations: 8

[RT34] F. Gabry, R. Thobaben, and M. Skoglund, “Outage performances for amplify-and-forward, decode-and-forward and cooperative jamming strategies for the wiretap channel,” in *Proc. IEEE Wireless Communications and Networking Conference (WCNC 2011)*, Cancun, Mexico, March 2011.

Number of citations: 12

[RT35] R. Blasco-Serrano, R. Thobaben, and M. Skoglund, “Bandwidth efficient compress-and-forward relaying based on joint source-channel coding,” in *Proc. IEEE Wireless Communications and Networking Conference (WCNC 2011)*, Cancun, Mexico, March 2011.

Number of citations: 5

[RT36] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, “Equivocation of Eve using two edge type LDPC codes for the erasure wiretap channel,” in *Proc. Asilomar Conference on Signals, Systems & Computers*, Pacific Grove, CA, USA, November 2010.

Number of citations: 4

[RT37] R. Blasco-Serrano, R. Thobaben, V. Rathi, and M. Skoglund, “Polar codes for compress-and-forward in binary relay channels,” in *Proc. Asilomar Conference on Signals, Systems & Computers*, Pacific Grove, CA, USA, November 2010.

Number of citations: 7

[RT38] Z. Si, R. Thobaben, and M. Skoglund, “Instantaneous relaying with bit-interleaved coded modulation: Design and optimization,” in *Proc. International Symposium on Turbo Codes & Iterative Information Processing*, Brest, France, Sept. 2010.

Number of citations: 4

[RT39] R. Thobaben, “Non-binary joint network/channel coding for multi-user ARQ,” in *Proc. International ICST Conference on Communications and Networking in China (ChinaCom 2010)*, invited paper, Beijing, China, August 2010.

Number of citations: -

[RT40] K. Kittichokechai, T. J. Oechtering, M. Skoglund, and R. Thobaben, "Source and channel coding with action-dependent partially known two-sided state information," in *Proc. IEEE International Symposium on Information Theory (ISIT 2010)*, Austin, TX, USA, June 2010.

Number of citations: 13

[RT41] P. Fouillot, C. J. Le Martret, and R. Thobaben, "Adaptive relaying strategies for collaborative spectrum sensing," in *Proc. International ICST Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM 2010)*, invited paper, Cannes, France, June 2010.

Number of citations: 2

[RT42] R. Blasco-Serrano, R. Thobaben, and M. Skoglund, "Compress-and-forward relaying based on symbol-wise joint source-channel coding," in *Proc. IEEE International Conference on Communications (ICC 2010)*, Cape Town, South Africa, May 2010.

Number of citations: 6

[RT43] E. G. Larsson, R. Thobaben, and G. Wang, "On diversity combining with unknown channel state information and unknown noise variance," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC 2010)*, Sydney, Australia, April 2010.

Number of citations: 3

[RT44] Z. Si, R. Thobaben, and M. Skoglund, "A practical approach to adaptive coding for the three-node relay channel," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC 2010)*, Sydney, Australia, April 2010.

Number of citations: 3

[RT45] Z. Si, R. Thobaben, and M. Skoglund, "Adaptive channel coding for the three-node relay channel with limited channel-state information," in *Proc. International Symposium on Communications, Control and Signal Processing (ISCCSP 2010)*, invited paper, Limassol, Cyprus, March 2010.

Number of citations: 2

[RT46] K. Kansanen, A. N. Kim, R. Thobaben, and J. Karlsson, "Low complexity bandwidth compression mappings for sensor networks," in *Proc. International Symposium on Communications, Control and Signal Processing (ISCCSP 2010)*, invited paper, Limassol, Cyprus, March 2010.

Number of citations: 11

[RT47] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Two edge type LDPC codes for the wiretap channel," in *Proc. Asilomar Conference on Signals, Systems & Computers*, Pacific Grove, CA, USA, Nov. 2009.

Number of citations: 14

[RT48] R. Thobaben, "Joint network/channel coding for bandwidth-efficient multi-user ARQ," in *Proc. IEEE International Workshop on Signal Processing Advances for Wireless Communications (SPAWC 2009)*, Perugia, Italy, June 2009.

Number of citations: 9

[RT49] Z. Si, R. Thobaben, and M. Skoglund, "On distributed serially concatenated codes," in *Proc. IEEE International Workshop on Signal Processing Advances for Wireless Communications (SPAWC 2009)*, Perugia, Italy, June 2009.

Number of citations: 8

[RT50] R. Thobaben, “On distributed codes with noisy relays,” in *Proc. Asilomar Conference on Signals, Systems & Computers*, Pacific Grove, CA, USA, Oct. 2008.

Number of citations: 25

[RT51] R. Thobaben, “A tutorial introduction to iterative source-channel decoding,” in *Proc. ITG Conference on Voice Communication*, invited paper, Aachen, Germany, Oct. 2008.

Number of citations: -

[RT52] R. Thobaben, L. Schmalen, and P. Vary, “Joint source-channel coding with inner irregular codes,” in *Proc. IEEE International Symposium on Information Theory (ISIT 2008)*, Toronto, Ontario, Canada, July 2008.

Number of citations: 11

[RT53] B. Mercier, V. Fodor, R. Thobaben, et. al, “Sensor networks for cognitive radio: theory and system design,” in *Proc. ICT Mobile Summit*, Stockholm, Sweden, June 2008.

Number of citations: 40

[RT54] R. Thobaben, “Joint network/channel coding for multi-user hybrid-ARQ,” in *Proc. International ITG Conference on Source and Channel Coding (SCC 2008)*, Ulm, Germany, Jan. 2008.

Number of citations: 21

[RT55] R. Thobaben and E. G. Larsson, “Sensor-network-aided cognitive radio: on the optimal receiver for estimate-and-forward protocols applied to the relay channel,” in *Proc. Asilomar Conference on Signals, Systems & Computers*, invited paper, Pacific Grove, CA, USA, Nov. 2007.

Number of citations: 25

[RT56] R. Thobaben, “EXIT functions for randomly punctured systematic codes,” in *Proc. IEEE Information Theory Workshop (ITW 2007)*, Lake Tahoe, CA, USA, Sept. 2007.

Number of citations: 8

[RT57] R. Thobaben, “A new transmitter concept for iteratively-decoded source-channel coding schemes,” in *Proc. IEEE Workshop on Signal Processing Advances in Wireless Communications (SPAWC 2007)*, Helsinki, Finland, June 2007.

Number of citations: 16

3 Monographs

[RT58] R. Thobaben, “Iterative Quellen- und Kanaldecodierung für Codes variabler Länge (Iterative source-channel decoding for variable-length codes),” in *Arbeiten über Digitale Signalverarbeitung*, Nr. 29, U. Heute, ed. Shaker Verlag, 2007.

4 Book Chapters

[RT59] G. Caso, L. De Nardis, R. Thobaben, and M.-G. Di Benedetto, “Cooperative Sensing of Spectrum Opportunities,” in *Opportunistic Spectrum Sharing and White Space Access: The Practical Reality,* First Edition, Chapter 7, O. Holland, H. Bogucka, and A. Medeisis, ed. John Wiley & Sons, Inc., 2015. (To appear.)

Number of citations: -

[RT60] A. Graell i Amat and R. Thobaben, “An introduction to distributed channel coding,” in *Channel Coding: Theory, Algorithms, and Applications,* Chapter 9, E. Biglieri, D. Declerq, and M. Fossorier, ed. Academic Press Library in Mobile and Wireless Communications, Aug. 2014. (To appear.)

Number of citations: -

5 Five Most Cited Publications

[1] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, “Nested polar codes for wiretap and relay channels,” *IEEE Communications Letters*, vol. 14, no. 8, pp. 752–754, August 2010.

Number of citations: 62

[2] J. Kliewer and R. Thobaben, “Iterative joint source-channel decoding of variable-length codes using residual source redundancy,” *IEEE Transactions on Wireless Communications*, vol. 4, no. 3, pp. 919–929, May 2005.

Number of citations: 56

[3] B. Mercier, V. Fodor, R. Thobaben, et al., “Sensor networks for cognitive radio: theory and system design,” in *Proc. ICT Mobile Summit*, Stockholm, Sweden, June 2008.

Number of citations: 40

[4] R. Thobaben and J. Kliewer, “Low complexity iterative joint source-channel decoding for variable-length encoded Markov sources,” *IEEE Transactions on Communications*, vol. 53, no. 12, pp. 2054–2064, December 2005.

Number of citations: 37

[5] R. Thobaben and J. Kliewer, “Robust decoding of variable-length encoded Markov sources using a three-dimensional trellis,” *IEEE Communications Letters*, vol. 7, no. 7, pp. 320–322, July 2003.

Number of citations: 34

CV

Name: Ragnar Thobaben	**Doctorial degree:** 2007-07-23
Birthdate: 19770707	**Academic title:** Docent
Gender: Male	**Employer:** Kungliga Tekniska högskolan

Research education

Dissertation title (swe)

Dissertation title (en)

Iterative source-channel decoding for variable-length codes

Organisation	**Unit**	**Supervisor**
Christian Albrechts University, Kiel, Germany Not Sweden - Higher Education institutes		Ulrich Heute
Subject doctors degree	**ISSN/ISBN-number**	**Date doctoral exam**
20204. Telekommunikation	3832263519	2007-07-23

Publications

Name: Ragnar Thobaben	**Doctorial degree:** 2007-07-23
Birthdate: 19770707	**Academic title:** Docent
Gender: Male	**Employer:** Kungliga Tekniska högskolan

Thobaben, Ragnar has not added any publications to the application.

Register

Terms and conditions

The application must be signed by the applicant as well as the authorised representative of the administrating organisation. The representative is normally the department head of the institution where the research is to be conducted, but may in some instances be e.g. the vice-chancellor. This is specified in the call for proposals.

The signature*from the applicant*confirms that:

- the information in the application is correct and according to the instructions form the Swedish Research Council
- any additional professional activities or commercial ties have been reported to the administrating organisation, and that no conflicts have arisen that would conflict with good research practice
- that the necessary permits and approvals are in place at the start of the project e.g. regarding ethical review.

The signature *from the administrating organisation* confirms that:

- the research, employment and equipment indicated will be accommodated in the institution during the time, and to the extent, described in the application
- the institution approves the cost-estimate in the application
- the research is conducted according to Swedish legislation.

The above-mentioned points must have been discussed between the parties before the representative of the administrating organisation approves and signs the application.

Project out lines are not signed by the administrating organisation. The administrating organisation only sign the application if the project outline is accepted for step two.

Applications with an organisation as applicant is automatically signed when the application is registered.