Vetenskapsrådet

Application

2015-03-31

2015-04528 **Johansson, Thomas** **NT-14**

Information about applicant

Name: Thomas Johansson

Doctorial degree: 1994-12-09

Birthdate: 19670901

Academic title: Professor

Gender: Male

Employer: Lunds universitet

Administrating organisation: Lunds universitet

Project site: Elektro- och informationsteknik 107201

Information about application

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

Type of grant: Projektbidrag

Focus: Fri

Subject area:

Project title (english): Future cryptographic primitives from LWE and related problems

Project start: 2016-01-01

Project end: 2019-12-31

Review panel applied for: NT-14, NT-2, NT-1

Classification code: 20203. Kommunikationssystem, 10201. Datavetenskap (datalogi), 10104. Diskret matematik

Keywords: cryptography, post-quantum, coding theory, learning with errors

Funds applied for

Year:	2016	2017	2018	2019
Amount:	1,306,000	1,338,000	1,372,000	1,405,000

Descriptive data

Project info

Project title (Swedish)*

Framtida kryptografiska primitiver från LWE och relaterade problem

Project title (English)*

Future cryptographic primitives from LWE and related problems

Abstract (English)*

The proposed project is aimed at examining how the Learning With Errors (LWE) problem and related structures can be exploited and further developed in the area of future cryptograpic primitives.

In particular, we investigate of the security of existing cryptographic primitives based on the LWE problem, the related LPN problem, and similar structures. We look for new and better algorithms for solving the LWE problem and related problems and how to build new and efficient cryptographic primitives based on LWE and LPN. The work is using connections between coding theory, LWE and lattice-based cryptographic primitives.

The LWE problem and similar problems is perhaps the most interesting platform for future cryptographic primitives, as there is currently no known attack even if a quantum computer is available. It is also the currently best technique we know to obtain homomorphic encryption, a feature of encryption that will be very important in future cloud-based information systems if we want to have security features in the cloud.

Popular scientific description (Swedish)*

Traditionellt sett har kryptologi varit ett militärt forskningsområde, men för cirka tjugofem år sedan framkom nya revolutionerande idéer inom området som gjorde att öppen forskning började växa fram inom universitetsvärlden. Utan att gå in på detaljer, kan man säga att de nya idéerna belyste hur stora och viktiga de civila tillämpningarna för kryptologi skulle kunna bli. Dagligen utnyttjar nu de flesta av oss resultat från forskningen genom att de är en viktig del av olika kommunikations eller informationssystem, exempelvis mobiltelefoner, butiks- och banktjänster på Internet samt epost. Kryptologi handlar om att studera olika kryptografiska primitiver, med vilket vi menar olika typer av byggstenar som kan användas för att skapa önskad säkerhet i ett informationssystem. Det vanligaste exemplet på en sådan primitiv är förmodligen ett symmetriskt krypteringssystem. Symmetriskt betyder här att den som krypterar (sändaren) och den som dekrypterar (mottagaren) båda måste ha tillgång till samma hemliga nyckel. Krypteringssystemet överför indata (klartexten) till utdata (kryptotexten) på ett sådant sätt att man genom att observera kryptotexten inte får någon som helst information om klartexten. Endast om man har tillgång till den hemliga nyckeln kan man, från en given kryptotext, återskapa klartexten. Sålunda kan en sändare och en mottagare överföra information på en avlyssnad kanal om de båda har tillgång till en gemensam hemlig nyckel.

De asymmetriska krypteringssystemen, det mest kända kallat RSA, fungerar istället så att man har två olika nycklar, en publik krypteringsnyckel och en annan hemlig dekrypteringsnyckel. Det betyder att vem som helst kan använda den öppna krypteringsnyckeln och sända ett krypterat meddelande, men bara den som har den hemliga dekrypteringsnyckeln kan avkoda och få fram meddelandet. Denna ide kan enkelt modifieras för att skapa digitala signaturer, dvs ett dokument signeras med en hemlig nyckel och dess äkthet kan sedan verifieras av vem som helst genom den publika nyckeln. Alla asymmetriska system byggs från ett antagande att vissa svåra problem inte går att lösa i rimlig tid. Ett typiskt sådant problem är faktoriseringsproblemet, tex givet produkten av två primtal, ta reda på vilka primtalen är. Är primtalen tillräckligt stora (ett par hundra decimala siffror) är detta idag inte möjligt att lösa inom rimlig tid.

En mycket intressant utveckling inom fysiken är de försök som görs med att bygga en kvantdator. Kvantdatorn använder kvantmekanik för att utföra vissa typer av beräkningar potentiellt mycket snabbare än vad dagens datorer klarar av. Speciellt har man visat att en stor kvantdator skulle kunna lösa faktoriseringsproblemet väldigt snabbt. Vissa forskare tror att en sådan kvantdator skulle kunna vara verklighet inom 20 år. Det skulle innebära att de flesta av de lösningar för informationssäkerhet som vi har idag i vårt samhälle plötsligen inte längre skulle vara säkra. Detta skulle innebära enorma omställningar och problem.

I detta projekt studerar vi alternativa metoder för att bygga asymmetriska kryptosystem som förhoppningsvis inte kan attackeras även om vi skulle ha tillgång till en kvantdator. Vi undersöker de system som istället för faktorisering utnyttjar andra svåra problem som står emot kvantdatorn. Vi testar både deras säkerhet samt försöker konstruera nya metoder som är bättre än de tidigare kända. De problem vi undersöker kallas "Learning with Errors" och har flera attraktiva egenskaper. En sådan är att man kan skapa så kallad homomorfisk kryptering som innebär att man kan bearbeta den krypterade texten utan att först dekryptera den. Detta kommer att vara viktigt i framtida molntjänster.

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 > 20203. Kommunikationssystem 1. Naturvetenskap > 102. Data- och informationsvetenskap (Datateknik) > 10201. Datavetenskap (datalogi) 1. Naturvetenskap > 101. Matematik > 10104. Diskret matematik

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

Keyword 1*

cryptography

Keyword 2*

post-quantum

Keyword 3*

coding theory

Keyword 4

learning with errors

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

PROJECT PLAN

Future cryptographic primitives from LWE and related problems

1 Purpose and aims

The proposed project is aimed at examining how the *Learning With Errors* (LWE) problem and related structures can be exploited and further developed in the area of future cryptograpic primitives. In particular, we look at problems like

- investigation of the security of existing cryptographic primitives based on the LWE problem, the related LPN problem, and similar structures.
- designing new and better algorithms for solving the LWE problem and related problems.
- how to build new and efficient cryptographic primitives based on LWE and LPN.
- the connection between coding theory, LWE and lattice-based cryptographic primitives.

2 Survey of the field

Communication and cyber security are important parts of the information infrastructure. All security systems rely on different cryptographic primitives, such as block ciphers, stream ciphers, public key cryptosystems (PKC), digital signatures, etc. The design of such primitives is an essential research area, creating the basic tools for building good security systems. The increasing importance of security solutions in general and cryptographic primitives in particular has been frequently documented in research evaluations as well as in media.

When cryptographic primitives are used in different contexts, their performance differ. Aspects like efficient hardware implementations, efficient software implementations with restricted memory use, low power consumption, etc., are central to the design of primitives. The designer aims at providing as good performance values as possible for the above mentioned requirements (high speed, small hardware implementation, etc., and results relating parameter choices to methods of cryptanalysis are significant. Most cryptographic research can be viewed as trying to achieve the best possible trade-off between implementation efficiency and security. There are a few important trends in current cryptographic research.

- Some years ago, physics entered cryptography and we got an area named quantum cryptography. The area contains two main ideas, one being the possibility of completely secure key distribution in a physical channel, the other one being the usefulness of a possible quantum computer in attacking cryptosystems. *Post-quantum cryptography* refers to a situation in the near future when a strong quantum computer exists [6].

  A quantum computer is a device for computation that uses quantum mechanical phenomena, such as superposition and entanglement, to perform operations on data. Usual computers require data to be encoded into bits, whereas quantum computation utilizes quantum properties to represent data and perform operations on these data. A quantum computer maintains as state a sequence of so-called qubits. The quantum computer with n qubits can be in an arbitrary superposition of up to 2^n different states simultaneously, compared to a normal computer that can only be in one of these states at any one time. The possibility of operating on 2^n different states simultaneously is the reason why a quantum computer with many qubits potentially can outperform any classical computer. Although we have not yet seen quantum computers outperforming classical computers, there has been some very interesting developments in this area. For example, the company *D-wave systems* markets some kind of "quantum computer" and got companies like Google to partner up. Its approach to quantum computing has been heavily criticised, though.

If a large quantum computer is reality in 20 years, then most of todays security solutions are completely broken. These solutions are typically based on a belief that for example integer factorization is computationally infeasible for large integers, e.g. a product of two 200-digit primes. But it was shown by Shor that a quantum computer could efficiently solve this problem using Shor's algorithm to find its factors [25]. This ability would allow a quantum computer to break most of the cryptographic systems in use today (for example everything using RSA). Most of the popular public key ciphers are based on the difficulty of factoring integers or the related discrete logarithm problem, which can also be solved in polynomial time by Shor's algorithm if a large enough quantum computer exists. This drastic change in security for most of our commonly used cryptographic primitives would have dramatic impact on privacy and security in our society. The conclusion is that we have to prepare ourselves for this situation and study how to achieve cryptographic security (if possible) in a post-quantum world. If a large quantum computer is getting closer in time, we need to remove many of the existing cryptographic solutions and replace them with something new.

Studying what cryptographic primitives remain in post-quantum cryptography, we note that quantum computers break for example RSA, DSA and also elliptic curve versions like ECDSA. However, there are a few important classes of cryptographic schemes not known to be broken by a quantum computer and **one such class contains schemes based on the LWE problem and similar problems**.

- A second trend in cryptography is *light-weight cryptography*, the area of devising schemes that are very simple in their nature and thus allow implementations on platforms with very restricted hardware. The general trend in society towards a future *Internet of Things* requires the use of crypto primitives running in a very restricted environment. Common solutions like RSA, making exponentiations of 1000-bit numbers, is simply not implementable. Extreme cases are e.g. security protocols implemented in RFID-tags. In this area, some very efficient light-weight crypto primitives based on LPN and LWE have been developed. For example, we have seen a large collection of proposed authentication protocols for RFID-tags based on the LPN problem (HB,HB$^+$,HB^{++}, HB-MP, HB-MP$^+$, HB$^?$, HB$^\#$, RANDOM-HB$^\#$, Trusted HB, HB-MAC, HB^N, GHB$^\#$, HB^b, NL-HB, PUF-HB, AUTH/MAC1/MAC2, and Lapin (see [3] for details)).

- A third trend to mention is the strong interest in *fully homomorphic encryption.* A general technical trend in society is the use of the "cloud" for storage or computing. From a security perspective, one of the main enablers to provide different security features in the cloud is the possibility of computing on encrypted data. In more detail, if ϕ is an encryption function, we would like to have the homomorphic property $\phi(x) + \phi(y) = \phi(x+y)$ and $\phi(x) \cdot \phi(y) = \phi(x \cdot y)$. This is a very complicated thing, but it was shown by Gentry [13] that it is indeed possible to achieve. Although Gentry's initial approach used lattices, the LWE problem and similar structures are today essential tools for building homomorphic encryption.

2.1 The LWE problem and related problems

Learning with Errors (LWE) is a problem that has received a lot of attention recently. Regev introduced LWE in [23] and it has proved to be a very useful tool for constructing cryptographic primitives. Although a great number of different applications in cryptography have been given since the introduction of the LWE problem, one of the most interesting ones is the recent work on constructing fully homomorphic encryption schemes [13, 8, 9, 14].

We already explained several motivating reasons for the interest in LWE-based cryptography. Another reason is the well-developed theory on lattice problems, which gives insights into the hardness of the LWE problem. There are theoretical reductions from worst-case lattice problems to average-case LWE [23]. Let us now state the LWE problem as in [23].

Definition 1 *Let n be a positive integer, q an odd prime, and let $\mathcal{X}$ be an error distribution selected as the discrete Gaussian distribution*[1] *on $\mathbb{Z}_q$. Fix $\mathbf{s}$ to be a secret vector in $\mathbb{Z}_q^n$, chosen according to a uniform distribution. Denote by $L_{\mathbf{s},\mathcal{X}}$ the probability distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, choosing an error $e \in \mathbb{Z}_q$ according to $\mathcal{X}$ and returning*

$$(\mathbf{a}, z) = (\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$$

in $\mathbb{Z}_q^n \times \mathbb{Z}_q$, where $\langle \mathbf{a}, \mathbf{s} \rangle = \sum_{i=1}^{n} a_i s_i \in \mathbb{Z}_q$. The (search) LWE *problem is to find the secret vector* $\mathbf{s}$ *given a fixed number of samples from $L_{\mathbf{s},\mathcal{X}}$.*

The definition above gives the *search* LWE problem, as the problem description asks for the recovery of the secret vector $\mathbf{s}$. Another variant is the so-called *decision* LWE problem. In this case the problem is to distinguish samples drawn from $L_{\mathbf{s},\mathcal{X}}$ and samples drawn from a uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

The parameters of an LWE instance are typically chosen with some internal relations. The prime q is chosen as a polynomial in n, and the discrete Gaussian distribution $\mathcal{X}$ has mean zero and standard deviation $\sigma = \alpha \cdot q$ for some small α. For example, in [23], Regev proposed to use parameters $q \approx n^2$ and $\alpha = 1/(\sqrt{2\pi n} \cdot \log_2^2 n)$.

We shortly describe some of the most important related problems. First, the *Ring-LWE problem* considers $\mathbf{s}$ and $\mathbf{a}$ as elements from the quotient ring $\mathbb{Z}_q[x]/(f(x))$, where $f(x)$ is a fixed polynomial in $\mathbb{Z}_q[x]$ of degree n. A returned sample is of the form

$$(\mathbf{a}, \mathbf{z}) = (\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + \mathbf{e},)$$

where $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ and $e_i \in \mathcal{X}$. Vectors are considered as elements in $\mathbb{Z}_q[x]/(f(x))$. Clearly, the Ring-LWE problem is a special case of LWE as one sample from Ring-LWE can be viewed as n LWE samples. However, the ring structure may allow for more efficient ways to solve the problem.

[1] obtained by assigning a probability proportional to $\exp(-x^2/2\sigma^2)$ to each $x \in \mathbb{Z}$ and then folding $\mathrm{mod} q$.

The *Learning Parity with Noise (LPN) problem* is the LWE problem when $q = 2$. The error distribution is then described by the Bernoulli distribution ($P(e = 0) = 1 - p$). Finally, the *Ring-LPN problem* is the Ring-LWE problem when $q = 2$ and each e_i is drawn independently from the Bernoulli distribution.

2.2 Previous Work on solving the LWE problem

A number of algorithms for solving the LWE problem have been given, using different approaches. As there is a strong connection to lattice problems, a direction for a subset of the algorithms has been to either rewrite the LWE problem as the problem of finding a short vector in a dual lattice, the Short Integer Solution (SIS) problem, or to solve the Bounded Distance Decoding (BDD) problem. Lattice reduction algorithms may be applied to solve these problems. Even though there has been a lot of research devoted to the study of lattice reduction algorithms, there still seems to be quite some uncertainty about the complexity and performance of such algorithms for higher dimensions. A collection of papers studying LWE with this direction is [5, 12, 10, 18, 15, 16, 19, 21, 22, 24].

Another interesting approach was given by Arora and Ge in [4], where they proposed a novel algebraic approach to solve the LWE problem. The asymptotic complexity of this algorithm is subexponential when $\sigma \leq \sqrt{n}$, but fully exponential otherwise. The algorithm is mainly of asymptotic interest as applying it on specific instances gives higher complexity than other solvers.

Finally, much work has been done on combinatorial algorithms for solving LWE, all taking the famous Blum-Kalai-Wasserman (BKW) algorithm [7] as a basis. The BKW algorithm resembles the generalized birthday approach by Wagner [26] and was originally given as an algorithm for solving the LPN problem. These combinatorial algorithms have the advantage that that their complexity can be analyzed in a standard way and we can get explicit values on the complexity for different instantiations of the LWE problem. Even though we use approximations in the analysis, the deviation between theoretical analysis and actual performance seems to be small [2, 11]. This approach tends to give algorithms with the best performance for larger parameter choices. A possible drawback with BKW-based algorithms is that they usually require a huge amount of memory, often of the same order as the time complexity. Some recent work in this direction is [1, 2, 11].

2.3 Cryptographic primitives from LWE

A large collection of cryptographic primitives based on the LWE problem can be found in literature. We review Regev's initial public key encryption scheme [23]. In the following, $m = 5n$, $n^2 < q < 2n^2$, $\alpha = 1/(\sqrt{2\pi n} \cdot \log_2^2 n)$ and all additions are performed in $\mathbb{Z}_q$.

- Private key: Choose $\mathrm{s} \in \mathbb{Z}_q^n$ uniformly at random as the private key.
- Public Key: For $i = 1, \ldots, m$ choose m vectors $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_m} \in \mathbb{Z}_q^n$ from the uniform distribution. Also choose elements $e_1, \ldots, e_m \in \mathbb{Z}_q$ independently according to the Gaussian distribution $\mathcal{X}$. The public key is the given by $(\mathbf{a_i}, b_i) = (\mathbf{a_i}, \langle \mathbf{a_i}, \mathrm{s} \rangle + e_i)$ for $i = 1, \ldots, m$.
- Encryption: In order to encrypt a bit x we choose a random subset $S \subset [1, m]$. The result of encryption is $(\sum_S \mathbf{a_i}, \sum_S b_i)$ if $x = 0$ and $(\sum_S \mathbf{a_i}, \lfloor q/2 \rfloor + \sum_S b_i)$ if $x = 1$.

- Decryption: The result of decryption of a pair $(\mathbf{a}, b)$ is 0 if $b - \langle \mathbf{a}, \mathbf{s} \rangle$ is closer to 0 than to $\lfloor q/2 \rfloor$ in $\mathbb{Z}_q$. Otherwise, the result of decryption is 1.

Some of the most interesting primitives constructed from the LWE problem are a large part of the more recent (2nd generation) homomorphic cryptosystems. Without getting into details, we note that two implementations of homomorphic cryptosystems are available in open source libraries: The HElib library implements the Brakerski-Gentry-Vaikuntanathan cryptosystem (BGV), and the FHEW library implements a combination of Regev's LWE cryptosystem with a special bootstrapping techniques. Both libraries implement fully homomorphic encryption including bootstrapping. Still, the schemes are too costly in time to be practical.

3 Project description

The project will include the applicant, one new PhD student, as well as a half-time postdoc position (candidate: Qian Guo). The remaining part of the postdoc position will be funded from other projects. The time frame is a four year period, after which the PhD student will graduate. Our project plans and ideas can be split in three parts, described in the following subsections.

3.1 New algorithms for solving LWE, LPN, and related problems

A fundamental problem is the study of how to solve LWE problems in the most efficient way. Not only is it necessary to know the complexity of the problems in order to instantiate constructed primitives, we may also find particular problem instances that are weaker than the general case and should be avoided.

Assume that we ask for m samples from the LWE distribution $L_{\mathbf{s},\mathcal{X}}$ and the response is

$$(\mathbf{a}_1, z_1), (\mathbf{a}_2, z_2), \ldots, (\mathbf{a}_m, z_m),$$

where $\mathbf{a}_i \in \mathbb{Z}_q^n, z_i \in \mathbb{Z}_q$. We introduce $\mathbf{z} = (z_1, z_2, \ldots, z_m)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_m) = \mathbf{sA}$. We can then write $\mathbf{A} = (\mathbf{a}_1^{\mathrm{T}}, \mathbf{a}_2^{\mathrm{T}}, \ldots, \mathbf{a}_n^{\mathrm{T}})$ and $\mathbf{z} = \mathbf{sA} + \mathbf{e}$, where $z_i = y_i + e_i = \langle \mathbf{s}, \mathbf{a}_i \rangle + e_i$ and $e_i \in \mathcal{X}$ is the noise and $\mathbf{e} = (e_1, e_2, \ldots, e_m)$. We see that the problem has been reformulated as a decoding problem. The matrix $\mathbf{A}$ serves as the generator matrix for a linear code over $\mathbb{Z}_q$ and $\mathbf{z}$ is the received word. Finding the codeword $\mathbf{y} = \mathbf{sA}$ such that the Euclidean distance $||\mathbf{y} - \mathbf{z}||$ is minimum [2] will give the secret vector $\mathbf{s}$.

A brief description of the famous BKW algorithm follows. Initially, one searches for all combinations of two columns in $\mathbf{A}$ with the same last b entries. Assume that one finds two columns $\mathbf{a}_{i_1}^{\mathrm{T}}, \mathbf{a}_{i_2}^{\mathrm{T}}$ such that

$$\mathbf{a}_{i_1} - \mathbf{a}_{i_2} = (* \quad * \quad \cdots \quad * \quad \underbrace{0 \quad 0 \quad \cdots \quad 0}_{b \text{ symbols}}),$$

where $*$ means any value. Then a new vector $\mathbf{a}_1^{(2)} = \mathbf{a}_{i_1} - \mathbf{a}_{i_2}$ is formed. An "observed symbol" is also formed, corresponding to this new column by forming $z_1^{(2)} = z_{i_1} - z_{i_2}$. If $y_1^{(2)} = \left\langle \mathbf{s}, \mathbf{a}_1^{(2)} \right\rangle$, then $z_1^{(2)} = y_1^{(2)} + e_1^{(2)}$, where now $e_1^{(2)} = e_{i_1} - e_{i_2}$. Recall that noise like e_{i_1} follows the Gaussian distribution with variance σ^2, so $e_1^{(2)} = e_{i_1} - e_{i_2}$ is considered to be Gaussian distributed with variance $2\sigma^2$. There is also a second obvious way of getting collisions, namely, combining any

[2] $\|\mathbf{x}\| = \sqrt{x_1^2 + \cdots + x_n^2}$.

two vectors where the sum of the collision sets is zero. The procedure is analog to the above, just replacing subtraction with addition.

Put all such new vectors in a matrix $\mathbf{A}_2$,

$$\mathbf{A}_2 = (\mathbf{a}_1^{(2)\mathrm{T}}\mathbf{a}_2^{(2)\mathrm{T}} \dots \mathbf{a}_{m_2}^{(2)\mathrm{T}}).$$

Now the last b entries of columns in $\mathbf{A}_2$ are all zero. In connection to this matrix, the vector of observed symbols is

$$\mathbf{z}_2 = (z_1^{(2)} z_2^{(2)} \cdots z_{m_2}^{(2)}),$$

where $e_i^{(2)} = z_i^{(2)} - y_i^{(2)}$ are assumed Gaussian with variance $2\sigma^2$, for $1 \leq i \leq m_2$. This completes one step of the BKW algorithm. The procedure is iterated $t-1$ times cancelling more positions in each step, until vectors have only a few nonzero positions. In each iteration, the noise is increased. Finally, the first positions in s are recovered through a hypothesis test on the samples, which after t steps have the form $z_i^{(t)} = y_i^{(t)} + e_i^{(t)}$.

There are some improved versions of BKW, one is using lazy modulus reduction [2] and another is the very recent improvement in [11].

- Based on an idea of using lattice codes, we sketch a new algorithm that quite substantially outperforms all previous solvers for LWE. Very briefly, in the ith BKW step we fix a q-ary linear code with parameters (N_i, k), called $\mathcal{C}_i$. The code gives rise to a lattice code. Let I be an index set and let $\mathbf{a}_I$ be the vector obtained from $\mathbf{a}$ by including only indices in I. In the ith BKW step we use an index set I of size N_i (for example, I is the last N_1 bits in step one, then the next N_2 bits in step 2, etc.). Now, for any given vector $\mathbf{a}_I$ as input to a BKW step, we approximate the vector by one of the codewords in the code $\mathcal{C}_i$.

  We rewrite $\mathbf{a}_I$ into two parts, the codeword part $\mathbf{c}_I \in \mathcal{C}_i$ and an error part $\mathbf{e}_I \in \mathbb{Z}_q^{N_i}$, i.e.,

  $$\mathbf{a}_I = \mathbf{c}_I + \mathbf{e}_I. \qquad (1)$$

  Clearly, we desire the error part to be as small as possible, so we adopt a decoding procedure to find the nearest codeword in the chosen code $\mathcal{C}_i$ using the Euclidean metric.

  Each vector $\mathbf{a}_I$ is then sorted according to which codeword it was mapped to. Altogether, there are q^k possible codewords. Finally, generate new vectors for the next BKW step by subtracting vectors mapped to the same codeword (or adding to the zero codeword). The inner product $\langle \mathbf{s}_I, \mathbf{a}_I \rangle$ is equal to

  $$\langle \mathbf{s}_I, \mathbf{a}_I \rangle = \langle \mathbf{s}_I, \mathbf{c}_I \rangle + \langle \mathbf{s}_I, \mathbf{e}_I \rangle .$$

  By subtracting two vectors mapped to the same codeword we cancel out the first part of the right hand side and we are left with the noise. The latter term is referred as the error term introduced by coding.

  Summing up, the new approach can cancel many more positions compared to standard BKW, at the expense of introducing an additional noise term. Current work indicates that the approach substantially outperforms all previous methods. There are however numerous theoretical questions to investigate, e.g., regarding decoding procedures, parameter choices for optimized performance and asymptotic analysis.

- A very common instance in cryptographic primitives is the Ring-LWE problem described before. Although general LWE solvers can be applied on this problem, there might be a possible gain in using the ring structure in the problem. We can split the problem using the Chinese Remainder Theorem (CRT), to get smaller instances of the problem, but the noise gets more complicated. We intend to investigate how to best approach this case and we have some interesting ideas using a vectorized approach, e.g., viewing two samples as a single sample in a larger alphabet ($\mathbb{Z}_q^2$).

- A lot of the above reasoning applies also to the LPN, Ring-LPN and similar problems. Due to the binary alphabet, the LPN problem is somewhat different from standard LWE and this opens up for alternative approaches. One interesting idea we intend to explore is to examine whether iterative methods from coding theory (like LDPC codes and its decoding) can be an efficient method to solve certain LPN problems.

3.2 Investigation of cryptographic primitives based on LWE, LPN and similar problems

There are numerous different proposals of primitives based on LWE or LPN. They are usually provably secure, i.e., if you can break the primitive then you can solve the underlying problem (some LWE problem or lattice problem in this case). Still, the reduction may be weak or perhaps not applicable. An attack on a primitive may be much more efficient than solving the LWE problem. There may also be new types of attacks not covered by the considered security model.

- We intend to examine different types of attacks on common primitives to give a better view of what parameter choices are needed for a given security level and how different proposals differ in efficiency and key sizes. For example, do primitives based on LWE (q large) generally perform better than primitives based on LPN?
- We are also very interested in the area of constructing new primitives based on LWE or LPN. In particular, constructions towards fully homomorphic encryption that can be even more efficient that existing ones is a given target.

3.3 Connections between coding theory, LWE and lattice-based cryptographic primitives

Finally, we would like to point at the connections between coding theory, LWE and lattice based cryptographic primitives as a very interesting area, where techniques from different areas may be shared. Here are a few thoughts.

- The LWE and LPN problems can be reformulated as decoding problems of random codes in coding theory. The code can be arbitrarily long, but the dimension is fixed. Are there further techniques in coding theory that can be useful in solving LWE and LPN? Or perhaps vice versa?
- The well known commercial cryptosystem NTRU [17], being a lattice-based scheme, has a public key which can be viewed as a generator matrix of a q-ary code. This code contains a codeword of particularly low weight in the Euclidean metric and finding it gives the private key. LWE solvers can be applied, but are there better approaches?
- The recent encryption scheme MDPC [20] is similar to NTRU, but uses the binary alphabet and uses LDPC structures and iterative decoding in the private decryption phase. Can

MDPC be a basis for developing new primitives like a signature scheme or homomorphic encryption?

3.4 Research excellence for the project

The crypto and security group at Lund University, headed by the applicant, has for a long time been Sweden's largest and strongest research group in the area of cryptology. It is among the leading groups in the world in symmetric crypto and code-based crypto. Some highlights from research.

- Inventors of the SNOW 2.0 stream cipher (ISO standard, etc.). Its modified version SNOW 3G is in the UMTS, LTE standards, etc.
- Inventors/Coinventors of authentication techniques used in GCM mode of operation (NIST standard) and in the UMTS, LTE standards, etc.
- Inventors of the Grain family of stream ciphers. Selected in the eSTREAM final portfolio (www.ecrypt.eu.org).
- Proposed some of the basic techniques in various attacks on stream ciphers, e.g. in correlation attacks, distinguishing attacks, resynchronization attacks.
- The group has a very strong publication record and is very visible in the research community. For example, IACR publishes publication statistics (IACR publications) of all ever existing cryptographers (about 3500 cryptographers with IACR publications listed). Thomas Johansson was ranked 83 regarding IACR publications and ranked 14 regarding participation in IACR program committees. PC co-chair in 2012 and 2013 of *Eurocrypt*, Europe's top conference in the area.

The cryptographic research interests has for a many years been targeting cryptographic problems related to coding theory. The leading researchers in the group have their background from a larger information theory group. With the strong connection between LWE-type problems and coding theory, we believe that we have the excellence in this area to produce very strong scientific results in the described project. We intend to publish results in top conferences (IACR conferences and workshops) or good journals like *Journal of Cryptology*, *Designs, Codes and Cryptography* and *IEEE Trans. on Information Theory*.

The applicant has for some years been devoted to administrative duties (deputy Head of department, etc.) and some development work in teaching. For example, in 2014 the applicant had officially 81% administration and teaching duties and 19% research. From January 1, 2015 the applicant has no administrative duties and is expecting to increase research efforts considerably.

4 Preliminary results

As a part of our ongoing VR project, we have received some extraordinary results which form the basis of this application. We mention the paper

Q. Guo, T. Johansson, C. Löndahl, "Solving LPN using covering codes", Asiacrypt 2014.

This paper gives a new algorithm for solving the LPN problem which is the currently best known approach. It received the best paper award on Asiacrypt[3] 2014 (255 submissions). We

[3] Asiacrypt is one of three top conferences in crypto (referred to as an IACR flagship conference)

have also as current work found some further improvements.

For the LWE problem, we have, as described before, some very interesting new ideas from the use of lattice codes to design a new algorithm for solving the general LWE problem. This has been documented in the submitted paper

Q. Guo, T. Johansson, P. Stankovski “Coded-BKW: A New Algorithm for Solving LWE Using Lattice Codes”, submitted to Crypto, 2015.

Regarding the investigation of the security of different primitives, we are publishing an attack on the authentication protocol *Lapin*, which is a recent efficient primitive for constrained devices. The paper is

Q. Guo, T. Johansson, C. Löndahl, "A New Algorithm for Solving Ring-LPN with a Reducible Polynomial", *IEEE Trans. on Info. Theory*, revision required , (http://arxiv.org/pdf/1409.0472.pdf)

5 Equipment

Lund University is very well equipped with the LUNARC cluster of computers. The group regularly uses this cluster for simulation purposes.

6 International collaboration

We have an extensive amount of international collaboration and regular contacts with many leading researchers in the area of symmetric cryptography as well as code-based cryptography. We also have extensive collaboration with industry, in particular Ericsson and Sony, including several joint research projects.

7 Significance

Needless to say, increasing research in data security is a demand you meet almost everywhere. Cryptology is a corner stone in this area and the importance of having strong research in this area cannot be underestimated. Unfortunately, there is not much strong research in crypto in Sweden. In fact, it is much easier to find funding for more applied research in the security area, so we feel that it is important that crypto gets proper funding, or researchers will move to other areas of security where the funding situation is better.

In this project, we look at an area that will be crucial if a large quantum computer is a reality. Even though this might be far away in time for most researchers, its impact on security in our society would be devastating, and thus we cannot ignore the possibility. Primitives based on LWE are also the currently best known way of creating homomorphic encryption, a very attractive feature for future cloud-based information systems. We also mentioned its importance in light-weight crypto, another very important area in future communication systems.

In this context, cryptographic primitives based on LWE are important and attractive. They are to some extent based on problems that have been studied before in lattice literature, but new insights in the difficulty as well as the usefulness of these problems are currently being published at highest rate ever.

References

[1] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. On the complexity of the BKW algorithm on LWE. *Designs, Codes and Cryptography*, pages 1–30, 2013.

[2] Martin R. Albrecht, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. Lazy Modulus Switching for the BKW Algorithm on LWE. In Hugo Krawczyk, editor, *Public-Key Cryptography–PKC 2014*, volume 8383 of *Lecture Notes in Computer Science*, pages 429–445. Springer Berlin Heidelberg, 2014.

[3] Frederik Armknecht, Matthias Hamann, and Vasily Mikhalev. Lightweight authentication protocols on ultra-constrained rfids-myths and facts. In *Radio Frequency Identification: Security and Privacy Issues*, pages 1–18. Springer, 2014.

[4] Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In *Automata, Languages and Programming*, pages 403–415. Springer, 2011.

[5] Anja Becker, Nicolas Gama, and Antoine Joux. A sieve algorithm based on overlattices. *LMS Journal of Computation and Mathematics*, 17(A):49–70, 2014.

[6] Daniel J Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, 2009.

[7] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*, 50(4):506–519, 2003.

[8] Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In *Advances in Cryptology–CRYPTO 2012*, pages 868–886. Springer, 2012.

[9] Zvika Brakerski and Vinod Vaikuntanathan. Efficient Fully Homomorphic Encryption from (Standard) LWE. In *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 97–106. IEEE Computer Society, 2011.

[10] Yuanmi Chen and Phong Q Nguyen. BKZ 2.0: Better lattice security estimates. In *Advances in Cryptology–ASIACRYPT 2011*, pages 1–20. Springer, 2011.

[11] Alexandre Duc, Florian Tramèr, and Serge Vaudenay. Better Algorithms for LWE and LWR. Cryptology ePrint Archive, Report 2015/056, 2015. http://eprint.iacr.org/.

[12] Nicolas Gama, Phong Q Nguyen, and Oded Regev. Lattice enumeration using extreme pruning. In *Advances in Cryptology–EUROCRYPT 2010*, pages 257–278. Springer, 2010.

[13] Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009.

[14] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Advances in Cryptology–CRYPTO 2013*, pages 75–92. Springer, 2013.

[15] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Algorithms for the shortest and closest lattice vector problems. In *Coding and Cryptology*, pages 159–190. Springer, 2011.

[16] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In *Advances in Cryptology–CRYPTO 2011*, pages 447–464. Springer, 2011.

[17] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *Algorithmic number theory*, pages 267–288. Springer, 1998.

[18] Richard Lindner and Chris Peikert. Better Key Sizes (and Attacks) for LWE-Based Encryption. In Aggelos Kiayias, editor, *Topics in Cryptology–CT-RSA 2011*, volume 6558 of *Lecture Notes in Computer Science*, pages 319–339. Springer Berlin Heidelberg, 2011.

[19] Mingjie Liu and Phong Q Nguyen. Solving BDD by enumeration: An update. In *Topics in Cryptology–CT-RSA 2013*, pages 293–309. Springer, 2013.

[20] Rafael Misoczki, J-P Tillich, Nicolas Sendrier, and Paulo SLM Barreto. Mdpc-mceliece: New mceliece variants from moderate density parity-check codes. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2069–2073. IEEE, 2013.

[21] Phong Q Nguyen. Lattice reduction algorithms: Theory and practice. In *Advances in Cryptology–EUROCRYPT 2011*, pages 2–6. Springer, 2011.

[22] Phong Q Nguyen and Damien Stehlé. Low-dimensional lattice basis reduction revisited. *ACM Transactions on Algorithms (TALG)*, 5(4):46, 2009.

[23] Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM*, 56(6):34:1–34:40, September 2009.

[24] Markus Rückert and Michael Schneider. Estimating the security of lattice-based cryptosystems. *IACR Cryptology ePrint Archive*, 2010:137, 2010.

[25] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE, 1994.

[26] David Wagner. A generalized birthday problem. In *Advances in cryptology–CRYPTO 2002*, pages 288–304. Springer, 2002.

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

Coding theory techniques in post-quantum cryptography and cryptanalysis

(dnr 621-2012-4259, 3 year project 2013-2015, 2730 kSEK)

Report of progress during 01/01/2013--31/03/2015

As described as a main idea in the original project plan (2012), we have examined how different techniques and tools in coding theory can be exploited and further developed in the areas of post-quantum cryptography and cryptanalysis of symmetric key ciphers. Some results from prior studies in 2012 are included.

- We have investigated the security of some existing public key cryptography proposals resisting attacks from quantum computers. This includes versions of the code-based public key cryptosystems McEliece PKC. In particular, the recent and very interesting scheme MDPC, allowing a much smaller public key than original McEliece, has been analyzed in the paper ``Squaring Attacks on McEliece Public-Key Cryptosystems using Quasi-Cyclic codes of Even Dimension", accepted for publication in *Designs codes and Cryptography*, 2015. Through the study of the complexity of the underlying problems for many other proposed schemes, we have been able to break proposed parameters for a number of different schemes, moving knowledge in this area forward considerably. We mention the awarded paper ``Solving LPN using covering codes", *Lecture Notes in Computer Science* (Asiacrypt 2014), which is significant for any scheme based on LPN. The paper ``Improved Algorithms for Finding Low-Weight Polynomial Multiples in GF(2)[x] and Some Cryptographic Applications", *Design, Codes and Cryptography*, 2014, presents the best known algorithm for finding low weight multiples of polynomials. In conclusion, we have developed the most efficient algorithms known today for solving the problem of finding low weight multiples of polynomials, the LPN problem, and many other related problems. The complexity of these algorithms determines the necessary parameters when instantiating a certain cryptographic primitive for some fixed security level. Altogether, there are many promising candidates for post-quantum cryptography. We mention the MDPC scheme and LPN-based schemes as top candidates. However, this project has only considered binary oriented problems and moving to q-ary symbols as in the proposed project on LWE opens up new possibilities.
- We have investigated new constructions of public key primitives resisting attacks from quantum computers. A single paper, ``A new version of McEliece PKC based on convolutional codes", *Lecture Notes in Computer Science* (Information and Communications Security 2012) has appeared, but we have some additional preliminary results that might be final during 2015.
- Finally, we have examined how to use techniques from coding theory to improve attacks on symmetric key primitives like stream ciphers. Iterative decoding methods using message passing techniques (as in decoding of LDPC codes) appeared in ``Improved Message Passing Techniques in Fast Correlation Attacks on Stream Ciphers", *Proc. of 7th International Symposium on Turbo Codes and Iterative Information Processing*, 2012. In general, we have taken advantage of coding methods in many of our publications as is evident from their titles. We have used a diversity of different techniques from coding.
- **Exellence of performed research in the project:** The work in the project includes several strong publications in conferences or journals, see below. Since 2005, IACR has introduced the selection of the best paper of each conference. The paper ``Solving LPN using covering codes" was selected the best paper in Asiacrypt 2014 (among 255 submission).
- **PhD students in the project:** During 2013-2014 Carl Löndahl worked in the project. He defended his PhD thesis in February 2015. Since 2014, we have PhD student Qian Guo included in this project. He has been a PhD student since 2013 and is expected to graduate in December 2016 (he already completed most courses when starting).

- **Relation to the new project:** The new project has its main focus on LWE and related problems which are problems using q-ary symbols. For q large the situation is quite different from what has been considered in this project and some typical approaches include lattices and associated theory. The new project do consider also q=2, when LWE becomes LPN, and will be a continuation of the LPN part of this project. With all the exiting new research around LWE, this is the right direction to move our current research.
- **Research resources for the project:** Apart from this VR project, there has only been internal university funding, supporting this project.

Some publications in the project

- C. Löndahl, T. Johansson,``A new version of McEliece PKC based on convolutional codes", *Lecture Notes in Computer Science* ***7618***, 2012, (Information and Communications Security), pp. 461-470.
- M. Ågren, M. Hell, T. Johansson, C. Löndahl, ``Improved Message Passing Techniques in Fast Correlation Attacks on Stream Ciphers", *Proc. of 7th International Symposium on Turbo Codes and Iterative Information Processing*, 2012, pp. 260-264.
- T. Johansson, C. Löndahl, ``A new algorithm for finding low-weight polynomial multiples and its application to TCHo", Preproceedings of WCC 2013, Bergen, Norway, pp.~203--214.
- P. Stankovski, M. Hell, T. Johansson, ``An Efficient State Recovery Attack on the X-FCSR Family of Stream Ciphers", J*ournal of Cryptology*, Vol. 27, No. 1, 2014, pp. 1-22.
- C. Löndahl, T. Johansson, ``Improved Algorithms for Finding Low-Weight Polynomial Multiples in GF(2)[x] and Some Cryptographic Applications", *Design, Codes and Cryptography*, Vol. 73, No. 2, 2014, pp. 625-640.
- Q.Guo, T. Johansson, C. Löndahl, ``Solving LPN using covering codes", *Lecture Notes in Computer Science* **8873**, 2014, (Asiacrypt 2014), pp.~1-20.
- H. Wang, P. Stankovski, T. Johansson, ``A generalized birthday approach for efficiently finding linear relations in l-sequences",
  Designs, Codes and Cryptography, Vol. 74, No. 1, 2015, pp. 41-57.
- C. Löndahl, T. Johansson, M. Koochak Shooshtari, M. Ahmadian-Attari, M. Reza Aref, ``Squaring Attacks on McEliece Public-Key Cryptosystems using Quasi-Cyclic codes of Even Dimension", accepted for publication in *Designs codes and Cryptography*, 2015.
- Q. Guo, T. Johansson, C. Löndahl,
  ``A New Algorithm for Solving Ring-LPN with a Reducible Polynomial", *IEEE Trans. on Info. Theory*, revision required.

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	Thomas Johansson	20
2	Other personnel without doctoral degree	ny doktorand	80
3	Other personnel with doctoral degree	postdoc	50

Salaries including social fees

	Role in the project	Name	Percent of salary	2016	2017	2018	2019	Total
1	Applicant	Thomas Johansson	5	63,000	65,000	67,000	69,000	264,000
2	Other personnel without doctoral degree	ny doktorand	80	418,000	431,000	444,000	457,000	1,750,000
3	Other personnel with doctoral degree	PostDoc	50	364,000	374,000	386,000	397,000	1,521,000
	Total			845,000	870,000	897,000	923,000	3,535,000

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

Running Costs

	Running Cost	Description	2016	2017	2018	2019	Total
1	Resekostnader		50,000	50,000	50,000	50,000	200,000
	Total		50,000	50,000	50,000	50,000	200,000

Depreciation costs

Depreciation cost	Description	2016	2017	2018	2019

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	845,000	870,000	897,000	923,000	3,535,000		3,535,000
Running costs	50,000	50,000	50,000	50,000	200,000		200,000
Depreciation costs					0		0
Premises					0		0
Subtotal	895,000	920,000	947,000	973,000	3,735,000	0	3,735,000
Indirect costs	411,000	418,000	425,000	432,000	1,686,000		1,686,000
Total project cost	1,306,000	1,338,000	1,372,000	1,405,000	5,421,000	0	5,421,000

Explanation of the proposed budget

Briefly justify each proposed cost in the stated budget.

Explanation of the proposed budget*

The project involves the applicant as supervisor, a new PhD student, and a partial support for a postdoc position. We know of several good postdoc candidates, both internationally and internally (e.g. Qian Guo, who will graduate during 2016).

We ask for partial support 5% of full time for the supervisor (but he is at least 20% active in the project, the remaining part supported from faculty funding) and full support 80% of full time for a new PhD student to work in the project.
For the postdoc we ask for partial support 50% of full time as we intend to use the postdoc also in another project. In case the full budget is not approved, we will lower the postdoc part in the project. Finally, we ask for partial support for travel costs for conference visits related to this project, 50 kSEK per year.

The amount for salary is computed using existing salary for the applicant and our university model for salaries for employed PhD students and postdocs, including social fees (LKP). The university overhead for Dept of EIT/LTH is adding another 46% in indirect 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

CV and publications

CV

Curriculum Vitae of Thomas Johansson,

March 2015

Personal data

Name	Thomas Johansson
Work address	Department of Electrical and Information Technology, Lund University, Box 118, SE-221 00 Lund, Sweden Phone: (46) 46 2223182, Fax: (46) 46 2224714, E-mail: thomas@eit.lth.se, Web: http://www.eit.lth.se/index.php?uhpuid=hs.tjo
Home address	Lögarekroken 13, SE-247 51 Dalby, Sweden
Born	Ljungby, Sweden, September 1, 1967

VR bullets:

1. [Degree] Master of Science in Computer Science and Engineering, Lund University, January 1990.

2. [PhD degree] Doctor of Philosophy in Engineering, Information Theory, Lund University, December 1994, PhD thesis: Contributions to unconditionally secure authentication (supervisor Ben Smeets).

3. [Postdoc visits] Shorter visits at Isaac Newton Institute, Cambridge, England 1996, and Dept. of Informatics, Bergen, Norway 1997.

4. [Docent degree] Docent (Swedish degree) in Information Technology, June 1999.

5. [Employment] Professor, Dept. of Electrical and Information Technology, Lund University, permanent employment, 19% research 2014 and 60% research 2015.

6. [Previous employments]
PhD student, Dept. of Information Theory, Lund University, 1990–1995.
Acting associate professor, Dept. of Information Technology, Lund University, 1995–1996.
Associate professor, Dept. of Information Technology, Lund University, 1997–2000.
Professor, Dept. of Information Technology (now Dept of EIT), Lund University, 2000-

7. [Absence from research] No longer absence from research.

8. [Graduated PhD students] Main supervisor for Dr. Fredrik Jönsson (2002), Dr. Enes Pasalic (2003), Dr. Patrik Ekdahl (2003), Dr. Alexander Maximov (2006), Dr. Martin Hell (2007), Dr. Håkan Englund (2007), Dr. Martin Ågren 2012, Dr. Paul Stankovski 2013, Dr. Carl Löndahl 2015, postdoc Dr. Sushmita Ruj, India 2009, [second supervisor for Dr. Elmar Trojer (Austria, 2004), Dr. Quchin Wang (China 2011), Dr. Hui Wang (China 2012)].

Teaching, administration etc.

Main responsibility for undergraduate courses,
Data network 94/95–97/98, Cryptography 95/96–14/15,
Information Theory 98/99, Data Security 00/01–01/02,
Mathematical cryptology 04/05–13/14. Design of Digital Circuits 13/14-14/15
Main responsibility for graduate course,
Cryptology 99/00, 04/05.
Participation in an education program on teaching and supervising,
"Kurs for blivande docenter".

Director of Graduate Studies, Dept. of Information Technology, 2006–2007.
Vice Head of Department (stf prefekt), Dept. of Information Technology, 2003–2007.
Deputy Head of Department (biträdande prefekt), Dept. of EIT, 2009–2014.

Research

The main research interests are all aspects of cryptography and coding, especially symmetric cryptography and topics that relate cryptography to information theory and coding.

I have served as program co-chair for Eurocrypt 2012 and 2013, Europe's top conference in the area., program chair for FSE 2003 and program co-chair for Indocrypt 2003.

I have additionally served on the following program committees: Crypto 2008, Crypto 2015, Eurocrypt'98, Eurocrypt 2000, Eurocrypt 2001, Eurocrypt 2002, Eurocrypt 2004, Eurocrypt 2009, Asiacrypt 2005, Asiacrypt 2007, Asiacrypt 2009, Asiacrypt 2010, FSE 2001, FSE 2002, FSE 2004, FSE 2005, FSE 2006, FSE 2007, FSE 2008, FSE 2010, SAC 2006, SAC 2009, SAC 2011 Indocrypt 2000, Indocrypt 2001, Indocrypt 2004, Indocrypt 2011, ACISP 2004, ICISC 2004, CANS 2005, SETA 2006, SETA 2010, Workshop on Coding and Cryptography in 2001, 2003, and 2005, 2007, 2009, 2015 Nordsec 2006, IEEE Symposium on Information Theory 2008, RSA Conference CT 2015.

I was Associate Editor for *IEEE Trans. on Information Theory* 2002–2005 and *IEEE Trans. on Information Forensics and Security* 2005–2007. I have had further editorial responsibilities in some additional journals. From 2015 I am editor for *Cryptography and Communications, Discrete Structures, Boolean Functions and Sequences.*

Best paper awards on Asiacrypt 2014 for the paper "Solving LPN using covering codes" (255 submissions) and shared best paper on Asiacrypt 2008 for the paper "Breaking the F-FCSR-H Stream Cipher in Real Time" (208 submissions). Also, the paper "An efficient state recovery attack on X-FCSR-256" was selected «among best three papers» on FSE 2009. Invited speaker at many occasions, e.g., FSE 2014, WCC 2007, RSA Security Japan.

Recipient of the SSF Junior Individual Grant in 2000.

Participation in a number of research evaluation boards. In 2011-2012 I participated in a board evaluating all ICT research in Norway. Participated in 2013-2014 in Swedish Research Council evaluation panel "Signals and Systems" and in 2014 in evaluation panel "ICT framework program".

Publications

I have published about 75 full papers either in journals or in books (Springer's Lecture Notes in Computer Science series). In addition, I have published a number of conference contributions.

In Google Scholar, I have 3667 citations, my h-index is 34. I have 12 papers with more than 100 citations. The full publication list is publicly available on Google's My Citations.

Publication list

Database: Google scholar

SCIENTIFIC OUTPUT LAST 8 YEARS

Original papers:

1. M. Hell, T. Johansson, "On the problem of finding linear approximations and cryptanalysis of Pomaranch Version 2", *Lecture Notes in Computer Science* **4356**, 2007, (SAC 2006), pp. 220-234. Number of citations: 6
2. H. Englund, T. Johansson, M. Hell, " Two General Attacks on Pomaranch-like Keystream Generators ", *Lecture Notes in Computer Science* **4593**, 2007, (FSE 2007), pp. 274–289. Number of citations: 7
3. H. Englund, T. Johansson, M. Sönmez Turan, " A framework for chosen IV statistical analysis of stream ciphers", *Lecture Notes in Computer Science* **4859**, 2007, (Indocrypt 2007), pp. 268–281. Number of citations: 87
4. M. Hell, T. Johansson, "A key recovery attack on Edon80 ", *Lecture Notes in Computer Science* **4833**, 2007, (Asiacrypt 2007), pp. 568–582. Number of citations: 4
5. A. Maximov, T. Johansson, "A linear distinguishing attack on Scream", *IEEE Trans. on Info. Theory*, vol 53, no. 9, 2007, pp. 3127–3144. Number of citations: 9
6. M. Hell, T. Johansson, "Cryptanalysis of Achterbahn-128/80 ", *IET Information Security*, vol. 1, no. 2, 2007, pp. 47-52. Number of citations: 9
7. M. Hell, T. Johansson, W. Meier "Grain - A stream cipher for constrained environments ", *International Journal of Wireless and Mobile Computing*, vol. 2, no. 1, 2007, pp. 86-93. Number of citations: 240
8. M. Hell, T. Johansson, "Breaking the F-FCSR-H Stream Cipher in Real Time ", *Lecture Notes in Computer Science* **5350**, 2008, (Asiacrypt 2008), pp 557–569. Number of citations: 46
9. The Grain Family of Stream Ciphers, M Hell, T Johansson, A Maximov, W Meier *Lecture Notes In Computer Science* **4986**, 2008, New Stream Cipher Designs: The eSTREAM Finalists, pp. 179–190. Number of citations: 104
10. M. Hell, T. Johansson, L. Brynielsson, "An overview of distinguishing attacks on stream ciphers", *Cryptography and Communications*, Vol. 1, No. 1, pp. 71-94, 2009. Number of citations: 21
11. M. Ågren, T. Johansson, M. Hell, "Improving the rainbow attack by reusing colours", *Lecture Notes in Computer Science* **5888**, 2009, (CANS 2009), pp. 362–378. Number of citations: 3
12. P. Stankovski, M. Hell, T. Johansson, "An efficient state recovery attack on X-FCSR-256", *Lecture Notes in Computer Science* **5665**, 2009, (FSE 2009), pp. 23–37. Number of citations: 15
13. Q. Wang, T. Johansson, "A note on fast algebraic attacks and higher order nonlinearities", *Lecture Notes in Computer Science* **6584**, 2011, (INSCRYPT 2010), pp. 404–414. Number of citations: 25
14. Q. Wang, T. Johansson, "On equivalence classes of Boolean functions", *Lecture Notes in Computer Science* **6829**, 2011, (ICISC 2010), pp. 311–324. Number of citations: 1

15. M. Hell, T. Johansson, “Breaking the stream ciphers F-FCSR-H and F-FCSR-16 in real time”, *Journal of Cryptology*, Vol. 24, No. 3, pp. 427-445, 2011. Number of citations: 15

16. M. Ågren, T. Johansson, “Linear cryptanalysis of PRINTcipher?trails and samples everywhere”, *Lecture Notes in Computer Science* **7107**, 2011, (INDOCRYPT 2011), pp. 114-133.

17. M. Ågren, M. Hell, T. Johansson, W. Meier, “Grain-128a: a new version of Grain-128 with optional authentication”, *International Journal of Wireless and Mobile Computing*, Vol. 5, No. 1, pp. 48-59, 2011. Number of citations: 43

18. M. Hell, T. Johansson: “Linear Attacks on Stream Ciphers” *Advanced Linear Cryptanalysis of Block and Stream Ciphers/Cryptology and Information Security Series*, pp. 55-85, ISBN 978-1-60750-843-4, IOS Press, 2011. Number of citations: 1

19. Q. Wang, T. Johansson, H. Kan, “Some results on fast algebraic attacks and higher-order non-linearities”, *IET Information Security*, Vol. 6, No. 1, pp. 41-46, 2012. Number of citations: 4

20. M. Ågren, C. Löndahl, M. Hell, T. Johansson, “A Survey on Fast Correlation Attacks”, *Cryptography and Communications*, Vol. 4, No. 3-4, pp. 173-202, 2012. Number of citations: 1

21. M. Hell, T. Johansson, L. Brynielsson, H. Englund, “Improved Distinguishers on Stream Ciphers with Certain Weak Feedback Polynomials”, *IEEE Transactions on Information Theory*, Vol. 58, No. 9, pp. 6183-6193, 2012. Number of citations: 1

22. M. Ågren, M. Hell, T. Johansson, “On Hardware-Oriented Message Authentication”, *IET Information Security*, Vol. 6, No. 4, pp. 329-336, 2012. Number of citations: 0

23. P. Stankovski, S. Ruj, M. Hell, T. Johansson, “Improved distinguishers for HC-128”, *Designs, Codes and Cryptography*, Vol. 63, No. 2, pp. 225-240, 2012. Number of citations: 9

24. P. Stankovski, M. Hell, T. Johansson, “Analysis of Xorrotation With Application to an HC-128 Variant”, *Lecture Notes in Computer Science* **7372**, 2012, (ACISP 2012), pp. 419–425. Number of citations: 2

25. C. Löndahl, T. Johansson, “A new version of McEliece PKC based on convolutional codes”, *Lecture Notes in Computer Science* **7618**, 2012, (Information and Communications Security), pp. 461–470. Number of citations: 7

26. H. Wang, M. Hell, T. Johansson, M. Ågren, “Improved Key Recovery Attack on the BEAN Stream Cipher”, *IEICE Transactions*, Vol. E96A, No. 6, 2013, pp. 1437-1444. Number of citations: 2

27. P. Stankovski, M. Hell, T. Johansson, “An Efficient State Recovery Attack on the X-FCSR Family of Stream Ciphers”, *Journal of Cryptology*, Vol. 27, No. 1, 2014, pp. 1-22. Number of citations: 1

28. C. Löndahl, T. Johansson, “Improved Algorithms for Finding Low-Weight Polynomial Multiples in GF(2)[x] and Some Cryptographic Applications”, *Design, Codes and Cryptography*, Vol. 73, No. 2, 2014, pp. 625-640. Number of citations: ? **(*)**

29. Q.Guo, T. Johansson, C. Löndahl, “Solving LPN using covering codes”, *Lecture Notes in Computer Science* **8873**, 2014, (Asiacrypt 2014), pp. 1–20. (solicited for publication in *Journal of Cryptology*) . Number of citations: 1 **(*)**

30. H. Wang, P. Stankovski, T. Johansson, "A generalized birthday approach for efficiently finding linear relations in l-sequences", *Designs, Codes and Cryptography*, Vol. 74, No. 1, 2015, pp. 41-57. Number of citations: 1

31. C. Löndahl, T. Johansson, M. Koochak Shooshtari, M. Ahmadian-Attari, M. Reza Aref, "Squaring Attacks on McEliece Public-Key Cryptosystems using Quasi-Cyclic codes of Even Dimension", accepted for publication in *Designs codes and Cryptography*, 2015. Number of citations: ? **(*)**

Refereed contributions at international conferences and workshops:

- H. Englund, M. Hell, T. Johansson, "A note on distinguishing attacks", IEEE Information Theory Workshop on Information Theory for Wireless Networks, Bergen, Norway, pp. 87-90, 2007. Number of citations: 22
- T. Johansson, A. Trofimov, "One-sweep APP decoding algorithm for binary block codes with reduced trellis memory", Proceedings of coding theory days in St.Petersburg, pp. 88-93, 2008-10-06/2008-10-10. Number of citations: ?
- M. Ågren, M. Hell, T. Johansson: On Hardware-Oriented Message Authentication with Applications Towards RFID 2011 Workshop on Lightweight Security & Privacy: Devices, Protocols, and Applications, LightSec 2011, Istanbul, Turkey, pp. 26-33, 2011-03-14/2011-03-15. Number of citations: 10
- M. Ågren, M. Hell, T. Johansson, W. Meier: A New Version of Grain-128 with Authentication Symmetric Key Encryption Workshop 2011, Lyngby, Denmark, 2011-02-16/2011-02-17. Number of citations: 27
- M. Ågren, M. Hell, T. Johansson, C. Löndahl, "Improved Message Passing Techniques in Fast Correlation Attacks on Stream Ciphers", Proc. of 7th International Symposium on Turbo Codes and Iterative Information Processing, 2012, pp. 260-264. Number of citations: 2 **(*)**
- M. Leonardo A, Z. Albin, B. Smeets, H. Sheikh M., T. Johansson, S. Nahid: Privacy, Security and Trust in Cloud Computing: The Perspective of the Telecommunication Industry The Third International Symposium on Multidisciplinary Emerging Networks and Systems (MENS 2012), Fukuoka, Japan, 2012-09-04/2002-09-07. Number of citations: 8
- T. Johansson, C. Löndahl, "A new algorithm for finding low-weight polynomial multiples and its application to TCHo", Preproceedings of WCC 2013, Bergen, Norway, pp. 203–214. Number of citations: ? **(*)**

Books

- David Pointcheval, Thomas Johansson (Eds.), Proc. of Eurocrypt 2012, *Lecture Notes in Computer Science* **7237**, Berlin: Springer-Verlag, 2012. Number of citations: 25
- T. Johansson, N. Phong Q.: Advances in Cryptology – EUROCRYPT 2013 ISBN 978-3-642-38348-9, 2013. Number of citations: 16

Most cited papers by Thomas Johansson:

- P. Ekdahl, T. Johansson, "A new version of the stream cipher SNOW", *Lecture Notes in Computer Science* **2595** (2002), Berlin: Springer-Verlag, (SAC 2002), pp.47–61. Number of citations: 241
- M. Hell, T. Johansson, W. Meier "Grain - A stream cipher for constrained environments ", *International Journal of Wireless and Mobile Computing*, vol. 2, no. 1, 2007, pp. 86-93. Number of citations: 240
- T. Johansson, F. Jönsson, "Improved fast correlation attacks on stream ciphers via convolutional codes", *Lecture Notes in Computer Science* **1592** (1999), Berlin: Springer-Verlag, (EUROCRYPT'99), pp. 347–362. Number of citations: 184
- V. Chepyshov, T. Johansson, B. Smeets, "A simple algorithm for fast correlation attacks on stream ciphers", *Lecture Notes in Computer Science* **1978** (2000), Berlin: Springer-Verlag,(Fast Software Encryption Conference 2000), pp. 181–195. Number of citations: 143
- T. Johansson, F. Jönsson, "Fast correlation attacks through reconstruction of linear polynomials", *Lecture Notes in Computer Science* **1880** (2000), Berlin: Springer-Verlag, (Crypto 2000), pp. 300–315. Number of citations: 137

Thomas Johansson's h-index: 34

CV

Name: Thomas Johansson	**Doctorial degree:** 1994-12-09
Birthdate: 19670901	**Academic title:** Professor
Gender: Male	**Employer:** Lunds universitet

Research education

Dissertation title (swe)

Contributions to Unconditionally Secure Authentication

Dissertation title (en)

Contributions to Unconditionally Secure Authentication

Organisation	Unit	Supervisor
Lunds universitet, Sweden Sweden - Higher education Institutes	Dept of Information Theory	Ben Smeets

Subject doctors degree	ISSN/ISBN-number	Date doctoral exam
20203. Kommunikationssystem	91-7167-004-1	1994-12-09

Publications

Name: Thomas Johansson	**Doctorial degree:** 1994-12-09
Birthdate: 19670901	**Academic title:** Professor
Gender: Male	**Employer:** Lunds universitet

Johansson, Thomas 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.