

THESIS FOR THE DEGREE OF LICENTIATE OF ENGINEERING

# Cryptographic Tools for Privacy Preservation and Verifiable Randomness

CARLO BRUNETTA



Division of Network and System  
Department of Computer Science & Engineering  
Chalmers University of Technology and Gothenburg University  
Gothenburg, Sweden, 2018

# Cryptographic Tools for Privacy Preservation and Verifiable Randomness

CARLO BRUNETTA

Copyright ©2018 Carlo Brunetta  
except where otherwise stated.  
All rights reserved.

Technical Report No 188L  
ISSN 1652-876X  
Department of Computer Science & Engineering  
Division of Network and System  
Chalmers University of Technology and Gothenburg University  
Gothenburg, Sweden

This thesis has been prepared using L<sup>A</sup>T<sub>E</sub>X.

Printed by Chalmers Reproservice,  
Gothenburg, Sweden 2018.

*“Whoever controls the media, controls the mind.”*  
(UNSOURCED) - *James Douglas Morrison*



# Abstract

Our society revolves around communication. The Internet is the biggest, cheapest and fastest digital communication channel used nowadays. Due to the continuous increase of daily communication among people worldwide, more and more data might be stolen, misused or tampered. We require to protect our communications and data by achieving *privacy and confidentiality*.

Despite the two terms, “*privacy*” and “*confidentiality*”, are often used as synonymous, in cryptography they are modelled in very different ways. Intuitively, cryptography can be seen as a tool-box in which every scheme, protocol or primitive is a tool that can be used to solve specific problems and provide specific communication security guarantees such as confidentiality. Privacy is instead not easy to describe and capture since it often depends on “*which*” information is available, “*how*” are these data used and/or “*who*” has access to our data.

This licentiate thesis raises research questions and proposes solutions related to: the possibility of defining encryption schemes that provide both strong security and privacy guarantees; the importance of designing cryptographic protocols that are compliant with real-life privacy-laws or regulations; and the necessity of defining a post-quantum mechanism to achieve the verifiability of randomness.

In more details, the thesis achievements are:

- (a) defining a new class of encryption schemes, by weakening the correctness property, that achieves Differential Privacy (DP), *i.e.*, a mathematically sound definition of privacy;
- (b) formalizing a security model for a subset of articles in the European General Data Protection Regulation (GDPR), designing and implementing a cryptographic protocol based on the proposed GDPR-oriented security model, and;
- (c) proposing a methodology to compile a post-quantum interactive protocol for proving the correct computation of a pseudorandom function into a non-interactive one, yielding a post-quantum mechanism for verifiable randomness.

## Keywords

Cryptography, Confidentiality, Privacy, Differential Privacy, GDPR, Verifiable Randomness



---

## Acknowledgment

---

I would like to thank **Katerina**. We may have had some issues in the beginning but we manage to solve them. Without you I would not be here. Thank you for giving me this opportunity to grow as a human and as a researcher.

Thank you to all the people in **my division**, Network and System, for sharing the good and bad moments of the daily work. I would really love to thank all the **administration** “**moms and dads**” for **all the support** that they give me either if it’s “*work related*” or “*it’s a blue day*”. **Tack <3**

A big thank you to the uncountable number of **friends** that crossed my life here in Chalmers. Thank you for all the good fika, the beers and the infinite discussions.

I would love to thanks all my Sahlgrenska’s real-science friends such as **Tugce, Lydia, Jasmine, Eleni, Axel, Giacomo and many more** for the good moments outside the Chalmers walls!

Thank you, **Bei and Georgia**, for the research discussions and shared funny moments. I am open to continue our future collaborations and our friendship!

A special thank you goes to **Pablo, Lara and Oliver**. I wish you all the best, always!

We shared a lot and we changed the band-name a lot of times. Thank you **Marco, Enzo, Pier, Evgenii and Grischa** for all the good bohemian-moments and the jams. You are like a family to me and even if we will have to split, our band will always be a beautiful memory in my music-career. I think that “*Band with Many Names*” is the best name we had!

A heart-*grazie* goes to **Elena**. You mean a lot to me and you were here, next to me in my *crazy journey*. I’m really lucky to know you and call you a Friend. I will always be grateful to you and I hope the best for you, anywhere on Earth. (==)

I know I shouldn’t cite you if there’s not a good impact-factor but thank you, **Eridan!** “*Rolling From Teh Kitchen*” is my family. Glad to have you in it :)

Looking forward to all the pizzas, films and tv-series!

My biggest thank you goes to my love, **Aura**. You are my precious “*stella alpina*”. *You are the reason of my smiles and, to me, that is all that matters in life.*

A big thank you to all the rest of the people that might, or not, be present in this too-small page. *No-margin will be able to contain you all!* I think this Pink Floyd quote from *Breathe* can explain what I think about all of you in my daily R-life:

All you touch and all you see,  
is all your life will ever be.

---

BREATHE - *Dark Side of the Moon*  
Pink Floyd



### Appended publications

This thesis is based on the following publications:

- Paper A:** C. Brunetta, C. Dimitrakakis, B. Liang, and A. Mitrokotsa  
“A Differentially Private Encryption Scheme”  
*20-th Information Security Conference (ISC), 2017, Ho Chi Minh city (Viet Nam)*. Springer, LNCS, Vol. 11124, 2017, pg. 309–326. [11]
- Paper B:** E. Pagnin, C. Brunetta, P. Picazo-Sanchez  
“HIKE: Walking the Privacy Trail”  
*17th International Conference on Cryptology And Network Security (CANS), 2018, Naples (Italy)*. Springer, LNCS, Vol. 10599, 2018, pg. 43–66 [62]
- Paper C:** C. Brunetta, B. Liang, and A. Mitrokotsa  
“Lattice-Based Simulatable VRFs: Challenges and Future Directions”  
*1st Workshop in the 12th International Conference on Provable Security (PROVSEC), 2018, Jeju (Rep. of Korea)*.  
To appear in *Journal of Internet Services and Information Security*, Vol. 8, No. 4 (November, 2018). [12]

## Other publications

The following publications were published during my PhD studies, or are currently under submission. However, they are not appended to this thesis.

- (a) **C. Brunetta**, M. Calderini, and M. Sala  
“On hidden sums compatible with a given block cipher diffusion layer”  
*Discrete Mathematics (Journal)*, Vol. 342 Issue 2, 2018 [[10](#)]
- (b) **C. Brunetta**, B. Liang, and A. Mitrokotsa  
“Strong Functional Signature”  
*Under submission*

## Research Contribution

In Paper A, I was involved in the initial brainstorming with Katerina and Christos who proposed me the idea of including differential privacy in the cryptographic domain. I had the idea of relaxing the correctness property of an encryption scheme, the key-idea that allows to define differentially private encryption schemes. I further formalized, defined and proved all the contents of the paper. In the final stage, I wrote the implementation and the statistical tests.

In Paper B, after many fruitful morning-fika and brainstorming with Elena and Pablo (and Oliver!), we all together traced the main structure and motivation for the HIKE protocol. During the development of the paper, I was the relay figure for the translation between theory and implementation. More specifically, I wrote the draft of some proofs and I was responsible for the theoretical aspects necessary for the implementation. Finally, I am the corresponding author of this work and I finalised the camera ready version.

In Paper C, I participated to the initial brainstorming discussion with Bei and Katerina after Bei's suggestion on the specific topic of constructing a post-quantum verifiable Pseudo Random Function. I completely wrote the first draft of the paper. After receiving some useful external feedback on the paper, I participated in finding different possible solutions while Bei and Katerina revised the draft. In this final and much shorter version, I conceived the summary of the entire research-exploration and I was responsible for the introduction-background sections of the final paper.



---

## Thesis Contents

---

<b>Abstract</b>	<b>v</b>
<b>Acknowledgement</b>	<b>vii</b>
<b>List of Publications</b>	<b>ix</b>
<b>Personal Contribution</b>	<b>xi</b>
<b>From Caves to the Internet: Privacy and Cryptography</b>	<b>1</b>
1 Sketchy 3-Sets-Data Privacy Model . . . . .	4
2 The Thesis' Contributions . . . . .	10
<b>Paper A - A Differentially Private Encryption Scheme</b>	<b>15</b>
1 Introduction . . . . .	18
2 Preliminaries . . . . .	22
3 Our Definition of $\alpha_{m_1, m_2}$ -correct Encryption Scheme . . . . .	23
4 Equality Between DP-then-Encrypt and Encrypt+DP . . . . .	28
5 Example of an $\alpha_{m_1, m_2}$ -Correct Homomorphic Encryption Scheme . . . . .	31
6 Conclusions & Future Work . . . . .	34
<b>Paper B - HIKE: Walking the Privacy Trail</b>	<b>37</b>
1 Introduction . . . . .	40
2 Preliminaries . . . . .	42
3 Labelled Elliptic-curve ElGamal (LEEG). . . . .	45
4 FEET: Feature Extensions to LEEG . . . . .	48
5 The HIKE protocol . . . . .	51
6 Security model and proofs for HIKE . . . . .	54
7 Implementation details and results . . . . .	59
8 Conclusions and directions for future work . . . . .	61
<b>Paper C - Lattice-Based Simulatable VRFs: Challenges and Future Directions</b>	<b>65</b>
1 Introduction . . . . .	68
2 Applying Lindell's Transformation . . . . .	70
3 Translation of Boneh's PRF . . . . .	76
4 Challenges and Future Directions . . . . .	79
<b>Bibliography</b>	<b>83</b>



---

## From Caves to the Internet: Privacy and Cryptography

---

Who are you? Why do you hide in the  
darkness and listen to my private thoughts?

---

ROMEO AND JULIET  
*William Shakespeare*

We are more than animals. We are **social animals** [43] who need to communicate, socialize and share our feelings, thoughts and ideas to others. Our *communication methods* evolved during our history and from primitive languages and abstract-paintings, we now use “*advanced*” languages and complex technologies that allow us to feel “*closer*” to other people that are not physically close to us.

Nowadays, our life is becoming more and more **digital** and the Internet is the biggest channel we use to communicate by using e-mails, social networks, blogs, instant messaging, video-calls and many others. Digital communication is *cheap*, *fast* and *practical* for the standard user: sending an email to someone on the other side of the world is just a matter of typing the words on a keyboard, clicking on the “*send*” button and almost instantaneously the email is sent and received.

*What does “digital” mean?*

Whenever we write an email, our thoughts are translated into words, and the words are typed into a keyboard which *encode* them into something easier to transmit. For this reason, the digital-world is dominated by discrete and finite sets of **symbols**, for example the **alphabet** in any latin-derived language. There is a finite amount of symbols that are composed in order to create words of which we, as humans, give a special meaning.

One of these finite alphabets is the *binary-set* with only the symbols 0 and 1. Claude Shannon gave a name to the symbols in this set: the **bits**. By combining bits, we obtain bit-strings and with these, we can just encode our previous latin-alphabet into bit-strings and share these 0s and 1s. It is possible to encode *everything* into a bit-string and facilitate its employment into technologies since only two different symbols are transmitted and not, for example, 26 latin-letters! For this and other reasons, the bit is **the** building block of *Information*

*Theory* [73], the mathematical field that, briefly, studies how information is exchanged during communication. A more tangible physical result of information theory is the **computer** as the “*automatic bits machine*” which is able to manipulate, communicate and use pieces of information encoded into bit-strings.

We love computers. They make our life easier and allow us to digitally communicate with anybody at any time. Research on computers is evolving into new directions and one the most promising and breakthrough ideas is building a **quantum computer**, based on **quantum bits, or qubits**. As the name suggests, *a quantum computer is still a computer but with something more*. Quantum computers are expected to offer the biggest performance boost in the history of technology and break the computational limits of current computers. Even if there is not yet any practical quantum computer, different quantum algorithms are ready to be deployed having a strong impact in mathematics, cryptography and many other fields. In particular, Shor’s [74] and Grover’s [40] algorithms will make possible to break down the security of some well-known cryptographic primitives used in our daily life in order to protect our bank accounts or emails. The primitives that will remain secure even when a quantum computer will be used, belong to what is called **post-quantum cryptography**.

*Why should we care about security?*

Everyone of us has at least one secret. Maybe it is our PIN code for the credit-card, the password for the email account, our health condition or anything that we do not want to share with *too many people*. Secrets are important in personal relationships in the sense that if I want to share with a friend a small piece of information that I want to keep secret, then, **trust** is needed. In other words, I need **confidentiality** guarantees.

It might sometimes be implicit, but we are used to require *privacy* or *confidentiality* when interacting with other people or computers. Is it practical to require “*secure communications*” or to ask “*keep it confidential!*”?

But, *what does it mean? What is privacy and confidentiality?*  
*What does “secure communication” mean?*

Historically, **cryptography** is a *tool-set* that allows us to protect our sensitive information and communications [67]. Cryptography evolved around the concept of **confidentiality** of a message and **security** of a communication channel. At the basic level, confidentiality and security *guarantee* that *only authorized* people can obtain the message and access its authentic contents. With a picturesque metaphor, we can think of cryptography as *locks and keys* that can be used to lock the chests that contain our gold coins. We know that a *specific key* will open the chest and *we will allow* a friend to open the chest by providing him/her the key. Therefore, *confidentiality is the guarantee* that the lock is so well-made and designed that no *pirate* can open the locked chest **or** deduce

the amount of coins in the chest without having access to the key. Nowadays, cryptography is not made with chests, locks and keys. Cryptography is based on mathematics, functions, bits and it is widely used on a daily basis for all the *sensitive* digital communication we have such as managing our bank accounts, browsing the Internet, storing our health test results, messaging with a friend or in other scenarios not so obvious, *e.g.*, in cars, public transportation, etc.

Cryptography has a pretty neat distinction between *secret* and *public* information, so neat that a piece of information cannot be both secret and public at the same time. This concept is quite old, tracing back to the ancient Greece. Aristotle, a 4th-century B.C. philosopher and scientist, wrote a collection of political-philosophical books titled “Πολιτικά” or “*Politics*”. In this collection, Aristotle explained the need for every politician to a neat separation between the public sphere called πόλις, or “*polis*”, related to the personal political-life, and a personal sphere called οἶκος, or “*oikos*”, that contains the family-life.

Aristotle’s idea was the starting concept that developed into **privacy**. Since his initial spheres’ distinction, the concept of privacy evolved in our **society and technology** and it can be considered as a **modern** human invention. In 1890, the journal Harvard Law Review contains a law review titled “*The Right To Privacy*” that expresses the need of laws that can protect the “*right to be alone*”. At the time, letters were read by post-employees and/or phones were easily eavesdropped or wiretapped. The World Wars moved even further the necessity to confidential military communication **but** governments started profiling, identifying and threatening individual people. The *mass surveillance* phenomenon was rising.

Society, as a whole, has managed to take a strong turn and today, we consider privacy as a form of a **personal-right** of an individual to selectively express, share information or seclude themselves from the others. In other words, the **right of privacy** is the human unconditional action of protecting and hiding chosen information to other entities. This means that no one, without the personal permission of an individual, can use, read, store or sell that information. One of the biggest examples of legislative documents, on human’s privacy-rights, is the European General Data Protection Regulation (GDPR) [18], focusing on the right of any European citizen to maintain his/her privacy over the data he/she generates.

Our digitalized society **requires** privacy, confidentiality and security.

Every day, our data are generated by our devices, such as our own **digital fingerprints**, stored in big companies servers and used to generate better services, advertising and **help** us in our daily life. Data are the *fuel* of our markets **but** can be used against us. *Information is the Power and the Weapon of our digital-era*. Our contemporary history shows us the personal damage that can be done when bigger IT-companies, like Facebook [38], or governmental security agencies, like the NSA [39], abuse their information-power. For this reason, societies start

raising questions and the will of achieving the right to be safe intellectually and to protect their own identity by asking:

*Can we protect our data? How can we use cryptography to achieve privacy?  
How is privacy related to confidentiality?*

In this licentiate thesis, I address these questions and provide some concrete *cryptographic tools* that can be deployed in real-life to protect our data.

## 1 Sketchy 3-Sets-Data Privacy Model

Confidentiality and privacy are similar concepts when considered into the Aristotle's sphere distinction between *private* and *public* information and they are commonly synonymous in our daily discussions with friends. They are indeed *interconnected* **however** there are substantial differences. In order to explain *how* privacy and cryptography differ, let us describe and explain a simplistic model that represent our data and their properties.

Firstly, let us define an order  $<$  to compare different data and their “**publicity**”. For example, let us consider the information  $x = \text{“Carlo is a PhD student”}$  and  $y = \text{“Carlo’s credit-card PIN is 1111”}$ . It is pretty clear that  $x$  is *more public* with respect to  $y$ , therefore we can denote it with  $x < y$ . Even if sometimes it is easy to decide how to order two pieces of information, it is required to state the axiom:

**Informal Axiom 1.** *The order  $<$  is **not-objective**, in the sense that every person has his/her own order.*

The second step is to define three sets to distinguish three categories of data, or *levels of publicity*:

- **Confidential Data**  $\mathfrak{C}$  is the set of information that we are not willing to share with anybody because these are **sensitive** data that can easily hurt us, in some sense. Some examples might be the PIN code of our credit-card or the passwords of our e-mail account.
- **Shared Data**  $\mathfrak{S}$  is the set of information that is sensitive but we *are willing* or we *need* to share for some reason. In this set we can find our personal health-measurements shared with a family doctor, our home address, our annual-income or similar data that will be **shared with some specific** people/entity but we do not want to disclose that information to the whole world.
- **Public Data**  $\mathfrak{P}$  is the set of information that is **not sensitive** and we do not mind to share it with the whole world.

**Informal Corollary 1.** *Since the Informal Axiom 1 holds, the sets are different for each person **and** the membership problem is ill-defined, i.e., given an information  $x$ , deciding which set contains  $x$  is a non-objective problem.*

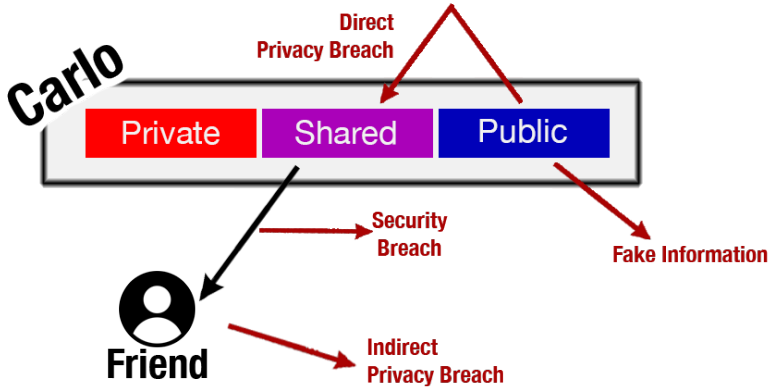
In different words, the order  $<$  and the distinct sets  $\mathfrak{C}, \mathfrak{S}, \mathfrak{P}$  are different among different people. We describe this *non-objectiveness* with the term **personal privacy-perception**, i.e., the individual perception of publicity. For example, Carlo might find that  $x = \text{“my personal email address”}$  is public information, i.e.,  $x \in \mathfrak{P}$ , while it might exist someone that thinks that it is just a piece of information that can be shared, i.e.,  $x \in \mathfrak{S}$ .

The last point of our construction is describing *how* data relate with respect to other data. We define the **inference/deduction** of information as the process that takes as input some set of data  $\{x_i\}_{i \in I}$  and outputs a new information  $z$ , denoted as  $\{x_i\}_{i \in I} \rightarrow z$ . In a nutshell, imagine that somebody knows that  $x = \text{“Carlo loves cooking”}$  and  $y = \text{“Carlo is Italian”}$ , then she might infer that  $z = \text{“Carlo loves Italian restaurants”}$ . In real-life, an advertising company will “bet” on  $z$  and it will start advertising Italian restaurants to Carlo. This inferred-concept is at the base of all the big advertising companies online.

**Informal Axiom 2.** *Data are **always dependent** with respect to other data: for every information  $z$ , there always exists a set of information  $\{x_i\}_{i \in I}$  that infers about  $z$ , i.e.,  $\{x_i\}_{i \in I} \rightarrow z$ .*

The “*always dependency*” axiom is **strong and scary** but it is exactly what research in *advertising, machine learning* and other fields, is willing to achieve in a close future. For example, let us imagine a future where an internet search engine will be able to predict Carlo’s research query **before** he finishes typing the query [41]. This can help Carlo in getting useful advertisements while he is navigating the internet. On the other hand, suppose Carlo is addicted to thai-food, if Carlo’s next *predicted* advertising describes “*the cheapest thai-restaurant*” with extremely high probability, Carlo will never be able to beat his addiction.

Additionally, inferring new information might have bigger consequences: suppose the input data  $\{x_i\}_{i \in I}$  are **public** data, we infer  $\{x_i\}_{i \in I} \rightarrow z$  and the output  $z$  is a **shared** or a **confidential** information. This is what we define either as a **privacy breach** or a **security breach**. These two breaches differ only on *when* the breach happens. If the breach happens *during the communication phase* of the data, then it is a *security breach*. Otherwise, if it happens after the communication is *finished*, then it is a *privacy breach*. We distinguish and define four different types of breaches named **direct privacy breach**, **indirect privacy breach**, **security breach** and **fake news phenomenon**. The entire 3-Sets-Data privacy model is depicted in Figure 1.



**Figure 1:** The Sketchy 3-Sets-Data Privacy Model. The black arrow indicates the communication between Carlo and his friend. The red arrows indicate all the possible inferences that are breaches: *direct privacy breach* from **public** to **shared/private**, *indirect privacy breach* from **publishing** Carlo’s **shared** information with his friend, *security breach* from the **communication** between Carlo and his friend, *fake information* from Carlo’s **public** data infer and publish a wrong inference.

## 1.1 Direct Privacy Breach

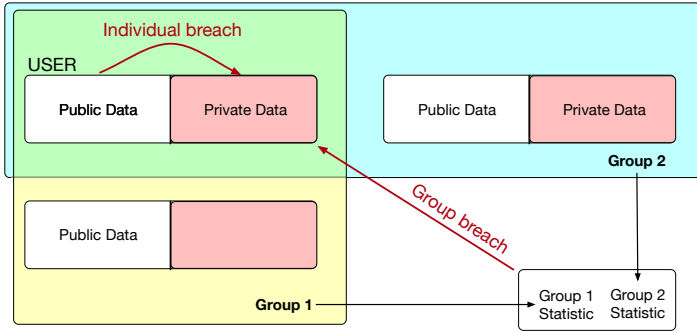
The **direct privacy** is the property that someone finds hard to infer secret information that he/she didn’t receive. Equivalently, whenever someone is able to infer a less public datum from the ones we gave him/her, this is a **direct privacy breach**.

When considering a direct privacy breach, we have to better understand *how it is possible* to have this breach. Let us consider a database in which Carlo has some sensitive information  $x$ . The database is not publicly available **but** it is possible to perform queries in order to obtain statistical analysis on the data-points contained, *i.e.*, it is not possible to directly query  $x$  but it is allowed to query some function  $f$  over some aggregation of sensitive data and obtain a public evaluation  $f(x, \dots)$ . For example, Carlo is pretty cautious not to share his birth-date with anybody. On the other hand, Carlo gave his birth-date in the national census form. The government now offers a free-of-charge web-service in which anyone can ask and get statistics over a population. It is therefore possible to get the answer to the query “*how many people are born every month*” but it is not possible to ask for “*the month when Carlo was born*”.

In 2006, Dwork *et al.* [22] presented the concept of **Differential Privacy** (DP) in which even by cleverly querying the database, it is impossible to infer information about  $x$ . For example, let us consider two queries with a specific *difference* that leak information: the first query is “*how many people are born every month*” while the second is “*how many people are born every month except Carlo*”. It is easy to understand that Carlo’s birth-month will be the difference of the two

queries. This is a consequence of the Informal Axiom 2, the “*always dependence*” axiom, because Carlo’s information is always contained in some **group**, either as the fact that Carlo is *participating in a dataset* by just sharing his information or simply because it is easy to create groups in statistics, for example “**counting with respect to categories**” as in “*count the number of people born each month*”.

For this reason, a direct privacy breach can be a **individual** breach, if the data used for the inference are just Carlo’s public data. Otherwise, if the data are collected from statistics over groups in which Carlo is (or not) a member, then we have a **group** breach. The direct privacy breach concept is depicted in Figure 2.



**Figure 2:** From Paper A: Individual and group privacy breaches.

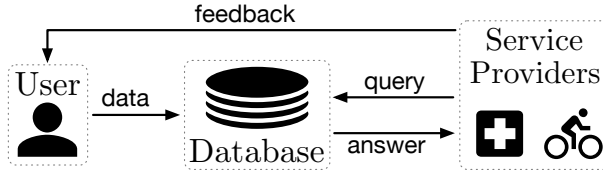
To avoid this information leakage, Dwork *et al.* [22] proposed the **DP framework** that starts by measuring the accuracy of the query  $f$ . In other terms, this means that it is necessary to compute “*how precisely the query  $f$  can allow some differential static privacy breach*” or, more empirically, compute all the possible differences between the statistics over the database. The result is used to define a random variable distribution and, whenever the database has to reply to the query  $f$ , a noise value is sampled and summed to the query result. The final result is a noisy output that makes impossible to infer information on a single user’s sensitive data, even when multiple and similar queries are performed to the database.

## 1.2 Indirect Privacy Breach

The **indirect privacy** is the property that someone will not be able to publish our shared information that he/she has. Equivalently, if someone is *malicious*, in the sense that he/she wants to hurt us, then a **indirect privacy breach** happens whenever he/she publishes some shared secret that was not allowed to share with third parties.

The indirect privacy notion is hard to formally define because it highly depends on the **trust** given to the receiver of the data. Let us consider a specific scenario common in our daily-life. This setting is depicted in Figure 3. Carlo, as a client,

uploads his data to a database in a cloud-service and allows a service-provider to compute some statistical functions on his data.



**Figure 3:** From Paper B: Setting: users send data to a database and enjoy some service.

Despite the pretty simple model, developing a protocol between the parties while achieving indirect privacy, this is not trivial to solve especially with the European General Data Protection Regulation (GDPR) [18] in mind. The GDPR is the new European collections of rules, procedures, rights and obligations that anyone has to follow when handling data from any European citizen.

To give an example, Carlo uploads all of his workout run-sessions and allows a fitness application called Strava [78]. Strava monitors Carlo’s data and provide him some statistical analysis on his workout and suggestions on how to improve. Apart from that, Strava also provides an interactive map in which Carlo can take a look for his running paths from his GPS-data **and** the path that other runners do but only if they have approved to publicly share their GPS-data with the rest of the users of the application. Unluckily, the option in the Strava application for “*sharing the GPS-position of run-sessions*” was set to **true by default**. Therefore, people were sharing their private (and sensitive) information without noticing it. The threats of online-sport social networks and the sensitivity of publishing GPS-data were theoretically studied in 2014 [77] and, in the beginning of 2018, it was possible to infer the life-style of a specific Strava user, *i.e.*, an American soldier running around his secret military base in Afghanistan [42].

Strava’s example demonstrates that handling data in a privacy-preserving way is hard to describe via cryptographic protocols because the receiver do not understand the level of confidentiality that other people give to data. This is the reason *why* we need specific privacy-laws, such as the GDPR, to protect how other people use the data we generate and, by changing focus from law to cryptography, try to solve the question:

*Is it possible to design privacy-preserving protocols that comply with some privacy-policies, such as the European GDPR?*

### 1.3 Security Breach

A **security breach** is indeed the **leakage of confidentiality** and it is therefore connected to the cryptographic property of the crypto-primitives used in communications. Let us consider, Carlo is willing to share his  $x_0 = \text{“secret lasagna”}$

*receipt*” with Elena. Simplistically, in order to share it, Carlo and Elena encrypt their messages while communicating, *e.g.*, the encryption of the secret receipt is  $\text{Enc}(x_0)$ . Since communication is made over a public channel, every eavesdropper can collect all the ciphertexts  $\{\text{Enc}(x_i)\}_{i \in I}$  and, if it is possible to infer  $\{\text{Enc}(x_i)\}_{i \in I} \rightarrow x_0$ , then we have a *security breach*.

Whenever a cryptographic primitive or protocol is not secure in a general sense, it means that it is somehow possible to have a security breach. To avoid this problem, one of the characteristics that an encryption scheme must have is that it produces ciphertexts that look like *chaotic messages* without any connection to the original plaintext. This “*chaos*” is indeed connected to the most important concept in cryptography: **randomness**. Despite the concept of randomness is easy to understand, when stated as “*sample a random value in a set*” or “*flip a fair-coin*”, designing a function that should have a *random-like* output is not an easy task. In fact, in cryptography we always refer to **pseudo-randomness** because “*it looks random*” but in fact “*it is not random*”. To be precise, such functions with random-looking outputs are called **PseudoRandom Functions** (PRF). It is therefore of extreme importance to always use proved-secure cryptographic primitives, such as proved-pseudorandom PRFs, in order to avoid security breaches.

Additionally, it might be of vital importance to **prove** the correct evaluation of a function. Imagine that Carlo needs to prepare a **vegan-pizza** for one of his friend, Elena, which means that Carlo has to use vegan-cheese. After cooking, Elena will require some guarantees that Carlo’s pizza is indeed vegan. Therefore Carlo, while preparing the pizza, will take some videos as **proofs** and show them to Elena before eating. Elena will *verify*, by checking the pizza **and** the videos, that the correct cheese was used.

This proof-idea can be extended to PRFs into the definition of **Verifiable Random Functions** (VRFs) which are PRFs that evaluate on pseudo-random output **and provide an additional proof** used to verify the output is a correct computation of a PRF.

## 1.4 Fake News Phenomenon

A possible problem that can arise is that the deducted results might be **incorrect** and it can be used in a malicious way by just publicly sharing these **fake information** which can be connected to a bigger phenomenon identifiable as **fake news phenomenon**. Publishing fake information may lead to **defamation**, the act of damaging another person’s reputation by publicly sharing wrong and/or malicious data.

With the help of social-networks and better communications tools, the spread of fake news increased year by year, making it hard to judge the sources of the news and the correctness of information. Our own society is affected by fake news since people changed their political ideas [3] or changed their memories about

the past [72].

It is hard to state *how* cryptography can help solving the fake-news problem. The only exception is whenever we think of *re-designing* the whole *news-publishing process*. In a nutshell, if it is possible to use cryptography to, *at least*, guarantee the correct handling of photographs by creating tamper-proof and certified photo-cameras, then we might help journalists to provide a “*proof of correctness*” that allow readers to verify the correct handling of pictures and prove that the photos are indeed **real and untampered**.

The under submission paper “*Strong Functional Signature*” by myself, B. Liang and A. Mitroksotsa, provides a cryptographic primitive that can be used to help journalists to provide these proofs. Since it has not been published yet, it is not included in this dissertation.

## 2 The Thesis’ Contributions

In this thesis, we focus on providing mechanisms that can be employed to combat the different privacy and security breaches. Our goal is to provide new cryptographic tools that help protecting our data and/or prove that cryptography **can** be used to design more privacy-oriented primitives while maintaining their confidentiality.

### 2.1 Direct Privacy Breach - Paper A

An encryption scheme has to be correct, in the sense that the decryption of a ciphertext **needs** to be the original message. When compared to an encryption scheme, a DP mechanism always replies with an almost-correct answer. For this reason, Paper A replies to the following question:

**Question A: A Differentially Private Encryption Scheme [11]**

*Is there a way to define/construct a differentially private encryption scheme?*

The differential privacy mechanism is different from an encryption algorithm while both can be seen as *frameworks*. Paper A studies the relation between the formal definitions of an encryption scheme and a differential private mechanism and merges them into a single cryptographic primitive.

To achieve this, we *relax* the encryption scheme’s correctness property. This means that the encryption scheme has to “*wrongly decrypt*” with some bounded probability, *i.e.*, the decryption of a ciphertext can return a wrong message  $m'$  with some probability  $\alpha_{m,m'}$  that depends on the original message  $m$  and the

final wrong message  $m'$ . By knowing these probabilities for all the messages, it is possible to prove that the “*faulty*” encryption scheme achieves differential privacy.

Additionally, we abstract and prove that using these “*faulty*” encryption schemes is equivalent of using a correct encryption scheme and a DP mechanism as two separate frameworks.

As a final contribution, an implementation is provided as a proof-of-concept.

## 2.2 Indirect Privacy Breach - Paper B

The main goal of Paper B is to provide a model/scheme with an implementation designed to provide privacy-guarantees with respect to privacy-policies/regulations, such as the GDPR, that are not always fully described in mathematical formalism. By considering the scenario of Figure 3, the paper answers the following question:

### Question B: HIKE: Walking the Privacy Trail [62]

*Is it possible to design privacy-preserving protocols that comply with some privacy-policies, such as the European GDPR?*

We start by selecting some specific articles contained in the GDPR and describe as formal cryptographic properties:

- (a) data has to be encrypted when stored;
- (b) the user decides to selectively allow third parties to access his/her data; and
- (c) the user can always delete his/her data from the database (*right to be forgotten*).

In order to describe the “*client, cloud and service provider*” model, we use the concept of *labelled encryption scheme* [4] in which every message, or ciphertext, has a *label* that can be seen as a unique public identifier for that message. With the labels and an algebraic “*magic trick*”, better described as associativity and commutativity in a group, we are able to define some *decryption token* generated by the client. This allows a service provider to decrypt some specific label-ciphertext. Finally, we exploit the additive homomorphic property in order to allow homomorphic evaluations on the client’s ciphertexts. Additionally, the client is able to generate a single token for a *labelled-program*, which is the homomorphic function to evaluate with a list of labels that are the inputs to the function.

Since the function to evaluate is seen by the clients, the clients can refuse to provide the decryption token and therefore **not-disclose** their data.

More concretely, we start from the ElGamal encryption scheme [25], we describe the scheme as a labelled encryption scheme called LEEG, expand it with some specific features regarding the decryption token into FEET and finally obtaining the HIKE protocol, depicted in Figure 4, that is then proven secure in the GDPR-oriented security model we defined.

As a final contribution, all our ideas are implemented and our code for the HIKE protocol is publicly available at <https://github.com/Pica4x6/HIKE>.

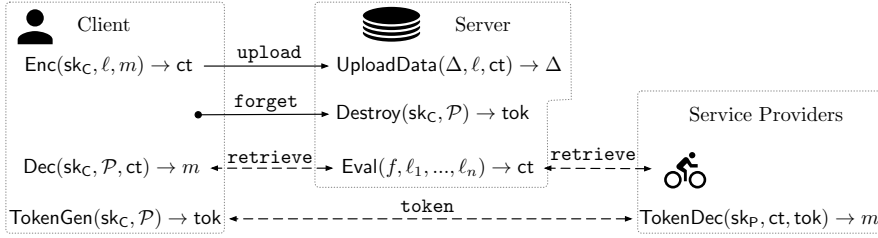


Figure 4: From Paper B: The HIKE protocol.

### 2.3 Security Breach - Paper C

We start by considering the general problem of achieving a post-quantum version of every cryptographic primitive. We focus on verifiable random functions and in particular on **simulatable VRFs** (sVRFs). In a nutshell, sVRFs are a family of VRFs in a public parameter security model, such as the common reference string. Paper C provides some directions in order to address the following question:

**Question C: Lattice sVRF: Challenges and Future Directions [12]**

Is it possible to define a post-quantum sVRF?

We proposed the possibility of defining a **lattice-based membership-hard with efficient sampling** language which can be used to define a lattice-based *dual-mode commitment scheme*. We partially conjecture the possibility to combine the dual-mode commitment scheme with Libert *et al.*'s protocol [52] and Lindell's transformation [54] and obtain an sVRF under post-quantum assumptions.

Given the non-triviality of the task, we raise and identify different open challenges in lattice-based cryptography and possible future directions for achieving a post-quantum sVRF.





---

## Bibliography

---

- [1] Ajtai, M.: Generating Hard Instances of Lattice Problems (Extended Abstract). In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. pp. 99–108. STOC '96, ACM, New York, NY, USA (1996), <http://doi.acm.org/10.1145/237814.237838>
- [2] Akinyele, J.A., Garman, C., Miers, I., Pagano, M.W., Rushanan, M., Green, M., Rubin, A.D.: Charm: a framework for rapidly prototyping cryptosystems. *Journal of Cryptographic Engineering* 3(2), 111–128 (Jun 2013)
- [3] Allcott, H., Gentzkow, M.: Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives* 31(2), 211–36 (May 2017), <http://www.aeaweb.org/articles?id=10.1257/jep.31.2.211>
- [4] Barbosa, M., Catalano, D., Fiore, D.: Labeled Homomorphic Encryption. In: ESORICS. pp. 146–166 (2017)
- [5] Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More Efficient Commitments from Structured Lattice Assumptions. Tech. Rep. 997 (2016), <https://eprint.iacr.org/2016/997>
- [6] Beimel, A., Nissim, K., Omri, E.: Distributed Private Data Analysis: On Simultaneously Solving How and What. arXiv:1103.2626 [cs] (Mar 2011), <http://arxiv.org/abs/1103.2626>
- [7] Benhamouda, F., Krenn, S., Lyubashevsky, V., Pietrzak, K.: Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings. In: Proceedings, Part I, of the 20th European Symposium on Computer Security – ESORICS 2015 - Volume 9326. pp. 305–325. Springer-Verlag New York, Inc., New York, NY, USA (2015), [http://dx.doi.org/10.1007/978-3-319-24174-6\\_16](http://dx.doi.org/10.1007/978-3-319-24174-6_16)
- [8] Boneh, D., Lewi, K., Montgomery, H., Raghunathan, A.: Key Homomorphic PRFs and Their Applications. In: Canetti, R., Garay, J.A. (eds.) *Advances in Cryptology – CRYPTO 2013*. pp. 410–428. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)

- [9] Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing* 43(2), 831–871 (2014)
- [10] Brunetta, C., Calderini, M., Sala, M.: On hidden sums compatible with a given block cipher diffusion layer. *Discrete Mathematics* 342(2), 373–386 (Feb 2019), <https://linkinghub.elsevier.com/retrieve/pii/S0012365X18303376>
- [11] Brunetta, C., Dimitrakakis, C., Liang, B., Mitrokotsa, A.: A Differentially Private Encryption Scheme. In: Nguyen, P.Q., Zhou, J. (eds.) *Information Security*. pp. 309–326. Springer International Publishing, Cham (2017)
- [12] Brunetta, C., Liang, B., Mitrokotsa, A.: Lattice-Based Simulatable VRFs: Challenges and Future Directions. 1th Workshop PROVSEC, 2018. To appear in *Journal of Internet Services and Information Security*, Vol. 8, No. 4 (November, 2018) (2018)
- [13] Canetti, R., Raghuraman, S., Richelson, S., Vaikuntanathan, V.: Chosen-ciphertext secure fully homomorphic encryption. In: *PKC*. pp. 213–240 (2017)
- [14] Catalano, D., Visconti, I.: Hybrid Commitments and Their Applications to Zero-knowledge Proof Systems. *Theor. Comput. Sci.* 374(1-3), 229–260 (Apr 2007), <http://dx.doi.org/10.1016/j.tcs.2007.01.007>
- [15] Chase, M., Lysyanskaya, A.: Simulatable VRFs with Applications to Multi-theorem NIZK. In: *Advances in Cryptology - CRYPTO 2007*. pp. 303–322. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg (Aug 2007), [https://link.springer.com/chapter/10.1007/978-3-540-74143-5\\_17](https://link.springer.com/chapter/10.1007/978-3-540-74143-5_17)
- [16] Ciampi, M., Persiano, G., Siniscalchi, L., Visconti, I.: A Transform for NIZK Almost as Efficient and General as the Fiat-Shamir Transform Without Programmable Random Oracles. In: Kushilevitz, E., Malkin, T. (eds.) *Theory of Cryptography*. pp. 83–111. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
- [17] Connolly, A.: Freedom of Encryption. *S&P* 16(1), 102–103 (2018)
- [18] Council of the European Union, European Parliament: Regulation (EU) 2016/679 (General Data Protection Regulation) (2016), <https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en>
- [19] David, B., Gaži, P., Kiayias, A., Russell, A.: Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain. In: Nielsen, J.B., Rijmen, V. (eds.) *Advances in Cryptology – EUROCRYPT 2018*. pp. 66–98. Lecture Notes in Computer Science, Springer International Publishing (2018)

- [20] Dijk, M.v., Gentry, C., Halevi, S., Vaikuntanathan, V.: Fully Homomorphic Encryption over the Integers. In: *Advances in Cryptology – EUROCRYPT 2010*. pp. 24–43. Springer, Berlin, Heidelberg (May 2010), [http://link.springer.com/chapter/10.1007/978-3-642-13190-5\\_2](http://link.springer.com/chapter/10.1007/978-3-642-13190-5_2)
- [21] Dwork, C.: Differential Privacy, vol. 4052 (Jul 2006), <https://www.microsoft.com/en-us/research/publication/differential-privacy/>
- [22] Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating Noise to Sensitivity in Private Data Analysis. In: Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Halevi, S., Rabin, T. (eds.) *Theory of Cryptography*, vol. 3876, pp. 265–284. Springer Berlin Heidelberg, Berlin, Heidelberg (2006), [http://link.springer.com/10.1007/11681878\\_14](http://link.springer.com/10.1007/11681878_14)
- [23] Dwork, C., Naor, M., Reingold, O.: Immunizing Encryption Schemes from Decryption Errors. In: *Advances in Cryptology - EUROCRYPT 2004*. pp. 342–360. Springer, Berlin, Heidelberg (May 2004), [http://link.springer.com/chapter/10.1007/978-3-540-24676-3\\_21](http://link.springer.com/chapter/10.1007/978-3-540-24676-3_21)
- [24] El Emam, K., Dankar, F.K.: Protecting Privacy Using k-Anonymity. *J Am Med Inform Assoc* 15(5), 627–637 (2008), <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2528029/>
- [25] El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: *CRYPTO*. pp. 10–18 (1985)
- [26] Erkin, Z., Troncoso-Pastoriza, J.R., Lagendijk, R., Pérez-González, F.: Privacy-Preserving Data Aggregation in Smart Metering Systems: An Overview. *IEEE Signal Processing Magazine* 30(2), 75–86 (2013)
- [27] Fiat, A., Shamir, A.: How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) *Advances in Cryptology — CRYPTO’ 86*, vol. 263, pp. 186–194. Springer Berlin Heidelberg, Berlin, Heidelberg (2006), [http://link.springer.com/10.1007/3-540-47721-7\\_12](http://link.springer.com/10.1007/3-540-47721-7_12)
- [28] Fiore, D., Mitrokotsa, A., Nizzardo, L., Pagnin, E.: Multi-key homomorphic authenticators. In: *ASIACRYPT*. pp. 499–530. Springer (2016)
- [29] Fischer, A., Fuhry, B., Kerschbaum, F., Bodden, E.: Computation on Encrypted Data using Data Flow Authentication. *CoRR* abs/1710.00390 (2017), <http://arxiv.org/abs/1710.00390>
- [30] Garcia, F.D., Jacobs, B.: Privacy-Friendly Energy-Metering via Homomorphic Encryption. In: *Security and Trust Management*. pp. 226–238. Springer, Berlin, Heidelberg (Sep 2010), [http://link.springer.com/chapter/10.1007/978-3-642-22444-7\\_15](http://link.springer.com/chapter/10.1007/978-3-642-22444-7_15)

- [31] Gehrke, J., Kifer, D., Machanavajjhala, A.: l-Diversity. In: Tilborg, H.C.A.v., Jajodia, S. (eds.) *Encyclopedia of Cryptography and Security*, pp. 707–709. Springer US (2011), [http://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5\\_899](http://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_899)
- [32] Gennaro, R., Gentry, C., Parno, B.: Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In: *CRYPTO*. pp. 465–482 (2010)
- [33] Gennaro, R., Wichs, D.: Fully Homomorphic Message Authenticators. In: Sako, K., Sarkar, P. (eds.) *ASIACRYPT*. pp. 301–320 (2013)
- [34] Gentry, C.: Fully Homomorphic Encryption Using Ideal Lattices. In: *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*. pp. 169–178. STOC '09, ACM, New York, NY, USA (2009), <http://doi.acm.org/10.1145/1536414.1536440>
- [35] Goldberg, S., Naor, M., Papadopoulos, D., Reyzin, L., Vasant, S., Ziv, A.: NSEC5: Provably Preventing DNSSEC Zone Enumeration. In: *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015* (2015)
- [36] Goldreich, O., Goldwasser, S., Micali, S.: How to Construct Random Functions. *J. ACM* 33(4), 792–807 (Aug 1986), <http://doi.acm.org/10.1145/6490.6503>
- [37] Goldwasser, S., Micali, S.: Probabilistic encryption & how to play mental poker keeping secret all partial information. In: *STOC*. pp. 365–377. ACM (1982)
- [38] Granville, K.: Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. *The New York Times* (2018)
- [39] Greenwald, G., MacAskill, E., Poitras, L.: Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian* 9(6), 2 (2013)
- [40] Grover, L.K.: A Fast Quantum Mechanical Algorithm for Database Search. In: *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*. pp. 212–219. STOC '96, ACM, New York, NY, USA (1996), <http://doi.acm.org/10.1145/237814.237866>
- [41] Guo, Q., Agichtein, E., Clarke, C.L.A., Ashkan, A.: In the Mood to Click? Towards Inferring Receptiveness to Search Advertising. In: *2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology*. pp. 319–324. IEEE, Milan, Italy (2009), <http://ieeexplore.ieee.org/document/5286052/>
- [42] Hern, A.: Fitness tracking app Strava gives away location of secret US army bases. *The Guardian* (Jan 2018), <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>

- [43] Hinde, R.A.: Biological bases of human social behaviour. McGraw-Hill (1974)
- [44] Hoffstein, J., Pipher, J., Silverman, J.H., Silverman, J.H.: An introduction to mathematical cryptography, vol. 1. Springer (2008)
- [45] Ji, Z., Lipton, Z.C., Elkan, C.: Differential Privacy and Machine Learning: a Survey and Review. arXiv:1412.7584 [cs] (Dec 2014), <http://arxiv.org/abs/1412.7584>
- [46] Katz, J., Lindell, Y.: Introduction to modern cryptography. CRC press (2014)
- [47] Kawachi, A., Tanaka, K., Xagawa, K.: Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems. In: Pieprzyk, J. (ed.) Advances in Cryptology - ASIACRYPT 2008. pp. 372–389. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
- [48] Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation 48(177), 203–203 (Jan 1987), <http://www.ams.org/jourcgi/jour-getitem?pii=S0025-5718-1987-0866109-5>
- [49] Li, N., Li, T., Venkatasubramanian, S.: t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In: 2007 IEEE 23rd International Conference on Data Engineering. pp. 106–115 (Apr 2007)
- [50] Li, W., Andreina, S., Bohli, J.M., Karame, G.: Securing Proof-of-Stake Blockchain Protocols. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (eds.) Data Privacy Management, Cryptocurrencies and Blockchain Technology, vol. 10436, pp. 297–315. Springer International Publishing, Cham (2017), [http://link.springer.com/10.1007/978-3-319-67816-0\\_17](http://link.springer.com/10.1007/978-3-319-67816-0_17)
- [51] Libert, B., Ling, S., Mouhartem, F., Nguyen, K., Wang, H.: Zero-knowledge arguments for matrix-vector relations and lattice-based group encryption. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 101–131. Springer (2016)
- [52] Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-Knowledge Arguments for Lattice-Based PRFs and Applications to E-Cash. In: Asiacrypt 2017. LNCS, Springer, Hong Kong, China (Dec 2017), <https://hal.inria.fr/hal-01621027>
- [53] Libert, B., Ling, S., Nguyen, K., Wang, H.: Lattice-Based Zero-Knowledge Arguments for Integer Relations. In: Annual International Cryptology Conference. pp. 700–732. Springer (2018)
- [54] Lindell, Y.: An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-programmable Random Oracle. In: Dodis, Y., Nielsen, J.B. (eds.) Theory of Cryptography, vol. 9014, pp. 93–109. Springer Berlin Heidelberg, Berlin, Heidelberg (2015), [http://link.springer.com/10.1007/978-3-662-46494-6\\_5](http://link.springer.com/10.1007/978-3-662-46494-6_5)

- [55] Meissen, R.: A Mathematical Approach to Fully Homomorphic Encryption. PhD Thesis, Worcester Polytechnic Institute (2012)
- [56] Micali, S., Rabin, M., Vadhan, S.: Verifiable random functions. In: 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039). pp. 120–130 (1999)
- [57] Micali, S., Rivest, R.L.: Micropayments Revisited. In: Proceedings of the The Cryptographer’s Track at the RSA Conference on Topics in Cryptology. pp. 149–163. CT-RSA ’02, Springer-Verlag, London, UK, UK (2002)
- [58] Micciancio, D., Peikert, C.: Hardness of SIS and LWE with small parameters. In: Advances in Cryptology–CRYPTO 2013, pp. 21–39. Springer (2013)
- [59] Montenegro, R., Tetali, P.: How Long Does It Take to Catch a Wild Kangaroo? In: Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. pp. 553–560. STOC ’09, ACM, New York, NY, USA (2009), <http://doi.acm.org/10.1145/1536414.1536490>
- [60] Nielsen, J.B.: Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case. In: Goos, G., Hartmanis, J., van Leeuwen, J., Yung, M. (eds.) Advances in Cryptology — CRYPTO 2002, vol. 2442, pp. 111–126. Springer Berlin Heidelberg, Berlin, Heidelberg (2002), [http://link.springer.com/10.1007/3-540-45708-9\\_8](http://link.springer.com/10.1007/3-540-45708-9_8)
- [61] NIST STS: Cryptographic Key Length Recommendation (2017), <https://www.keylength.com/en/4/>
- [62] Pagnin, E., Brunetta, C., Picazo-Sanchez, P.: HIKE: Walking the Privacy Trail. In: Camenisch, J., Papadimitratos, P. (eds.) Cryptology and Network Security. pp. 43–66. Springer International Publishing, Cham (2018)
- [63] Paillier, P.: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In: Stern, J. (ed.) EUROCRYPT. pp. 223–238 (1999)
- [64] Panjwani, M., Jäntti, M.: Data Protection & Security Challenges in Digital & IT Services: A Case Study. In: ICCA. pp. 379–383. IEEE (2017)
- [65] Papadopoulos, D., Wessels, D., Huque, S., Naor, M., Včelák, J., Reyzin, L., Goldberg, S.: Making NSEC5 Practical for DNSSEC (2017), published: Cryptology ePrint Archive, Report 2017/099
- [66] Peikert, C.: A Decade of Lattice Cryptography. Foundations and Trends® in Theoretical Computer Science 10(4), 283–424 (2016), <http://www.nowpublishers.com/article/Details/TCS-074>
- [67] Policy, C.t.S.N.C., Board, C.S.a.T., Sciences, D.o.E.a.P., Council, N.R.: Cryptography’s Role in Securing the Information Society. National Academies Press (Nov 1996)

- [68] Pollard, J.M.: Kangaroos, Monopoly and Discrete Logarithms. *Journal of Cryptology* 13(4), 437–447 (Sep 2000), <https://link.springer.com/article/10.1007/s001450010010>
- [69] Pollard, J.M.: Monte Carlo methods for index computation (mod  $p$ ). *Mathematics of computation* 32(143), 918–924 (1978)
- [70] Regev, O.: The Learning with Errors Problem (Invited Survey). In: *Proceedings of the 2010 IEEE 25th Annual Conference on Computational Complexity*. pp. 191–204. IEEE Computer Society (2010)
- [71] Rivest, R.L., Adleman, L., Dertouzos, M.L.: On Data Banks and Privacy Homomorphisms. *Foundations of Secure Computation*, Academia Press (1978)
- [72] Sacchi, D.L.M., Agnoli, F., Loftus, E.F.: Changing history: doctored photographs affect memory for past public events. *Applied Cognitive Psychology* 21(8), 1005–1022 (Dec 2007), <http://doi.wiley.com/10.1002/acp.1394>
- [73] Shannon, C.E.: A mathematical theory of communication. *Bell system technical journal* 27(3), 379–423 (1948)
- [74] Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* 26(5), 1484–1509 (Oct 1997), <http://dx.doi.org/10.1137/S0097539795293172>
- [75] Smart, N.P., Vercauteren, F.: Fully homomorphic encryption with relatively small key and ciphertext sizes. In: *PKC*. pp. 420–443 (2010)
- [76] Stern, J.: A new paradigm for public key identification. *IEEE Transactions on Information Theory* 42(6), 1757–1768 (Nov 1996)
- [77] Stottelaar, B., Senden, J., Montoya, L.: Online social sports networks as crime facilitators. *Crime Science* 3(1) (Dec 2014), <http://www.crimesciencejournal.com/content/3/1/8>
- [78] Strava: Strava (Nov 2018), <https://www.strava.com>