Czech Technical University in Prague
Faculty of Electrical Engineering

Department of Telecommunications Engineering

# DIPLOMA THESIS ASSIGNMENT

Student: **Marku Enio**

Study programme: Communications, Multimedia, Electronics
Specialisation: Networks of Electronic Communication

Title of Diploma Thesis: **Privacy for Secure Distributed Storage Networks**

Guidelines:

Study methods of the privacy assurance in the cryptographic storage networks based on secret sharing. Focus on sensitive data retrieval and the possibility of hidden access controls in the context of user interaction in the open source Archistar framework. Do a survey on existing secret sharing schemes as well as their adoption and possible performance improvements for the Archistar project. In hands-on part implement designed protocols and recommended enhancements in suitable software and do measurement of its performance in real world configurations.

Bibliography/Sources:

[1] Loruenser, T.; Happe, A.; Slamanig D.: *ARCHISTAR: A Framework for Secure Distributed Storage*. GNU General Public License. Avalable at http://ARCHISTAR.at [on-line]
[2] Goldberg, I.: *Improving the Robustness of Private Information Retrieval*. Procedings of 2007 IEEE Symposium on Security and Privacy (Oakland 2007), May 2007. Available at: http://www.cypherpunks.ca/~iang/pubs/robustpir.pdf [on-line]
[3] Devet, C.; Goldberg, I.; Heninger, N.: *Optimally Robust Private Information Retrieval*. 21st USENIX Security Symposium, August 2012. Available at: http://www.cypherpunks.ca/~iang/pubs/orpir-usenix.pdf [on-line]
[4] Lueks, W.; Goldberg, I.: *Sublinear Scaling for Multi-Client Private Information Retrieval*. 19th International Conference on Financial Cryptography and Data Security, January 2015. Available at: http://www.cypherpunks.ca/~iang/pubs/slspir-fc15.pdf [on-line].

Diploma Thesis Supervisor: Ing. Tomáš Vaněk, Ph.D.

Valid until the end of the summer semester of academic year 2016/2017

prof. Ing. Boris Šimák, CSc.
Head of Department

L.S.

prof. Ing. Pavel Ripka, CSc.
Dean

Prague, December 21, 2015

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

# ZADÁNÍ DIPLOMOVÉ PRÁCE

## I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Marku** Jméno: **Enio** Osobní číslo: **437928**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra teorie obvodů**

Studijní program: **Komunikace, multimédia a elektronika**

Studijní obor: **Komunikační systémy**

## II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

**Zajištění soukromí v bezpečných distribuovaných síťových úložištích.**

Název diplomové práce anglicky:

**Privacy for Secure Distributed Storage Networks**

Pokyny pro vypracování:

Study methods of the privacy assurance in the cryptographic storage networks based on secret sharing. Focus on sensitive data retrieval and the possibility of hidden access controls in the context of user interaction in the open source Archistar framework. Do a survey on existing secret sharing schemes as well as their adoption and possible performance improvements for the Archistar project. In hands-on part implement designed protocols and recommended enhancements in suitable software and do measurement of its performance in real world configurations.

Seznam doporučené literatury:

[1] T. Loruenser, A. Happe, D. Slamanig (2014). “ARCHISTAR – A framework for secure distributed storage”. GNU General Public License. http://ARCHISTAR.at
[2] I. Goldberg, Improving the Robustness of Private Information Retrieval, Proc. of 2007 IEEE Symposium on Security and Privacy (Oakland 2007), May 2007, available at: http://www.cypherpunks.ca/~iang/pubs/robustpir.pdf [online]
[3] C. Devet, I. Goldberg, N. Heninger, Optimally Robust Private Information Retrieval, 21st USENIX Security Symposium, August 2012, available at: http://www.cypherpunks.ca/~iang/pubs/orpir-usenix.pdf [online]
[4] W. Lueks, I. Goldberg, Sublinear Scaling for Multi-Client Private Information Retrieval, 19th International Conference on Financial Cryptography and Data Security, January 2015, available at: http://www.cypherpunks.ca/~iang/pubs/slspir-fc15.pdf [online]

Jméno a pracoviště vedoucí(ho) diplomové práce:

**Ing. Tomáš Vaněk Ph.D., katedra telekomunikační techniky FEL**

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **21.12.2015** Termín odevzdání diplomové práce: **09.01.2017**

Platnost zadání diplomové práce: _____

| Podpis vedoucí(ho) práce | Podpis vedoucí(ho) ústavu/katedry | Podpis děkana(ky) |
|---|---|---|

## III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

07.01.2017 E. Marku

Datum převzetí zadání Podpis studenta

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

**Fakulta elektrotechnická**
Technická 2, 16627 Praha 6

**LICENČNÍ SMLOUVA**
**POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO**

uzavřená mezi smluvními stranami:

Pan
Jméno a příjmení: Enio Marku
Bytem: Rakip Jacellari , Lushnje,
Albánie Narozen: 02.12.1992
(dále jen **„Autor“**)

a

České vysoké učení technické v
Praze se sídlem Zikova 4, 166 36
Praha 6 IČ 68407700
zastoupená: prof. Ing. Pavel Ripka, CSc.
Fakulta elektrotechnická, Technická 2, 16627 Praha
6 (dále jen **„Nabyvatel“**)

**Čl. 1**
**Předmět a účel Licenční smlouvy**

1. Předmětem Licenční smlouvy je úprava práv a povinností Nabyvatele a Autora při nevýdělečném užití školních děl nad rámec vnitřní potřeby Nabyvatele, a to prostřednictvím poskytnutí licence Nabyvateli k jednotlivým školním dílům.
2. Účelem Licenční smlouvy je zajištění nerušeného nevýdělečného užití školních děl Nabyvatelem v souladu s posláním a zájmy Nabyvatele jakožto vysoké školy.

**Čl. 2**
**Specifikace školního díla**

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP) [(1)]:
   - ☐ disertační práce
   - ☒ diplomová práce
   - ☐ bakalářská práce
   - ☐ jiná práce, jejíž druh je specifikován jako .....

   (dále jen **„dílo“**)

   Název: Zajištění soukromí v bezpečných distribuovaných síťových úložištích.
   Vedoucí/školitel: Ing. Tomáš Vaněk, Ph.D.
   Katedra/vysokoškolský ústav: katedra teorie obvodů

   Dílo odevzdal Autor Nabyvateli v [(1)]:
   - ☒ tištěné formě
   - ☒ elektronické formě
2. Autor prohlašuje, že dílo shora popsané a specifikované vytvořil samostatnou vlastní tvůrčí činností. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo podle autorského zákona v platném znění.

---

[(1)] hodící se zaškrtněte

**Čl. 3**

**Udělení licenčního oprávnění**

1. Autor touto smlouvou poskytuje Nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence se poskytuje vzhledem k nevýdělečnosti užití jako bezúplatná.
3. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu. Množstevní rozsah licence je neomezený.
4. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti [2]
   - ☒ ihned po uzavření této smlouvy
   - ☐ [3] .....let po uzavření této smlouvy (z důvodu utajení v něm obsažených informací).
5. Licence je poskytována jako nevýhradní. Nabyvatel není povinen dílo užít.
6. Nabyvatel je oprávněn udělovat podlicence a poskytovat rozmnoženiny díla, které Autor odevzdal Nabyvateli, jiným osobám v rámci meziknihovní výpůjční služby v České republice i v zahraničí k účelu půjčování rozmnoženin díla těmito osobami dalším osobám k jejich dočasné potřebě. Nabyvatel je oprávněn dílo při užití spojovat s jinými díly i zařadit dílo do díla souborného. Nabyvatel není oprávněn postoupit tuto licenci třetí osobě.
7. Smluvní strany se dohodly, že Autor souhlasí spolu s odevzdáním díla v tištěné podobě také s případným předáním díla v elektronické formě. Dále Autor svoluje, že Nabyvatel může po uplynutí doby stanovené předpisy o archivnictví hmotné rozmnoženiny díla, které mu Autor odevzdal, skartovat a uchovávat dílo dále jen v elektronické podobě.

**Čl. 4**

**Závěrečná ustanovení**

1. Smlouva je sepsána ve dvou vyhotoveních s platností originálu, z toho Nabyvatel obdrží jedno vyhotovení smlouvy a Autor obdrží jedno vyhotovení smlouvy.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy. Na nakládání s rozmnoženinami díla se vztahují právní předpisy o knihovnictví a o archivnictví.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Praze dne: .....

.....
Nabyvatel

V Praze dne: .06.01.2017

Autor : Enio Marku....

---

[2] hodící se zaškrtněte

[3] doplňte správný text (možno doplnit počet roků)