KU LEUVEN

FACULTY OF ENGINEERING TECHNOLOGY

DE NAYER (SINT-KATELIJNE-WAVER) CAMPUS

# Object Detection on Encrypted Data

## Using Secure Multiparty Computation

**Felix LERNER**

Promotor(en): Prof. dr. ir. Toon Goedemé
Dr. Pradip Mainali (Onespan)

Masterproef ingediend tot het behalen van de graad van master of Science in de industriële wetenschappen: Elektronica ICT afstudeerrichting ICT

Academiejaar 2019 - 2020

# Voorwoord

Het voorwoord vul je persoonlijk in met een appreciatie of dankbetuiging aan de mensen die je hebben bijgestaan tijdens het verwezenlijken van je masterproef en je hebben gesteund tijdens je studie.

# Samenvatting

De (korte) samenvatting, toegankelijk voor een breed publiek, wordt in het Nederlands geschreven en bevat **maximum 3500 tekens**. Deze samenvatting moet ook verplicht opgeladen worden in KU Loket.

# Abstract

We are affected with machine learning in many aspects of our daily lives, applications ranges from facial recognition to enhanced healthcare to self-driving cars. Nowadays most of these neural networks are computed in the hardware of the client and the data stays clientside. As more and more companies move their processing serverside, because it's easier to debug and it's faster to roll out a new update. We see a rise in "questions about the privacy of our data". Would you want to have a picture of your face sent to a server everytime you want to unlock your phone with your face? Even if the company of said server promises they won't do anything other than run the neural network on the image of your face, there still exist the risk of them doing it anyway. So we need to find a method that bars the company of being able to have access to the picture of your face but give them enough access so they can process the image in the neural network.

**Keywords**: Deep learning, secure multiparty computation, privacy preserving, convolutional neural network

# Contents

# List of Figures

# List of Tables

# Lijst van symbolen

Maak een lijst van de gebruikte symbolen. Geef het symbool, naam en eenheid. Gebruik steeds SI-eenheden en gebruik de symbolen en namen zoals deze voorkomen in de hedendaagse literatuur en normen. De symbolen worden alfabetisch gerangschikt in opeenvolgende lijsten: kleine letters, hoofdletters, Griekse kleine letters, Griekse hoofdletters. Onderstaande tabel geeft het format dat kan ingevuld en uitgebreid worden. Wanneer het symbool een eerste maal in de tekst of in een formule wordt gebruikt, moet het symbool verklaard worden. Verwijder deze tekst wanneer je je thesis maakt.

| | | |
|---|---|---|
| $b$ | Breedte | $[mm]$ |
| $A$ | Oppervlakte van de dwarsdoorsnede | $[mm^2]$ |
| $c$ | Lichtsnelheid | $[m/s]$ |

# Lijst van afkortingen

Secure multiparty computation MPC

# Chapter 1

# Vormelijke richtlijnen van de scriptie

## 1.1 Verplichte onderdelen en volgorde in de scriptie

De masterproefscriptie bevat volgende onderdelen

- Voorkaft met titelblad
- Herhaling titelblad
- Bladzijde met verplichte tekst copyright
- Voorwoord
- Samenvatting
- Abstract
- Inhoudstafel
- Symbolenlijst
- Masterproeftekst
- Referentielijst
- Bijlagen
- Achterkaft met gegevens van de campus

## 1.2 Lay-out

De scriptie is standaard in het Nederlands, maar mag in het Engels geschreven worden mits motivatie.

Dit document is opgesteld volgens de vereiste lay-out van de faculteit. Hieronder volgen een aantal specifieke richtlijnen die ook in de template[1] verwerkt zijn.

### 1.2.1 Papierformaat en bladspiegel

Deze LaTeX-template is opgesteld volgens de geldende regels van de faculteit. Het is dus niet toegalaten zelf aanpassingen aan de stijl ervan te doen. Bij voorkeur wordt de thesis recto-verso afgedrukt.

### 1.2.2 Titelblad

Volg nauwgezet de aanwijzigen in deze template voor het opstellen van het titelblad.

Is een masterproef uitgevoerd onder *embargo*, dan wordt dit expliciet vermeld op het titelblad (onder voorbehoud van goedkeuring van de fPOC). De cover wordt geprint in kleur op wit papier. Indien meerdere studenten samen een masterproef realiseren, worden de namen alfabetisch op achternaam weergeven op het titelblad door deze in de juiste volgorde in de template in te vullen. Een student die een Nederlandstalige opleiding volgt en de toelating heeft gekregen om zijn masterproefscriptie in het Engels te schrijven, moet het Nederlandstalige titelblad nog steeds gebruiken. De titel zelf is dan wel in het Engels.

[1] Deze template dient gebruikt te worden in combinatie met LaTeX. Voor meer informatie over de installatie en het gebruik hiervan, wordt doorverwezen naar de website: www.latex-project.org.

# Chapter 2

# Structuur van de masterproeftekst

## 2.1 Opdeling in hoofdstukken

De masterproeftekst vormt de kern van de scriptie. De tekst wordt logisch opgedeeld in een aantal hoofdstukken. Het eerste hoofdstuk is altijd een inleiding, het tweede en eventueel derde de literatuurstudie of een *state of the art*, gevolgd door een hoofdstuk dat de methodologie beschrijft. De volgende hoofdstukken bevatten de elementen van het eigen onderzoek. Het laatste hoofdstuk bevat de algemene besluiten van de masterproef. Elk hoofdstuk vormt een afgerond geheel (m.a.w. met inleiding en conclusie!).

## 2.2 Verdere onderverdeling binnen een hoofdstuk

De tekst wordt onderverdeeld in logische paragrafen met een aangepaste nummering. De nummering van de onderliggende delen van een hoofdstuk bevat begint steeds met het hoofstuknummer en gaat maximum tot drie subniveaus. Volgende onderverdeling wordt gebruikt:

## 2.3 Dit is een voorbeeld van een sectie

### 2.3.1 Dit is een voorbeeld van een subsectie

#### 2.3.1.1 Dit is een voorbeeld van een subsubsectie

**Dit is een voorbeeld van een paragraaf**

# Chapter 3

# Figuren en tabellen

## 3.1 Algemene richtlijnen

Alle figuren en tabellen worden genummerd en binnen een float omgeving geplaatst (`\begin{figure} figuurcontent \end{figure}`)

Foto's, grafieken, schema's,... worden alle onder de benaming 'Figuur' gecatalogeerd.

Het is belangrijk dat tabellen en figuren duidelijk zijn en dat ze alle informatie bevatten die nodig is om ze te begrijpen.

Tabellen worden bij voorkeur niet gesplitst over twee bladzijden. Indien een tabel niet op één bladzijde past, wordt het bijschrift op de volgende bladzijde hernomen en aangevuld met (vervolg). Ook de kolomkoppen van de tabel worden hernomen.

In de tekst wordt naar alle tabellen en figuren verwezen met het itemnummer. Schrijf dus niet 'onderstaande figuur toont....', maar wel 'Figuur 3.1 toont...'. Doe dit door gebruik te maken van de commando's `\label{}` en `\ref{}`. Geef figuren ook zinvolle captions (`\caption{Caption}`). Figuren worden gecentreerd op de bladzijde. Ook het bijschrift wordt gecentreerd en onder de figuur geplaatst. Na de figuurnummer volgt een de beschrijving van de figuur.

Figuur 3.1 toont een voorbeeld gegeven van een float omgeving voor een figuur. Hieronder wordt de syntax weergegeven.

```
\begin{figure}[!ht]
\centering
\includegraphics[width=0.75\linewidth]{image.jpg}
\caption{Dit is een voorbeeld van een figuur-float}
\label{fig:VoorbeeldFigFloat}
\end{figure}
```

Tabellen worden links uitgelijnd op de bladzijde. Ook het bijschrift wordt links uitgelijnd en boven de tabel geplaatst. Na de tabelnummer volgt de beschrijving van de tabel. Tabel 3.1 toont een voorbeeld van een eigen tabel. Vermijd om tabellen te kopieëren van andere werken, maar herwerk ze en plaats de nodige bronvermelding. De nodige syntax om tabel 3.1 te generen wordt hieronder

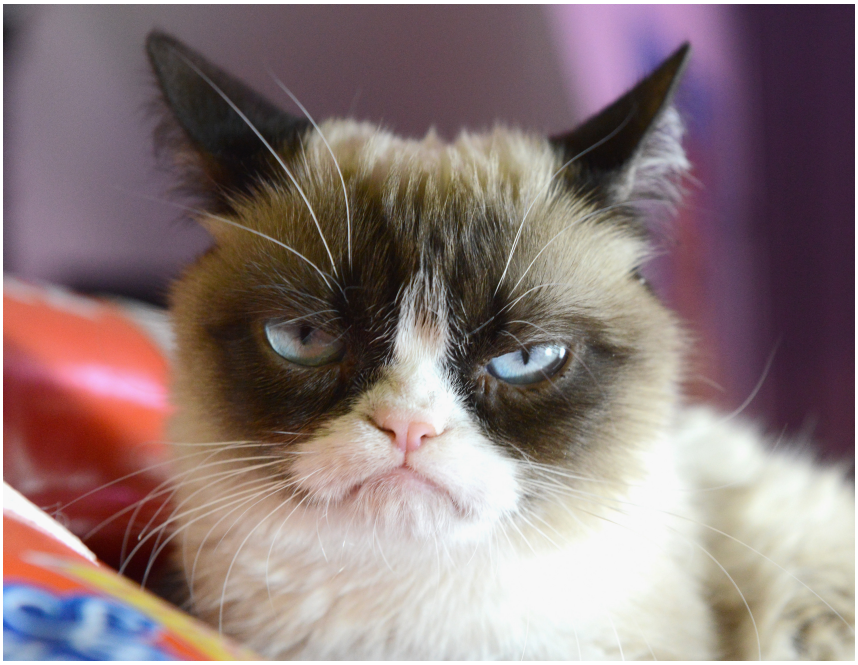

**Figure 3.1:** Dit is een voorbeeld van een figuur-float

weergegeven:

```
\begin{table}[!ht]
\caption{Dit is een voorbeeld van een tabel}
\begin{tabular}{ccc}
\hline
Kolom 1 & Kolom 2 & Kolom 3\
\hline
1 & 2 & 3\\
4 & 5 & 6\\
\hline
\end{tabular}
\label{tab:VoorbeeldTableFloat}
\end{table}
```

Tot slot, let er op dat er expliciet naar elke tabel en figuur verwezen wordt vanuit de tekst.

**Table 3.1** Dit is een voorbeeld van een tabel

| Kolom 1 | Kolom 2 | Kolom 3 |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |

# Chapter 4

# Richtlijnen voor formules

Er zijn twee manieren om formules in LaTeX in te voeren:

- Inline: $a^2+b^2=c^2$ (`$a^2+b^2 = c^2$`)
- In een equation omgeving (`\begin{equation} a^2+b^2 = c^2 \end{equation}`):

$$a^2+b^2=c^2 \tag{4.1}$$

Griekse letters geef je in d.m.b. het backslash commando. Bijvoorbeeld de letter sigma $\sigma$ verkrijg je door `$\sigma$` inline in te geven. Dit is analoog voor griekse letters in de equation omgeving. Een beknopte lijst van symbolen vind je op de Wikibooks pagina voor LaTeX (link). Alle andere nuttige informatie omtrent het gebruik van LaTeX voor formules vind je hier ook terug.

# Chapter 5

# Richtlijnen voor referenties

## 5.1 Inleiding

De referentielijst bevat de volledige lijst van literatuur en bronnen waarnaar in de tekst wordt verwezen. Door systematisch de referentielijst aan te vullen bij het schrijven van het literatuuroverzicht gaat er achteraf geen tijd verloren aan het opnieuw opzoeken van referenties.

## 5.2 Referentiestijl

Voor het verwijzen naar informatiebronnen wordt gebruik gemaakt van het numerisch systeem of van het auteur-jaar systeem. Dit kies je door volgend commando in het latex bronbestand aan te passen:

- numerisch (IEEE) : `\bibliographystyle{ieee}`
- alfabetisch (APA) : `\bibliographystyle{apalike}`

Plaats je bronnen in een *bibtex* bestand (evt. via software zoals bv. Jabref Endnote of Mendeley), waarnaar je verwijst vanuit je thesis text a.d.h.v. het commando `\cite`. Enkele links naar nuttige software in deze context:

- JabRef (Open Source)
- Mendeley (Freeware)
- EndNote (Paid license)

Indien je zelf een .bibtex bestand wil aanleggen dien je volgende syntax te volgen voor een tijdschriftartikel:

```
@article{hughes2005,
title={Isogeometric analysis: CAD, finite elements, NURBS, exact geometry
and mesh refinement},
author={Hughes, Thomas JR and Cottrell, John A and Bazilevs, Yuri},
journal={Computer methods in applied mechanics and engineering},
volume={194},
number={39},
pages={4135--4195},
year={2005},
publisher={Elsevier}
}
```

Enkele voorbeelden van het gebruik van bronnen in een tekst (in APA stijl):

Recent werd het Higgs boson experimenteel vastgesteld door Aad et al. Aad et al. (2012) (syntax: `\cite{aad2012}`).

Als alternatief voor het discretiseren van een CAD model vooraleer een eindige elementenanalyse te kunnen toepassen, stellen Hughes et al. voor om de nodige elementenformulering rechtstreeks uit de NURBS beschrijving van de CAD geometrie te halen Hughes et al. (2005) (syntax: `\cite{hughes2005}`). Daarnaast introduceren ze tevens een k-iteratieve procedure als een verfijning van de geldende p- en h-iteratieve procedures in eindige elementen methoden Cottrell et al. (2009) (syntax: `\cite{cottrell2009}`).

# Bibliography

Aad, G., Abajyan, T., Abbott, B., Abdallah, J., Khalek, S. A., Abdelalim, A., Abdinov, O., Aben, R., Abi, B., Abolins, M., et al. (2012). Observation of a new particle in the search for the standard model higgs boson with the atlas detector at the lhc. *Physics Letters B*, 716(1):1–29.

Cottrell, J. A., Hughes, T. J., and Bazilevs, Y. (2009). *Isogeometric analysis: toward integration of CAD and FEA*. John Wiley & Sons.

Hughes, T. J., Cottrell, J. A., and Bazilevs, Y. (2005). Isogeometric analysis: Cad, finite elements, nurbs, exact geometry and mesh refinement. *Computer methods in applied mechanics and engineering*, 194(39):4135–4195.

# Appendix A

# Uitleg over de appendices

Bijlagen worden bij voorkeur enkel elektronisch ter beschikking gesteld. Indien essentieel kunnen in overleg met de promotor bijlagen in de scriptie opgenomen worden of als apart boekdeel voorzien worden.

Er wordt wel steeds een lijst met vermelding van alle bijlagen opgenomen in de scriptie. Bijlagen worden genummerd het een drukletter A, B, C,...

Voorbeelden van bijlagen:

Bijlage A: Detailtekeningen van de proefopstelling

Bijlage B: Meetgegevens (op USB)

FACULTY OF ENGINEERING TECHNOLOGY
DE NAYER (SINT-KATELIJNE-WAVER) CAMPUS
Jan De Nayerlaan 5
2860 SINT-KATELIJNE-WAVER, België
tel. + 32 16 30 10 30
fet.denayer@kuleuven.be
www.fet.kuleuven.be