KU LEUVEN

FACULTY OF ENGINEERING TECHNOLOGY

DE NAYER (SINT-KATELIJNE-WAVER) CAMPUS

Object Detection on Encrypted Data

Using Secure Multiparty Computation

Felix LERNER

Promotor: Prof. dr. ir. Toon Goedemé
Co-promotor: Dr. Pradip Mainali (Onespan)

Masterproef ingediend tot het behalen van de graad van master of Science in de industriële wetenschappen: Industriele Wetenschappen Electronica-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 the backend processing serverside, because it's easier to debug and it's faster to roll out new updates. 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

1 Introduction

1.1 Problem

1.2 Hypothesis

2

Literature study

2.1 Background concepts

2.1.1 Deep learning

2.1.2 Cryptography

2.2 Convolutional neural network

2.2.1 Architecture

2.2.1.1 Convolution layer

2.2.1.2 Activation function

2.2.1.3 Pooling layer

2.2.1.4 Fully connected layer

2.2.1.5 Loss function

2.2.2 Evaluation

2.3 Secure multiparty computation

2.3.1 Secret sharing

2.3.2 Operations

2.3.2.1 Artithmetic operators

2.3.2.2 Relational operators

2.3.3 Share recombination

2.4 Malicious adverseries

2.5 Conclusion

3

Implementation

3.1 Specifications

3.2 Design

3.3 Conclusion

4 Evaluation

4.1 Results

4.1.1 Reliability results

4.1.2 Timing results

4.2 Discussion

4.3 Conclusion

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 σ 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.

5 Conclusion

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.

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