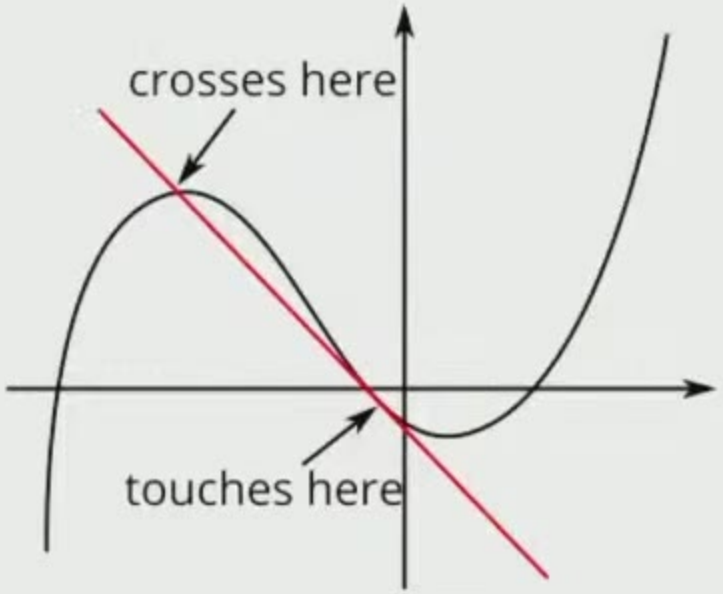
Touching Points of Cryptography and AI



Moti Yung

AI and Cryptography ????

- Crypto is theory-oriented, precise, clean notions of security, have Proofs which explain security of primitives, etc. (...then comes the messy implementations)...
- AI: practice oriented, approximation, computing that has no exact explanation but it works well…

So, what do they have in common???????

I will argue: It's not a "Match Made in Heaven" But "it's not Hell" either to find connections!

AI and Cryptography ????

- Crypto is theory-oriented, precise, clean notions of security, have Proofs which explain security of primitives, etc. (...then comes the messy implementations)...
- AI: practice oriented, approximation, computing that has no exact explanation but it works well…

So, what do they have in common???????

I will argue: It's not a "Match Made in Heaven" But "it's not Hell" either to find connections!

AI and Cryptography ????

- Crypto is theory-oriented, precise, clean notions of security, have Proofs which explain security of primitives, etc. (...then comes the messy implementations)...
- AI: practice oriented, approximation, computing that has no exact explanation but it works well…

So, what do they have in common???????

I will argue: It's not a "Match Made in Heaven" But "it's not Hell" either to find connections!

AI and Cryptography ????

- Crypto is theory-oriented, precise, clean notions of security, have Proofs which explain security of primitives, etc. (...then comes the messy implementations)...
- AI: practice oriented, approximation, computing that has no exact explanation but it works well…

So, what do they have in common???????

I will argue: It's not a "Match Made in Heaven" But "it's not Hell" either to find connections!

AI and Cryptography ????

- Crypto is theory-oriented, precise, clean notions of security, have Proofs which explain security of primitives, etc. (...then comes the messy implementations)...
- AI: practice oriented, approximation, computing that has no exact explanation but it works well…

So, what do they have in common???????

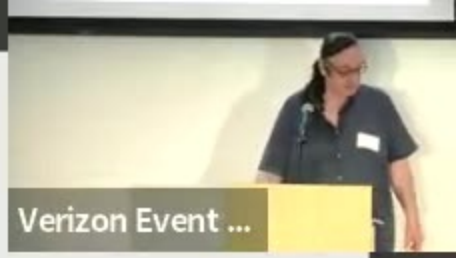
I will argue: It's not a "Match Made in Heaven" But "it's not Hell" either to find connections!

Talk about AI and Cryptography ????

- In [Crypto 23] Scott Aaronson gave a talk about Cryptography and AI, claiming he is an expert in neither…

- Why now? AI is in the process of development where due to investment in algorithms, storage, hw, and other computing resources, it is solving problems that are meaningful…

- Like any technology, it needs protection, & protection of various sorts needs cryptography!
- AI works very well [we don't always know why]-- until attacks start!



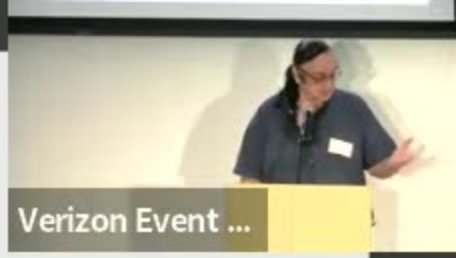
Agenda

I will cover some points of interest in the intersection of AI and Cryptography

I think it is an interesting general area: AI will augment everything, so it has to augment Cryptographic R&D.

I will point at issues, the treatment is of a survey nature: no deep technical details, and the focus is on the broad sense in which AI can influence Cryptography and vice versa! (Some is based on my work, others' work, some thoughts, some plans).

I will try to convince you that it does not matter what your crypto subfield of interest, AI is important to consider!



Agenda

I will cover some points of interest in the intersection of AI and Cryptography

I think it is an interesting general area: AI will augment everything, so it has to augment Cryptographic R&D.

I will point at issues, the treatment is of a survey nature: no deep technical details, and the focus is on the broad sense in which AI can influence Cryptography and vice versa! (Some is based on my work, others' work, some thoughts, some plans).

I will try to convince you that it does not matter what your crypto subfield of interest, AI is important to consider!

Agenda

I will cover some points of interest in the intersection of AI and Cryptography

I think it is an interesting general area: AI will augment everything, so it has to augment Cryptographic R&D.

I will point at issues, the treatment is of a survey nature: no deep technical details, and the focus is on the broad sense in which AI can influence Cryptography and vice versa! (Some is based on my work, others' work, some thoughts, some plans).

I will try to convince you that it does not matter what your crypto subfield of interest, AI is important to consider!

Agenda

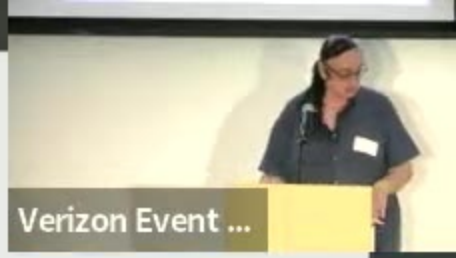
I will cover some points of interest in the intersection of AI and Cryptography

I think it is an interesting general area: AI will augment everything, so it has to augment Cryptographic R&D.

I will point at issues, the treatment is of a survey nature: no deep technical details, and the focus is on the broad sense in which AI can influence Cryptography and vice versa! (Some is based on my work, others' work, some thoughts, some plans).

I will try to convince you that it does not matter what your crypto subfield of interest, AI is important to consider!

01
Introduction



AI and Crypto: First Touching Point
A.M. Turing

- Pragmatic View of early Machine Intelligence: The Turing Test (leave philosophy aside and let us be pragmatic!!)
- Worked in Cryptography: Breaking Enigma during WWII- pragmatism!

AI and Crypto: First Touching Point
A.M. Turing

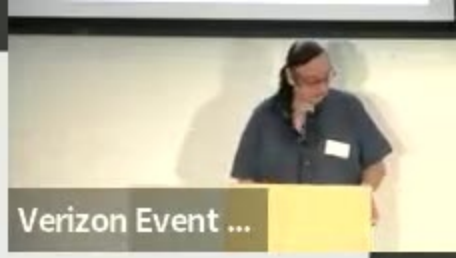
- Pragmatic View of early Machine Intelligence: The Turing Test (leave philosophy aside and let us be pragmatic!!)
- Worked in Cryptography: Breaking Enigma during WWII- pragmatism!

Two Different Fields- AI Evolution

- Invented as a term in the 50s (name given in 56)
- Philosophical foundations: Theory of the Human Mind: is the brain a computer?
- Practical Foundations (like Cybernetics before) to automate tasks that require learning and inference.
- Goals: Let computing Systems Think like humans, Act like humans, be rational (already some contradiction here!)
- The father of AI, John McCarthy defines AI as, "The science and engineering of making intelligent machines, especially intelligent computer programs."
  - [THIS IS DELIBERATELY SELF-REFERENCIAL]

Two Different Fields- AI Evolution

- Invented as a term in the 50s (name given in 56)
- Philosophical foundations: Theory of the Human Mind: is the brain a computer?
- Practical Foundations (like Cybernetics before) to automate tasks that require learning and inference.
- Goals: Let computing Systems Think like humans, Act like humans, be rational (already some contradiction here!)
- The father of AI, John McCarthy defines AI as, "The science and engineering of making intelligent machines, especially intelligent computer programs."
  - [THIS IS DELIBERATELY SELF-REFERENCIAL]



Two Different Fields- AI Evolution

- Invented as a term in the 50s (name given in 56)
- Philosophical foundations: Theory of the Human Mind: is the brain a computer?
- Practical Foundations (like Cybernetics before) to automate tasks that require learning and inference.
- Goals: Let computing Systems Think like humans, Act like humans, be rational (already some contradiction here!)
- The father of AI, John McCarthy defines AI as, "The science and engineering of making intelligent machines, especially intelligent computer programs."
  - [THIS IS DELIBERATELY SELF-REFERENCIAL]

More AI Characteristics

- AI in the early/mid 80s (post the General Problem Solver (GPS) of Simon, Show, Newell) identified practical subareas:
  - Learning: inductive inference
  - Planning: breaking a task to sub-tasks
  - Speech/ Language Recognition: recognition, understanding, and generation
  - Problem-solving (e.g., fast heuristic search)
  - Knowledge (representation and processing)
  - Perception (vision)

1980-87 a lot of activities (partially motivated by the Japanese 5th gen computing)

In 1987-2000 AI 2d winter re-started, people were overly pessimistic but in the last ~20 years a very fast moving evolution re-started! (1st winter was 1974-1980 after GPS failure)

More AI Characteristics

- AI in the early/mid 80s (post the General Problem Solver (GPS) of Simon, Show, Newell) identified practical subareas:
  - Learning: inductive inference
  - Planning: breaking a task to sub-tasks
  - Speech/ Language Recognition: recognition, understanding, and generation
  - Problem-solving (e.g., fast heuristic search)
  - Knowledge (representation and processing)
  - Perception (vision)

1980-87 a lot of activities (partially motivated by the Japanese 5th gen computing)

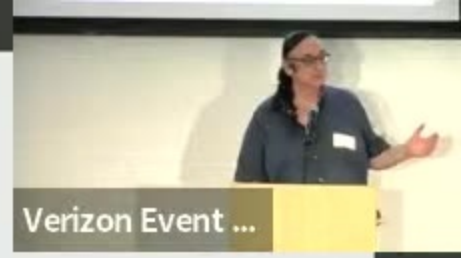
In 1987-2000 AI 2d winter re-started, people were overly pessimistic but in the last ~20 years a very fast moving evolution re-started! (1st winter was 1974-1980 after GPS failure)

More AI Characteristics

- AI in the early/mid 80s (post the General Problem Solver (GPS) of Simon, Show, Newell) identified practical subareas:
  - Learning: inductive inference
  - Planning: breaking a task to sub-tasks
  - Speech/ Language Recognition: recognition, understanding, and generation
  - Problem-solving (e.g., fast heuristic search)
  - Knowledge (representation and processing)
  - Perception (vision)

1980-87 a lot of activities (partially motivated by the Japanese 5th gen computing)

In 1987-2000 AI 2d winter re-started, people were overly pessimistic but in the last ~20 years a very fast moving evolution re-started! (1st winter was 1974-1980 after GPS failure)



More AI Characteristics

- AI in the early/mid 80s (post the General Problem Solver (GPS) of Simon, Show, Newell) identified practical subareas:
  - Learning: inductive inference
  - Planning: breaking a task to sub-tasks
  - Speech/ Language Recognition: recognition, understanding, and generation
  - Problem-solving (e.g., fast heuristic search)
  - Knowledge (representation and processing)
  - Perception (vision)

1980-87 a lot of activities (partially motivated by the Japanese 5th gen computing)

In 1987-2000 AI 2d winter re-started, people were overly pessimistic but in the last ~20 years a very fast moving evolution re-started! (1st winter was 1974-1980 after GPS failure)

More AI Characteristics

- AI in the early/mid 80s (post the General Problem Solver (GPS) of Simon, Show, Newell) identified practical subareas:
  - Learning: inductive inference
  - Planning: breaking a task to sub-tasks
  - Speech/ Language Recognition: recognition, understanding, and generation
  - Problem-solving (e.g., fast heuristic search)
  - Knowledge (representation and processing)
  - Perception (vision)

1980-87 a lot of activities (partially motivated by the Japanese 5th gen computing)

In 1987-2000 AI 2d winter re-started, people were overly pessimistic but in the last ~20 years a very fast moving evolution re-started! (1st winter was 1974-1980 after GPS failure)

Modern Cryptography Evolution

- Started as a research discipline: 70s: DES, DH, RSA (as an art it is ancient).
- Foundations (proofs for PKC, canonical distinguishers for SKC): 80s
- Practical Foundations (90s) and ZK/MPC.
- Standardizations and competitions (NIST etc.) as a tool
- 2000's: Crypto currencies/ applied industrial use of MPC/ FHE
- 2010: Post-Quantum; Post-Snowden, light-weight
- …. Government involvement (Crypto wars) and Legal/Policy consideration as global systems like cloud/ mobile are built

Essentially: a solid field with foundations moving ahead, and practice advances in support of information security as well

But: is advances in AI mean we have insurmountable challenges now? opportunities?

Modern Cryptography Evolution

- Started as a research discipline: 70s: DES, DH, RSA (as an art it is ancient).
- Foundations (proofs for PKC, canonical distinguishers for SKC): 80s
- Practical Foundations (90s) and ZK/MPC.
- Standardizations and competitions (NIST etc.) as a tool
- 2000's: Crypto currencies/ applied industrial use of MPC/ FHE
- 2010: Post-Quantum; Post-Snowden, light-weight
- …. Government involvement (Crypto wars) and Legal/Policy consideration as global systems like cloud/ mobile are built

Essentially: a solid field with foundations moving ahead, and practice advances in support of information security as well

But: is advances in AI mean we have insurmountable challenges now? opportunities?

Modern Cryptography Evolution

- Started as a research discipline: 70s: DES, DH, RSA (as an art it is ancient).
- Foundations (proofs for PKC, canonical distinguishers for SKC): 80s
- Practical Foundations (90s) and ZK/MPC.
- Standardizations and competitions (NIST etc.) as a tool
- 2000's: Crypto currencies/ applied industrial use of MPC/ FHE
- 2010: Post-Quantum; Post-Snowden, light-weight
- …. Government involvement (Crypto wars) and Legal/Policy consideration as global systems like cloud/ mobile are built

Essentially: a solid field with foundations moving ahead, and practice advances in support of information security as well

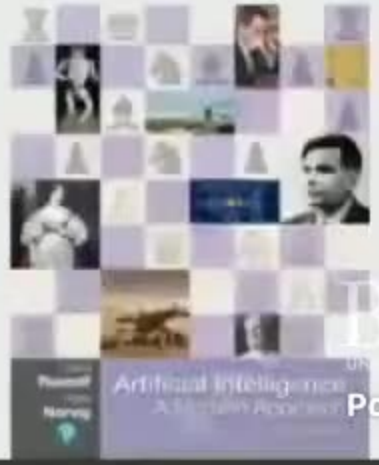
But: is advances in AI mean we have insurmountable challenges now? opportunities?

BTW:My First Encounters with AI: Heuristic Search in

Worked on Heuristic Search (83-85):

- Bruce Abramson, Moti Yung: **Construction Through Decomposition: A Divide-and-Conquer Algorithm for the N-Queens Problem.** FJCC 1986, (J. Parallel Distributed Comput, 1989)
  - N-Queen was a classical "Heuristic Search/ backtracking" example; we found an algorithm Making General Search Obsolete! O(n) algorithm!
- Othar Hansson, Andrew Mayer, Moti Yung: **Criticizing solutions to relaxed models yields powerful admissible heuristics.** Inf. Sci. 1992, (tech report 1985)
  - Relaxing models to guide Heuristic Search -- sometimes you can tighten the relaxation to get a better search…..

Cited in "The Book": Russell and Norvig: Artificial Intelligence: A modern Approach (section 3: Heuristic Search pages 110, 119)



BTW:My First Encounters with AI: Heuristic Search in

Worked on Heuristic Search (83-85):

- Bruce Abramson, Moti Yung: **Construction Through Decomposition: A Divide-and-Conquer Algorithm for the N-Queens Problem.** FJCC 1986, (J. Parallel Distributed Comput, 1989)
  - N-Queen was a classical "Heuristic Search/ backtracking" example; we found an algorithm Making General Search Obsolete! O(n) algorithm!
- Othar Hansson, Andrew Mayer, Moti Yung: **Criticizing solutions to relaxed models yields powerful admissible heuristics.** Inf. Sci. 1992, (tech report 1985)
  - Relaxing models to guide Heuristic Search -- sometimes you can tighten the relaxation to get a better search…..

Cited in "The Book": Russell and Norvig: Artificial Intelligence: A modern Approach (section 3: Heuristic Search pages 110, 119)

What is the Second Touching Point?

Obviously……..…

2d Touching Point: Indistinguishability as a security notion in cryptography

…is modeled after the Turing Test!

[a major pragmatic attraction for theory and foundations of the field]

What is the Second Touching Point?

Obviously……..…

2d Touching Point: Indistinguishability as a security notion in cryptography

…is modeled after the Turing Test!

[a major pragmatic attraction for theory and foundations of the field]

What is the Second Touching Point?

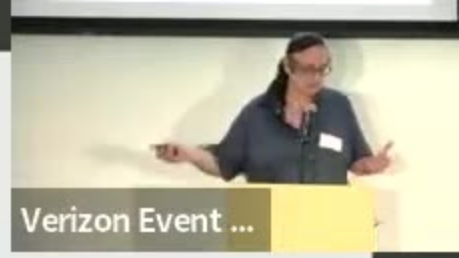
Obviously……..…

2d Touching Point: Indistinguishability as a security notion in cryptography

…is modeled after the Turing Test!

[a major pragmatic attraction for theory and foundations of the field]

What is the Second Touching Point?



Obviously…….…

2d Touching Point: Indistinguishability as a security notion in cryptography

…is modeled after the Turing Test!

[a major pragmatic attraction for theory and foundations of the field]

02

Modern AI and Cryptography
The current touching points

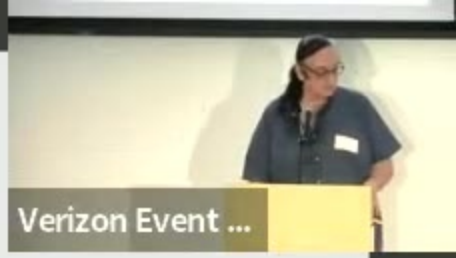
02

Modern AI and Cryptography
The current touching points

Berkeley
UNIVERSITY OF CALIFORNIA

02

Modern AI and Cryptography
The current touching points



Natural Touching Points 3: Crypto-Computing

- Modern Cryptographic Computing has developed tools that are universal computing engines (at least when the computing program size is known)
  - MPC
  - FHE
- This is a natural meeting point where a single centralized agent who knows all the data and build a model and applies the model is replaced by a committee of two or more agents which perform the task where no one knows more than the input contribution.

Natural Touching Points 3: Crypto-Computing

- Modern Cryptographic Computing has developed tools that are universal computing engines (at least when the computing program size is known)
  - MPC
  - FHE
- This is a natural meeting point where a single centralized agent who knows all the data and build a model and applies the model is replaced by a committee of two or more agents which perform the task where no one knows more than the input contribution.

Natural Touching Points 3: Crypto-Computing

- Modern Cryptographic Computing has developed tools that are universal computing engines (at least when the computing program size is known)
  - MPC
  - FHE
- This is a natural meeting point where a single centralized agent who knows all the data and build a model and applies the model is replaced by a committee of two or more agents which perform the task where no one knows more than the input contribution.

Natural Touching Points 3: Crypto-Computing

- Modern Cryptographic Computing has developed tools that are universal computing engines (at least when the computing program size is known)
  - MPC
  - FHE
- This is a natural meeting point where a single centralized agent who knows all the data and build a model and applies the model is replaced by a committee of two or more agents which perform the task where no one knows more than the input contribution.

Natural Touching Points 3: Crypto-Computing

- Modern Cryptographic Computing has developed tools that are universal computing engines (at least when the computing program size is known)
  - MPC
  - FHE
- This is a natural meeting point where a single centralized agent who knows all the data and build a model and applies the model is replaced by a committee of two or more agents which perform the task where no one knows more than the input contribution.

Next: Security/Crypto to protect AI/ AI to augment security

- In General people talk about:
  - AI to augment security (like architecture reviews etc.)
  - Security to protect AI (protect models etc.). **What's here:**

Touching point 4:

- Blackbox probing of a model→ learning a model (resembles cryptanalysis or learning a cipher from probes) [Crypto'20: Carlini, Jagielski, and Mironov; Eurocrypt'24: Shamir et al.].

Next: Security/Crypto to protect AI/ AI to augment security

- In General people talk about:
  - AI to augment security (like architecture reviews etc.)
  - Security to protect AI (protect models etc.). **What's here:**

Touching point 4:

- Blackbox probing of a model→ learning a model (resembles cryptanalysis or learning a cipher from probes) [Crypto'20: Carlini, Jagielski, and Mironov; Eurocrypt'24: Shamir et al.].

Touching Point 5

- Augment Security (in particular augment Cryptography)
  - Help or Automate Proofs of Complex Cryptographic Protocols. Go beyond formal methods…
  - Model behavior; Model Attacks; model Inability to perform the attack
  - Use statistical inference (LLMs say) to aid cryptographers? Can it be done effectively, helping design/ finding design bugs/ etc.

Touching Point 5

- Augment Security (in particular augment Cryptography)
  - Help or Automate Proofs of Complex Cryptographic Protocols. Go beyond formal methods…
  - Model behavior; Model Attacks; model Inability to perform the attack
  - Use statistical inference (LLMs say) to aid cryptographers? Can it be done effectively, helping design/ finding design bugs/ etc.

Touching Point 6:

Distributed Learning and privacy
Federated Learning and variants

- When I was in Snapchat (2016-18) ….. We had a case of distributed events at Mobile Phone, so we got a learning alg that was federated.-- (You use AI when needed…) Differentially-Private "Draw and Discard" Machine Learning (DDML)

- Meanwhile in Google, the Federated Learning effort was strong and important!!!

Touching Point 6:

Distributed Learning and privacy
Federated Learning and variants

- When I was in Snapchat (2016-18) ….. We had a case of distributed events at Mobile Phone, so we got a learning alg that was federated.-- (You use AI when needed…) Differentially-Private "Draw and Discard" Machine Learning (DDML)

- Meanwhile in Google, the Federated Learning effort was strong and important!!!

Touching Point 7: Side Channel Attacks

- (1) 1996: Kocher initiated SCA (Crypto 96).

- (2) 2009: François-Xavier Standaert, Tal Malkin, Moti Yung: **A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks.** EUROCRYPT 2009:
  - One of the point is an extended attack model adding a preliminary statistical study/ model with known keys and learn the chip behavior!!! [BTW: ****ToT Eurocrypt-2024]

- Hence, stronger AI techniques can also be used in the extended model: (3) Elie Bursztein, Luca Invernizzi, Karel Král, Daniel Moghimi, Jean Michel Picod, Marina Zhang: **Generic Attacks against Cryptographic Hardware through Long-Range Deep Learning.** CoRR abs/2306.07249 (2023)

Touching Point 7: Side Channel Attacks

- (1) 1996: Kocher initiated SCA (Crypto 96).

- (2) 2009: François-Xavier Standaert, Tal Malkin, Moti Yung: **A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks.** EUROCRYPT 2009:
  - One of the point is an extended attack model adding a preliminary statistical study/ model with known keys and learn the chip behavior!!! [BTW: ****ToT Eurocrypt-2024]

- Hence, stronger AI techniques can also be used in the extended model: (3) Elie Bursztein, Luca Invernizzi, Karel Král, Daniel Moghimi, Jean Michel Picod, Marina Zhang: **Generic Attacks against Cryptographic Hardware through Long-Range Deep Learning.** CoRR abs/2306.07249 (2023)

Touching Point 8

- Using AI/ML in Cryptanalysis in general (Thanks to Elie Bursztein for this part)

Touching Point 8

- Using AI/ML in Cryptanalysis in general (Thanks to Elie Bursztein for this part)

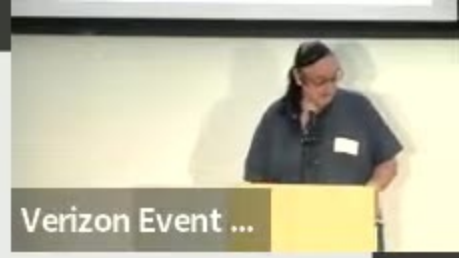
Touching Point 9

- Using Cryptographic Protections to modify models and attacks on data
- The case of Reliable AI.
  - Attacks on Data are very strong, attacker can do everything to inputs…
  - What if data manipulation is limited:
  - Sources **sign the data items**? One cannot add data only drop some….

- **Deniz Koyuncu, Alex Gittens, Bülent Yener, Moti Yung**:

Deception by Omission: Using Adversarial Missingness to Poison Causal Structure Learning. KDD 2023

The work shows that learning a causal structure (DAG of causal dependencies) can be attacked with targeted non-random missingness only (i.e. even when data is signed by reliable source)!



Touching Point 10

- **Deep fake**
  - We use to Authentication (signing MAC-ing) etc. serving as data authenticity.
  - But with Deep Fake the attack is on the cleartext value.
  - What needs to be done to detect Fake and Attest for originality?

This is a current challenge. What a solution can attempt to do using AI and Cryptography??

More questions (????) than definite answers (!!!!)

Touching Point 10

- **Deep fake**
  - We use to Authentication (signing MAC-ing) etc. serving as data authenticity.
  - But with Deep Fake the attack is on the cleartext value.
  - What needs to be done to detect Fake and Attest for originality?

This is a current challenge. What a solution can attempt to do using AI and Cryptography??

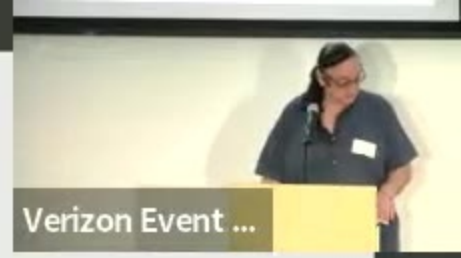
More questions (????) than definite answers (!!!!)

Touching Point 10

- **Deep fake**
  - We use to Authentication (signing MAC-ing) etc. serving as data authenticity.
  - But with Deep Fake the attack is on the cleartext value.
  - What needs to be done to detect Fake and Attest for originality?

This is a current challenge. What a solution can attempt to do using AI and Cryptography??

More questions (????) than definite answers (!!!!)



Touching Point 11

What can Cryptographic methods add to AI understanding/ Theory of AI?

FOCS 22: Shafi Goldwasser, Michael P. Kim, Vinod Vaikuntanathan, Or Zamir:
Planting Undetectable Backdoors in Machine Learning Models.

- Planting Backdoor by a server learning a model (assuming digital signature scheme)
- Indistinguishability between backdoored model and clean model under cryptographic assumption.

So: Cryptographic computational complexity assumptions tell us something about modeling malicious errors!

Touching Point 11

What can Cryptographic methods add to AI understanding/ Theory of AI?

FOCS 22: Shafi Goldwasser, Michael P. Kim, Vinod Vaikuntanathan, Or Zamir:
Planting Undetectable Backdoors in Machine Learning Models.

- Planting Backdoor by a server learning a model (assuming digital signature scheme)
- Indistinguishability between backdoored model and clean model under cryptographic assumption.

So: Cryptographic computational complexity assumptions tell us something about modeling malicious errors!

Touching Point 11

What can Cryptographic methods add to AI understanding/ Theory of AI?

FOCS 22: Shafi Goldwasser, Michael P. Kim, Vinod Vaikuntanathan, Or Zamir:
Planting Undetectable Backdoors in Machine Learning Models.

- Planting Backdoor by a server learning a model (assuming digital signature scheme)
- Indistinguishability between backdoored model and clean model under cryptographic assumption.

So: Cryptographic computational complexity assumptions tell us something about modeling malicious errors!

Touching Point 11

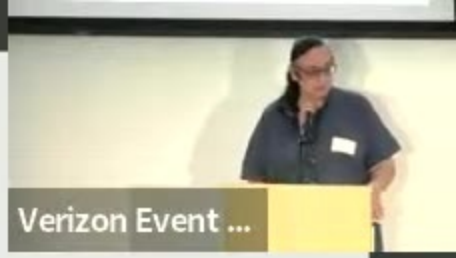
What can Cryptographic methods add to AI understanding/ Theory of AI?

FOCS 22: Shafi Goldwasser, Michael P. Kim, Vinod Vaikuntanathan, Or Zamir:
Planting Undetectable Backdoors in Machine Learning Models.

- Planting Backdoor by a server learning a model (assuming digital signature scheme)
- Indistinguishability between backdoored model and clean model under cryptographic assumption.

So: Cryptographic computational complexity assumptions tell us something about modeling malicious errors!

Touching Point 12: a non technical one



What are the societal impact & implications of AI and Cryptography?

- Cryptography makes remote interactions safe and automates transactions (e.g., cryptocurrency replacing physical payments)
- AI makes human-like missions automated (e.g., recommendation systems automate planning of daily life).

So: Together and in combination, how life/ work/ society/ is going to evolve as traditional face to face human transactions and traditional human experts are being misplaced?

03
Conclusions

03
Conclusions

03
Conclusions

So… I hope I convinced you…

- Many ways for AI and Cryptography to touch each other.
- I just chose some points I worked on/ heard about/ like/ think about in general/ and still do not know much about.
- Some problems are heavily investigated, some other important ones are ignored.
- The notion of touching points is open ended, and I am sure this is not an exhaustive list (AI is in a fast path of change).
- The field connecting AI and Crypto is young (embryonic, in fact): Find your own new point! I think it is fascinating!
- Noted: it does not matter what sub-field of cryptography one works in, AI will touch or be touched by it!

So:

Berkeley Center for Responsible, Decentralized Intelligence

Summit on Responsible Decentralized Intelligence — Future of Decentralization and AI

August 6, 2024

Verizon Center, NYC

Berkeley UNIVERSITY OF CALIFORNIA

Powered by Zoom

Berkeley Center for Responsible, Decentralized Intelligence

Summit on Responsible Decentralized Intelligence — Future of Decentralization and AI

August 6, 2024

Verizon Center, NYC

Berkeley UNIVERSITY OF CALIFORNIA

Powered by Zoom

Berkeley Center for Decentraliz

Session II: Decentralized AI, Cryptography & Confidential Compute

Decentralized Confidential AI: Federated Learning with Confidential Computing

Chester Chen
Senior Manager
Nvidia

Summit on Responsible Decentralized Intelligence
— Future of Decentralization and AI

August 6, 2024
Verizon Center, NYC

Berkeley
UNIVERSITY OF CALIFORNIA

Powered by Zoom

Berkeley Center for Decentraliz

Session II: Decentralized AI, Cryptography & Confidential Compute

Decentralized Confidential AI: Federated Learning with Confidential Computing

Chester Chen
Senior Manager
Nvidia

Berkeley Center for Decentraliz

Session II: Decentralized AI, Cryptography & Confidential Compute

Decentralized Confidential AI: Federated Learning with Confidential Computing

Chester Chen
Senior Manager
Nvidia