Homomorphic Voting Scheme

By Raj Thimmiah

Goal

- To understand the importance of privacy and integrity in a fair voting scheme
- Illustrate a basic working example of a homomorphic voting scheme which solves the two aforementioned issues
- To understand that no voting scheme is perfect

Why is privacy important in general?

- Access to someone's personal information can be used to:
  - Threaten
  - Influence
  - Damage reputations
  - Violate freedoms in thinking, beliefs, daily actions

Why is privacy critical for voting?

- Privacy can be implemented by service providers
- Usage of privacy is optional
  - Users can violate privacy by sharing their own data
- In voting, **violating your own privacy cannot be allowed for a fair vote!**

Do you like Python or Java better?

Why was lack of privacy harmful?

- Group think/peer pressure
- Discrimination and retribution
- Bribery

All of these issues violate the sanctity and trustability of the results of the vote

Do you like Python or Java better?

Did we have the same privacy issues?

- Group think/peer pressure
  - No risk of someone judging you or you seeing what everyone else thinks
- Discrimination and retribution
  - No one can prove you voted a certain way (except me) and thus no risk of discrimination or retribution
- Bribery
  - You could accept Martin's bribe, vote for Java and lie to him about the result
  - There is no "receipt" that could prove you voted a certain way

The authorities in charge of the vote can still violate privacy

Was the vote really added up correctly?

Verifiability

- Cast-as-intended (important for digital systems):
  - The voting system marked the choice correctly
- Recorded-as-cast
  - The vote that was cast was also recorded by the system correctly
- Tallied-as-recorded
  - The vote was added correctly

Verifiability

- Eligibility verification
- Accountability
  - Ability to prove failure of the system and to re-submit a vote
- Robustness
- Usability
- Accessibility

End to End Verifiability

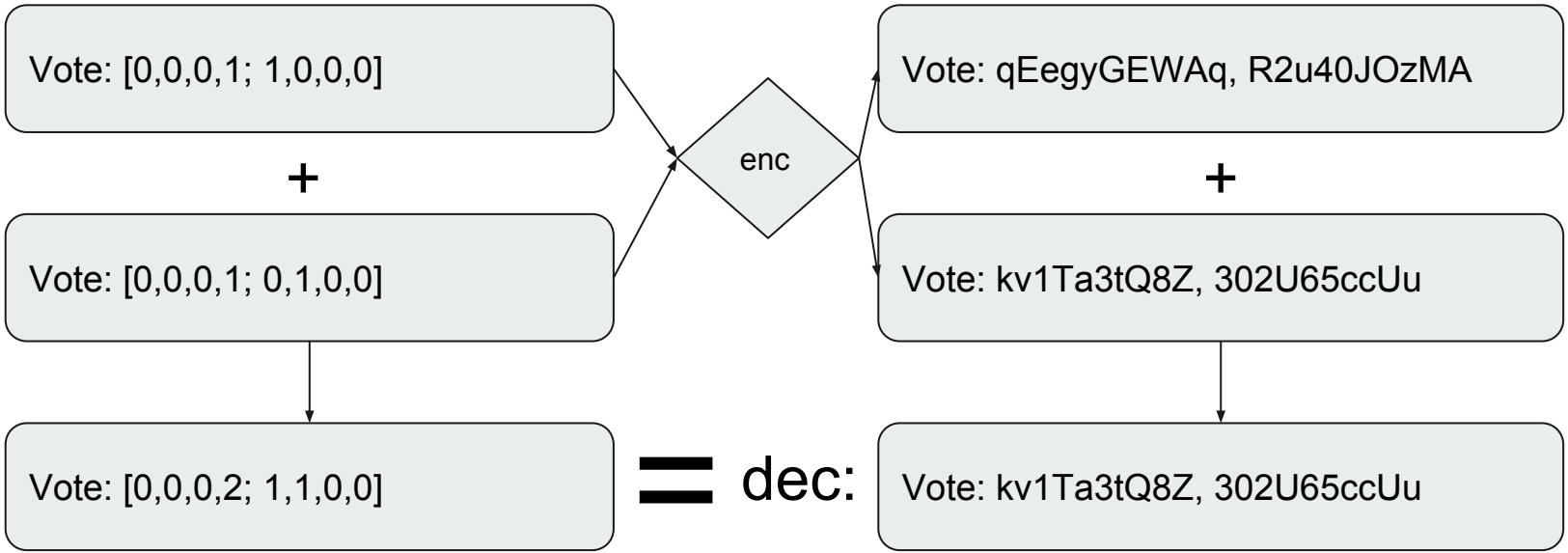
Raj	Java
Martin	Python
Adel	Python

Python	2
Java	1

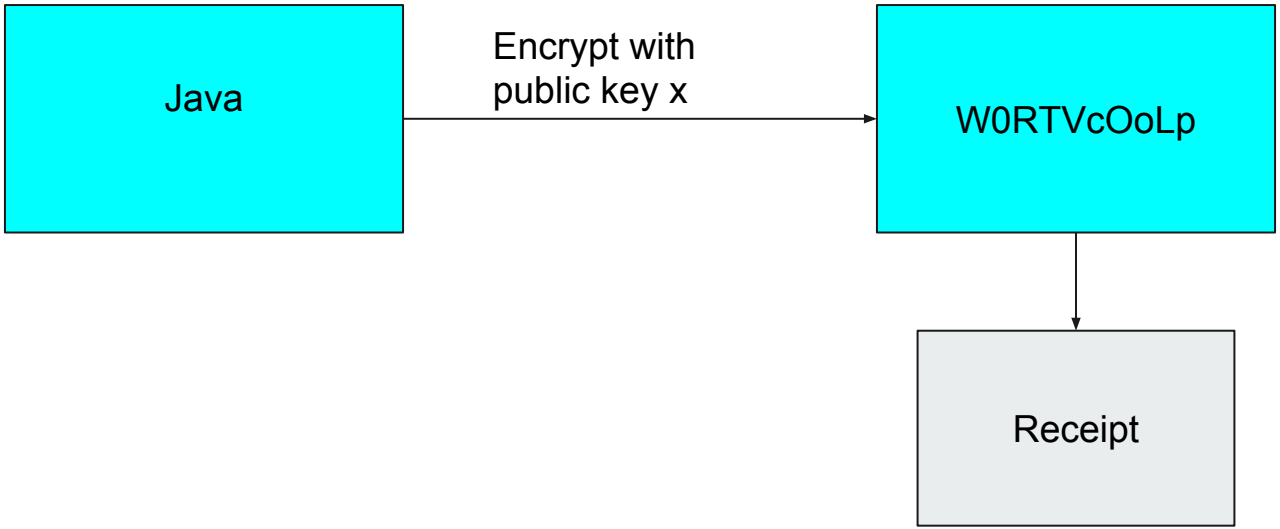
Homomorphic Encryption

- Additively Homomorphic Scheme:
  - X + Y
  - ENC(X) + ENX(Y) = ENC(X + Y)

Homomorphic Encryption



Vote



End to End Verifiability

Raj	W0RTVcOoLp
Martin	56LjKngjOk
Adel	g4k23fsCom

Python	uGYHrEnVNT
Java	kgKoepq8L0

Public/Private Key Encryption

- Public key is shared with everyone
  - Can be used to encrypt data
- Private key is hidden
  - Can be used to decrypt data encrypted with a corresponding public key

Threshold Encryption

- Split private key into n shares
- N shares are given to people
- X out of N shares are needed to decrypt
- Until X nodes are malicious and collude, individual privacy is guaranteed

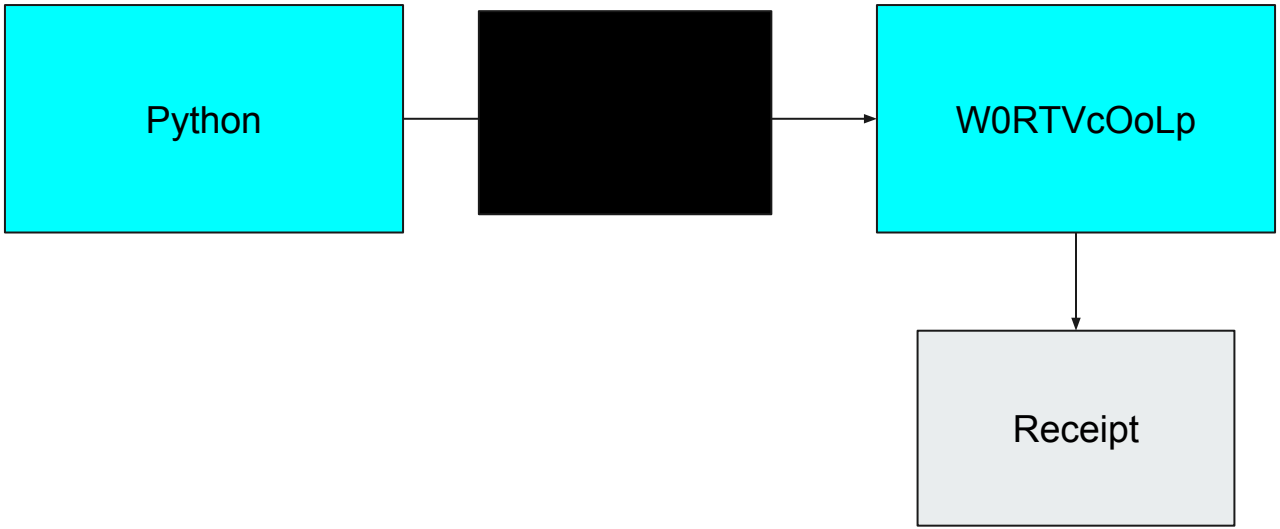
Verifiability

- Cast-as-intended (important for digital systems):
  - The voting system marked the choice correctly
- Recorded-as-cast
  - The vote that was cast was also recorded by the system correctly
- Tallied-as-recorded
  - The vote was added correctly

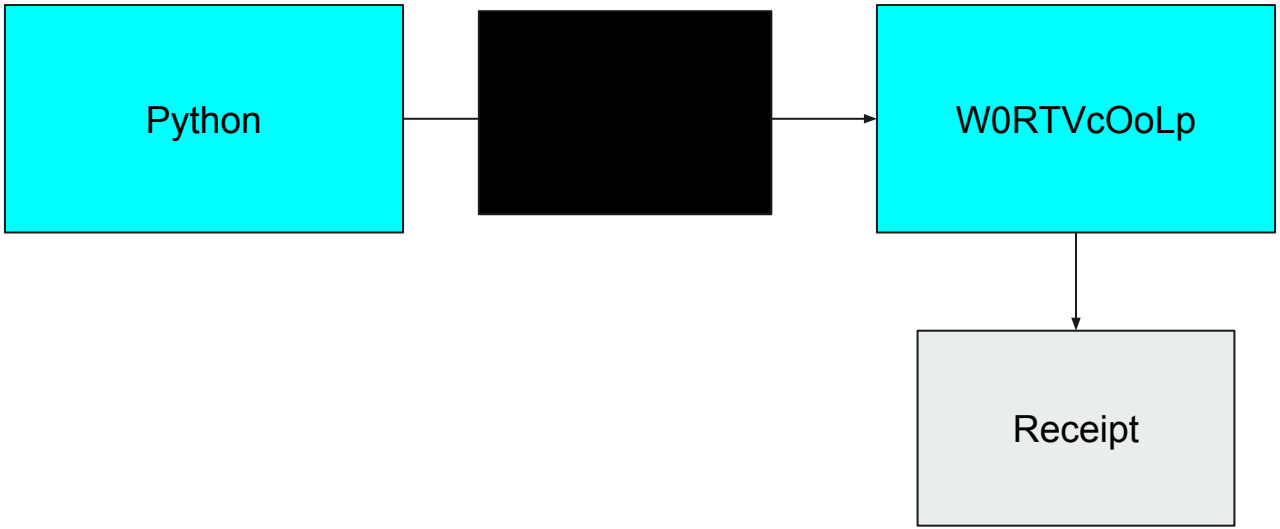
Verifiability

- Cast-as-intended (important for digital systems):
  - The voting system marked the choice correctly
- Recorded-as-cast
  - The vote that was cast was also recorded by the system correctly
- Tallied-as-recorded
  - The vote was added correctly

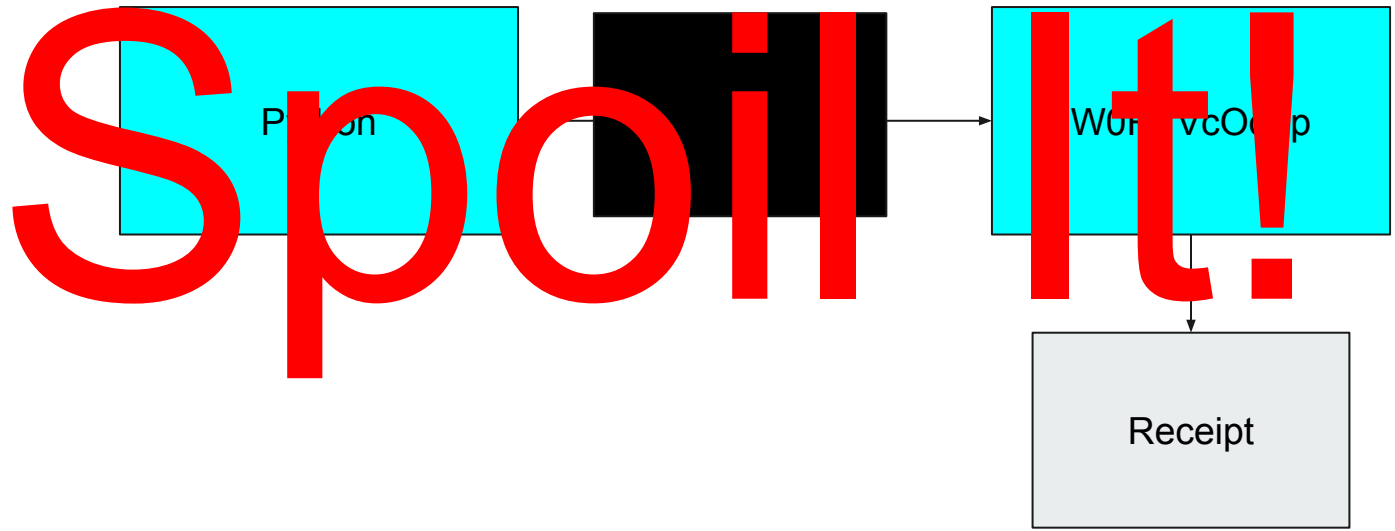
Voting Machines are Black Boxes



Challenge the machine!



Challenge the machine!



Spoiling Ballots

- When you want to challenge, you spoil the ballot
- Spoiled ballots are added in a separate section
- They are decrypted at the end and you can check that it was encoded correctly

End to End Verifiability

Raj	W0RTVcOoLp
Martin	56LjKngjOk
Adel	g4k23fsCom

Python	uGYHrEnVNT
Java	kgKoepq8L0

Java	48giABRpkR (Spoiled Ballot)

Verifiability

- Cast-as-intended (important for digital systems):
  - The voting system marked the choice correctly
- Recorded-as-cast
  - The vote that was cast was also recorded by the system correctly
- Tallied-as-recorded
  - The vote was added correctly

Why can’t we vote remotely?

- Can be coerced to vote a certain way more easily
- Malware can also cause issues
- Might be difficult to use for some voters

We can’t actually prevent coercion!

Coercion Resistance

- On site coercion should not be able to violate privacy
- Cannot be forced into submitting voting materials
- Cannot be forced to not vote
- Cannot be forced to randomly vote
- JCJ/Civitas

Verifiability

- Eligibility verification
- Accountability
  - Ability to prove failure of the system and to re-submit a vote
- Robustness
- Usability
- Accessibility

Star Vote

https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell

Please fill out this survey!

Citations

1. https://robindoherty.com/2016/01/06/nothing-to-hide.html
2. https://teachprivacy.com/10-reasons-privacy-matters/
3. https://www.youtube.com/watch?v=zC-rJX0Nmxg
4. An Overview of End-to-End Verifiable Voting Systems
5. https://www.usenix.net/legacy/events/evt06/tech/full_papers/benaloh/benaloh.pdf
6. https://www.usenix.org/system/files/conference/evtwote13/jets-0101-bell.pdf
7. https://eprint.iacr.org/2013/464.pdf