Anamorphic Encryption: Private Communication against a Dictator

Based on the paper by: Giuseppe Persiano, Moti Yung and Duong Hieu Phang

By: Deanna Dixon

What is Encryption and Cryptography?

Encryption

This is the process of converting information into code. This is usually used to try and prevent unauthorized access

Cryptography

- This is a process of hiding and coding information so only certain people can read it.
- Assumes that decryption and encryption process are done privately by sender and receiver
- Sender-Freedom: The sender chooses what him/her wants on the message freely
- Receiver-Freedom: The receiver(s) only know what the decryption key entails

Modern threats of both

- Technology has gotten more advanced
- Governments want access to the messages

The Dictator

The dictator is someone who has control over the communication systems

- What he can do:
- Can legally have users surrender to the private keys which breaks the privacy of the receiver
- Can force users to send certain messages which breaks the freedom of a sender

- The challenges that come with that:
- There is no privacy in which the dictator can decrypt messages and control what it contains
- Such governments can/will seek similar control

The Situation

Current situation: A lot of governments might/will demand power of private keys
Kerckhoffs Principle: This is when the security of the cryptographic system should not rely on how secure the algorithm is and instead it should be based on how secret the cryptography key is.
Normative Assumptions: this is when users won't be forced to reveal their keys. But governments can override this
Computational Assumptions: hardness of inverting one-way function and can't be changed by an order. This is a more mathematical approach
Dictators can override the Normative Assumptions but can't override the mathematical laws that come with Computational Assumptions

The Anamorphic Encryption

The response to the Dictator:

- This paper suggests the idea of Anamorphic Encryption, so even if/when a dictator acquires the keys, secret communication is possible

How it works:

- The dictator will select the message and how random the encryption is, and the users will have to follow the command
- In this secret channel, the trusted users can use the public-key cryptosystem in a special way to plant a hidden message in the ciphertext
- To extract the message: only the people who have the special anamorphic key will be able to extract the hidden messages while others (ex: dictator) can only see the dictated message

Why this can work:

- This can work because users can disguise the ciphertext like a regular message and users can prove to the dictator that it encrypts only certain detailed content

Technical Implications

01

Construction

- This is built on already existing public-key cryptosystems
- Many standard cryptosystems like El Gamal and RSA can be extended to support functionality

02

Challenges

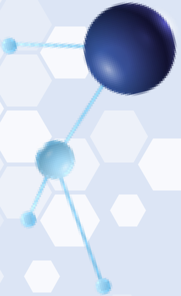
- Needs to be hidden so that the government doesn't make it illegal
- Anamorphic keys must be blended in with standard key management practices
- Must have trustworthy people
- Size can be smaller depending on the mesaage

03

Security and Practical

Dictators usually can't tell if a ciphertext contains hidden information

This field is changing and developing rapidly so there will be new methods coming out



Societal and Policy Impact

How it goes against control:

- Shows that government efforts to try and control policy encryptions are pointless
- Even if some cryptosystems are outlawed, secret communication still remains possible

Implications for human rights

- Protects journalists and ordinary citizens from authoritarian overreach
- Reinforces that privacy is a human right and not just for a technology feature
- Gives individuals more rights

Summary

- Anamorphic encryption enables secret and private communication between a sender and receiver. This can be used even when a dictator (or high power) controls both keys and messages by using the public key cryptosystems
- Traditional cryptography relies on sender-freedom and receiver-freedom privacy that can be taken away by government. (normative)
- Instead, it uses a mathematical approach to this so governments can't override this. (computational)
- There are some limitations like the size of the messages could be smaller
- But even if the dictator owns keys and messages, covert communication is possible.
- This is an attempt to help individuals gain privacy back