ANAMORPHIC ENCRYPTION: PRIVATE COMMUNICATION AGAINST A DICTATOR

BYPASSING COERCION IN MODERN CRYPTO SYSTEMS

Fanizza Tahir
James Madison University
June 16, 2025

THE PROBLEM: CRYPTO UNDER COERCION

Traditional Cryptography's Vulnerable Assumptions:

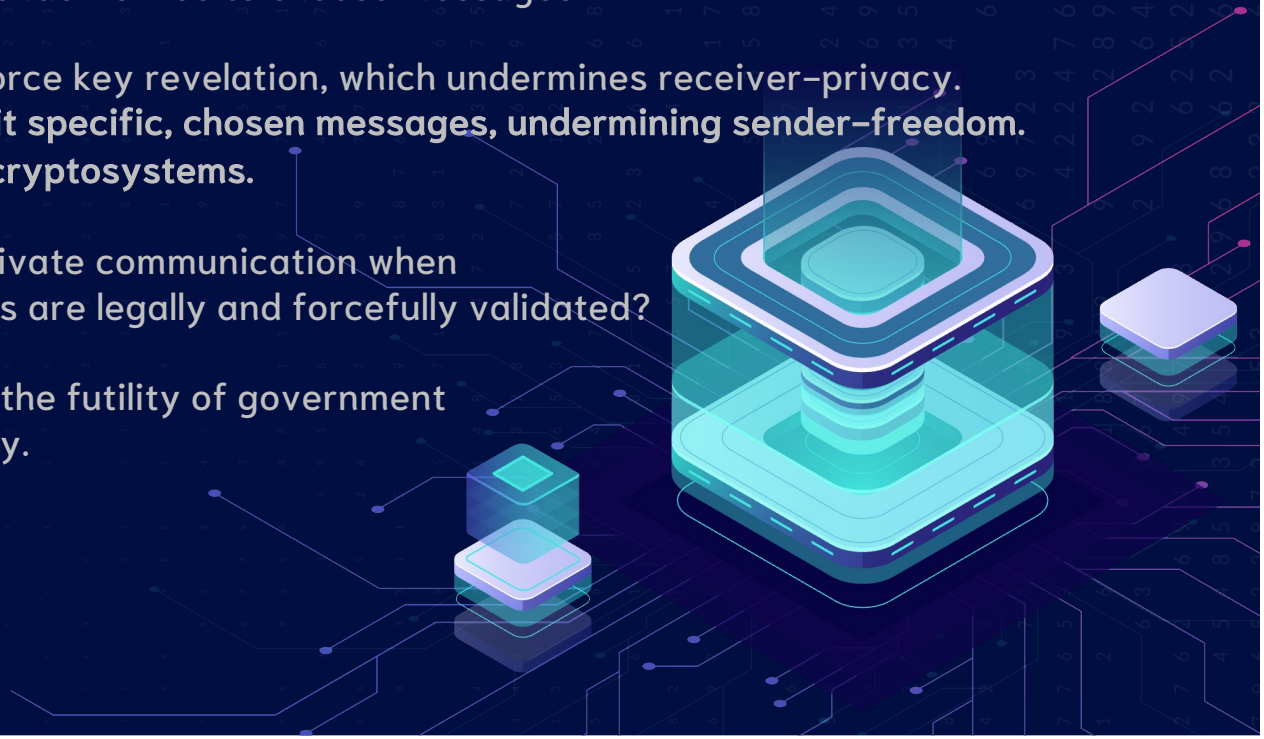
- **Receiver-Privacy: Assumes that a receiver's private key remains secure.**
- **Sender-Freedom:** Assumes sender is free to choose messages.

The Dictator's Challenge:

- Coercive governments can force key revelation, which undermines receiver-privacy.
- **Can force senders to transmit specific, chosen messages, undermining sender-freedom.**
- **This may outlaw alternative cryptosystems.**

The Core Problem: How do we ensure private communication when fundamental cryptographic assumptions are legally and forcefully validated?

Motivation: To technically demonstrate the futility of government attempts to control strong cryptography.



WHAT IS ANAMORPHIC ENCRYPTION?

Anamorphic Encryption: a special encryption scheme whose public keys can be generated in one of two modes: normal or anamorphic.

Analogy: Like a distorted drawing that appears normal when viewed from a specific point or with a suitable mirror or lens.

Core Idea: Two messages in One Ciphertext:

- **Overt Message (m_0): The normal message, visible to the dictator upon decryption with the normal secret key.**
- **Covert/Anamorphic Message (m_1):** The hidden, special message that's only visible to parties with the double secret key.

Key Requirements for Plausibility & Security:

- Anamorphic public/secret key pairs must be indistinguishable from normal corresponding pairs.
- Ciphertexts produced using an anamorphic public key must be indistinguishable from those produced by a normal public key.

Goals: Zero-latency communication and high anamorphic bandwidth rate.

RECEIVER-ANAMORPHIC ENCRYPTION (COMBATTING KEY SURRENDER)

GOAL: "To protect a receiver's private message (m_1), even if the secret key is surrendered."

Naor–Yung Basis Mechanism

STEP 1	STEP 2	STEP 3	STEP 4
Bob generates 'aPK', 'aSK' (for dictator), 'dkey' (for Alice).	Alice encrypts (m_0, m_1) with 'dkey' to 'act'.	Dictator decrypts 'act' with 'aSK' to m_0.	Bob decrypts 'act' with 'dkey' to m_1.

Key Feature:
Simulated NIZK makes 'act' appear normal

Benefits:
Bandwidth Rate 1, Zero-Latency

SENDER-ANAMORPHIC ENCRYPTION

GOAL: "Alice sends (m_1) to Bob, while appearing to send (m_0) to Carol, even if coerced."

Key Idea:
No prior shared secret between Alice and Bob needed.

Lattice-Based Mechanism:

1. Alice uses 'fRandom' (coin-toss faking algorithm)
2. Generates randomness R* for ct = Enc(fPK, m_0; R*)
3. ct decrypts to m_0 (with Carol's fSK) and m_1 (with Bob's dSK)

Requirements: "Common randomness," "message recovery from randomness," "equal distribution of plaintexts."

SECURITY AND INDISTINGUISHABILITY

CORE PRINCIPLE: "Dictator cannot distinguish between 'normal' and 'fully anamorphic'"

FORMAL PROOF (VIA GAMES)

'NormalGame' vs. 'FullyAGame'

Probably of distinguishing is negligible.

IMPLICATIONS

Secrecy of m_1: Covert message remains hidden

Plausibility: Operations appear legitimate; no suspicion raised.

UNDERLYING TOOLS

Underlying Tools: IND-CPA secure PKE and Simulation Sound NIZK.

PRACTICALITY AND LIMITATIONS

ADVANTAGES

- Leverages Existing Cryptosystems.
- Zero-Latency Communication
- High Bandwidth Rate (Receiver-AM)
- No Shared Secret (Sender-AM)

CHALLENGES

- Simple Rejection Sampling in Inefficient
- Shared ‘dkey’ for Receiver-AM (can be a physical exchange).
- Not all PKEs naturally Anamorphic (Ex. Goldwasser-Micali for Sender-AM).
- Potential “Crypto Wars” of banning specific schemes

CONCLUSION

SUMMARY Anamorphic Encryption demonstrates the futility of government control over strong crypto.

IMPACT Empowers private communication even under extreme duress.

FUTURE Explore anamorphic properties in more cryptosystems

Combine Anamorphism with other covert techniques (steganography, kleptography)

Analyze broader policy and societal implications.


THANK YOU