Anamorphic Encryption

Private Communication against a Dictator

Giuseppe Persiano, Duong Hieu Phan, Moti Yung

Eurocrypt 2022 – Trondheim

Privacy as a Human Right

UDHR, Article 12: (1948)

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence,...

End to End Encryption

- Cryptography has been very successful in providing tools for encrypting communication
  - The Signal protocol and app

But its success relies on two assumptions that might be challenged in dictatorial states

Privacy as a Human Right

UDHR, Article 12: (1948)

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence,...

End to End Encryption

- Cryptography has been very successful in providing tools for encrypting communication
  - The Signal protocol and app

But its success relies on two assumptions that might be challenged in dictatorial states

Privacy as a Human Right

UDHR, Article 12: (1948)

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence,...

End to End Encryption

- Cryptography has been very successful in providing tools for encrypting communication
  - The Signal protocol and app

But its success relies on two assumptions that might be challenged in dictatorial states

The receiver-privacy assumption

Encryption guarantees message confidentiality only with respect to parties that do not have access to the receiver's private key

The receiver-privacy assumption

The receiver keeps his secret key in a private location

The sender-freedom assumption

A ciphertext carries the message that was provided as an input, not the one that the sender wishes to encrypt

The sender-freedom assumption

The sender is free to pick the message to be encrypted

Ok...two more assumptions

Why is this a problem?

Theorem

Assume existence of one-way functions and receiver privacy. Then, there exist secure symmetric encryption schemes.

Two assumptions

- Existence of one-way functions
- Ability to hide my key

Law of Nature vs Normative Prescription

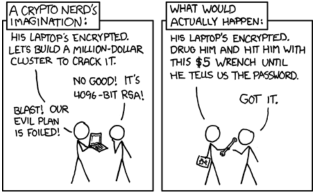
- Assumption of the existence of one-way functions comes from *our current scientific understanding of Nature*
  - if true, it is enforced by Nature
  - it might be false but then it is false for all

- Receiver privacy is a *norm*:
  - it is enforced by political power
  - it can be changed by law, decree, force
  - it could change for some but not for all

Receiver privacy and Sender freedom

- Both assumptions are realistic for "normal" settings
- No wonder Encryption has been developed under these assumptions
  - with no explicit mention

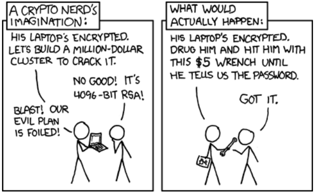
- In a dictatorship, instead
  - No receiver privacy: citizens might be invited to surrender their private keys



  - No sender freedom: citizens might be invited to send messages to international newspapers to make the dictator look good

Receiver privacy and Sender freedom

- Both assumptions are realistic for “normal” settings
- No wonder Encryption has been developed under these assumptions
  - with no explicit mention
- In a dictatorship, instead
  - No receiver privacy: citizens might be invited to surrender their private keys

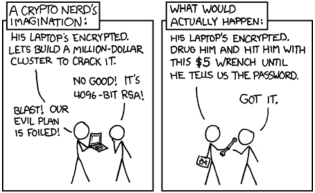


  - No sender freedom: citizens might be invited to send messages to international newspapers to make the dictator look good

Receiver privacy and Sender freedom

- Both assumptions are realistic for "normal" settings
- No wonder Encryption has been developed under these assumptions
  - with no explicit mention

- In a dictatorship, instead
  - No receiver privacy: citizens might be invited to surrender their private keys



  - No sender freedom: citizens might be invited to send messages to international newspapers to make the dictator look good

Not only dictators...

Various attempts to regulate, limit, cripple encryption

Crypto Wars

Presently, anyone can obtain encryption devices for voice or data transmissions. [...] if criminals can use advanced encryption technology in their transmissions, electronic surveillance techniques could be rendered useless because of law enforcement's inability to decode the message.

Howard S. Dakoff
The Clipper Chip Proposal
J. Marshall L. Rev., 29, 1996.

Crypto Wars

- Combination of cryptographic tools and normative prescription
- From [Micali 1992] to [Green-Kaptchuk-van Laer 2021]
  - Rely on the existence of an independent judiciary system (missing in a Dictatorship!)
- Kleptography [Young-Yung 97]
- Subvertable encryption

How can we fix this?

Not by designing new schemes

- Suppose we design an encryption scheme that is secure without assuming receiver privacy and/or sender freedom
- What is the dictator going to do?
  - It will be considered illegal
  - The simple act of using the new scheme will be self accusatory
  - The encryption scheme and its use will be seen as provocations

Rather, we should look at existing *schemes to see if they can be used to defeat the dictator*

Existing schemes cannot be disallowed as there are legitimate uses for them. Legitimate, even for the dictator.

How can we fix this?

Not by designing new schemes

- Suppose we design an encryption scheme that is secure without assuming receiver privacy and/or sender freedom
- What is the dictator going to do?
  - It will be considered illegal
  - The simple act of using the new scheme will be self accusatory
  - The encryption scheme and its use will be seen as provocations

Rather, we should look at existing *schemes to see if they can be used to defeat the dictator*

Existing schemes cannot be disallowed as there are legitimate uses for them. Legitimate, even for the dictator.

How can we fix this?

Not by designing new schemes

- Suppose we design an encryption scheme that is secure without assuming receiver privacy and/or sender freedom
- What is the dictator going to do?
  - It will be considered illegal
  - The simple act of using the new scheme will be self accusatory
  - The encryption scheme and its use will be seen as provocations

Rather, we should look at existing *schemes to see if they can be used to defeat the dictator*

Existing schemes cannot be disallowed as there are legitimate uses for them. Legitimate, even for the dictator.

How can we fix this?

Not by designing new schemes

- Suppose we design an encryption scheme that is secure without assuming receiver privacy and/or sender freedom
- What is the dictator going to do?
  - It will be considered illegal
  - The simple act of using the new scheme will be self accusatory
  - The encryption scheme and its use will be seen as provocations

Rather, we should look at existing *schemes to see if they can be used to defeat the dictator*

Existing schemes cannot be disallowed as there are legitimate uses for them. Legitimate, even for the dictator.

Our approach

Let us focus first on receiver privacy

Constraints

- If the dictator has the secret key $\mathtt{sk}$, it can decrypt and read the message.
- But only the message encrypted with respect to $\mathtt{sk}$ can be decrypted.

Our approach

- A ciphertext is associated with two secret keys $\mathtt{sk}_0, \mathtt{sk}_1$
- A ciphertext carries two plaintexts m_0, m_1, one for each key
- ...and there is **no** second key
  - at least, that's what the dictator thinks

Our approach

Let us focus first on receiver privacy

Constraints

- If the dictator has the secret key $\mathtt{sk}$, it can decrypt and read the message.
- But only the message encrypted with respect to $\mathtt{sk}$ can be decrypted.

Our approach

- A ciphertext is associated with two secret keys $\mathtt{sk}_0, \mathtt{sk}_1$
- A ciphertext carries two plaintexts m_0, m_1, one for each key
- ...and there is **no** second key
  - at least, that's what the dictator thinks

Our approach

Let us focus first on receiver privacy

Constraints

- If the dictator has the secret key $\mathtt{sk}$, it can decrypt and read the message.
- But only the message encrypted with respect to $\mathtt{sk}$ can be decrypted.

Our approach

- A ciphertext is associated with two secret keys $\mathtt{sk}_0, \mathtt{sk}_1$
- A ciphertext carries two plaintexts m_0, m_1, one for each key
- ...and there is **no** second key
  - at least, that's what the dictator thinks

Rejection Sampling Encryption

Bellare, Paterson, Rogaway [CRYPTO14]
Horel, Park, Richelson, Vaikuntanathan [ITCS19]

Normal mode

- $\mathcal{E} = (\texttt{KG}, \texttt{Enc}, \texttt{Dec})$ any encryption scheme
- Alice has $(\texttt{pk}, \texttt{sk})$
- Bob computes $\texttt{ct} = \texttt{Enc}(\texttt{pk}, \text{"Glory to our Leader"})$
- Dictator decrypts $\texttt{ct}$ using $\texttt{sk}$

Anamorphic mode

- Alice and Bob share a randomly chosen seed K for a PRF $\mathcal{F}$
- Bob wants to send a bit b to Alice
  - samples $\texttt{ct} = \texttt{Enc}(\texttt{pk}, \text{"Glory to our Leader"})$
  - until $\mathcal{F}(K, \texttt{ct}) = b$

Rejection Sampling Encryption

Bellare, Paterson, Rogaway [CRYPTO14]
Horel, Park, Richelson, Vaikuntanathan [ITCS19]

Normal mode

- $\mathcal{E} = (\mathtt{KG}, \mathtt{Enc}, \mathtt{Dec})$ any encryption scheme
- Alice has $(\mathtt{pk}, \mathtt{sk})$
- Bob computes $\mathtt{ct} = \mathtt{Enc}(\mathtt{pk}, \text{“Glory to our Leader”})$
- Dictator decrypts $\mathtt{ct}$ using $\mathtt{sk}$

Anamorphic mode

- Alice and Bob share a randomly chosen seed K for a PRF $\mathcal{F}$
- Bob wants to send a bit b to Alice
  - samples $\mathtt{ct} = \mathtt{Enc}(\mathtt{pk}, \text{“Glory to our Leader”})$
  - until $\mathcal{F}(K, \mathtt{ct}) = b$

Receiver privacy

Feasibility result

Rejection sampling encryption gives a one-bit symmetric encryption scheme whose secure does not rely on the receiver-privacy assumption.

Rate

- *Rejection Sampling* can be extended to any length ℓ
- Average encryption time is exponential in ℓ

Receiver Anamorphic

Receiver privacy

Feasibility result

Rejection sampling encryption gives a one-bit symmetric encryption scheme whose secure does not rely on the receiver-privacy assumption.

Rate

- *Rejection Sampling* can be extended to any length ℓ
- Average encryption time is exponential in ℓ

Receiver Anamorphic

Receiver privacy

Feasibility result

Rejection sampling encryption gives a one-bit symmetric encryption scheme whose secure does not rely on the receiver-privacy assumption.

Rate

- *Rejection Sampling* can be extended to any length ℓ
- Average encryption time is exponential in ℓ

Receiver Anamorphic

Our technical contribution

- Receiver Anamorphic for many bits
  - Rejection Sampling only work for few bits

- Sender Anamorphic with no shared key
  - Rejection Sampling assumes Alice and Bob share a key

  for this we need extra properties

The Naor-Yung Encryption Scheme

Normal Mode

- Let $\mathcal{E} = (\mathtt{KG}, \mathtt{Enc}, \mathtt{Dec})$ any encryption scheme
- Alice runs $\mathtt{KG}$ twice, randomly selects Σ and sets $\mathtt{pk} = (\mathtt{pk}_0, \mathtt{pk}_1, \Sigma)$ and $\mathtt{sk} = \mathtt{sk}_0$
- If Bob wants to send "Glory to our Leader" to Alice
  - Compute $\mathtt{ct}_0 = \mathtt{Enc}(\mathtt{pk}_0, \text{"Glory to our Leader"})$
  - Compute $\mathtt{ct}_1 = \mathtt{Enc}(\mathtt{pk}_1, \text{"Glory to our Leader"})$
  - Compute NIZK proof Π that $\mathtt{ct}_0$ and $\mathtt{ct}_1$ carry the same plaintext
  - Set $\mathtt{ct} = (\mathtt{ct}_0, \mathtt{ct}_1, \Pi)$
- To decrypt $\mathtt{ct}$, Alice
  - Checks Π is a valid proof
  - If valid decrypts $\mathtt{ct}_0$ using $\mathtt{sk}$

The Naor-Yung Encryption Scheme

Anamorphic Mode

- Alice runs $\mathtt{KG}$ twice, runs the simulator to get $(\Sigma, \mathtt{aux})$ and sets $\mathtt{pk} = (\mathtt{pk}_0, \mathtt{pk}_1, \Sigma)$ and $\mathtt{sk} = (\mathtt{sk}_0, \mathtt{sk}_1)$
- $\mathtt{aux}$ is shared with Bob
- If Bob wants to send "Glory to our Leader" to the dictator and "F*** our Leader" to Alice
  - Compute $\mathtt{ct}_0 = \mathtt{Enc}(\mathtt{pk}_0, \text{"Glory to our Leader"})$
  - Compute $\mathtt{ct}_1 = \mathtt{Enc}(\mathtt{pk}_1, \text{"F*** our Leader"})$
  - Simulate NIZK proof Π that $\mathtt{ct}_0$ and $\mathtt{ct}_1$ carry the same plaintext
  - Set $\mathtt{ct} = (\mathtt{ct}_0, \mathtt{ct}_1, \Pi)$
- To decrypt $\mathtt{ct}$, Alice uses $\mathtt{sk}_1$ to decrypt $\mathtt{ct}_1$
- If asked to surrender her secret key, Alice gives $\mathtt{sk}_0$
  - The dictator verifies Π, decrypts $\mathtt{ct}_0$ and reads "Glory to our Leader"

Why does this work?

Informal

- NIZK implies that the anamorphic and the normal public keys are indistinguishable
- NIZK+IND CPA imply ciphertexts are indistinguishable
- If asked to surrender secret key, Alice gives $\mathtt{sk} := \mathtt{sk}_0$
  - $\mathtt{pk}_1$ could be generated without the associated secret key (e.g., El Gamal has this property)
- $(\mathtt{pk}_0, \mathtt{pk}_1, \Sigma, \mathtt{aux})$ is a symmetric encryption key

The Sender-Freedom Assumption

- *The sender is free to choose the message*

The dictator can force the sender to send a message of his choice

Sender Anamorphic Encryption

The story of Oscar and John

- Oscar, an opposition leader, is "asked" by the Leader to send the following message to some media outlet

  $$m_0 = \text{"I am fine and in good health"}$$

  to a forced public key $\mathtt{fpk}$

- Oscar wants also to send message

  $$m_1 = \text{"I am in prison"}$$

  to the public key $\mathtt{dpk}$ of a journalist John

- Oscar computes special coin tosses $R^\star$ such that by setting $\mathtt{ct} = \mathtt{Enc}(\mathtt{fpk}, m_0; R^\star)$ it holds that

  $$m_1 = \mathtt{Dec}(\mathtt{dsk}, \mathtt{ct})$$

No prior shared knowledge is needed between Oscar and John

Sender Anamorphic Encryption

The story of Oscar and John

- Oscar, an opposition leader, is "asked" by the Leader to send the following message to some media outlet

  $$m_0 = \text{“I am fine and in good health”}$$

  to a forced public key $\mathtt{fpk}$

- Oscar wants also to send message

  $$m_1 = \text{“I am in prison”}$$

  to the public key $\mathtt{dpk}$ of a journalist John

- Oscar computes special coin tosses $R^\star$ such that by setting $\mathtt{ct} = \mathtt{Enc}(\mathtt{fpk}, m_0; R^\star)$ it holds that

  $$m_1 = \mathtt{Dec}(\mathtt{dsk}, \mathtt{ct})$$

No prior shared knowledge is needed between Oscar and John

Sender Anamorphic Encryption

The story of Oscar and John

- Oscar, an opposition leader, is "asked" by the Leader to send the following message to some media outlet
$$m_0 = \text{"I am fine and in good health"}$$
to a forced public key $\mathtt{fpk}$
- Oscar wants also to send message
$$m_1 = \text{"I am in prison"}$$
to the public key $\mathtt{dpk}$ of a journalist John
- Oscar computes special coin tosses $R^\star$ such that by setting $\mathtt{ct} = \mathtt{Enc}(\mathtt{fpk}, m_0; R^\star)$ it holds that
$$m_1 = \mathtt{Dec}(\mathtt{dsk}, \mathtt{ct})$$

No prior shared knowledge is needed between Oscar and John

Sender Anamorphic Encryption

The story of Oscar and John

- Oscar, an opposition leader, is “asked” by the Leader to send the following message to some media outlet

$$m_0 = \text{“I am fine and in good health”}$$

  to a forced public key $\mathtt{fpk}$
- Oscar wants also to send message

$$m_1 = \text{“I am in prison”}$$

  to the public key $\mathtt{dpk}$ of a journalist John
- Oscar computes special coin tosses $R^\star$ such that by setting $\mathtt{ct} = \mathtt{Enc}(\mathtt{fpk}, m_0; R^\star)$ it holds that

$$m_1 = \mathtt{Dec}(\mathtt{dsk}, \mathtt{ct})$$

No prior shared knowledge is needed between Oscar and John

Sender Anamorphic Encryption

The story of Oscar and John

- Oscar, an opposition leader, is "asked" by the Leader to send the following message to some media outlet
$$m_0 = \text{"I am fine and in good health"}$$
to a forced public key $\mathtt{fpk}$
- Oscar wants also to send message
$$m_1 = \text{"I am in prison"}$$
to the public key $\mathtt{dpk}$ of a journalist John
- Oscar computes special coin tosses $R^\star$ such that by setting $\mathtt{ct} = \mathtt{Enc}(\mathtt{fpk}, m_0; R^\star)$ it holds that
$$m_1 = \mathtt{Dec}(\mathtt{dsk}, \mathtt{ct})$$

No prior shared knowledge is needed between Oscar and John

Sender Anamorphic vs Deniable Encryption

Deniable encryption:

- applies to the *same* public key
- is not suitable for dictator setting: It was mentioned in [CDNO97] that deniability is impossible where "*Eve [the adversary] approaches Alice [the sender]* before *the transmission and requires Alice [the sender] to send specific messages*".
- is impossible for a standard encryptions [CDNO97] (This contradicts our objective to use standard encryptions).

Sender Anamorphic Encryption can be used to provide some form of deniability

- ciphertext is now broadcast over a public channel and not sent on a point to point channel
- denying having sent a message m to John under the ciphertext $\mathtt{ct}$, by proving that $\mathtt{ct}$ corresponds to a message m' sent to Carol.

Sender Anamorphic vs Deniable Encryption

Deniable encryption:

- applies to the *same* public key
- is not suitable for dictator setting: It was mentioned in [CDNO97] that deniability is impossible where "*Eve [the adversary] approaches Alice [the sender]* before *the transmission and requires Alice [the sender] to send specific messages*".
- is impossible for a standard encryptions [CDNO97] (This contradicts our objective to use standard encryptions).

Sender Anamorphic Encryption can be used to provide some form of deniability

- ciphertext is now broadcast over a public channel and not sent on a point to point channel
- denying having sent a message m to John under the ciphertext $\mathtt{ct}$, by proving that $\mathtt{ct}$ corresponds to a message m' sent to Carol.

Sufficient conditions for Sender Anamorphic with no shared key

Any PKE satisfying the 3 following conditions is sender anamorphic.

1. *Common randomness property*.
   For any $c = \texttt{Enc}(\texttt{pk}, m, r)$ and any $\texttt{pk}'$, there is a m' such that $c = \texttt{Enc}(\texttt{pk}', m', r)$
2. *Message recovery from randomness*.
   Given the ciphertext and the used randomness, one can recover the corresponding message.
3. *Equal Distribution of Plaintexts*.
   Given any c in the ciphertext space, for a randomly generated secret key sk: $Pr[\texttt{Dec}(sk, c) = 0] = Pr[\texttt{Dec}(sk, c) = 1]$

Consequently:

- LWE encryption by Regev, 2005
- Dual LWE encryption by Gentry, Peikert, and Vaikuntanathan, 2008

are sender anamorphic encryption schemes.

Sufficient conditions for Sender Anamorphic with no shared key

Any PKE satisfying the 3 following conditions is sender anamorphic.

1. *Common randomness property*.
   For any $c = \texttt{Enc}(\texttt{pk}, m, r)$ and any $\texttt{pk}'$, there is a m' such that $c = \texttt{Enc}(\texttt{pk}', m', r)$
2. *Message recovery from randomness*.
   Given the ciphertext and the used randomness, one can recover the corresponding message.
3. *Equal Distribution of Plaintexts*.
   Given any c in the ciphertext space, for a randomly generated secret key sk: $Pr[\texttt{Dec}(sk, c) = 0] = Pr[\texttt{Dec}(sk, c) = 1]$

Consequently:

- LWE encryption by Regev, 2005
- Dual LWE encryption by Gentry, Peikert, and Vaikuntanathan, 2008

are sender anamorphic encryption schemes.

Conclusions

- We introduced two new concepts:
  - receiver anamorphic encryption
    the receiver of a communication is under the dictator's control
  - sender anamorphic encryption
    the sender of a message is under the dictator's control
- We show implementations with existing cryptosystem from the literature
- Our results gives technical evidence of the futility of the Crypto Wars
  - the dictator doomed to read Crypto papers and outlaw schemes as they are shown to be *anamorphic*
- How this is going to affect policy, law and other societal aspects is beyond the scope of this work
- Anamorphic encryption is not an isolated phenomenon.
  More to come...