Anamorphic Encryption

Private Communication against a Dictator

G. P., Duong Hieu Phan, Moti Yung

June 4, 2022

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

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 wish 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

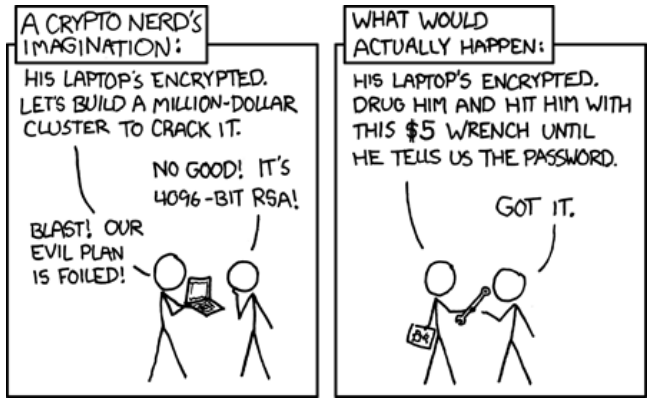
- Assumption of the existence of one-way functions comes from *our current scientific understanding of Nature*
  - if true, it is enforced by Nature
  - it might be false but then it is false for all

- 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

In normal settings

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.

- 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

How can we fix it?

A new research problem

Design new encryption schemes that can be proved secure without relying on the receiver-privacy assumption

Another new research problem

Design new encryption schemes that can be proved secure without relying on the sender-freedom assumption

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 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

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 $\mathcal{F}(K, \mathtt{ct}) = b$

Our approach

- A ciphertext is associated with two secret keys $\mathtt{sk}_0, \mathtt{sk}_1$

$$\mathtt{sk}_0 := \mathtt{sk} \qquad \mathtt{sk}_1 := K$$

- A ciphertext carries two plaintexts m_0, m_1, one for each key

$$m_0 := \text{“Glory to our Leader”} \qquad m_1 := b$$

- ...and there is **no** second key
  - $\mathcal{E}$ is just an off-the-shelf encryption scheme
  - no need for K

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

- Construction can be extended to any length ℓ
- Average encryption time is exponential in ℓ

Receiver Anamorphic

The Naor-Yung transform

The NY transform – 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 transform

The NY transform – 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

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 $\texttt{fpk}$
- Oscar wants also to send message

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

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

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

No prior shared knowledge is needed between Oscar and John

Sender Anamorphic vs Deniable Encryption

- Deniable encryption applies to the *same* public key
- The dictator cannot force the message
- Sender Anamorphic Encryption can be used to provide some form of deniability
-
- denying having sent a message to John
- ciphertext is broadcast over a public channel and not sent on a point to point channgel

Sender Anamorphic Encryption

We prove that

- 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 requiring to register/to escrow decryption keys
- 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