The Self-Anti-Censorship Nature of Encryption

On the Prevalence of Anamorphic Encryption

M.Kutyłowski[1], GP[2], D.H.Phan[3], M.Yung[4], M.Zawada[5]

[1]Wrocław University of Science and Technology, and NASK - National Research Institute

[2]Università di Salerno and Google

[3]Telecom Paris, Institute Polytechnique de Paris

[4]Google and Columbia University

[5]Wrocław University of Science and Technology

PETS 2023 – Lausanne

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 an assumption 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 an assumption 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 an assumption 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

Ok...one more assumption

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 protect my key

Law of Nature vs Normative Prescription

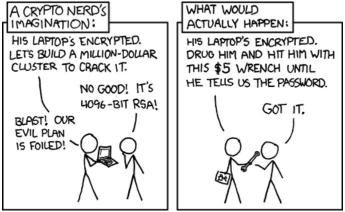
- Assumption of the existence of one-way functions comes from *our current scientific understanding of Nature*
  - if true, it is enforced by Nature
  - it might be false but then it is false for all

- 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

- Realistic for “normal” settings
- No wonder that encryption has been developed under this assumption
  - with no explicit mention

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



thanks to https://xkcd.com/538/

Not only dictators...

The Clipper Chip

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.

Ban of E2E encryption

In our country, do we want to allow a means of communication between people which even in extremis, with a signed warrant from the Home Secretary personally, that we cannot read?

David Cameron
UK Prime Minister
January 2015

How can we fix this?

Not by designing new schemes

- Suppose we design an encryption scheme that is secure without assuming receiver privacy
- 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
- 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
- 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
- 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.

Anamorphic Encryption [PPY – Eurocrypt 2022]

The anamorphic approach [P-Phan-Yung Eurocrypt '22]

- one public key $\mathtt{pk}$, one ciphertext, one secret key $\mathtt{sk}$
  - that's what the dictator thinks
- one public key $\mathtt{pk}$, one ciphertext, two secret keys $\mathtt{sk}, \mathtt{dkey}$,
  - one ciphertext, two plaintexts $\mathtt{msg}, \mathtt{amsg}$

Anamorphic Encryption [PPY – Eurocrypt 2022]

The anamorphic approach [P-Phan-Yung Eurocrypt '22]

- one public key pk, one ciphertext, one secret key sk
  - that's what the dictator thinks
- one public key pk, one ciphertext, two secret keys sk, dkey,
  - one ciphertext, two plaintexts msg, amsg

Anamorphic Encryption [PPY – Eurocrypt 2022]

The anamorphic approach [P-Phan-Yung Eurocrypt '22]

- one public key $\mathtt{pk}$, one ciphertext, one secret key $\mathtt{sk}$
  - that's what the dictator thinks
- one public key $\mathtt{pk}$, one ciphertext, two secret keys $\mathtt{sk}, \mathtt{dkey}$,
  - one ciphertext, two plaintexts $\mathtt{msg}, \mathtt{amsg}$

Anamorphic Encryption [PPY – Eurocrypt 2022]

The anamorphic approach [P-Phan-Yung Eurocrypt '22]

- one public key $\mathtt{pk}$, one ciphertext, one secret key $\mathtt{sk}$
  - that's what the dictator thinks
- one public key $\mathtt{pk}$, one ciphertext, two secret keys $\mathtt{sk}, \mathtt{dkey}$,
  - one ciphertext, two plaintexts $\mathtt{msg}, \mathtt{amsg}$

Anamorphic Encryption [PPY – Eurocrypt 2022]

The anamorphic approach [P-Phan-Yung Eurocrypt '22]

- one public key pk, one ciphertext, one secret key sk
  - that's what the dictator thinks
- one public key pk, one ciphertext, two secret keys sk, dkey,
  - one ciphertext, two plaintexts msg, amsg

Previous work

P-Phan-Yung [Eurocrypt '22]

- every scheme can be made anamorphic with low rate
  - $\mathtt{amsg}$ of length *logarithmic* in λ
- Naor-Yung encryption scheme is anamorphic
  - $\mathtt{amsg}$ of length *polynomial* in λ

Contributions of this paper

Contributions

- present refined notion
  - Single-Receiver anamorphic encryption
  - Multi-Receiver anamorphic encryption
- give evidence of the *prevalence* of anamorphic encryption
  - RSA-OAEP, Goldwasser-Micali, Paillier, ElGamal, Cramer-Shoup, Smooth Projective Hash Function are efficiently anamorphic

This talk

- RSA-OAEP is anamorphic
- Single- vs Multi-Receiver anamorphic
- RSA-OAEP is Multi-Receiver anamorphic

Contributions of this paper

Contributions

- present refined notion
  - Single-Receiver anamorphic encryption
  - Multi-Receiver anamorphic encryption
- give evidence of the *prevalence* of anamorphic encryption
  - RSA-OAEP, Goldwasser-Micali, Paillier, ElGamal, Cramer-Shoup, Smooth Projective Hash Function are efficiently anamorphic

This talk

- RSA-OAEP is anamorphic
- Single- vs Multi-Receiver anamorphic
- RSA-OAEP is Multi-Receiver anamorphic

In concrete terms

An encryption scheme $\mathsf{E} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ is *anamorphic* if it admits an *anamorphic triplet* $(\mathsf{aKG}, \mathsf{aEnc}, \mathsf{aDec})$ that is *indistinguishable* from E to the eyes of the dictator $\mathcal{D}$ (that has the secret key).

RSA-OAEP: an example

To show that RSA-OAEP$=$ (KG, Enc, Dec) is anamorphic, we design an *anamorphic triplet* (aKG, aEnc, aDec)

- aKG outputs one public key `apk`, and two secret keys `ask` and `dkey`
- aEnc takes two messages, regular `msg` and *anamorphic* `amsg`, and outputs one ciphertext `act`
- Dec on input `act` and `ask` outputs `msg`
- aDec on input `act` and `dkey` outputs `amsg`

- share `dkey` with your intended recipients
- you pretend to be using RSA-OAEP and, when asked, you surrend `ask`
- the dictator $\mathcal{D}$ cannot tell if you are using (aKG, aEnc, aDec) or RSA-OAEP $=$ (KG, Enc, Dec)

Anamorphic Triplet

(aKG, aEnc, aDec)

- *anamorphic key generation* aKG
  - input: the security parameter 1^λ
  - output: $(\mathtt{apk}, \mathtt{ask})$ pair of keys and *double* key $\mathtt{dkey}$;
- *anamorphic encryption* aEnc
  - input:
    two keys: public key $\mathtt{apk}$ and *double key* $\mathtt{dkey}$, and
    two messages: *regular message* $\mathtt{msg}$, and *anamorphic message* $\mathtt{amsg}$
  - output: one ciphertext $\mathtt{act}$;
- *anamorphic decryption* algorithm aDec
  - input:
    two keys: $\mathtt{ask}, \mathtt{dkey}$
    one ciphertext: $\mathtt{act}$;
  - output: message $\mathtt{msg}$;

$\mathsf{RealG}_{\mathsf{E},\mathcal{D}}(\lambda)$

1. Set $(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathsf{KG}(1^\lambda)$
2. Return $\mathcal{D}^{\mathsf{Oe}(\mathtt{pk},\cdot,\cdot)}(\mathtt{pk}, \mathtt{sk})$, where $\mathsf{Oe}(\mathtt{pk}, \mathtt{msg}, \mathtt{amsg}) = \mathsf{Enc}(\mathtt{pk}, \mathtt{msg})$.

$\mathsf{AnamorphicG}_{\mathsf{AME},\mathcal{D}}(\lambda)$

1. Set $((\mathtt{apk}, \mathtt{ask}), \mathtt{dkey}) \leftarrow \mathsf{aKG}(1^\lambda)$
2. Return $\mathcal{D}^{\mathsf{Oa}(\mathtt{apk},\mathtt{dkey},\cdot,\cdot)}(\mathtt{apk}, \mathtt{ask})$, where $\mathsf{Oa}(\mathtt{pk}, \mathtt{dkey}, \mathtt{msg}, \mathtt{amsg}) = \mathsf{aEnc}(\mathtt{apk}, \mathtt{dkey}, \mathtt{msg}, \mathtt{amsg})$.

A general strategy for proving anamorphism

- IND-CPA $\mathsf{E} = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ must be randomized
- Some encryption schemes allow to extract the randomness used to produce the ciphertext by running rrDec
  - $\mathsf{rrDec}(\mathsf{Enc}(\mathtt{pk}, \mathtt{msg}; R), \mathtt{sk}) \to (R, \mathtt{msg})$
- Replace the randomness with the ciphertext of an encryption scheme $\mathsf{prE} = (\mathsf{prKG}, \mathsf{prEnc}, \mathsf{prDec})$ with pseudo-random ciphertexts

Pseudo-random ciphertexts from one-way functions
AES ciphertexts are conjectured to be pseudo-random

The anamorphic triplet

Anamorphic key generation $\mathsf{aKG}(1^\lambda)$

- compute $(\mathtt{apk}, \mathtt{ask}) \leftarrow \mathsf{KG}(1^\lambda)$;
- compute $\mathtt{prK} \leftarrow \mathsf{prKG}(1^\lambda)$;
- set $\mathtt{dkey} = (\mathtt{prK}, \mathtt{ask})$;

Anamorphic encryption $\mathsf{aEnc}(\mathtt{apk}, \mathtt{dkey}, \mathtt{msg}, \mathtt{amsg})$

- compute $R \leftarrow \mathsf{prEnc}(\mathtt{dkey}, \mathtt{amsg})$
- compute $\mathtt{act} \leftarrow \mathsf{Enc}(\mathtt{apk}, \mathtt{msg}; R)$

Anamorphic decryption $\mathsf{aDec}(\mathtt{ask}, \mathtt{dkey}, \mathtt{act})$

- compute $(R, \mathtt{msg}) \leftarrow \mathsf{Dec}(\mathtt{ask}, \mathtt{act})$
- compute $\mathtt{amsg} \leftarrow \mathsf{prDec}(R, \mathtt{dkey})$

RSA-OAEP is Anamorphic

RSA-OAEP encryption

To encrypt $\texttt{msg}$ of length $n/2$ with hash functions G and H

- randomly select $R \leftarrow \{0,1\}^n$
- set $M = \texttt{msg}||0^{n/2}$
- set $\hat{M} = G(R) \oplus M$
- set $P = \hat{M}||(R \oplus (H(\hat{M})))$
- encrypt P using RSA

To recover R from P, just XOR the hash of the left half and the right half of P.

Multi- vs Single-Receiver

- `dkey` for RSA-OAEP contains `ask`
- necessary to extract randomness
- one obtains both `msg` and `amsg`
- `msg` (and `amsg`) is *multi-receiver*: every user with `dkey` can read it.

Single-Receiver Anamorphic

IND-CPA holds also for users that have dkey

Game for Single-Receiver Anamorphism

$\mathsf{SingleAnG}^{\beta}_{\mathsf{AME},\mathcal{A}}(\lambda)$

- Set $((\mathtt{apk}, \mathtt{ask}), \mathtt{dkey}) \leftarrow \mathsf{aKG}(1^{\lambda})$
- $(\mathtt{msg}_0, \mathtt{msg}_1, \mathtt{amsg}, \mathtt{st}) \leftarrow \mathcal{A}(\mathtt{apk}, \mathtt{dkey});$
- $\mathtt{act} \leftarrow \mathsf{Oe}^{\beta}(\mathtt{apk}, \mathtt{dkey}, \mathtt{msg}_0, \mathtt{msg}_1, \mathtt{amsg});$
- return $\mathcal{A}(\mathtt{act}, \mathtt{st})$, where
  $\mathsf{Oe}^{\beta}(\mathtt{apk}, \mathtt{dkey}, \mathtt{msg}_0, \mathtt{msg}_1, \mathtt{amsg}) = \mathsf{aEnc}(\mathtt{apk}, \mathtt{dkey}, \mathtt{msg}_{\beta}, \mathtt{amsg})$.

Theorem

Cramer-Shoup is single-receiver anamorphic

Conclusion

anamorphic encryption is fairly practical and implementable with many standard schemes for anamorphic messages of a few hundred of bits

Related ePrint reports

- Extended version of this paper:
  Mirek Kutylowski, Giuseppe Persiano, Duong Hieu Phan, Moti Yung, Marcin Zawada: *The Self-Anti-Censorship Nature of Encryption: On the Prevalence of Anamorphic Cryptography.* IACR Cryptol. ePrint Arch. 2023: 434 (2023)
- Original paper from Eurocrypt 2022:
  Giuseppe Persiano, Duong Hieu Phan, Moti Yung: *Anamorphic Encryption: Private Communication against a Dictator.* IACR Cryptol. ePrint Arch. 2022: 639 (2022)
- Upcoming paper on anamorphic signatures from CRYPTO 2023:
  Mirek Kutylowski, Giuseppe Persiano, Duong Hieu Phan, Moti Yung, Marcin Zawada: *Anamorphic Signatures: Secrecy From a Dictator Who Only Permits Authentication!* IACR Cryptol. ePrint Arch. 2023: 356 (2023)