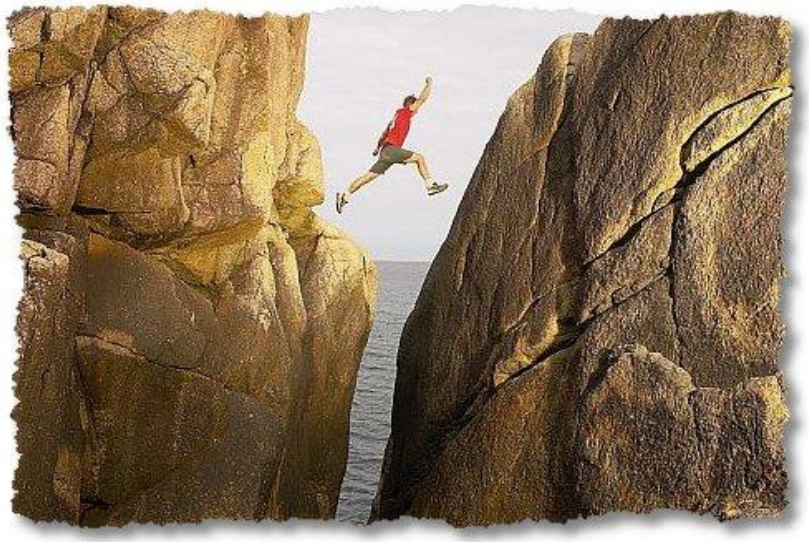
Anamorphic Signatures: Secrecy from a Dictator Who Only Permits Authentication



Miroslaw Kutylowsky
Giuseppe Persiano
Duong Hieu Phan
Moti Yung
Marcin Zawada

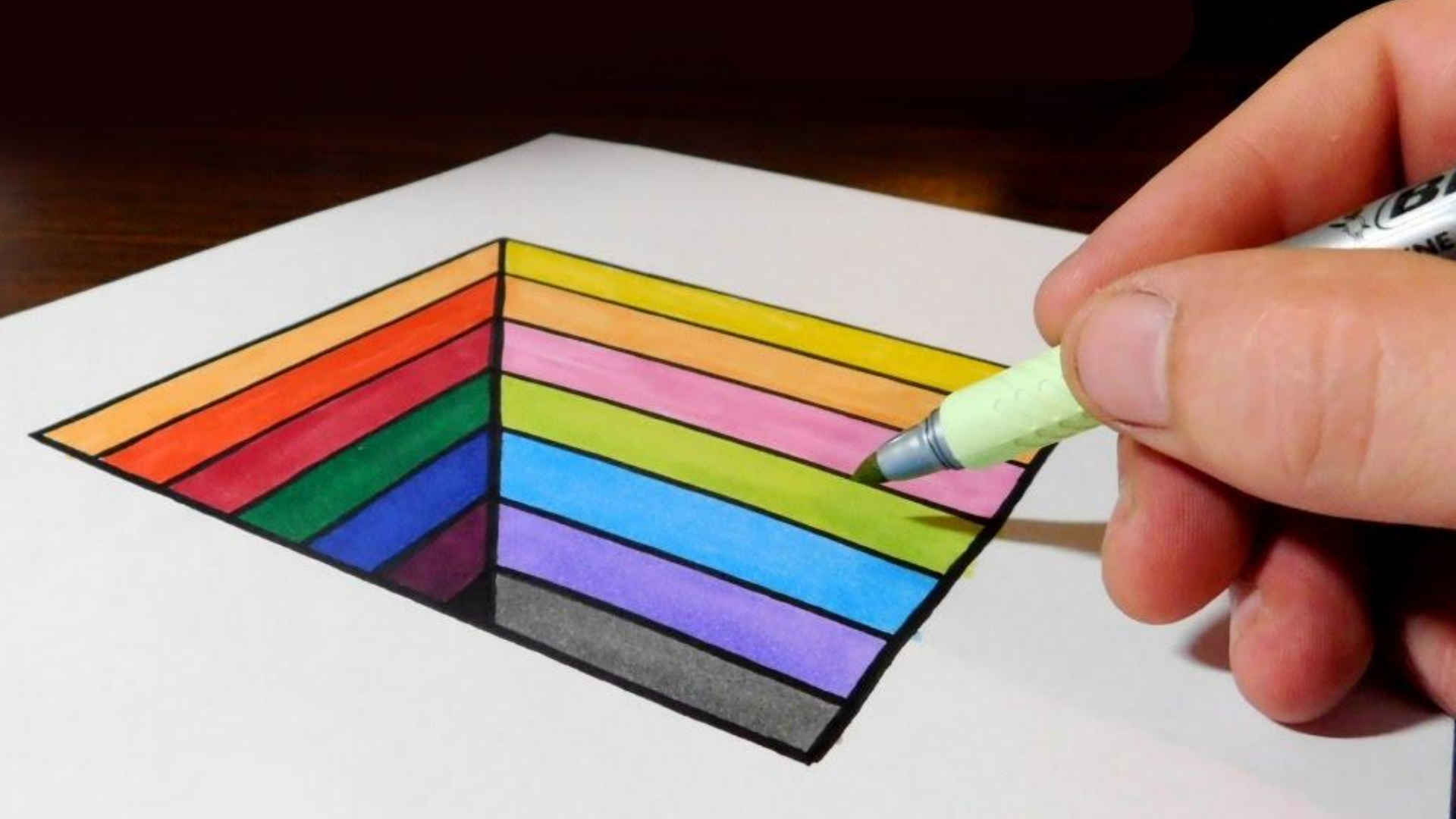
Agenda

- Cryptography as a science (some reflections)
- Malicious Cryptography: the notion of “repurposing schemes”
- Anamorphic Cryptography Encryption (survey)
- Anamorphic Signatures (setting and results)
- Conclusion and a final note

Usual Q: What is Anamorphic?????

It’s a term in Arts (paintings, etc.)

If you move to a different angle around the painting or view it with a different perspective, you see a different second image…



Cryptography as a Science: external relations

- Scientific Inputs: basic Math & Science- Modern Cryptography is based on and related to Mathematics (obviously: Algebra, Probability, combinatorics, Info th.,), TCS (complexity, logic, learning), Physics,..
- Scientific I/O: Applications/ results in other areas- Secure systems and Privacy, Distributed Systems, Coding, ….
- Scientific output: Technological Sciences & Engineering- EE, Hardware & Software Engineering.

Cryptography as a Field: internal relationships

- Designs, Proofs, Models (they have to agree)
- Math validation: Cryptanalysis underlying assumptions
- Reduction proofs [or validation: best attacks- sym. crypto]
- Foundations: define primitives [encryption, signature, auth, secure computing, etc.], reductions among primitives (implications, possibilities and impossibilities)
- Applied: improve performance and simplify assumption of a primitive.

Essentially: everything is a goal-oriented logical sequence of discoveries (theoretical or practical), primitive given

Further Internal relationships

- Primitives w/ correctness goals and security requirements!
- Cryptography a defense against bad behavior; a protection!
- But…: any security technology when added to a system increases the system's attack vector!

THEN:

- Can we possibly change (reformulate, repurpose) the primitive's goal (without changing the primitive)?
- Can cryptography be used for attack?!?? For other purpose then its main actual goal??

This gives rise to what I call "MALICIOUS CRYPTOGRAPHY"

I. The Joy of Malicious Cryptography; preliminary

"It was not designed for that, so let's reverse its logic and do it!"

- The first hint was government wish to add itself as an additional recipient of all messages (aka as the crypto wars: escrow encryption- the clipper chip).In [Yair Frankel, Moti Yung: **Escrow Encryption Systems Visited: Attacks, Analysis and Designs.** CRYPTO 1995] we broke the Clipper Chip -- authenticated source not bound to key used!
- The second hint was Cryptovirology:[Adam L. Young, Moti Yung: **Cryptovirology: Extortion-Based Security Threats and Countermeasures.** IEEE S&P 1996] gave all ingredients for a ransomware attack, and proposed countermeasures (which were ignored until ~15 years after!!!).

II. The Joy of Malicious Cryptography: KLEPTOGRAPHY

So how will the gov try to control Cryptographic devices/ algorithms?

- Kleptography (aka Algorithm substitution attacks, aka as subversion attack) show that changing & hiding the algorithm (or the parameters generating it), the attacker can gain exclusive access to secret messages.
- Essentially, allow the attacker to modify the algorithm (e.g. add an asymmetric algorithm it knows the trapdoor to), to the blackbox/ obfuscated algorithm!! This reverses the logic.
- It shows what authorities/ manufacturers/ etc. can do to win the crypto wars!

[Adam Young, M. Yung: Crypto96, Eurocrypt97,Crypto97, FSE98, CT-RSA,..] and by others… ……. Ignored, until:

III. Post-Snowden Cryptography; Cliptography

Snowden 2012: The methods have been employed?

- The Dual-EC DRBG (built on the logic of the repeated DH kleprtogram of [YY Crypto 97] paper) was employed.
- Numerous works to clip the power of klepto attacks by architectural and algorithmic additions [from BPR: Crypto14, and on.. Numerous works….]
- I call this effort Cliptography: clipping the power of kleptographic attacks.

So, Malicious Cryptography, thus far, shows how the authorities can abuse /(apparently abused) cryptographic systems and how to resists such attacks.

Next:

ANAMORPHISM

IV. Anamorphic Encryption -background

Now, let us reverse the logic again: Assume authorities (dictator) are bad and get to have the keys …

Can we apply “repurposing” to evade massive attacks on privacy?!

- It took a few years to reverse the logic, but realizing the crypto wars continue, it seemed necessary to react.
- We knew already that there are good policy/systems reasons to avoid key escrow (since the system allows another door to attacks, etc.). But the aim is a technical “once and for all” intra cryptographic arguments reg. the futility of the war:

a. Assume a dictator gets the receiver’s key (and dictates the messages to send)
b. Can we nevertheless use the very deployed system to evade the dictator.

A note: Assumptions in Cryptography

- There are complexity assumptions about primitives, and key sizes: These are sumptions about nature/ mathematics!
- The other typically implicit assumptions are that

a. The receiver's key is secure
b. The choice of message by the sender is free.

- These are normative assumptions.
- So, assume they do not hold in society; as said: the dictator determines the message and gets the key and controls the courts. (We aim at democratic countries where there are pushes to behave dictatorially toward Cryptography!)
- Can we do anything?
- Anamorphic Cryptography is about investigating existing cryptosystems designed for a purpose, and repurposing them!

Anamorphic Encryption.

- We allow the sender and receiver to exchange another key on the side (or via steganography, time permitting)..
- Then (receiver) Anamorphic systems exist: They comply with the dictator requests, but within the ciphertext there is a hidden ciphertext that allows sending the extra (anamorphic) cleartext message.

- The subject started in [Eurocrypt'22: Persiano, Phan, Yung: **Anamorphic Encryption: Private Communication Against a Dictator**] with examples, models, definitions…
- An extended treatment of Anamorphic Encryption: [PETS'23: The authors of the current work: **The Self-Anti-Censorship Nature of Encryption: On the Prevalence of Anamorphic Cryptography.**]

Schemes that are Anamorphic & properties

- Under various sharing conditions (the extra key only, the extra key+trapdoor, and under different corruption modes);
  i. CCS-systems: The NY-based schemes. Cramer-Shoup
  ii. Goldwasser-Micali, Pailler, RSA-OAEP,...
  iii. El-Gamal based schemes

- (Notion compared to related notions: subliminal comm./ deniable enc./ etc.)

Anamorphic Encryption properties

- None of the schemes was design with anamorphism in mind, nevertheless using various techniques they can turn into anamorphic schemes. If they are deployed as basic secure communication schemes
- The dictator with the trapdoor cannot tell anamorphic version from non anamorphic version of the scheme so it has no way to know if the extra message is sent and
- parties can pretend there was no extra message (so dictator in control, but secure message flow anyway!!!)
- → Futile to control → Doubts about the crypto wars (if it does not stop the bad guys why make life difficult for all?!)

So today: Direct Sender-Receiver Encryption is disallowed!

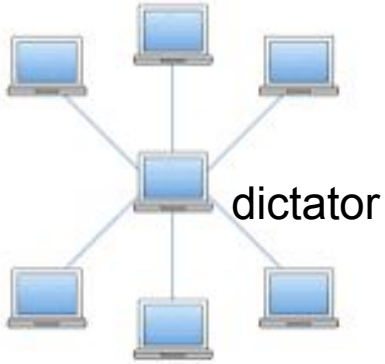
- There is no direct connection between parties, all secure communication goes via the dictator

a. sender → dictator: E(dict-key, message),
b. then dictator → receiver: E(receiver-key, message)

No anamorphic encryption channel is used by the dictator

BUT: Dictator can send any(!!) message on behalf of anyone!!!??

- To prevent this we need to Authenticate (i.e., Sign) the origin, otherwise useless setting!



Star Configuration:
dictator in the middle

So (1) Sender →Dictator: C0=E(K-dictator, message)
(2) Dictator→ Sender: C1=E(K-receiver, message) + ZKP (c1 ok)
(3) Sender → Dictator: C1, S=SIGN(sender, C1)
(4) Dictator→ Receiver: C1, S

(5) When the signature certificate expires: Signing key is given to the dictator to inspect past communication (unlike in the chaffing-and-winnowing model).

Anamorphic Channels?

- The only possibility is via the Signature Mechanism
- This gives rise to the question:

  Are there anamorphic signature schemes which can carry a hidden messages, in spite of the dictator eventually having access to the signing key?

Results

Two modes of anamorphism:

-One to Many: only sender keeps the signing trapdoor.

-Many to Many: Trapdoor shared (with a trusted group) as part of anamorphic key (sharing and publishing trapdoors was consider an issue from the dawn of signature schemes)

Anamorphic message revealed via verification.

We

- Add: the extra anamorphic key
- Give: definitions, models, constructions, proofs…
- Achieve: high bandwidth (poly. In the signature size) constructions
- Discuss: Relation of anamorphic signature to watermarking given

Examples: schemes w/ anamorphic channels

- If the verification process exposes a random value, a pseudorandom encryption can be embedded in this value (anamorphic). e.g. Boneh-Boyen
- If the verification process+ the knowledge of the trapdoor exposes a random value (symmetric anamorphic). e.g. El-Gamal/ Schnorr

Two traditional signature construction families Give anamorphism

- From: 3-message Public-coin protocol transform to Fiat Shamir like sig: results in a symmetric anamorphic scheme.

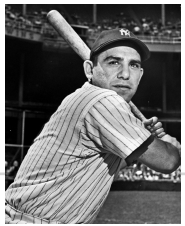
- From one time (Lamport Diffie style) signature to regular signature (the Naor-Yung 1989 signature via UOWHF) is anamorphic (Namely, the anamorphic message remains private even if the signing key is given to the dictator; the dynamic introduction of more “one-time signatures” allow choosing the messages online hidden in the preimages). See Sphincs

Conclusions

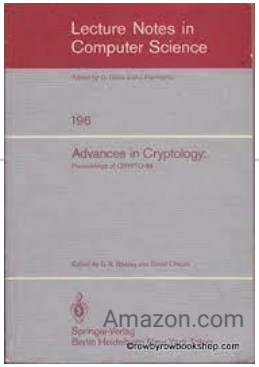
- Dictator allowing only signing as part of the crypto war, cannot stop secure communication using the system!
  -Anamorphism appears systematically in old schemes
- → Crypto restrictions easy to overcome, [while hard on honest applications/ users]
- New notions: so more applications and findings are coming/ expected…. (revisit the golden era)

It ain’t over till it’s over …

Next…. A final note…..



A final note:



- My first Crypto was at 1984
- I presented my M.Sc. Thesis work based abstract:

[Cryptoprotocols: Subscription to a Public Key, the Secret Blocking, and the Multi-Player Mental Poker Game]

- From then I have come/ attended every year, making this conference **my 40-th Crypto!**

Thank You!