Anamorphic cryptography

How can we ensure private communication?

Cryptosystems have been developed to send secure messages with the assumption that the receiver's key – what the intended recipient needs to read the message – is secure from adversaries. However, there have been tensions, dubbed as 'Crypto Wars'. Friction has arisen between governments, hoping to access encryption keys to learn about potential threats, and industry, which believes that the benefits of encryption outweigh the risks. An international team led by Professor Moti Yung at the Privacy, Security, and Safety Research Group at Google LLC and at Columbia University, USA, has conceptualised 'anamorphic' cryptography so that even if the keys are known to the adversary, pre-existing cryptographic systems can nevertheless directly transfer secure messages.

In our society, we increasingly rely on electronic forms of communication and have heard about the methods put in place to protect our privacy, such as end-to-end encryption in messaging apps. Typically, if you want to send your friend a message, each of you has a public key and the corresponding private key. Anyone can have access to your public key, but your private key is unique to you. So, you can choose to write a message and encrypt it using your friend's public key. Then, only your friend can decrypt it using their private key, meaning that they are the only one with the means to read your message. But what happens if an external party has access to your friend's private key, or what if you are not free to choose what message to send? The privacy between you and your friend is then no longer upheld.

The privacy guaranteed by encryption relies on two assumptions: the assumption that you are free to choose and encrypt your message is called the 'sender-freedom assumption', and the assumption that your friend is the only person with the means to access the message is called the 'receiver-privacy assumption'. These assumptions are the default case. However, they are sometimes impinged upon by governments, to various extents. External parties, dubbed 'dictators', may have legal means to gain access to private keys, or may be able to force people to send incorrect messages of their choice. The most extreme cases are often found in dictatorships, but increasingly, governments are asking for some knowledge of keys to identify national threats. This can create and indeed, has already created tension between industry or privacy advocates and governments, known as Crypto Wars.

Professor Moti Yung and his international colleagues argue, however, that the dictator may not always have this control. Within cryptosystems, they show that messages can be sent that satisfy the requests of the dictator, such as getting the receiver key, while still managing to send a private message to the intended recipient, through a method of anamorphic cryptography.

HOW HAS CRYPTOGRAPHY DEVELOPED?

The same questions have arisen throughout the development of cryptography: how can we ensure privacy, but at the same time have the means to enforce laws and prevent malicious behaviour, and how do we develop cryptography law? One solution was the Clipper chip proposal in the early 1990s, where the US government proposed that a strong cryptographic system needed to keep a copy of the keys required to decrypt the messages and make it available to a trusted third party encrypting it on every ciphertext message. Passing the ciphertext to its receiver was predicated upon this very action being authenticated. If there was a legal requirement to access the messages, the key would legally have to be recovered (from any ciphertext message) and handed over by the third party in a key disclosure law. This configuration is known as a key escrow system.

However, this proposal was flawed in a number of ways – the additional keys could be used to violate privacy or used by law enforcement for surveillance, which introduced a lot of trust elements to the cryptosystem. In particular, Yung found at the time that the authentication above did not bind the ciphertext to point at the right key to be opened. Since then, cryptographers have been working to construct a means by which a fair system can be enacted. One example is a system with three parties – a user, who sends encrypted messages, a law enforcement body which may request access to messages, and an independent adjudicator who arbitrates if a request from the law enforcement body is fair.

We increasingly rely on electronic forms of communication.

But what happens if the dictator – rather than a law-abiding government – acts in this system? They can act both as law enforcement and as adjudicators, giving themselves the power to overcome the system in place and gain access to encrypted messages. Likewise, with a key escrow system, they can force third parties to reveal the private keys. So, how can we send encrypted messages without a dictator accessing them in our pre-existing cryptographic systems?

HOW CAN WE SIDESTEP A DICTATOR'S REQUEST?

As we have seen in the previous example, if the dictator has the private key required to read the message, we cannot get around their requests. This has led Yung and his team to think more about the keys in use. They propose a second key that the dictator has no knowledge of. So, their system has two modes – a regular case, and the researchers' new anamorphic case. In the regular case, Alice encrypts her message to Bob using his public key. Bob can then decrypt it using his private key – just like the example between you and your friend we considered earlier. However, if the dictator can get hold of the encrypted message, they can force Bob to give them the secret key, thus gaining access to the message.

However, in the anamorphic case, Alice uses an anamorphic public key to encrypt her message. The anamorphic key is associated with two private keys – a regular private key, like that in the regular case discussed above, and an additional secret anamorphic private key. When Alice uses Bob's anamorphic public key to encrypt her message, she generates a ciphertext that has two messages – let's call them message 1 and message 2. If the regular private key is applied to the ciphertext, we reveal message 1, and if the secret private key

How can we send encrypted messages without a dictator accessing them in our pre-existing cryptographic systems?

Encryption plays a vital role in protecting our privacy. But what if an external party is able to decode our messages?

Anamorphic encryption works via a second channel with an additional secret private key.

> ***The anamorphic public key is associated with two private keys – a normal private key, and an additional secret private key.***

is applied, we reveal message 2. So, if Bob is forced to hand over the private key to the dictator, they can hand over the regular private key and reveal message 1. Only the intended recipient – in this case, Bob – has access to the secret private key, and to message 2. This relies on the ciphertext in the anamorphic case being effectively identical to that produced in the regular case, and that a pair of anamorphic public and private keys are indistinguishable from a regular pair. This means the dictator does not know that there is a second message and the secret private key, and the private message (message 2) can be securely sent between Alice and Bob.

CAN WE CONSTRUCT ANAMORPHIC ENCRYPTION IN OUR CURRENT CRYPTOSYSTEMS?

Yung and his team highlight the need for anamorphic encryption to work within existing systems as we need the ciphertexts for both a regular and anamorphic case to look the same, so that they don't arouse suspicion in the dictator. We can't start adding additional strings to ciphertexts as this is unappealing and creates additional work for the user in the normal case, who doesn't have any interest in keeping the second message secret. Instead, they highlight the importance of incorporating this within systems that already have a second channel. Then the second channel will not create suspicion, but can be used as a covert channel for the anamorphic encryption, without any detriment to normal users of the system.

Even if the keys are known to the adversary, pre-existing cryptographic systems can still transfer secure messages.

The researchers highlight how anamorphic encryption can apply to a variety of systems – for example, what if we remove the sender-freedom assumption? Say that Alice is in a position where she may be forced to send a fake message. She could privately set up a shared anamorphic key system with Bob – so if she sent him a fake message, he could reproduce the ciphertext that carries the fake message and a set of coin tosses which are used to create the ciphertext. If Bob decrypts the coin tosses with the shared key, he can receive the private message that Alice wished to send him. While this does require the setting up of the shared key in advance, it highlights how the anamorphic protocol can be adapted to account for limitations on the sender and the recipient, all while overcoming the impositions of the dictator.

Overall, Yung and his team highlight how dictators could previously enforce/use a number of key escrow systems. They conceptualise anamorphic encryption systems, using both the regular channel for users who are not concerned about their messages being accessed, and an anamorphic channel with an additional secret private key. This allows for both a regular and a secret anamorphic message to be sent, and for a regular key to be turned over to the dictator if necessary (eg, via an escrow process), without revealing the second secret message. This holds the potential to overcome the Crypto Wars dilemma and demonstrate its futility: the dictators/governments having the keys to strongly encrypted information, only allowing dictators to access message 1, but still offering privacy in our communications for the future on the anamorphic channel message (message 2).

Behind the Research

Professor Moti Yung

E: motiyung@gmail.com **T:** +1 917 842 4912 **W:** research.google/people/106617
W: www.cs.columbia.edu/~moti

Research Objectives

Professor Moti Yung conceptualised anamorphic cryptography, a form of encryption that is secure even when keys are known to the adversary.

Detail

Bio

Moti Yung is a Security and Privacy Principal Research Scientist with Google, and an adjunct senior research faculty at Columbia. Yung is a fellow of the IEEE, the ACM, the IACR, and the EATCS. His awards include the IEEE-CS McDowell Award (2018) and the Computer Pioneer Award (2021). He is a member of the American Academy of Arts and Sciences.

Funding

- The Privacy, Security, and Safety Research, Google LLC

Collaborators

- Giuseppe Persiano (University of Salerno, Italy)
- Duong Hieu Phan (Telecom Paris, France)

Competing interest statement

While Moti Yung has been conducting research on malicious/subversive use of cryptography and research related to the crypto wars from the mid-1990s, the goal of this line of research is to enhance the community's knowledge, awareness, and understanding of cryptographic techniques and the variety of its uses and abuses. This line is independent of his work for Google and has developed among other findings: a break of the US government's Clipper Chip; cryptovirology, which predicted ransomware; kleptography, which designed and predicted attacks on cryptosystems by designers and via algorithm substitution (which was put to use according to Snowden's revelations); and the recent Anamorphic Encryption. It is important to note that in Google, in fact, his main work is centred on using foundations and novel research findings to keep security and privacy systems in Google on behalf of its clients and users.

References

- Kutylowski, M, et al, (2023) Anamorphic signatures: secrecy from a dictator who only permits authentication! *Cryptology ePrint Archive*, Paper 2023/356. ia.cr/2023/356 (a version to appear in the proceedings of Crypto 2023)
- Kutylowski, M, et al, (2023) The self-anti-censorship nature of encryption: on the prevalence of anamorphic cryptography. *Cryptology ePrint Archive*, Paper 2023/434. ia.cr/2023/434 (a version to appear in Privacy Enhancing Technologies Symposium, 2023)
- Persiano, G, Phan, DH, Yung, M, (2022) Anamorphic encryption: private communication against a dictator. In: Dunkelman, O, Dziembowski, S, (eds) *Advances in Cryptology – EUROCRYPT 2022*. Lecture Notes in Computer Science, 13276. Springer, Cham. doi.org/10.1007/978-3-031-07085-3_2

Personal Response

How do you think the study of cryptography is going to affect the communications of the future?

" Cryptography has contributed in an amazing fashion thus far. First, with cryptography, securing Internet connections, e-commerce, mobile communication, financial technologies, and storage, was made possible. Secondly, the field's scientific and technical development is vast, and many careers in research and development have opened for cryptographers. However, technology keeps evolving and advancing (examples are AI, Machine Learning, Distributed Systems, Internet of Things), and society has to adapt to it. This mandates further innovation in cryptography to answer the new emerging challenges as part of an expanded role for cybersecurity and data privacy, which is suitable for the new era of technology. "

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Google