Reverse Kuleshov effect in cryptography

(silent slides)

The Kuleshov effect is a film editing (montage) effect.

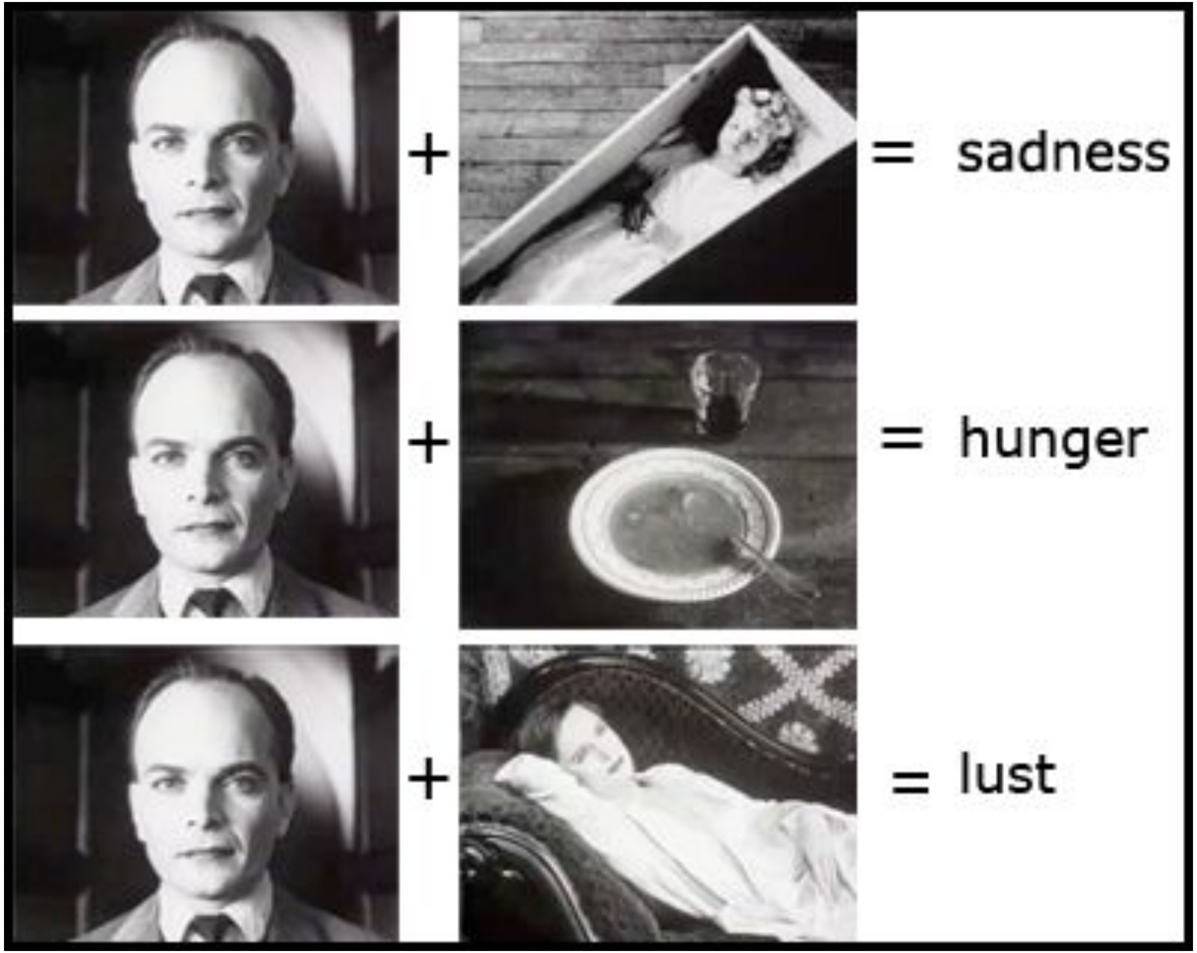
The Kuleshov effect is a film editing (montage) effect.

It says viewers derive more meaning from the interaction of two sequential shots than from a single shot in isolation.

--- Wikipedia

Examples

pay attention to the facial expression of the man



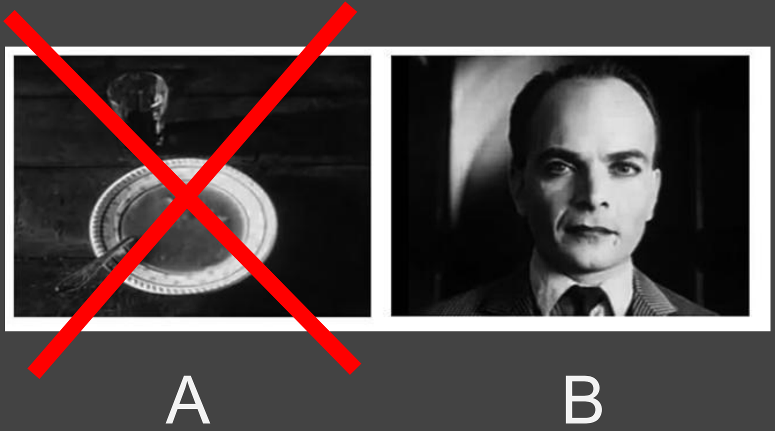
Cheating sheet

Kuleshov effect: viewers derive more meaning from the interaction of two sequential shots than from a single shot.

(recap)

Kuleshov effect: viewers derive more meaning from the interaction of two sequential shots than from a single shot.

Reverse Kuleshov effect: for potentially correlated objects A and B, if A disappears, then B looks like nothing.



Reverse Kuleshov effect in cryptography:
Here’s an example

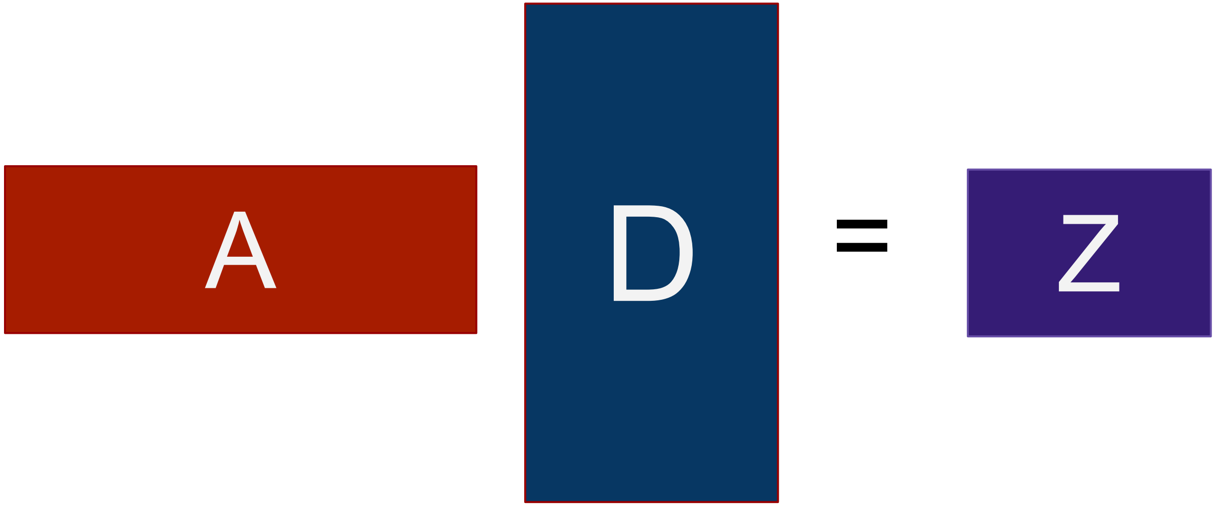
Recall preimage sampling in lattice cryptography

A

Z

Given a matrix A, and the trapdoor of A, and an arbitrary vector Z,

Recall preimage sampling in lattice cryptography

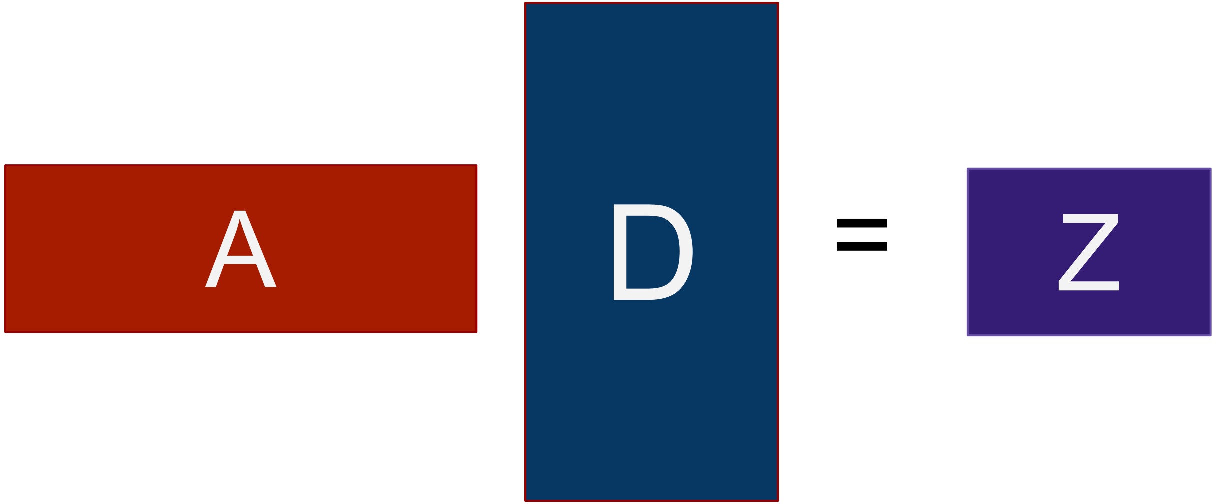


Given a matrix A, and the trapdoor of A, and an arbitrary vector Z, can sample a discrete Gaussian preimage D s.t. AD = Z mod q

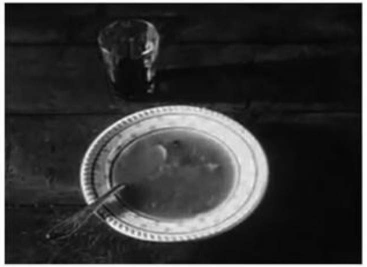
D

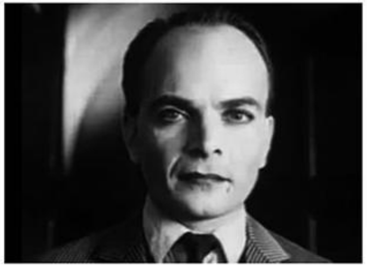
Question: how does D look like without A?

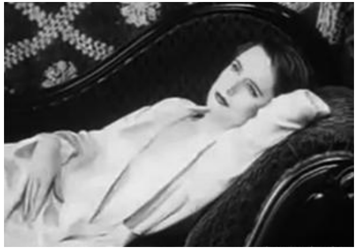
Kuleshov effect: Think of D as the man.



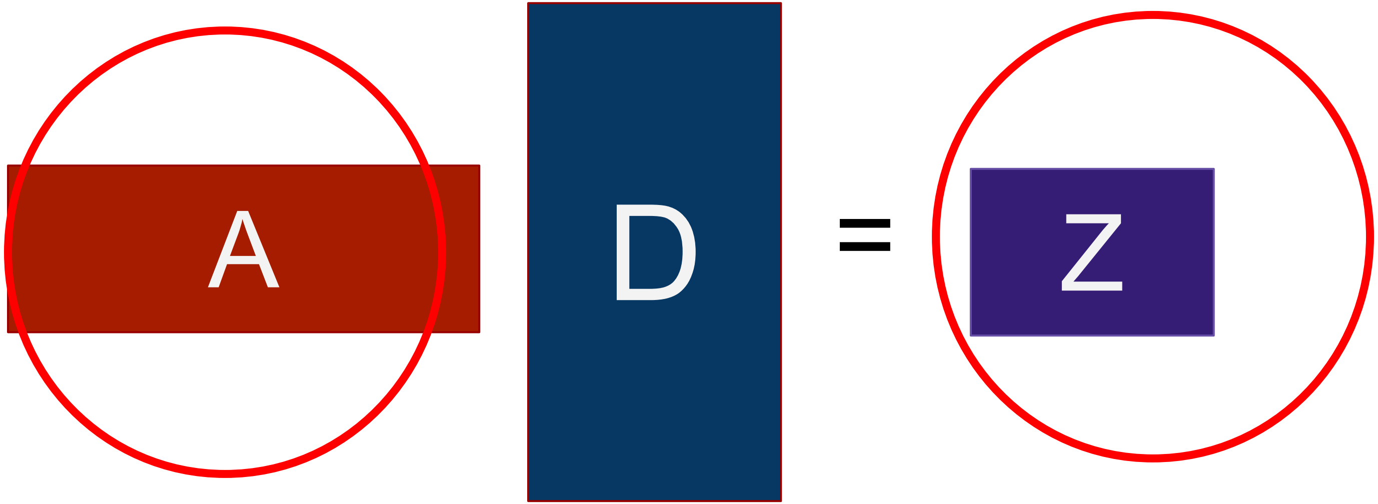
A D = Z



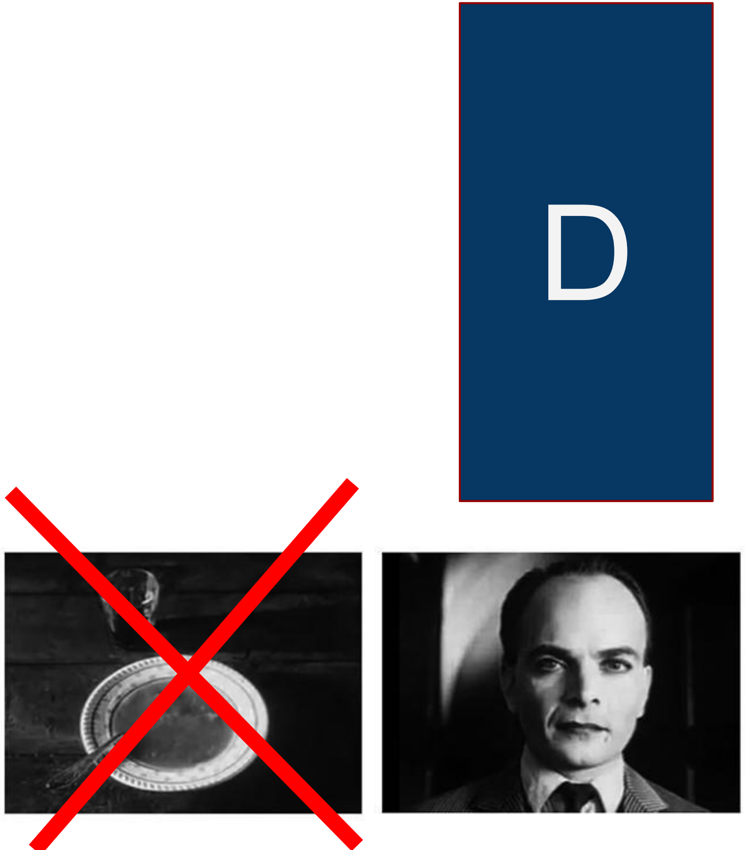




Kuleshov effect: Think of D as the man.
D has is clearly the preimage of Z under function A given A.



Reverse Kuleshov effect:



D

Question: how does D look like without A?

Reverse Kuleshov effect in lattice cryptography

D

????

Reverse Kuleshov effect in lattice cryptography

D

Theorem: if A is hidden, D is indistinguishable from random Gaussian assuming LWE.

Reverse Kuleshov effect in lattice cryptography

D

Theorem: if A is hidden, D is indistinguishable from random Gaussian assuming LWE.
(not true when A is not hidden, due to Kuleshov effect)

(caveat: thm holds when sampling a preimage of “Z+small noise” instead of Z)

Reverse Kuleshov effect in cryptography

Wish you find examples in your area :)

Directors:

Yilei Chen, Vinod Vaikuntanathan, Hoeteck Wee

More (irrelevant stuffs) in:

GGH15 Beyond Permutation Branching Programs:
Proofs, Attacks, and Candidates

https://eprint.iacr.org/2018/360