Cliptography:

Clipping the Power of Kleptographic Attacks

Moti Yung
Google & Columbia Univ

joint with

Alexander Russell, Univ Connecticut
Qiang Tang, Univ Connecticut
Hong-Sheng Zhou, Virginia Commonwealth Univ

Kleptography

The science of stealing information securely and subliminally from black-box cryptographic implementations

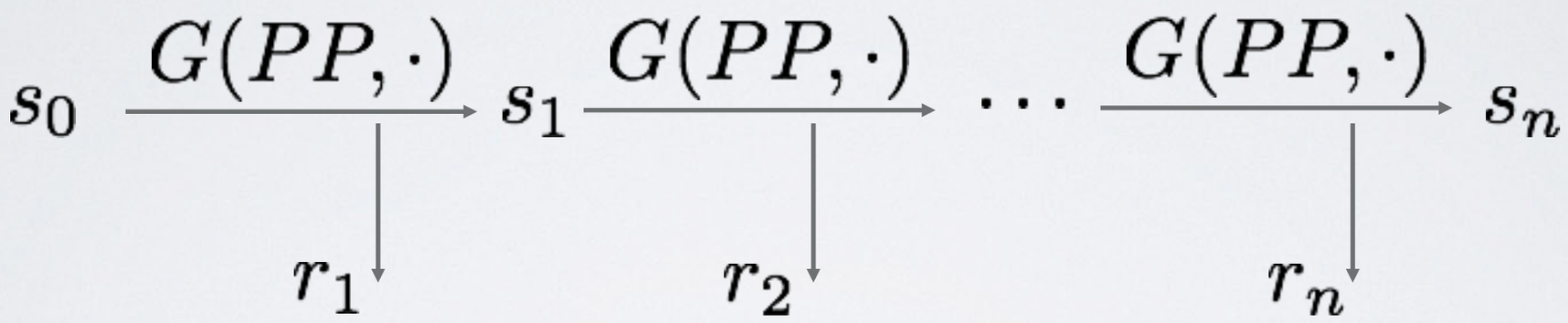
Young & Yung 1996, 97, …

Two Decades Later

- We might be too naïve

Backdoored Dual EC

$$PP = (P, Q) \text{ for a random } Q, P = Q^z$$



$$s_i = P^{s_{i-1}}, r_i = Q^{s_i}$$

$$s_2 = P^{s_1} = Q^{z s_1} = r_1^z$$

Having z, r_2 can be computed from r_1

(P, Q) look as randomly generated

Renewed Attention Received

- Bellare et al study symmetric key encryption & other algorithms with a unique output, assuming key generation is honest

- Dodis et al study backdoor-free PRG, by applying a keyed hash function to the output, but assuming the key is unknown to the adversary in the public parameter generation phase.

- other works … under various assumptions/settings

Question

Can **all** algorithms (given by the adversary) in a cryptosystem be subject to kleptographic attacks, including key generation?

We employ honest lab to test these cryptosystem components

Technical Observations

Detection by honest lab enforces deterministic algorithms with public input distribution to be (almost) consistent with the specification

Random oracle with a given input distribution still behaves as a RO

We study
(trapdoor) one-way functions
in the complete subversion model

OWF family

Specification

Gen

i

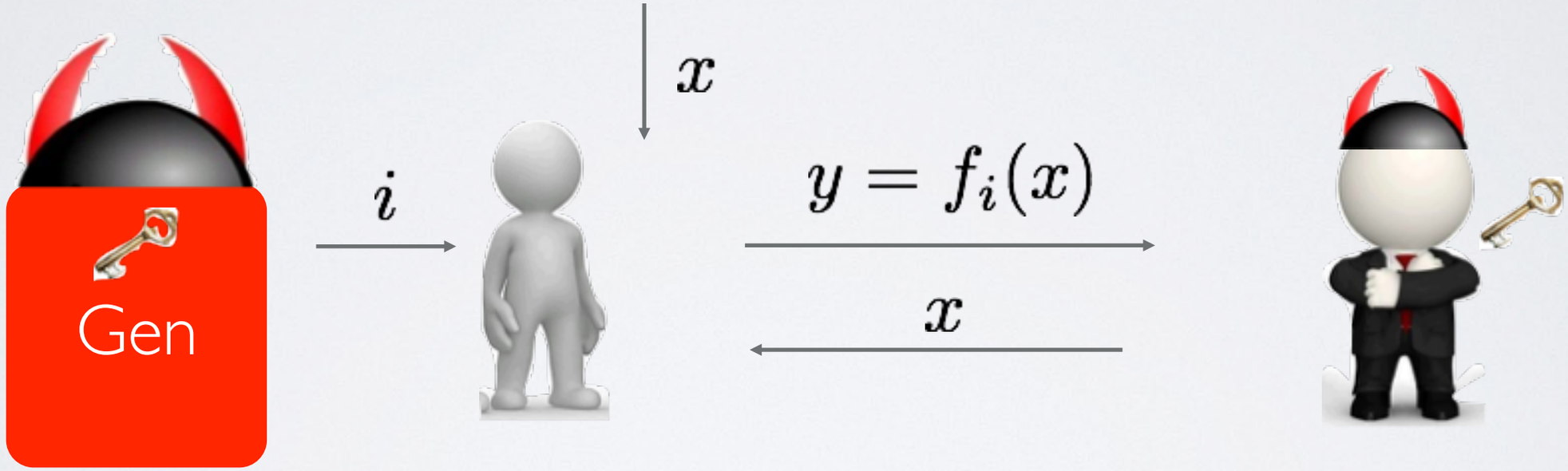
x

$y = f_i(x)$

?

OWF under subversion

Condition 1:
Inversion is easy for the adversary using his Gen algorithm



OWF under subversion

Condition II:
Family distributions are computationally indistinguishable

Two index distributions are indistinguishable

Cliptographic Defense strategy:
Randomize the Index

$$g_i(x) := f_{h(i)}(x)$$

Theorem: $\{g_i\}$ is a family of strongly unforgeable OWFs

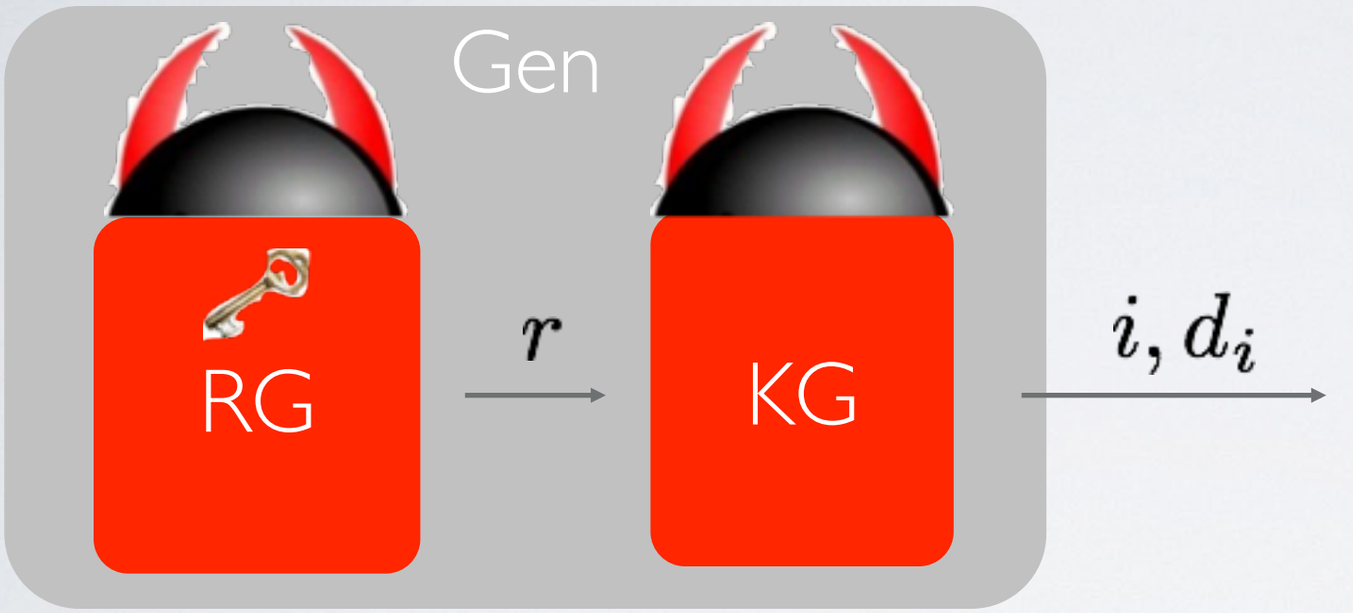
Assuming h is RO, and index domain is “simple”

Intuition

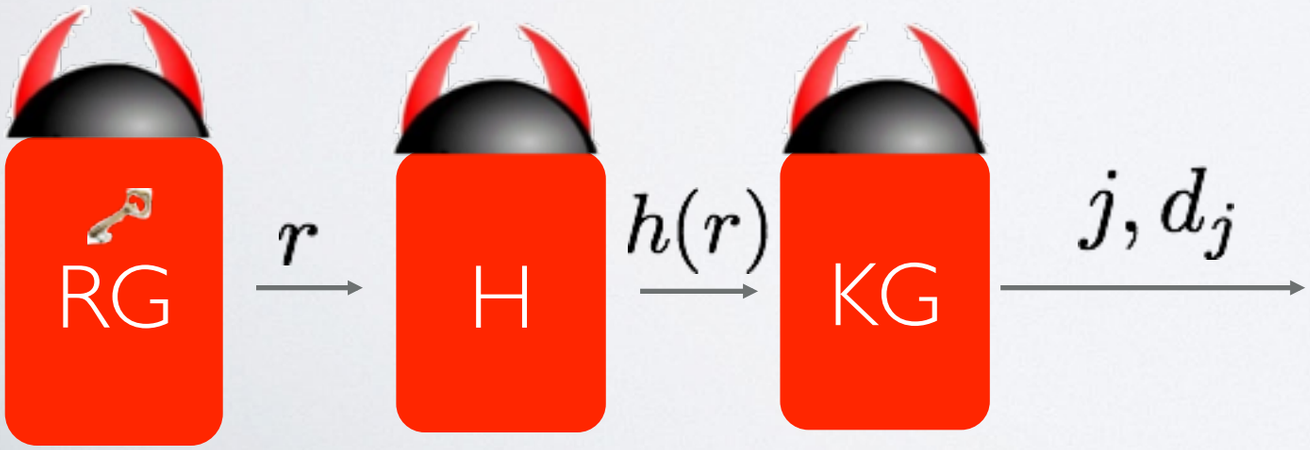
Randomizing the index can map to a function index that the backdoor is useless; if useful, the adversary reverses RO

Any backdoor can only be used to invert a sparse subset of functions, otherwise such Adv can break the specification

Cliptographic Defense Strategy:
Split-Program Model



KG, H are deterministic with public input distribution



configuration is subversion free if each component has been tested by lab

Applications

- Preserving security of a signature scheme even if all algorithms are subverted;
  Previous results assume an honest KeyGen

- Using our strongly unforgeable-OWP, the Blum-Micali PRG is backdoor free—output is pseudorandom even given the backdoor

- Randomizing the public parameter pk instead of the output results in a general public immunizing strategy for backdoored PRG.