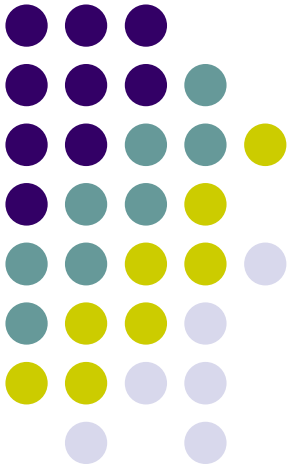
INDOCRYPT 2018
@New Delhi, India

Public Key Encryption Secure against Related Randomness Attacks

Takahiro Matsuda (***AIST***)

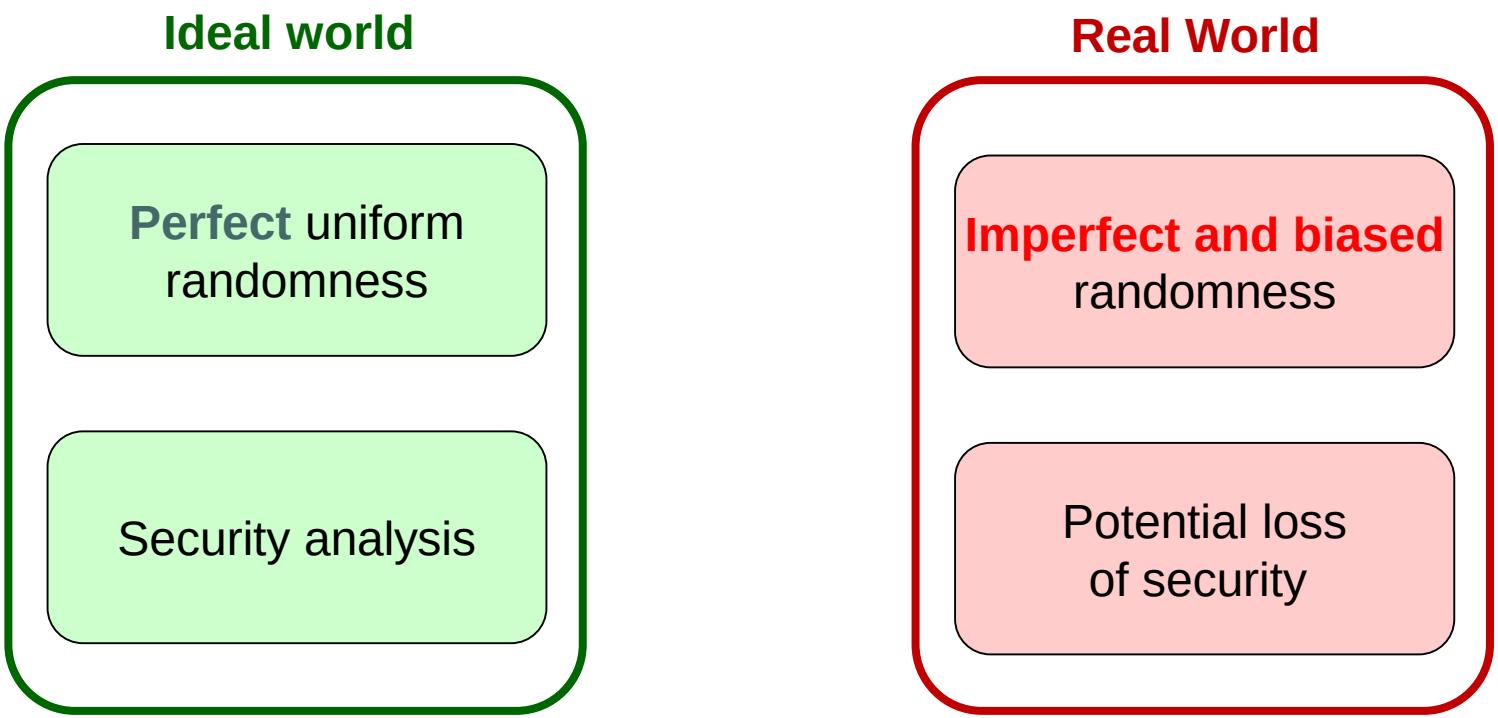
Dec. 11, 2018



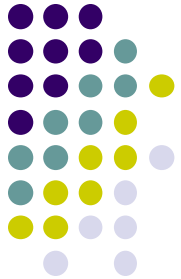
Based on the joint work with Jacob Schuldt

Randomness in Cryptography

- Randomness plays a crucial role in most cryptographic primitives

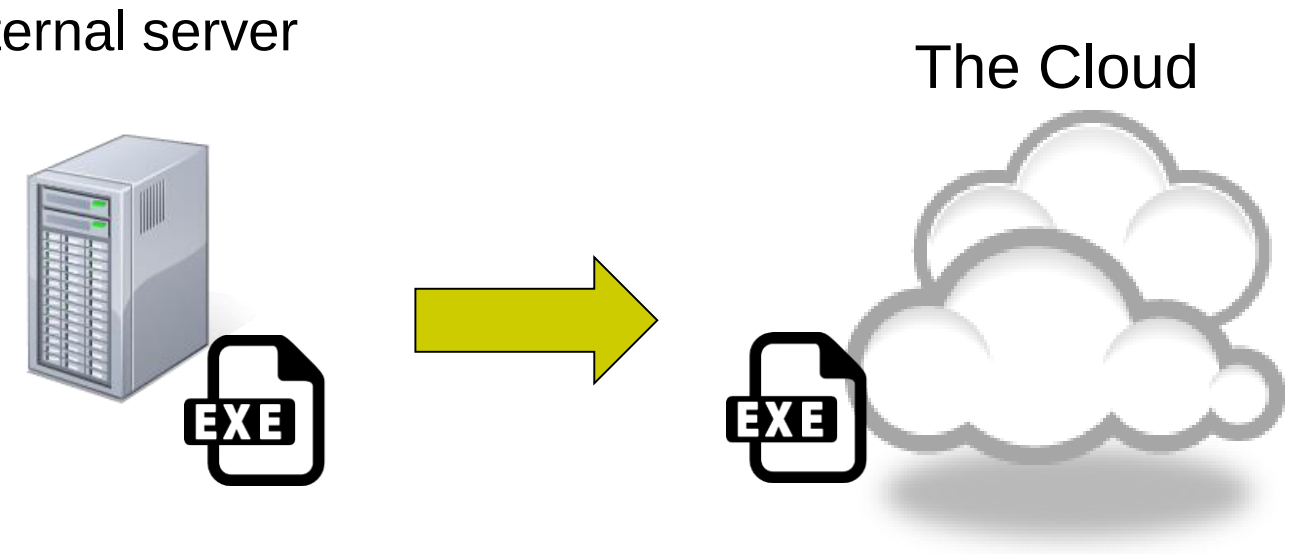


Security Incidents Due To Randomness Failures



1) http://arstechnica.com/security/2013/09/fatal-crypto-flaw-in-some-government-certified-smartcards-makes-forgery-a-snap/
2) http://www.bbc.com/news/technology-12116051
3) http://arstechnica.com/security/2013/08/google-confirms-critical-android-crypto-flaw-used-in-5700-bitcoin-heist/

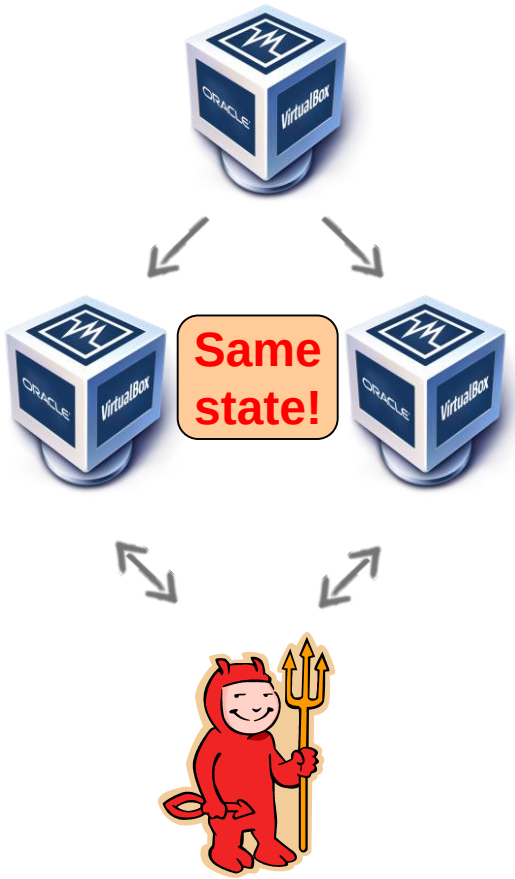
Running Applications in the Cloud



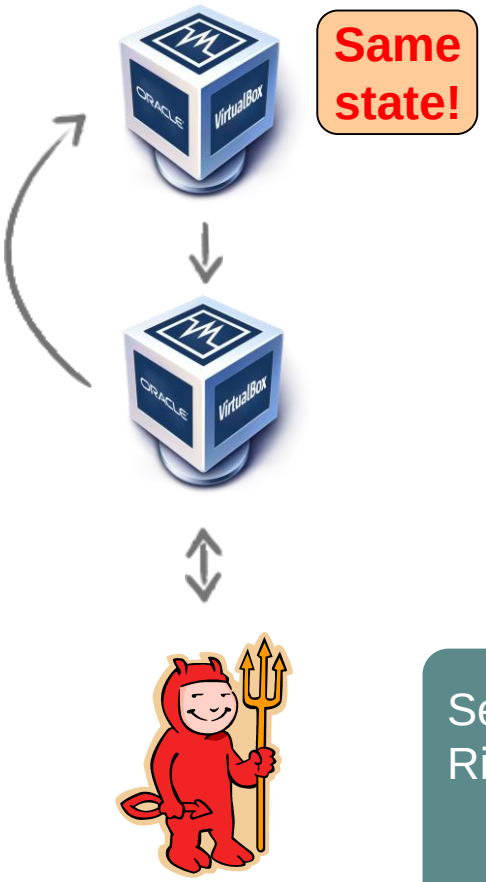
- Virtualized servers:
  - Easy to deploy
  - Easy to clone/backup
  - Ability to restore server to a known good state

Randomness Security Risks in Virtualized Environments

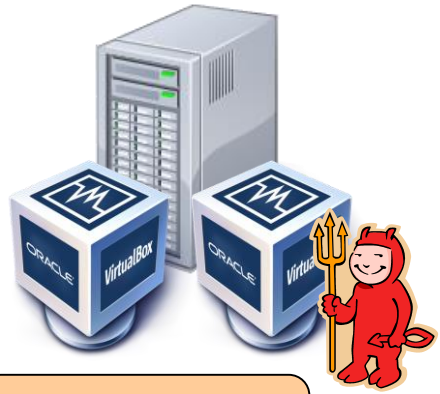
Cloning



Restoration



Co-location



Security risk demonstrated by Ristenpart and Yilek (NDSS'10):
- Recovery of TLS server signing keys via reset attack

Related Randomness Security for Public Key Encryption

PKE = (***KG***, ***Enc***, ***Dec***)

$c' = \mathbf{Enc}(pk', m'; r')$

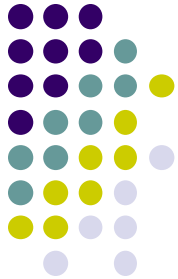
r and *r'* related

$c = \mathbf{Enc}(pk, m; r)$

Device using imperfect randomness

Will m remain confidential?

Purpose of This Talk



- Overview of the technical results of 3 papers on **related randomness security** for PKE

- [PSS14]
  - Paterson, Schuldt, Sibborn: “Related Randomness Attacks for Public Key Encryption” PKC 2014.
- [PSSW15]
  - Paterson, Schuldt, Sibborn: Wee: “Security Against Related Randomness Attacks via Reconstructive Extractors” IMA C&C 2015
- [MS18]
  - Matsuda, Schuldt: “Related Randomness Security for Public Key Encryption” PKC 2018

Talk Outline

- Definition of Related Randomness Security for PKE
- Constructions in [PSS14] and [PSSW15]
- Results of [MS18]

Talk Outline

➔ Definition of Related Randomness Security for PKE

- Constructions in [PSS14] and [PSSW15]

- Results of [MS18]

Related Randomness Security for Public Key Encryption

PKE = (***KG***, ***Enc***, ***Dec***)

$c' = \mathbf{Enc}(pk', m'; r')$

r and *r'* related

$c = \mathbf{Enc}(pk, m; r)$

Device using imperfect randomness

Will m remain confidential?

Security Against Related Randomness Attacks [PSS14]

Security notion is parameterize by function class Φ

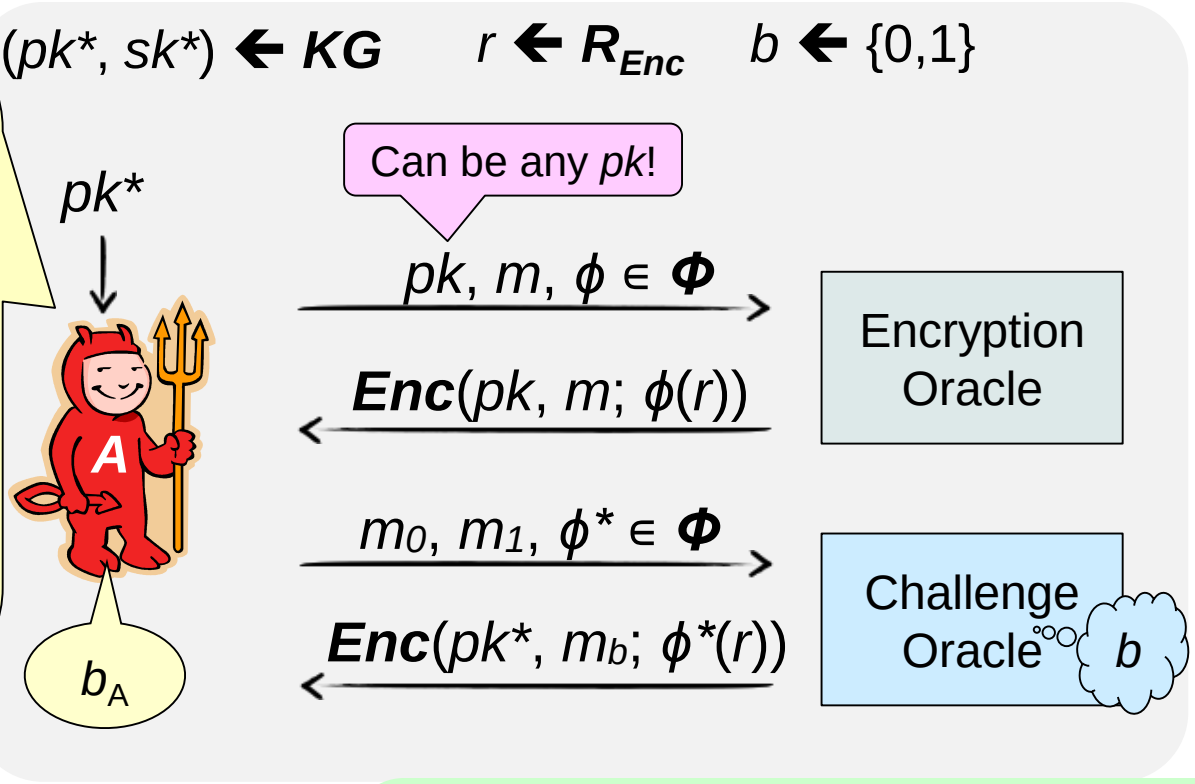
- **Φ-IND-RR-CPA** security game

Equality-pattern respecting adversary:

For all challenge queries (m_0, m_1, ϕ) and (m_0', m_1', ϕ') :

1) if $\phi = \phi'$:
$m_0 = m_0' \Leftrightarrow m_1 = m_1'$

2) m_0 and m_1 were not submitted to enc. oracle together with pk^* and ϕ



- Captures security against reset attacks [Yilek10] as a special case
- **CCA** ver. considered by adding dec. oracle

PKE is **Φ-IND-RR-CPA** secure if $\forall$ PPT EQ-pattern respecting A, $Adv(A) := | \Pr[b_A = b] - 1/2 | = neg.$

When RR-Security is Unachievable (1/2)

- A function class $\boldsymbol{\Phi}$ is **unpredictable** if

$$\forall\ \phi \in \boldsymbol{\Phi},\ y \in \boldsymbol{R}_{\boldsymbol{Enc}}:$$

$$\Pr[r \leftarrow \boldsymbol{R}_{\boldsymbol{Enc}} : \phi(r) = y\ ] = \text{neg}.$$

Proposition:

Assume $\exists\, \phi_{weak} \in \boldsymbol{\Phi}$ s.t. $y = \phi(r)$ can be guessed with non-neg. prob.
➔ **$\boldsymbol{\Phi}$-IND-RR-CPA** security is unachievable

Proof:

1. Challenge query (m_0, m_1, ϕ_{weak}) and obtain $c^* = \boldsymbol{Enc}(pk^*, m_b; \phi_{weak}(r))$
2. Make a guess y for $\phi_{weak}(r)$
3. Return 1 iff $c^* = \boldsymbol{Enc}(pk^*, m_1; y)$

➔ $\textbf{Adv}(\boldsymbol{A}) = \Pr[\ \phi_{weak}(r) = y\ ]$

When RR-Security is Unachievable (2/2)

- A function class $\boldsymbol{\Phi}$ is **collision resistant** if

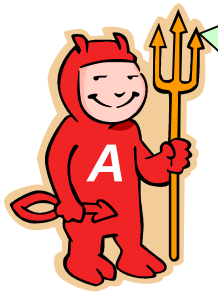
$\forall$ distinct $\phi_1, \phi_2 \in \boldsymbol{\Phi}$:

$$\Pr[r \leftarrow \boldsymbol{R}_{\boldsymbol{Enc}} : \phi_1(r) = \phi_2(r)\ ] = \text{neg}.$$

Proposition:

Assume $\exists\, \phi_{weak1}, \phi_{weak2} \in \boldsymbol{\Phi}$ s.t. $\Pr[\ \phi_{weak1}(r) = \phi_{weak2}(r)\ ] > \text{non-neg}.$
➔ **$\boldsymbol{\Phi}$-IND-RR-CPA** security is unachievable

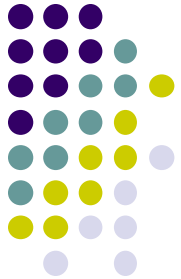
Proof:



1. Challenge query (m_0, m_1, ϕ_{weak1}) and obtain $c^* = \boldsymbol{Enc}(pk^*, m_b; \phi_{weak1}(r))$
2. Enc. query (pk^*, m_1, ϕ_{weak2}) and obtain $c' = \boldsymbol{Enc}(pk^*, m_1; \phi_{weak2}(r))$
3. Return 1 iff $c^* = c'$

➔ $\textbf{Adv}(\boldsymbol{A}) = \Pr[\ \phi_{weak1}(r) = \phi_{weak2}(r)\ ]$

RR Security and Other Security Notions



- RR security can be thought of as “tampering on enc.-randomness”
  - Dual of “tampering on a secret key”
  - Capture a restricted form of “subversion” attack where the randomness generator of PKE may be maliciously implemented

- There are several other types of security notions fighting against bad enc.-randomness, which are incomparable to RR security
  - Security against chosen distribution attacks [BNRSSY09] (AC’09)
  - Randomness-dependent message security [BCPT13] (TCC’13)
  - Cryptography with tamperable randomness [ACMPS14] (C’14)
  - Nonce-based PKE [Bellare-Tackmann17] (EC’17)

Talk Outline

- Definition of Related Randomness Security for PKE

➔ Constructions in [PSS14] and [PSSW15]

- RO Model construction
- Std. Model construction 1
- Std. Model construction 2

- Results of [MS18]

Talk Outline

- Definition of Related Randomness Security for PKE

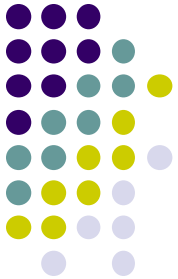
➔ Constructions in [PSS14] and [PSSW15]

➔ RO Model construction

- Std. Model construction 1
- Std. Model construction 2

- Results of [MS18]

Randomized Encryption with Hash (REwH)



- Introduced by Bellare et al. [BBNRSSY09] (AC'09) to obtain a hedged encryption scheme

Aims to achieve security against a chosen distribution attack in which (m, r) is assumed to have min-entropy

- **REwH** Scheme

Building Blocks:

- **PKE** = (***KG***, ***Enc***, ***Dec***)
- $H : \{0,1\}^* \rightarrow R_{Enc}$

REwH.KG:

1. (pk, sk) ← ***KG***
2. Return (pk, sk)

REwH.Enc(pk, m; ***r***):

1. r' ← ***H***($pk||m||$***r***)
2. c ← ***Enc***(pk, m; r')
3. Return c

REwH.Dec(sk, c):

1. m ← ***Dec***(sk, c)
2. Return m

RR-Security of REwH

Thm: Assume

- ***Φ*** is **unpredictable**
- ***Φ*** is **collision resistant**
- **PKE** is **IND-CPA / CCA**

➔ **REwH** is ***Φ*-IND-RR-CPA / CCA** in RO model

Proof Intuition:

Φ is unpredictable
➔ Input to ***H*** is unpredictable

$$c = \mathbf{Enc}(pk, m; \mathbf{H}(pk \,||\, m \,||\, \phi(r)))$$

Φ is collision resistant
➔ Input to ***H*** is not repeated

Output of ***H*** is uniform and independent

Reduction to **IND-CPA / CCA** security of **PKE**

Talk Outline

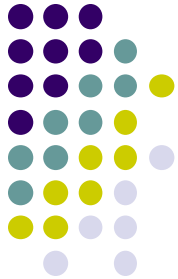
- Definition of Related Randomness Security for PKE

➔ Constructions in [PSS14] and [PSSW15]

- RO Model construction
- ➔ Std. Model construction 1
- Std. Model construction 2

- Results of [MS18]

PRF-Based Construction



Encrypt-with-PRF

- **EwP** Scheme

[Yilek10] (CT-RSA'10) showed "reset attack"-security of this scheme

REwH can be viewed as a specific instantiation of this scheme, because ***PRF***(*k*, *x*) := ***H***(*k* || *x*) is a PRF

Building Blocks:

PKE = (***KG***, ***Enc***, ***Dec***)

PRF: $K_{PRF} \times \{0,1\}^* \rightarrow R_{Enc}$

EwP.KG:

1. (*pk*, *sk*) ← ***KG***
2. Return (*pk*, *sk*)

EwP.Enc(*pk*, *m*; ***r***):

1. *r'* ← ***PRF***(***r***, *pk*||*m*)
2. *c* ← ***Enc***(*pk*, *m*; *r'*)
3. Return *c*

EwP.Dec(*sk*, *c*):

1. *m* ← ***Dec***(*sk*, *c*)
2. Return *m*

How to Prove Security ?

RR-adversary

$m_0, m_1, \boldsymbol{\phi^*}$ →

← c^*

Not possible to simulate using ordinary PRFs

$r' \leftarrow \boldsymbol{PRF}(\boldsymbol{\phi^*(r)}, pk^* || m_b)$

$c^* \leftarrow \boldsymbol{Enc}(pk^*, m_b; r')$

Φ-RKA security for ***PRF*** [BK03] (EC'03)

$x, \phi \in \boldsymbol{\Phi}$ →

← y or random

$k \leftarrow \boldsymbol{K_{PRF}}$

$y \leftarrow \boldsymbol{PRF}(\phi(k), x)$

PRF-Based Construction

Encrypt-with-PRF

- **EwP** Scheme

Building Blocks:

PKE = (***KG***, ***Enc***, ***Dec***)

PRF: $K_{PRF} \times \{0,1\}^* \rightarrow R_{Enc}$

Thm: Assume

- ***PRF*** is ***Φ*-RKA secure**
- **PKE** is **IND-CPA / CCA**

➔ **EwP** is ***Φ*-IND-RR-CPA / CCA**

[ABPP14]: Φ_{poly}-**RKA** secure **PRF**

Corollary:

EwP: Φ_{poly}-**IND-RR-CPA / CCA** secure

EwP.KG:

1. (*pk*, *sk*) ← ***KG***
2. Return (*pk*, *sk*)

EwP.Enc(*pk*, *m*; ***r***):

1. *r'* ← ***PRF***(***r***, *pk*||*m*)
2. *c* ← ***Enc***(*pk*, *m*; *r'*)
3. Return *c*

EwP.Dec(*sk*, *c*):

1. *m* ← ***Dec***(*sk*, *c*)
2. Return *m*

Talk Outline

- Definition of Related Randomness Security for PKE

➔ Constructions in [PSS14] and [PSSW15]

- RO Model construction
- Std. Model construction 1

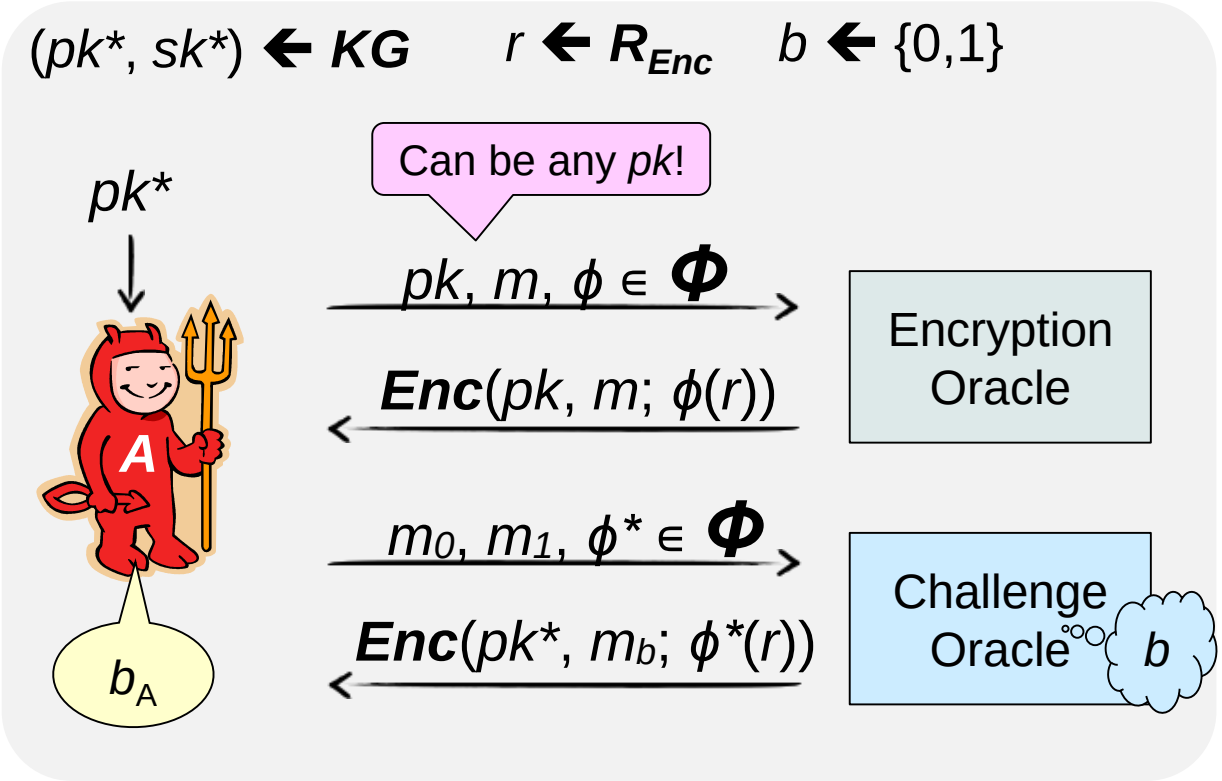
➔ Std. Model construction 2

(RR Security for Non-algebraic functions classes)

- Results of [MS18]

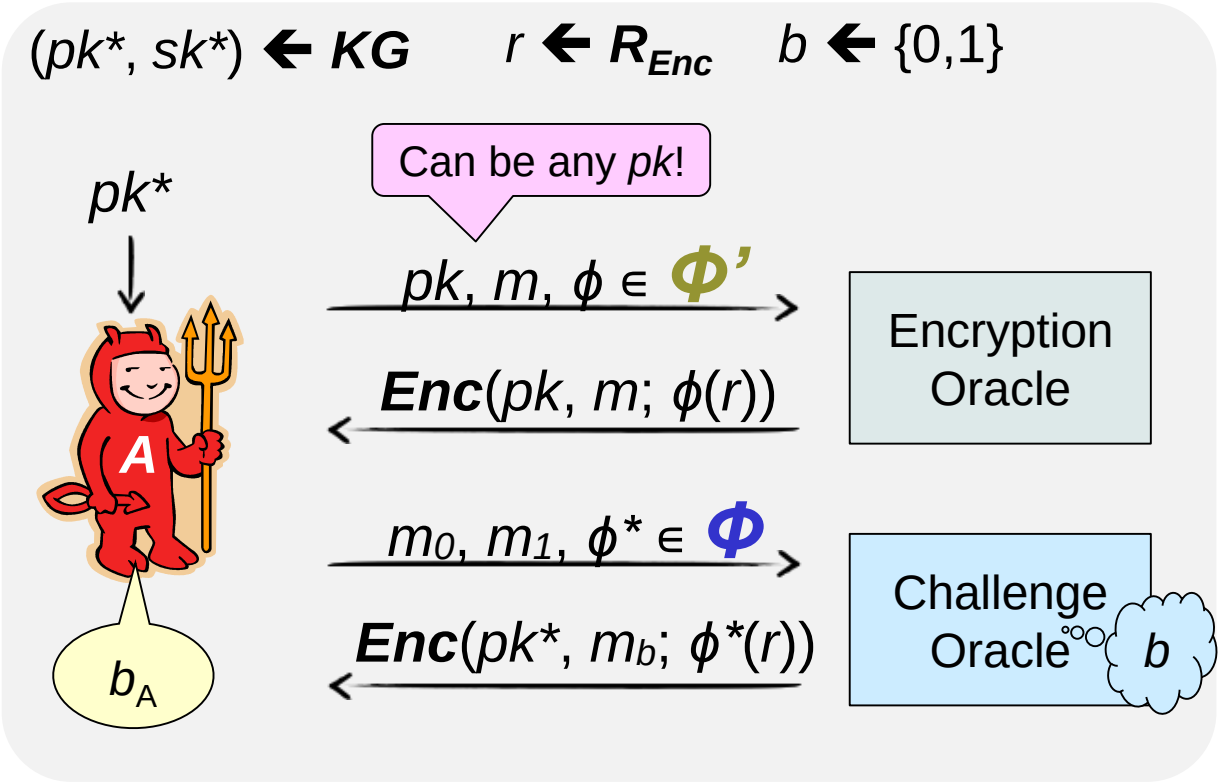
Separation of Randomness-deriving Function

- **Φ-IND-RR-CPA** security game



Separation of Randomness-deriving Function

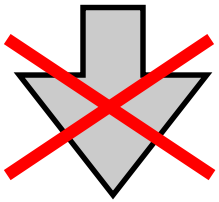
- **(Φ, Φ')-IND-RR-CPA** security game



Hard-to-Compute Function Vector Families

$\{\varphi_i(x)\}_{i\in[q]}$ is hard to compute wrt. $\{\varphi_j'(x)\}_{j\in[q']}$ if

$\{\varphi'_j(x)\}_{j\in[q']}$



$\varphi_i(x)$

Computationally hard for random x and any i

For function vector families $\boldsymbol{\Phi}$, $\boldsymbol{\Phi}'$:

$\boldsymbol{\Phi}$ is hard to compute wrt. $\boldsymbol{\Phi}'$ if

$\forall \{\varphi_i(x)\}_{i\in[q]} \in \boldsymbol{\Phi}$, $\forall \{\varphi'_j(x)\}_{j\in[q']} \in \boldsymbol{\Phi}'$:

$\{\varphi_i(x)\}_{i\in[q]}$ is hard to compute wrt. $\{\varphi'_j(x)\}_{j\in[q']}$

Reconstructive Extractor

- Requirement 1: (standard randomness extractor)

Seed
$s \leftarrow \boldsymbol{S}$

Input
$x \leftarrow \boldsymbol{D}$

Drawn from distribution with sufficient min-entropy

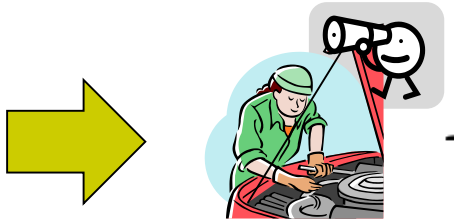
s, $\boldsymbol{Ext}(s, x)$
≈
uniform

- Requirement 2:

∃ PPT algorithm ***Rec***  s.t.

$\forall x$: s, $\boldsymbol{Ext}(s,x)$ or uniform →  → guess

Distinguisher



Rec

→ x

(Φ, Φ')-Auxiliary-Input Reconstructive Extractor

- Requirement 1: (standard randomness extractor)

Seed
$s \leftarrow \boldsymbol{S}$

Input
$x \leftarrow \boldsymbol{D}$

Drawn from distribution with sufficient min-entropy

s, $\boldsymbol{Ext}(s, x)$
≈
uniform

- Requirement 2: ∃ PPT algorithm ***Rec***  s.t.

$aux = \{\varphi_i'(x)\}_{i\in[q]}$

$aux = \{\ \varphi_i'(x)\ \}_{i\in[q]}$

$\forall x$: s, $\{\ \boldsymbol{Ext}(s,\varphi_j(x))\ \}_{j\in[q']}$ or uniform

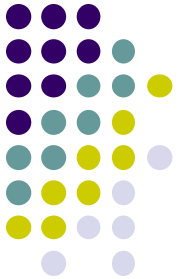
Distinguisher

guess

Rec

x

Encrypt with Extractor and PRF [PSSW15]



Encrypt with Extractor and PRF

- **EwE** Scheme

Building Blocks:

PKE = (***KG***, ***Enc***, ***Dec***)

Ext : $S \times D \rightarrow K_{PRF}$

PRF: $K_{PRF} \times \{0,1\}^* \rightarrow R_{Enc}$

EwE.KG:

1. (*pk*, *sk*) ← ***KG***
2. *s* ← ***S***
3. *PK* ← (*pk*, *s*)
4. Return (*PK*, *sk*)

EwE.Enc(*PK*, *m*; ***r***):

1. *k* ← ***Ext***(*s*, ***r***)
2. *r'* ← ***PRF***(*k*, *pk*||*m*)
3. *c* ← ***Enc***(*pk*, *m*; *r'*)
4. Return *c*

EwE.Dec(*sk*, *c*):

1. *m* ← ***Dec***(*sk*, *c*)
2. Return *m*

RR-Security of EwE

Thm: Assume

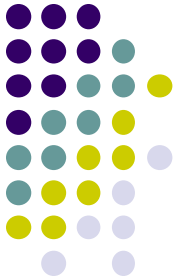
- ***PRF*** is a standard PRF
- ***Ext*** is a (***Φ***, ***Φ'***)-auxiliary input reconstructive extractor
- **PKE** is **IND-CPA / CCA**

➔ **EwE** is **selective** **(*Φ*, *Φ'*)-IND-RR-CPA / CCA**

Adversary must commit to functions $\{\phi_i\}_{i \in [q]}, \{\phi'_j\}_{j \in [q]}$ before seeing *PK*

Separate function classes ***Φ***, ***Φ'*** are considered

Reconstructive Extractor from Goldreich-Levin over Large Fields

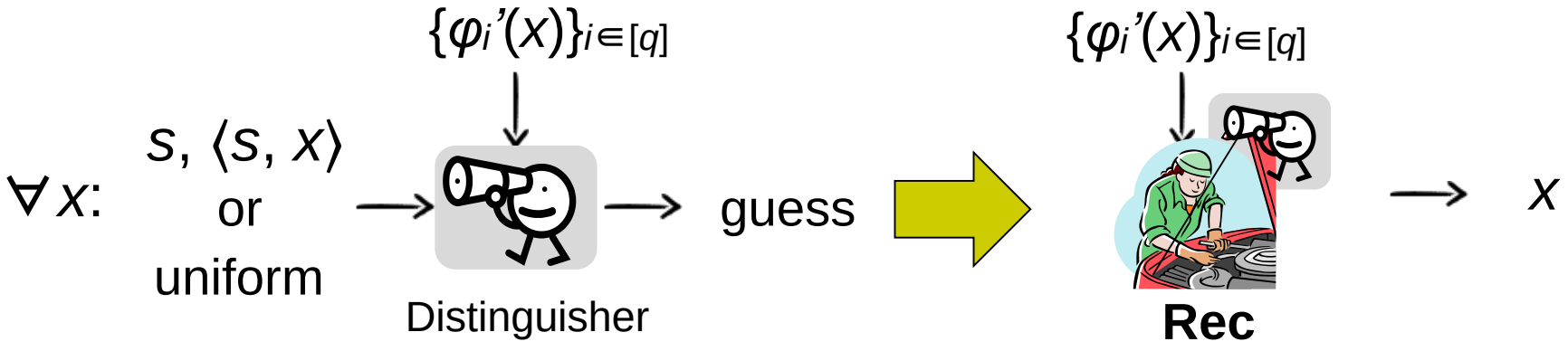


$s = (s_1,\ldots,s_n) \leftarrow (\mathbb{Z}_p)^n$
$x = (x_1,\ldots,x_n) \leftarrow \boldsymbol{H}^n \subset (\mathbb{Z}_p)^n$

$\boldsymbol{Ext}(s, x) := \langle s, x \rangle$

Thm: ***Ext*** is a (**id**, **Φ**')-auxiliary input reconstructive extractor for a hard-to-invert function family **Φ'**

Proof based on [DGKPV10] (TCC'10)

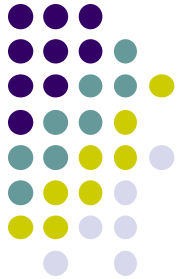


$2 \cdot \Pr[\text{Distinguisher succeeds}] - 1 =: \varepsilon$

$\Pr[\text{Rec succeeds}] = \varepsilon^3 / 512 \cdot n \cdot p^2$

$\textbf{Time}(\text{Rec}) = \textbf{Time}(\text{Distinguisher}) \times \textbf{poly}(n, |\boldsymbol{H}|, 1/\varepsilon)$

Comparison of Schemes in [PSS14,PSSW15]



	Construction	Selective vs. Adaptive	Function Family
[PSS14]	**REwH**	adaptive, in RO model	∀ coll. resistant and unpredictable functions
[PSSW15]	**EwP**	adaptive	polynomials
[PSSW15]	**EwE**	adaptive	hard-to-invert **Φ**' for encrypt queries

[PSS14] proposes another concrete construction of a **Φ-IND-RR-CPA** secure scheme for hard-to-invert func. class **Φ,** from a variant of DDH assumption, but omitted in this talk

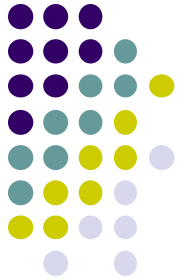
Talk Outline

- Definition of Related Randomness Security for PKE

- Constructions in [PSS14] and [PSSW15]
  - RO Model construction
  - Std. Model construction 1
  - Std. Model construction 2

➔ Results of [MS18]

Results of [MS18] in One Slide



- 1: Limitation of **IND-RR** security model
  - ... and a small positive news for **REwH**
- 2: New security model:
  Related Refreshable Randomness (RRR) Security
- 3: Generic Construction of **IND-RRR-CCA** secure PKE
  for function families with size $\leqq 2^{poly}$
  - CCA PKE + PRF + Correlated Input Secure (CIS) Hash
  - Technical tool:
    Φ-correlated input secure (CIS) hash for $|\Phi| \leqq 2^{poly}$
    based on a t-wise ind. hash with a new leftover hash lemma

Talk Outline

- Definition of Related Randomness Security for PKE

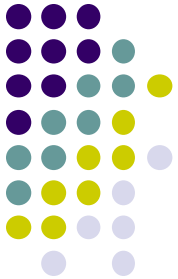
- Constructions in [PSS14] and [PSSW15]
  - RO Model construction
  - Std. Model construction 1
  - Std. Model construction 2

➔ Results of [MS18]

➔ Limitation of IND-RR security model

- Definition of Related Refreshable Randomness Security
- Generic construction

Limit on Complexity of Function Classes: Φ-IND-RR-CPA attack on any PKE



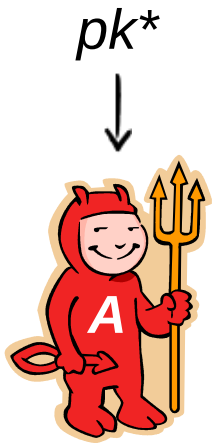
Thm:

Assume $\phi^*(\cdot) := f(\ \mathbf{Enc}(pk^*, 0; \cdot\ )\ ) \in \Phi$

for some $f : \mathbf{C} \rightarrow \mathbf{R}_{\mathbf{Enc}}$

➔ **No** PKE scheme is **Φ-IND-RR-CPA** secure

The attack:



$pk^*, m = 0, \mathbf{id}()$ →

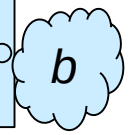
← $c = \mathbf{Enc}(pk^*, 0; r)$

Encryption Oracle

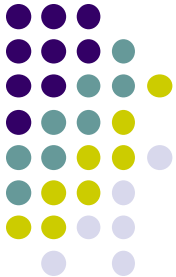
$m_0 = 0, m_1 \neq 0, \phi^*$ →

← $\mathbf{Enc}(pk^*, m_b; f(c))$

Challenge Oracle



Limit on Complexity of Function Classes: Φ-IND-RR-CPA attack on any PKE



- 

has obtained c and $c^* = \mathbf{Enc}(pk^*, m_b; f(c))$

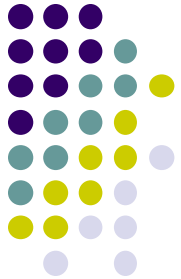
- Then, compute $c' = \mathbf{Enc}(pk^*, 0; f(c))$ by itself and check if $c' = c^*$
  - ➔ $c' = c^*$ iff $b = 0$
  - ➔ Win the **IND-RR-CPA** game with max. advantage

- Note: Unpredictable and collision-resistant function family can contain $\phi^*(\cdot) := f(\mathbf{Enc}(pk^*, 0; \cdot))$

Unpredictable for appropriate f

Does not collide with r

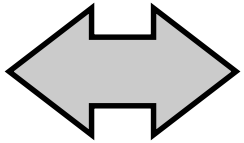
Another Look at REwH in the Random Oracle Model



[PSS14]:

REwH is ***Φ*-IND-RR-CPA** in RO model for unpredictable and collision-resistant ***Φ***

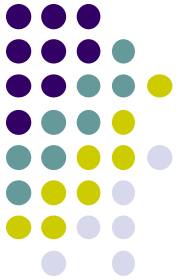
Contradiction?



[MS18]:

Φ-IND-RR-CPA security can't be achieved for **Φ** that includes the ***Enc*** algorithm of the scheme

Another Look at REwH in the Random Oracle Model

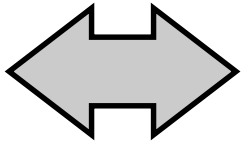


[PSS14]:

REwH is ***Φ*-IND-RR-CPA** in RO model for unpredictable and collision-resistant ***Φ***

Assumes that ***Φ*** is independent of the RO

Contradiction?



[MS18]:

Φ-IND-RR-CPA security can't be achieved for **Φ** that includes the ***Enc*** algorithm of the scheme

If ***Φ*** depends on ***H***, security is not achieved

Another Look at REwH in the Random Oracle Model

is said to respect
Indirect *H*-query uniqueness
if all indirect queries made to the RO via enc. and challenge queries, are unique

REwH:
$c = \mathbf{Enc}(pk, m; \mathbf{H}(pk||m||r))$

Thm: Assume

- ***Φ*** is unpredictable
- **PKE** is **IND-CPA / CCA**

➔ **REwH** is **(*Φ*, *Φ'*)-IND-RR-CPA / CCA in RO model** against indirect ***H***-query uniqueness respecting adversaries

Not so satisfactory ☹ because indirect ***H***-query uniqueness is artificial and whether ***A*** respects it can't be checked in general

Talk Outline

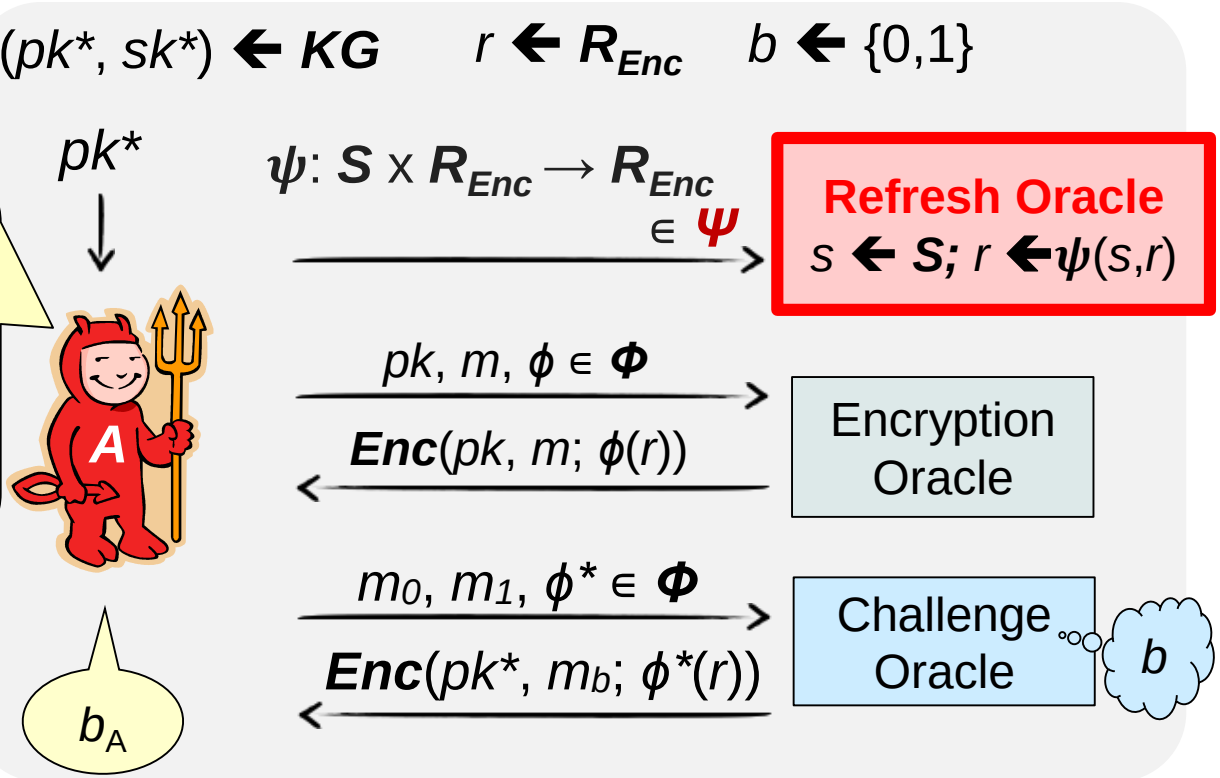
- Definition of Related Randomness Security for PKE

- Constructions in [PSS14] and [PSSW15]
  - RO Model construction
  - Std. Model construction 1
  - Std. Model construction 2

➔ Results of [MS18]
  - Limitation of IND-RR security model
  - ➔ Definition of Related Refreshable Randomness Security
  - Generic construction

Extension:
Related Refreshable Randomness Security

- **(*n*, *Φ*, *Ψ*)-IND-RRR-CPA** security game



***n*-refresh respecting adversary**:

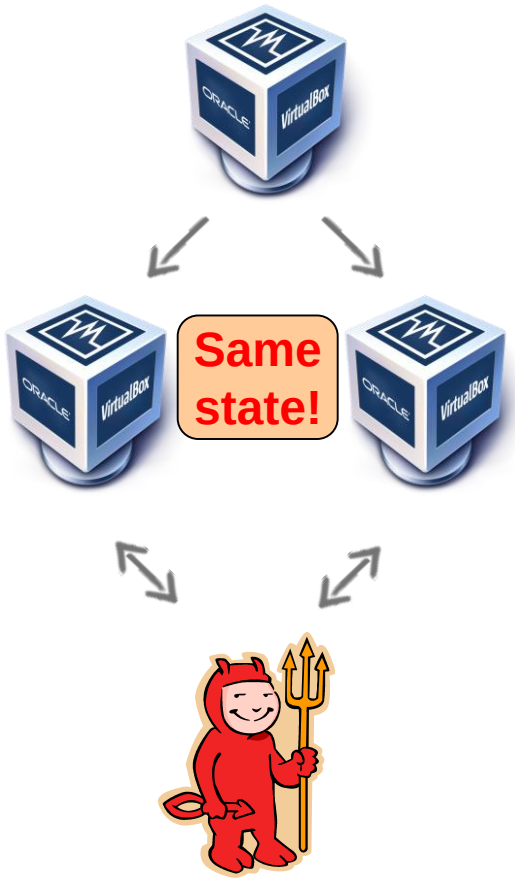
makes in total at most
n enc. and challenge queries
between each refresh query

PKE is **(*n*, *Φ*, *Ψ*)-IND-RRR-CPA** secure
if ∀ PPT EQ-pattern & ***n***-refresh respecting ***A***,
Adv(***A***) := | Pr[$b_A = b$] − 1/2 |

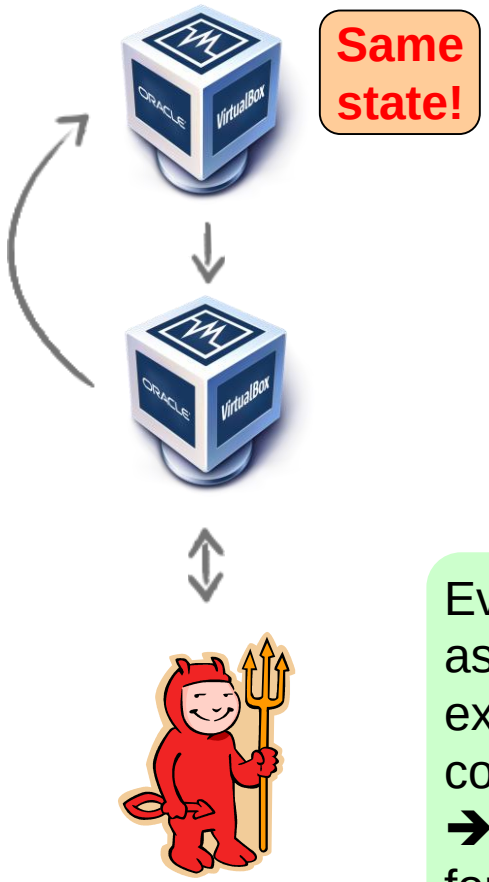
- **CCA** ver. considered by adding dec. oracle

Rationale behind Related Refreshable Randomness Security

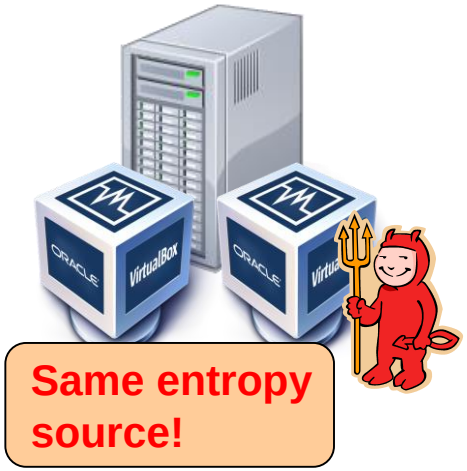
Cloning



Restoration



Co-location



Even if a reset occurs, as soon as the system is connected to external network, new entropy comes in

➔ The “same state” does not last for a long time period (hopefully)

Talk Outline

- Definition of Related Randomness Security for PKE

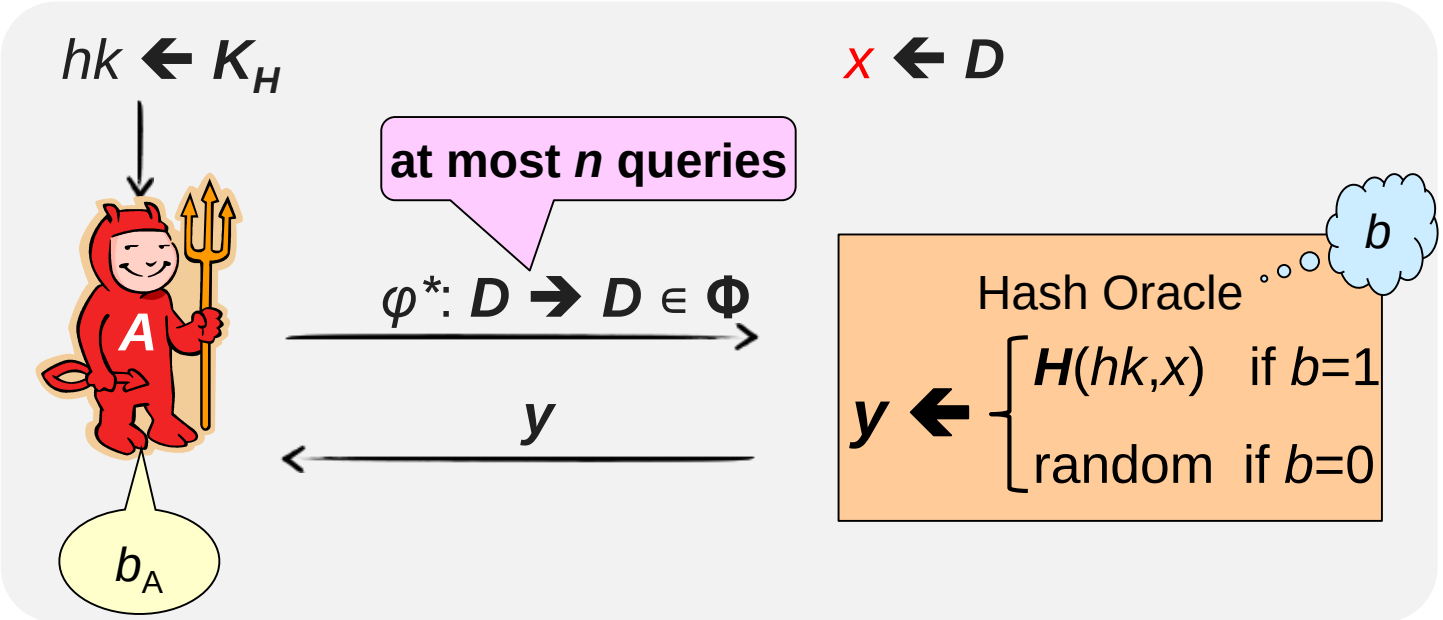
- Constructions in [PSS14] and [PSSW15]
  - RO Model construction
  - Std. Model construction 1
  - Std. Model construction 2

➔ Results of [MS18]
  - Limitation of IND-RR security model
  - Definition of Related Refreshable Randomness Security

  ➔ Generic construction

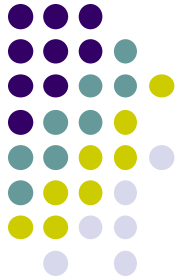
Correlated Input-Secure (CIS) Hash Functions [GOR11] (TCC'11)

- Let H: $K_H \times D \rightarrow R$ be a keyed hash function



H is a **(n, Φ)-CIS** hash function
if $\forall$ PPT A,
$\mathbf{Adv}(A) := | \Pr[b_A = b] - 1/2 | = \text{neg}.$

Encrypt with CIS Hash and PRF



Encrypt with CIS hash and PRF

- **EwC** Scheme

Building Blocks:

PKE = (***KG***, ***Enc***, ***Dec***)

$H : K_H \times D \rightarrow K_{PRF}$

PRF: $K_{PRF} \times \{0,1\}^* \rightarrow R_{Enc}$

EwC.KG:

1. (*pk*, *sk*) ← ***KG***
2. *hk* ← K_H
3. *PK* ← (*pk*, *s*)
4. Return (*PK*, *sk*)

EwC.Enc(*PK*, *m*; ***r***):

1. *k* ← ***H***(*hk*, ***r***)
2. *r'* ← ***PRF***(*k*, *pk*||*m*)
3. *c* ← ***Enc***(*pk*, *m*; *r'*)
4. Return *c*

EwE.Dec(*sk*, *c*):

1. *m* ← ***Dec***(*sk*, *c*)
2. Return *m*

Construction itself appeared in [PSS14]

RRR-Security of EwC

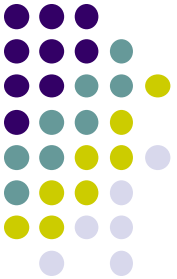
Thm: Assume

- ***H*** is a (*n*,***Γ***)-**CIS** hash for $\Gamma := \{ \varphi(\psi(r, \cdot)) \}_{\varphi \in \Phi, \psi \in \Psi, r \in D}$
- ***PRF*** is a standard PRF
- **PKE** is **IND-CPA / CCA**

➔ **EwC** is **(*n*, *Φ*, *Φ'*)-IND-RRR-CPA / CCA**

- Proof intuition:
  - PRF + ***F*-CIS** hash ➔ ***F*-RKA-PRF** for any function class ***F***
  - PKE + (*n*,***Γ***)-**RKA-PRF** ➔ (*n*,*Φ*,*Ψ*)-**IND-RRR** secure PKE

CIS Hash Based on t-wise Independent Hash



- A keyed hash function $\boldsymbol{H}$: $\boldsymbol{K_H} \times \boldsymbol{D} \rightarrow \boldsymbol{R}$ is t-wise independent if

$\forall$ distinct $x_1, \ldots, x_t$ and $\forall y_1, \ldots, y_t$:

$$\Pr[hk \leftarrow \boldsymbol{K_H} : \boldsymbol{H}(hk, x_1)=y_1 \wedge \ldots \wedge \boldsymbol{H}(hk, x_t)=y_t] = 1/|\boldsymbol{R}|^t$$

Thm: Assume

1. $\boldsymbol{H}$ is a t-wise independent hash with $|\boldsymbol{D}| \geqq |\boldsymbol{R}| = 2^{\lambda}$
2. $\boldsymbol{\Phi}$ is unpredictable and collision resistant and $\boldsymbol{\Gamma}$ is δ-unpredictable and ε-collision resistant
3. $|\boldsymbol{\Gamma}| \leqq 2^p$ where p is a polynomial
4. $t \geqq (p + 2\lambda) \cdot n$
5. $\delta \leq O(2^{-(3n+3)\lambda})$
6. $\varepsilon \leq O(2^{-n\lambda})$

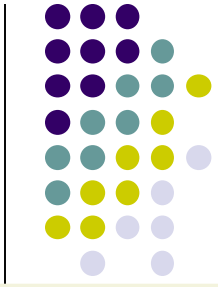
$\boldsymbol{\Gamma} = \{ \varphi(\psi(r, \cdot)) \}_{\varphi \in \boldsymbol{\Phi}, \psi \in \boldsymbol{\Psi}, r \in \boldsymbol{D}}$

δ and ε need to be very small ☹ (Can we relax?)

This result follows from our new variant of leftover hash lemma

➔ For any (comp. unbounded) n-query adversary $\boldsymbol{A}$ against the $(n, \boldsymbol{\Gamma})$-CIS security of $\boldsymbol{H}$, $\mathbf{Adv}(\boldsymbol{A}) \leqq O(2^{-\lambda})$

Encrypt with CIS Hash and PRF



- **EwC** Scheme

Building Blocks:

PKE = (***KG***, ***Enc***, ***Dec***)

$H : K_H \times D \rightarrow K_{PRF}$

PRF: $K_{PRF} \times \{0,1\}^* \rightarrow R_{Enc}$

Corollary: Assume

1. ***H*** is a t-wise indep. Hash with $|D| \geqq |R| = 2^{\lambda}$
2. ***Φ*** is unpredictable and collision resistant and ***Γ*** is δ-unpredictable and ε-collision resistant
3. $|\Gamma| \leqq 2^{p}$ where p is a polynomial
4. $t \geqq (p + 2\lambda) \cdot n$
5. $\delta \leq O(2^{-(3n+3)\lambda})$
6. $\varepsilon \leq O(2^{-n\lambda})$
7. **PKE** is **IND-CPA / CCA**

→ ***EwC*** is (***n***, ***Φ***, ***Ψ***)-**IND-RRR-CPA / CCA**

EwC.KG:

1. (*pk*, *sk*) ← ***KG***
2. *hk* ← K_H
3. *PK* ← (*pk*, *s*)
4. Return (*PK*, *sk*)

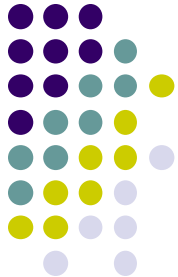
EwC.Enc(*PK*, *m*; ***r***):

1. *k* ← H_{hk}(***r***)
2. *r'* ← ***PRF***(*k*, *pk*||*m*)
3. *c* ← ***Enc***(*pk*, *m*; *r'*)
4. Return *c*

EwE.Dec(*sk*, *c*):

1. *m* ← ***Dec***(*sk*, *c*)
2. Return *m*

Overview of Constructions



	Scheme	PK	$C = Enc(pk, m; r')$ where r' =?	Security	Function Family
[PSS14]	**REwH**	*pk*	$r' = \boldsymbol{H}(pk \,\|\|\, m \,\|\|\, \boldsymbol{r})$	IND-RR-ATK, RO model	coll. resistant and unpred, independent of ***H***
[MS18]	**REwH**	*pk*	$r' = \boldsymbol{H}(pk \,\|\|\, m \,\|\|\, \boldsymbol{r})$	IND-RR-ATK, RO model indirect ***H***-query uniqueness	coll. resistant and unpred. dependent on ***H***
[PSSW15]	**EwP**	*pk*	$r' \leftarrow \boldsymbol{PRF}(\boldsymbol{r}, pk \,\|\|\, m)$	IND-RR-ATK	polynomials
[PSSW15]	**EwE**	(*pk, s*)	$k \leftarrow \boldsymbol{Ext}(s, \boldsymbol{r})$ $r' \leftarrow \boldsymbol{PRF}(k, pk \,\|\|\, m)$	selective IND-RR-ATK	hard-to-invert $\boldsymbol{\Phi}'$ for enc. queries
[MS18]	**EwC**	(*pk*, *hk*)	$k \leftarrow \boldsymbol{H}(hk, \boldsymbol{r})$ $r' \leftarrow \boldsymbol{PRF}(k, pk \,\|\|\, m)$	IND-RRR-ATK ***n***-refresh respecting	coll. resistant* and unpred.* $\|\boldsymbol{\Gamma}\| \leq 2^p$

Summary

- Be aware of randomness failures
  - Both in design and use of cryptographic primitives
- Full **IND-RR-CPA / CCA** security cannot be achieved if related randomness functions capture the encryption function of the scheme
- In the random oracle model
  - "Optimal" **IND-RR-ATK** security achievable via simple **REwH** construction (assuming independence of related randomness functions and ***H***)
- In the standard model
  - RKA-secure PRF leads to **IND-RR-CPA/CCA** secure encryption
  - **IND-RRR-CPA / CCA** security achievable for function families with a-priori bounded size 2^{poly}

Open Problems

- Construct ***Φ*-IND-RR-CCA** / (***n***, ***Φ***, ***Ψ***)-**IND-RRR-CCA** secure PKE schemes with richer function classes ***Φ***, ***Ψ***
  - Promising approaches will be to construct ***Φ*-CIS** hash functions with richer classes ***Φ***
- RR-/RRR-security for other encryption primitives (e.g. IBE, ABE, PE, FE), and even other primitives (e.g. key-exchange)

Thank you !