
On the Key Dependent Message Security of the Fujisaki-Okamoto Constructions

Fuyuki Kitagawa (Tokyo Institute of Technology / AIST)

Takahiro Matsuda (AIST)

Goichiro Hanaoka (AIST)

Keisuke Tanaka (Tokyo Institute of Technology)

Security notions for public key encryption (PKE)

◆ It has been considered “IND-CCA security = standard”

- ◆ takes active adversaries into consideration
- ◆ implies non-malleability

but!

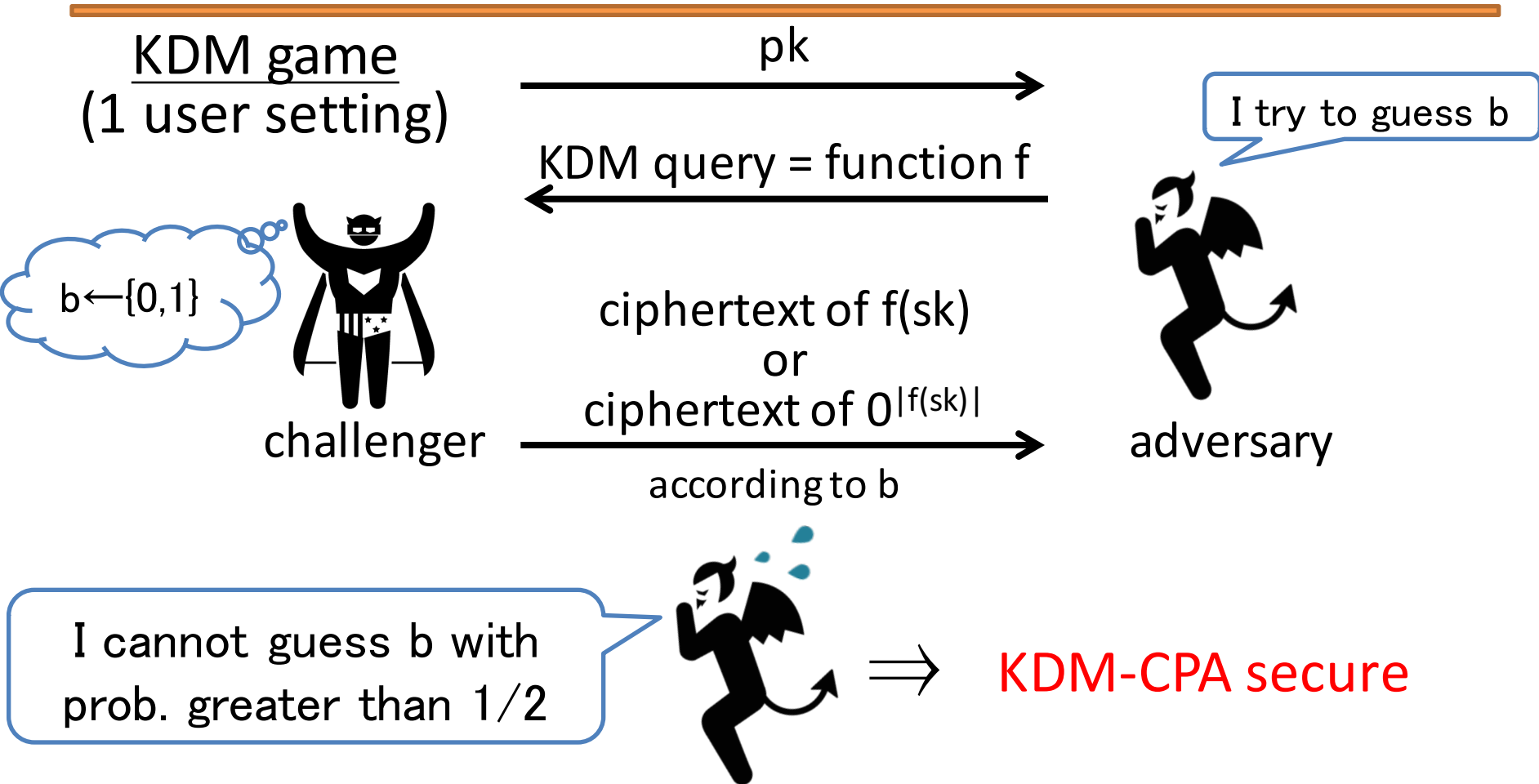


There is a situation where
IND-CCA security is not sufficient

↳ One typical example is encrypting secret keys

➔ Key dependent message (KDM) security [BRS02]

KDM security



◆ The adversary can also make a decryption query

\Rightarrow **KDM-CCA secure**

IND-CCA vs KDM-CCA

◆ It has been considered “IND-CCA security = standard”

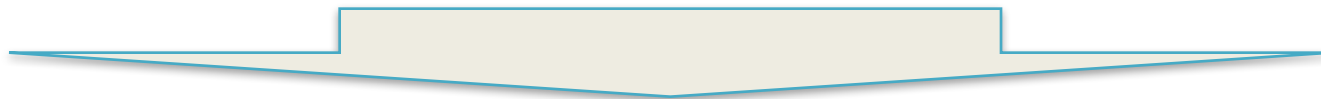


The security of standardized PKE schemes has been analyzed only in the sense of IND-CCA security

◆ These schemes remain secure

in the situation of encrypting secret keys...?

↳ It can occur in complicated systems



It is very important to clarify whether

**Standardized schemes are secure
in the sense of KDM-CCA security ?**



related works

◆ OAEP satisfies KDM-CCA security ? [BDU08]



A. Yes (in the random oracle model)

if the underlying TDP satisfies
partial-domain one-wayness

◆ hybrid encryption satisfies KDM-CCA security ? [DS14]



[KEM : OW-CCA
DEM : OT-CCA
KDF : hash function



KDM-CCA secure
(in the random oracle model)

There are many schemes these works do not capture !

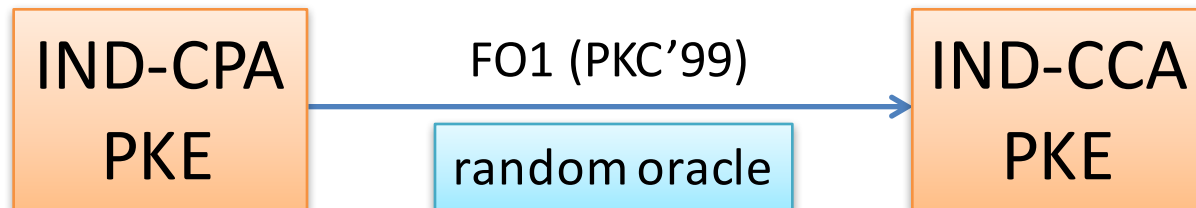
This work

◆ We clarify

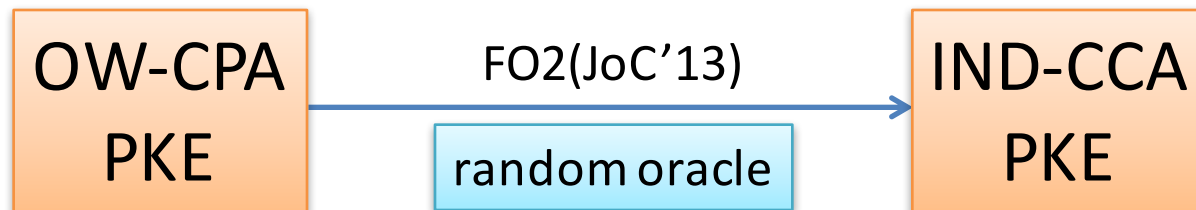
Fujisaki-Okamoto constructions satisfy KDM-CCA security

→ Concrete instantiation “EPOC” has been included by IEEE p1363a

Fujisaki-Okamoto constructions



Not KDM-CCA secure in general
New!



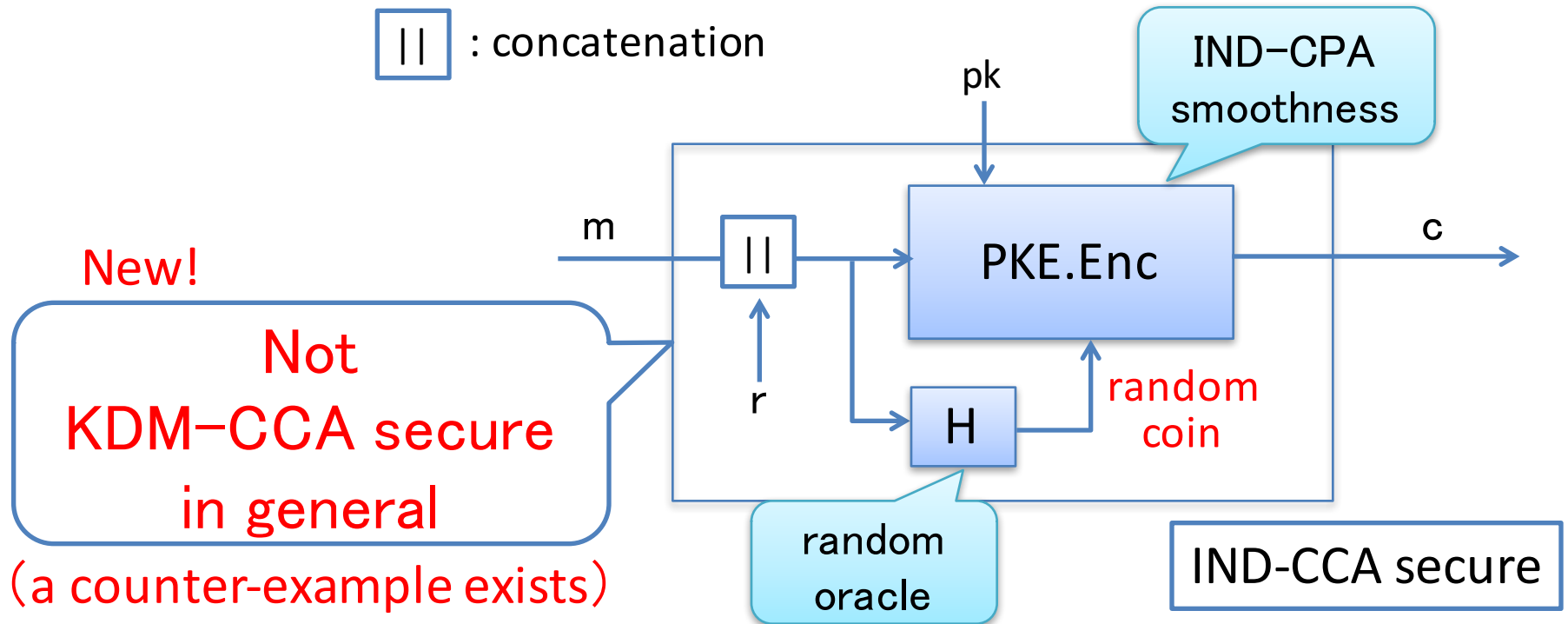
KDM-CCA secure in general
New!



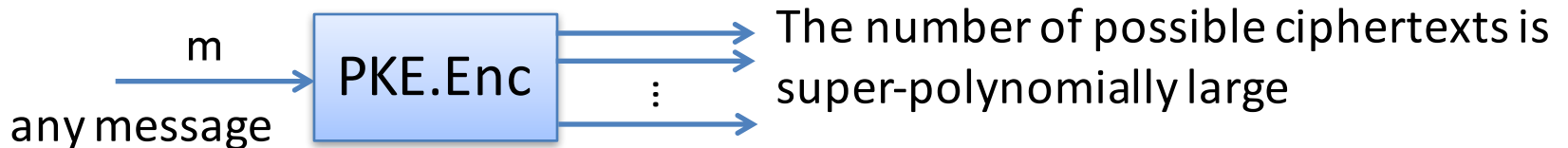
(* based on CRYPTO'99 ver.)

FO1(PKC'99)

\parallel : concatenation



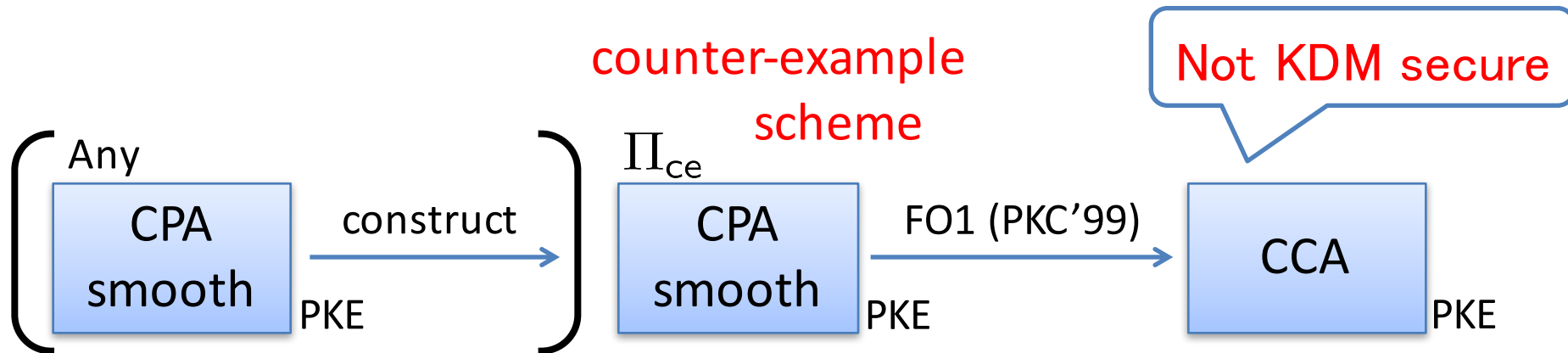
smoothness



*many CPA PKE satisfy smoothness

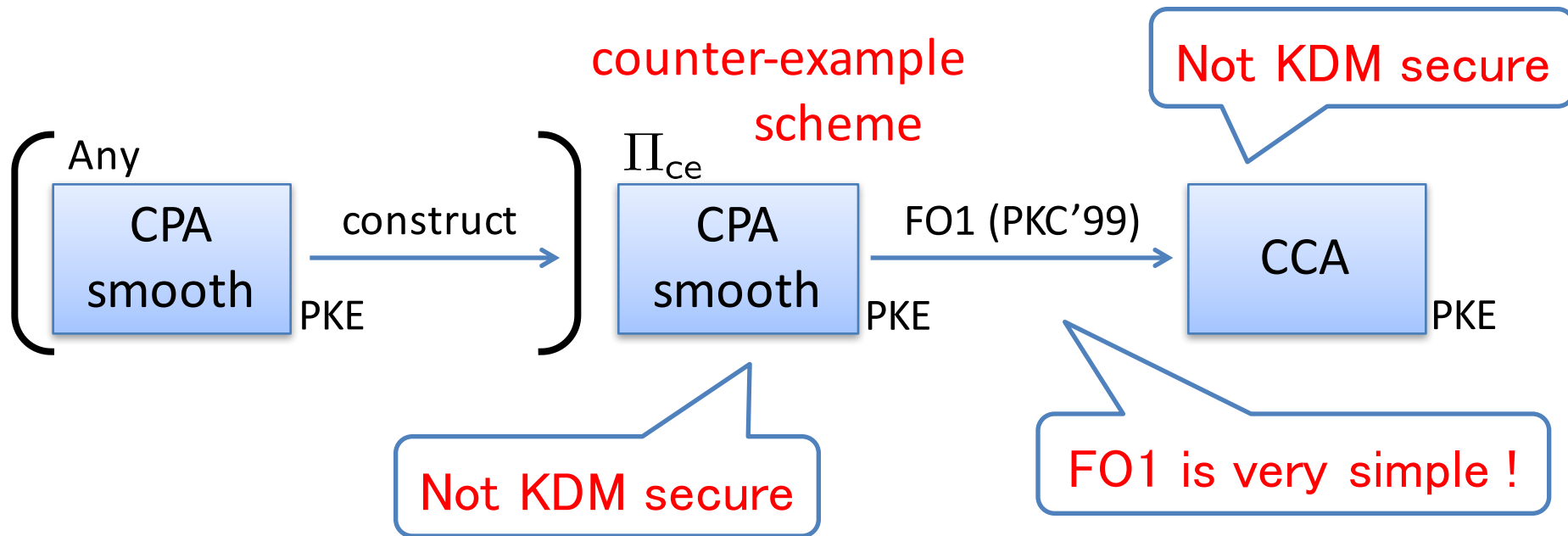
Outline of the proof

- ◆ We show a counter-example scheme



Outline of the proof

- ◆ We show a counter-example scheme



This work

◆ We clarify

Fujisaki-Okamoto constructions satisfy KDM-CCA security

Concrete instantiation EPOC has been included by IEEE p1363a

Fujisaki-Okamoto constructions

IND-CPA
PKE

FO1 (PKC'99)

random oracle

IND-CCA
PKE

Not
KDM-CCA secure
in general



New!

Next

OW-CPA
PKE

FO2 (JoC'13)

random oracle

IND-CCA
PKE

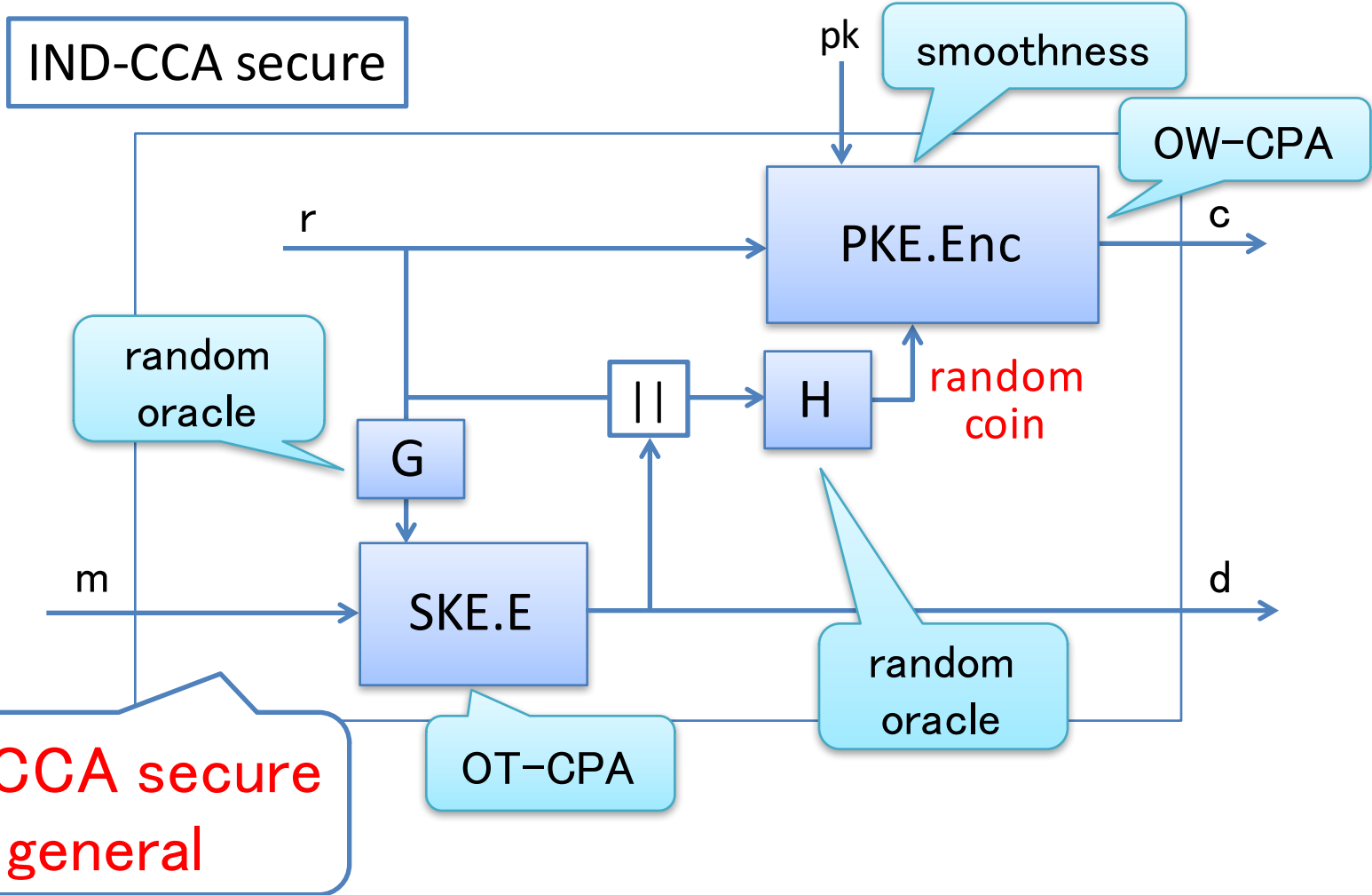
KDM-CCA secure
in general



New!

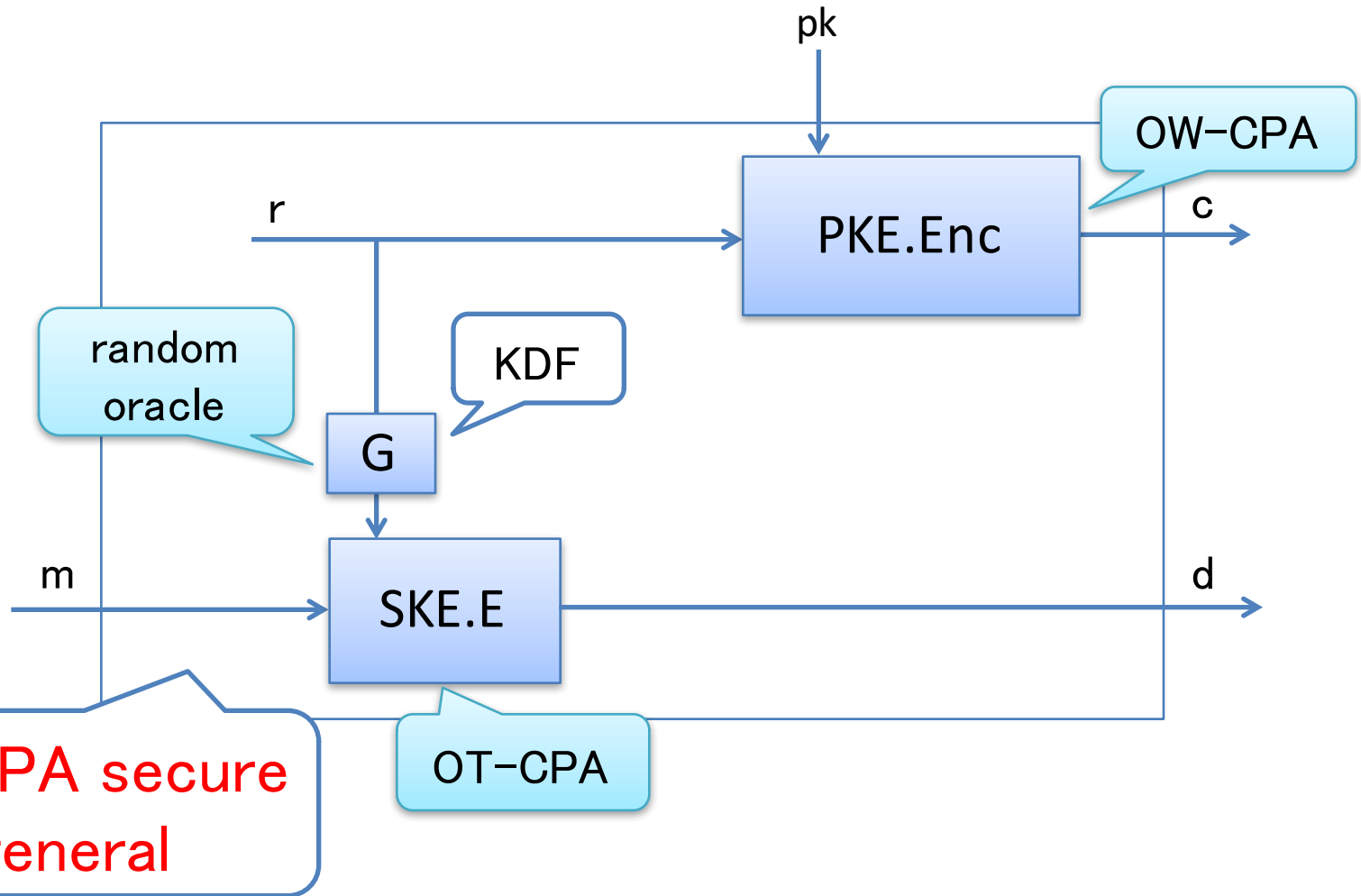
+
OT-CPA
SKE

FO2 (JoC'13)



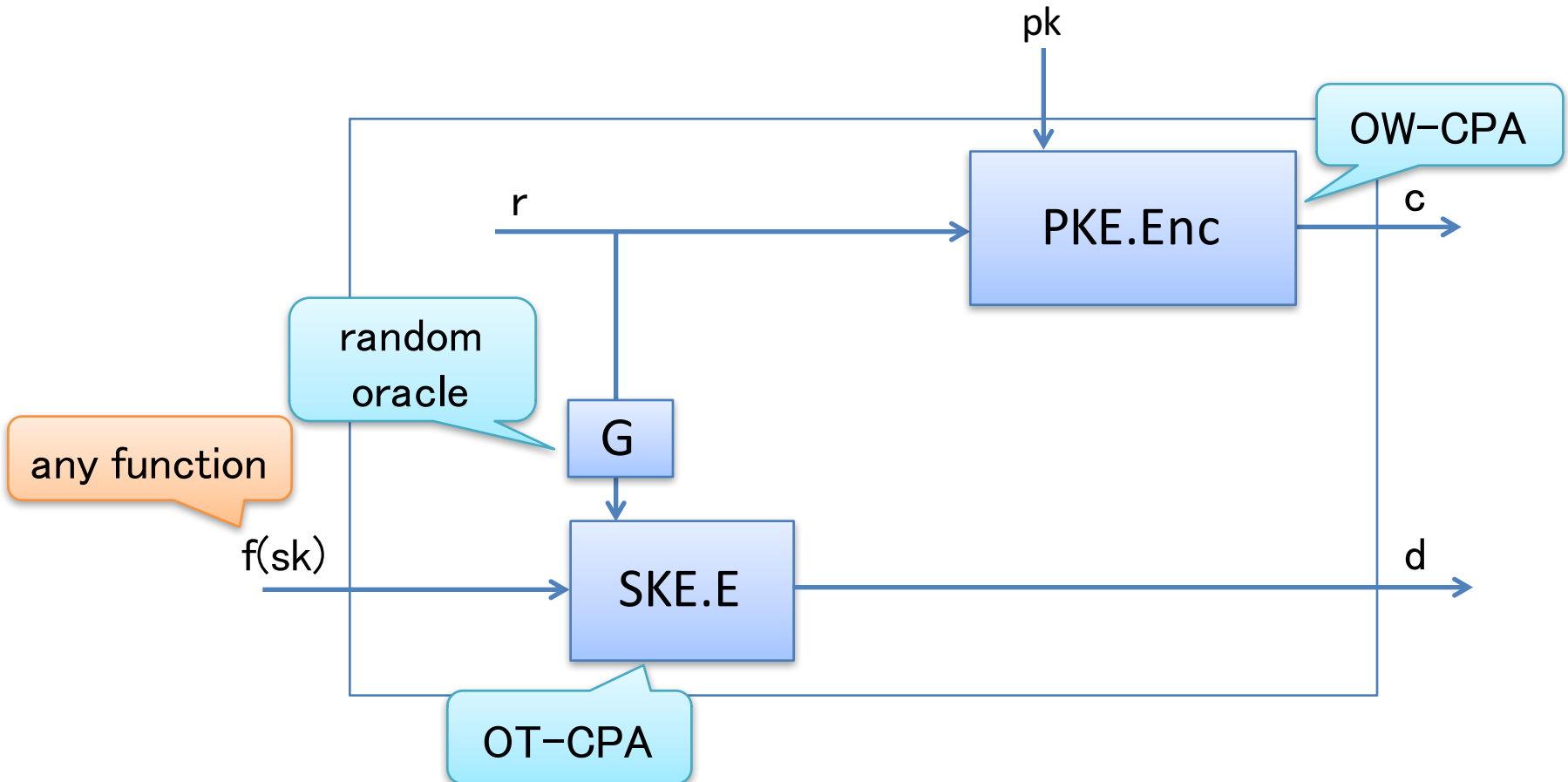
$$(c := \text{Enc}(pk, r; H(r, d)), d := E(G(r), m))$$

essentially hybrid encryption

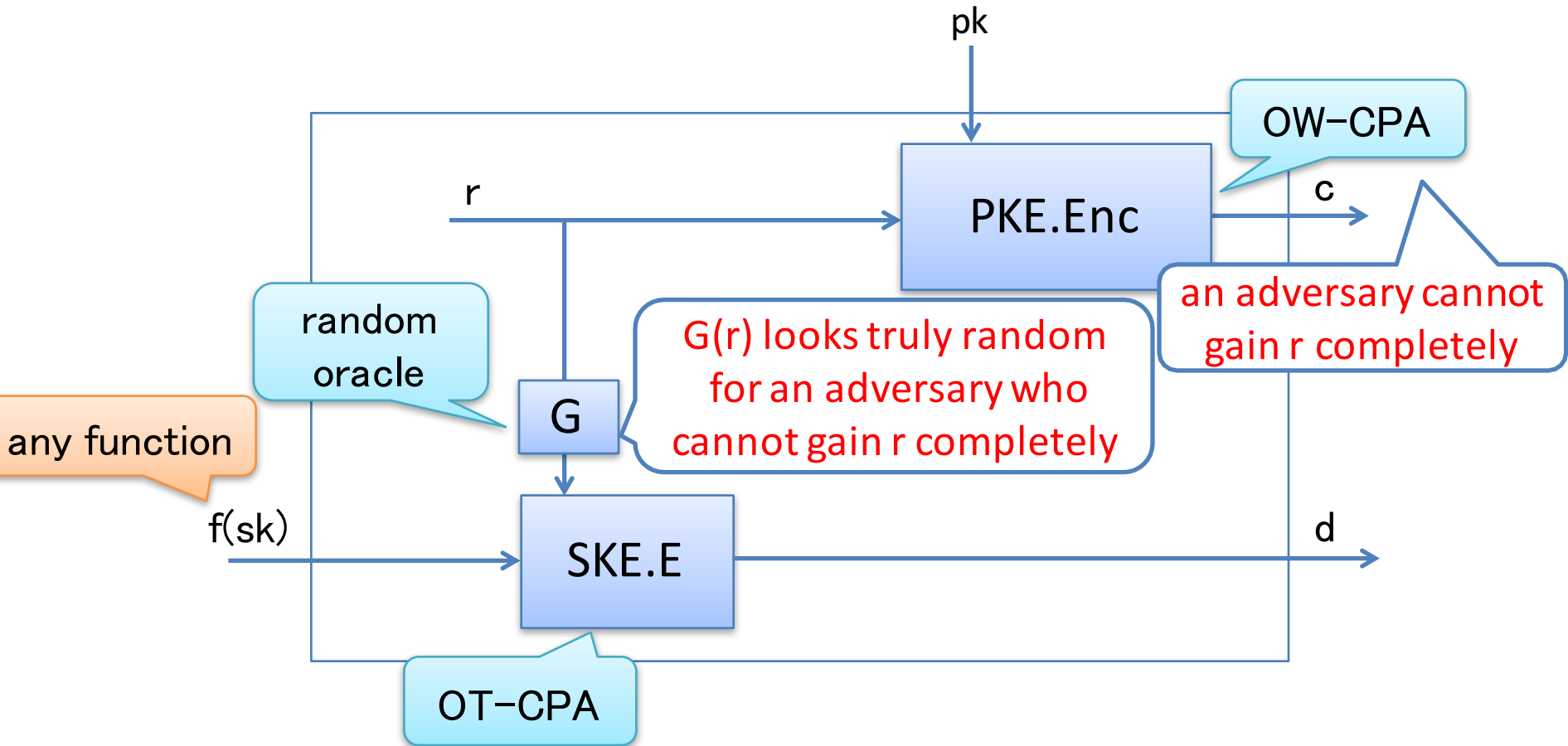


$$(c := \text{Enc}(pk, r), d := E(G(r), m))$$

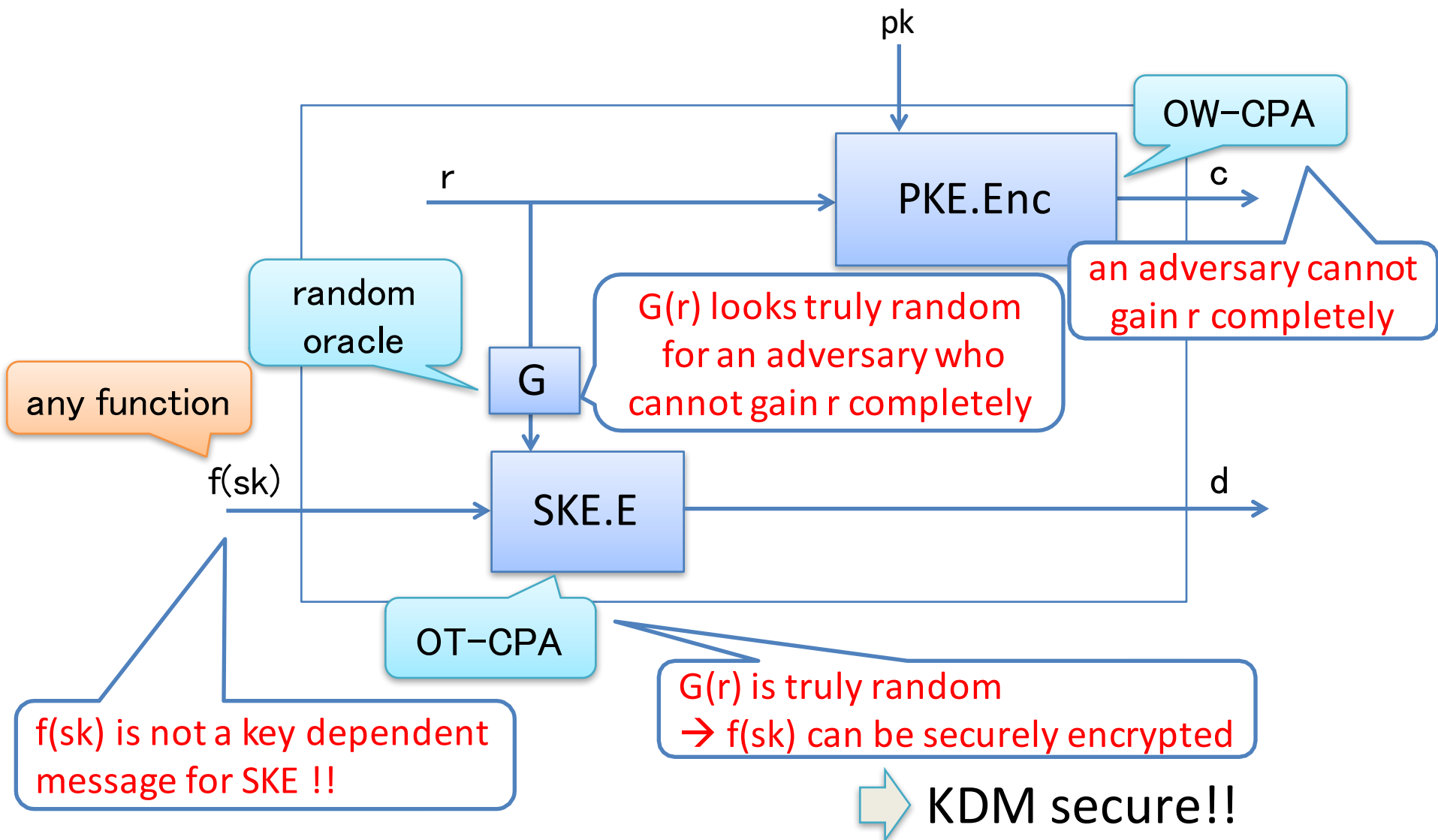
Intuition



Intuition



Intuition



Random oracle access of KDM functions

- ◆ We have to allow
a KDM function to access to random oracles

captures more
widely situations

$$(\text{Enc}(pk, r), E(G(r), f^G(sk)))$$

There is a problem:



An adversary can get an encryption of
past keys for the SKE scheme

This makes difficult to complete the formal proof...

To complete the formal proof

◆ [DS14] studied KDM security of hybrid encryption in RO model



overcame the problem by using



[divide the random oracle
(use *deferred analysis*)

+

replace the random oracle
with PRF

◆ security bound has the PRF term...

◆ we cannot use it
since FO2 includes [2 random oracles
smoothness of PKE

To complete the formal proof

◆ [DS14] studied KDM security of hybrid encryption in RO model



➔ overcame the problem by using

divide the random oracle
(use *deferred analysis*)

+

~~replace the random oracle
with PRF~~

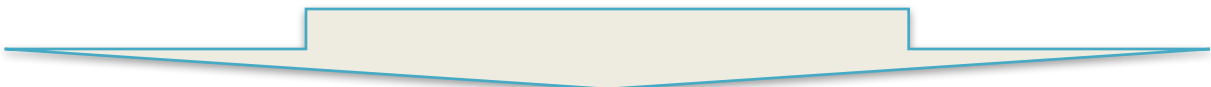
◆ security bound has the PRF term...

◆ we cannot use it

since FO2 includes $\left[\begin{array}{l} 2 \text{ random oracles} \\ \text{smoothness of PKE} \end{array} \right.$

We only use this by

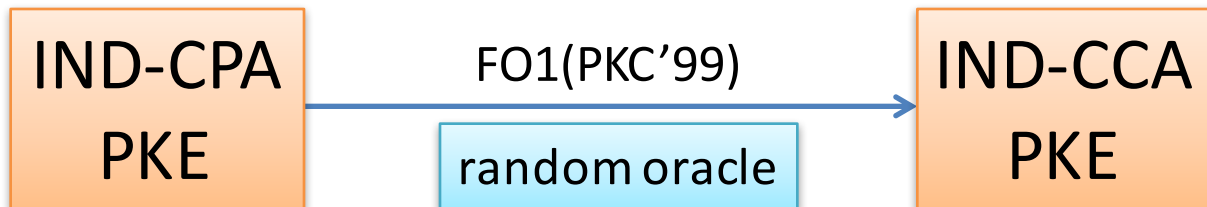
devising the order of the hybrid games
defining bad events carefully



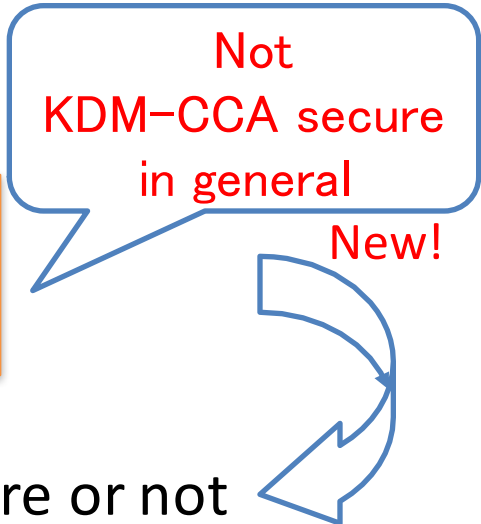
We prove the KDM-CCA security of FO2 with Simple & Natural proof

Conclusion

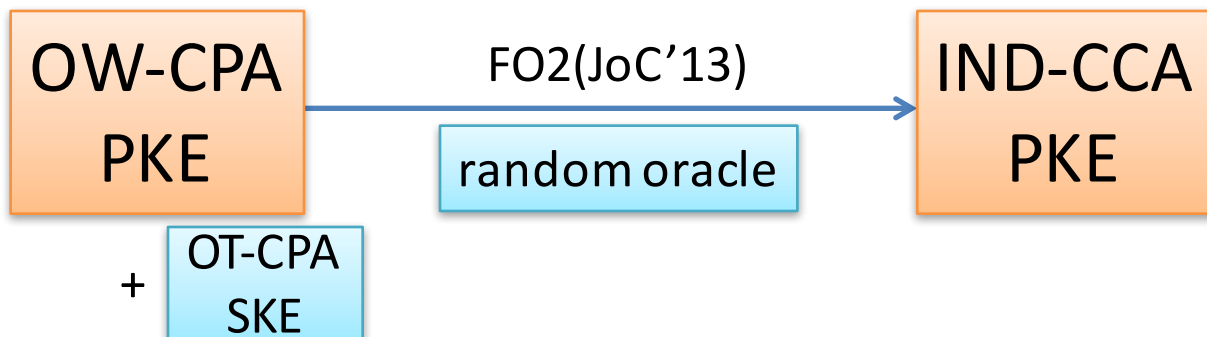
Fujisaki-Okamoto construction



Not
KDM-CCA secure
in general
New!



it is open whether EPOC-1 is KDM-CCA secure or not



KDM-CCA secure
in general
New!



EPOC-2 is KDM-CCA secure !

Reference

- *M. Backes, M. Durmuth, and D. Unruh. OAEP is secure under key-dependent messages. ASIACRYPT 2008, LNCS 5350, pp. 506–523. 2008.*
- *M. Bellare and P. Rogaway. Optimal asymmetric encryption. EUROCRYPT 1994, LNCS 950, pp. 92–111. 1994.*
- *J. Black, P. Rogaway, and T. Shrimpton. Encryption-scheme security in the presence of key-dependent messages. SAC 2002, LNCS 2595, pp. 62–75. 2002.*
- *G. Davies and M. Stam. KDM security in the hybrid framework. CT-RSA2014, LNCS8366, pp. 461–480. 2014.*
- *E. Fujisaki and T. Okamoto. How to enhance the security of public-key encryption at minimum cost. PKC 1999, LNCS 1560, pp. 53–68. 1999.*
- *E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. J. Cryptology, 26(1):80–101, 2013.*