Toward Fine-Grained Blackbox Separations Between Semantic and Circular-Security Notions

Mohammad Hajiabadi (University College London)
Bruce Kapron (University of Victoria)

May 3, 2017

1-Circular security

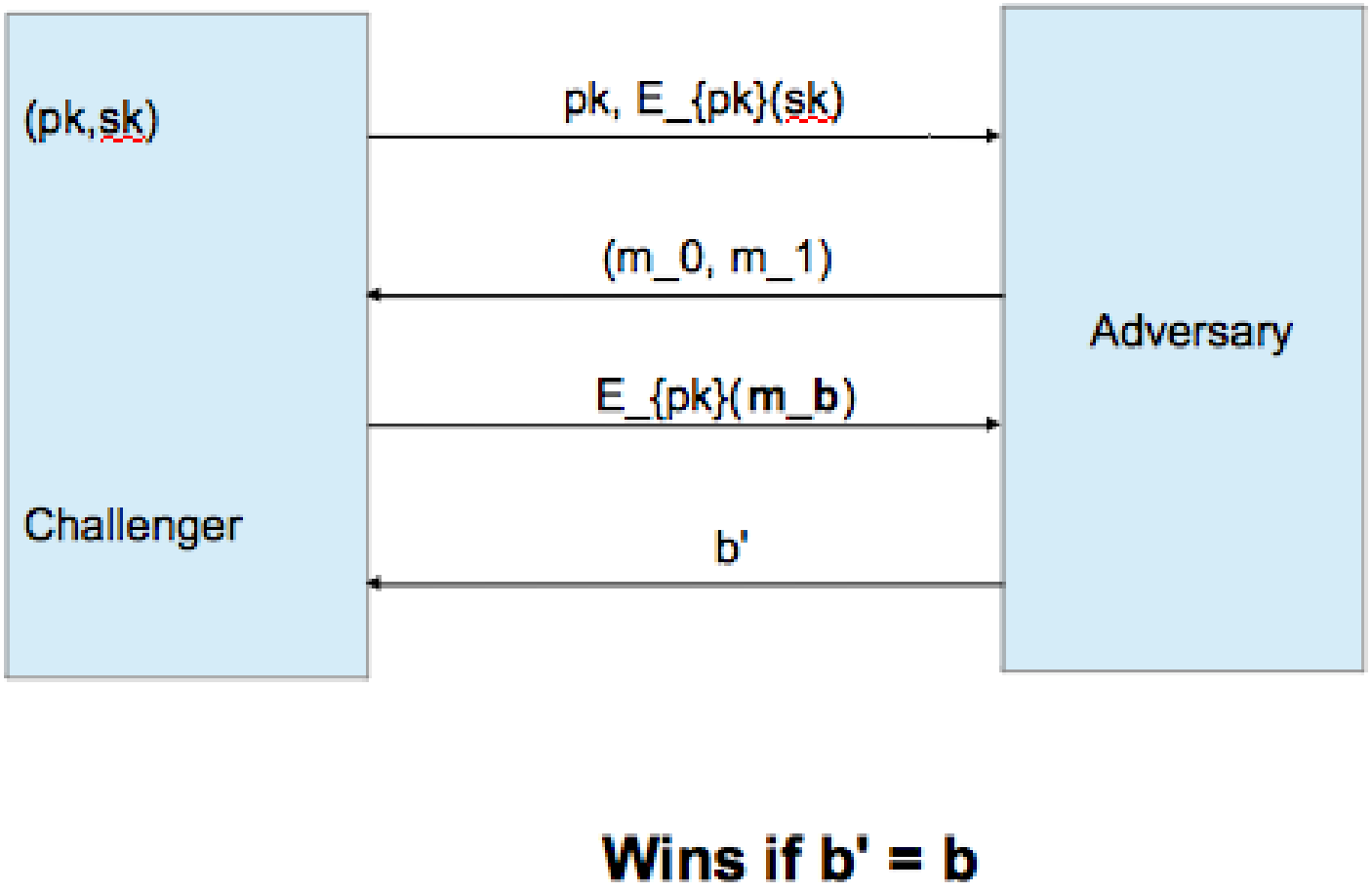


Figure: 1-circular security

Versions of 1-circular

Two extreme cases:

- **Extreme 1: bit circular security:** *sk* is encrypted bit-by-bit
- **Intermediate:** *sk* encrypted block-by-block
- **Extreme 2: full-length circular security:** *sk* is encrypted as a whole.

t-Circular security

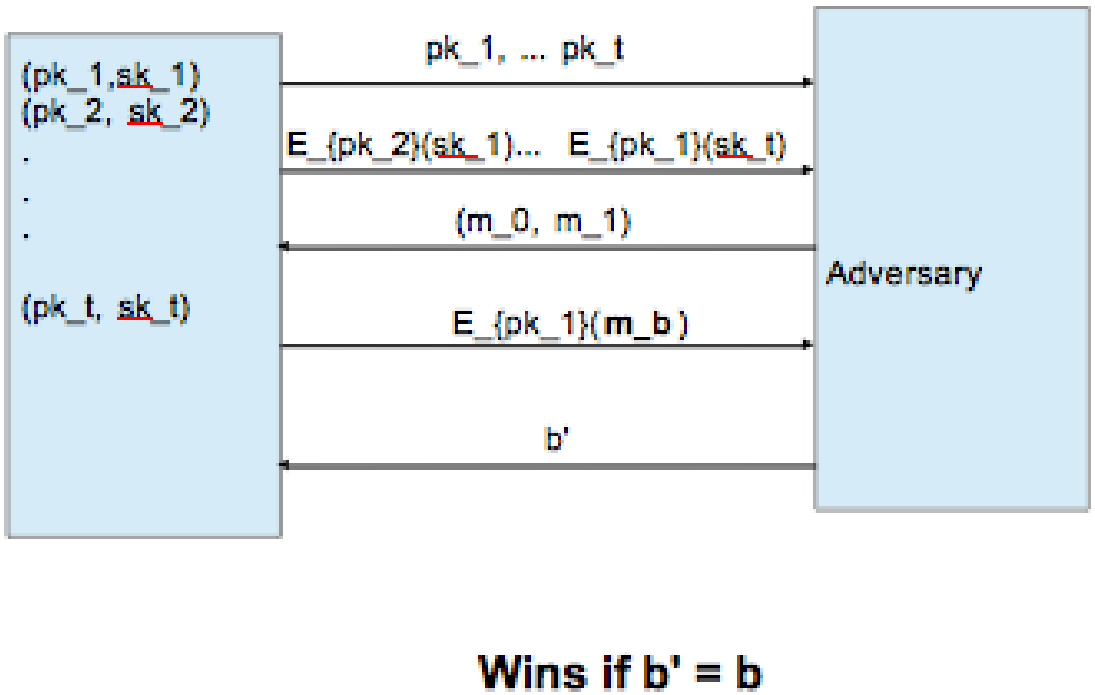


Figure: t-circular security

t-circular security from minimal CPA security?

t-circular security from minimal CPA security?
$t = 1$: easy (full-length case)

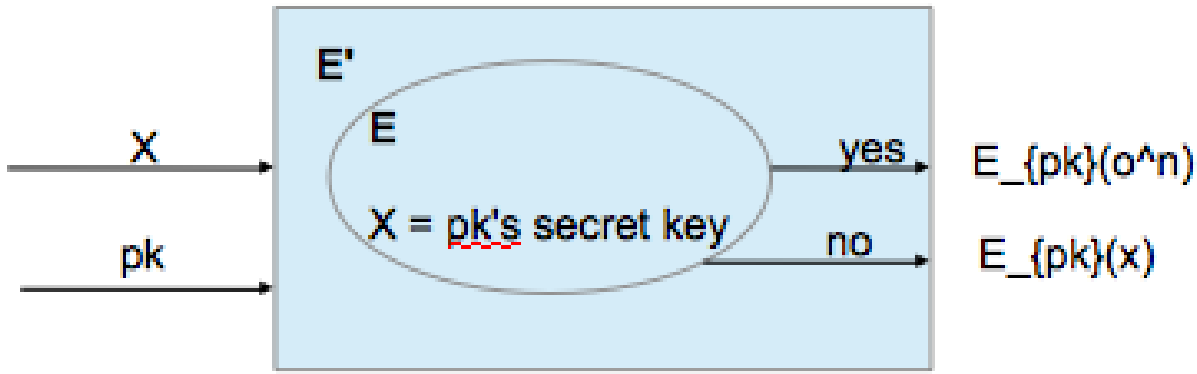


Figure: 1-circular construct

G: 1-1 ✓

t-circular security from minimal CPA security?
$t = 1$: easy (full-length case)

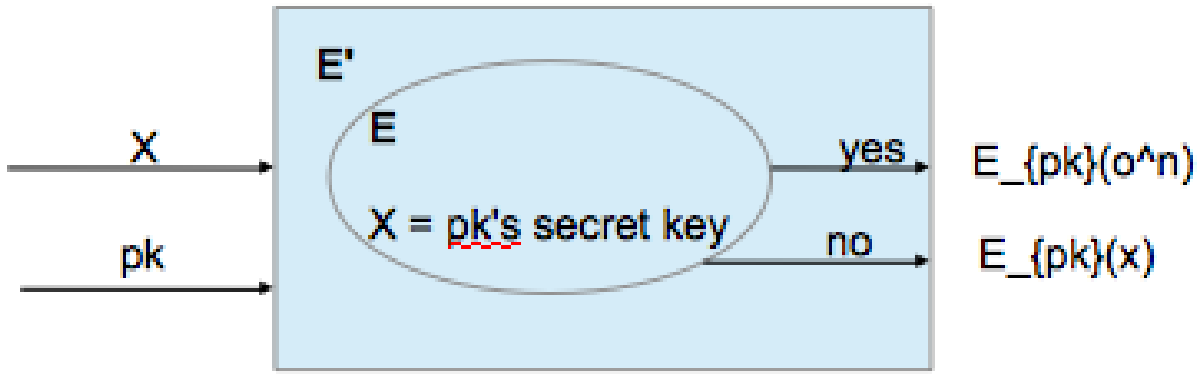


Figure: 1-circular construct

G: 1-1 ✓

- Hard to extend to bit case.
- Hard to extend to $t > 1$.

Background

- Applications: FHE constructions
- **Positive results** Circular-secure schemes under DDH, LWE, QR/DCR etc (BHHO08,ACPS'09,BG10)
  - for multiple-key case: t-circular: $E_{pk_1}(sk_2), \ldots, E_{pk_t}(sk_1)$ ☺
- **Negative results**
  - NO BB reduction can prove any CPA bit-by-bit PKE is also circular secure (Rothblum'13)
  - Concrete CPA-secure schemes that are circular insecure (Koppula-Waters'16, Alamati-Peikert'16, etc.)
  - TDP $\not\rightarrow^{\mathsf{BB}}$ full-KDM PKE (Haitner-Holenstein'09).

Our results

Lingering questions:

1. 1-circular secure bit encryption from CPA encryption?
2. t-circular secure encryption (bit or full length) from CPA encryption? ($t > 1$)

Our results

Lingering questions:

1. 1-circular secure bit encryption from CPA encryption?
2. t-circular secure encryption (bit or full length) from CPA encryption? ($t > 1$)

We address (1) and (2) for seed-circular security.

- encrypting the seed of G.
- Seed circular encryption $\Rightarrow$ circular encryption

Our results

Lingering questions:

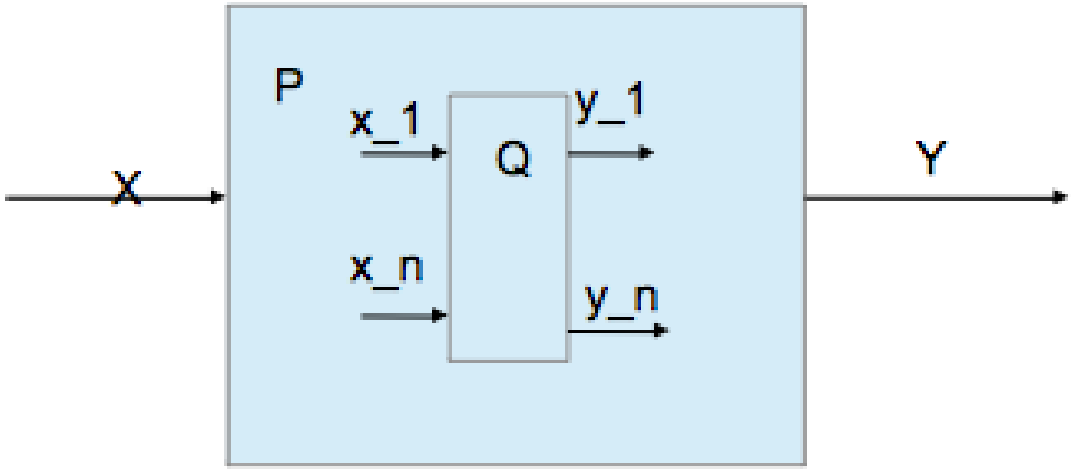
1. 1-circular secure bit encryption from CPA encryption?
2. t-circular secure encryption (bit or full length) from CPA encryption? ($t > 1$)

We address (1) and (2) for seed-circular security.

- encrypting the seed of G.
- Seed circular encryption $\Rightarrow$ circular encryption
- CPA encryption $\overset{blackbox}{\not\longrightarrow}$ 1-seed-circular bit encryption
  - CPA encryption $\overset{blackbox}{\not\longrightarrow}$ $(c \log n)$-seed-circular bit encryption
- t-seed circular bit encryption $\overset{blackbox}{\not\longrightarrow}$ $(t+1)$-full-length seed-circular encryption

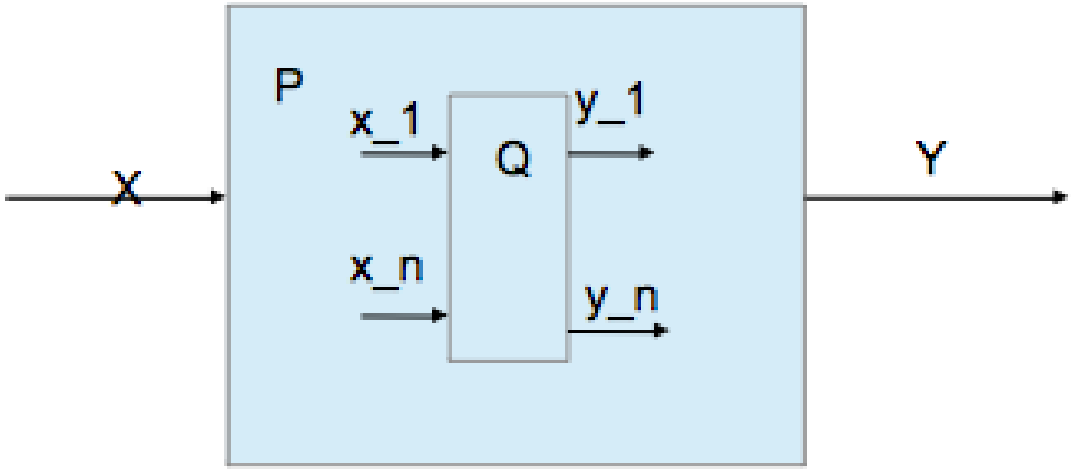
Fully blackbox reductions

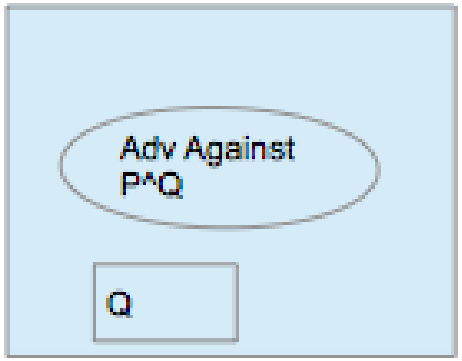
$Q \Rightarrow^{FBB} P$: construction and security proof



Fully blackbox reductions

$Q \Rightarrow^{FBB} P$: construction and security proof





Breaks Q

Two Templates for BB separation proofs

$Q \not\Rightarrow^{FBB} P$

Two Templates for BB separation proofs

$Q \not\Rightarrow^{FBB} P$

- Give an ideal oracle O for Q;
- Any G^O for P can be broken by small number of queries to O.

Used in [IR'89: OWP $\not\Rightarrow^{FBB}$ KA], [BPRVW'08: TDP $\not\Rightarrow$ IBE], etc

Two Templates for BB separation proofs

$Q \not\Rightarrow^{FBB} P$

- Give an ideal oracle O for Q;
- Any G^O for P can be broken by small number of queries to O.

Used in [IR'89: OWP $\not\Rightarrow^{FBB}$ KA], [BPRVW'08: TDP $\not\Rightarrow$ IBE], etc

Second template: Give an ideal oracle O for Q plus some weakening component W:

- No $\mathcal{A}^{O,W}$ can break Q security of O
- Any G^O for P can be broken by some $\mathcal{B}^{O,W}$

Used in [Simon'98: OWP $\not\Rightarrow$ CRHF], [HR'04 secret-coin CRHF $\not\Rightarrow$ public-coin CRHF], [GMM'07 CPA PKE $\not\Rightarrow^{shielding}$ CCA PKE], etc

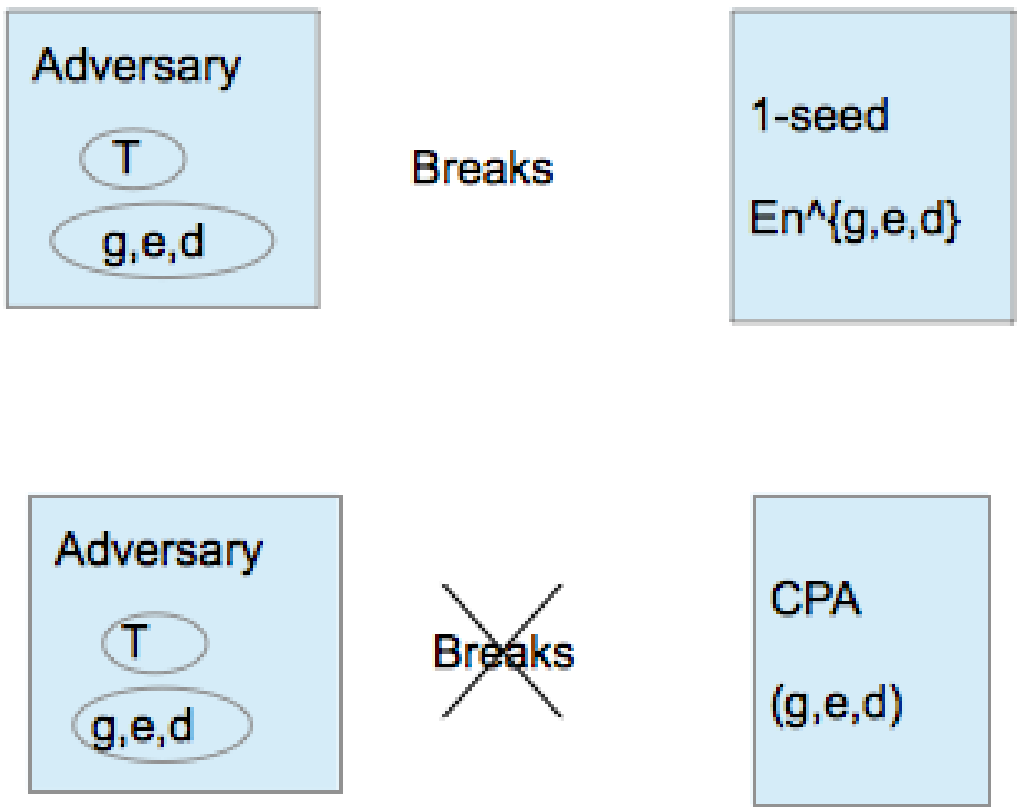
These templates do not work for our case.

Separation model [GMR'01]

CPA PKE $\not\Rightarrow^{FBB}$ 1-seed circular bit PKE

Fix $En = (Gen^{\circ}, Enc^{\circ}, Dec^{\circ})$

Define T in such a way that for random (g, e, d):



Details of oracles

- $\mathbf{O}_n$:
  - $\mathbf{g}_n : \{0,1\}^n \to \{0,1\}^{5n}$ random injective.
  - $\mathbf{e}_n : \{0,1\}^{5n} \times \{0,1\} \times \{0,1\}^n \to \{0,1\}^{7n}$ random injective
  - $\mathbf{d}_n : \{0,1\}^n \times \{0,1\}^{7n} \to \{0,1\} \cup \{\perp\}$ agrees with g and e.
- $\mathbf{u}_n : \{0,1\}^{5n} \times \{0,1\}^{7n} \to (\{0,1\} \times \{0,1\}^n) \cup \{\perp\}$ decrypting relative to public keys, returning also the randomness.
- $\mathbf{w}_n : \{0,1\}^{5n} \to \{\perp, \top\}$: public-key validity check.

Fix $(Gen^{g,e,d}, Enc^{g,e,d}, Dec^{g,e,d})$. **naive try** $T(PK, C_1, \ldots, C_n)$

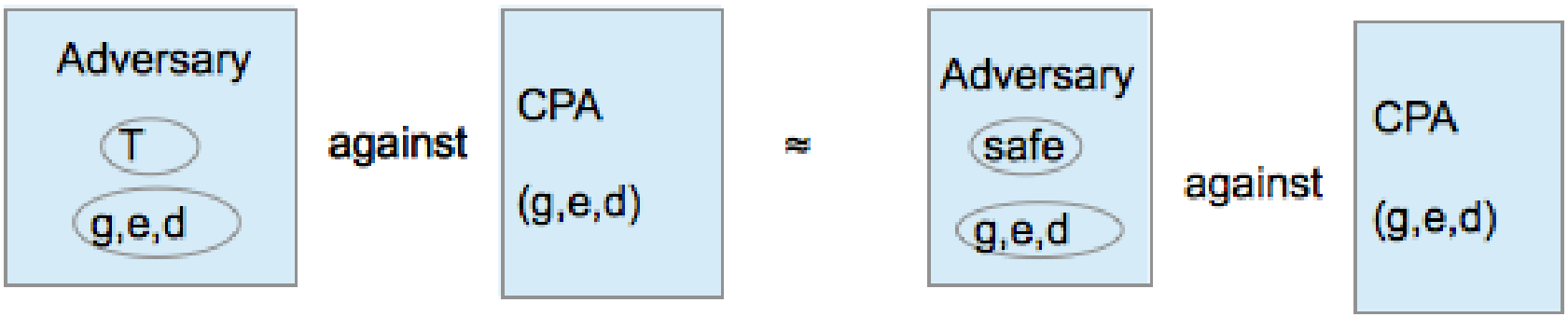
- Decrypt $(C_1, ..., C_n)$ relative to PK to get S.
- if $Gen^{g,e,d}(S) = (PK, *)$ return S

Fix $(Gen^{g,e,d}, Enc^{g,e,d}, Dec^{g,e,d})$. **naive try** $T(PK, C_1, \ldots, C_n)$

- Decrypt $(C_1, ..., C_n)$ relative to PK to get S.
- if $Gen^{g,e,d}(S) = (PK, *)$ return S

Several problems:

1. What if PK isn't valid?
2. How to simulate?

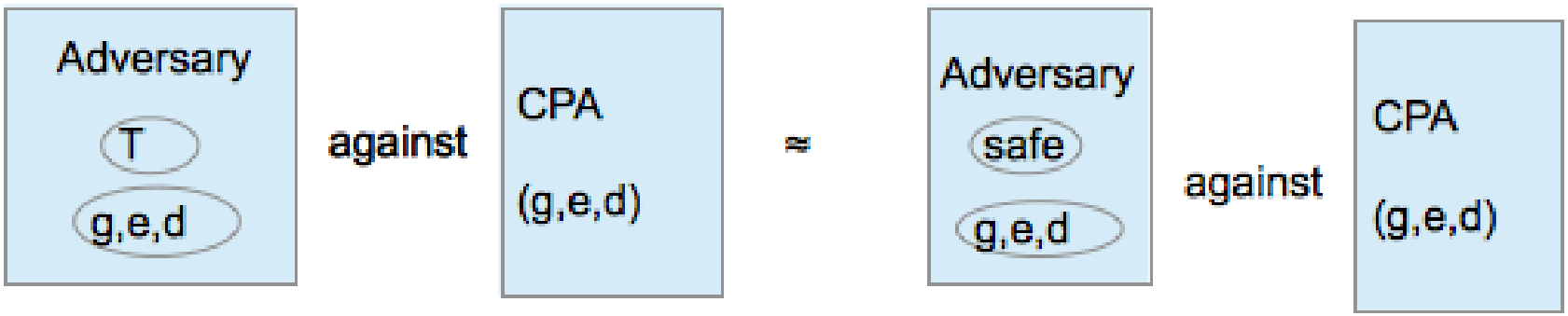


Fix $(Gen^{g,e,d}, Enc^{g,e,d}, Dec^{g,e,d})$. **naive try** $T(PK, C_1, \ldots, C_n)$

- Decrypt $(C_1, ..., C_n)$ relative to PK to get S.
- if $Gen^{g,e,d}(S) = (PK, *)$ return S

Several problems:

1. What if PK isn't valid?
2. How to simulate?



Solution to 1: T perform $Dec^{\widetilde{O}}(SK', C_1 \ldots C_n)$:

(A) $(PK, SK') \in Gen^{\widetilde{O}}$

(B) $\widetilde{O}$ close to $O = (g, e, d)$: w.h.p.

$Enc^{\mathbf{O}}(PK, b; R) = Enc^{\widetilde{\mathbf{O}}}(PK, b, R)$ for $b = 0, 1$.

implication: $(PK, SK) \leftarrow Gen(S)$, $(C_1, ..., C_n) \leftarrow Enc(PK, S) \Rightarrow$ $Dec^{\widetilde{O}}(SK', C_1 \ldots C_n) = S$.

One step of $\mathbf{T}$: CPA PKE $\not\Rightarrow^{FBB}$ circular bit PKE.

Type-1 case: (Gen^g, Enc^e, Dec^d). Let $O = (g, e, d)$ and $\mathbf{T}(PK, C_1 \ldots C_n)$ a query.

Goal: define $\widetilde{O} = (\widetilde{g}, \widetilde{e}, \widetilde{d})$ that is:

1. $(PK, SK') \in G^{\widetilde{\mathbf{O}}}$;
2. $Enc^{\mathbf{O}}(PK, b; R) = Enc^{\widetilde{\mathbf{O}}}(PK, b, R)$ for $b = 0, 1$.

One step of $\mathbf{T}$: CPA PKE $\not\Rightarrow^{FBB}$ circular bit PKE.

Type-1 case: (Gen^g, Enc^e, Dec^d). Let $O = (g, e, d)$ and $\mathbf{T}(PK, C_1 ... C_n)$ a query.

Goal: define $\widetilde{O} = (\widetilde{g}, \widetilde{e}, \widetilde{d})$ that is:

1. $(PK, SK') \in G^{\widetilde{\mathbf{O}}}$;
2. $Enc^{\mathbf{O}}(PK, b; R) = Enc^{\widetilde{\mathbf{O}}}(PK, b, R)$ for $b = 0, 1$.

Idea:

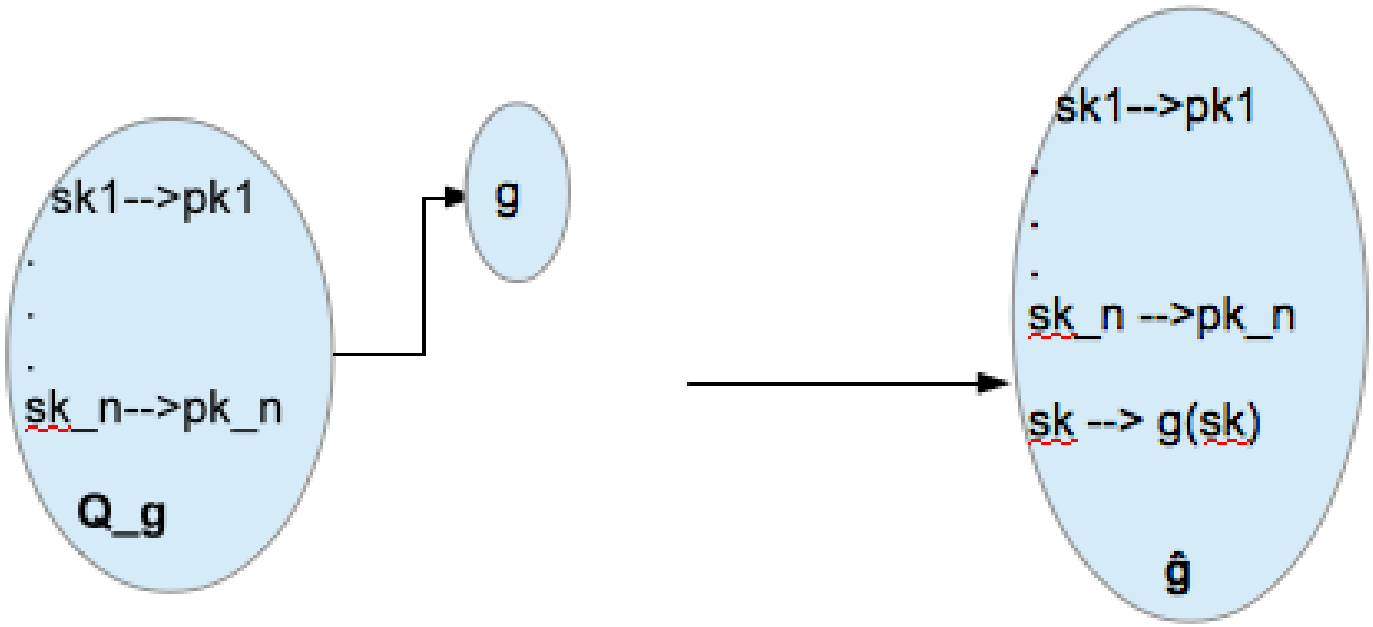
- Sample set of query/response pairs Q_g such that $(PK, *) \in Gen^{Q_g}$;
- $\widetilde{g}$: Super-impose $\mathrm{Q_g}$ on g .

$\widetilde{e} = e$

$\widetilde{d}$: will define later

Superimposing g queries

$(g, e, d) \Rightarrow^{Q_g} (\widetilde{g}, \widetilde{e}, \widetilde{d})$, where Q_g: g-type query/answer pairs



$$\widetilde{e} = e$$

$$\widetilde{d}(sk, c) = \begin{cases} d(sk, c), & \text{if } sk \notin \{sk_1, \ldots, sk_n\} \\ u(pk_i, c), & \text{if } sk = sk_i \end{cases}$$

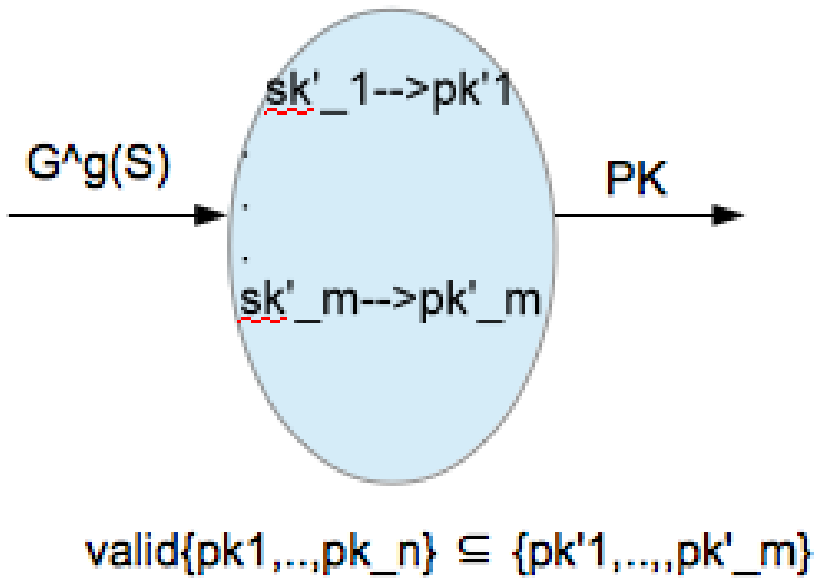
Simple case: (Gen^g, Enc^e, Dec^d). Let $O = (g, e, d)$ and $\mathbf{T}(PK, C_1 \ldots C_n)$ a query.
High-level operations of $\mathbf{T}$:

(A) Sample set of query/response pairs Q_g such that $(PK, SK') \in G^{Q_g}$;

(B) Superimpose $\mathrm{Q_g} = \{sk_1 \rightarrow pk_1, \ldots, sk_m \rightarrow pk_m\}$ on O to get $\widetilde{O}$;

(C) $S = D^{\widetilde{O}}(SK', C_1 \ldots C_n)$

(D) **Release S subject to check:** Return S if



Main Theorems

Theorem
(Breaking 1-seed circularity of (G^g, E^e, D^d))

$$\Pr_{\mathbf{Env},\mathbf{T}}[\mathbf{T}(PK, C_1, \ldots, C_n) = S] \geq 1 - \frac{1}{2^{2n}}, \tag{1}$$

for random (g, e, d), $S \leftarrow \{0,1\}^n$, $(PK, SK) = G^g(S)$, $(C_1, \ldots, C_n) \leftarrow E^e(PK, S)$.

Theorem
(Not Breaking CPA of (g, e, d))
$\mathcal{A}$ *at most* $2^{n/8}$ *queries:*

$$\Pr_{\mathbf{O},\mathbf{T},b,pk,c}[\mathcal{A}^{\mathbf{O},\mathbf{T}}(1^n, pk, c) = b] \leq \frac{1}{2} + \frac{1}{2^{n/4}}, \tag{2}$$

$\mathbf{O} \leftarrow \Psi$, $b \leftarrow \{0,1\}$, $sk \leftarrow \{0,1\}^n$, $pk = \mathbf{g}(sk)$ *and* $c \leftarrow \mathbf{e}(pk, b)$.

Theorem

(Breaking 1-seed circularity of (G^g, E^e, D^d))

$$\Pr_{\mathbf{Env},\mathbf{T}}[\mathbf{T}(PK, C_1, \ldots, C_n) = S] \geq 1 - \frac{1}{2^{2n}}, \tag{3}$$

for random (g, e, d), $S \leftarrow \{0,1\}^n$, $(PK, SK) = G^g(S)$, $(C_1, \ldots, C_n) \leftarrow E^e(PK, S)$.

Proof main idea: If $T(PK, C_1, ..., C_n) \neq S \Rightarrow$ **check** in Step (D) didn't hold $\Rightarrow$ we can **forge** some $pk \in \{0,1\}^{3n}$ w/o calling $g^{-1}(pk)$

$$g : \{0,1\}^n \rightarrow \{0,1\}^{3n}$$

Theorem

(Not Breaking CPA of (g, e, d))

$\mathcal{A}$ at most $2^{n/8}$ queries:

$$\Pr_{\mathbf{O},\mathbf{T},b,pk,c}[\mathcal{A}^{\mathbf{O},\mathbf{T}}(1^n, pk, c) = b] \leq \frac{1}{2} + \frac{1}{2^{n/4}}, \tag{4}$$

$\mathbf{O} \leftarrow \Psi$, $b \leftarrow \{0,1\}$, $sk \leftarrow \{0,1\}^n$, $pk = \mathbf{g}(sk)$ *and* $c \leftarrow \mathbf{e}(pk, b)$.

Proof main idea: $\mathcal{A}^{\mathbf{O},\mathbf{T}}(1^n, pk, c)$ can be simulated by $\mathcal{B}^{\mathbf{O},u^*,w}$, where $u^*(pk, c) = \perp$.

- $u\colon \{0,1\}^{5n} \times \{0,1\}^{7n} \to (\{0,1\} \times \{0,1\}^n) \cup \{\perp\}$ decrypting relative to public keys, returning also the randomness.
- $w\colon \{0,1\}^{5n} \to \{\perp, \top\}$: public-key validity check.

General case

Main difficulties:

- The idea of superimposing for other types of queries
- Making $\widetilde{O}$ close to O is much more difficult.
  - Requiring to learn heavy queries during key generation.

t-seed circular $\not\Rightarrow$ $(t+1)$-seed circular

$t = 1$: 1-seed circularity cannot be extended to 2-seed circularity. We define T that breaks 1-seed circularity of (g, e, d) but not 2-seed circularity of $\mathcal{E}^{g,e,d}$. Main ideas $T(PK_1, PK_2, C_1, C_2)$:

- We learn likely public keys pk embedded in a random execution $G^g(1^n)$.
- Define $\widetilde{O}$ to decrypt C_1 and C_2 to get S_1 and S_2.
- T makes sure the set of un-learned public keys embedded in S_1 and S_2 be disjoint.

Conclusions and Open Problems

Summary of results:

- CPA encryption $\overset{blackbox}{\not\longrightarrow}$ 1-seed-circular bit encryption
  - CPA encryption $\overset{blackbox}{\not\longrightarrow}$ $(c \log n)$-seed-circular bit encryption
- t-seed circular bit encryption $\overset{blackbox}{\not\longrightarrow}$ $(t+1)$-full-length seed-circular encryption

Open problems:

1. Separating circular from CPA PKE.
2. FHE $\Rightarrow$ circular PKE? NOTE: non-blackbox techniques