TOSHIBA
Leading Innovation

Blanchetフレームワークにおける CDH仮定の定式化方針について

○ 花谷 嘉一 †
國分 雄一 ‡
米山 一樹 ‡
太田 和夫 ‡

† (株) 東芝 研究開発センター
‡ 電気通信大学

背景

安全性証明の手間の軽減や，証明中のミスを防ぐために
形式的検証技術が注目されている.

Blanchetのフレームワークはその一種.

証明に必要な書き換え規則の生成には
手間がかかるし，ミスが混入する恐れがある.

しかし，フレームワークの性質上，絶対に 書き換え規則は必要.

一回だけ頑張って作っておき，以降 それを使い回せるなら
なんとか 我慢できそう.

使い回す機会が多いと思われる，
計算量的仮定の定式化方針を探ろう.

背景

計算量的仮定の定式化は，できればやりたくない・・・

The design of such equivalences can be delicate,

but this is a one-time effort: the same equivalence can be reused for proofs that rely on the same assumption. [BP06]

Blanchetの定式化した 一方向性置換で証明できるもの.

FDH署名,PFDH署名の**UF-CMA**
[BR93]の公開鍵暗号の**IND-CPA**, **IND-CCA**

確かに，使いまわしできてるみたい・・・

ただ，使い回しがきく理由について明確に議論されていない.
CDH仮定も定式化さえすれば使い回せるのかな？

本日の内容

- **Blanchetフレームワークのための計算量的仮定の定式化**
  汎用性の高い計算量的仮定の定式化を行うためには、
  どんな方針で定式化すればいいのか？

4通りの安全性

4通りの定式化をした
CDH仮定

安全性 / CDH仮定	1	2	3	4
1				
2		?		
3				
4				

CryptoVerifを用いて検証を実行
それぞれ証明できる安全性を調べる.

結果: より強力な能動的攻撃モデルを採用して定式化すると,
汎用性が高い.

目次

- 計算量的仮定を書き換え規則で表現する手順

- CDH仮定の定式化方針 ・・・ 4通り
- 評価する安全性 ・・・ 4通り
- CDH仮定による証明結果
- まとめ

計算量的仮定を書き換え規則で表現する手順

普通の仮定

問題

答え

正しく答えるのは難しい.

計算量的仮定の書き換え規則

問題

解きやすそうな問題を選ぶ.
解くためのヒントを得る.

答え

計算量的仮定の下での，能動的攻撃による差

A ⟺ A’

- 書き換えの形を考える. ⇒ 証明できるかどうかに影響
- 観測等価性を評価する. ⇒ 証明結果の正しさに影響

計算量的仮定の定式化には，手間がかかる！

CDH仮定の定式化

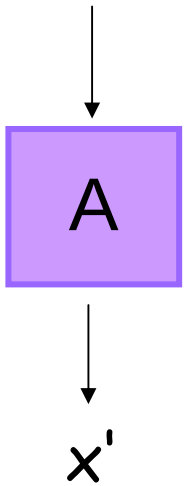
落とし戸付一方向性置換

普通のモデル

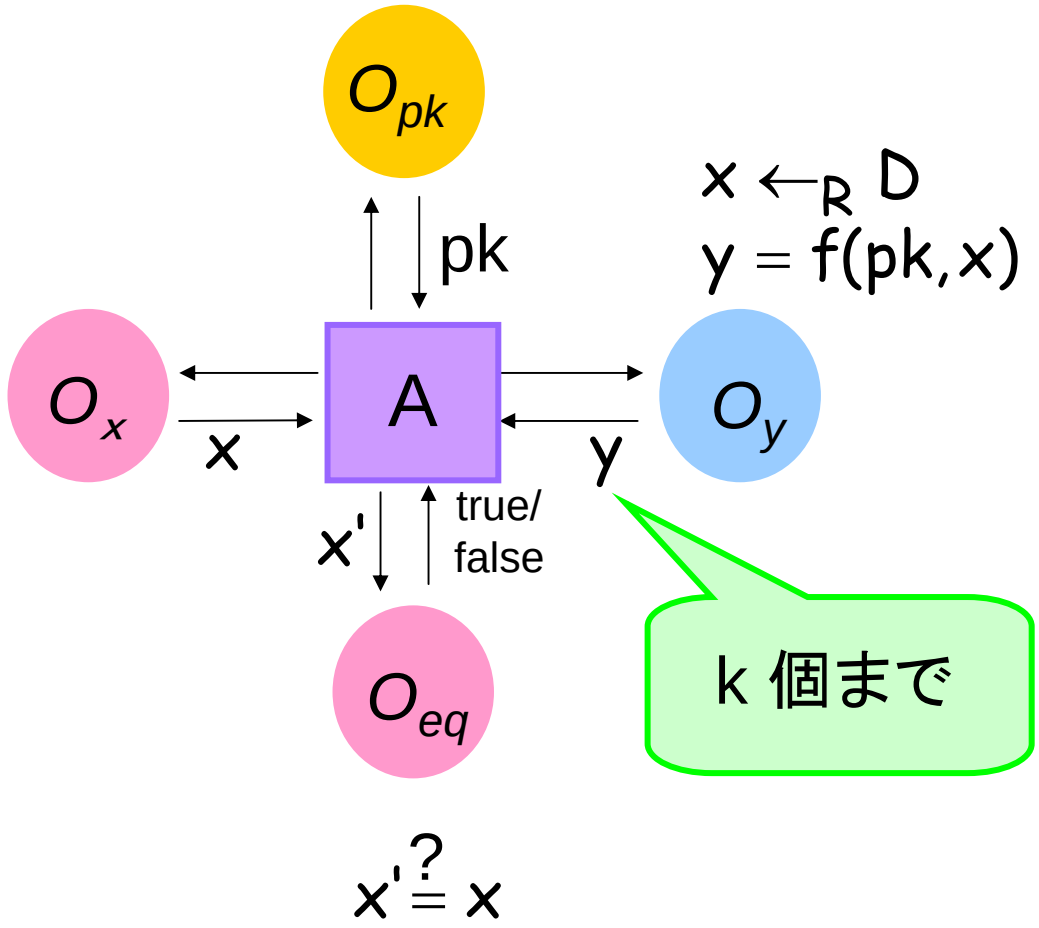
$x \leftarrow_R D$

$y = f(pk, x)$

$pk,\ y = f(pk, x)$



定式化しているモデル

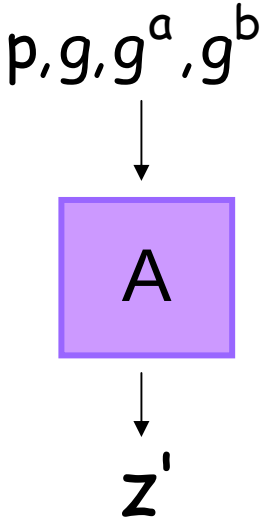


計算 Diffie-Hellman 仮定

普通のモデル

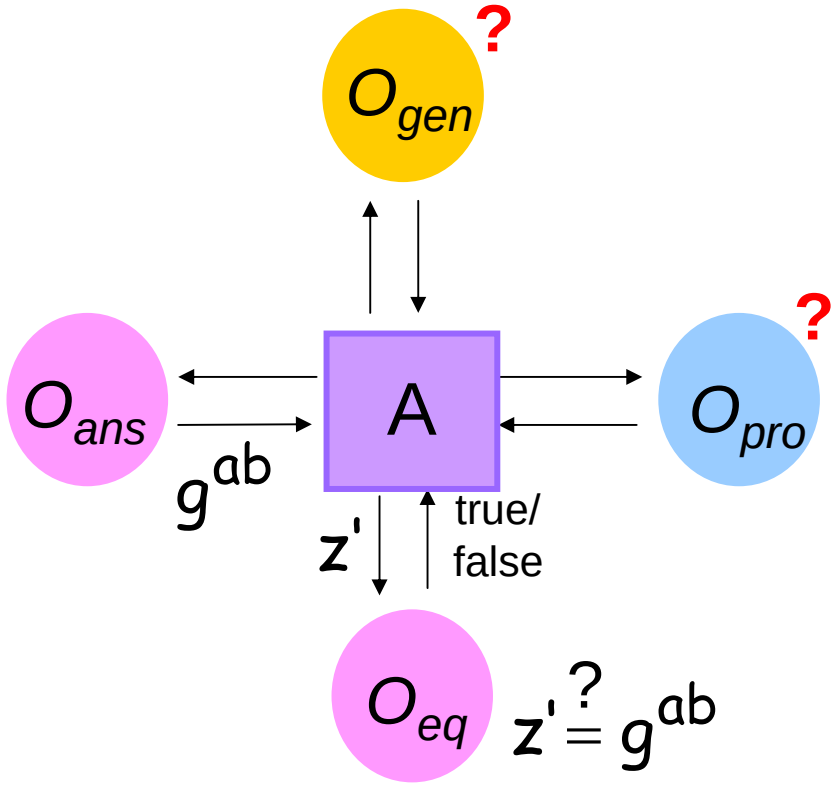
$(\mathfrak{p}, g) \leftarrow \mathrm{Ggen}(r)$

$(a, b) \xleftarrow{R} [1, |G_{\mathfrak{p}}|]^2$



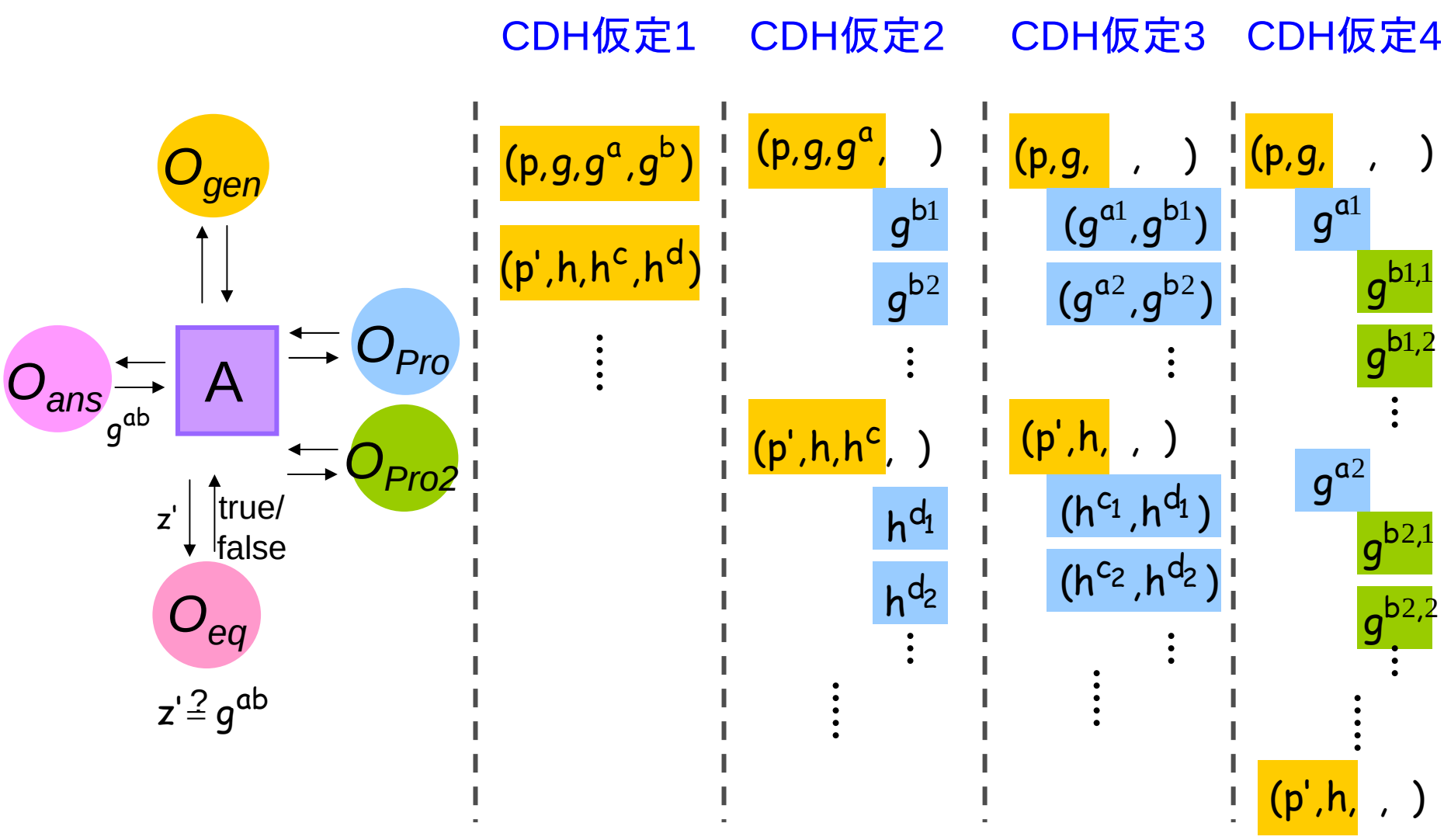
時間t 以内では，いかなるAで
あっても　$z' = g^{ab}$　となる
確率は ε 以以下.

定式化するモデル



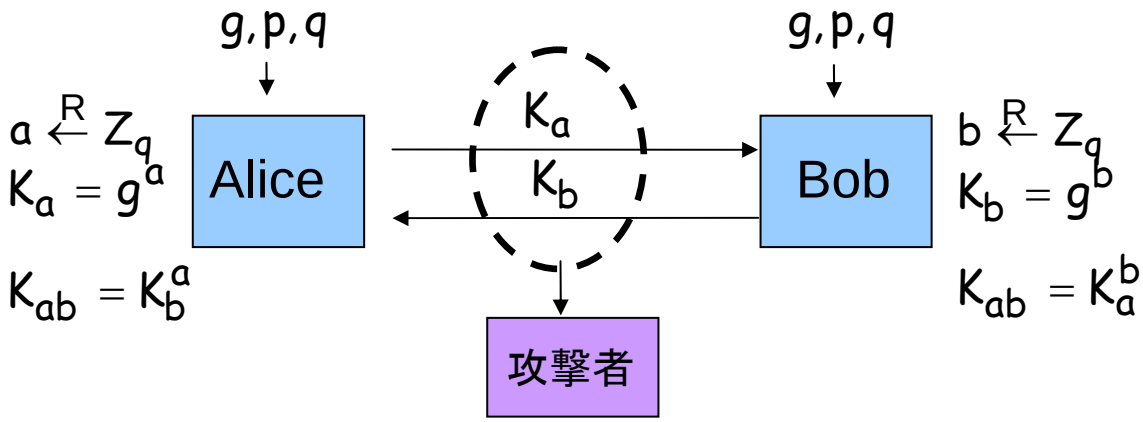
問題の4成分をどのように
与えればよいか？

4つの能動的攻撃モデル



検証する安全性

盗聴攻撃



共有鍵 K_{ab} を求める

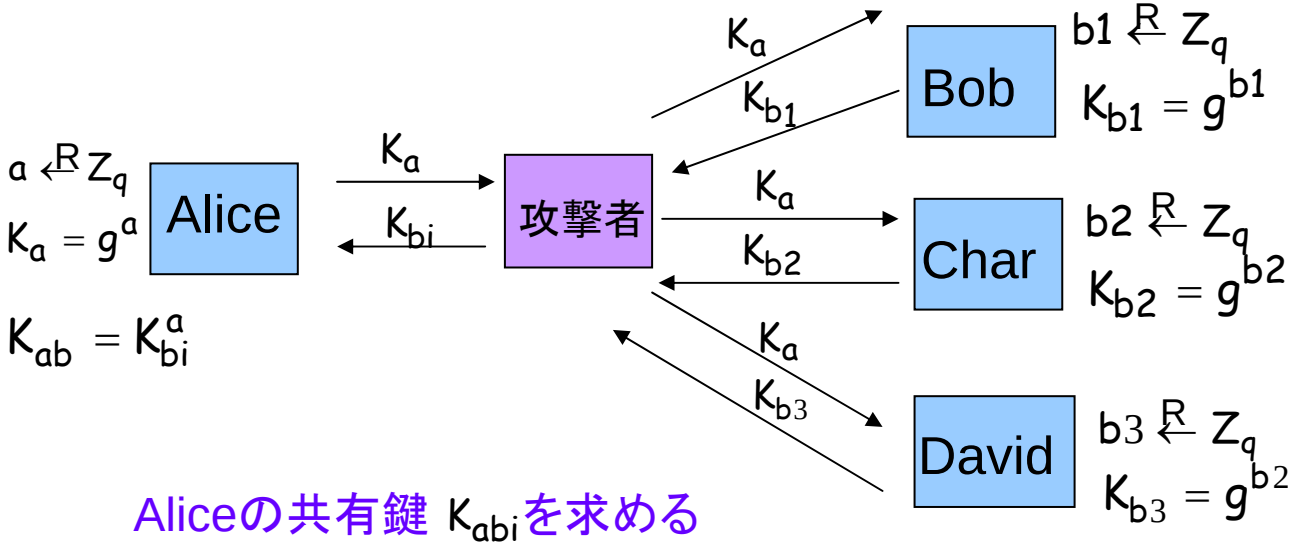
安全性1:

一回だけ鍵交換を実行.
2者間の共有鍵 K_{ab} を求めるのは難しい.

安全性2:

複数回 鍵交換を実行.
2者間の共有鍵 K_{ab} を1つ求めることすら難しい.

Unknown Key Share **攻撃** [CBH05]



Aliceの共有鍵 K_{abi}を求める

安全性3:

Aliceが**一回だけ**鍵交換を実行.
Aliceの共有鍵 K_{abi} を求めるのは難しい.

安全性4:

Aliceが**複数回** 鍵交換を実行.
Aliceの共有鍵 K_{abi} を1つ求めることすら難しい.

CryptoVerif を用いた安全性検証

実験デモ

CDH仮定 \ 安全性	1	2	3	4
1	○			
2				
3				
4	▲			

▲：CryptoVerifで証明する際，
“auto” では証明できなかった．
仮定の適用箇所を指定することで
証明可能．

結果

CDH仮定 \ 安全性	1	2	3	4
1	○	×	×	×
2	○	×	×	×
3	▲	▲	×	×
4	▲	▲	▲	▲

CDH仮定4が，最も多くの証明に適用できた.

強力な能動的攻撃モデルを採用して定式化すれば，
汎用性が高まることが確認できた.

まとめ

Blanchetフレームワークのために,
使いまわしのきく書き換え規則として
計算量的仮定を定式化する方針を探った.

方法
- CDH仮定を4通りのモデルで定式化
- CryptoVerifでDH鍵交換の4通りの安全性を検証

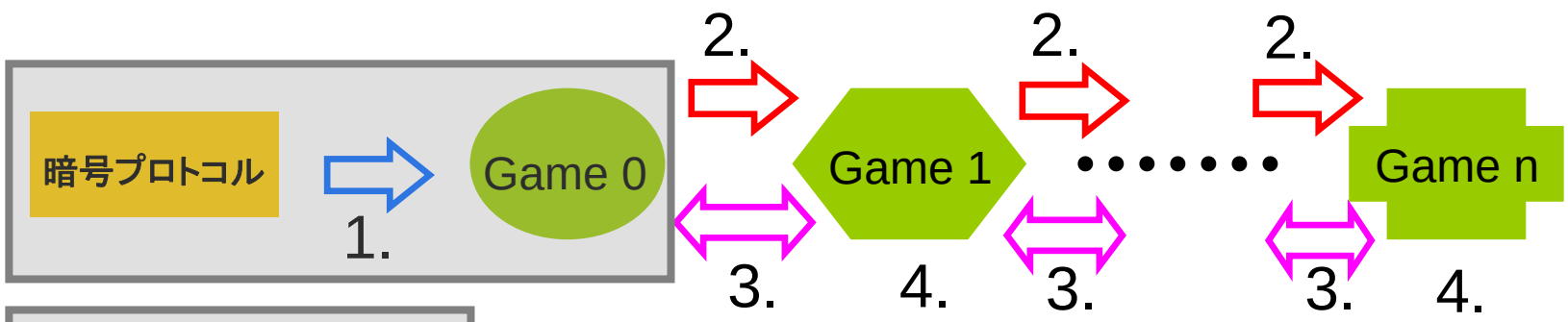
結果
- **定式化したCDH仮定が使用可能なことを確認**
- **できるだけ強力な能動的攻撃モデルを採用して定式化すれば, 使い回しが効く傾向がある.**

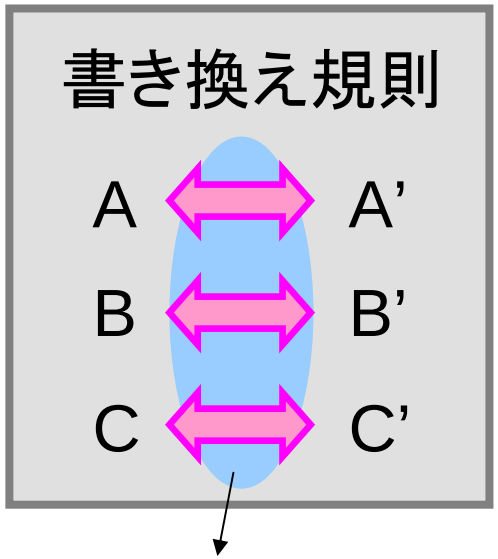
- **ただし, 強力な能動的攻撃モデルを採用した場合, 証明には人間の補助が必要となった.**


TOSHIBA
Leading Innovation

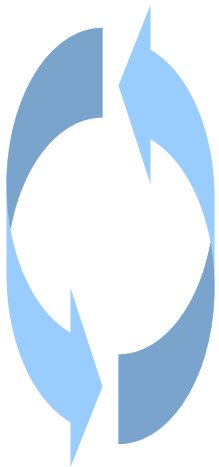
参考資料

Blanchetフレームワーク





観測等価性
置き換えにより生じる差



2. 書き換え規則が適用可能か判定
   適用できる場合は書き換え，
   新たなゲームを生成.

3. 適用した規則に与えられている
   観測等価性 を基に評価.

4. 安全性要件を満たすか判定.

安全な状態との差を評価.

フレームワークに基づく自動検証ツールCryptoVerif が公開されている.

証明結果

安全性1（CDH仮定1,2,3,4 の下で同じ証明結果となった. ）

RESULT Proved event bad ==> false with probability
PCDH(time + time(context for game 4))
RESULT time(context for game 4) = time(true)

安全性2（CDH仮定3,4 の下で同じ証明結果となった. ）

RESULT Proved event bad ==> false with probability
na * PCDH(-3. * time(f) + 3. * na * time(f) + time + time(context for game 4))
RESULT time(context for game 4) = time(true) * na

安全性3（CDH仮定4 でのみ証明できた. ）

RESULT Proved event bad ==> false with probability
nb * PCDH(2. * nb * time(f) + -2. * time(f) + time + time(context for game 4))
RESULT time(context for game 4) = time(true) * nb

安全性4（CDH仮定4 でのみ証明できた. ）

RESULT Proved event bad ==> false with probability
na * nb * PCDH(2. * na * nb * time(f) + na * time(f) + -3. * time(f) + time + time(context for game 4))
RESULT time(context for game 4) = time(true) * na * nb

CDH仮定1

$$
\begin{aligned}
&L : \mathbf{foreach}\ i_k \le n_k \mathbf{do}\ O_{gr} := r \xleftarrow{R} seed; O_{gA}() := a \xleftarrow{R} [1, |G_{\mathfrak{p}}|]; O_{gaB}() := b \xleftarrow{R} [1, |G_{\mathfrak{p}}|]; \mathbf{return};\\
&\quad (O_G := \mathbf{return}(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r))\\
&\quad |O_A() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a))\\
&\quad |O_{aB}() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), b))\\
&\quad |\mathbf{foreach}\ i_1 \le n_1\ \mathbf{do}\ O_{eq'}(z' : G_{\mathfrak{p}}) := \mathbf{return}(z' \stackrel{?}{=} f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))\\
&\quad |O_{ans}() := \mathbf{return}(f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))))\\
&\approx_{p^{CDH1}(t) = n_k \mathsf{Succ}^{CDH}_{\mathbb{G}}(t + (n_k - 1)t_{\mathsf{Ggen}} + 3(n_k - 1)t_f)}\\
&R : \mathbf{foreach}\ i_k \le n_k \mathbf{do}\ O_{gr} := r \xleftarrow{R} seed; O_{gA}() := a \xleftarrow{R} [1, |G_{\mathfrak{p}}|]; O_{gaB}() := b \xleftarrow{R} [1, |G_{\mathfrak{p}}|]; \mathbf{return};\\
&\quad (O_G := \mathbf{return}(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r))\\
&\quad |O_A() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a))\\
&\quad |O_{aB}() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), b))\\
&\quad |\mathbf{foreach}\ i_1 \le n_1 \mathbf{do}\ O_{eq'}(z' : G_{\mathfrak{p}}) :=\\
&\qquad \mathbf{if\ defined}(k)\ \mathbf{then\ return}(z' \stackrel{?}{=} f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))\\
&\qquad \mathbf{else\ return}(\mathsf{false})\\
&\quad |O_{ans}() := k \leftarrow \mathsf{mark}; \mathbf{return}(f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))))
\end{aligned}
$$

CDH仮定2

$$
\begin{aligned}
&L : \textbf{foreach } i_k \le n_k \textbf{do } O_{gr} := r \xleftarrow{R} seed; O_{gA}() := a \xleftarrow{R} [1, |G_{\mathrm{p}}|]; \textbf{return};\\
&\quad (O_G := \textbf{return}(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r))\\
&\quad |O_A() := \textbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a))\\
&\quad |\textbf{foreach } i_f \le n_{f2} \textbf{ do } O_{gaB}() := b \xleftarrow{R} [1, |G_{\mathrm{p}}|]; \textbf{return};\\
&\qquad (O_{aB}() := \textbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), b));\\
&\qquad |\textbf{foreach } i_1 \le n_1 \textbf{ do } O_{eq'}(z' : G_{\mathrm{p}}) := \textbf{return}(z' \stackrel{?}{=} f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))\\
&\qquad |O_{ans}() := \textbf{return}(f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))))\\
&\approx_{p^{CDH2}(t) = n_k n_{f2} \mathsf{Succ}^{CDH}_{\mathbb{G}}(t + (n_k - 1)t_{\mathsf{Ggen}} + (2n_k n_{f2} + n_k - 3)t_f)}\\
&R : \textbf{foreach } i_k \le n_k \textbf{do } O_{gr} := r \xleftarrow{R} seed; O_{gA}() := a \xleftarrow{R} [1, |G_{\mathrm{p}}|]; \textbf{return};\\
&\quad (O_G := \textbf{return}(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r))\\
&\quad |O_A() := \textbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a))\\
&\quad |\textbf{foreach } i_{f2} \le n_f \textbf{ do } O_{gaB}() := b \xleftarrow{R} [1, |G_{\mathrm{p}}|]; \textbf{return};\\
&\qquad (O_{aB}() := \textbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), b))\\
&\qquad |\textbf{foreach } i_1 \le n_1 \textbf{do } O_{eq'}(z' : G_{\mathrm{p}}) :=\\
&\qquad\quad \textbf{if defined}(k) \textbf{ then return}(z' \stackrel{?}{=} f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))\\
&\qquad\quad \textbf{else return}(\mathsf{false})\\
&\qquad |O_{ans}() := k \leftarrow \mathsf{mark}; \textbf{return}(f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))))
\end{aligned}
$$

CDH仮定3

$$
\begin{aligned}
&L : \mathbf{foreach}\ i_k \le n_k \mathbf{do}\ O_{gr}() := r \xleftarrow{R} seed; \mathbf{return};\\
&\quad (O_G() := \mathbf{return}(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r))\\
&\quad |\mathbf{foreach}\ i_f \le n_{f3}\ \mathbf{do}\ O_{gA}() := a \xleftarrow{R} [1, |G_{\mathbb{p}}|]; O_{gaB}() := b \xleftarrow{R} [1, |G_{\mathbb{p}}|]; \mathbf{return};\\
&\quad\quad (O_A() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a))\\
&\quad\quad |O_{aB}() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), b))\\
&\quad\quad |\mathbf{foreach}\ i_1 \le n_1\ \mathbf{do}\ O_{eq'}(z' : G_{\mathbb{p}}) := \mathbf{return}(z' \stackrel{?}{=} f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b));\\
&\quad\quad |O_{ans}() := \mathbf{return}(f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b)))).\\
&\approx_{p^{CDH3}(t) = n_k n_{f3} \mathsf{Succ}^{CDH}_{\mathbb{G}}(t + (n_k - 1)t_{\mathsf{Ggen}} + 3(n_k n_{f3} - 1)t_f)}\\
&R : \mathbf{foreach}\ i_k \le n_k \mathbf{do}\ O_{gr}() := r \xleftarrow{R} seed; \mathbf{return};\\
&\quad (O_G() := \mathbf{return}(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r))\\
&\quad (\mathbf{foreach}\ i_f \le n_{f3}\ \mathbf{do}\ O_{gA}() := a \xleftarrow{R} [1, |G_{\mathbb{p}}|]; O_{gaB}() := b \xleftarrow{R} [1, |G_{\mathbb{p}}|]; \mathbf{return};\\
&\quad\quad (O_A() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a))\\
&\quad\quad |O_{aB}() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), b))\\
&\quad\quad |\mathbf{foreach}\ i_1 \le n_1 \mathbf{do}\ O_{eq'}(z' : G_{\mathbb{p}}) :=\\
&\quad\quad\quad \mathbf{if}\ \mathbf{defined}(k)\ \mathbf{then}\ \mathbf{return}(z' \stackrel{?}{=} f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b));\\
&\quad\quad\quad \mathbf{else}\ \mathbf{return}(\mathsf{false})\\
&\quad\quad |O_{ans}() := k \leftarrow \mathsf{mark}; \mathbf{return}(f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b)))))
\end{aligned}
$$

CDH仮定4

L : **foreach** $i_k \le n_k$ **do** $O_{gr}() := r \xleftarrow{R} seed$; **return**;
$(O_G() := \mathbf{return}(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r))$;
|**foreach** $i_{fa} \le n_{f4a}$ **do** $O_{gA}() := a \xleftarrow{R} [1, |G_{\mathfrak{p}}|]$; **return**;
$(O_A() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a))$
|**foreach** $i_{fb} \le n_{f4b}$ **do** $O_{gaB}() := b \xleftarrow{R} [1, |G_{\mathfrak{p}}|]$; **return**;
$(O_{aB}() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), b))$
|**foreach** $i_1 \le n_1$ **do** $O_{eq'}(z' : G_{\mathfrak{p}}) := \mathbf{return}(z' \stackrel{?}{=} f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))$
$|O_{ans}() := \mathbf{return}(f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b)))))$

$\approx_{p^{CDH4}=n_k n_{fa} n_{fb} \mathsf{Succ}^{CDH}_{\mathbb{G}}(t+(n_k-1)t_{\mathsf{Ggen}}+(2n_k n_{f4a} n_{f4b}+n_k n_{f4a}-3)t_f)}$

R : **foreach** $i_k \le n_k$ **do** $O_{gr}() := r \xleftarrow{R} seed$; **return**;
$(O_G() := \mathbf{return}(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r))$
|**foreach** $i_{f4a} \le n_{fa}$ **do** $O_{gA}() := a \xleftarrow{R} [1, |G_{\mathfrak{p}}|]$; **return**;
$(O_A() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a))$
|**foreach** $i_{f4b} \le n_{fab}$ **do** $O_{gaB}() := b \xleftarrow{R} [1, |G_{\mathfrak{p}}|]$; **return**;
$(O_{aB}() := \mathbf{return}(f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), b))$
|**foreach** $i_1 \le n_1$ **do** $O_{eq'}(z' : G_{\mathfrak{p}}) :=$
if defined(k) **then return**$(z' \stackrel{?}{=} f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b))$
else return(false)
$|O_{ans}() := k \leftarrow \mathsf{mark}$; **return**$(f(\mathsf{Ggen1}(r), f(\mathsf{Ggen1}(r), \mathsf{Ggen2}(r), a), b)))))$