Poly-Many Hardcore Bits for Any One-Way Function and a Framework for Differing-Inputs Obfuscation

Mihir Bellare (University of California, San Diego)

Igors Stepanovs (University of California, San Diego)

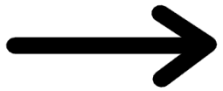
Stefano Tessaro (University of California, Santa Barbara)

ASIACRYPT 2014

December 10, 2014

Classical Problem

Extract poly-many hardcore bits from any one-way function

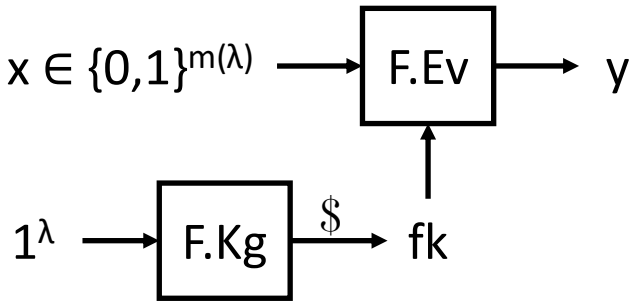


We describe the first solution

Main tool: indistinguishability obfuscation

Function Families

Function family F = (F.Kg, F.Ev)

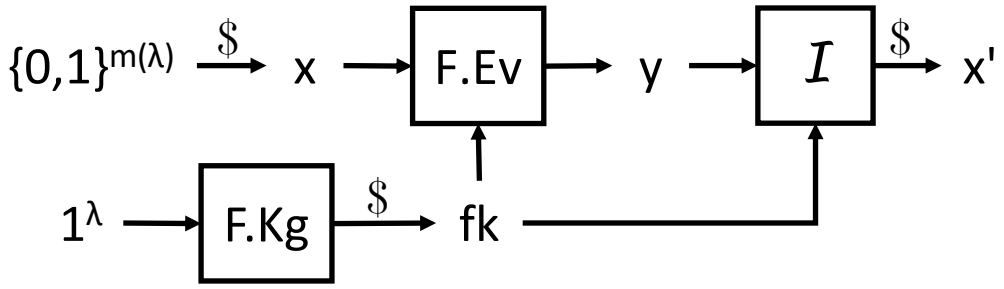


Example: RSA function family

fk = (N, e)

F.Ev(fk, x) = x^e mod N

One-Way Functions



$$\underline{\mathrm{OW}_{\mathsf{F}}^{\mathcal{I}}(\lambda)}$$
$$x \xleftarrow{\$} \{0,1\}^{m(\lambda)}$$
$$\mathrm{fk} \xleftarrow{\$} \mathsf{F.Kg}(1^{\lambda})$$
$$y \leftarrow \mathsf{F.Ev}(\mathrm{fk}, x)$$
$$x' \xleftarrow{\$} \mathcal{I}(\mathrm{fk}, y)$$
$$\text{Return } (\mathsf{F.Ev}(\mathrm{fk}, x') = y)$$

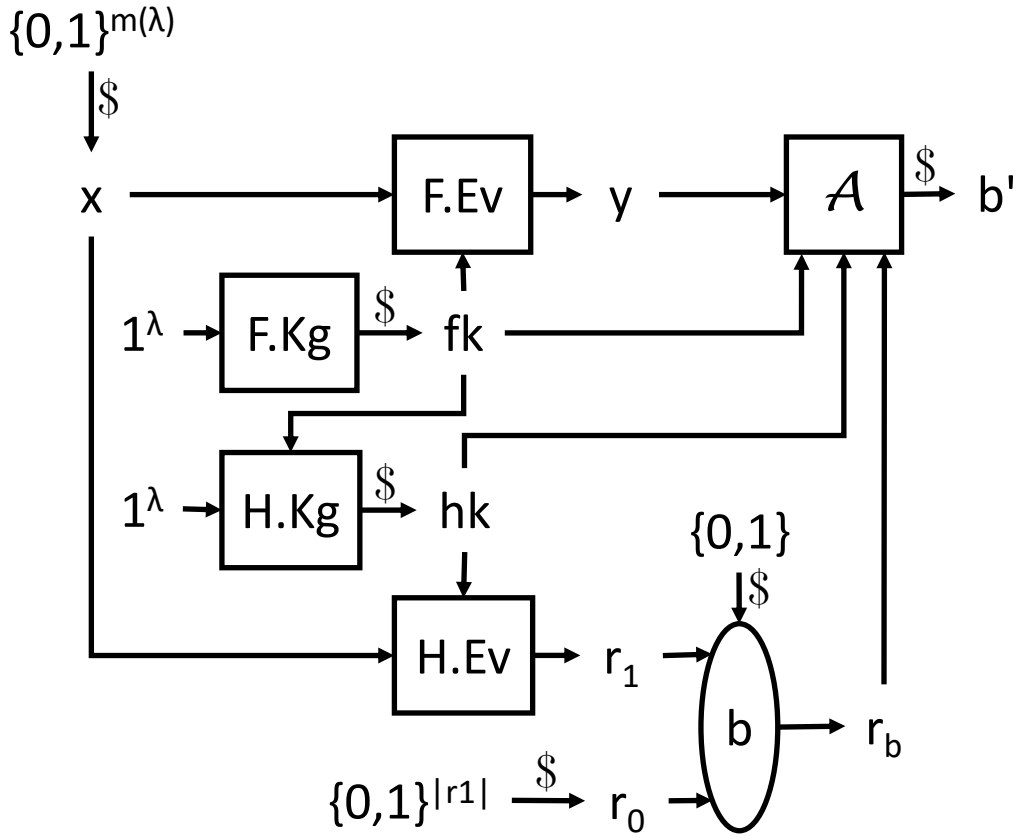
Function family F is one-way if

$$\forall \mathrm{PT}\ \mathcal{I}\colon \Pr\left[\mathsf{F.Ev}(\mathrm{fk}, x') = y\right]$$

is negligible

Hardcore Functions

Let F be a one-way function family



$\underline{\mathrm{HC}^{\mathcal{A}}_{\mathsf{F},\mathsf{H}}(\lambda)}$

$x \xleftarrow{\$} \{0,1\}^{m(\lambda)}$

$\mathrm{fk} \xleftarrow{\$} \mathsf{F.Kg}(1^\lambda);\ y \leftarrow \mathsf{F.Ev}(\mathrm{fk}, x)$

$\mathrm{hk} \xleftarrow{\$} \mathsf{H.Kg}(1^\lambda, \mathrm{fk});\ b \xleftarrow{\$} \{0,1\}$

If $b = 1$ then $r \leftarrow \mathsf{H.Ev}(\mathrm{hk}, x)$

else $r \xleftarrow{\$} \{0,1\}^{z(\lambda)}$

$b' \xleftarrow{\$} \mathcal{A}(\mathrm{fk}, \mathrm{hk}, y, r)$

Return $(b' = b)$

Function family H is hardcore for F if

$$\forall \mathrm{PT}\ \mathcal{A}\colon \Pr[b' = b] - 1/2$$

is negligible

Example: PKE scheme from RSA

RSA function family:

$fk = (N, e)$

$F.Ev(fk, x) = x^e \bmod N$

Conjecture: F is one-way

RSA public-key encryption scheme:

$pk = fk = (N, e)$

$Enc(1^\lambda, pk, m) = m^e \bmod N$

Not IND-CPA secure!

IND-CPA secure public-key encryption scheme from RSA:

$Enc_H(1^\lambda, pk, m) = (x^e \bmod N, H.Ev(hk, x) \oplus m)$, where:

indistinguishable from a uniformly random string

- H is hardcore for F
- $hk \xleftarrow{\$} H.Kg(1^\lambda, fk)$
- $x \xleftarrow{\$} \{0,1\}^{m(\lambda)}$

Limitation: how many bits can be encrypted?

$|H.Ev(hk, x)|$ – "span" of the hardcore function

We measure span as a function of $|x|$

History

One-Way Function	Hardcore Span	Required Assumption, Beyond One-Wayness	References
Any OWF (Goldreich-Levin hardcore bits)	1, log	–	[GL89]
RSA	poly	Φ-hiding; SSRSA	[LOS13]; [SPW06]
Rabin	poly	FSRSA	[SPW06]
Paillier	poly	BCCRA	[CGH01], [CGH02]
Discrete exponentiation modulo safe prime	poly	DLSE	[PS98], [MP05]
Discrete exponentiation modulo a composite	poly	Blum integer factorization	[HSS93], [GR03]
GPV lattice-based OWF [GPV08]	poly	LWE	[AGV09]
Niederreiter	poly	SDA + IA	[FGKRS10]
Any OWF	poly	UCE[$S^{cup} \cap S^{splt} \cap S^{one}$]	[BHK13]

Ad hoc solutions!

No polynomial span known for:

- discrete exponentiation modulo a prime
- discrete exponentiation in an elliptic curve group

Our Results

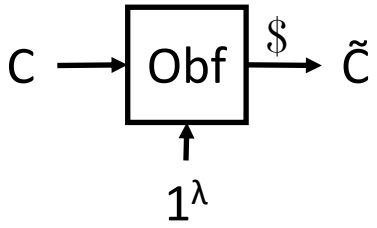
One-Way Function	Hardcore Span	Required Assumption, Beyond One-Wayness
Any injective OWF	poly	iO
Any OWF with polynomial pre-image size	poly	iO
Any OWF	poly	diO^{-}

Subsequent results:

One-Way Function	Hardcore Span	Required Assumption, Beyond One-Wayness	References
Any OWF	poly	iO + AIPO	[Brzuska-Mittelbach-14]
Any OWF	poly	Witness PRF	[Zhandry-14]

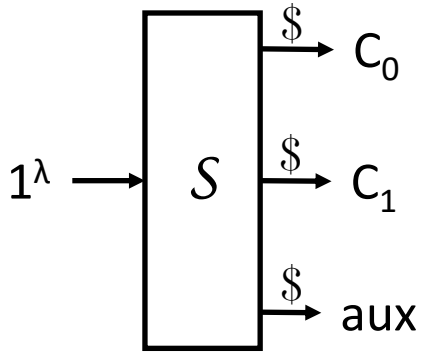
$\mathcal{S}$-secure Circuit Obfuscators

Circuit Obfuscators



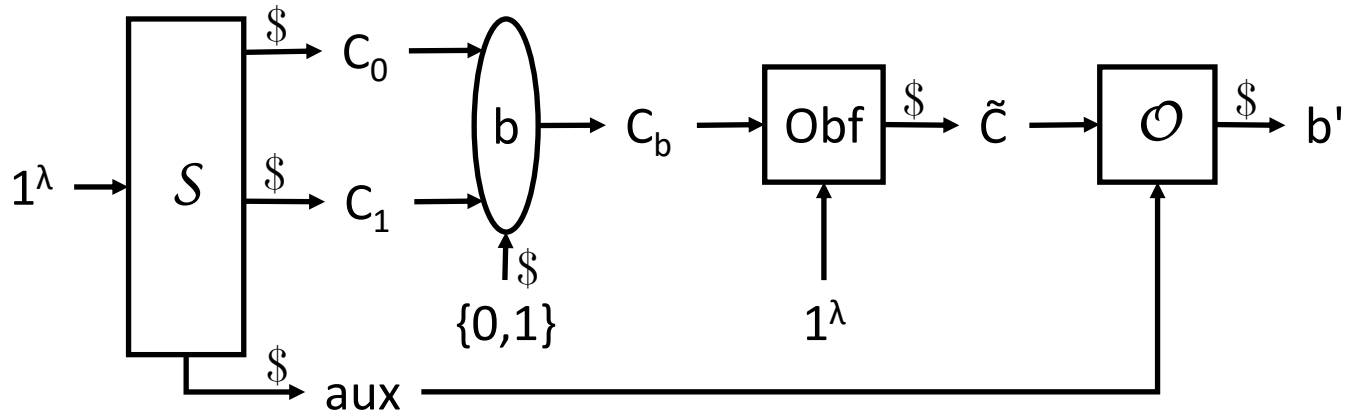
Correctness: $\forall x$: $C(x) = \tilde{C}(x)$

Circuit Samplers



Require: $|C_0| = |C_1|$

$\mathcal{S}$-secure Circuit Obfuscators



$\underline{\mathrm{IO}^{\mathcal{O}}_{\mathrm{Obf},\mathcal{S}}(\lambda)}$

$(\mathrm{C}_0, \mathrm{C}_1, aux) \xleftarrow{\$} \mathcal{S}(1^\lambda)$

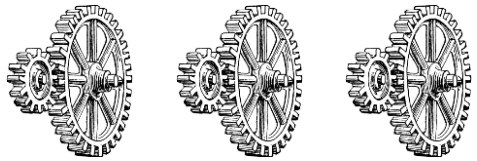
$b \xleftarrow{\$} \{0,1\}$

$\overline{\mathrm{C}} \xleftarrow{\$} \mathrm{Obf}(1^\lambda, \mathrm{C}_b)$

$b' \xleftarrow{\$} \mathcal{O}(\overline{\mathrm{C}}, aux)$

$\mathrm{Return}\ (b' = b)$

Let $\mathcal{S}$ be a class of circuit samplers

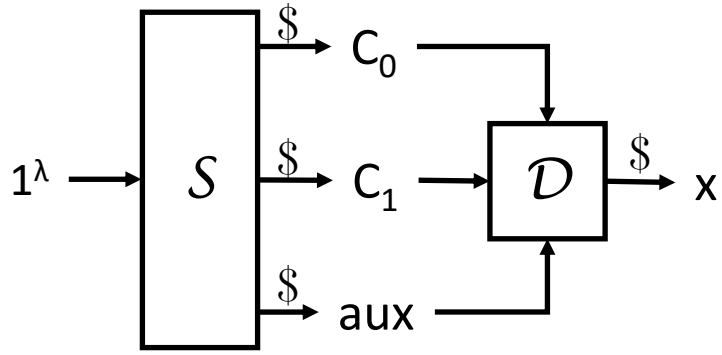


An obfuscator Obf is $\mathcal{S}$-secure if

$$\forall \mathrm{PT}\ \mathcal{O}\colon \Pr[b' = b] - 1/2$$

is negligible for all $\mathcal{S} \in \mathcal{S}$

Difference-Secure Circuit Samplers



$\underline{\mathrm{DIFF}_{\mathcal{S}}^{\mathcal{D}}(\lambda)}$

$(\mathrm{C}_0, \mathrm{C}_1, aux) \xleftarrow{\$} \mathcal{S}(1^\lambda)$

$x \xleftarrow{\$} \mathcal{D}(\mathrm{C}_0, \mathrm{C}_1, aux)$

Return $(\mathrm{C}_0(x) \neq \mathrm{C}_1(x))$

A circuit sampler $\mathcal{S}$ is difference-secure if

$$\forall \mathrm{PT}\ \mathcal{D}\colon \Pr\left[\mathrm{C}_0(x) \neq \mathrm{C}_1(x)\right]$$

is negligible

Let $\mathcal{S}_{\mathrm{diff}}$ be a class of difference-secure circuit samplers

Parametrized diO Framework

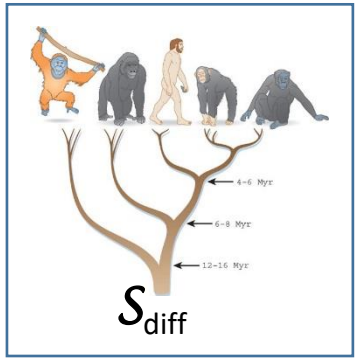
Abbreviation	Circuit Samplers	Definition
$\mathcal{S}_{\text{diff}}$	are difference-secure	see previous slide
$\mathcal{S}_{\text{eq}}$	produce equivalent circuits	C_0 and C_1 always agree on all inputs
$\mathcal{S}_{\text{diff}}(d)$	are difference-secure; produce d-differing circuits	C_0 and C_1 differ on at most $d(\lambda)$ inputs
$\mathcal{S}^{\text{sh}}$	have short auxiliary inputs	$\lvert aux \rvert < \lvert C_b \rvert$ for all $b \in \{0,1\}$

Definitions:

$\mathcal{S}_{\text{eq}}$-secure obfuscator is an indistinguishability obfuscator
$\mathcal{S}_{\text{diff}}$-secure obfuscator is a differing-inputs obfuscator

[Boyle-Chung-Pass-14]:

If d is a polynomial then any $\mathcal{S}_{\text{eq}}$-secure obfuscator
is also a $\mathcal{S}_{\text{diff}}(d)$-secure obfuscator.



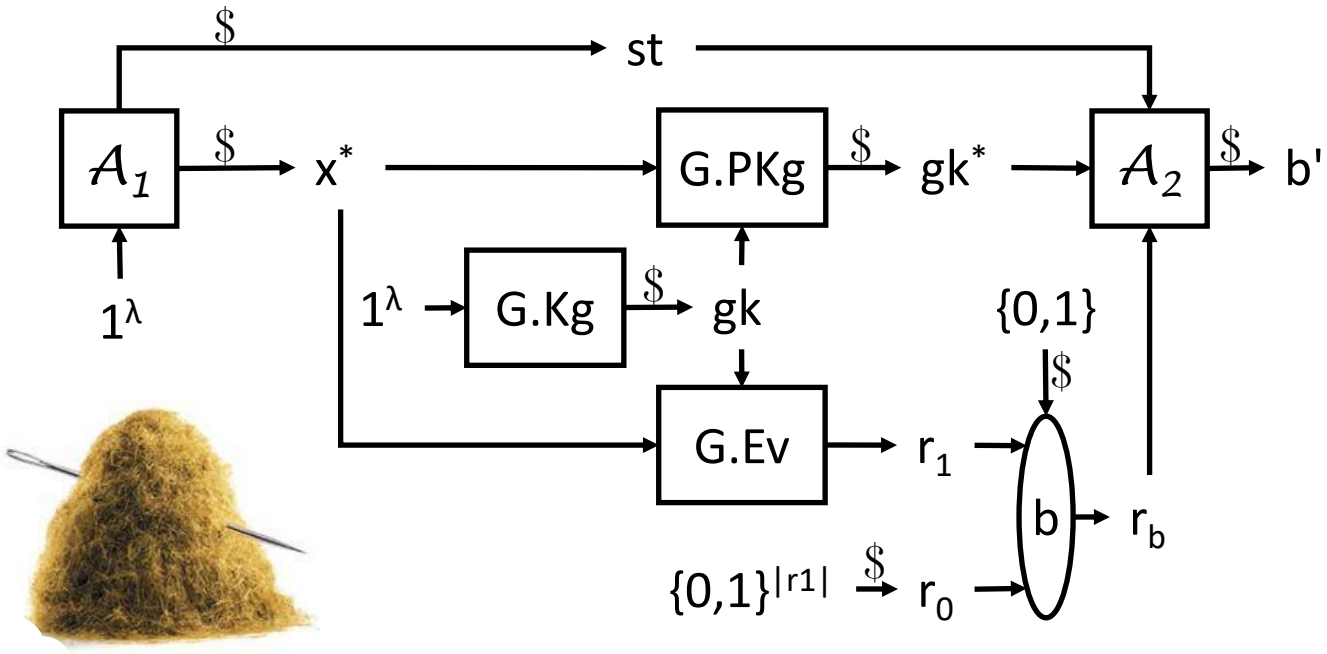
$\mathcal{S}_{\text{diff}}$

Punctured PRF

Let G be a function family extended with PKg

For any input x*: $gk^* \xleftarrow{\$} G.PKg(gk, x^*)$ such that

$$G.Ev(gk^*, x) = \begin{cases} G.Ev(gk, x), & x \neq x^* \\ \perp, & \text{otherwise} \end{cases}$$



$$\underline{\mathrm{PPRF}_{\mathsf{G}}^{\mathcal{A}}(\lambda)}$$
$$(x^*, \mathrm{st}) \xleftarrow{\$} \mathcal{A}_1(1^\lambda)$$
$$\mathrm{gk} \xleftarrow{\$} \mathsf{G.Kg}(1^\lambda)$$
$$\mathrm{gk}^* \xleftarrow{\$} \mathsf{G.PKg}(\mathrm{gk}, x^*)$$
$$b \xleftarrow{\$} \{0,1\}$$
$$\text{If } b = 1 \text{ then } r^* \leftarrow \mathsf{G.Ev}(\mathrm{gk}, x^*)$$
$$\text{else } r^* \xleftarrow{\$} \{0,1\}^{n(\lambda)}$$
$$b' \xleftarrow{\$} \mathcal{A}_2(\mathrm{st}, \mathrm{gk}^*, r^*)$$
$$\text{Return } (b' = b)$$

G is a punctured-PRF if

$$\forall \mathrm{PT}\ \mathcal{A}\colon \Pr[b' = b] - 1/2$$

is negligible

Our Result for Injective OWFs

Assume the following:

- Injective OWF F
- Punctured PRF G
- $S_{\text{diff}}(1)$-secure obfuscator Obf
  [BCP14]: S_{eq} is sufficient

Then there exists a polynomial s such that the function family

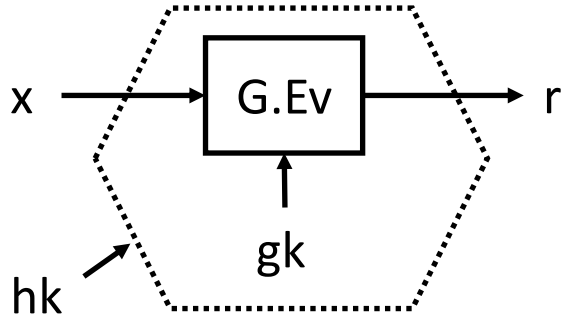
HC1[G, Obf, s] = (H.Kg, H.Ev)

is hardcore for F

$\underline{\mathsf{H.Kg}(1^\lambda, \mathrm{fk})}$
$\mathrm{gk} \xleftarrow{\$} \mathsf{G.Kg}(1^\lambda)$
$\mathrm{C} \leftarrow \mathsf{Pad}_{s(\lambda)}(\mathsf{G.Ev}(\mathrm{gk}, \cdot))$
$\overline{\mathrm{C}} \xleftarrow{\$} \mathsf{Obf}(1^\lambda, \mathrm{C})$
$\mathrm{hk} \leftarrow \overline{\mathrm{C}}$; Return hk

$\underline{\mathsf{H.Ev}(\mathrm{hk}, x)}$
$\overline{\mathrm{C}} \leftarrow \mathrm{hk}$
$r \leftarrow \overline{\mathrm{C}}(x)$
Return r

Note: polynomial s depends on F



Challenge: show that iO hides gk

Our Result for Any OWF

Assume the following:

- OWF F
- Polynomial d = PreImg_F
- Punctured PRF G
- ($\mathcal{S}_{\text{diff}}(d) \cap \mathcal{S}^{\text{sh}}$)-secure obfuscator Obf
  [BCP14]: $\mathcal{S}_{\text{eq}}$ is sufficient for polynomial d

Then there exists a polynomial s such that the function family

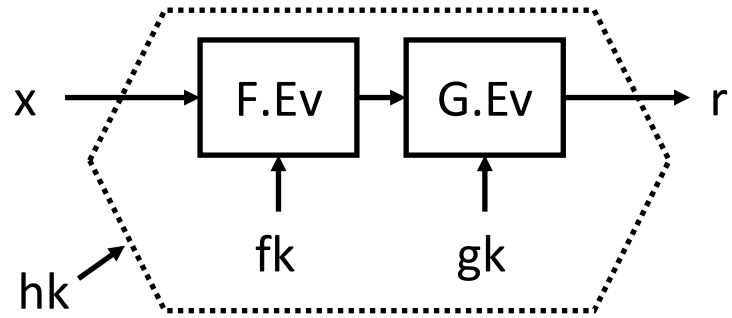
HC2[F, G, Obf, s] = (H.Kg, H.Ev)

is hardcore for F

$\underline{\mathsf{H.Kg}(1^\lambda, \mathrm{fk})}$
$\mathrm{gk} \xleftarrow{\$} \mathsf{G.Kg}(1^\lambda)$
$\mathrm{C} \leftarrow \mathsf{Pad}_{s(\lambda)}(\mathsf{G.Ev}(\mathrm{gk}, \mathsf{F.Ev}(\mathrm{fk}, \cdot)))$
$\overline{\mathrm{C}} \xleftarrow{\$} \mathsf{Obf}(1^\lambda, \mathrm{C})$
$\mathrm{hk} \leftarrow \overline{\mathrm{C}}$; Return hk

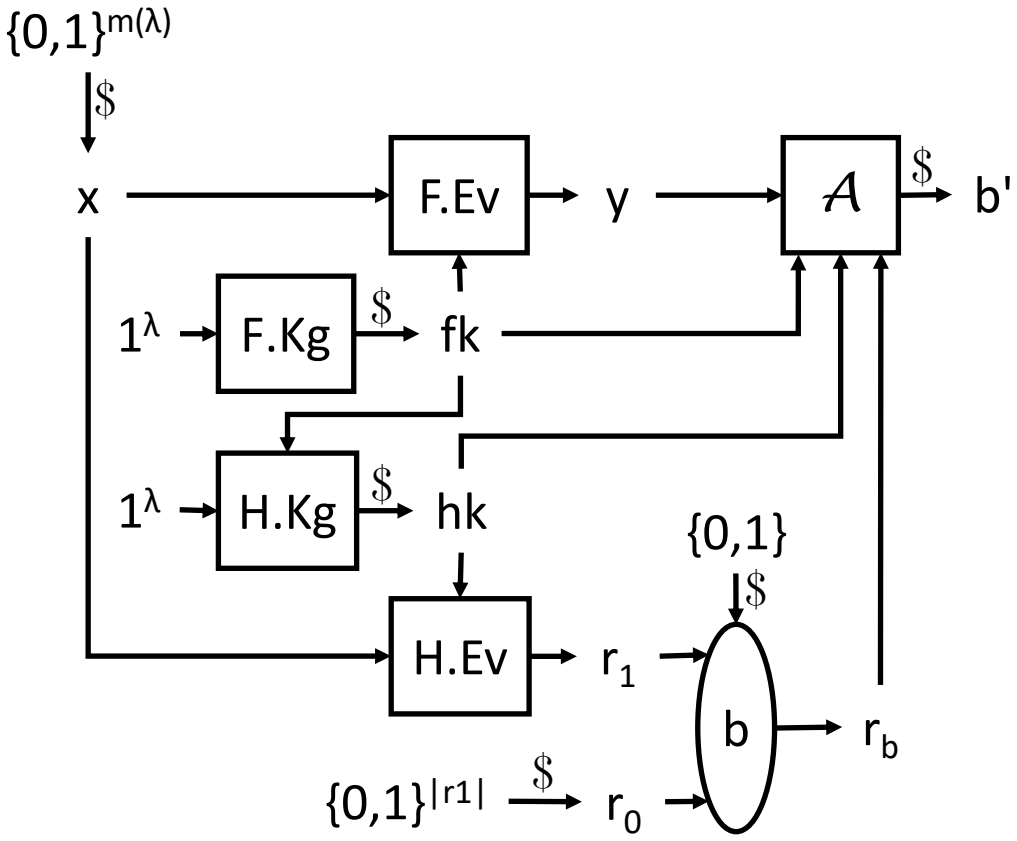
$\underline{\mathsf{H.Ev}(\mathrm{hk}, x)}$
$\overline{\mathrm{C}} \leftarrow \mathrm{hk}$
$r \leftarrow \overline{\mathrm{C}}(x)$
Return r

Note: H is "output-only dependent"



[GGHW14]: implausibility of diO and output-only dependent hardcore bits

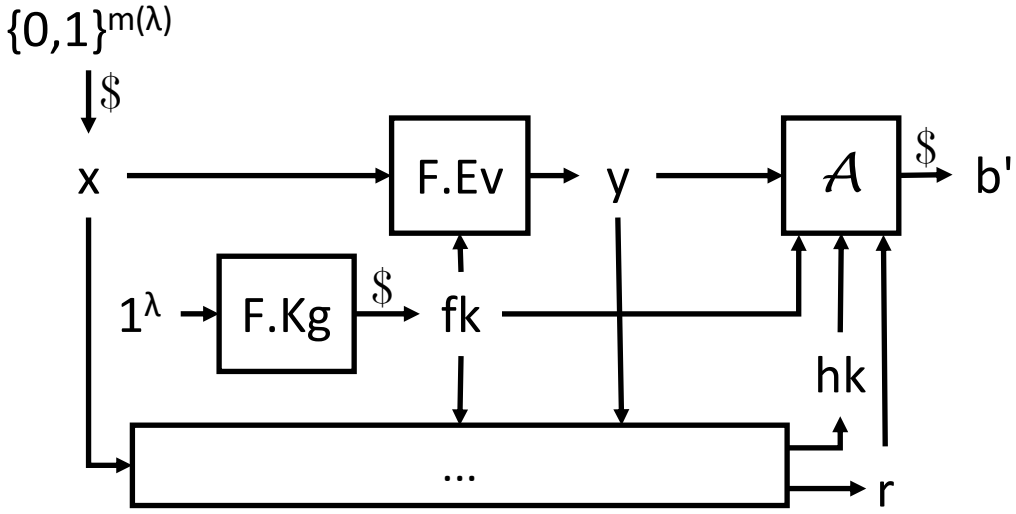
Injective OWFs: Proof Outline



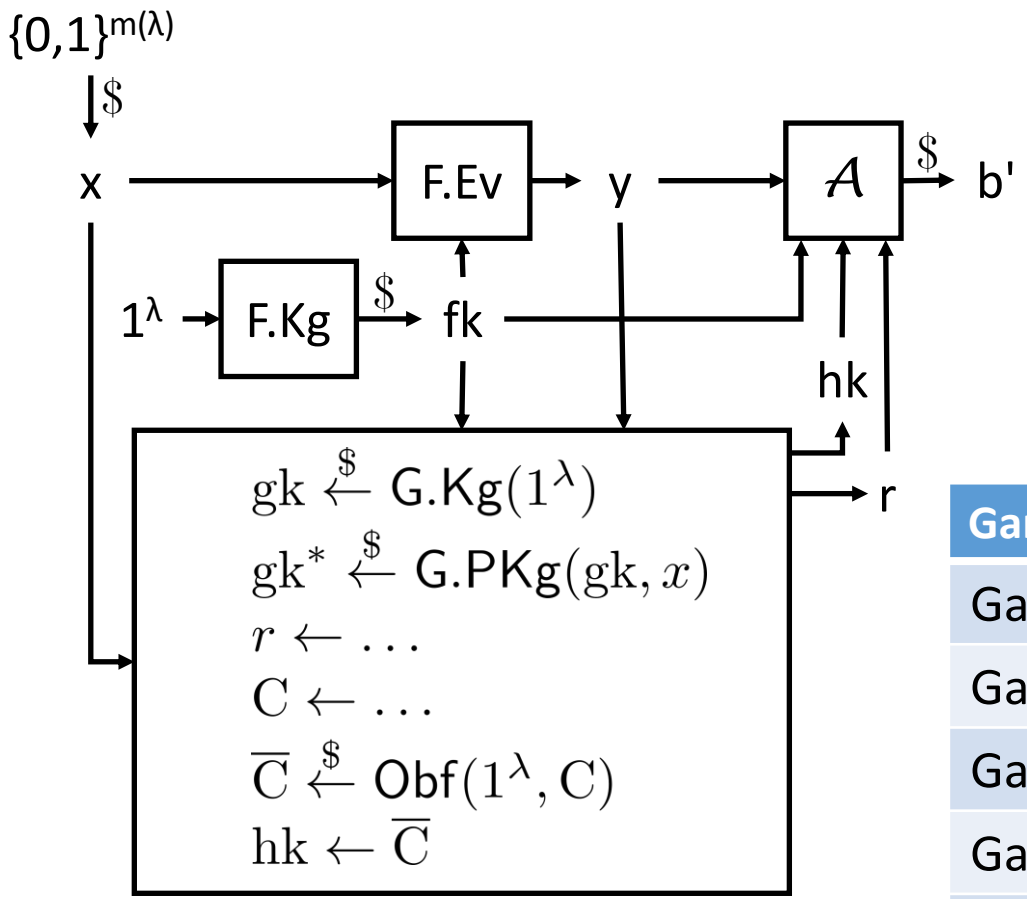
Hybrid games: $Game_0$, …, $Game_4$

$Game_0$ is equivalent to case b=1

$Game_4$ is equivalent to case b=0



Injective OWFs: Hybrid Games



Circuit $\mathrm{C}^{1}_{\mathrm{gk}^*,x,r}(x')$

If $x' \neq x$ then return $\mathsf{G.PEv}(\mathrm{gk}^*, x')$
Else return r

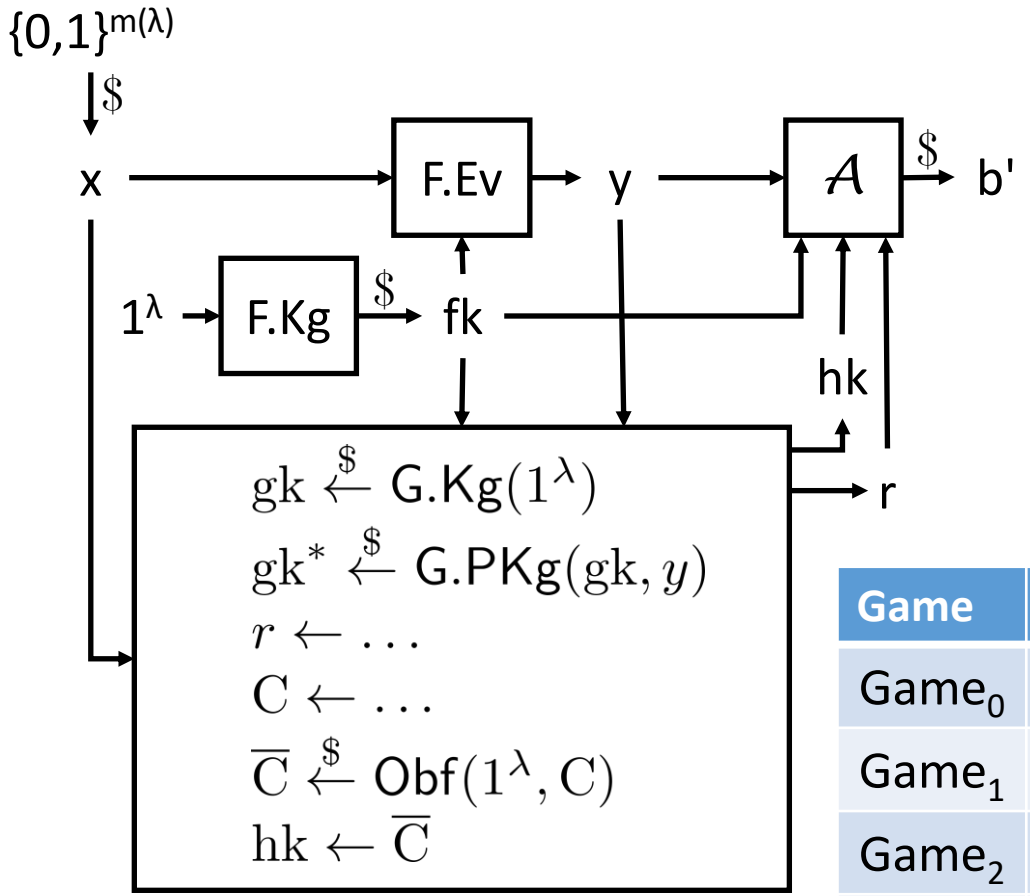
Circuit $\mathrm{C}^{2}_{\mathrm{fk},\mathrm{gk},y,r}(x')$

If $\mathsf{F.Ev}(\mathrm{fk}, x') \neq y$ then return $\mathsf{G.Ev}(\mathrm{gk}, x')$
Else return r

Game	r	C
Game_0	$r \leftarrow \mathsf{G.Ev}(\mathrm{gk}, x)$	$\mathrm{C} \leftarrow \mathsf{Pad}_{s(\lambda)}(\mathsf{G.Ev}(\mathrm{gk}, \cdot))$
Game_1	$r \leftarrow \mathsf{G.Ev}(\mathrm{gk}, x)$	$\mathrm{C} \leftarrow \mathsf{Pad}_{s(\lambda)}(\mathrm{C}^{1}_{\mathrm{gk}^*,x,r})$
Game_2	$r \xleftarrow{\$} \{0,1\}^{n(\lambda)}$	$\mathrm{C} \leftarrow \mathsf{Pad}_{s(\lambda)}(\mathrm{C}^{1}_{\mathrm{gk}^*,x,r})$
Game_3	$r \xleftarrow{\$} \{0,1\}^{n(\lambda)}$	$\mathrm{C} \leftarrow \mathsf{Pad}_{s(\lambda)}(\mathrm{C}^{2}_{\mathrm{fk},\mathrm{gk}^*,y,r})$
Game_4	$r \xleftarrow{\$} \{0,1\}^{n(\lambda)}$	$\mathrm{C} \leftarrow \mathsf{Pad}_{s(\lambda)}(\mathsf{G.Ev}(\mathrm{gk}, \cdot))$

iO
PPRF
iO + inj.
diO + OW

Any OWF: Hybrid Games



$$\frac{\text{Circuit } \mathrm{C}^{1}_{\mathrm{fk},\mathrm{gk}^*,y,r}(x')}{y' \leftarrow \mathsf{F.Ev}(\mathrm{fk}, x')}$$
$$\text{If } y' \neq y \text{ then return } \mathsf{G.PEv}(\mathrm{gk}^*, y')$$
$$\text{else return } r$$

Game	r	C	
Game_0	$r \leftarrow \mathsf{G.Ev}(\mathrm{gk}, y)$	$\mathrm{C} \leftarrow \mathrm{Pad}_{s(\lambda)}(\mathsf{G.Ev}(\mathrm{gk}, \mathsf{F.Ev}(\mathrm{fk}, \cdot)))$	iO
Game_1	$r \leftarrow \mathsf{G.Ev}(\mathrm{gk}, y)$	$\mathrm{C} \leftarrow \mathrm{Pad}_{s(\lambda)}(\mathrm{C}^{1}_{\mathrm{fk},\mathrm{gk}^*,y,r})$	PPRF
Game_2	$r \xleftarrow{\$} \{0,1\}^{n(\lambda)}$	$\mathrm{C} \leftarrow \mathrm{Pad}_{s(\lambda)}(\mathrm{C}^{1}_{\mathrm{fk},\mathrm{gk}^*,y,r})$	diO + OW
Game_3	$r \xleftarrow{\$} \{0,1\}^{n(\lambda)}$	$\mathrm{C} \leftarrow \mathrm{Pad}_{s(\lambda)}(\mathsf{G.Ev}(\mathrm{gk}, \mathsf{F.Ev}(\mathrm{fk}, \cdot)))$	

Hardcore Functions for Correlated Inputs

Assume the following:

- Arbitrary distribution D on d inputs
- Injective function family F one-way on D
- Punctured PRF G
- $\mathcal{S}_{\text{diff}}(d)$-secure obfuscator Obf
  [BCP14]: $\mathcal{S}_{\text{eq}}$ is sufficient for polynomial d

Then there exists a polynomial s such that the function family

HC1[G, Obf, s]

is hardcore for F with respect to D

Limitation: the size of hk grows with d

EwHCore construction by [Fuller-O'Neill-Reyzin-12]:

Yields a PRIV-secure D-PKE scheme for any input distribution

Limitation: the size of pk grows with the number of elements one can securely encrypt

Fin