Nesting Hybrids

Georg Fuchsbauer (IST Austria)
Momchil Konstantinov (Oxford)
Krzysztof Pietrzak (IST Austria)
Vanishree Rao (UCLA)

IST AUSTRIA
Institute of Science and Technology

Visions of Cryptography
Weizmann Institute, December 11th 2013

Adaptive vs. Selective Security

adaptive attack by A on $\{\Pi_n\}_{n\in\mathbb{N}}$

- A queries $\Pi_n(.)$
- A chooses challenge $x^* \in \{0,1\}^n$
- A must break $\Pi_n(.)$ on input x^*

Adaptive vs. Selective Security

selective attack by A on $\{\Pi_n\}_{n\in\mathbb{N}}$

- A chooses challenge $x^* \in \{0,1\}^n$
- A queries $\Pi_n(.)$
- A must break $\Pi_n(.)$ on input x^*

Adaptive vs. Selective Security

Lemma (Security Leveraging)

If A breaks adaptive security with advantage $\epsilon \Rightarrow$ can use A to break selective security with advantage $\epsilon/2^n$.

selective attack using adaptive A

- guess random challenge $x' \in \{0,1\}^n$
- A queries $\Pi_n(.)$
- A chooses challenge x^*
- if $x' \neq x^*$ give up
- A must break $\Pi_n(.)$ on input x^*

Nested Hybrids in a Nutshell

proving adaptive security via leveraging

1. adaptive $\Pi_n \rightarrow$ selective Π_n (losing factor 2^n).
2. selective $\Pi_n \rightarrow \Phi$ (hybrid argument looses poly(n)).

Nested Hybrids in a Nutshell

proving adaptive security via leveraging

1. adaptive $\Pi_n \rightarrow$ selective Π_n (losing factor 2^n).
2. selective $\Pi_n \rightarrow \Phi$ (hybrid argument looses poly(n)).

nesting hybrids

1. adaptive $\Pi_n \rightarrow$ adaptive* Π_n (losing small factor α)
2. adaptive* $\Pi_n \rightarrow$ adaptive $\Pi_{n/2}$ (hybrid losing factor β)
3. iterate 1 and 2 $\log(n)$ times:
   adaptive $\Pi_n \rightarrow$ adaptive Π_1 losing $(\alpha\beta)^{\log(n)}$
4. adaptive $\Pi_1 \rightarrow \Phi$ lossless.

Applications

	old	new
GGM Constrained PRF[1] loss in reduction to PRG $n =$ input length, $q = \#$ queries	2^n	$q^{\log n}$
Generalized Selective Decryption[2] loss in reduction to ENC caveat : on trees $n = \# keys$	2^n	$2^{\log^2 n}$

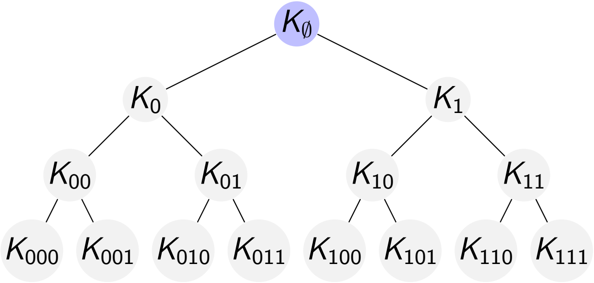
[1] *Functional Signatures and Pseudorandom Functions.* Elette Boyle, Shafi Goldwasser, Ioana Ivan **eprint.iacr.org/2013/401**
Constrained Pseudorandom Functions and Their Applications. Dan Boneh and Brent Waters **Asiacrypt 2013**
Delegatable Pseudorandom Functions and Applications. A.Kiayias, S.Papadopoulos, N.Triandopoulos, T.Zacharias. **CCS 2013**

[2] *Tackling Adaptive Corruptions in Multicast Encryption Protocols.* Saurabh Panjwani **TCC 2007**

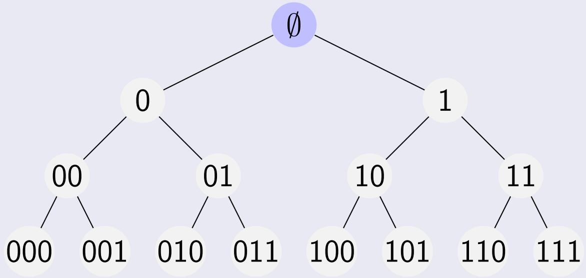
Goldreich-Goldwasser-Micali 84

GGM PRF $\mathsf{F}_K(x) = K_x$

- PRG $\mathsf{G} : \{0,1\}^n \to \{0,1\}^{2n}$
- $K = K_\emptyset \leftarrow \{0,1\}^n$
- $K_{x\|0} \| K_{x\|1} = \mathsf{G}(K_x)$



GGM Hybrid Argument

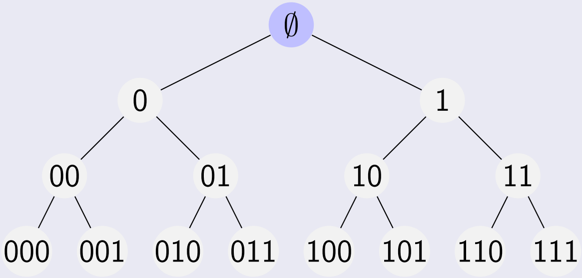


- $\mathsf{Adv}(H_0, H_{qn}) = \epsilon$ $\quad$ $q = \#$queries , n=input length.

$\Rightarrow$ $\mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/qn$

$\Rightarrow$ $\mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/qn$

GGM Hybrid Argument

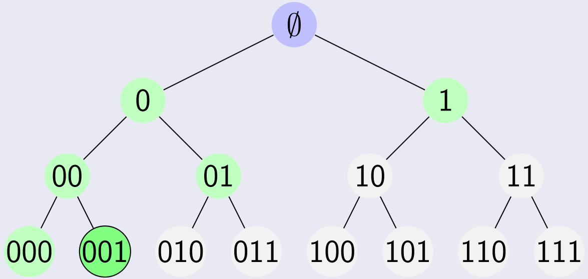


- $\mathsf{Adv}(H_0, H_{qn}) = \epsilon$ $\qquad q = \#\text{queries}$, n=input length.

$\Rightarrow \mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/qn$

$\Rightarrow \mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/qn$

GGM Hybrid Argument



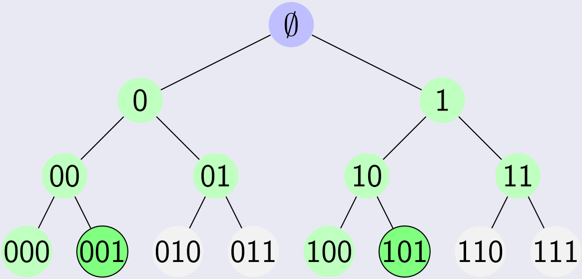
- $\mathsf{Adv}(H_0, H_{qn}) = \epsilon$ $\quad$ $q = \#$queries , n=input length.

$\Rightarrow$ $\mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/qn$

$\Rightarrow$ $\mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/qn$

GGM Hybrid Argument

Hybrid H_0 (the real game)



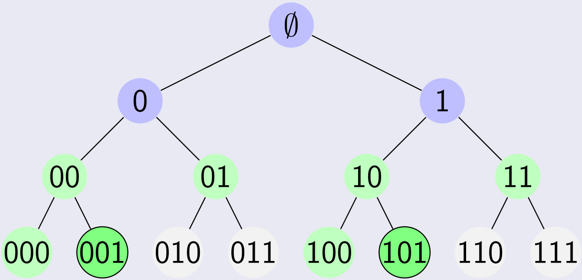
- $\mathrm{Adv}(H_0, H_{qn}) = \epsilon$ $\quad$ $q = \#$queries , n=input length.

$\Rightarrow$ $\mathrm{Adv}(H_i, H_{i+1}) \geq \epsilon/qn$

$\Rightarrow$ $\mathrm{Adv}(\mathrm{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/qn$

GGM Hybrid Argument

Hybrid H_1



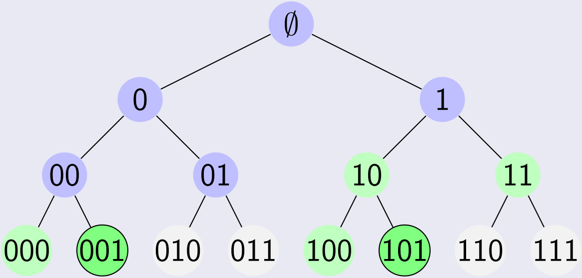
- $\text{Adv}(H_0, H_{qn}) = \epsilon$ $\quad$ $q = \#$queries , n=input length.

$\Rightarrow$ $\text{Adv}(H_i, H_{i+1}) \geq \epsilon/qn$

$\Rightarrow$ $\text{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/qn$

GGM Hybrid Argument

Hybrid H_2



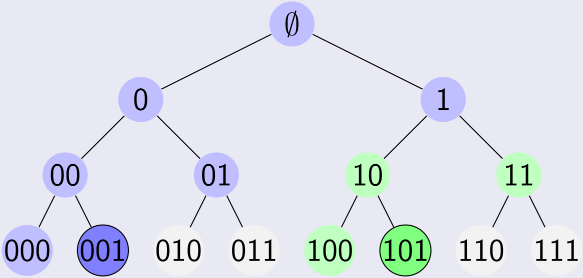
- $\mathsf{Adv}(H_0, H_{qn}) = \epsilon$ $\qquad$ $q = \#$queries , n=input length.

$\Rightarrow$ $\mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/qn$

$\Rightarrow$ $\mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/qn$

GGM Hybrid Argument

Hybrid H_3



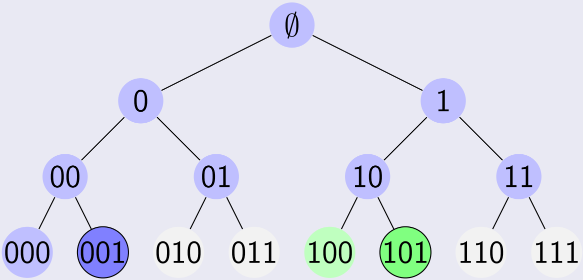
- $\mathrm{Adv}(H_0, H_{qn}) = \epsilon$ $\qquad$ $q = \#$queries , n=input length.

$\Rightarrow$ $\mathrm{Adv}(H_i, H_{i+1}) \geq \epsilon/qn$

$\Rightarrow$ $\mathrm{Adv}(\mathrm{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/qn$

GGM Hybrid Argument

Hybrid H_4



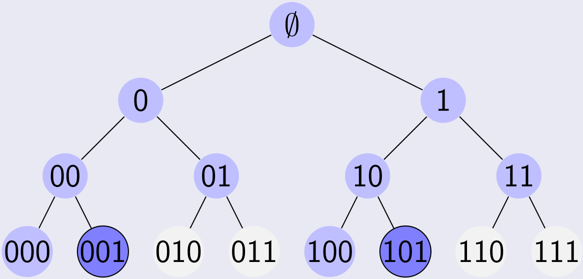
- $\mathsf{Adv}(H_0, H_{qn}) = \epsilon$ $\quad$ $q = \#\text{queries}$, n=input length.

$\Rightarrow$ $\mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/qn$

$\Rightarrow$ $\mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/qn$

GGM Hybrid Argument

Hybrid H_5 (the random game)

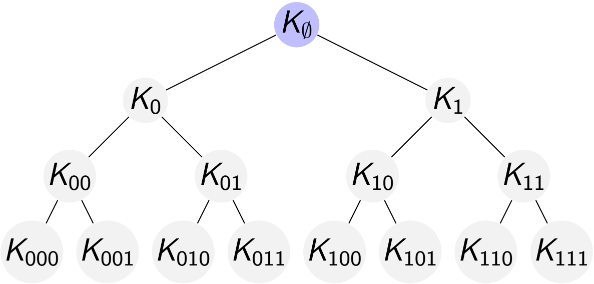


- $\mathsf{Adv}(H_0, H_{qn}) = \epsilon$ $\qquad q = \#\text{queries}$, n=input length.

$\Rightarrow \mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/qn$

$\Rightarrow \mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/qn$

Constrained/Delegatable/Functional GGM PRF

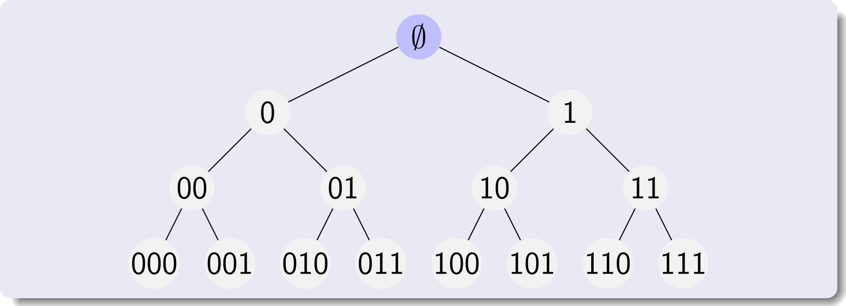


Functional Signatures and Pseudorandom Functions. Elette Boyle, Shafi Goldwasser, Ioana Ivan **eprint.iacr.org/2013/401**

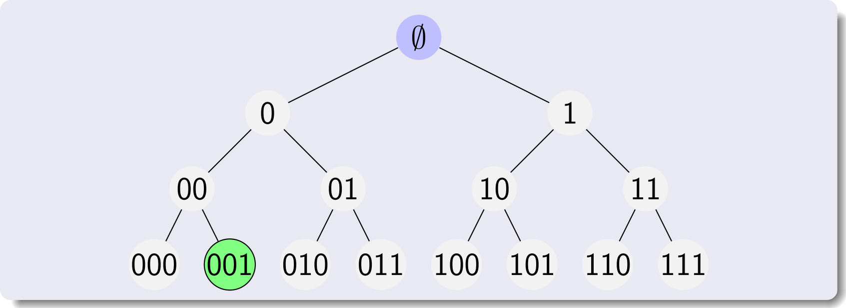
Constrained Pseudorandom Functions and Their Applications. Dan Boneh and Brent Waters **Asiacrypt 2013**

Delegatable Pseudorandom Functions and Applications. A.Kiayias, S.Papadopoulos, N.Triandopoulos, T.Zacharias. **CCS 2013**

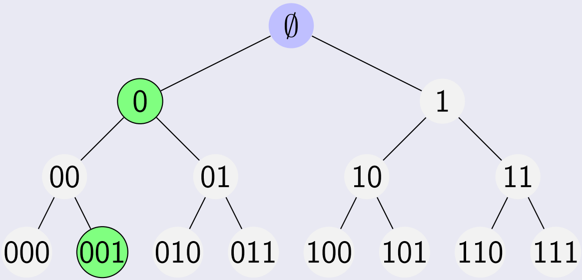
Constrained/Delegatable/Functional GGM PRF



Constrained/Delegatable/Functional GGM PRF

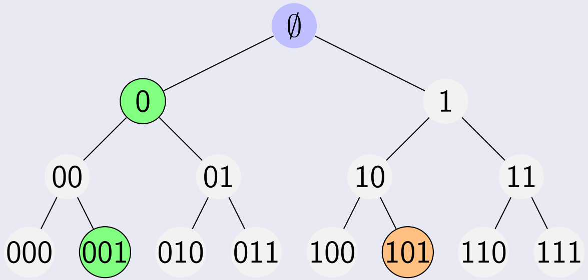


Constrained/Delegatable/Functional GGM PRF



$K_{x\|y}$ trivially distinguishable from random given K_x.

Constrained/Delegatable/Functional GGM PRF

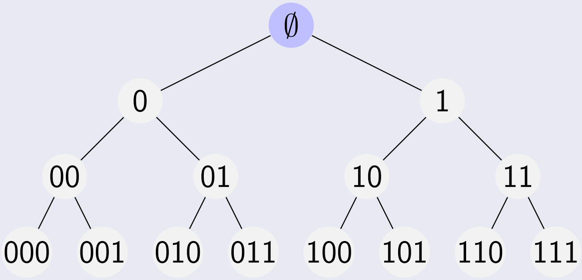


$K_{x\|y}$ trivially distinguishable from random given K_x.

Security game for constrained PRFs

- choose x^* where no prefix of x^* was queried.
- distinguish K_{x^*} from random.

Proving Selective Security



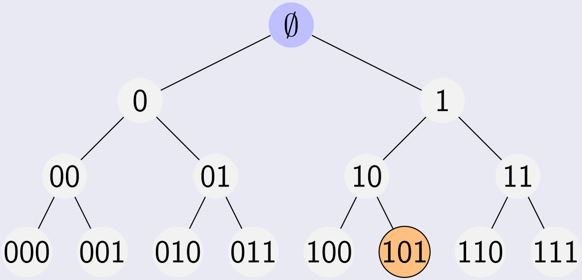
- $\mathsf{Adv}(H_0, H_6) = \epsilon$

$\Rightarrow$ $\mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/6$

$\Rightarrow$ $\mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/6$

Proving Selective Security

Choose challenge



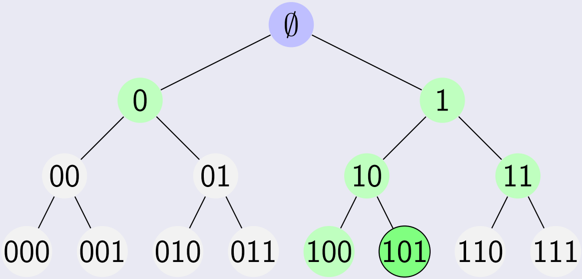
- $\mathsf{Adv}(H_0, H_6) = \epsilon$

$\Rightarrow$ $\mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/6$

$\Rightarrow$ $\mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/6$

Proving Selective Security

Hybrid H_0 (real game)



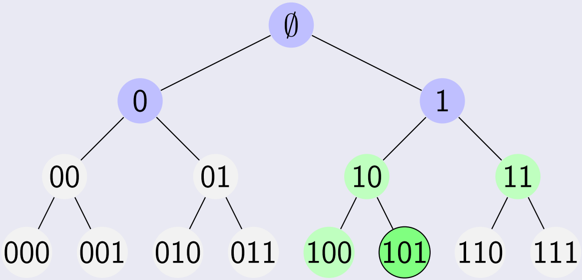
- $\mathsf{Adv}(H_0, H_6) = \epsilon$

$\Rightarrow$ $\mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/6$

$\Rightarrow$ $\mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/6$

Proving Selective Security

Hybrid H_1



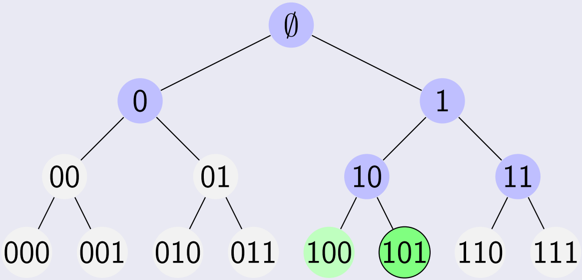
- $\mathsf{Adv}(H_0, H_6) = \epsilon$

$\Rightarrow$ $\mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/6$

$\Rightarrow$ $\mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/6$

Proving Selective Security

Hybrid H_2



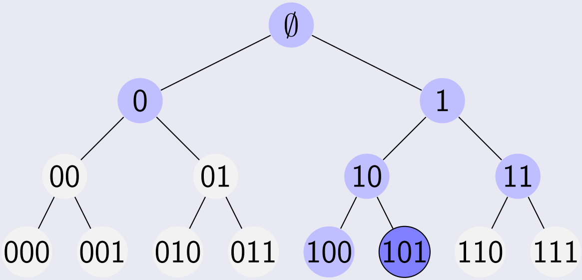
- $\mathsf{Adv}(H_0, H_6) = \epsilon$

$\Rightarrow$ $\mathsf{Adv}(H_i, H_{i+1}) \geq \epsilon/6$

$\Rightarrow$ $\mathsf{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/6$

Proving Selective Security

Hybrid H_3



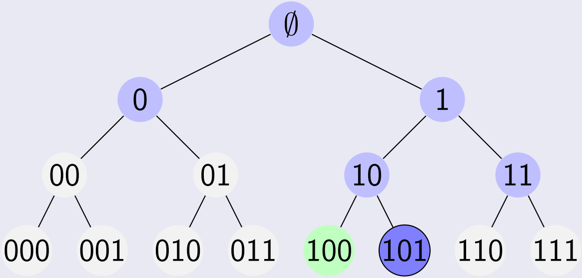
- $\mathrm{Adv}(H_0, H_6) = \epsilon$

$\Rightarrow$ $\mathrm{Adv}(H_i, H_{i+1}) \geq \epsilon/6$

$\Rightarrow$ $\mathrm{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/6$

Proving Selective Security

Hybrid H_4



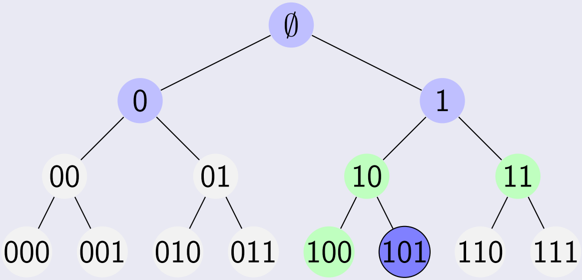
- $\mathrm{Adv}(H_0, H_6) = \epsilon$

$\Rightarrow$ $\mathrm{Adv}(H_i, H_{i+1}) \geq \epsilon/6$

$\Rightarrow$ $\mathrm{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/6$

Proving Selective Security

Hybrid H_5



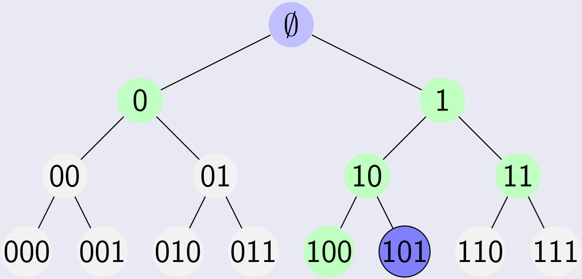
- $\mathrm{Adv}(H_0, H_6) = \epsilon$

$\Rightarrow$ $\mathrm{Adv}(H_i, H_{i+1}) \geq \epsilon/6$

$\Rightarrow$ $\mathrm{Adv}(\mathsf{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/6$

Proving Selective Security

Hybrid H_6 (random game)



- $\mathrm{Adv}(H_0, H_6) = \epsilon$

$\Rightarrow$ $\mathrm{Adv}(H_i, H_{i+1}) \geq \epsilon/6$

$\Rightarrow$ $\mathrm{Adv}(\mathrm{G}(U_\lambda), U_{2\lambda}) \geq \epsilon/6$

Proving Adaptive Security using Leveraging

H_0 $0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \rightarrow 8$

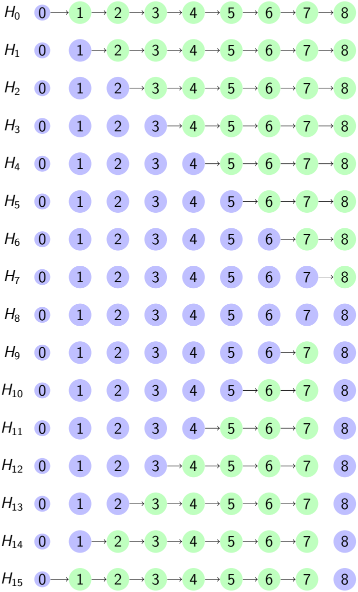
Proof

- Leveraging: Guess Challenge

$$\epsilon \rightarrow \frac{\epsilon}{2^n}$$

H_{15} $0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \quad 8$

Proving Adaptive Security using Leveraging



Proof

- Leveraging: Guess Challenge
- Hybrid Argument

$$\epsilon \to \frac{\epsilon}{2^n} \to \frac{\epsilon}{2^n \cdot 2n}$$

Proving Adaptive Security by Nesting

$$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \rightarrow 8$$

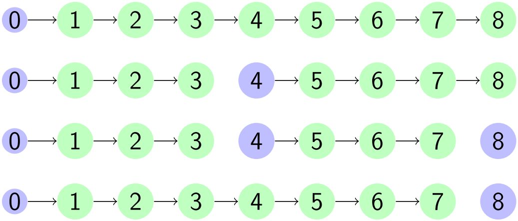
$$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \quad 8$$

Proof

1. Guess first query that agrees with x^* on 4-prefix.

$$\epsilon \rightarrow \frac{\epsilon}{q}$$

Proving Adaptive Security by Nesting



Proof

1. Guess first query that agrees with x^* on 4-prefix.
2. Hybrid argument.

$$\epsilon \to \frac{\epsilon}{q} \to \frac{\epsilon}{3q}$$

Proving Adaptive Security by Nesting

$$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \quad 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \rightarrow 8$$

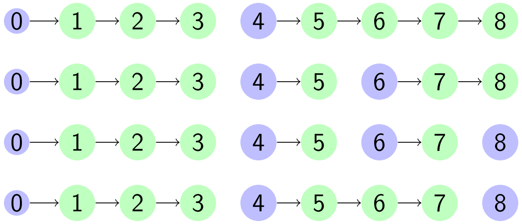
$$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \quad 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \quad 8$$

Proof

1. Guess first query that agrees with x^* on 6-prefix.
2. Hybrid argument.

$$\epsilon \rightarrow \frac{\epsilon}{q} \rightarrow \frac{\epsilon}{3q} \rightarrow \ldots \rightarrow$$

Proving Adaptive Security by Nesting



Proof

1. Guess first query that agrees with x^* on 6-prefix.
2. Hybrid argument.

$$\epsilon \to \frac{\epsilon}{q} \to \frac{\epsilon}{3q} \to \ldots \to$$

Proving Adaptive Security by Nesting

$$0 \to 1 \to 2 \to 3 \quad 4 \to 5 \to 6 \to 7 \to 8$$

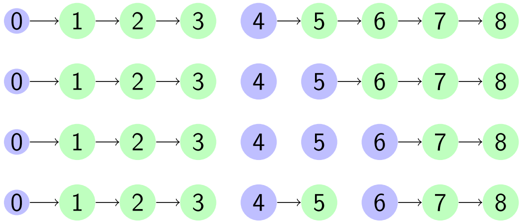
$$0 \to 1 \to 2 \to 3 \quad 4 \to 5 \quad 6 \to 7 \to 8$$

Proof

1. Guess first query that agrees with x^* on 5-prefix.
2. Hybrid argument.

$$\epsilon \to \frac{\epsilon}{q} \to \frac{\epsilon}{3q} \to \ldots \to$$

Proving Adaptive Security by Nesting



Proof

1. Guess first query that agrees with x^* on 5-prefix.
2. Hybrid argument.

$$\epsilon \to \frac{\epsilon}{q} \to \frac{\epsilon}{3q} \to \dots \to \frac{\epsilon}{(3q)^{\log n}}$$