The Random Oracle Model and the Ideal Cipher Model are Equivalent

Jean-Sébastien Coron [1], Jacques Patarin [2], and Yannick Seurin [2,3]

(1) Univ. Luxembourg, (2) Univ. Versailles, (3)Orange Labs

Séminaire ENS – June 19, 2008

ftgroup

orange™

the context

- two fundamental primitives of cryptology:
  - block ciphers: $E : \{0,1\}^k \times \{0,1\}^n \mapsto \{0,1\}^n$, $E(K,\cdot)$ bijective, efficiently computable and invertible
  - hash functions: $H : \{0,1\}^* \mapsto \{0,1\}^n$, efficiently computable
- security definition in the standard model? well . . .
- block cipher = pseudorandom permutation; OK for most applications, but:
  - doesn't take related-key attacks into account
  - insufficient for (black-box) constructing CRHFs [Simon89]
- hash function = OWF, CRHF, PRF, unpredictable . . .
- there's a need for stronger, idealised models

outline

- ROM and ICM
- indifferentiability: definition, usefulness . . .
- building a random permutation from a random function using the Luby-Rackoff construction:
  - why 5 rounds are not enough
  - indifferentiability for 6 rounds
    - description of the simulator
    - main ideas of the proof
- ongoing work & conclusion

idealised models: ROM

- ultimately, we want a hash function to behave as a random function
- *Random Oracle Model* [BellareR93]: a publicly accessible oracle, returning a n-bit random value for each new query
- widely used in PK security proofs (OAEP, PSS . . .)
- also widely criticized: uninstantiability results [CanettiGH98, Nielsen02] removing ROs has become a popular sport
- schemes provably secure in the plain standard model
  - Cramer-Shoup encryption
  - Boneh-Boyen signatures . . .

  are often less efficient and come at the price of stronger complexity assumptions
- sometimes no scheme at all (non-sequential aggregate signatures)

idealised models: ICM

- ultimately, we want a block cipher to behave as a family of random permutations $(E_K)_{K \in \{0,1\}^k}$
- *Ideal Cipher Model* [Shannon49, Winternitz84]: a pair of publicly accessible oracles $E(\cdot,\cdot)$ and $E^{-1}(\cdot,\cdot)$, such that $E(K,\cdot)$ is a random permutation for each key K
- less popular than the ROM, but:
  - widely used for analyzing block cipher-based hash functions [BlackRS02, Hirose06]
  - used for the security proof of some PK schemes (encryption, Authenticated Key Exchange . . .)
- uninstantiability results as well [Black06]

idealised models: is ICM > ROM?

- the ICM seems to be "richer" than the ROM since an ideal cipher has much more structure than a random oracle
- Coron et al. CRYPTO 2005 paper: the ICM implies the ROM, *i.e.* one can replace a random oracle by a block cipher-based hash function in any cryptosystem and the resulting scheme remains as secure in the ICM as in the ROM
- what about the other direction?
- Bellare, Pointcheval, Rogaway, Eurocrypt 2000:

  The ideal-cipher model is richer than the RO-model, and you can't just say "apply the Feistel construction to your random oracle to make the cipher." While this may be an approach to instantiating an ideal-cipher, there is no formal sense we know in which you can simulate the ideal-cipher model using only the RO-model.

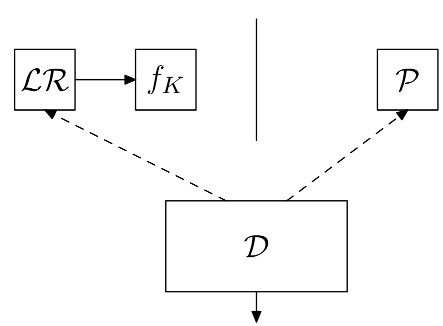
the "classical" indistinguishability notion

- usual security definition for a block cipher: (Strong)-PRP

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{SPRP}}(E) = \left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k, A^{E_K(\cdot), E_K^{-1}(\cdot)} = 1 \right] - \Pr\left[G \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^n), A^{G(\cdot), G^{-1}(\cdot)} = 1 \right] \right|$$
$$= \mathsf{negl}(k) \text{ for any PPT adversary } \mathcal{A}$$

- well-known Luby-Rackoff result: the Feistel scheme with 4 rounds and pseudorandom internal functions yields a strong pseudorandom permutation

- useful only in secret-key applications, useless when the internal functions are public (*e.g.* for block cipher-based hash functions)



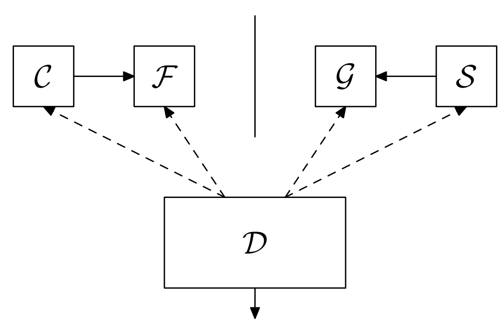
indifferentiability: definition

- let $\mathcal{G}$ be an ideal primitive (*e.g.* a random permutation), and $\mathcal{C}^{\mathcal{F}}$ be a construction using another ideal primitive $\mathcal{F}$ (*e.g.* the Feistel construction using a random oracle)

- $\mathcal{C}$ is said (q, t_S, q_S, ϵ)-indifferentiable from $\mathcal{G}$ if there is a PPT simulator $\mathcal{S}$ running in time at most t_S, making at most q_S queries such that for any distinguisher $\mathcal{D}$ making at most q queries,

$$\left| \Pr\left[\mathcal{D}^{\mathcal{C}^{\mathcal{F}},\mathcal{F}} = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{G},\mathcal{S}^{\mathcal{G}}} = 1\right] \right| \leqslant \epsilon$$

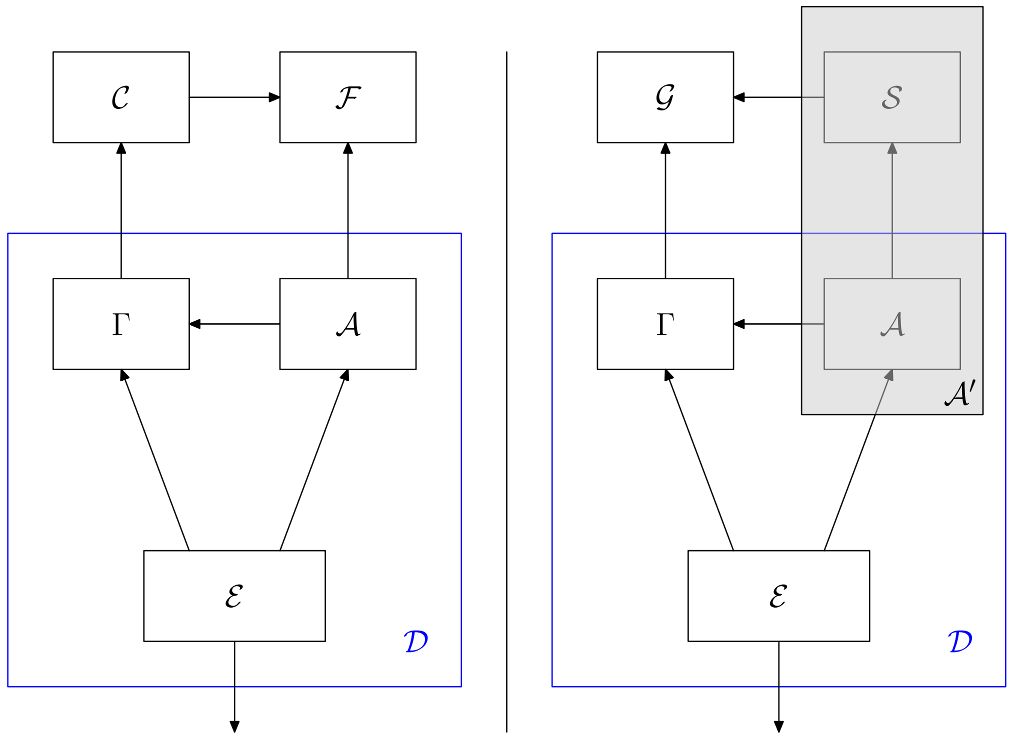
- the simulator cannot see the distinguisher's queries to $\mathcal{G}$!



indifferentiability: usefulness

- indifferentiability implies a kind of "universal composability" property (less general than Canetti's UC though)
- let Γ be a cryptosystem using a primitive $\mathcal{G}$; let $\mathcal{C}^{\mathcal{F}}$ be a construction using a primitive $\mathcal{F}$; if $\mathcal{C}^{\mathcal{F}}$ is indifferentiable from $\mathcal{G}$, then $\Gamma(\mathcal{C}^{\mathcal{F}})$ is at least as secure as $\Gamma(\mathrm{G})$
- more precisely, any attacker $\mathcal{A}$ against $\Gamma(\mathcal{C}^{\mathcal{F}})$ can be turned into an attacker $\mathcal{A}'$ against $\Gamma(\mathcal{G})$ with advantage negligibly close to the advantage of $\mathcal{A}$

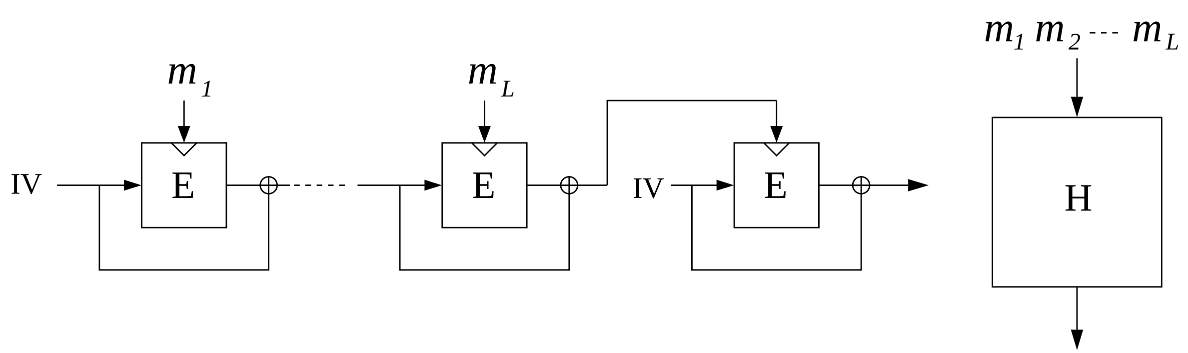
indifferentiability: usefulness



$$\begin{aligned}|\Pr[\mathcal{A}\text{ succeeds}] - \Pr[\mathcal{A}'\text{ succeeds}]| &= \left|\Pr\left[\mathcal{E}(\Gamma^{\mathcal{C}},\mathcal{A}^{\mathcal{F}})=1\right] - \Pr\left[\mathcal{E}(\Gamma^{\mathcal{G}},\mathcal{A}^{\mathcal{G}})=1\right]\right| \\ &= \left|\Pr\left[\mathcal{D}^{\mathcal{C}^{\mathcal{F}},\mathcal{F}}=1\right] - \Pr\left[\mathcal{D}^{\mathcal{G},\mathcal{S}^{\mathcal{G}}}=1\right]\right| \\ &= \mathrm{negl}(k)\end{aligned}$$

previous indifferentiability results

- function constructions:
  - hash functions constructions (FIL to VIL, block cipher-based) [CoronDMP05, ChangNLY06]

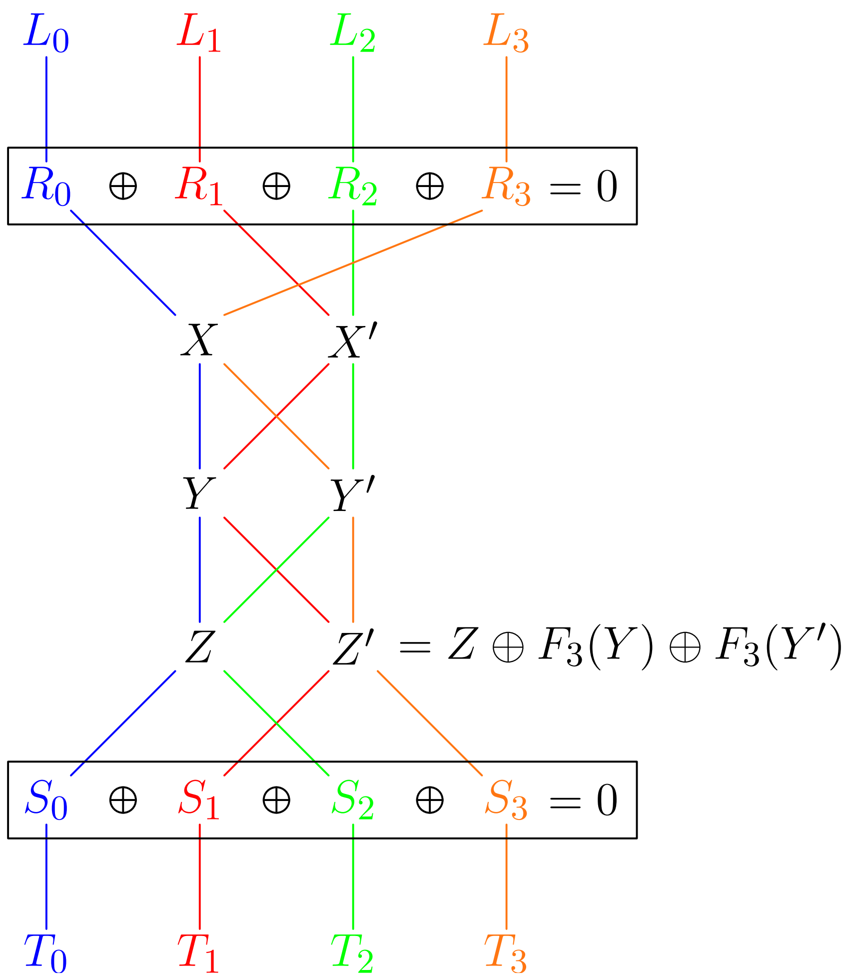


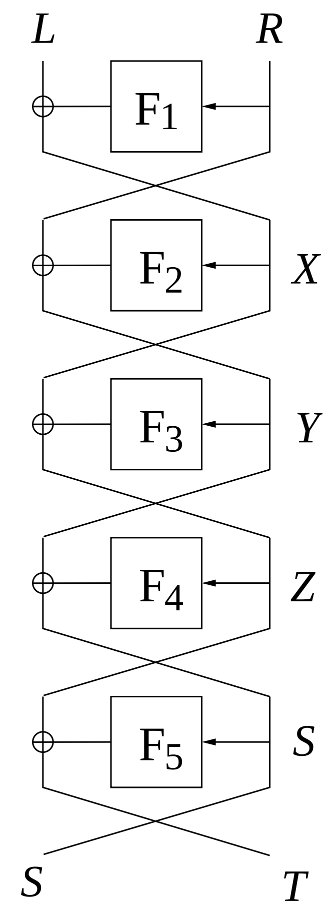
  - sponge construction [BertoniDPvA08]: construction of a VIL random function from a FIL random function or permutation
  - constructions with security beyond the birthday barrier [MaurerT07]

previous indifferentiability results

- permutation constructions:
  - Luby-Rackoff with super-logarithmic number of rounds is indifferentiable from a random permutation in the "honest-but-curious" model of indifferentiability [DodisP06]
  - what about the general indifferentiability model?
    is a constant number of rounds sufficient?

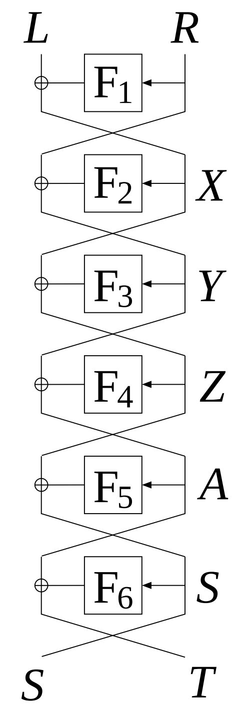
5 rounds are not enough

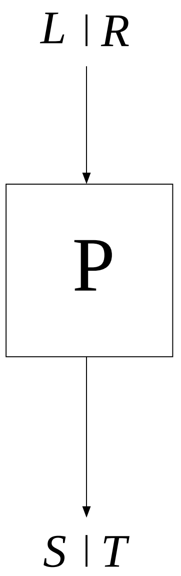




indifferentiability of the 6R Luby-Rackoff construction

- **Theorem:** The Luby-Rackoff construction with 6 rounds is (q, t_S, q_S, ϵ)-indifferentiable from a random permutation, with $t_S, q_S = \mathcal{O}(q^4)$ and $\epsilon = 2^{18}q^8/2^n$.
- prepending a k-bit key to the random oracle calls yields a construction indifferentiable from an ideal cipher
- to prove this result, we will construct a simulator for the inner random oracles $F_1, \ldots, F_6$ such that the resulting Feistel scheme "matches" the random permutation P



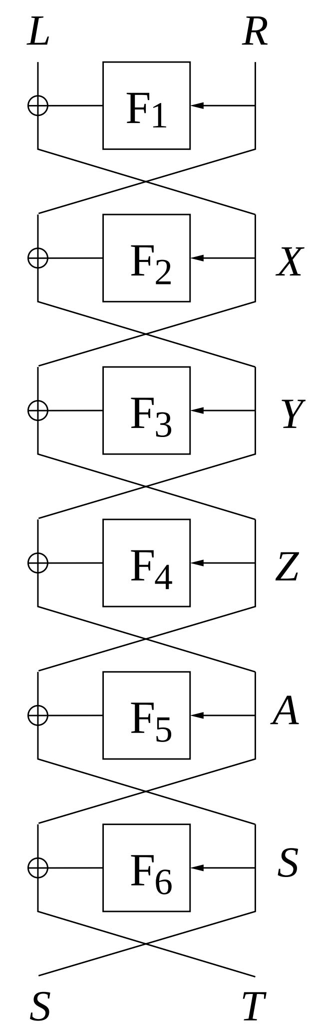


the simulation strategy

- $\mathcal{S}$ must anticipate future queries of the distinguisher; when does it have to react?
- definition: a k-chain, $k > 2$, $(x_i, x_{i+1}, \ldots, x_{i+k-1})$ is a sequence of round values such that

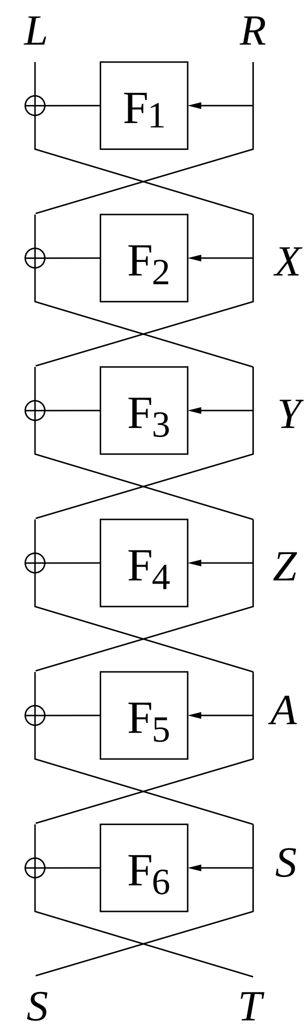
$$x_{i+2} = F_{i+1}(x_{i+1}) \oplus x_i$$
$$\vdots$$
$$[\quad x_{j+1} = \mathcal{P}(x_j \| x_{j-1} \oplus F_j(x_j))_{\text{right}} \quad]$$
$$\vdots$$
$$x_{i+k-1} = F_{i+k-2}(x_{i+k-2}) \oplus x_{i+k-3}$$

- waiting for 5-chains or 4-chains: to late
- reacting on 2-chains: to early (exponential simulator runtime)
- $\Rightarrow$ reacting on 3-chains



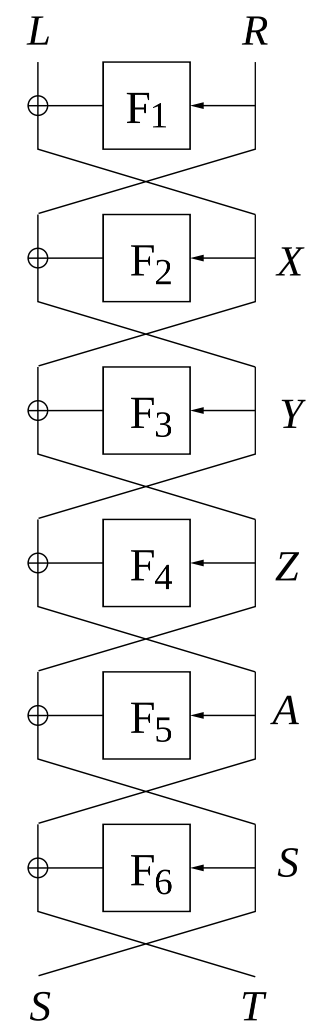
simulation: adapting 3-chains

- the simulator maintains an history of already defined F_i values
- F_i values are defined randomly, and 3-chains are completed to match the random permutation $\mathcal{P}$
- for example, on a query X to F_2:
  - there's a "downward" 3-chain if there are Y in F_3's history and Z in F_4's history such that $X = F_3(Y) \oplus Z$
  - there's an "upward" 3-chain if there are R in F_1's history and S in F_6's history such that $\mathcal{P}(X \oplus F_1(R) \| R) = S \| T$ for some T



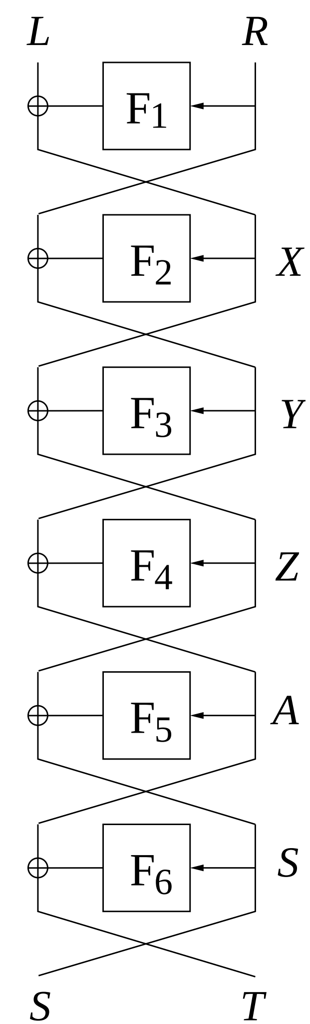
simulation: adapting 3-chains

- example with a query X to F_2:
  - $F_2(X) \xleftarrow{\$} \{0,1\}^n$
  - look in F_3 and F_4 history if there are Y and Z such that $X = F_3(Y) \oplus Z$
  - $R = Y \oplus F_2(X)$, $F_1(R) \xleftarrow{\$} \{0,1\}^n$, $L = X \oplus F_1(R)$
  - query $S\|T = \mathcal{P}(L\|R)$
  - $A = Y \oplus F_4(Z)$
  - adapt $F_5(A) \leftarrow Z \oplus S$ and $F_6(S) \leftarrow A \oplus T$
- what could go wrong:
  - "chain reaction" leading to exponential running time
  - impossibility to adapt a round value: $\mathcal{S}$ aborts



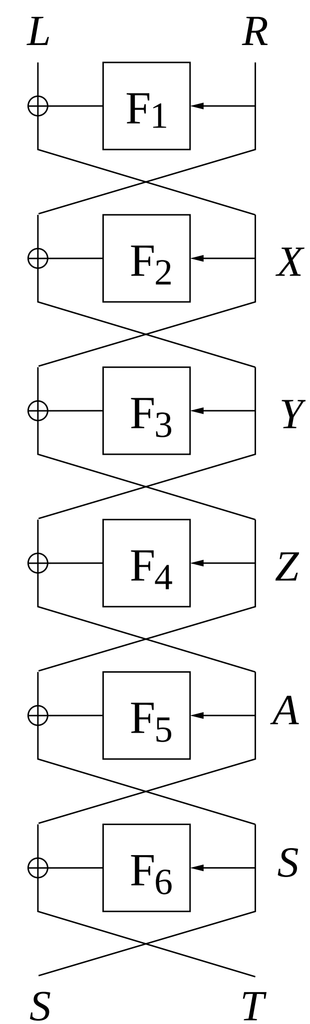
the simulator

Query	Direction	History	Call	Compute	Adapt
F_1	-	(F_6, F_5)	F_4	$S\|\|T$	(F_3, F_2)
F_1	+	(F_2, F_3)	F_4	$L\|\|R$	(F_5, F_6)
F_2	-	(F_1, F_6)	F_5	$L\|\|R$	(F_4, F_3)
F_2	+	(F_3, F_4)	F_1	$L\|\|R$	(F_5, F_6)
F_3	-	(F_2, F_1)	F_6	$L\|\|R$	(F_5, F_4)
F_3	+	(F_4, F_5)	F_6	$S\|\|T$	(F_1, F_2)
F_4	-	(F_3, F_2)	F_1	$L\|\|R$	(F_6, F_5)
F_4	+	(F_5, F_6)	F_1	$S\|\|T$	(F_2, F_3)
F_5	-	(F_4, F_3)	F_6	$S\|\|T$	(F_2, F_1)
F_5	+	(F_6, F_1)	F_2	$S\|\|T$	(F_3, F_4)
F_6	-	(F_5, F_4)	F_3	$S\|\|T$	(F_2, F_1)
F_6	+	(F_1, F_2)	F_3	$L\|\|R$	(F_4, F_5)



the simulator

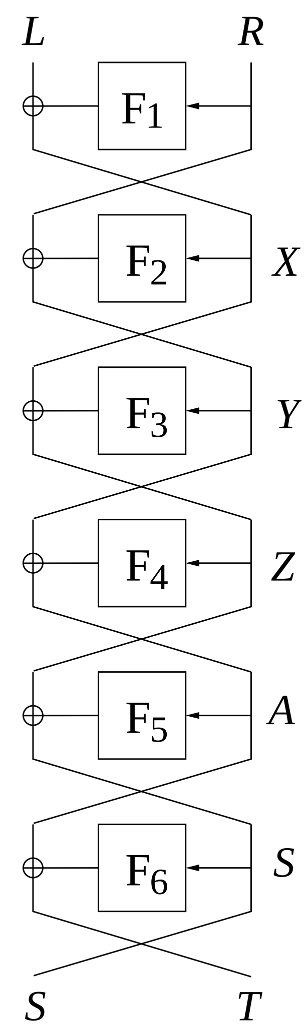
Query	Direction	History	Call	Compute	Adapt	involves $\mathcal{P}$
F_1	-	(F_6, F_5)	F_4	$S\|T$	(F_3, F_2)	Y
F_2	-	$(F_1, \tilde{F}_6)$	F_5	$L\|R$	(F_4, F_3)	Y
F_2	+	(F_3, F_4)	F_1	$L\|R$	(F_5, F_6)	
F_3	+	(F_4, F_5)	F_6	$S\|T$	(F_1, F_2)	
F_4	-	(F_3, F_2)	F_1	$L\|R$	(F_6, F_5)	
F_5	-	(F_4, F_3)	F_6	$S\|T$	(F_2, F_1)	
F_5	+	$(F_6, \tilde{F}_1)$	F_2	$S\|T$	(F_3, F_4)	Y
F_6	+	(F_1, F_2)	F_3	$L\|R$	(F_4, F_5)	Y



- **fact:** the total number of calls to the four lines involving $\mathcal{P}$ is less than q, except with negligible probability
- **consequence 1:** $|F_3|$ and $|F_4| \leqslant 2q$, except with negligible probability

the simulator

Query	Direction	History	Call	Compute	Adapt	involves P
F_1	-	(F_6, F_5)	F_4	$S\|T$	(F_3, F_2)	Y
F_2	-	$(F_1, \tilde{F}_6)$	F_5	$L\|R$	(F_4, F_3)	Y
F_2	+	(F_3, F_4)	F_1	$L\|R$	(F_5, F_6)	
F_3	+	(F_4, F_5)	F_6	$S\|T$	(F_1, F_2)	
F_4	-	(F_3, F_2)	F_1	$L\|R$	(F_6, F_5)	
F_5	-	(F_4, F_3)	F_6	$S\|T$	(F_2, F_1)	
F_5	+	$(F_6, \tilde{F}_1)$	F_2	$S\|T$	(F_3, F_4)	Y
F_6	+	(F_1, F_2)	F_3	$L\|R$	(F_4, F_5)	Y



- **consequence 2:** the total number of calls to the four other lines is less than $4q^2$, except with negl. probability
- **consequence 3:** $|F_1|$, $|F_2|$, $|F_4|$ and $|F_6| \leqslant q + 4q^2$, except with negl. probability

sketch of the proof of the theorem

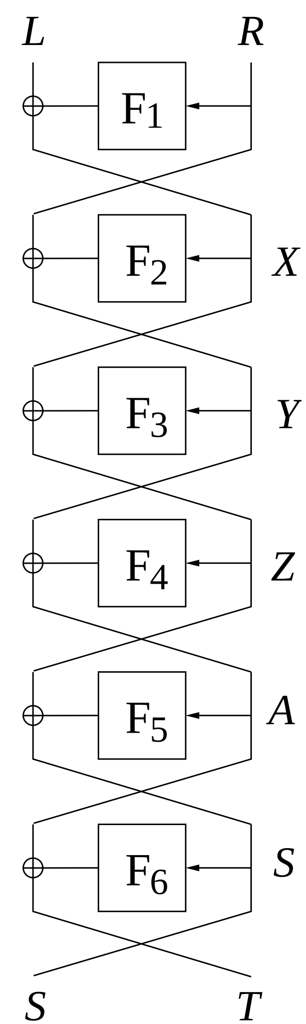
- we need to prove that:
  - the simulator runs in polynomial time: done, according to the previous analysis
  - the simulator aborts with negligible probability
  - its output is indistinguishable from the output of random functions

the simulator does not abort

- we must show that the values which are adapted are not already in the simulator history, except with negl. probability
- for this, we show that the inputs to be adapted are always randomly determined
- example with line $(F_1, -)$

Query	Direction	History	Call	Compute	Adapt
F_1	-	(F_6, F_5)	F_4	$S\|T$	(F_3, F_2)
F_3	+	(F_4, F_5)	F_6	$S\|T$	(F_1, F_2)
F_5	-	(F_4, F_3)	F_6	$S\|T$	(F_2, F_1)

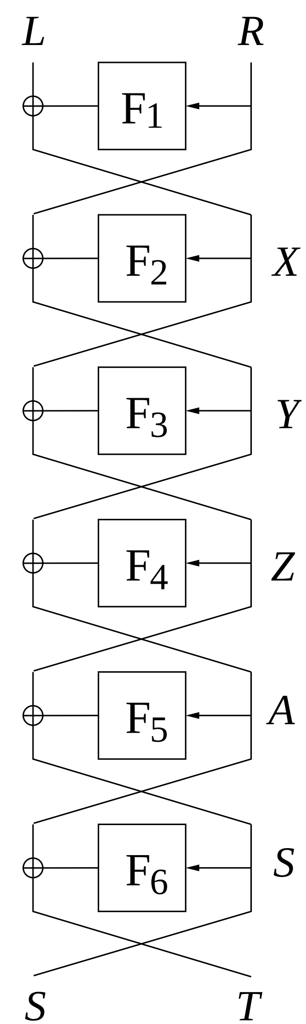
- complete proof: read the f*** paper



the simulator does not abort

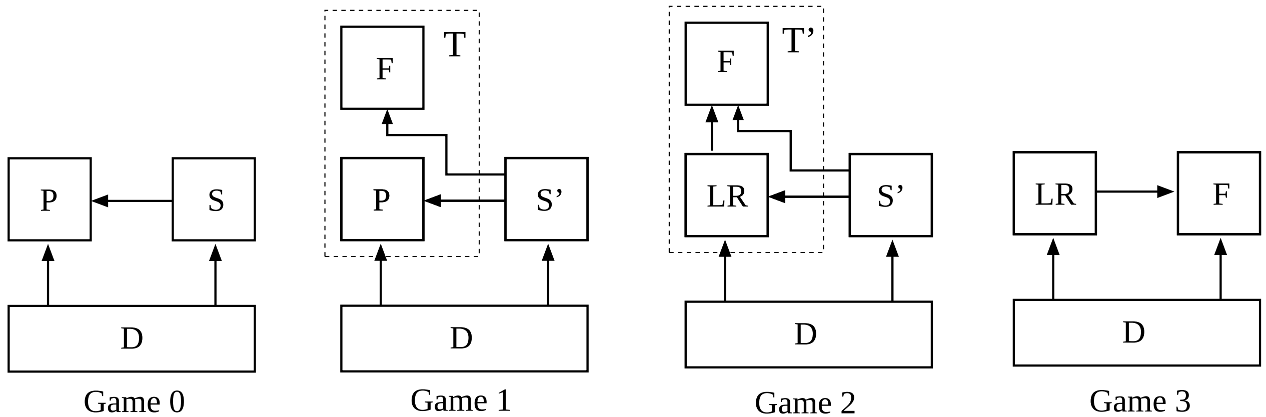
- we must show that the values which are adapted are not already in the simulator history, except with negl. probability
- for this, we show that the inputs to be adapted are always randomly determined
- example with line $(F_1, -)$

Query	Direction	History	Call	Compute	Adapt
F_1	-	(F_6, F_5)	F_4	$S\|\|T$	(F_3, F_2)
F_3	+	(F_4, F_5)	F_6	$S\|\|T$	(F_1, F_2)
F_5	-	(F_4, F_3)	F_6	$S\|\|T$	(F_2, F_1)



- complete proof: read the full paper

indifferentiability proof



- Game0 is the same as Game1
- Game2 is indistinguishable from Game3 unless $\mathcal{S}'$ aborts, which happens with negligible probability
- Game1 is indistinguishable from Game2:

$$\mathcal{LR}(L\|R) = (L \oplus r_1 \oplus r_3 \oplus r_5)\|(R \oplus r_2 \oplus r_4 \oplus r_6)$$

  - the output of $\mathcal{T}'$ always omits two consecutive values $r_i = \mathcal{F}_i(\cdot)$, $r_{i+1} = \mathcal{F}_{i+1}(\cdot)$ (the ones that are adapted by the simulator)

practical impacts

- example of the Phan-Pointcheval 3R-OAEP scheme:
  - in the random permutation model $\mathcal{P}$

$$\mathsf{Enc}_{pk}(m; r) = \mathsf{TOWP}_{pk}(\mathcal{P}(m\|r))$$

  - can be replaced in the ROM by a 3R Feistel scheme

$$s = m \oplus \mathcal{F}_1(r); \quad t = r \oplus \mathcal{F}_2(s); \quad u = s \oplus \mathcal{F}_3(t)$$
$$\mathsf{Enc}_{pk}(m; r; \rho) = \mathsf{TOWP}_{pk}(t\|u\|\rho)$$

- example of the Even-Mansour cipher: $E_{k_1,k_2}(m) = k_2 \oplus \mathcal{P}(m \oplus k_1)$
  - secure in the random permutation model $\mathcal{P}$
  - secure in the ROM model with a 4R Feistel scheme [GentryR04]
- a dedicated analysis will often enable to replace a random permutation by a Feistel scheme with < 6 rounds

open questions, ongoing work

- improve the tightness of the analysis
- best (exponential) attacks
- conjectured security $\Theta(\frac{q^2}{2^n})$
- weaker (but still useful) models of indifferentiability:
  - relation with the known-key "distinguishers" of Knudsen and Rijmen (Asiacrypt '07), correlation intractability
- minimal number of calls to the random oracle to build a random permutation: are there constructions with < 6 calls to the RO?

conclusion

The 6-round Luby-Rackoff construction with public random inner functions is indifferentiable from a random permutation.

- our result says nothing about the rightfulness to replace an ideal cipher by AES, or a random oracle by SHAx
- now that it is proved that ROM $\simeq$ ICM, you may:
  - use the ICM with more confidence, since it isn't stronger than the more "standard" ROM
  - *or*, as pointed out by a reviewer, look at the ROM with even more defiance, since it leads to the "over ideal" ICM!!!

thanks for your attention!

comments $\vee$ questions?