On the Streaming Indistinguishability of a Random Permutation and a Random Function

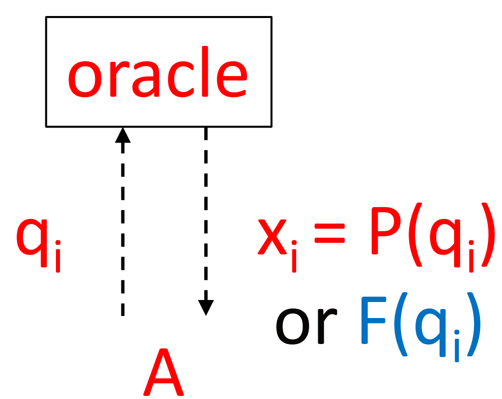
Itai Dinur

Ben-Gurion University

Eurocrypt 2020

"Switching Lemma" for Random Permutation\Function

- Classical problem: adversary A tries to **distinguish** a **random permutation** P:[N]->[N] from **random function** F:[N]->[N] with Q queries
- "Switching Lemma": A has **advantage** bounded by $O(Q^2/N)$
  - $|\Pr[A^{P(.)} = 1] - \Pr[A^{F(.)} = 1]| \in O(Q^2/N)$
- Widely used to establish concrete security of cryptosystems up to **birthday bound** of $Q = \sqrt{N}$
  - E.g., modes of operation (counter-mode)



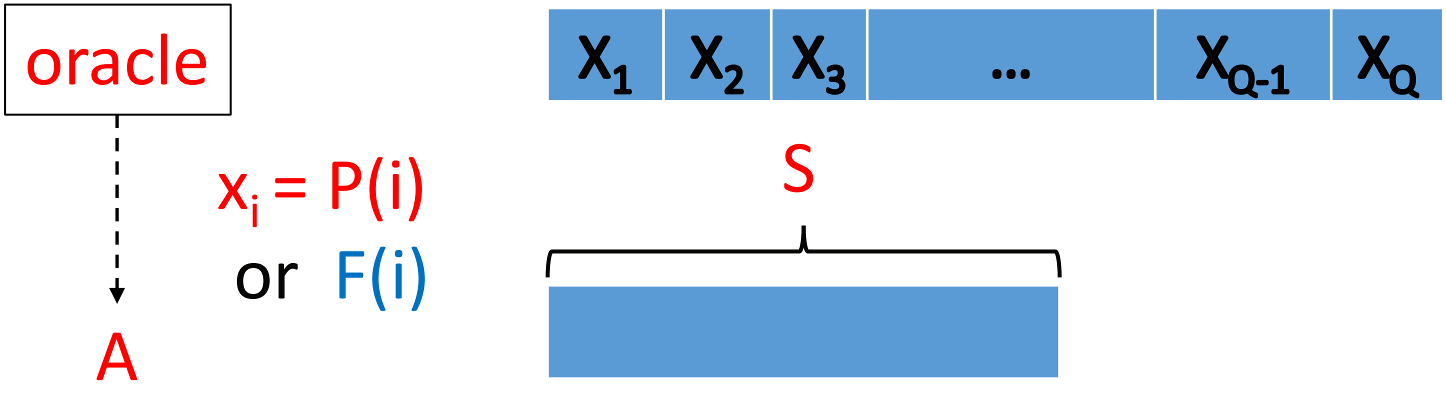
"Switching Lemma" for Random Permutation\Function

- "Switching Lemma": A has **advantage** bounded by $O(Q^2/N)$
  - $| \Pr[A^{P(.)} = 1] - \Pr[A^{F(.)} = 1] | \in O(Q^2/N)$
- Matching algorithm: **store** the Q query outputs and look for **collision** ($F(q_i) = F(q_j)$ for $q_i \neq q_j$)

X_1	X_2	X_3	…	X_{Q-1}	X_Q

Memory-Restricted Adversaries

- Algorithm requires **memory** ≈Q bits
- What about **memory-restricted** adversaries?
- Use **cycle detection algorithm** to obtain **optimal** $O(Q^2/N)$ advantage with ≈log(N) memory
- Requires **adaptive queries** to primitive
- What if adversary with S memory bits only given **stream** of Q elements produced by **random function\permutation**?
- Considered by Jaeger and Tessaro at EUROCRYPT 2019 [JT'19]



Streaming Switching Lemma [JT'19]

- "Streaming switching lemma" [JT'19]: adversary with S bits of memory with (1-pass) access to stream of Q elements from **random permutation\function** has distinguishing advantage of **at most** $\sqrt{Q \cdot S/N}$

- Application: better **security bounds** against **memory-restricted** adversaries for some modes of operation

Streaming Switching Lemma [JT'19]

- Application: better **security bounds** against **memory-restricted** adversaries for some modes of operation
- AES-based counter-mode:
- m_i encrypted to $(r_i , c_i = AES_K(r_i) \oplus m_i)$ for uniform r_i
- Eavesdropping adversary sees stream $(r_1 , c_1), (r_2 , c_2),\ldots$

- **Replace** AES by random P +
  apply streaming switching lemma (several times):
- show $(r_1 , c_1), (r_2 , c_2),\ldots$ Indistinguishable from
- $(r_i, \alpha_i) , (r_i , \alpha_i),\ldots$ for uniform α_i

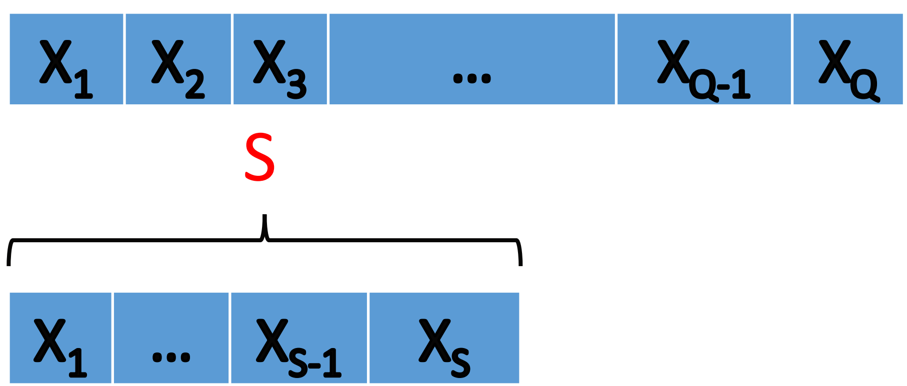
Streaming Switching Lemma

- “Streaming switching lemma“ [JT’19]: adversary with S bits of memory with access to stream of Q elements from **random permutation\function** has distinguishing advantage of **at most** $\sqrt{Q \cdot S/N}$
- Application: if S is limited, counter-mode secure **beyond birthday bound**

- Limitations of [JS’19]:
- 1) Proof based on unproven combinatorial **conjecture**
- 2) Bound $\sqrt{Q \cdot S/N}$ **not tight** when $Q \cdot S \ll N$
  - E.g., when $S = Q$, bound is $\sqrt{Q^2/N}$, but (original) switching lemma gives Q^2/N

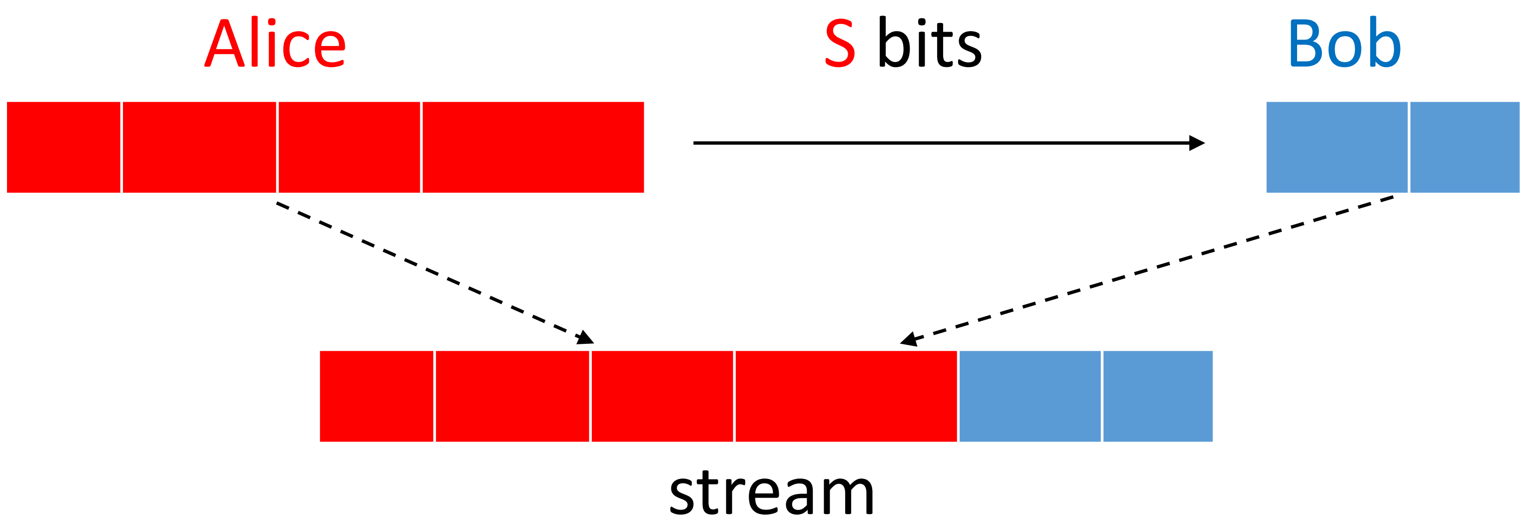
New Streaming Switching Lemma

- In this work: overcome limitations
- **New** streaming switching lemma bound $O(\log Q \cdot Q \cdot S/N)$
- **Tight** (up to poly-log factors):
  - Algorithm: store **first** S elements and look for collision with Q elements
  - Advantage: $\approx Q \cdot S/N$
- Note: when $S = Q$, we get (original) switching lemma



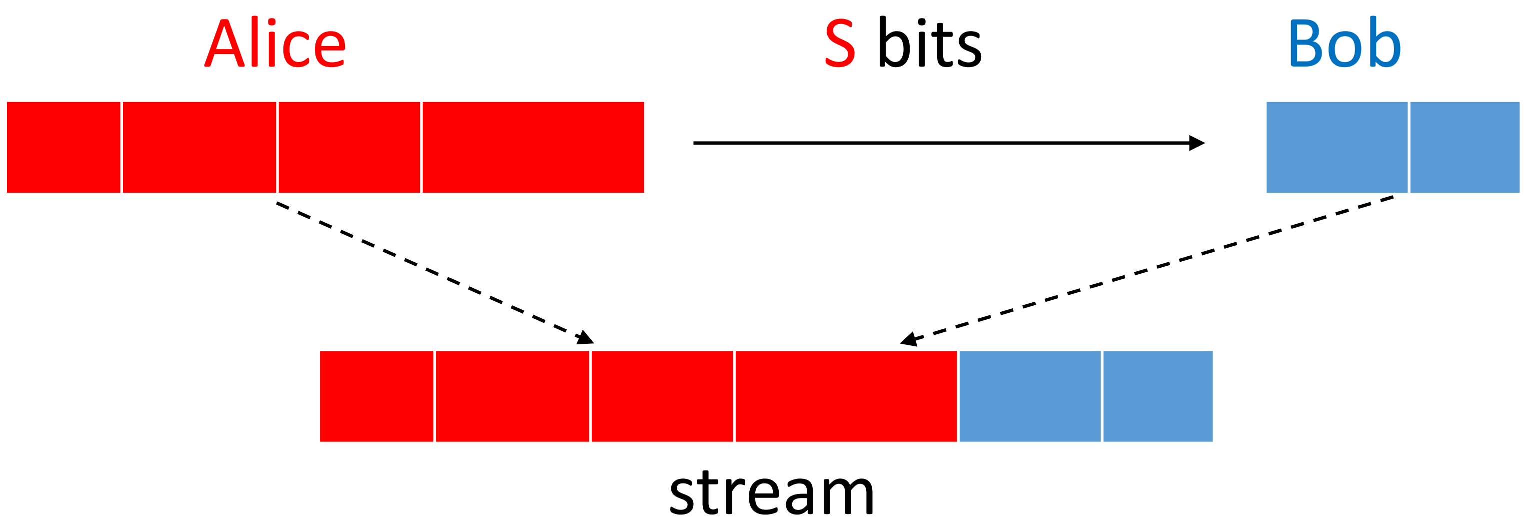
CC → Streaming

- Main idea: **reduce** from **communication complexity** (**CC**) problem (with **strong lower bounds**) to streaming
- General reduction framework from **one-way** CC problem:
  - Alice, Bob **solve CC problem** given access to **streaming** algorithm:
  - View concatenated inputs as stream
  - Alice **simulates** streaming algorithm on her input, **passes state** to Bob which continues simulation, outputs result



CC → Streaming

- Streaming algorithm with **memory** S gives **one-way** communication protocol with communication **cost** S (and **same advantage**)
- Lower bound on **cost** of communication protocol → lower bound on **memory** of streaming algorithm



Reduction Attempt for Random Permutation\Function

- Attempt: CC problem – each player gets Q/2 elements, chosen using rand permutation\function
- Useless: CC problem is **easy**
  - E.g., if $Q > \sqrt{N}$, players can **trivially distinguish** between permutation\function with **no communication**
  - Each player has **unlimited resources** and can detect a collision locally

Alice

$x_1,\ldots,x_{Q/2}$

Bob

$x_{Q/2+1},\ldots,x_Q$

Reduction Attempt for Random Permutation\Function

- General restriction: in **hard CC problem** joint distributions for Alice and Bob's inputs should have **identical marginals**
  - Alice and Bob should have same **local view**
- **Impossible** when considering rand permutation\function distributions

- Solution: use **hybrid argument**
  - Consider **intermediate hybrid distributions** between random permutation and random function
  - Prove indistinguishability of **neighboring hybrid distributions** by reduction from CC

Hybrid Argument

- Attempt: define Q hybrids games
  - Game i: $x_1, \ldots \boldsymbol{x_{Q-i}}, x_{Q-i+1}, \ldots, x_Q$ or $x_1, \ldots x_{Q-i-1}, \boldsymbol{x_{Q-i}}, \ldots, x_Q$

    w\o replacement w replacement   w\o replacement w replacement

- (Standard) hybrid argument **far from tight**
  - (Distinguishing advantage) x (num of hybrids) **too large**

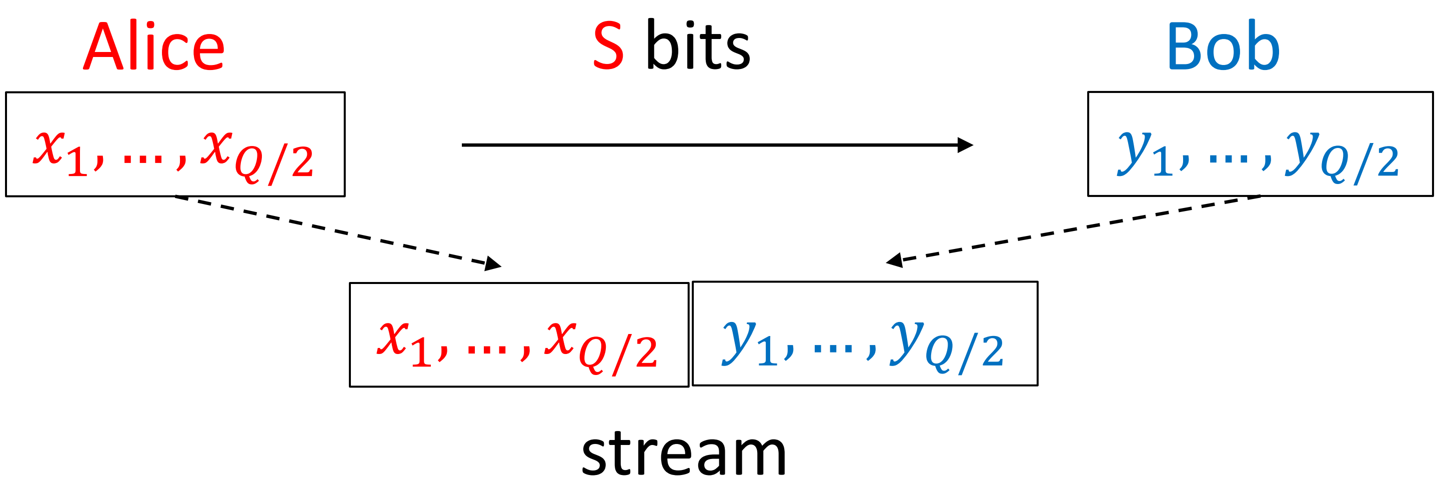
Improved Hybrid Argument

- Main idea: break dependency between **halves**
- Denote 1st sequence by $x_1, x_2, \ldots, x_{Q/2}, y_1, y_2, \ldots, y_{Q/2}$
- 1st distribution: elements chosen using (**same**) **permutation**
- 1st **intermediate** hybrid: $x_1, x_2, \ldots, x_{Q/2}$ and $y_1, y_2, \ldots, y_{Q/2}$ chosen using **independent permutations**

- Reduction from (one-way) CC:
- Alice gets 1st half of sequence, Bob gets 2nd half (decide if they obtain **same** or **independent** permutations)
  - Marginals are identical

Permutation Dependence

- (one way) CC problem - **permutation dependence** (**PDEP**):
- Alice and Bob decide if their inputs were drawn using **same** or **independent** permutations
- **PDEP** to **streaming** reduction:



UDISJ-> PDEP

- Communication **cost** \ **advantage** tradeoff for **PDEP**?
- Reduction from (unique) **disjointness (UDISJ)**
  - Each player receives a set of size n (domain size *O*(n)), need to decide if sets **intersect** or **disjoint**
- Theorem (informal)[BM'13, GW'14]**:** if Alice and Bob communicate c bits for **DISJ** (**UDISJ**) in the **worst case**, their **max advantage** is *O*(c/n)
  - Even when given access to **public randomness**

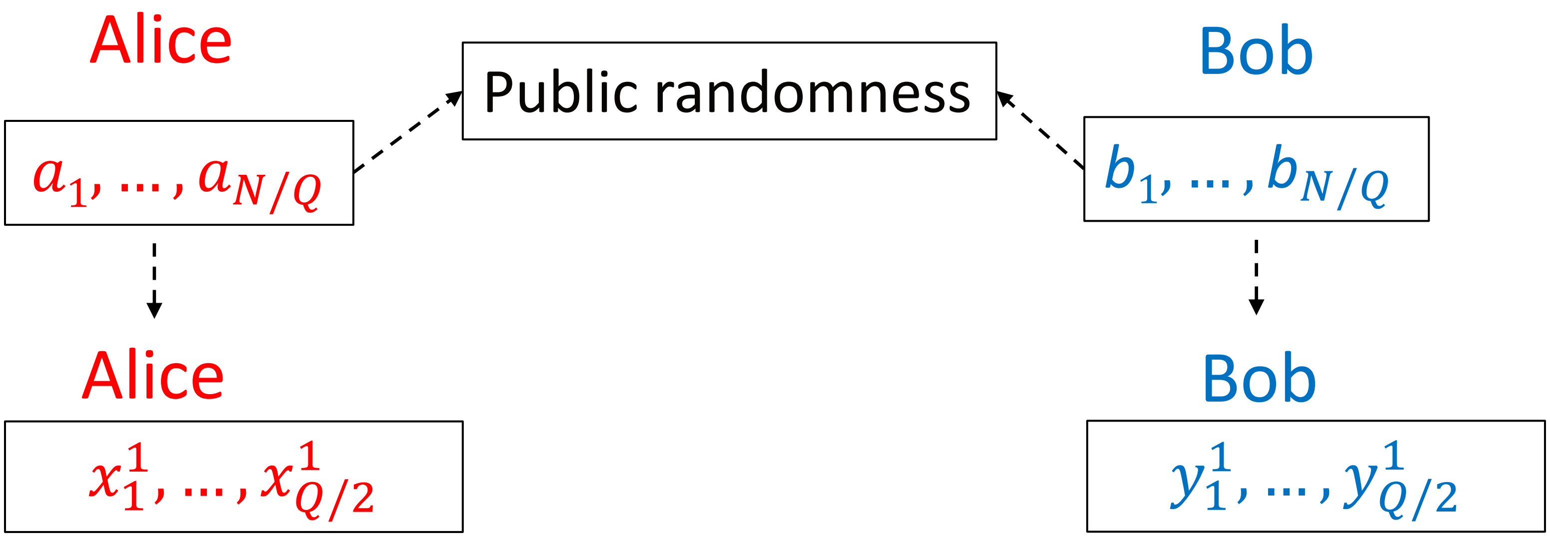
Alice

$a_1, \ldots, a_n$

Bob

$b_1, \ldots, b_n$

UDISJ-> PDEP



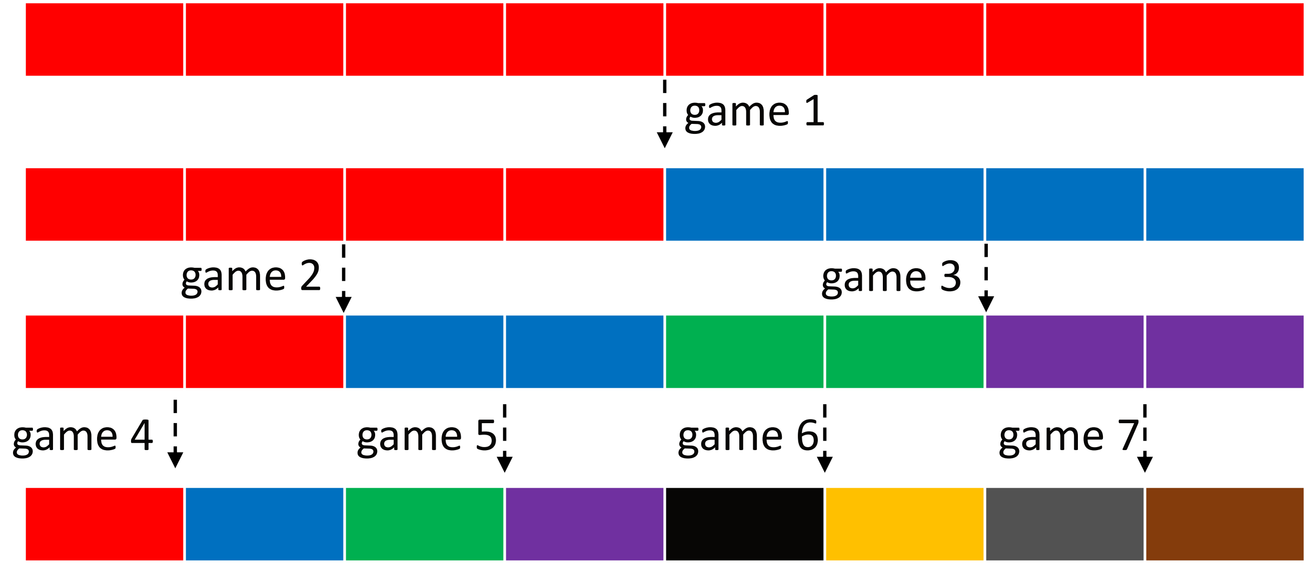
- Theorem (informal): there is a public coin **local** reduction that converts a **UDISJ** instance of size n=N/Q to a **PDEP** instance of size Q
  - **Shorter** inputs **harder** from **PDEP**, but **easier** for **UDISJ**
- Overall: UDISJ -> PDEP-> streaming

  bounds **max advantage** for hybrid game by

  $O(c/n) = O(S/(N/Q)) = O(Q \cdot S/N)$

The Full Hybrid Argument

- Once dependency between 2 halves broken:
  - Continue recursively (tree structure)
- 2'nd level: 2 games of distinguishing stream distributions on Q/2 elements
- Final distribution: Q elements divided into Q independent permutations == random function
- **Max advantage** for each level: $O(Q \cdot S/N)$
- **Total** max advantage: $O(\log Q \cdot Q \cdot S/N)$



Conclusions

- **New** streaming switching lemma bound $O(\log Q \cdot Q \cdot S/N)$
- **Tight** up to poly-log factors
- Reduction from CC to streaming uses **unconventional** hybrid argument
- Standard streaming problems defined in **worst case setting**
  - Gives **freedom to choose** hard distributions for CC problem
- In our (cryptographic) setting **streams distributions fixed**
  - Hybrid argument reduction applicable to more problems?
- Extension: **multi-pass** streaming switching lemma
  - Streaming alg allowed multiple passes over data

Thanks for your attention!