RSA Conference 2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: CRYP-W03

Lossy Trapdoor Permutations with Improved Lossiness

Benedikt Auerbach

Ruhr University Bochum

#RSAC

Agenda

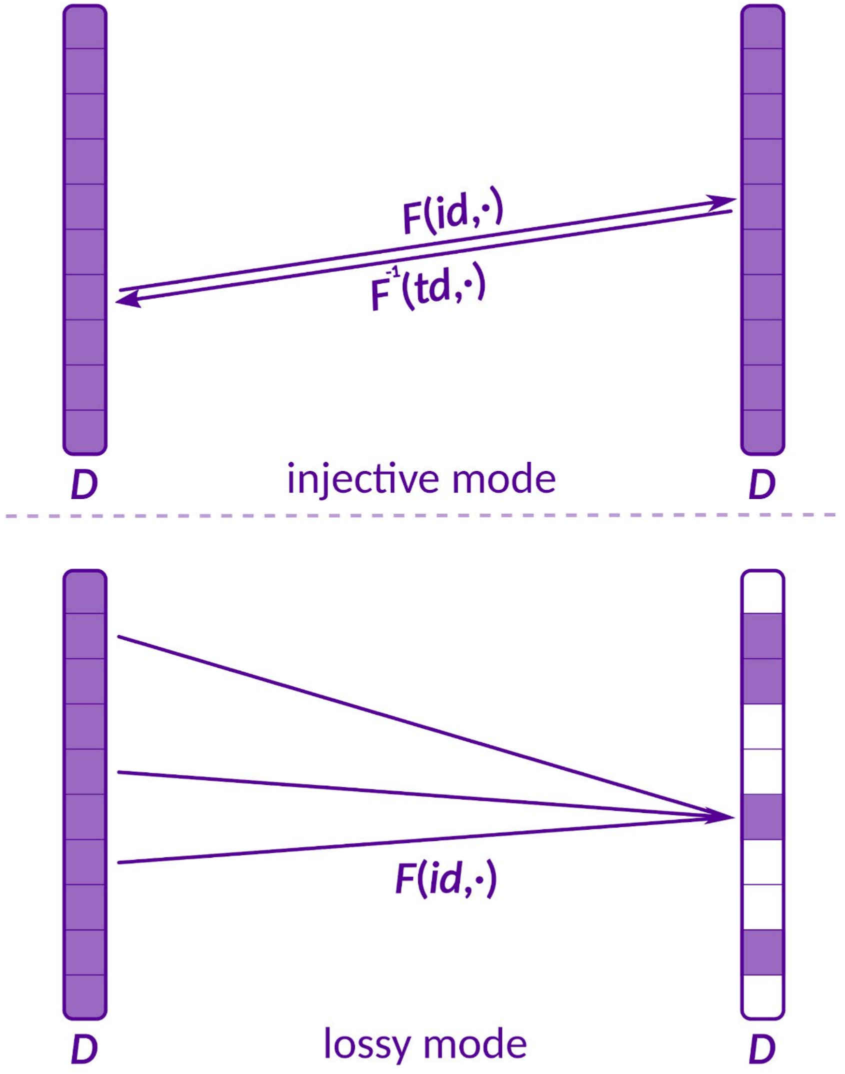
- Index-dependent and index-independent lossy trapdoor permutations
  - Lossy trapdoor permutations
  - From index-dependence to index-independence
  - Instantiations in the RSA setting
- An all-but-one lossy trapdoor permutations from Phi-hiding
  - All-but-one lossy trapdoor permutations
  - Prime family generators
  - Instantiation from Phi-hiding

Lossy Trapdoor Permutations

Lossy Trapdoor Permutations (LTP)
Index-independent Domains [PeiWat08]

Syntax

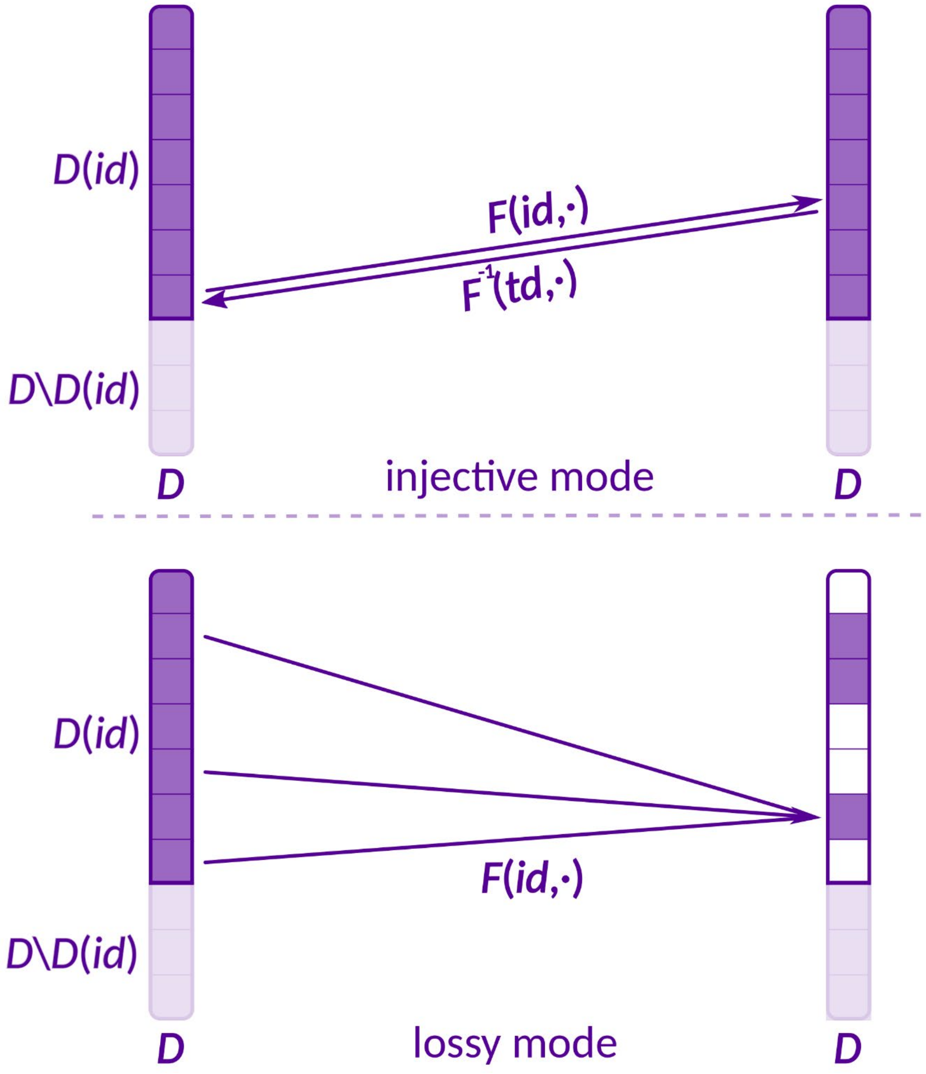
- Instance Generation
  - Injective mode: $(id,td) \longleftarrow Gen(1)$
  - Lossy mode: $(id,\perp) \longleftarrow Gen(0)$
- Domain D
- Function Evaluation
  - $F(id,\cdot): D \longrightarrow D$
- Function Inversion
  - $F^{-1}(td,\cdot): D \longrightarrow D$



Lossy Trapdoor Permutations (LTP)
Index-dependent Domains [FGKRS13]

Syntax

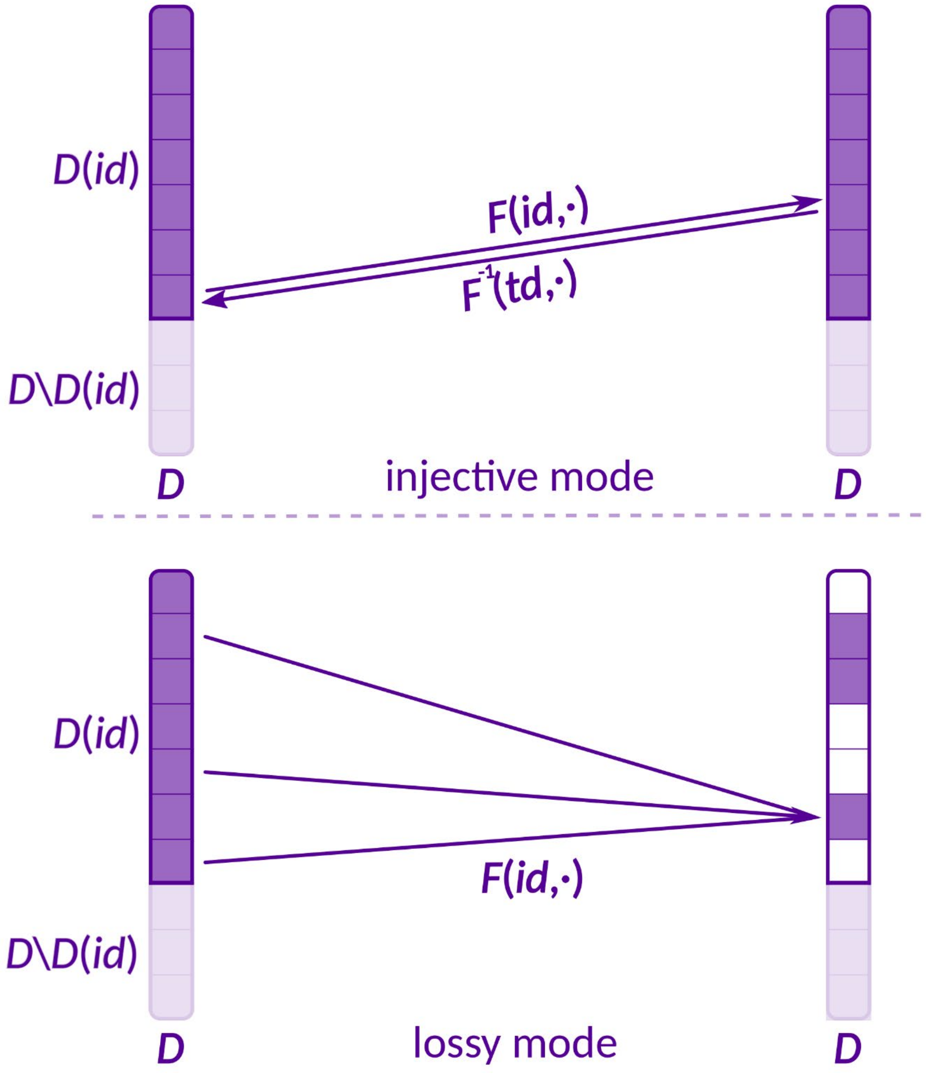
- Instance Generation
  - Injective mode: $(id,td) \longleftarrow Gen(1)$
  - Lossy mode: $(id,\perp) \longleftarrow Gen(0)$
- Domains $D(id) \subseteq D$
- Function Evaluation
  - $F(id,\cdot): D(id) \longrightarrow D(id)$
- Function Inversion
  - $F^{-1}(td,\cdot): D(id) \longrightarrow D(id)$



Lossy Trapdoor Permutations (LTP)
Index-dependent Domains [FGKRS13]

Example: LTP from Phi-Hiding

- Instance Generation
  - RSA modulus $id=(N,e)$, $td=(N,d)$
    - Injective mode: $\gcd(\varphi(N),e)=1$
    - Lossy mode: $e \mid \varphi(N)$
- Domains $D(id)=\mathbb{Z}/N\mathbb{Z}$, $D=[2^k]$
- Function Evaluation
  - $F(id,x)=x^e \bmod N$
- Function Inversion
  - $F^{-1}(td,y)=y^d \bmod N$



Lossy Trapdoor Permutations

Security Properties

I) Lossiness

- LTP is lossy with lossiness factor L if for all $(id,\perp) \longleftarrow Gen(0)$

$$|F(id,D(id))| \leq |D(id)| \; / \; L$$

- Example
  - $e \mid \varphi(N)$
  - Then $x \mapsto x^e \bmod N$ is roughly e-to-1

II) Lossy Mode $\approx_c$ Injective Mode

- id and *id’* computationally indistinguishable for
  - $(id,td) \longleftarrow Gen(1)$
  - $(id',\perp) \longleftarrow Gen(0)$

- Example
  - Equivalent to Phi-hiding assumption
  - $(N,e) \approx_c (N,e')$ where $\gcd(\varphi(N),e)=1$, $e' \mid \varphi(N)$

Applications

- Applications of LTPs
  - One-way functions
  - CPA-secure encryption
  - CCA-secure encryption
  - Hedged encryption
  - …
- Some of the constructions require index-independence

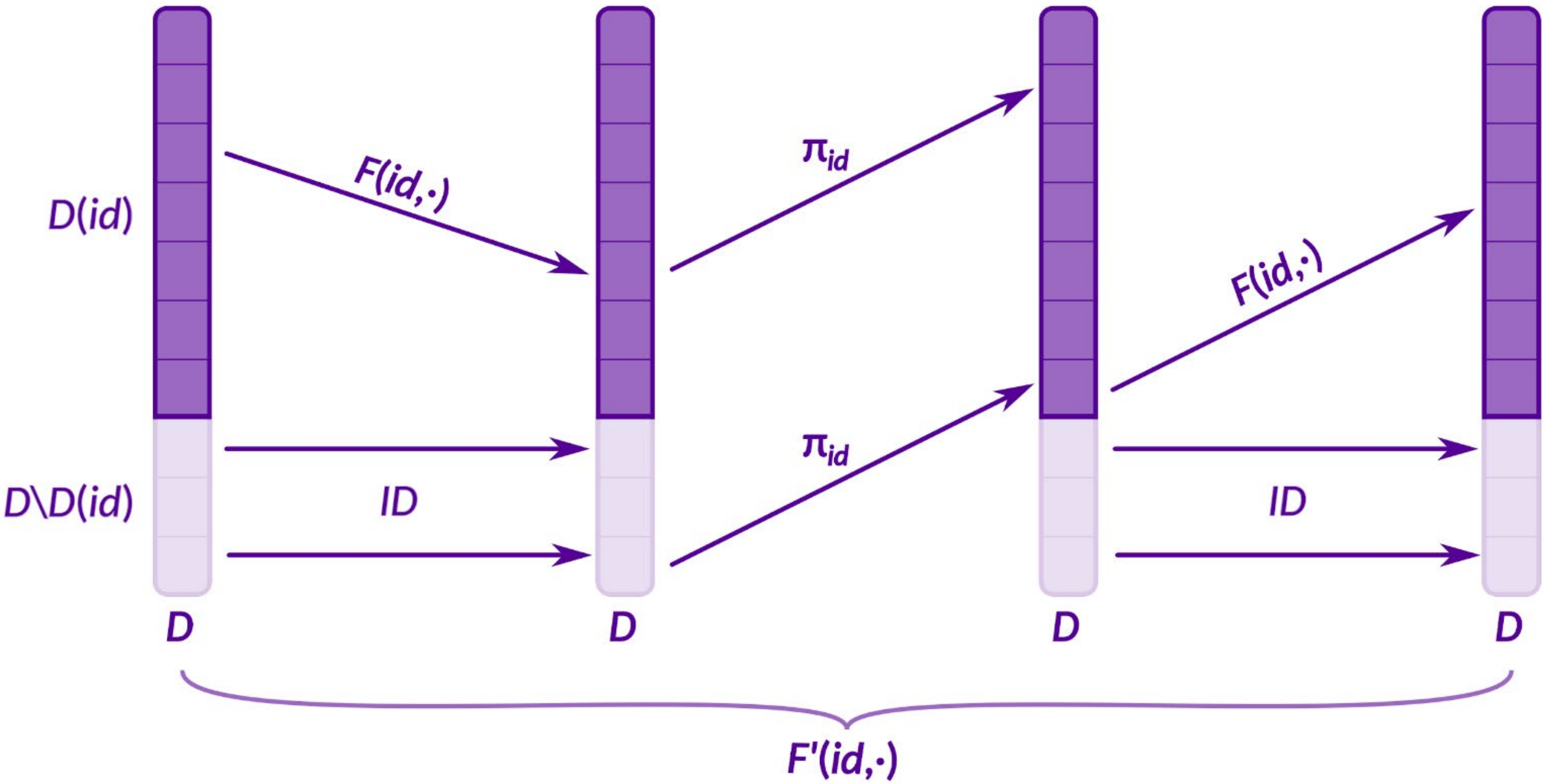
RSAConference2019

From Index-dependence to Index-independence

From Index-dependence to Index-independence

- Give transformation from index-dep. LTP to index-indep. LTP
  - Generalization of construction from [HOT04] for extending range of RSA one-way permutation
- Transformation
  - In:
    - LTP (Gen,F,F^{-1}) with index-dependent domains $D(id)\subseteq D$
    - Permutation family π_{id}: $D \longrightarrow D$ with $\pi_{id}(D\backslash D(id))\subseteq D(id)$
  - Out:
    - LTP (Gen',F',F'^{-1}) with index-independent domain D
  - Instance Generation: $Gen'=Gen$

From Index-dependence to Index-independence



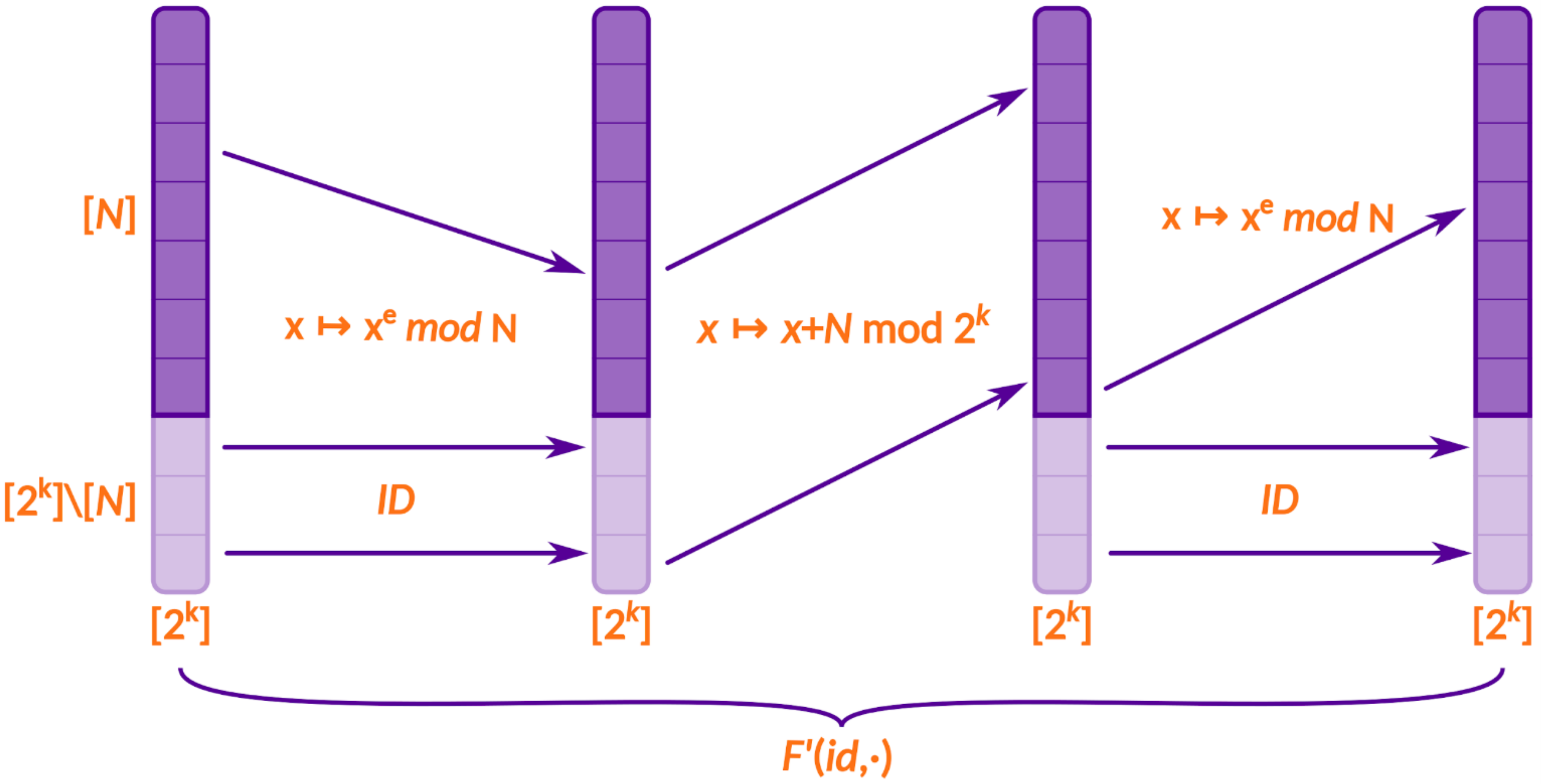
Working principle of function evaluation

From Index-dependence to Index-independence

Security of the construction

- Correctness: ✓
- Lossy mode $\approx_c$ injective mode: ✓
- Lossiness:
  - Theorem: *If* (Gen, F, F^{-1}) *is* L*-lossy then* $(Gen', F', F^{-1\prime})$ *is* $L/2$*-lossy*
  - Idea behind construction: Every element of D is permuted with $F(id,\cdot)$ at least once

From Index-dependence to Index-independence



Example: Index-independent LTP from Phi-hiding

Instantiations

- Comparison to the index-indep. LTPs from [FGKRS13]:

Assumption	D	$D(id)$ (index-dep.)	L [FGKRS13]	L (our transform)
Phi-hiding	$[2^k]$	$\mathbb{Z}/N\mathbb{Z}$	2	$2^{k/4}$
Quadratic Residuosity	$[2^k]$	$\mathbb{Z}/N\mathbb{Z}$	4/3	2
Composite Residuosity	$[2^{k(s+1)}]$	$\mathbb{Z}/N^{s+1}\mathbb{Z}$	$2^{(k-1)s-k/2-1}$	$2^{(k-1)s-2}$

RSA Conference 2019

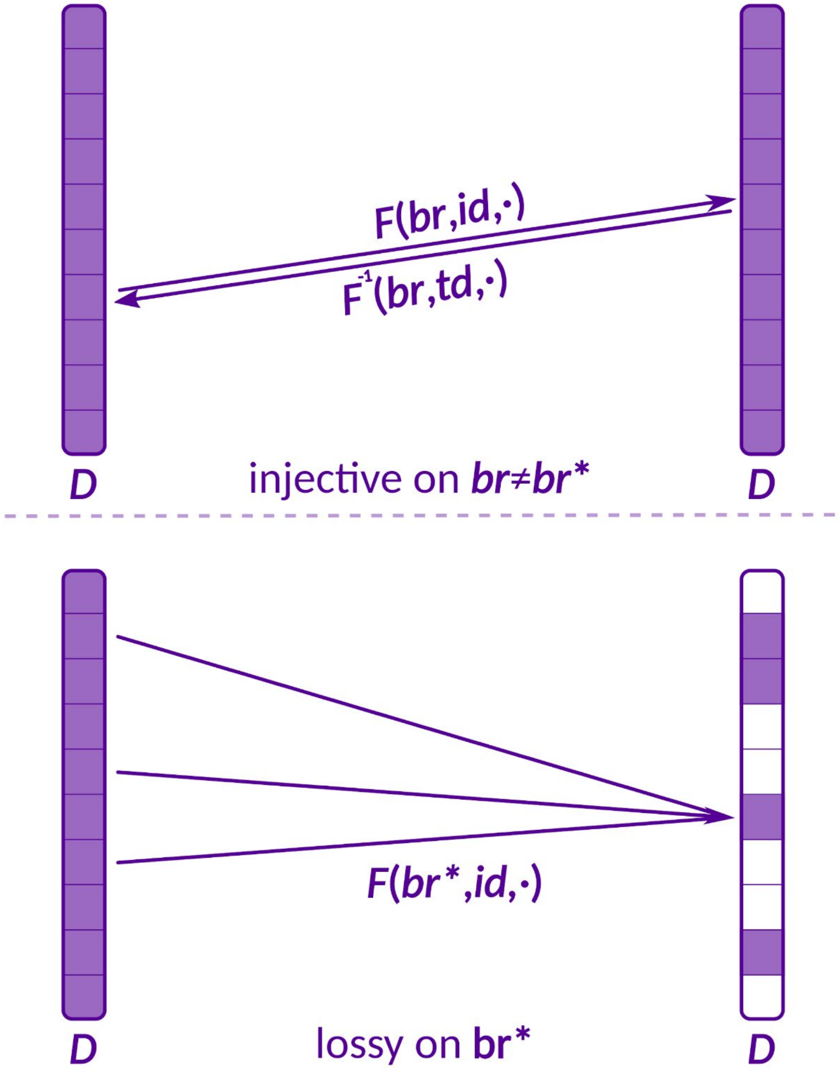
An All-but-one Lossy Trapdoor Permutation from Phi-hiding

All-but-one Lossy Trapdoor Permutations

Index-independent Domains [PeiWat08]

Syntax

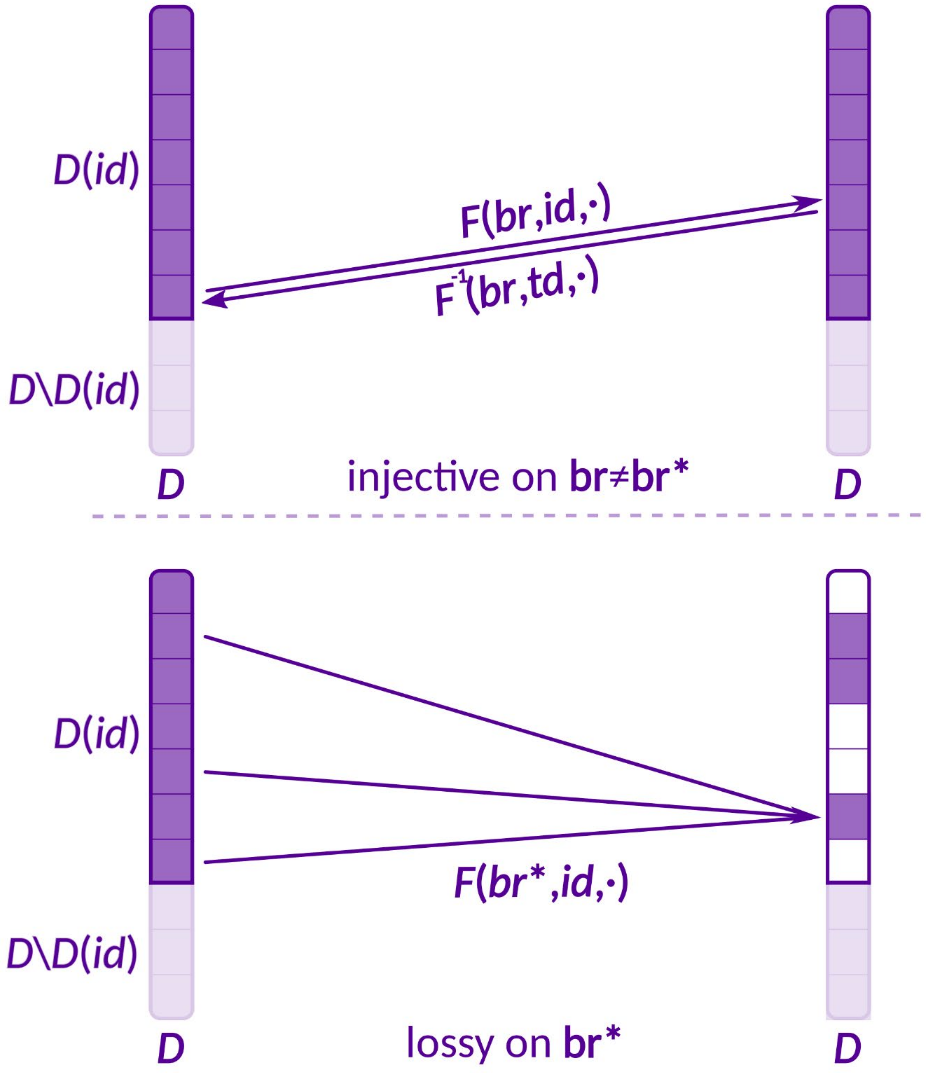
- Branch set *Br*
- Instance generation
  - Pick branch $br^* \in Br$
  - Instance $(id,td) \longleftarrow Gen(br^*)$
- Domain *D*
- Function evaluation
  - $F(br,id,\cdot): D \longrightarrow D$
- Function inversion (for $br \neq br^*$)
  - $F^{-1}(br,td,\cdot): D \longrightarrow D$



All-but-one Lossy Trapdoor Permutations
Index-dependent Domains

Syntax

- Branch set Br
- Instance generation
  - Pick branch $br^* \in Br$
  - Instance $(id, td) \longleftarrow Gen(br^*)$
- Domains $D(id) \subseteq D$
- Function evaluation
  - $F(br, id, \cdot): D(\mathrm{id}) \longrightarrow D(\mathrm{id})$
- Function inversion (for $br \neq br^*$)
  - $F^{-1}(br, td, \cdot): D(\mathrm{id}) \longrightarrow D(\mathrm{id})$



All-but-one Lossy Trapdoor Permutations
Security

I) Lossy on *br**

- ABO is lossy with lossiness factor L: For all br^* and $(id,td) \longleftarrow Gen(br^*)$

$$|F(br^*,id,D(id))| \leq |D(id)| \,/\, L$$

II) Hidden Lossy Branch

- id and id' are computationally indistinguishable for
  - $(id,td) \longleftarrow Gen(br_0)$
  - $(id',td') \longleftarrow Gen(br_1)$

An ABO from Phi-hiding

Idea of our construction

- Branches $Br \sim \{p_1,\dots,p_m\}$ set of primes
- Instance generation
  - For branch p^* sample N s.t.
    - $p^* \mid \varphi(N)$
    - $\gcd(\varphi(N),p_i)=1$ for $p_i \neq p^*$
- Domains $D(id)=\mathbb{Z}/N\mathbb{Z}$

- Function evaluation
  - $F(p,N,x) = x^p \bmod N$
- Function inversion
  - $d=p^{-1} \bmod \varphi(N)$
  - $F^{-1}(p,N,x)=x^d \bmod N$

Prime Family Generators

- Problem: Cannot directly use $\{p_1,\ldots,p_m\}$
  - Inefficient
  - Restricts admissible RSA moduli N
- Solution: *Prime Family Generator* (PFG)
  - Maps $[m]$ to set of primes $\{p_1,\ldots,p_m\}$
  - Particular choice of p_i depends on seed sd
  - Recover i-th prime with algorithm $p_i \longleftarrow \mathrm{PGet}(sd,i)$
- Instantiation via d-wise independent hash functions
  - similar to construction from [CMS99]
  - different security properties

An ABO from Phi-hiding

Our construction

- Branches $Br=[m]$
- Instance generation for branch br^*
  - Sample sd for PFG
  - $p^* \longleftarrow \mathrm{PGet}(sd,br^*)$
  - Sample N such that
    - $p^* \mid \varphi(N)$
    - $\gcd(\varphi(N),p_{br})=1$ for $p_{br}\neq p^*$
  - $id=(sd,N)$, $td=(sd,N,\varphi(N))$
- Domains $D(id)=\mathbb{Z}/N\mathbb{Z}$

- Function evaluation $F(br,id,x)$
  - $p \longleftarrow PGet(sd,br)$
  - Return $x^p \bmod N$
- Function inversion $F^{-1}(br,td,y)$
  - $p \longleftarrow PGet(sd,br)$
  - $d=p^{-1} \bmod \varphi(N)$
  - Return $y^d \bmod N$

An ABO from Phi-hiding

Security of the construction

- Hidden lossy branch under a variant of Phi-hiding
- Lossiness factor $L=2^{k/4}$
- Index-independent variant via our transform

RSA Conference 2019

Summary

Summary

- From index-dependence to index-independence
  - We give a transform from index-dep. LTPs to index-indep. LTPs
    - Preserves indistinguishability
    - Preserves lossiness up to factor of 2
  - Applicable to several instantiations in the RSA setting
- An all-but-one lossy trapdoor permutation from Phi-hiding
  - First known construction from Phi-hiding
  - Builds on prime family generators