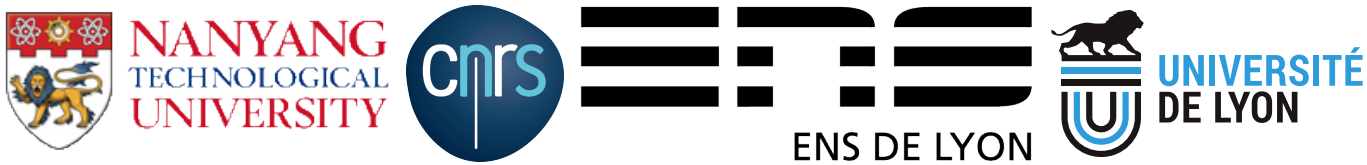
Adaptive Oblivious Transfer with Access Control from Lattice Assumptions

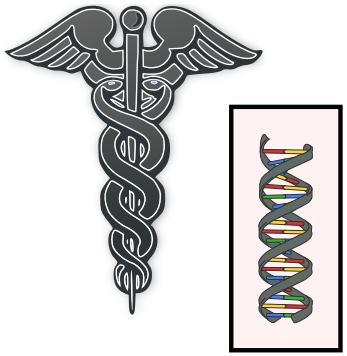
Benoît Libert[1,2] San Ling[3] **Fabrice Mouhartem**[1]
Khoa Nguyen[3] Huaxiong Wang[3]

[1]École Normale Supérieure de Lyon (France),
[2]CNRS (France),
[3]Nanyang Technological University (Singapore)

Asiacrypt, Hong Kong,
04/12/2017



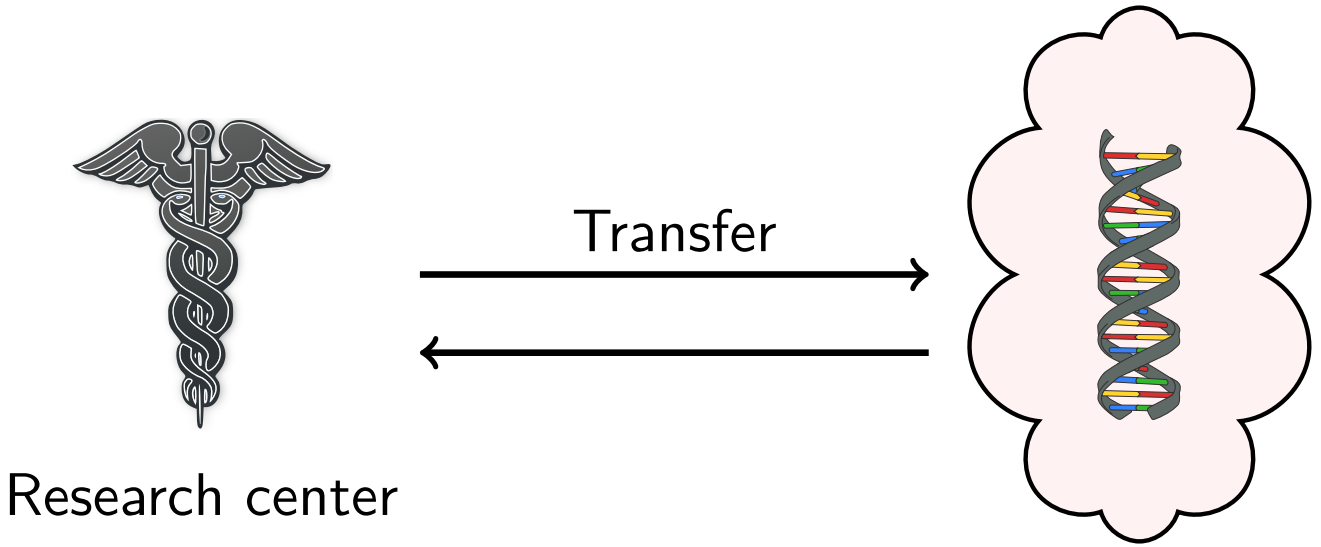
Anonymous Access to Remote Databases



Research center

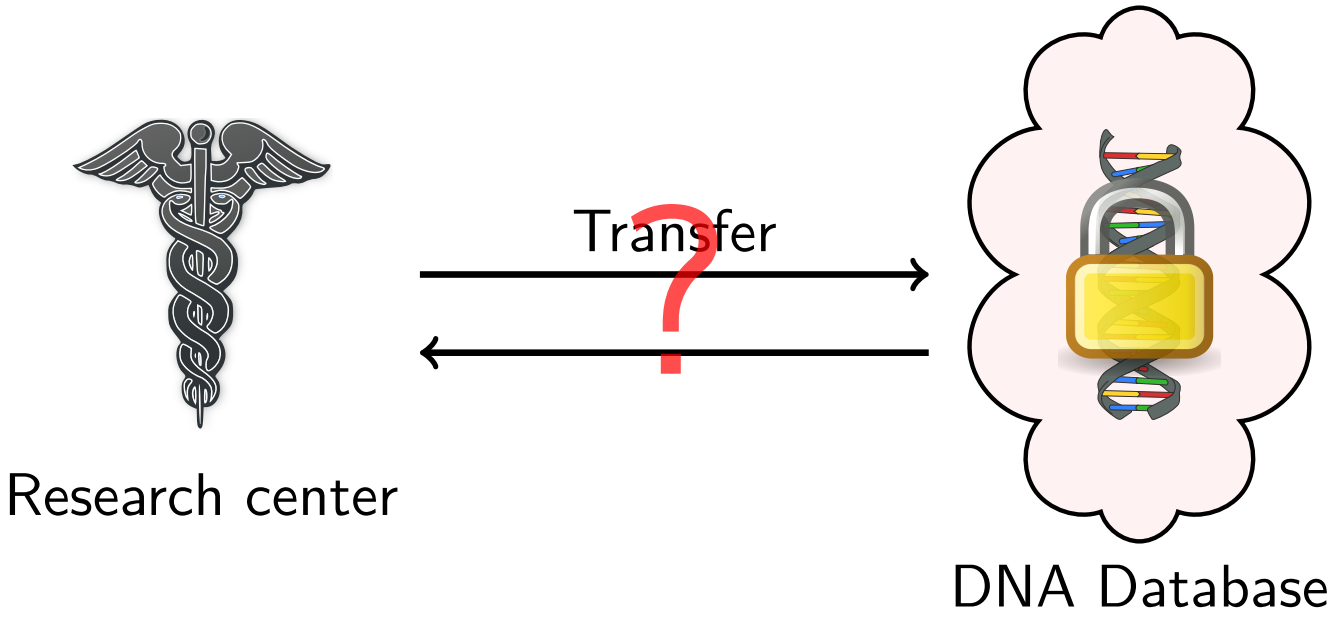
- DNA storage is expensive

Anonymous Access to Remote Databases



- DNA storage is expensive
- DNA database queries are sensitive information

Anonymous Access to Remote Databases

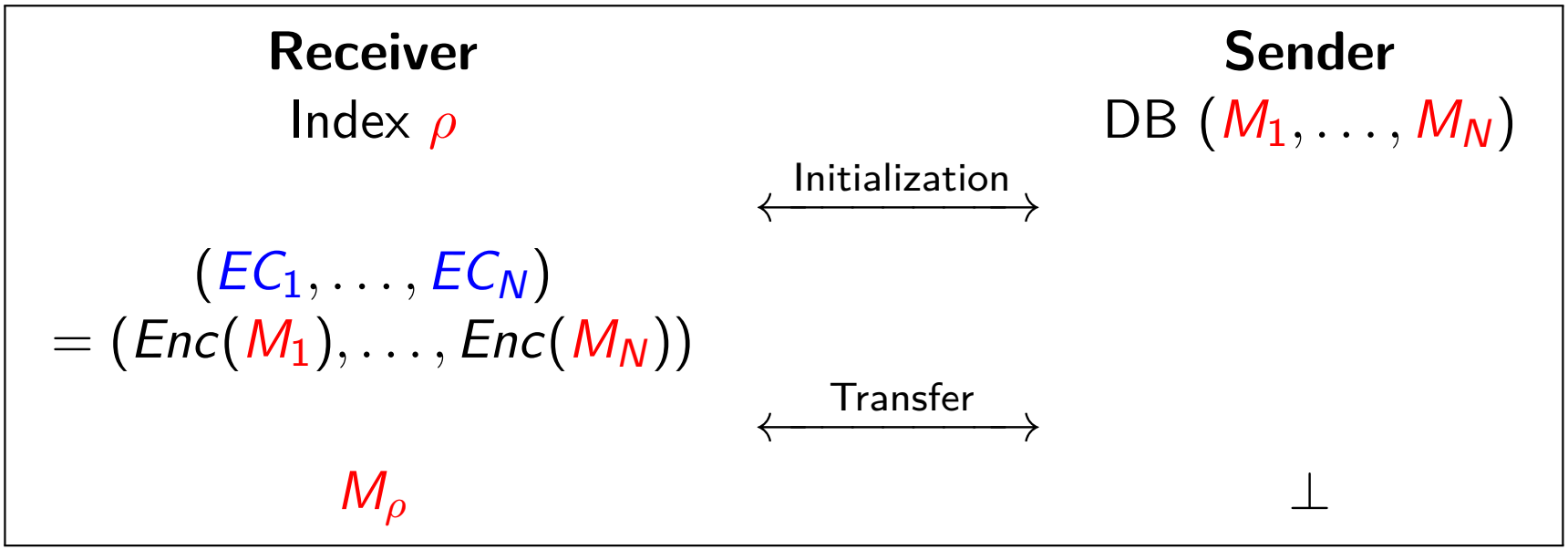


- DNA storage is expensive
- DNA database queries are sensitive information

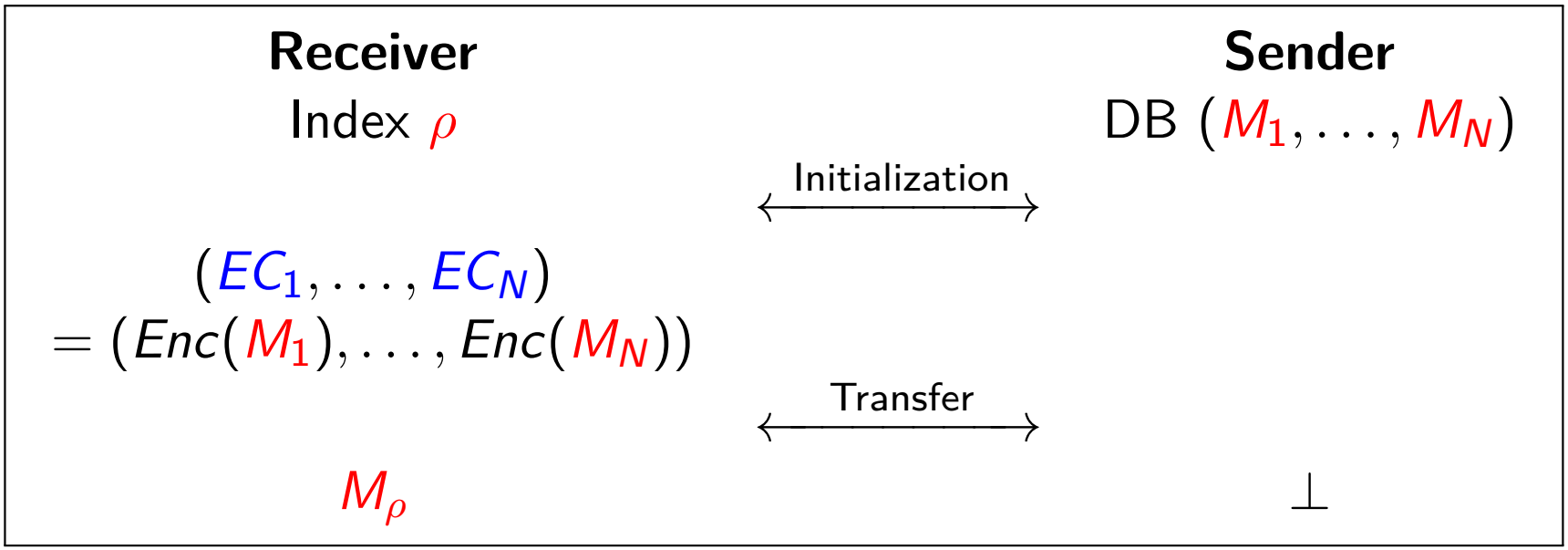
$\longrightarrow$ queries should be private (receiver security)

$\longrightarrow$ unqueried entries should remain hidden (receiver security)

(Adaptive) Oblivious Transfer (OT) [Rab81]

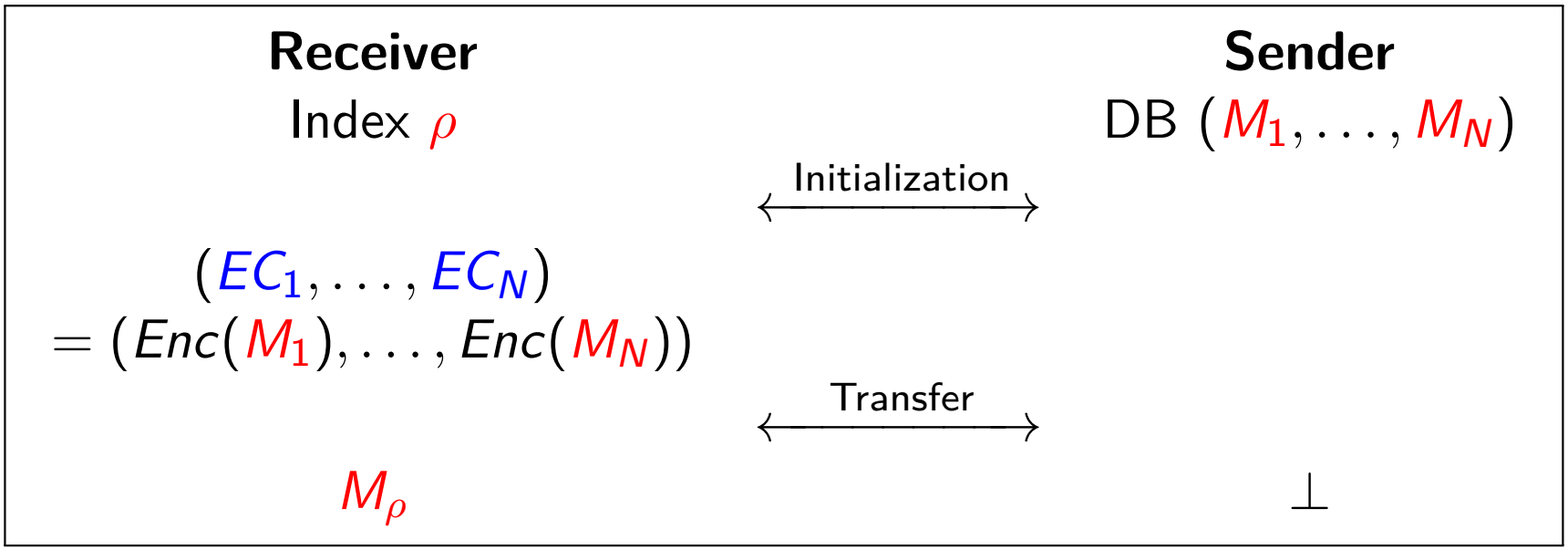


(Adaptive) Oblivious Transfer (OT) [Rab81]



- Complete building block for cryptography [GMW87]

(Adaptive) Oblivious Transfer (OT) [Rab81]



- Complete building block for cryptography [GMW87]
- Adaptive OT: receiver adaptively obtains k messages [NP99]
  - Usage: Sensitive DB (DNA, financial data,...).

History

1981 Rabin: introduction

1985 Even, Goldreich and Lempel: extension

History

1981 Rabin: introduction

1985 Even, Goldreich and Lempel: extension

1987 Goldreich, Micali and Wigderson: allows general MPC

History

1981 Rabin: introduction

1985 Even, Goldreich and Lempel: extension

1987 Goldreich, Micali and Wigderson: allows general MPC

1999 Naor and Pinkas: OT with **adaptive** queries

2007 Camenisch, Neven and shelat: assisted decryption paradigm and full simulatability

2008 Green and Hohenberger: adaptive OT in the UC model under q-type assumptions

2011 Green and Hohenberger: adaptive OT from pairings under simple assumptions

History

1981 Rabin: introduction

1985 Even, Goldreich and Lempel: extension

1987 Goldreich, Micali and Wigderson: allows general MPC

1999 Naor and Pinkas: OT with **adaptive** queries

2007 Camenisch, Neven and shelat: assisted decryption paradigm and full simulatability

2008 Green and Hohenberger: adaptive OT in the UC model under q-type assumptions

2009 Camenisch, Dubovitskaya and Neven: access control

2011 Green and Hohenberger: adaptive OT from pairings under simple assumptions

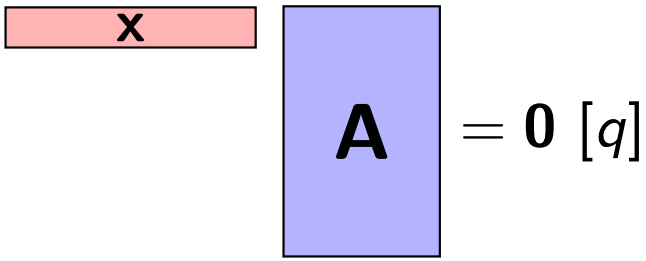
- Also possible from FHE + PRF + ZK

No fully simulatable adaptive OT with access control from lattice assumptions

Hardness Assumptions: SIS and LWE [Ajt96, Reg05]

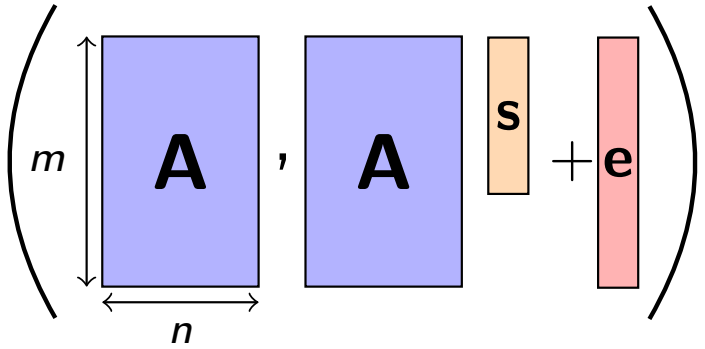
Parameters: n dimension, $m \geq n$, q modulus.
For $\mathbf{A} \hookleftarrow \mathcal{U}(\mathbb{Z}_q^{m \times n})$:

Small Integer Solution



Goal: Given $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m \backslash \{\mathbf{0}\}$ small

Learning With Errors



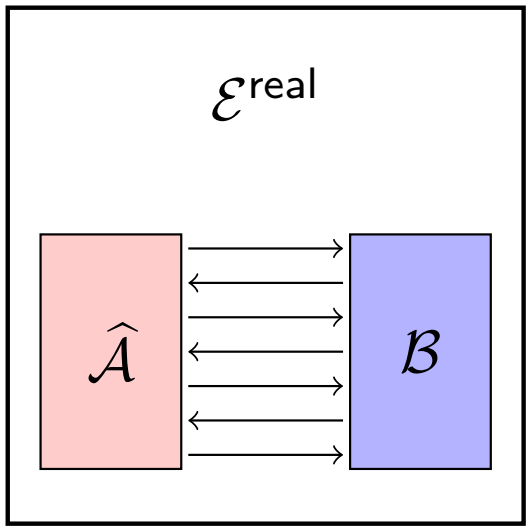
$\mathbf{s} \hookleftarrow \mathbb{Z}_q^n$ $\mathbf{e}$ small error

Goal: Given $\left(\mathbf{A}, \mathbf{A}\,\mathbf{s} + \mathbf{e}\right)$, find $\mathbf{s} \in \mathbb{Z}_q^n$

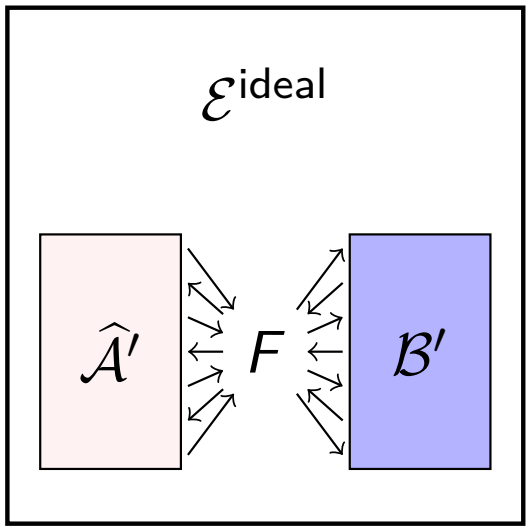
Full Simulation-Based Security [Can01]

For any cheating $\widehat{\mathcal{A}}$, there exists $\widehat{\mathcal{A}}'$ s.t.

Real world



Ideal world



$$View(\mathcal{E}^{\text{real}}) \approx_s View(\mathcal{E}^{\text{ideal}})$$

- Strictly stronger security model than indistinguishability-based or half-simulation models.

Assisted Decryption Technique [CNs07]

Idea: R gets S to decrypt one EC_i without revealing which one.

Assisted Decryption Technique [CNs07]

Idea: R gets S to decrypt one EC_i without revealing which one.

Transfer$_i$

Receiver		**Sender**
ρ_i		$(EC_1, \ldots, EC_N)$
Sample μ at random		
$C_i \leftarrow \text{Rerand}(EC_{\rho_i}, \mu)$		
$= \text{Enc}(M_{\rho_i} \oplus \mu)$		
	$\xrightarrow{C_i}$	

Assisted Decryption Technique [CNs07]

Idea: R gets S to decrypt one EC_i without revealing which one.

Transfer$_i$

Receiver		**Sender**
ρ_i		$(EC_1, \ldots, EC_N)$
Sample μ at random		
$C_i \leftarrow \mathsf{Rerand}(EC_{\rho_i}, \mu)$		
$= \mathsf{Enc}(M_{\rho_i} \oplus \mu)$		
	$\xrightarrow{C_i}$	
		$\widetilde{M}_i \leftarrow \mathsf{Dec}(C_i)$
	$\xleftarrow{\widetilde{M}_i}$	
$M_{\rho_i} = \widetilde{M}_i \oplus \mu$		

Assisted Decryption Technique [CNs07]

Idea: R gets S to decrypt one EC_i without revealing which one.

Transfer$_i$

Receiver		**Sender**
ρ_i		$(EC_1, \ldots, EC_N)$
Sample μ at random		
$C_i \leftarrow \text{Rerand}(EC_{\rho_i}, \mu)$		
$= \text{Enc}(M_{\rho_i} \oplus \mu)$		
	$\xrightarrow{C_i}$	
		$\widetilde{M}_i \leftarrow \text{Dec}(C_i)$
	$\xleftarrow{\widetilde{M}_i}$	
$M_{\rho_i} = \widetilde{M}_i \oplus \mu$		

\+ Zero-Knowledge Proofs:

- To convince S that he is decrypting a "legal" ciphertext
- PoK of signature
- Proof of correct decryption

Primal Regev Cryptosystem [Reg05]

Keygen:

Secret key: $\mathbf{S} \hookleftarrow \chi^{n \times t}$

Public key: $(\mathbf{F}, \mathbf{P})$ s.t. $\mathbf{F} \hookleftarrow U(\mathbb{Z}_q^{n \times m})$, $\mathbf{P} = \mathbf{F}^T \mathbf{S} + \mathbf{E}$ with $\mathbf{E} \hookleftarrow \chi^{m \times t}$

Encryption: $(\mathbf{a}, \mathbf{b}) = (\mathbf{a}, \mathbf{S}^T \mathbf{a} + \mathbf{x} + M\lfloor \frac{q}{2} \rfloor) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^t$

Decryption: $M = \lfloor (\mathbf{b} - \mathbf{S}^T \cdot \mathbf{a}) / (\frac{q}{2}) \rceil$

Rerand: $(\mathbf{a}', \mathbf{b}') = (\mathbf{a} + \mathbf{F}\ \mathbf{e}, \mathbf{b} + \mathbf{P}^T \mathbf{e} + \mu\lfloor \frac{q}{2} \rfloor) = Enc(M \oplus \mu)$

Primal Regev Cryptosystem [Reg05]

Keygen:

Secret key: $\mathbf{S} \hookleftarrow \chi^{n \times t}$

Public key: $(\mathbf{F}, \mathbf{P})$ s.t. $\mathbf{F} \hookleftarrow U(\mathbb{Z}_q^{n \times m})$, $\mathbf{P} = \mathbf{F}^T \mathbf{S} + \mathbf{E}$ with $\mathbf{E} \hookleftarrow \chi^{m \times t}$

Encryption: $(\mathbf{a}, \mathbf{b}) = (\mathbf{a}, \mathbf{S}^T \mathbf{a} + \mathbf{x} + M\lfloor \frac{q}{2} \rfloor) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^t$

Decryption: $M = \lfloor (\mathbf{b} - \mathbf{S}^T \cdot \mathbf{a})/(\frac{q}{2}) \rceil$

Rerand: $(\mathbf{a}', \mathbf{b}') = (\mathbf{a} + \mathbf{F}\ \mathbf{e}, \mathbf{b} + \mathbf{P}^T \mathbf{e} + \mu\lfloor \frac{q}{2} \rfloor) = Enc(M \oplus \mu)$

+ ZK proofs

Smudging [AJL+12]

Problem

The Sender only proves bounded noise $\mathbf{x}$ for Regev encryption.

Smudging [AJL+12]

Problem

The Sender only proves bounded noise $\mathbf{x}$ for Regev encryption.

Attack scenario:

- DB $= (M_0, M_1)$
- Sender encrypts M_0 with noise $\mathbf{x}_0$ and M_1 with noise $\mathbf{x}_1$ s.t. $\|\mathbf{x}_0\| \ll \|\mathbf{x}_1\| \leq B_\chi$
- Upon receiving $(\mathbf{c}_0, \mathbf{c}_1)$, decryption leaks $\|\mathbf{x}_i + \mathbf{e}\|$

$\Rightarrow$ Sender can break Receiver messages' anonymity

Smudging [AJL+12]

Problem

The Sender only proves bounded noise $\mathbf{x}$ for Regev encryption.

Attack scenario:

- DB $= (M_0, M_1)$
- Sender encrypts M_0 with noise $\mathbf{x}_0$ and M_1 with noise $\mathbf{x}_1$ s.t. $\|\mathbf{x}_0\| \ll \|\mathbf{x}_1\| \leq B_\chi$
- Upon receiving $(\mathbf{c}_0, \mathbf{c}_1)$, decryption leaks $\|\mathbf{x}_i + \mathbf{e}\|$

$\Rightarrow$ Sender can break Receiver messages' anonymity

Solution: Flood the noise with ν s.t. $\|\nu\| \gg B_\chi$.

Rerand: $(\mathbf{a}', \mathbf{b}') = (\mathbf{a} + \mathbf{F}\ \mathbf{e}, \mathbf{b} + \mathbf{P}^T\mathbf{e} + \mu\lfloor\frac{q}{2}\rfloor + \nu)$

Access Control [CDN09]

OT-AC

Encrypted database consists in $(EC_i, AP_i)_{i=1}^{N}$.

Receiver can retrieve message M_i iff it possesses cert_x for some $x \in \{0,1\}^*$ s.t. $AP_i(x) = 1$.

Access Control [CDN09]

OT-AC

Encrypted database consists in $(EC_i, AP_i)_{i=1}^{N}$.

Receiver can retrieve message M_i iff it possesses cert_x for some $x \in \{0,1\}^*$ s.t. $AP_i(x) = 1$.

[CDN09, ACDN13]: access policy made of conjunctions: $x_1 \wedge \ldots \wedge x_\ell$
Disjunctions possible through replication

[ZAW+10]: use CP-ABE to handle NC^1 access policies

[CDEN12]: Hidden policy, but on a restricted version of CNF

Access Control [CDN09]

OT-AC

Encrypted database consists in $(EC_i, AP_i)_{i=1}^{N}$.

Receiver can retrieve message M_i iff it possesses cert_x for some $x \in \{0,1\}^*$ s.t. $AP_i(x) = 1$.

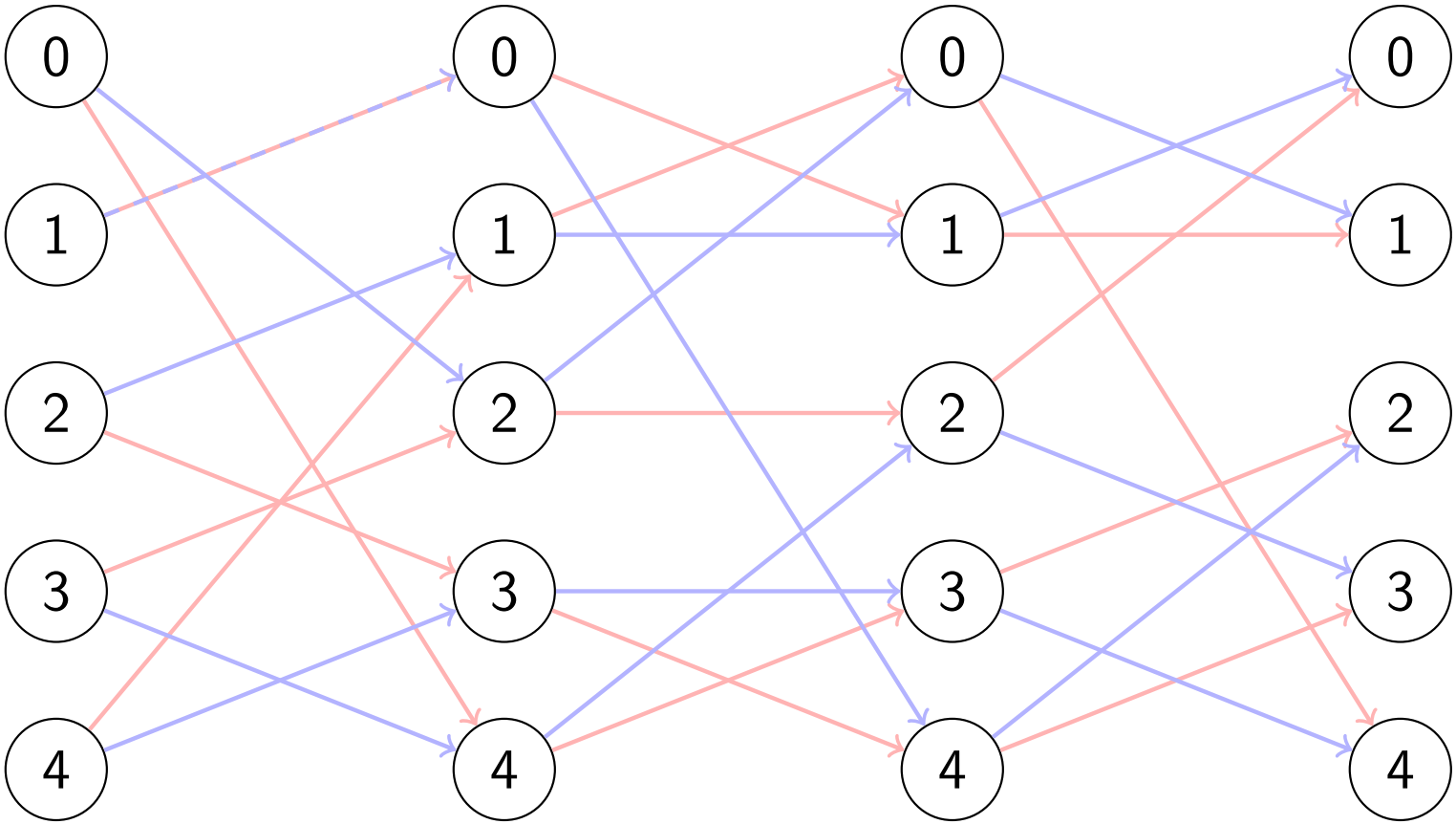
[CDN09, ACDN13]: access policy made of conjunctions: $x_1 \wedge \ldots \wedge x_\ell$
Disjunctions possible through replication

[ZAW+10]: use CP-ABE to handle NC^1 access policies

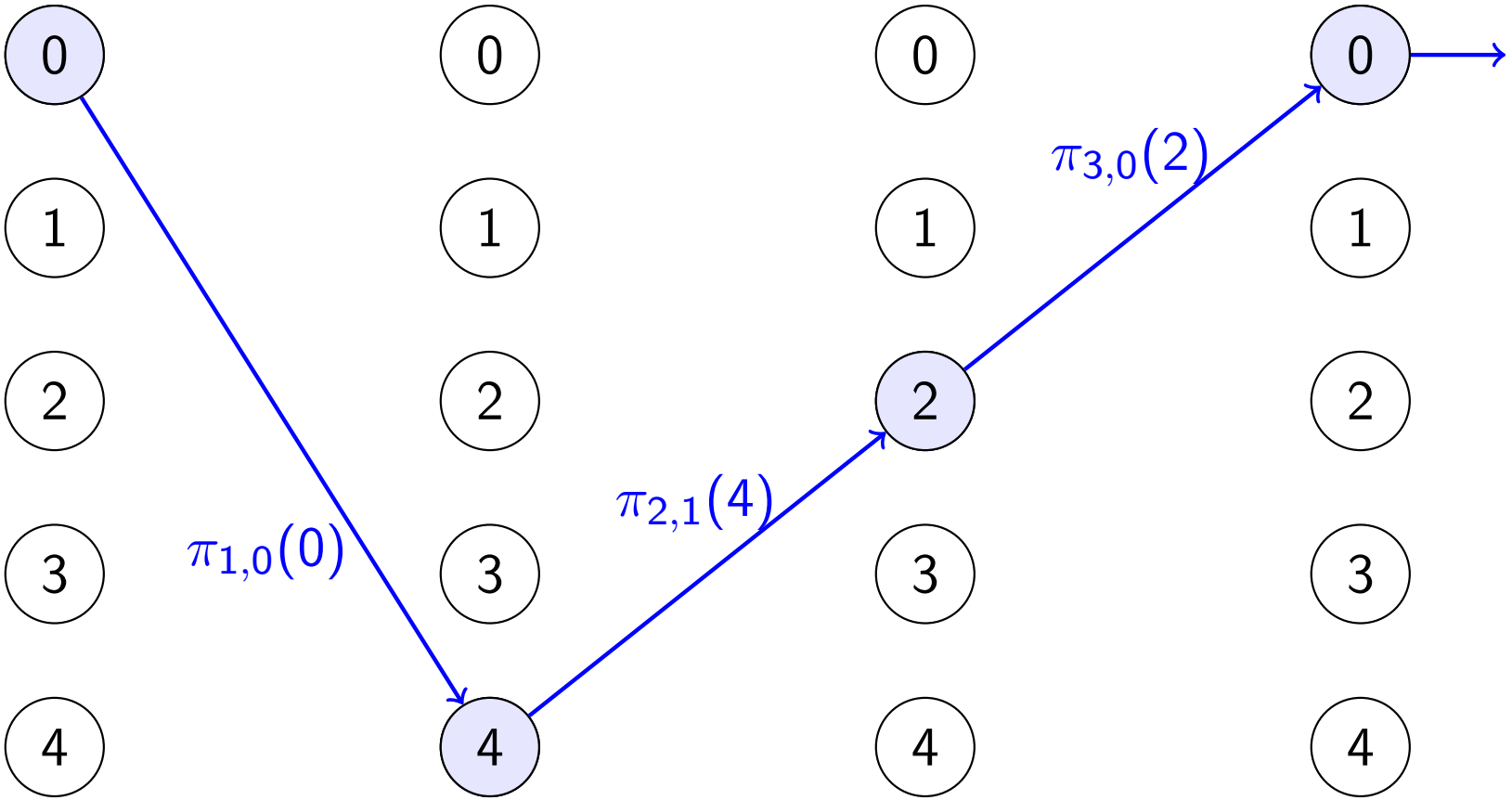
[CDEN12]: Hidden policy, but on a restricted version of CNF

Here: access policy made of a branching program (BP)

Branching Programs

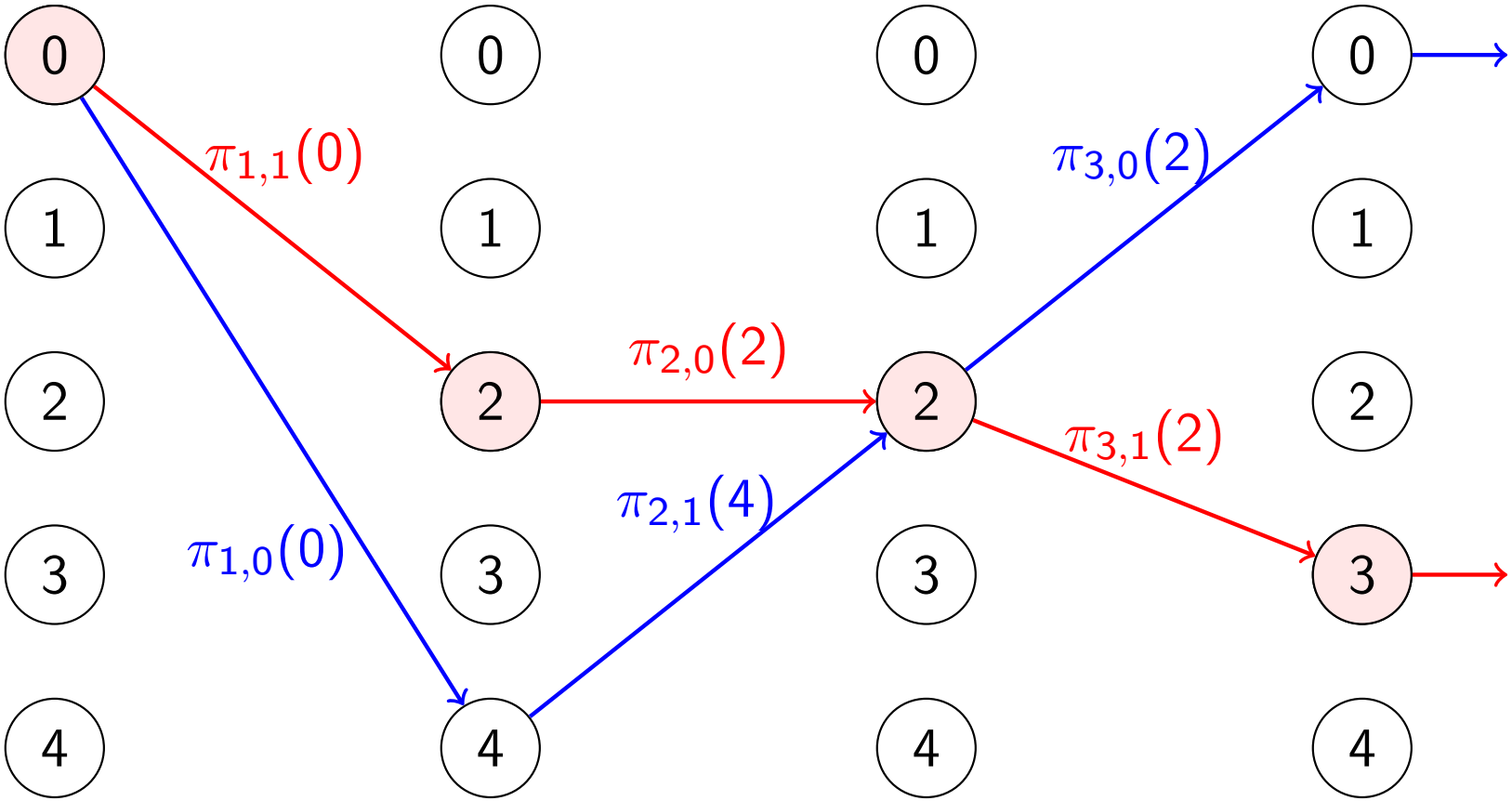


Branching Programs



$x = 010$: accepted

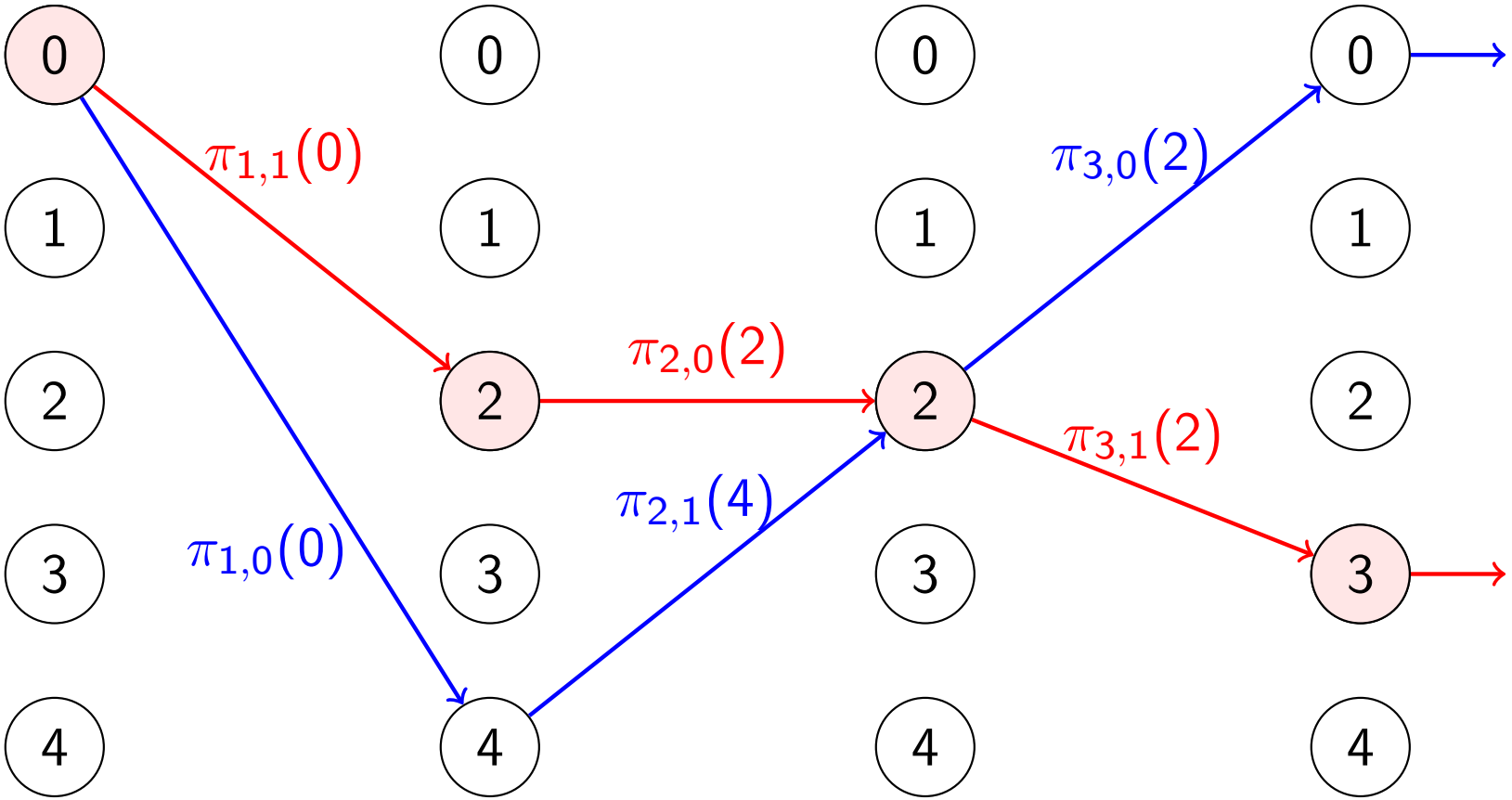
Branching Programs



$x = 010$: accepted

$y = 101$: rejected

Branching Programs

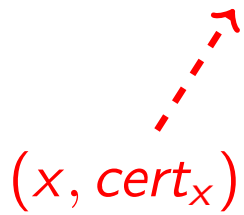


$x = 010$: accepted
$y = 101$: rejected

[Barr86]: polynomially-long BP are equivalent to NC^1

Branching Programs

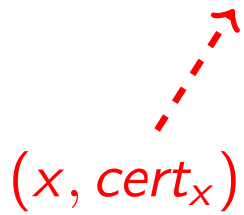
$$\{(EC_1, BP_1), (EC_2, BP_2), \ldots, (EC_N, BP_N)\}.$$



Goal: Prove knowledge of $cert_x = Sign(x)$ s.t. $\exists i : BP_i(x) = 1$.

Branching Programs

$$\{(EC_1, BP_1), (EC_2, BP_2), \ldots, (EC_N, BP_N)\}.$$



Goal: Prove knowledge of $cert_x = Sign(x)$ s.t. $\exists i : BP_i(x) = 1$.

This work

Make BP's statements work with Stern-like ZK arguments [Ste93]

Branching Programs

Encoding of a branching program:

$$\mathbf{z}_{BP} = (d_{1,1}, \ldots, d_{1,\delta_\kappa}, \ldots, d_{L,1}, \ldots, d_{L,\delta_\kappa}, \pi_{1,0}(0), \ldots, \pi_{1,0}(4), \pi_{1,1}(0), \ldots, \pi_{1,1}(4), \ldots, \pi_{L,0}(0), \ldots, \pi_{L,0}(4), \pi_{L,1}(0), \ldots, \pi_{L,1}(4)) \in [0,4]^{\zeta}$$

$d_{\theta,1}, \ldots, d_{\theta,\delta_\kappa}$: bit representation of $\mathrm{var}(\theta)$

Step-by-step evaluation:

$$\eta_\theta = \pi_{\theta,x_{\mathrm{var}(\theta)}}(\eta_{\theta-1}) = \pi_{\theta,0}(\eta_{\theta-1}) \cdot \bar{x}_{\mathrm{var}(\theta)} + \pi_{\theta,1}(\eta_{\theta-1}) \cdot x_{\mathrm{var}(\theta)}$$

Branching Programs

Encoding of a branching program:

$$\mathbf{z}_{BP} = (d_{1,1}, \ldots, d_{1,\delta_\kappa}, \ldots, d_{L,1}, \ldots, d_{L,\delta_\kappa}, \pi_{1,0}(0), \ldots, \pi_{1,0}(4), \pi_{1,1}(0), \ldots, \pi_{1,1}(4), \ldots, \pi_{L,0}(0), \ldots, \pi_{L,0}(4), \pi_{L,1}(0), \ldots, \pi_{L,1}(4)) \in [0,4]^{\zeta}$$

$d_{\theta,1}, \ldots, d_{\theta,\delta_\kappa}$: bit representation of $\mathrm{var}(\theta)$

Step-by-step evaluation:

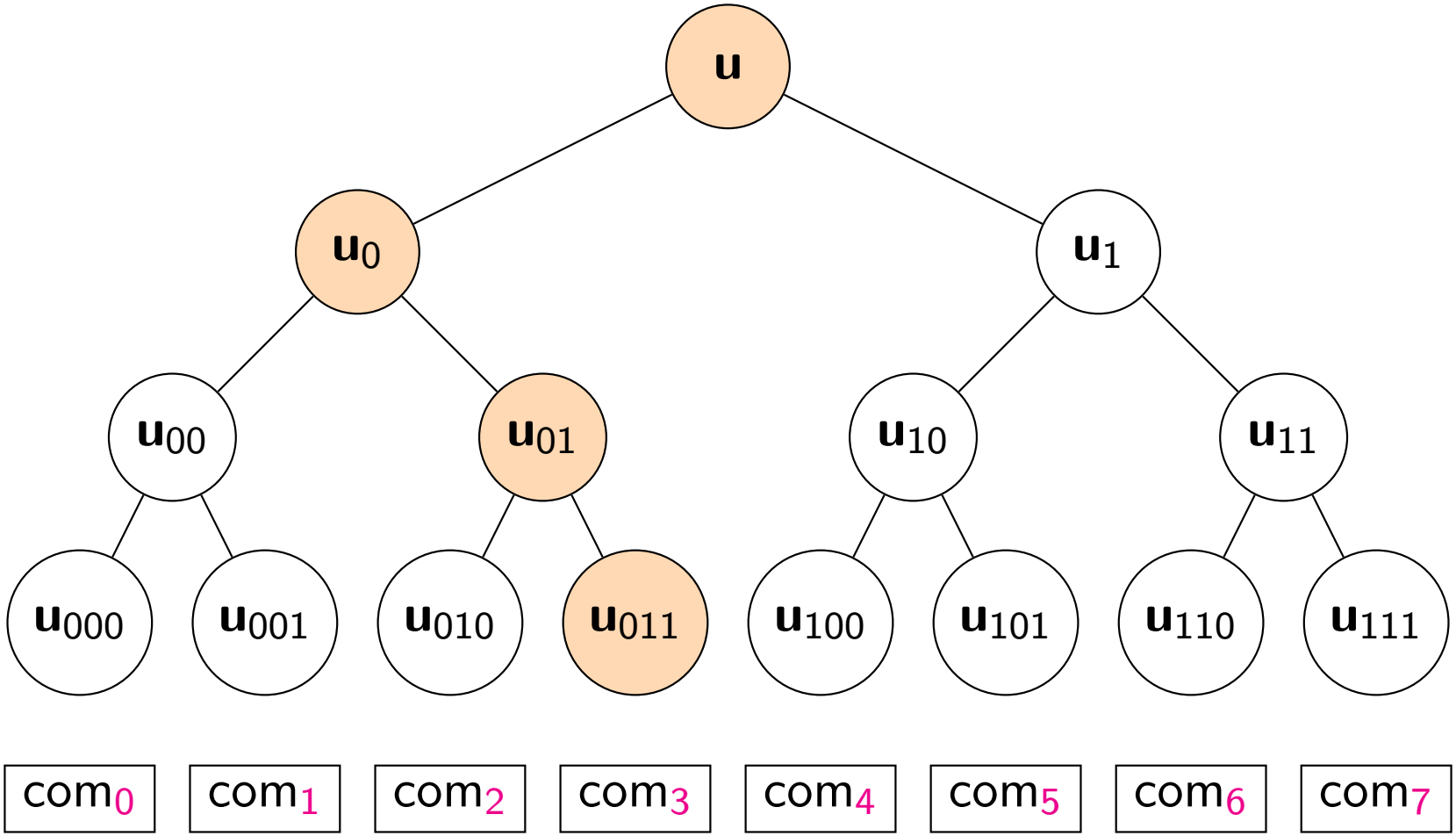
$$\eta_\theta = \pi_{\theta,x_{\mathrm{var}(\theta)}}(\eta_{\theta-1}) = \pi_{\theta,0}(\eta_{\theta-1}) \cdot \bar{x}_{\mathrm{var}(\theta)} + \pi_{\theta,1}(\eta_{\theta-1}) \cdot x_{\mathrm{var}(\theta)}$$

Proving correct evaluation

Naively: prove each step $\rightarrow O(L \cdot \kappa)$

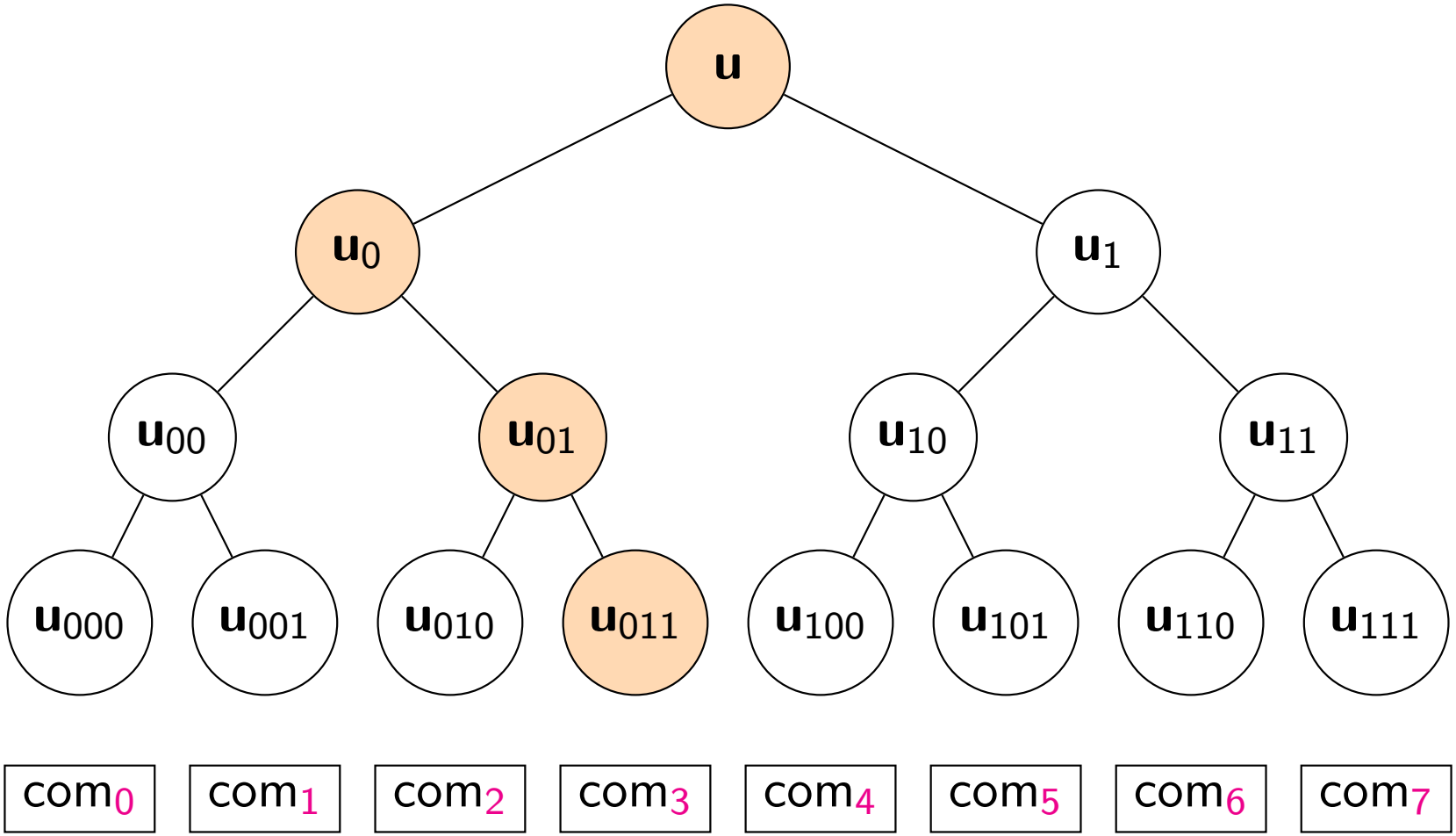
Our idea: use binary-search $\rightarrow O(L \cdot \log(\kappa))$ [LLNW16]

Branching Programs



$\mathsf{com}_i = \mathsf{Com}(x_i)$

Branching Programs



$\mathsf{com}_i = \mathsf{Com}(x_i) \rightarrow$ correct binary-search $\Rightarrow$ knowledge of $x_{\mathrm{var}(\theta)}$

Zero-Knowledge Proofs for Lattices

Difficulty

No equivalent of Groth-Sahai proofs!

Why?

Lattices propose less algebraic structure than pairing groups.

Zero-Knowledge Proofs for Lattices

Difficulty

No equivalent of Groth-Sahai proofs!

Why?
Lattices propose less algebraic structure than pairing groups.

Two main proof systems in lattice-based cryptography:

Lyubashevky-like [Lyu09]: From Ring-LWE, relatively efficient but not expressive. Algebraic

Stern-like [Ste93]: From LWE (in standard lattices), heavy but expressive. Combinatorial

Both are interactive.

Stern-Like ZK Argument [Ste93]

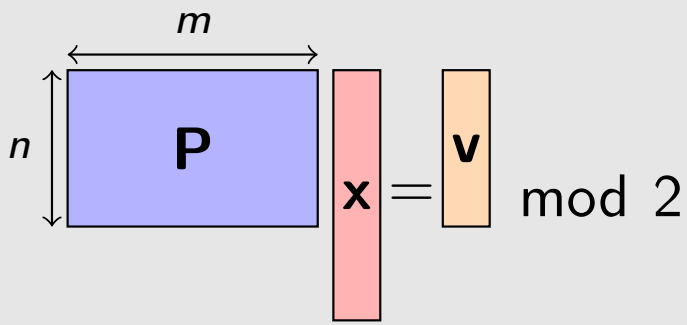
Stern's protocol: ZK proof for Syndrome Decoding Problem.

Stern-Like ZK Argument [Ste93]

Stern's protocol: ZK proof for Syndrome Decoding Problem.

Syndrome Decoding Problem

Given $\mathbf{P} \in \mathbb{Z}_2^{n \times m}$ and $\mathbf{v} \in \mathbb{Z}_2^n$, find $\mathbf{x}$ s.t. $\mathrm{w}(\mathbf{x}) = w$ and



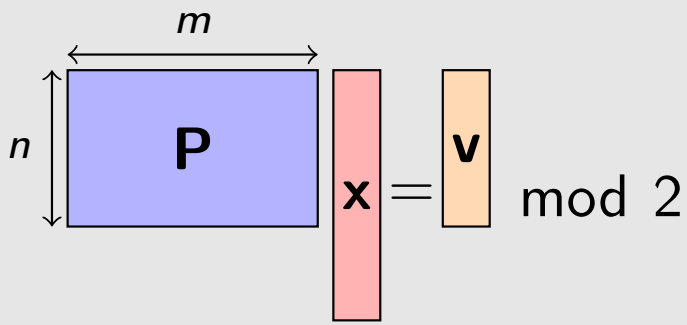
$\mod 2$

Stern-Like ZK Argument [Ste93]

Stern's protocol: ZK proof for Syndrome Decoding Problem.

Syndrome Decoding Problem

Given $\mathbf{P} \in \mathbb{Z}_2^{n \times m}$ and $\mathbf{v} \in \mathbb{Z}_2^n$, find $\mathbf{x}$ s.t. $\mathrm{w}(\mathbf{x}) = w$ and



mod 2

[KTX08]: mod 2 $\rightarrow$ mod q

[LNSW13]: Extends Stern's protocol for SIS and LWE statements

Recent uses of Stern-like protocols in lattice-based crypto:
[LNW15, LLNW16, LLN**M**W16a, LLN**M**W16b, LLNW17]

Signature with Efficient Protocols [CL02]

A signature scheme ($\mathbf{Keygen}, \mathbf{Sign}_{\mathsf{sk}}, \mathbf{Verif}_{\mathsf{vk}}$) with companion protocols:

- 2-party protocol for signing a committed value
- Prove possession of a signature in ZK

Signature with Efficient Protocols [CL02]

A signature scheme ($\mathbf{Keygen}, \mathbf{Sign}_{sk}, \mathbf{Verif}_{vk}$) with companion protocols:

- 2-party protocol for signing a committed value
- Prove possession of a signature in ZK

Security

- Unforgeability

Signature with Efficient Protocols [CL02]

A signature scheme ($\mathbf{Keygen}, \mathbf{Sign}_{sk}, \mathbf{Verif}_{vk}$) with companion protocols:

- 2-party protocol for signing a committed value
- Prove possession of a signature in ZK

Security

- Unforgeability
- Security of the two protocols
- Anonymity

Signature with Efficient Protocols [CL02]

A signature scheme ($\mathbf{Keygen}, \mathbf{Sign}_{sk}, \mathbf{Verif}_{vk}$) with companion protocols:

- 2-party protocol for signing a committed value
- Prove possession of a signature in ZK

Security

- Unforgeability
- Security of the two protocols
- Anonymity

$\rightarrow$ many applications for privacy-based protocols (e.g., e-cash, anonymous credentials, ...)

Signature with Efficient Protocols [CL02]

A signature scheme ($\mathbf{Keygen}, \mathbf{Sign}_{\mathsf{sk}}, \mathbf{Verif}_{\mathsf{vk}}$) with companion protocols:

- 2-party protocol for signing a committed value
- Prove possession of a signature in ZK

Security

- Unforgeability
- Security of the two protocols
- Anonymity

$\rightarrow$ many applications for privacy-based protocols (e.g., e-cash, anonymous credentials, ...)

We use a SIS-based construction from Asiacrypt'16 [LLNMW16].

Our Construction

Ingredients

- Assisted decryption technique [CNs07]
- A simplification of [LLNMW16]'s signatures as certificates
- Access control using BP
- ZK proofs *à la* Stern

Our Adaptive OT Construction

Initialization

Sender side:

1. Generate $(\mathsf{VK}_{sig}, \mathsf{SK}_{sig}) \leftarrow \Sigma.keygen(1^\lambda)$
2. Compute $((\mathbf{S}, \mathbf{E}), (\mathbf{F}, \mathbf{P})) \leftarrow Regev.keygen(1^\lambda)$
3. Use $\mathbf{S}$ to compute encryptions of $M_i \rightarrow (\mathbf{a}_i, \mathbf{b}_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^t$
4. Use SK_{sig} to compute signatures of $(\mathbf{a}_i, \mathbf{b}_i) \rightarrow \sigma_i$
5. $EC_i \leftarrow (\sigma_i, (\mathbf{a}_i, \mathbf{b}_i))$

Our Adaptive OT Construction

Initialization

Sender side:

1. Generate $(\mathsf{VK}_{sig}, \mathsf{SK}_{sig}) \leftarrow \Sigma.keygen(1^\lambda)$
2. Compute $((\mathbf{S}, \mathbf{E}), (\mathbf{F}, \mathbf{P})) \leftarrow Regev.keygen(1^\lambda)$
3. Use $\mathbf{S}$ to compute encryptions of $M_i \rightarrow (\mathbf{a}_i, \mathbf{b}_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^t$
4. Use SK_{sig} to compute signatures of $(\mathbf{a}_i, \mathbf{b}_i) \rightarrow \sigma_i$
5. $EC_i \leftarrow (\sigma_i, (\mathbf{a}_i, \mathbf{b}_i))$

Sender sends $(\mathsf{VK}_{sig}, (\mathbf{F}, \mathbf{P}), EC_i)$ to the Receiver and proves that everything was done correctly.

Sender keeps the previous information and $(\mathbf{S}, \mathbf{E})$.

Our Adaptive Oblivious Transfer Construction

Transfer

Receiver(ρ_i)

Sample $\mu \leftarrow U(\{0,1\}^t)$

Rerandomize $(\mathbf{a}_{\rho_i}, \mathbf{b}_{\rho_i})$

into $(\mathbf{c}_0, \mathbf{c}_1) = (\mathbf{a}_{\rho_i} + \mathbf{F}\ \mathbf{e},$

$\mathbf{b}_{\rho_i} + \mathbf{P}^T \mathbf{e} + \mu\lfloor q/2 \rfloor + \nu)$

Sender

$(\mathbf{c}_0, \mathbf{c}_1)$ →

prove knowledge of σ_{ρ_i} ↔

$\widetilde{M}_i = \mathsf{Dec}(\mathbf{c}_0, \mathbf{c}_1)$

← $\widetilde{M}_i$

prove correct decryption ↔

$M_{\rho_i} = \widetilde{M}_i \oplus \mu$

Our Adaptive Oblivious Transfer Construction

Final steps

- Access control can be plugged into our scheme
  - Proof of correct binary-search via Merkle-tree [LLNW16]

Our Adaptive Oblivious Transfer Construction

Final steps

- Access control can be plugged into our scheme
  - Proof of correct binary-search via Merkle-tree [LLNW16]
- Our scheme is proven secure in the standard model
  - In the ROM: optimizations using NIWI/NIZK proofs [FS86]

Conclusion

- First OT-AC in the lattice setting that handles expressive statements (NC^1)
- Relies on LWE with superpolynomial modulus
- Security proof in the full simulation-based model

Possible improvements:

- Avoid smudging and work with polynomial-size moduli
- Improve efficiency
- Generalize it to circuit policies

Questions?