HB^N: A MIM-SECURE HB-LIKE PROTOCOL

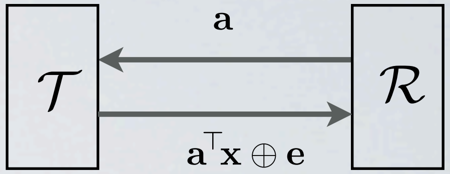
Carl Bosley, Stevens Institute of Technology
Joint work with Antonio Nicolosi and Kristiyan Haralambiev

[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise

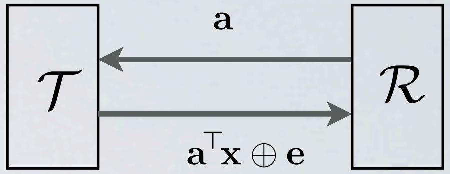
[HB01] and descendents

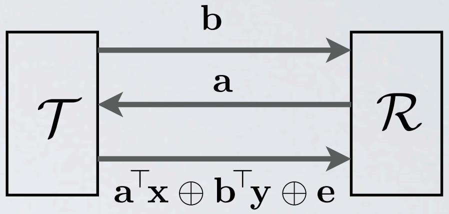
- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise
- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure



[HB01] and descendents

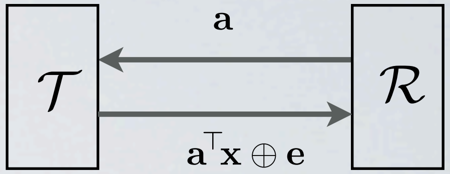
- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise
- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB$^+$ actively secure

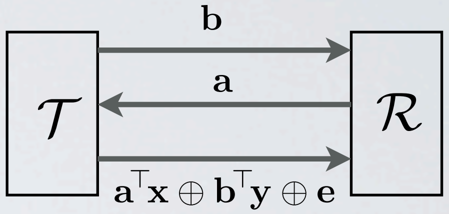


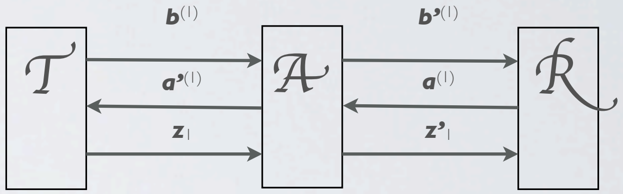

$\mathbf{b}$
$\mathbf{a}$
$\mathcal{T}$
$\mathcal{R}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$

[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise
- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB$^+$ actively secure
    - [GRS05] MIM attack

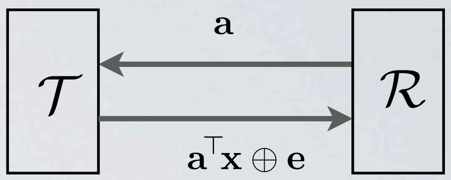


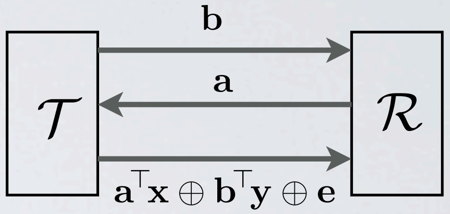

$\mathbf{b}$
$\mathbf{a}$
$\mathcal{T}$
$\mathcal{R}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$



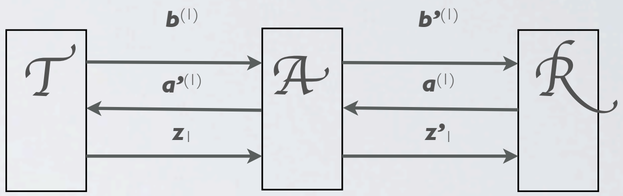
[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise
- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB^{+} actively secure
    - [GRS05] MIM attack
  - Several MIM-secure variants: HB*, HB-MP, HB-MP', Trusted-HB



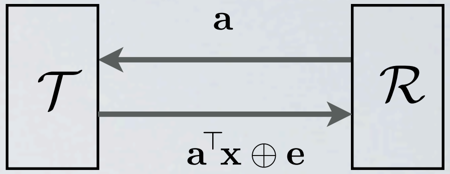


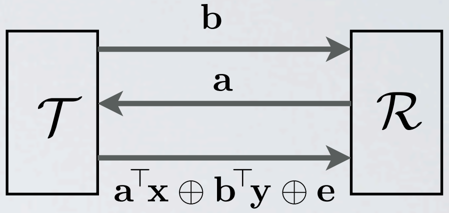
$\mathcal{T}$
$\mathbf{b}$
$\mathbf{a}$
$\mathbf{a}^{\top}\mathbf{x} \oplus \mathbf{b}^{\top}\mathbf{y} \oplus \mathbf{e}$
$\mathcal{R}$

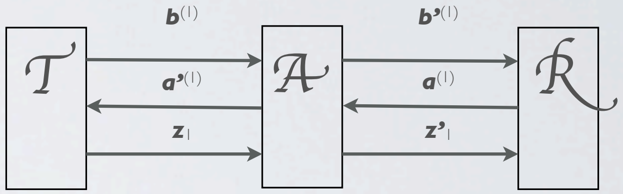


[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise
- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB$^+$ actively secure
    - [GRS05] MIM attack
  - Several MIM-secure variants: HB*, HB-MP, HB-MP', Trusted-HB
    - "If I call a tail a leg, how many legs does a dog have?"

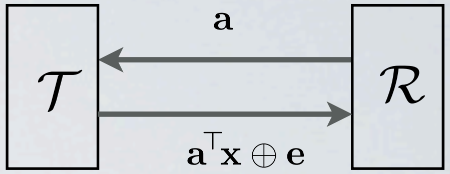


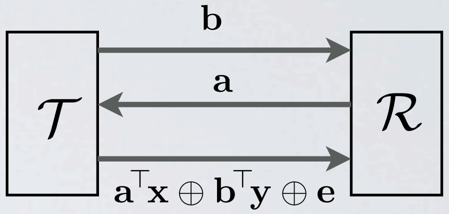

$\mathbf{b}$
$\mathbf{a}$
$\mathcal{T}$
$\mathcal{R}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$



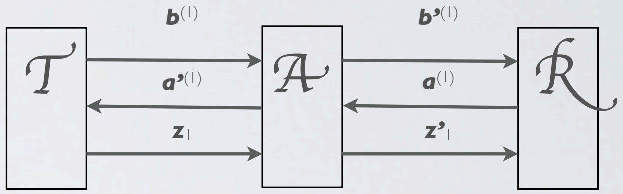
[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise
- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB$^+$ actively secure
    - [GRS05] MIM attack
  - Several MIM-secure variants: HB*, HB-MP, HB-MP', Trusted-HB
    - "If I call a tail a leg, how many legs does a dog have?"
      - Lincoln may or may not have said that, but it is linked to him by 1862: see snopes.com: http://tinyurl.com/3eff3nk



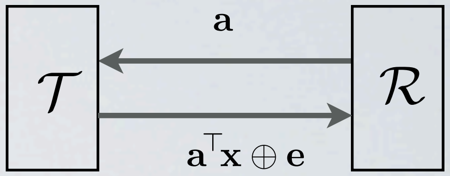


$\mathbf{b}$
$\mathbf{a}$
$\mathcal{T}$
$\mathcal{R}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$

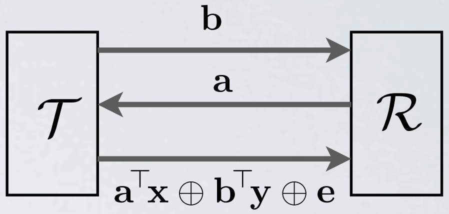


[HB01] and descendents

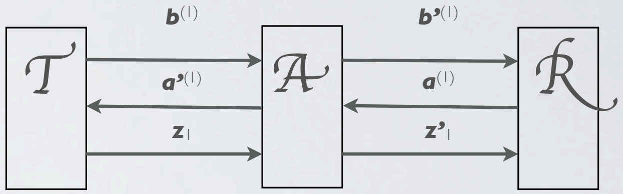
- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise



- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB$^+$ actively secure


b
a
$\mathcal{T}$
$\mathcal{R}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$

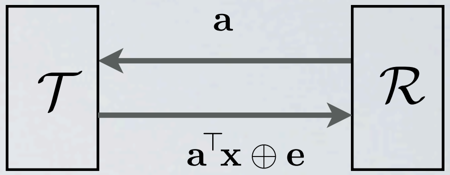
    - [GRS05] MIM attack

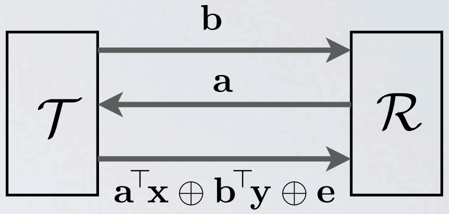


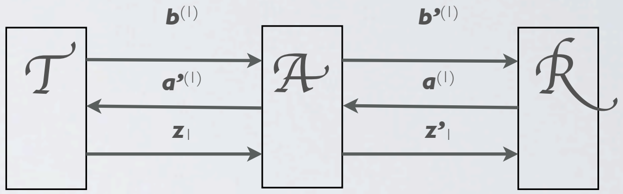
  - Several MIM-secure variants: HB*, HB-MP, HB-MP', Trusted-HB
    - "If I call a tail a leg, how many legs does a dog have?"
      - Lincoln may or may not have said that, but it is linked to him by 1862: see snopes.com: http://tinyurl.com/3eff3nk
    - [GRS08a,FS09] Actually, **not** secure

[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise
- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB$^+$ actively secure
    - [GRS05] MIM attack
  - Several MIM-secure variants: HB*, HB-MP, HB-MP', Trusted-HB
    - "If I call a tail a leg, how many legs does a dog have?"
      - Lincoln may or may not have said that, but it is linked to him by 1862: see snopes.com: http://tinyurl.com/3eff3nk
    - [GRS08a,FS09] Actually, **not** secure
  - [GRS08b] random-HB$^\#$ MIM-secure

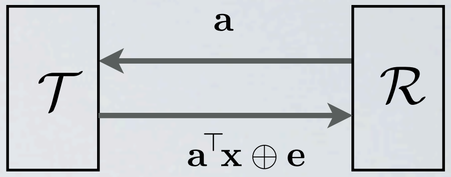


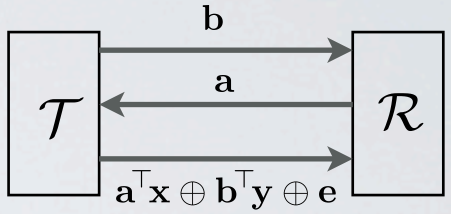

$\mathcal{T}$
$\mathbf{b}$
$\mathbf{a}$
$\mathcal{R}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$

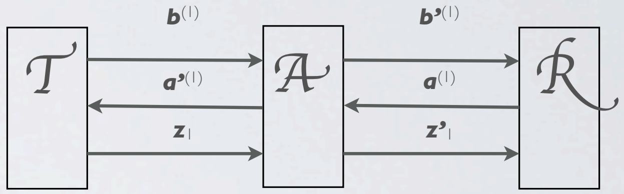


[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise
- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB$^+$ actively secure
    - [GRS05] MIM attack
  - Several MIM-secure variants: HB*, HB-MP, HB-MP', Trusted-HB
    - "If I call a tail a leg, how many legs does a dog have?"
      - Lincoln may or may not have said that, but it is linked to him by 1862: see snopes.com: http://tinyurl.com/3eff3nk
    - [GRS08a,FS09] Actually, **not** secure
  - [GRS08b] random-HB$^\#$ MIM-secure
    - [OOV08] Actually, it's **not** MIM-secure

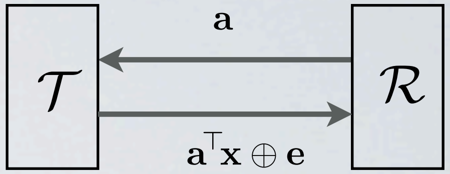



$\mathbf{b}$
$\mathbf{a}$
$\mathcal{T}$
$\mathcal{R}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$

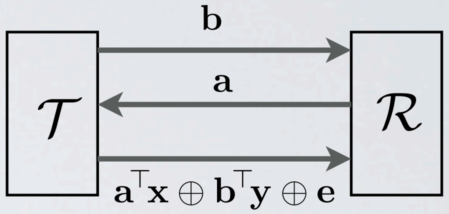


[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise

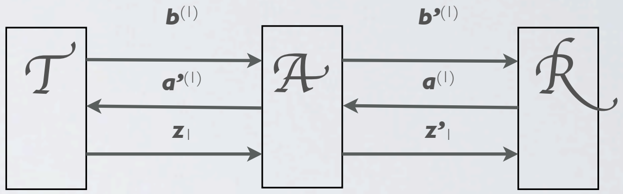


- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB^+ actively secure



$\mathcal{T}$
$\mathbf{b}$
$\mathbf{a}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$
$\mathcal{R}$

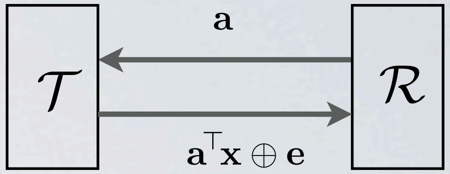
  - [GRS05] MIM attack

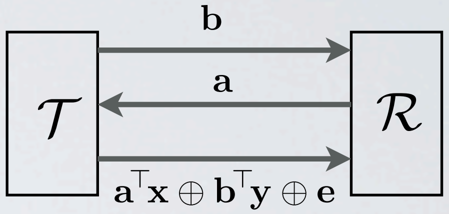


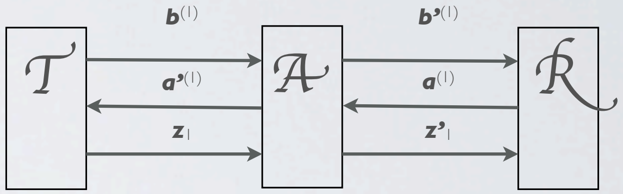
  - Several MIM-secure variants: HB*, HB-MP, HB-MP', Trusted-HB
    - "If I call a tail a leg, how many legs does a dog have?"
      - Lincoln may or may not have said that, but it is linked to him by 1862: see snopes.com: http://tinyurl.com/3eff3nk
    - [GRS08a,FS09] Actually, **not** secure
  - [GRS08b] random-$\text{HB}^\#$ MIM-secure
    - [OOV08] Actually, it's **not** MIM-secure
  - [KPCJV11] MAC_1, MAC_2 **provably** MIM-secure

[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise
- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB^+ actively secure
    - [GRS05] MIM attack
  - Several MIM-secure variants: HB*, HB-MP, HB-MP', Trusted-HB
    - "If I call a tail a leg, how many legs does a dog have?"
      - Lincoln may or may not have said that, but it is linked to him by 1862: see snopes.com: http://tinyurl.com/3eff3nk
    - [GRS08a,FS09] Actually, **not** secure
  - [GRS08b] random-$HB^{\#}$ MIM-secure
    - [OOV08] Actually, it's **not** MIM-secure
  - [KPCJV11] MAC_1, MAC_2 **provably** MIM-secure
    - but rather complicated

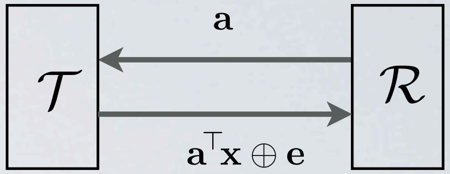



$\mathcal{T}$
$\mathbf{b}$
$\mathbf{a}$
$\mathcal{R}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$

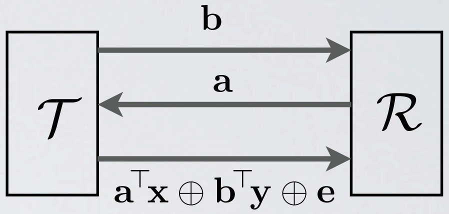


[HB01] and descendents

- **Setting**
  - RFID Authentication: Tag=Prover, Reader=Verifier
    - Hardness based on Learning Parity with Noise

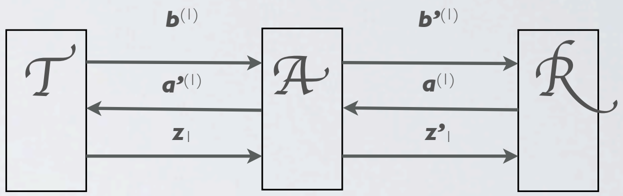


- **The Evolution of HB: A Whirlwind Tour**
  - [HB01] passively secure
  - [JW05] HB$^+$ actively secure



$\mathbf{b}$
$\mathbf{a}$
$\mathcal{T}$
$\mathcal{R}$
$\mathbf{a}^\top\mathbf{x} \oplus \mathbf{b}^\top\mathbf{y} \oplus \mathbf{e}$

    - [GRS05] MIM attack



  - Several MIM-secure variants: HB*, HB-MP, HB-MP', Trusted-HB
    - "If I call a tail a leg, how many legs does a dog have?"
      - Lincoln may or may not have said that, but it is linked to him by 1862: see snopes.com: http://tinyurl.com/3eff3nk
    - [GRS08a,FS09] Actually, **not** secure

  - [GRS08b] random-HB$^\#$ MIM-secure
    - [OOV08] Actually, it's **not** MIM-secure

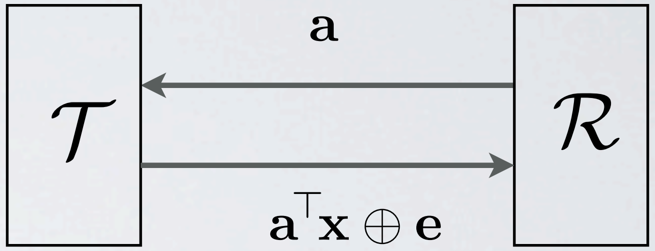
  - [KPCJV11] MAC$_1$, MAC$_2$ **provably** MIM-secure
    - but rather complicated

[BHN] HB^N Protocol

- Tools:
  - ⊕: [0,1] x [0,1] -> [0,1]
  - LSN <=> LPN
  - Probabilistic Verification
  - Sequence of Games

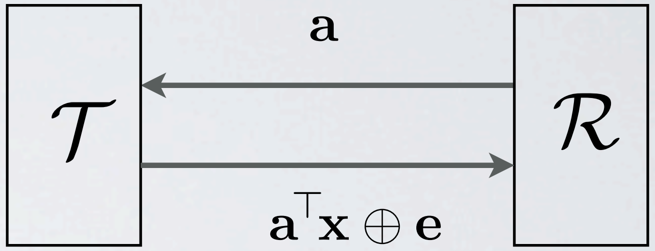
HB and HB^N

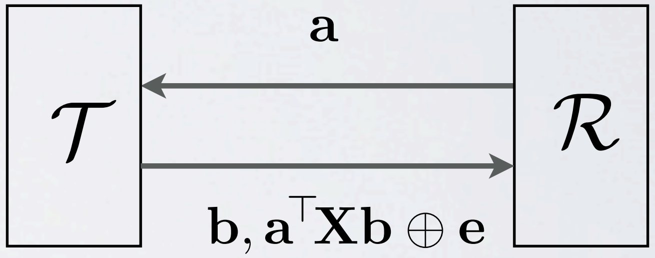
- HB is **extremely simple**:
  - Tag computes noisy parity.

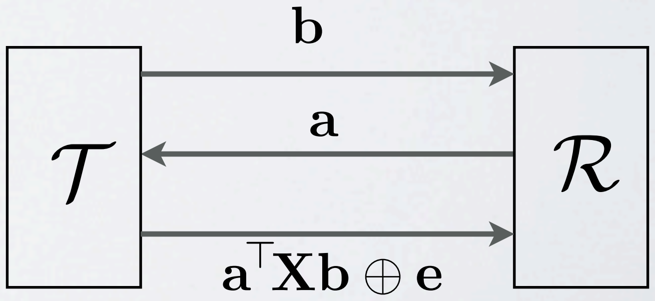


HB and HB^{N}

- HB is **extremely simple**:
  - Tag computes noisy parity.
- **HB^{N}** is extremely simple:
  - Tag computes noisy bilinear function.

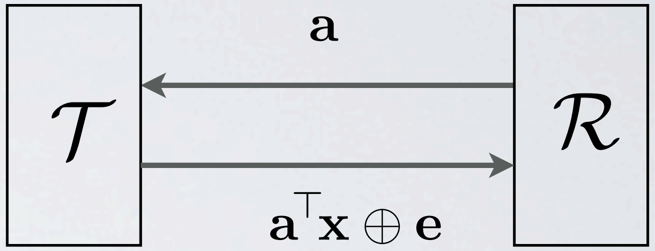


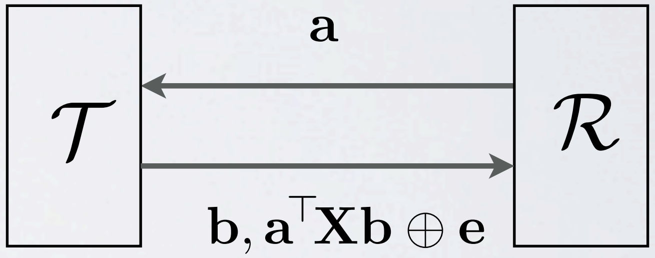

$\mathbf{a}$
$\mathcal{T}$
$\mathcal{R}$
$\mathbf{b}, \mathbf{a}^{\top}\mathbf{X}\mathbf{b} \oplus \mathbf{e}$

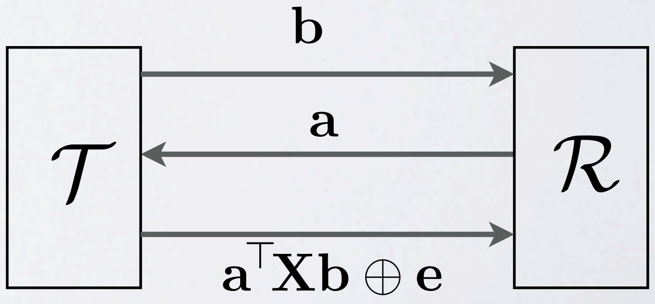


HB and HB^N

- HB is **extremely simple**:
  - Tag computes noisy parity.
- **HB^N** is extremely simple:
  - Tag computes noisy bilinear function.
- Interestingly, **HB^N** is not the first bilinear protocol: [KPCJV11] can be rewritten as applying a noisy bilinear map

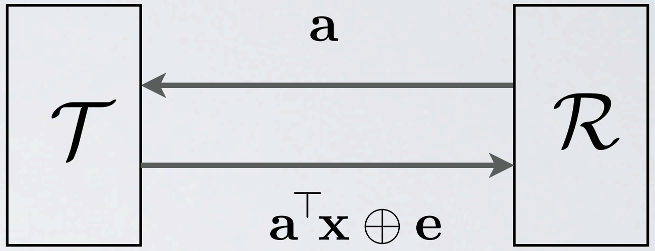


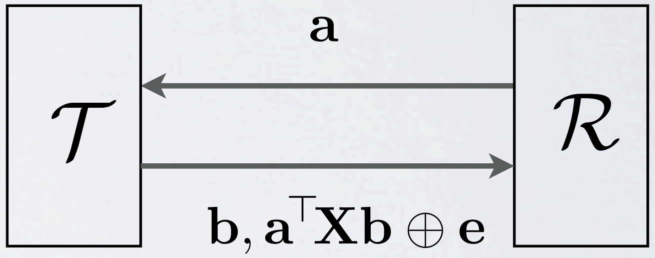

$\mathcal{T}$
$\mathbf{a}$
$\mathbf{b}, \mathbf{a}^\top \mathbf{X} \mathbf{b} \oplus \mathbf{e}$
$\mathcal{R}$

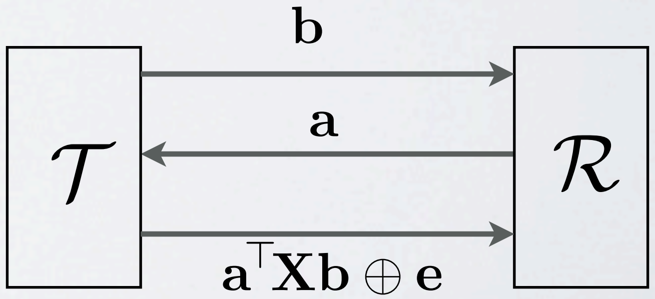


HB and HB$^{\mathbf{N}}$

- HB is **extremely simple**:
  - Tag computes noisy parity.
- **HB$^{\mathbf{N}}$** is extremely simple:
  - Tag computes noisy bilinear function.
- Interestingly, **HB$^{\mathbf{N}}$** is not the first bilinear protocol: [KPCJV11] can be rewritten as applying a noisy bilinear map
- New technique for defending against verify queries: **Probabilistic Verification.**
  - $\mathcal{R}$ computes $\mathbf{w}_i = \mathbf{a}^{\top}\mathbf{X}\mathbf{b}+\mathbf{f}_i$




$\mathbf{a}$
$\mathcal{T}$
$\mathcal{R}$
$\mathbf{b}, \mathbf{a}^{\top}\mathbf{X}\mathbf{b} \oplus \mathbf{e}$



Adding Noise: $\oplus$ and $\overline{\rho}$

- Define $\oplus$: $[0,1] \times [0,1] \rightarrow [0,1]$: $\mathrm{Ber}_{\varepsilon} \oplus \mathrm{Ber}_{\rho} = \mathrm{Ber}_{\varepsilon \oplus \rho}$

Adding Noise: $\oplus$ and $\overline{\rho}$

- Define $\oplus$: $[0,1] \times [0,1] \rightarrow [0,1]$: $\mathrm{Ber}_{\varepsilon} \oplus \mathrm{Ber}_{\rho} = \mathrm{Ber}_{\varepsilon \oplus \rho}$
  - $\varepsilon \oplus \rho = (1-\varepsilon)\rho + (1-\rho)\varepsilon$
  - $\oplus$ restricted to $Z_2 \times Z_2$ is equivalent to $\oplus$

Adding Noise: $\oplus$ and $\overline{\rho}$

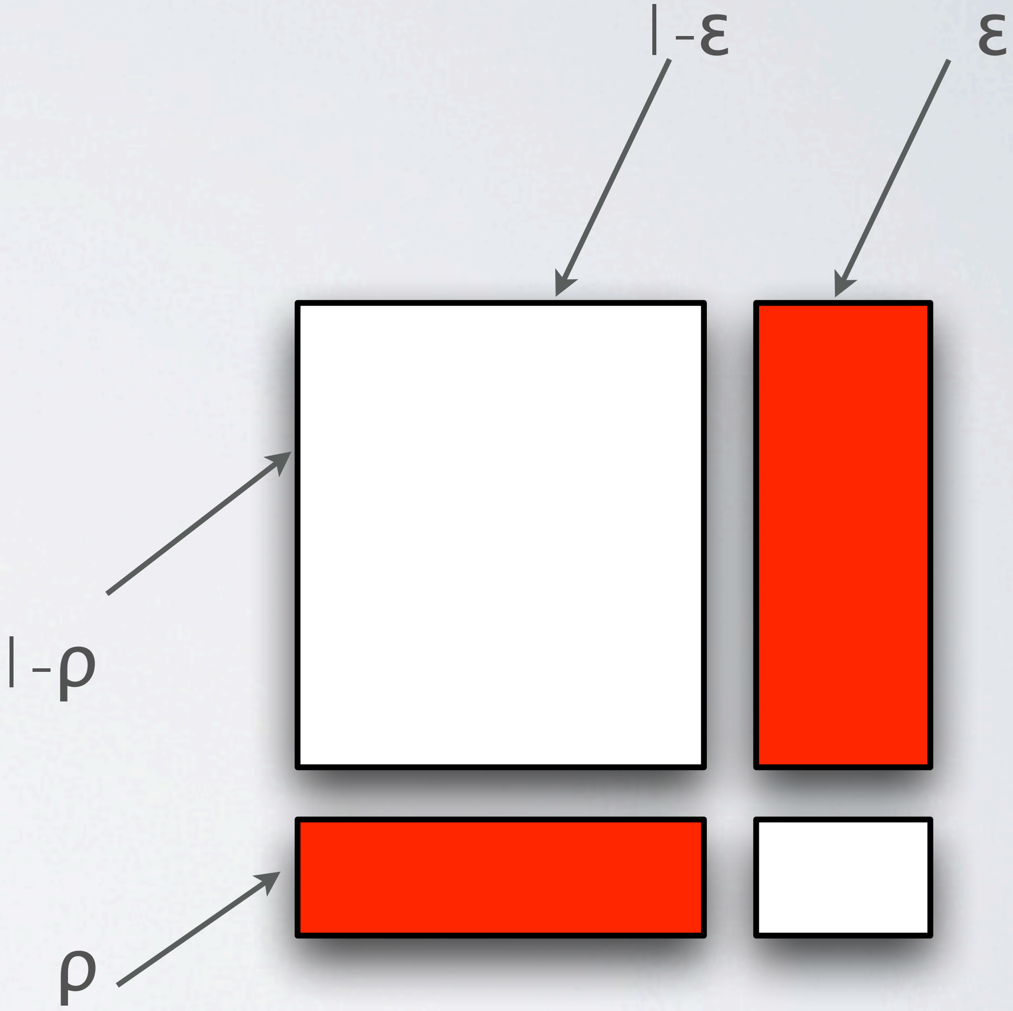
- Define $\oplus$: $[0,1] \times [0,1] \to [0,1]$: $\mathrm{Ber}_{\varepsilon} \oplus \mathrm{Ber}_{\rho} = \mathrm{Ber}_{\varepsilon\oplus\rho}$
  - $\varepsilon\oplus\rho = (1-\varepsilon)\rho + (1-\rho)\varepsilon$
  - $\oplus$ restricted to $Z_2 \times Z_2$ is equivalent to $\oplus$
  - ½ annihilates: $\rho \oplus ½ = ½$

Adding Noise: $\oplus$ and $\overline{\rho}$

- Define $\oplus$: [0,1] × [0,1]→[0,1]: $\mathrm{Ber}_\varepsilon \oplus \mathrm{Ber}_\rho = \mathrm{Ber}_{\varepsilon\oplus\rho}$
  - $\boldsymbol{\varepsilon\oplus\rho} = (1-\boldsymbol{\varepsilon})\boldsymbol{\rho} + (1-\boldsymbol{\rho})\boldsymbol{\varepsilon}$
  - $\oplus$ restricted to $Z_2 \times Z_2$ is equivalent to $\oplus$
  - ½ annihilates: $\boldsymbol{\rho} \oplus ½ = ½$
- $\Pr[\mathrm{Ber}_\varepsilon = b] = b \oplus \overline{\boldsymbol{\varepsilon}}$
- $\Pr[(\mathbf{a},b)\leftarrow\mathrm{LPN}_\varepsilon{}^{\mathbf{x}}] = 2^{-n}(\mathbf{a}^T\mathbf{x} \oplus b \oplus \overline{\boldsymbol{\varepsilon}})$
- $\Pr[(\mathbf{a},b)\leftarrow\mathrm{LSN}_{\rho,\varepsilon}{}^{\mathbf{x}}] = (b \oplus \overline{\boldsymbol{\rho}})(b \oplus \mathbf{a}^T\mathbf{x} \oplus \overline{\boldsymbol{\varepsilon}})2^{-n+1}$

$\mathrm{LPN}_{\varepsilon} \leq \mathrm{LSN}_{\rho,\varepsilon} \leq \mathrm{LPN}_{\varepsilon}$

- $\mathrm{LSN}_{\rho,\varepsilon}^{\mathbf{x}}$ is a method of producing a noisy subspace for **a**, using $\mathrm{LPN}_{\varepsilon}^{\mathbf{x}}$
  - Obtain $\breve{b}$ from Ber_{ρ}
  - Sample $\mathrm{LPN}_{\varepsilon}^{\mathbf{x}}$ until $b = \breve{b}$
- We can annihilate, **conditionally**
  - $b \leftarrow \mathrm{Ber}_{½}$ when $\mathbf{a}^{\mathsf{T}}\mathbf{x} = 1$



Game Sequence: Overall Idea

- Phase I & II keys: X_j & Y_j
  - Initially, $X_0 = Y_0$
- At each step, add random rank 1 matrix:
  - $(X,Y) \text{ -> } (X+(t+r)s^T, Y+ts^T) \text{ -> } (X, Y+rs^T)$
  - With each layer, X_j and Y_j grow further apart
  - after sufficiently many applications, $a^T X_j b^T$ is completely independent of $a^T Y_j b^T$

Conclusion

- MIM-secure HB-like protocol
  - Simple, Efficient
  - Technical tools may be useful elsewhere
  - Available on eprint: 2011/350

Conclusion

- MIM-secure HB-like protocol
  - Simple, Efficient
  - Technical tools may be useful elsewhere
  - Available on eprint: 2011/350
- Open question: Improve efficiency
  - HB, HB^+ are $O(n^2)$ computation

Conclusion

- MIM-secure HB-like protocol
  - Simple, Efficient
  - Technical tools may be useful elsewhere
  - Available on eprint: 2011/350
- Open question: Improve efficiency
  - HB, HB^+ are $O(n^2)$ computation
  - HB^N and [KPCJV] achieve $O(n^3)$ computation

Conclusion

- MIM-secure HB-like protocol
  - Simple, Efficient
  - Technical tools may be useful elsewhere
  - Available on eprint: 2011/350
- Open question: Improve efficiency
  - HB, HB^+ are $O(n^2)$ computation
  - HB^N and [KPCJV] achieve $O(n^3)$ computation
  - In upcoming work [BN] obtain $\omega(n^2)$
    - via $\omega(\log n)$ rank matrix key
    - and Four Russians Matrix Multiplication trick