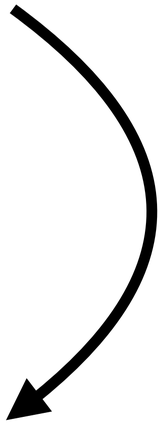
Let Attackers Program Ideal Models:
Modularity and Composability for Adaptive Compromise

Joseph Jaeger

Georgia Tech College of Computing
School of Cybersecurity and Privacy

2 Second Summary

SIM-AC definitions
[Jaeger, Tyagi C'20]



SIM*-AC definitions
[this work]

2 Second Summary

SIM-AC definitions
[Jaeger, Tyagi C'20]

SIM*-AC definitions
[this work]

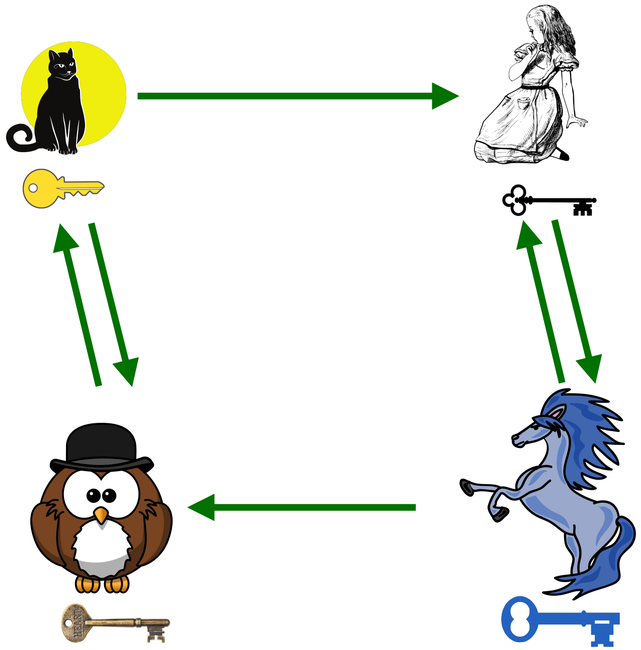
Key Differences:

- Simulator **explicitly** program ideal model
- **Attacker** allowed to program ideal model
- Universal quantification of simulator

Georgia Tech College of Computing
School of Cybersecurity and Privacy

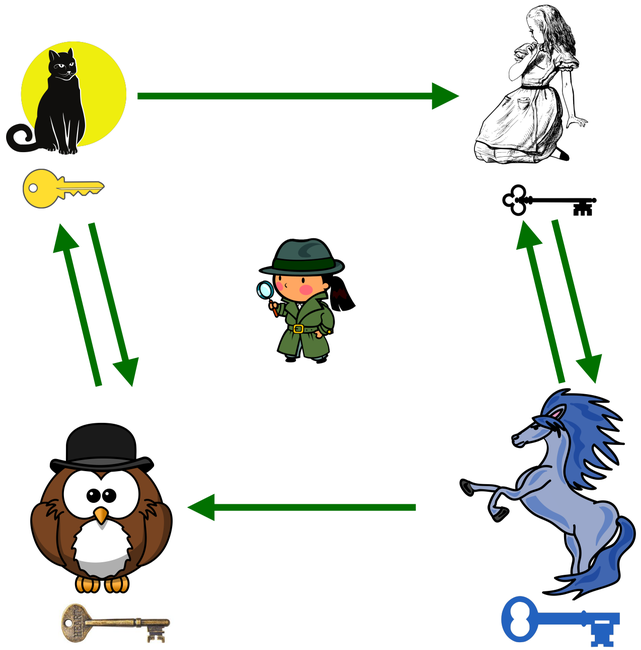
Adaptive Compromise Setting

(See also: Adaptive Corruptions/Security, Selective Opening Attacks, Non-committing encryption…)



Adaptive Compromise Setting

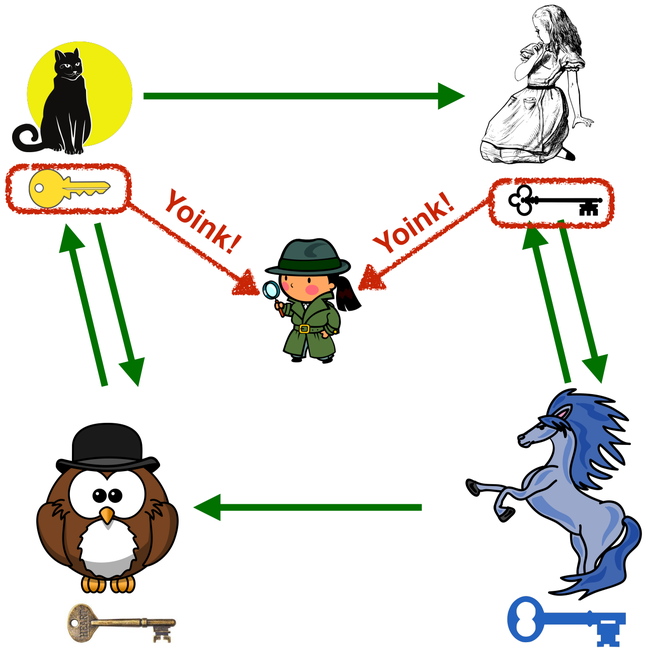
(See also: Adaptive Corruptions/Security, Selective Opening Attacks, Non-committing encryption…)



Georgia Tech College of Computing
School of Cybersecurity and Privacy

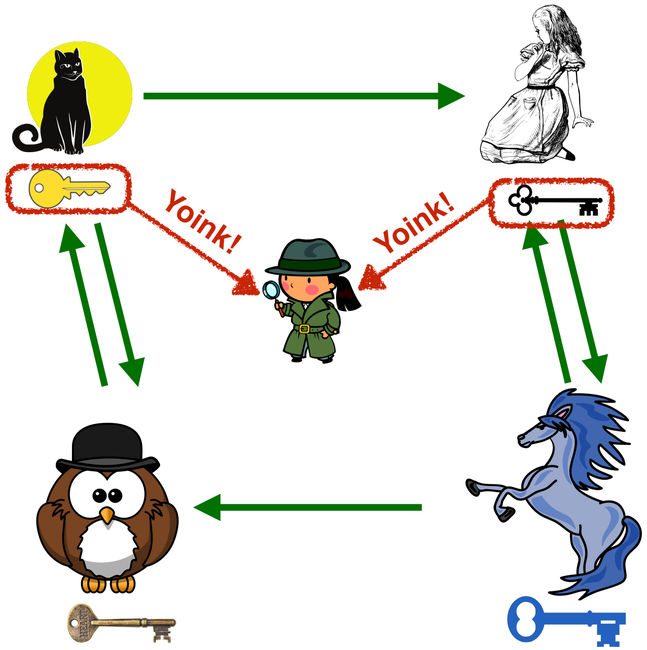
Adaptive Compromise Setting

(See also: Adaptive Corruptions/Security, Selective Opening Attacks, Non-committing encryption…)



Adaptive Compromise Setting

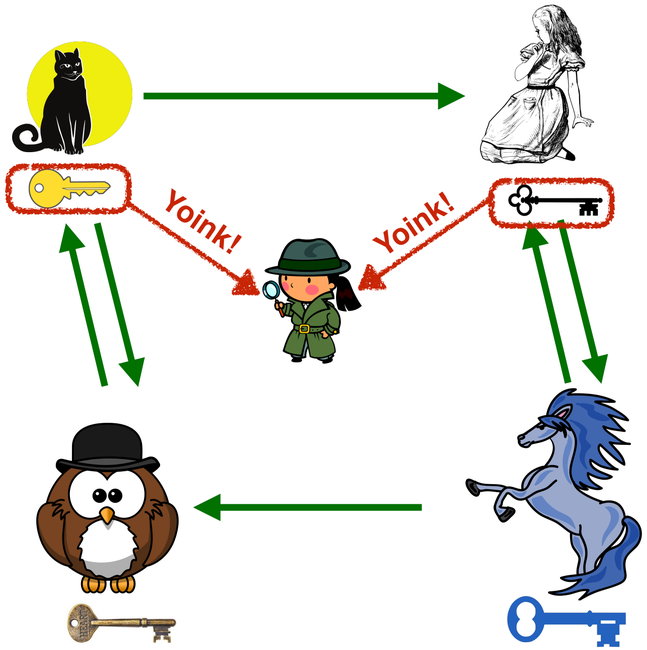
(See also: Adaptive Corruptions/Security, Selective Opening Attacks, Non-committing encryption…)



Arises in many settings

Adaptive Compromise Setting

(See also: Adaptive Corruptions/Security, Selective Opening Attacks, Non-committing encryption…)



Arises in many settings

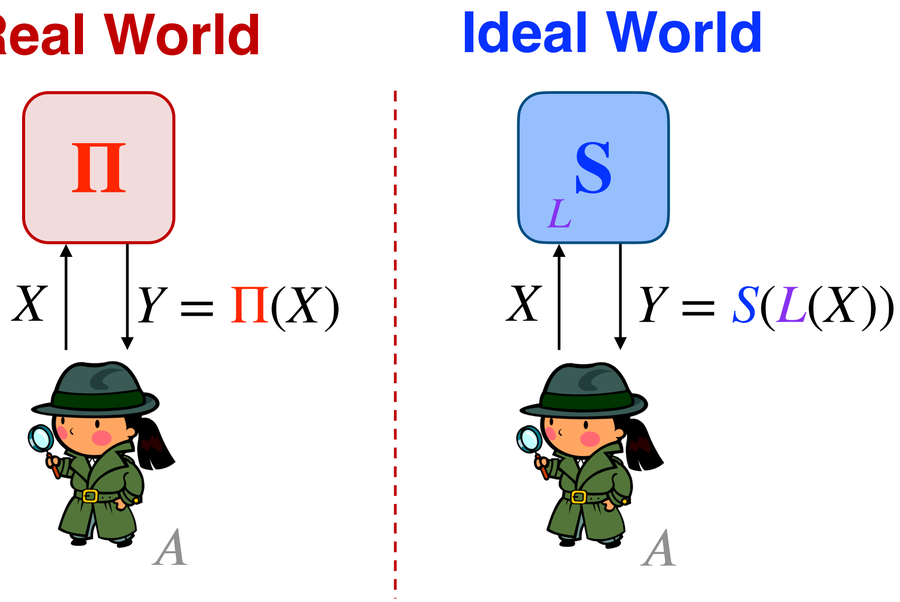
Primitives: Secure Computation, Commitment Schemes, Encryption, PRFs…

Definitional Frameworks: Game-based, Simulation-based (UC, CC, …)

Georgia Tech College of Computing
School of Cybersecurity and Privacy

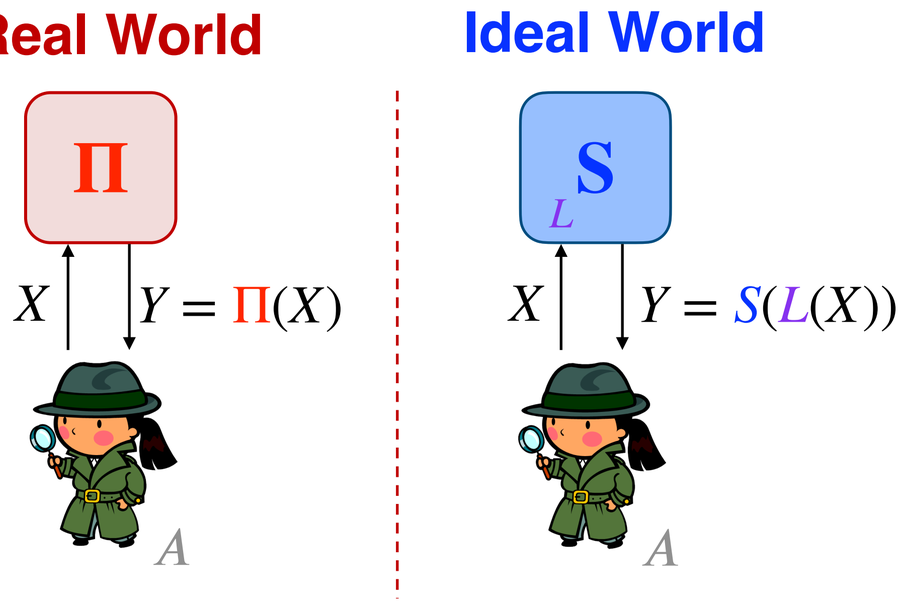
SIM-AC Definitions [Jaeger, Tyagi C'20]

Online Simulation Setting



SIM-AC Definitions [Jaeger, Tyagi C'20]

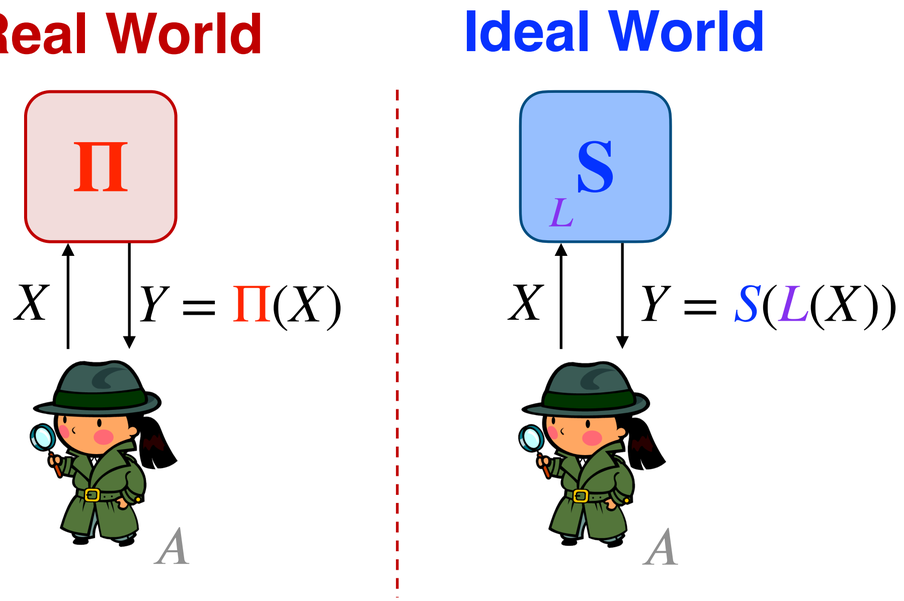
Online Simulation Setting



$$\mathbf{Adv}(A) = \Pr[A(\Pi) = 1] - \Pr[A(S) = 1]$$

SIM-AC Definitions [Jaeger, Tyagi C'20]

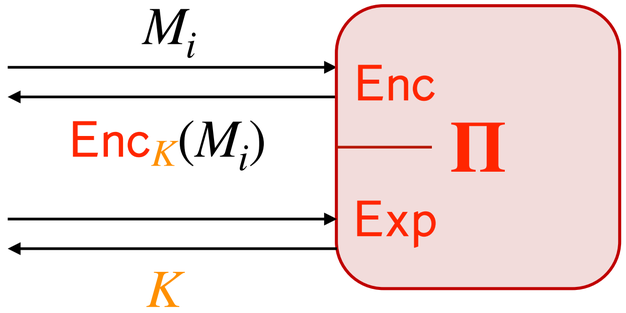
Online Simulation Setting



$$\mathbf{Adv}(A) = \Pr[A(\Pi) = 1] - \Pr[A(S) = 1]$$

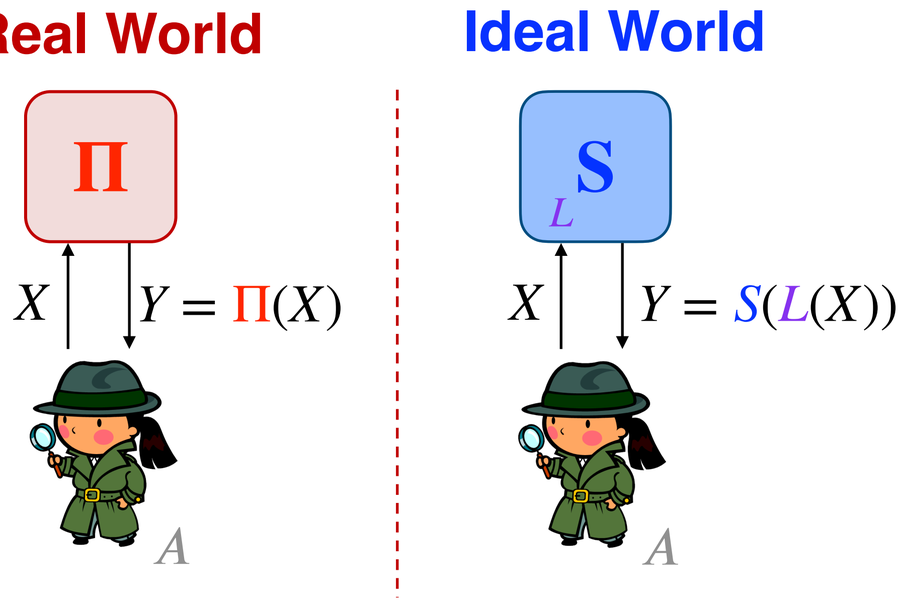
Symmetric Encryption (SIM-AC-CPA)

Real World



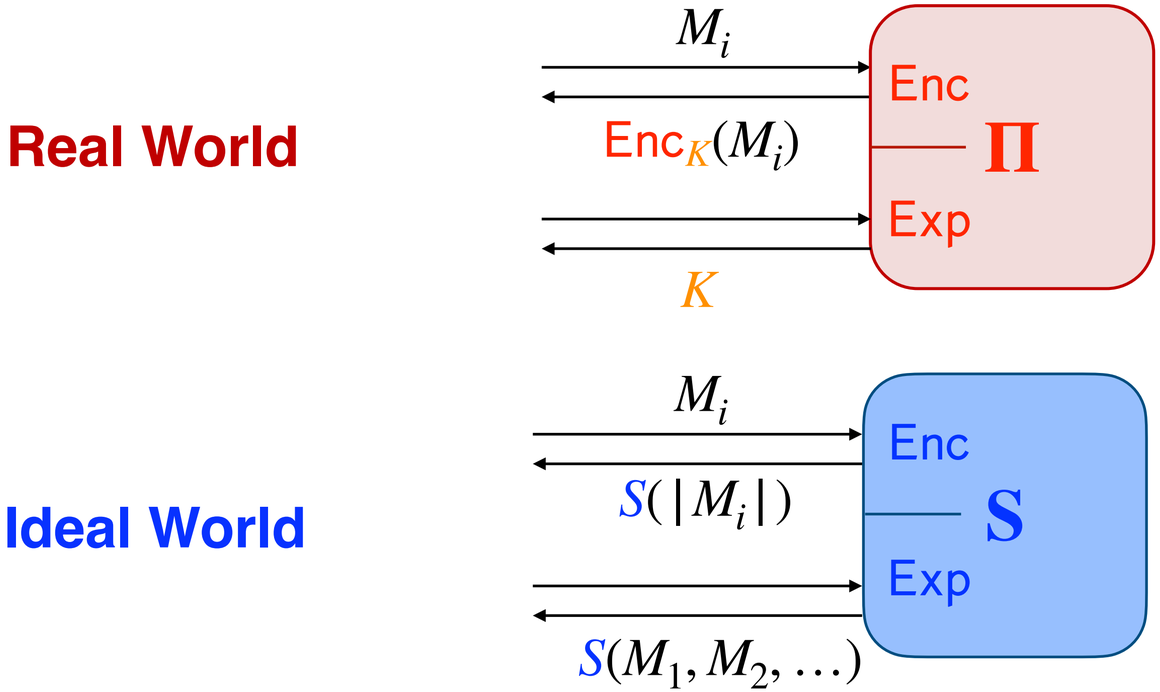
SIM-AC Definitions [Jaeger, Tyagi C'20]

Online Simulation Setting



$$\mathbf{Adv}(A) = \Pr[A(\Pi) = 1] - \Pr[A(S) = 1]$$

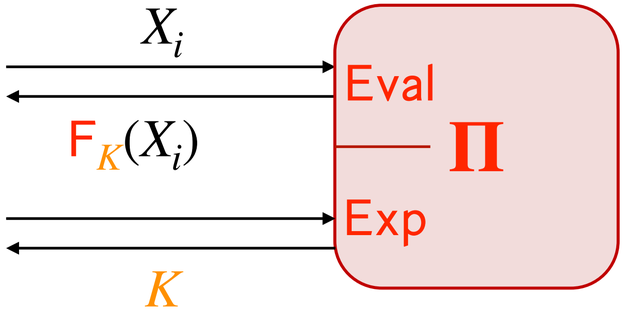
Symmetric Encryption (SIM-AC-CPA)



SIM-AC Definitions [Jaeger, Tyagi C'20]

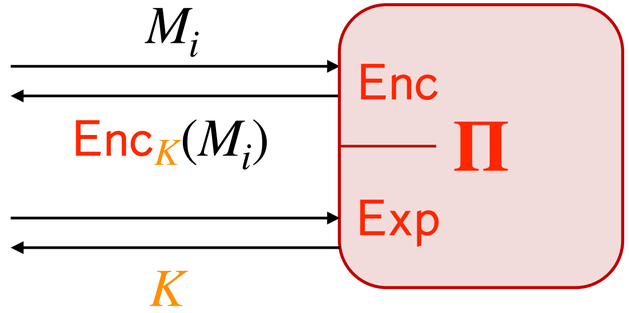
Pseudorandom Function (SIM-AC-PRF)

Real World

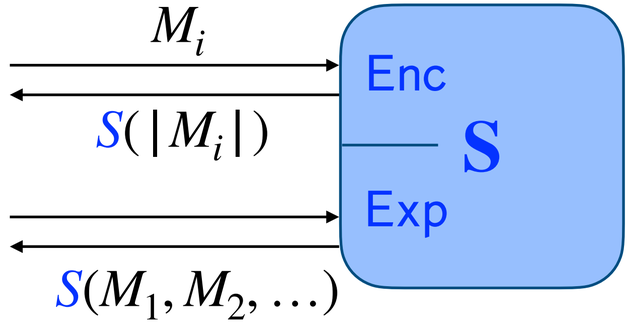


Symmetric Encryption (SIM-AC-CPA)

Real World



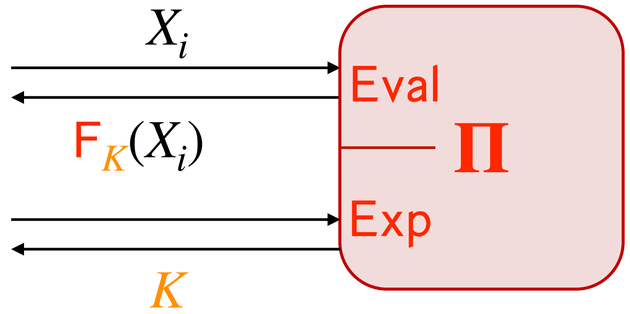
Ideal World



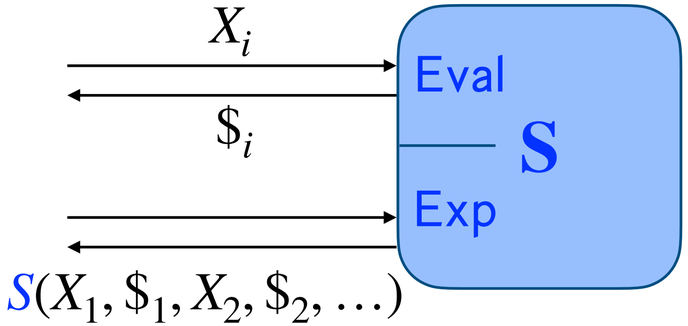
SIM-AC Definitions [Jaeger, Tyagi C'20]

Pseudorandom Function (SIM-AC-PRF)

Real World

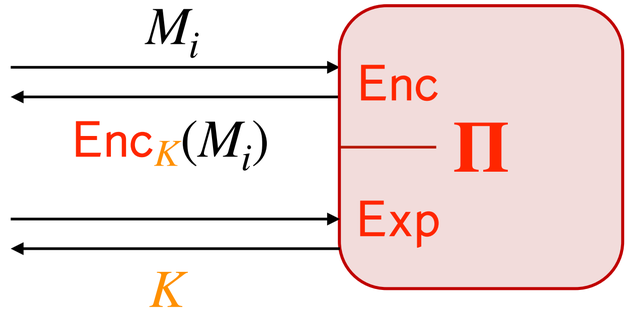


Ideal World

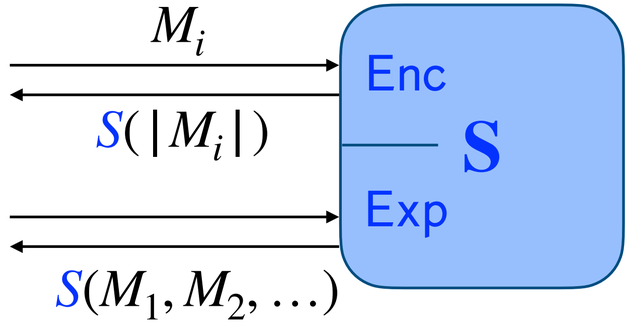


Symmetric Encryption (SIM-AC-CPA)

Real World



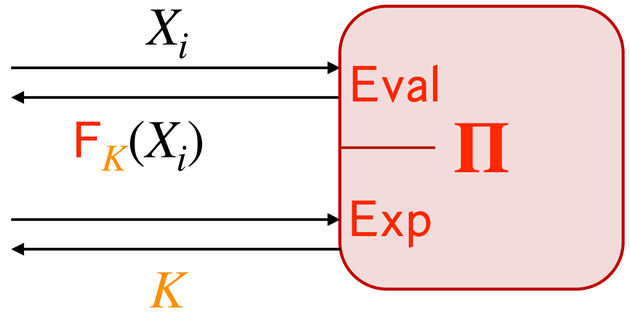
Ideal World



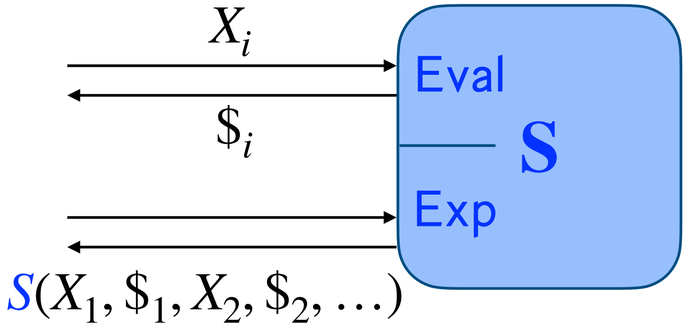
SIM-AC Definitions [Jaeger, Tyagi C'20]

Pseudorandom Function (SIM-AC-PRF)

Real World

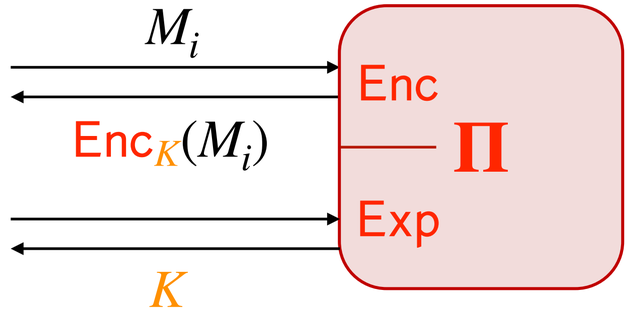


Ideal World

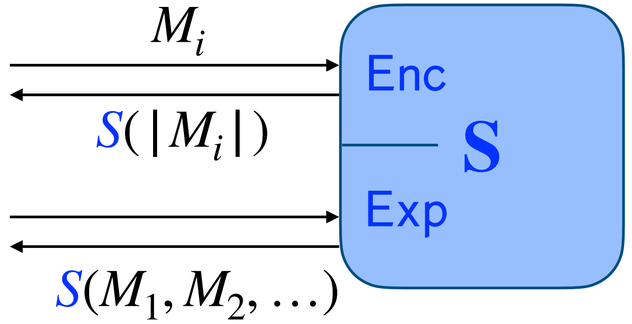


Symmetric Encryption (SIM-AC-CPA)

Real World



Ideal World



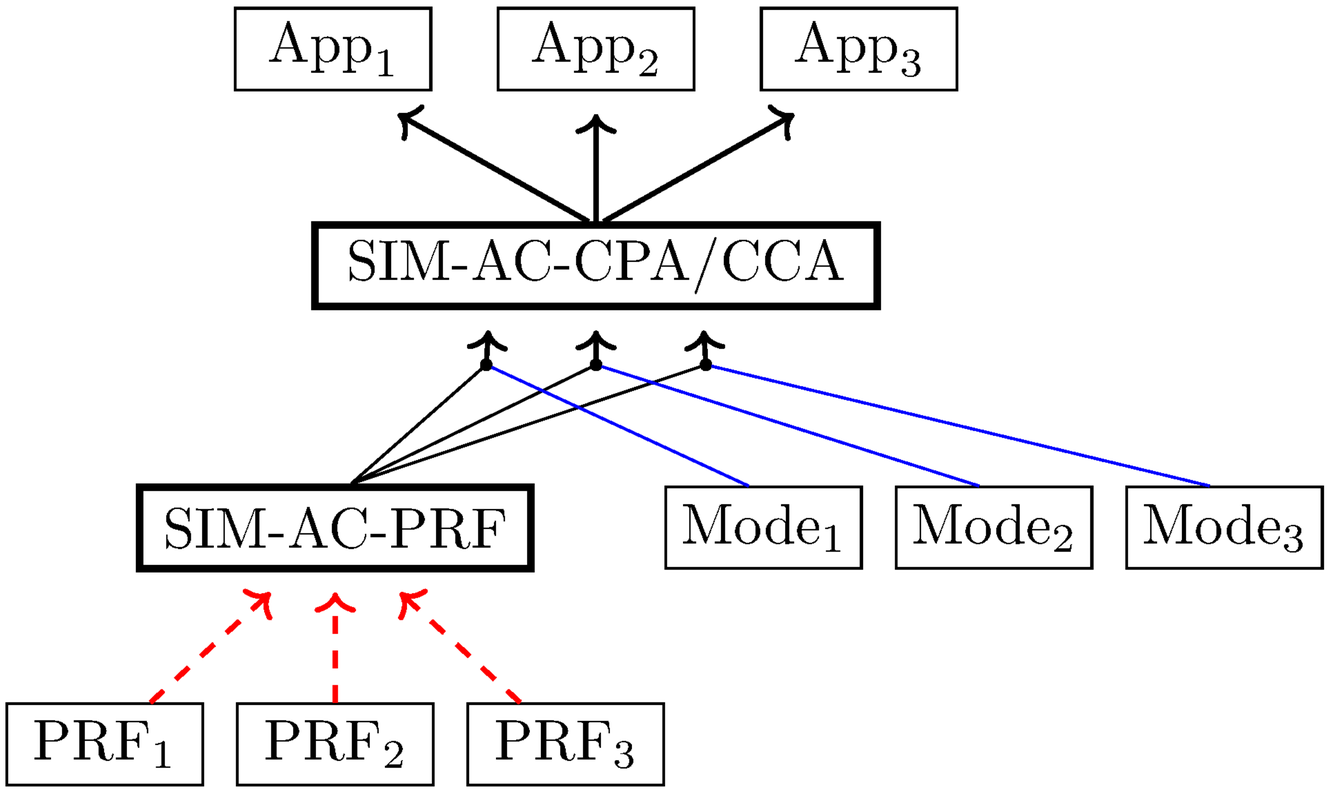
Not shown:

Requires ideal model. [Nielsen C'02]

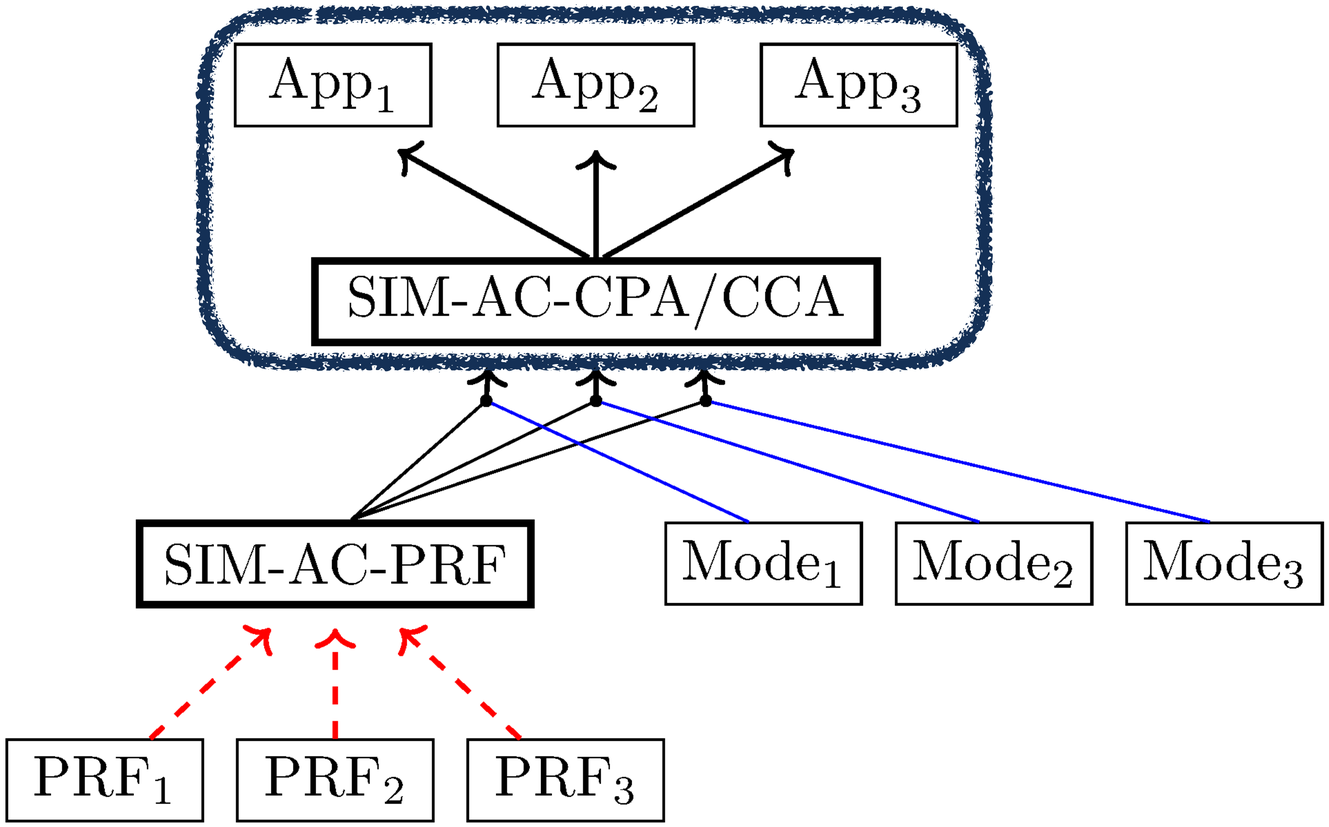
Multi-user definitions.

Georgia Tech College of Computing
School of Cybersecurity and Privacy

Benefits of SIM-AC [Jaeger, Tyagi C'20]



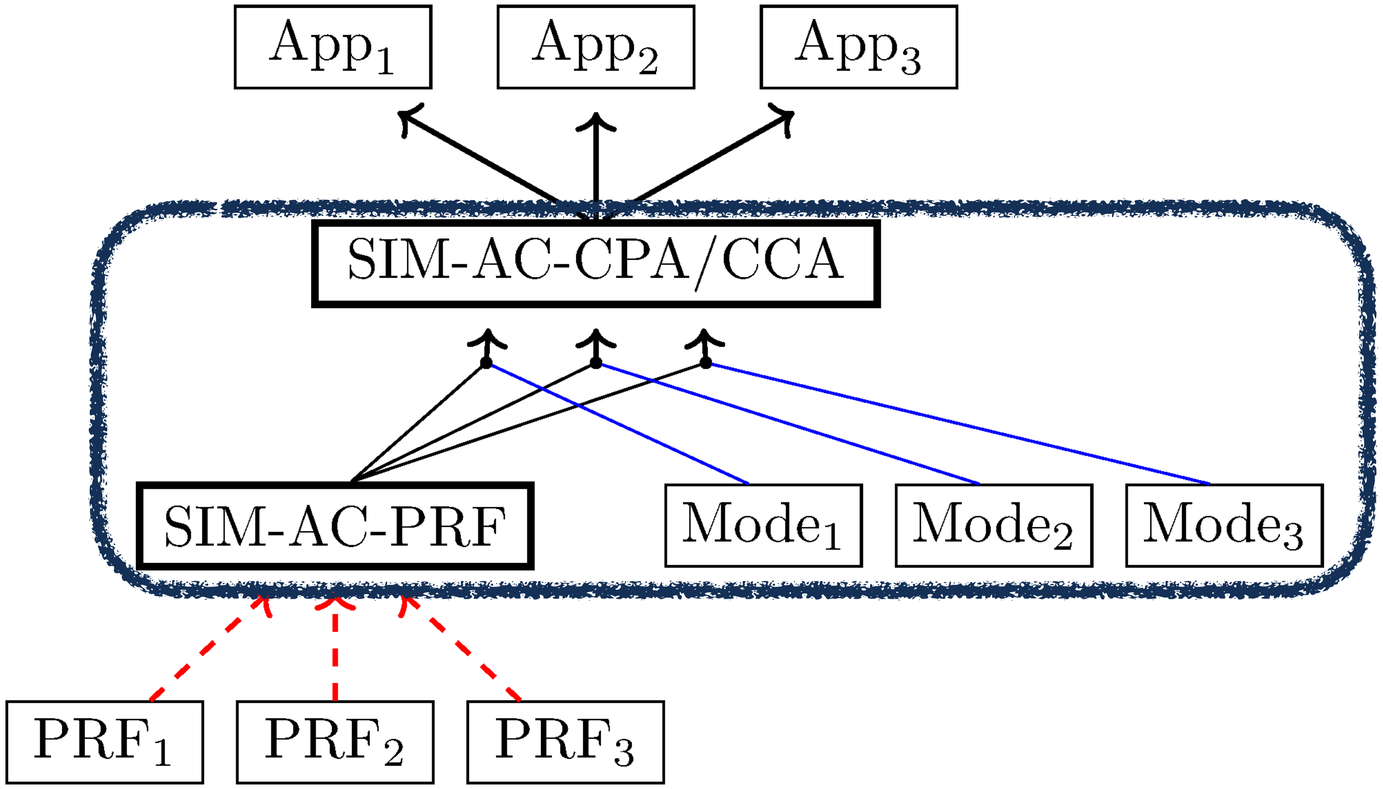
Benefits of SIM-AC [Jaeger, Tyagi C'20]



High-level proofs:

Searchable encryption
Revocable Cloud Storage
OPAQUE

Benefits of SIM-AC [Jaeger, Tyagi C'20]



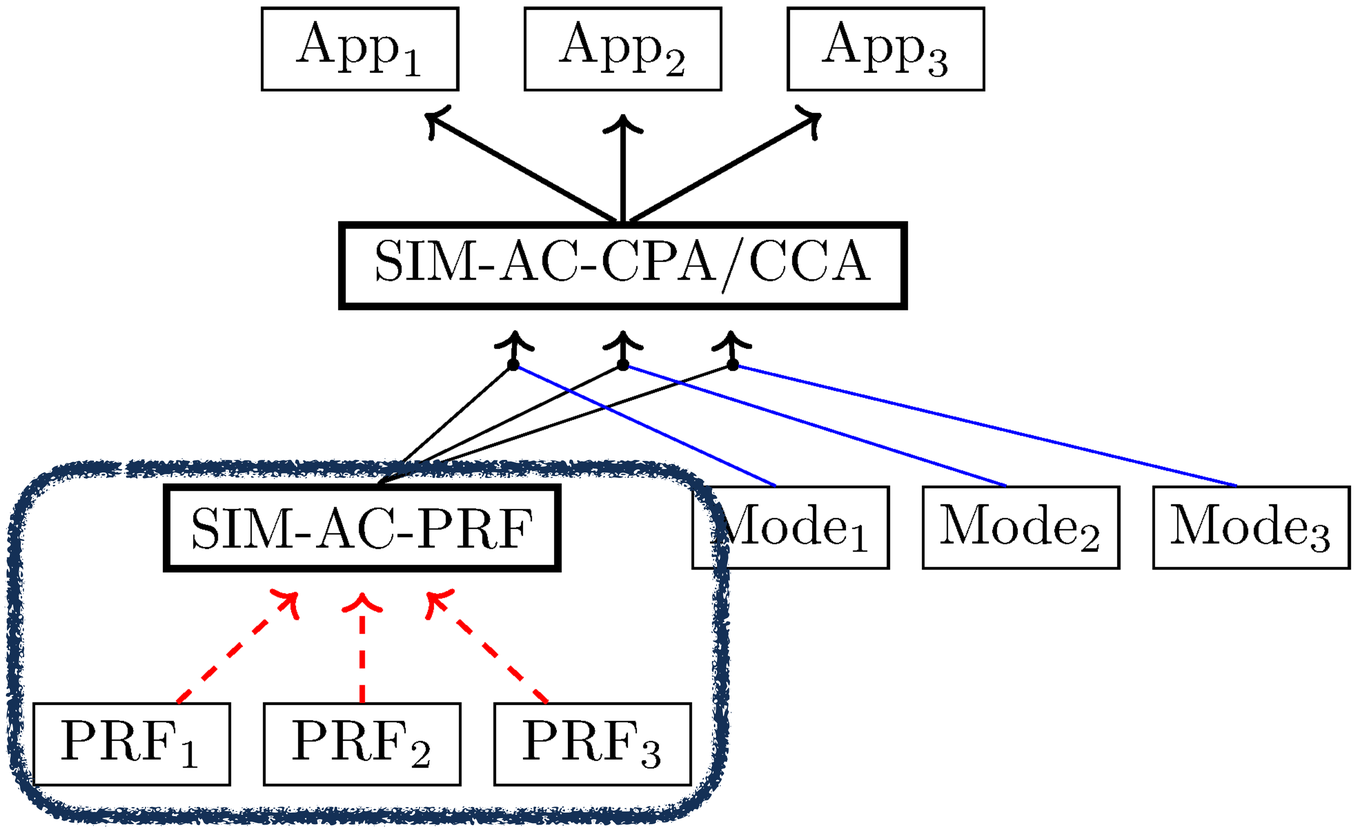
High-level proofs:

Searchable encryption
Revocable Cloud Storage
OPAQUE

Intermediate-level proofs:

CTR, CBC, …
Enc-then-Mac

Benefits of SIM-AC [Jaeger, Tyagi C'20]



High-level proofs:

Searchable encryption
Revocable Cloud Storage
OPAQUE

Intermediate-level proofs:

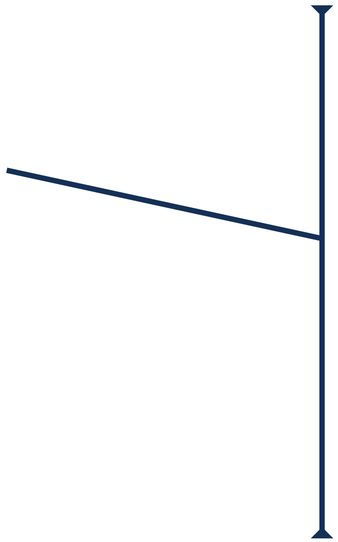
CTR, CBC, …
Enc-then-Mac

Low-level proofs:

Random oracle PRF
Ideal cipher PRF

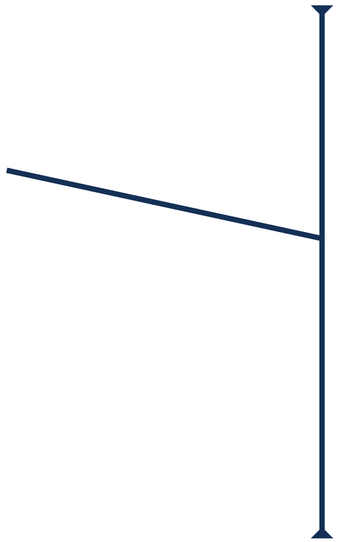
Benefits of SIM-AC [Jaeger, Tyagi C'20]

Current work shows shortcomings here



Benefits of SIM-AC [Jaeger, Tyagi C'20]

Current work shows shortcomings here



High-level proofs:

Searchable encryption
Revocable Cloud Storage
OPAQUE

Intermediate-level proofs:

CTR, CBC, …
Enc-then-Mac

Low-level proofs:

Random oracle PRF
Ideal cipher PRF

Our Contributions

1. SIM-AC and it **shortcomings**.

Our Contributions

1. SIM-AC and it **shortcomings**.

2. SIM*-AC and it **solution** to shortcomings.

   - Multiple schemes with same primitive
   - Multiple uses of same scheme
   - Single-user security → Multi-user security

Our Contributions

1. SIM-AC and it **shortcomings**.

2. SIM*-AC and it **solution** to shortcomings.

   - Multiple schemes with same primitive
   - Multiple uses of same scheme
   - Single-user security → Multi-user security

3. **Recovering prior results:** SIM-AC results hold with SIM*-AC.

Georgia Tech College of Computing
School of Cybersecurity and Privacy

Our Contributions

1. SIM-AC and it **shortcomings**.

2. SIM*-AC and it **solution** to shortcomings.
   - Multiple schemes with same primitive
   - Multiple uses of same scheme
   - Single-user security → Multi-user security

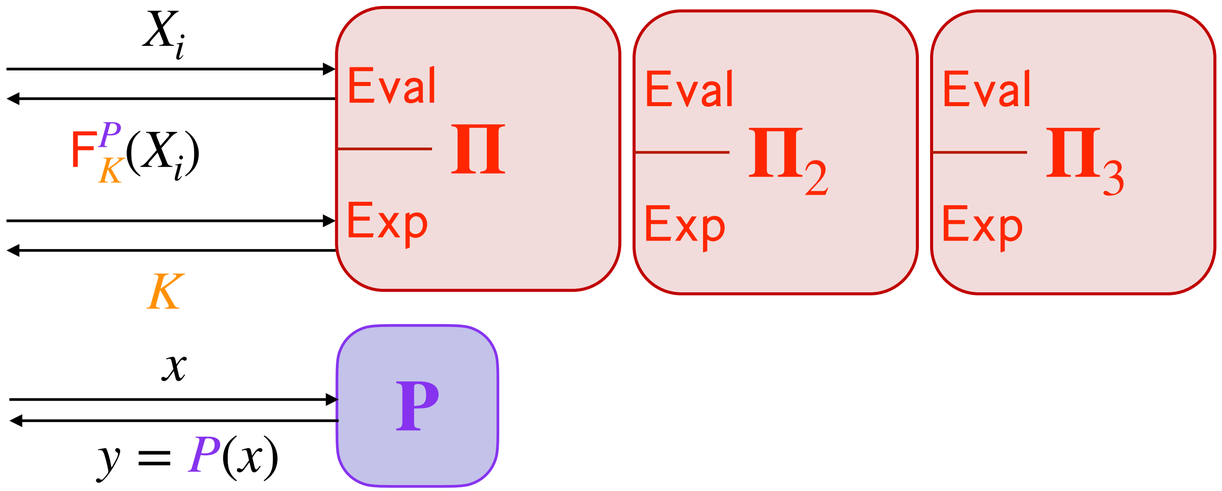
3. **Recovering prior results:** SIM-AC results hold with SIM*-AC.

4. SIM*-AC for **asymmetric encryption**.
   - Comparisons to prior definitions
   - KEM/DEM hybrid encryption
   - Fujisaki-Okamoto style transforms

Georgia Tech College of Computing
School of Cybersecurity and Privacy

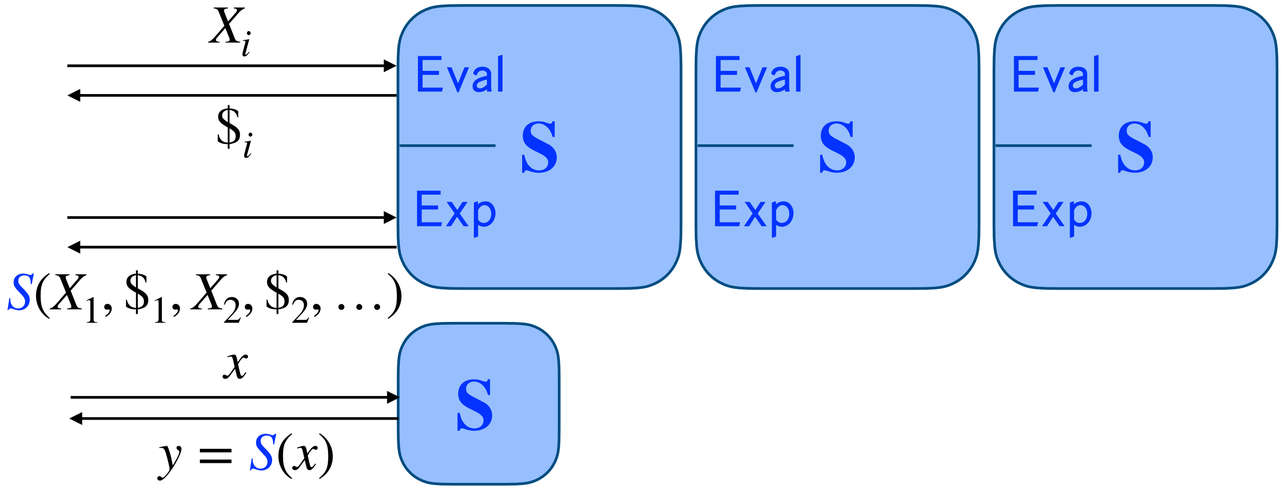
1. SIM-AC Shortcomings

Real World



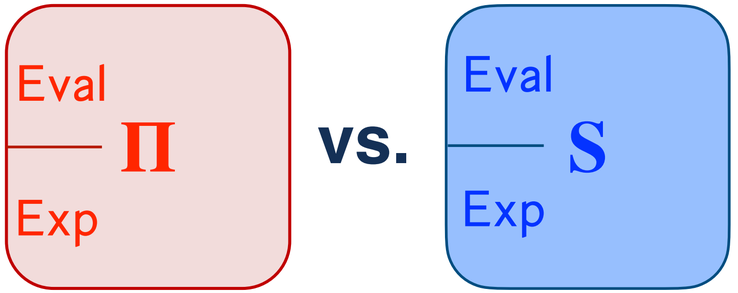
SIM-AC-PRF

Ideal World



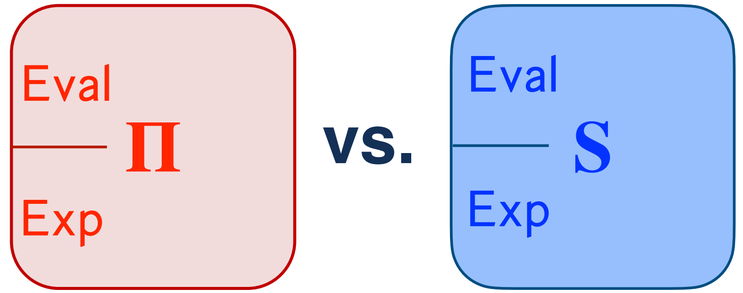
1. SIM-AC Shortcomings

Does single-user security → multi-user security?

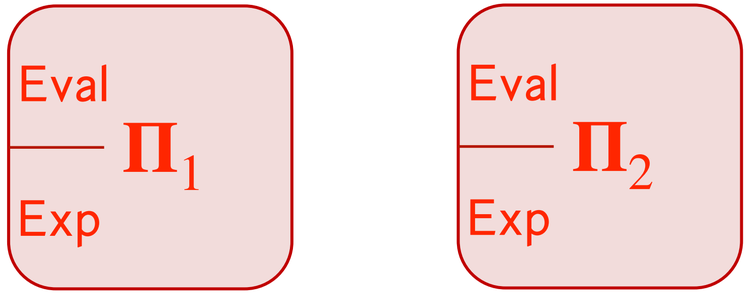


1. SIM-AC Shortcomings

Does single-user security → multi-user security?

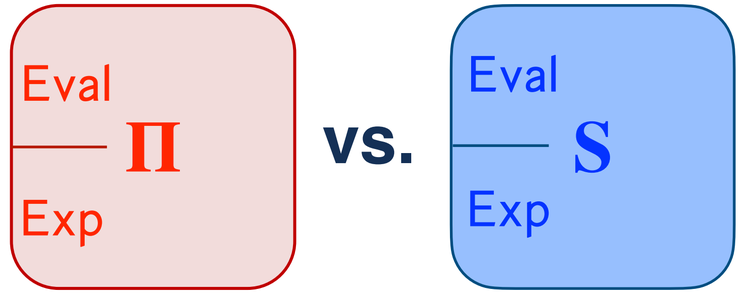


Real World

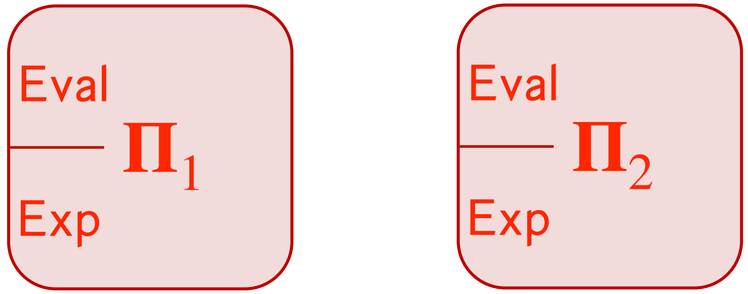


1. SIM-AC Shortcomings

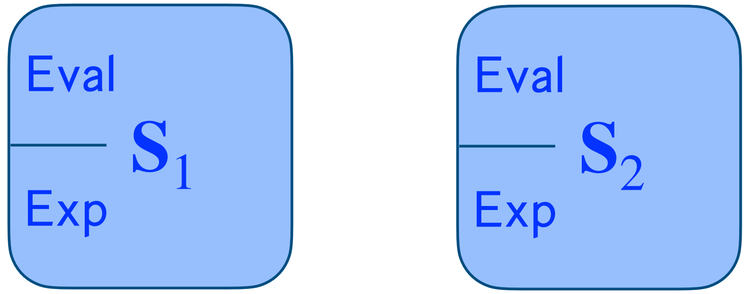
Does single-user security → multi-user security?



Real World

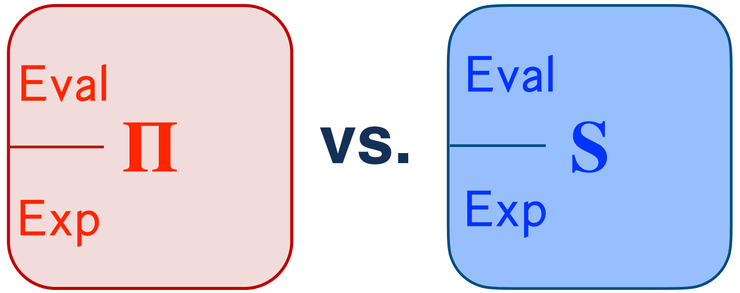


Ideal World

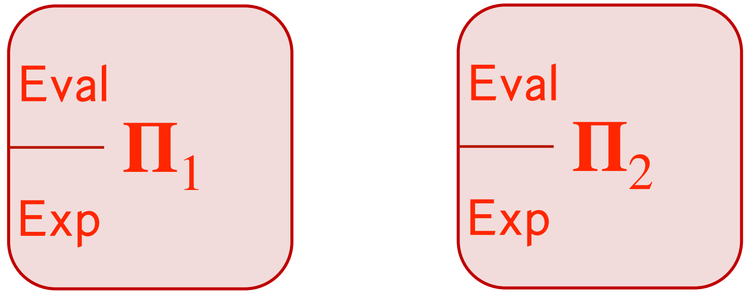


1. SIM-AC Shortcomings

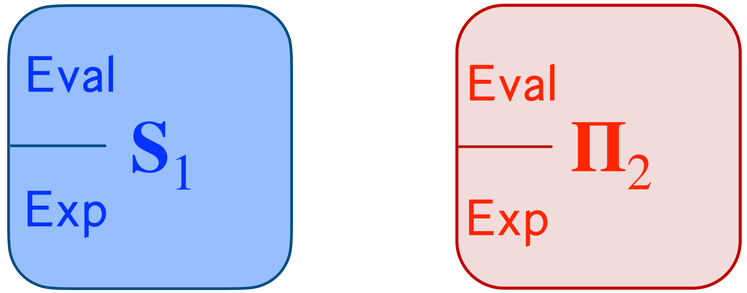
Does single-user security → multi-user security?



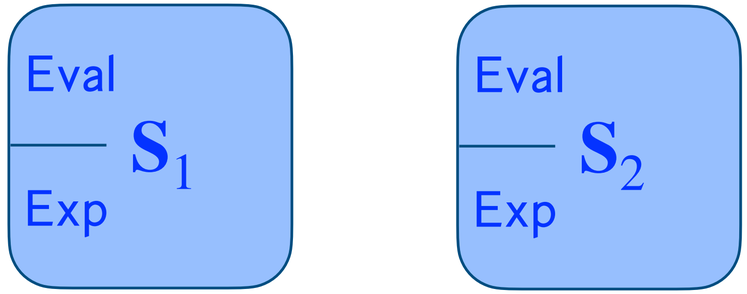
Real World



Hybrid World



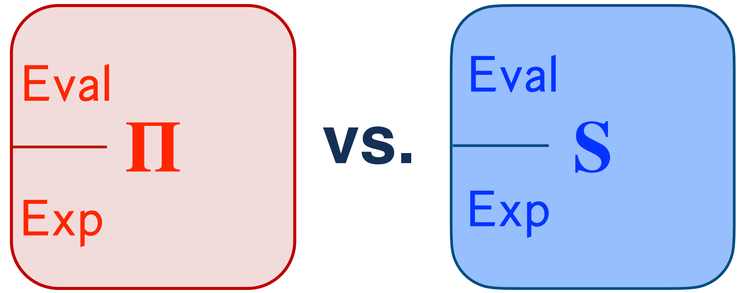
Ideal World

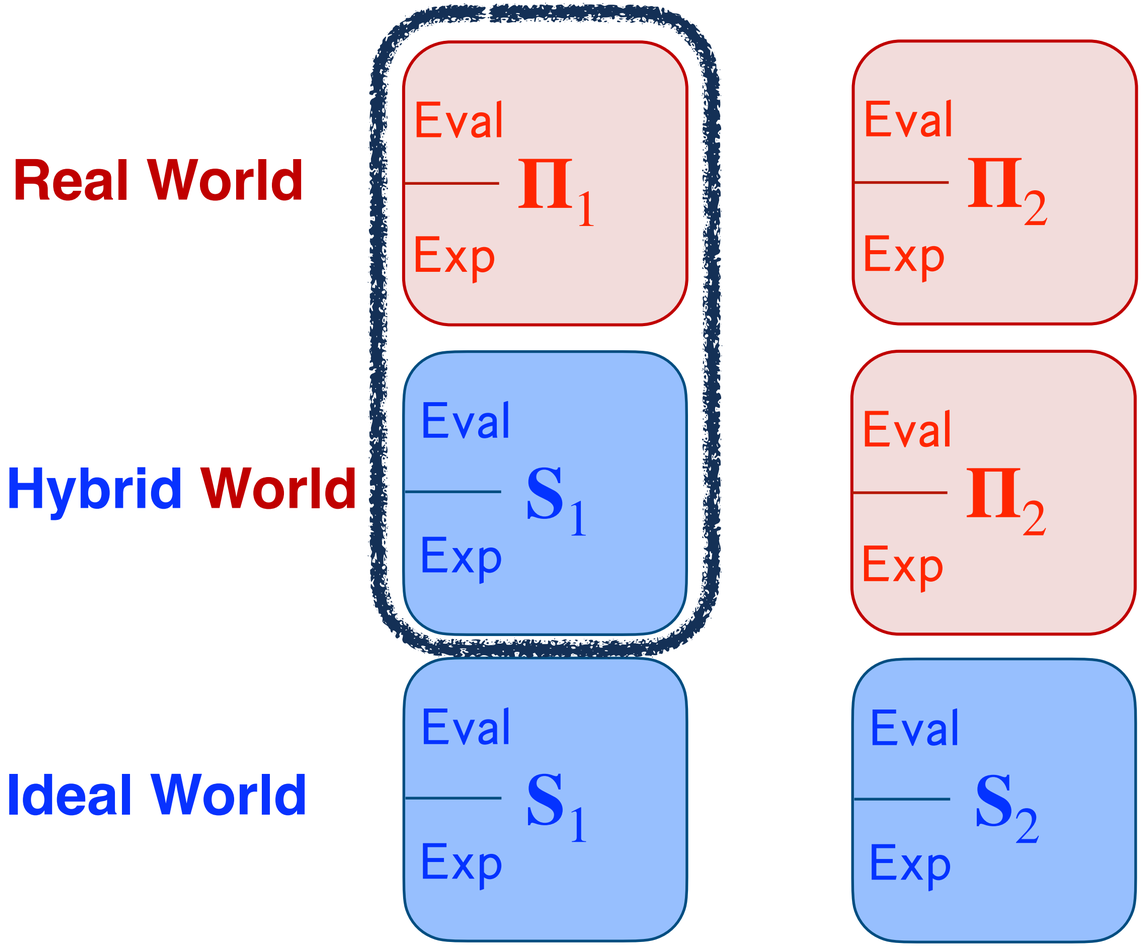


Georgia Tech College of Computing
School of Cybersecurity and Privacy

1. SIM-AC Shortcomings

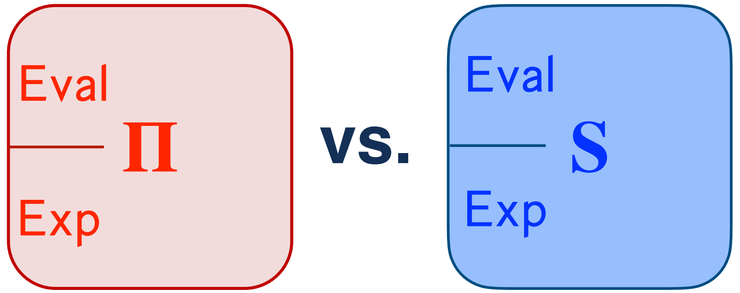
Does single-user security → multi-user security?





1. SIM-AC Shortcomings

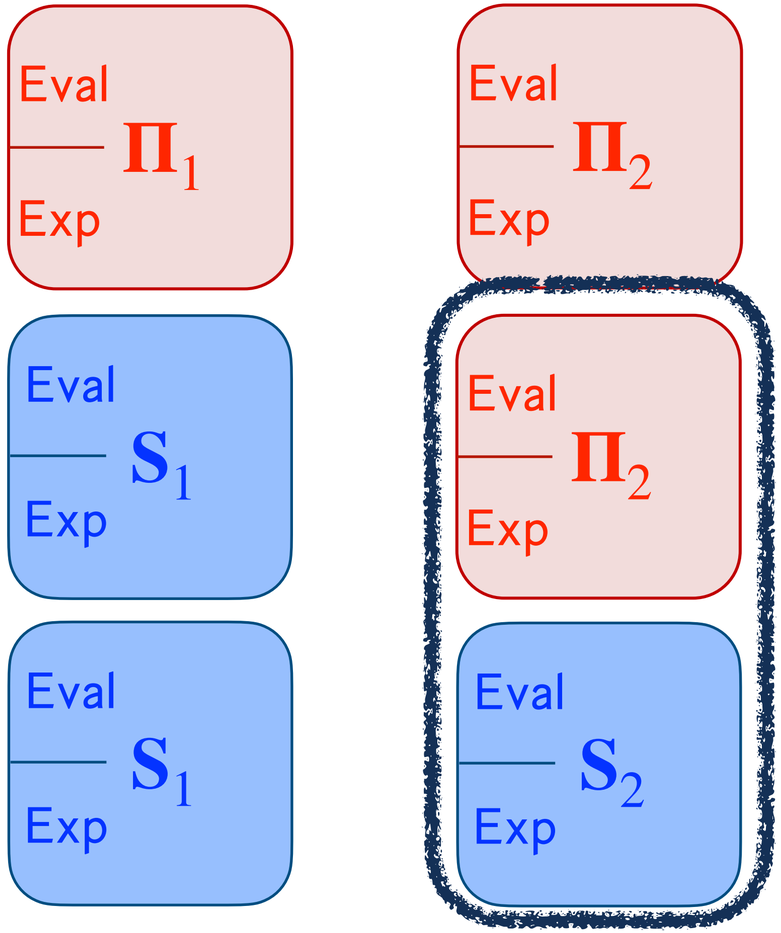
Does single-user security → multi-user security?



Real World

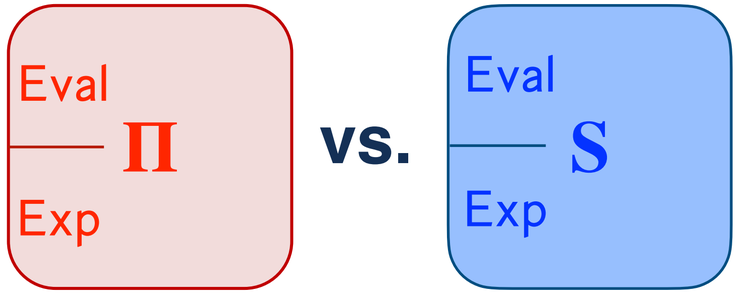
Hybrid World

Ideal World

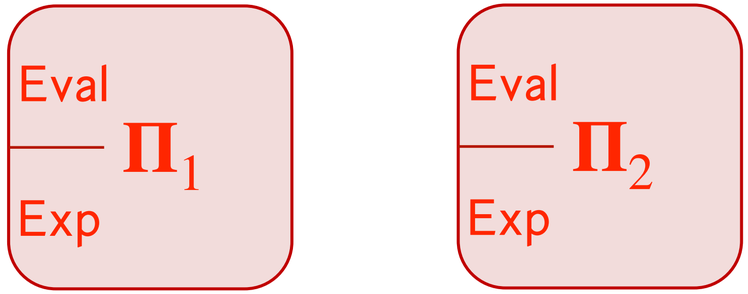


1. SIM-AC Shortcomings

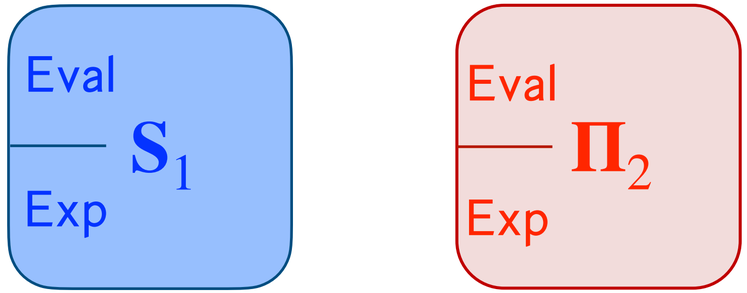
Does single-user security → multi-user security?



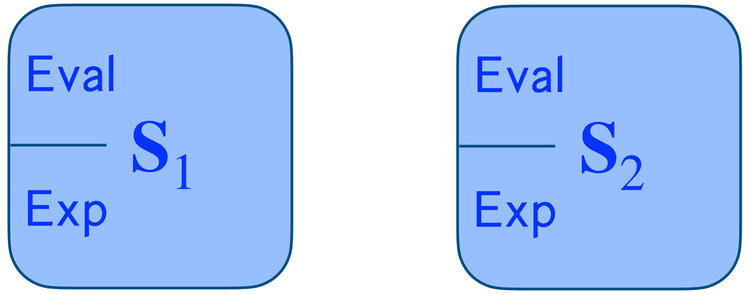
Real World



Hybrid World



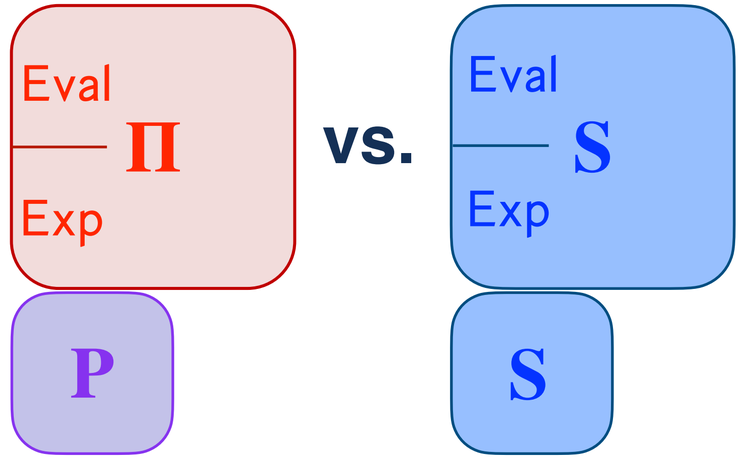
Ideal World



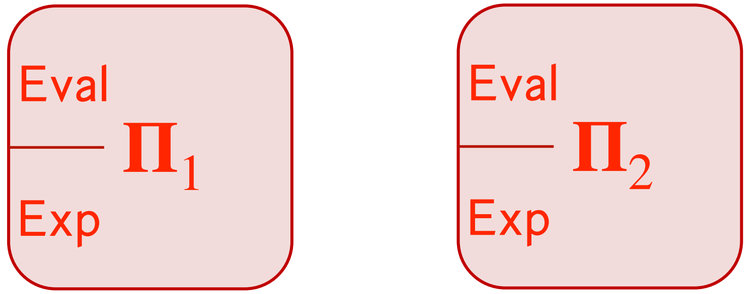
Georgia Tech College of Computing
School of Cybersecurity and Privacy

1. SIM-AC Shortcomings

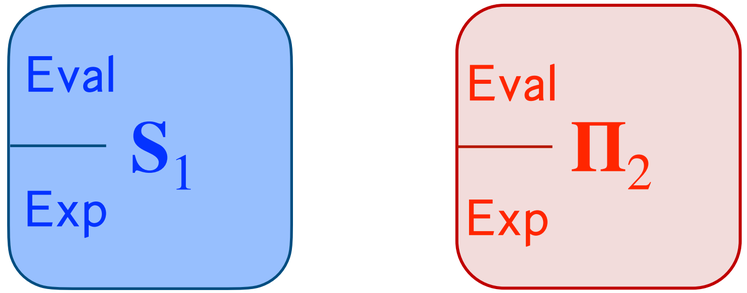
Does single-user security → multi-user security?



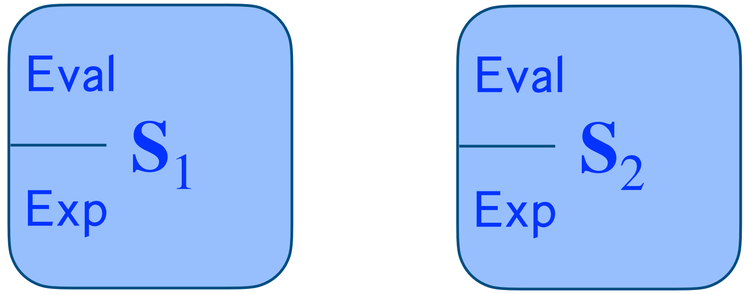
Real World



Hybrid World

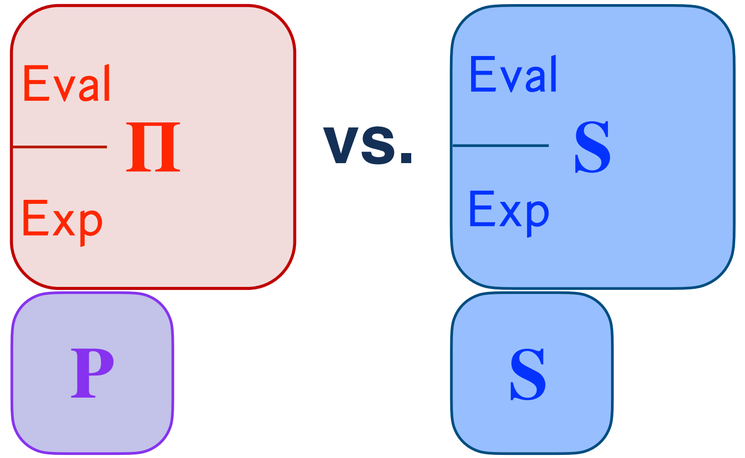


Ideal World



1. SIM-AC Shortcomings

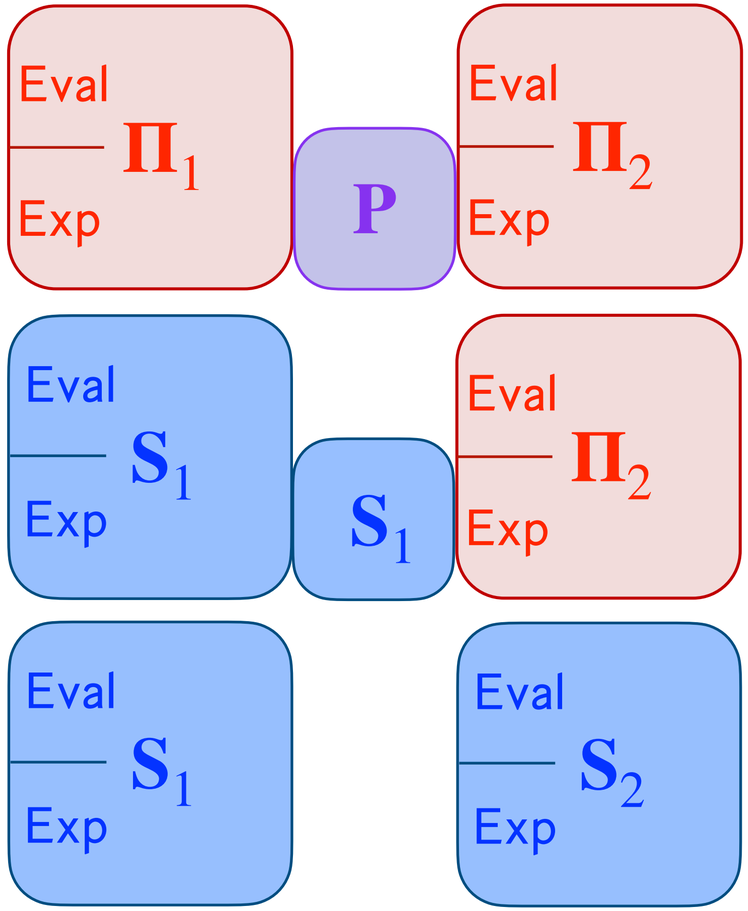
Does single-user security → multi-user security?



Real World

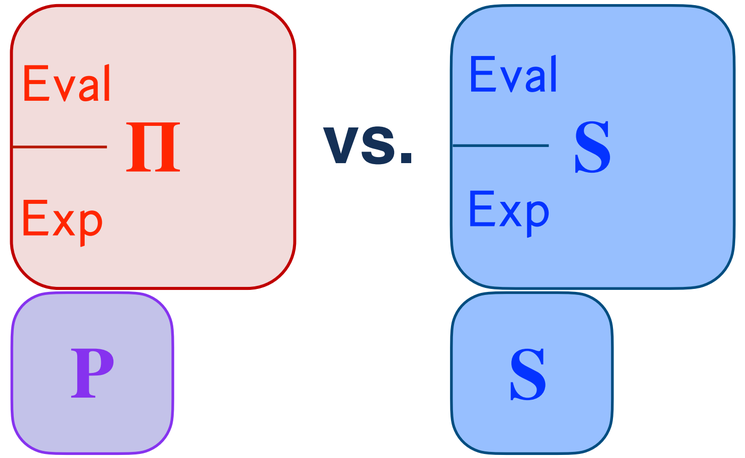
Hybrid World

Ideal World



1. SIM-AC Shortcomings

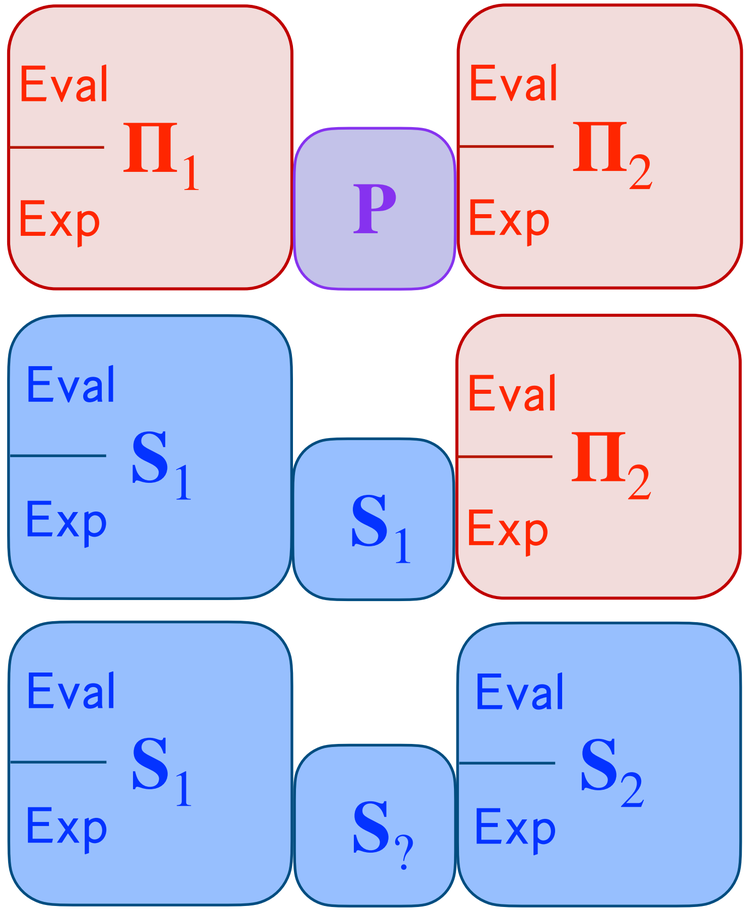
Does single-user security → multi-user security?



Real World

Hybrid World

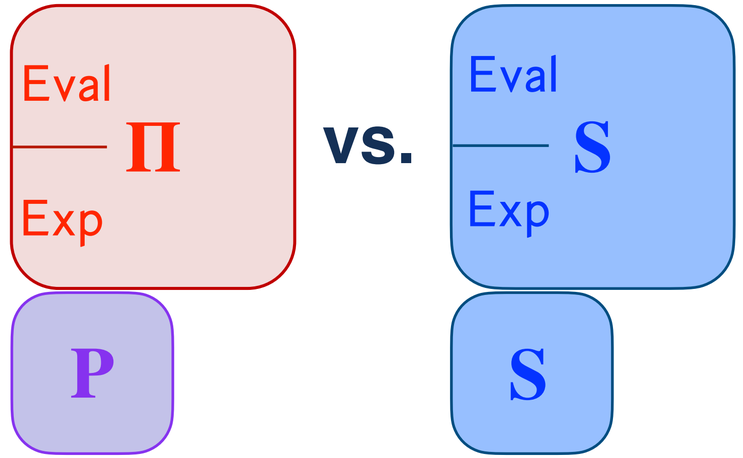
Ideal World

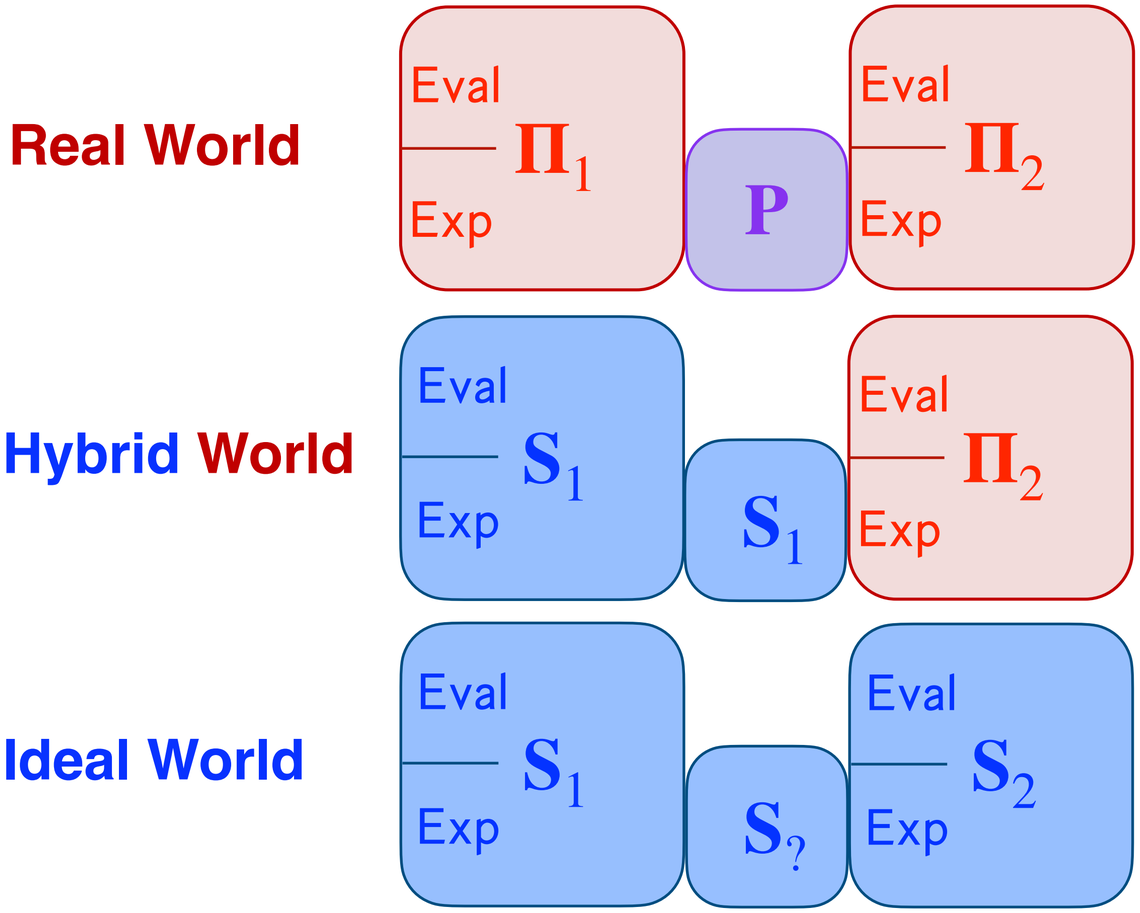


Georgia Tech College of Computing
School of Cybersecurity and Privacy

1. SIM-AC Shortcomings

Does single-user security → multi-user security?

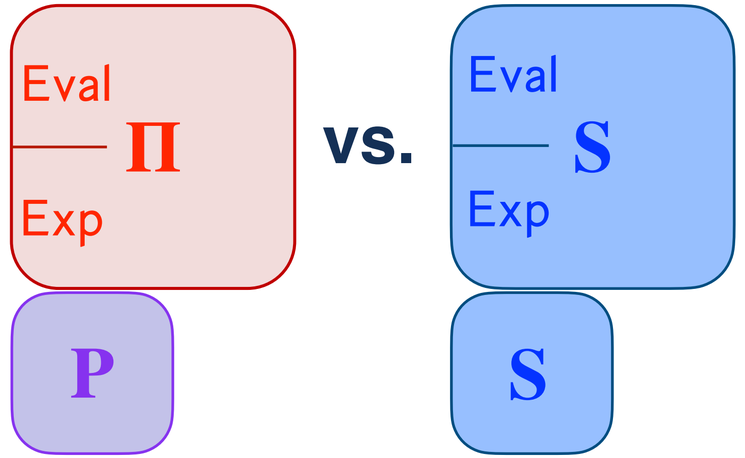


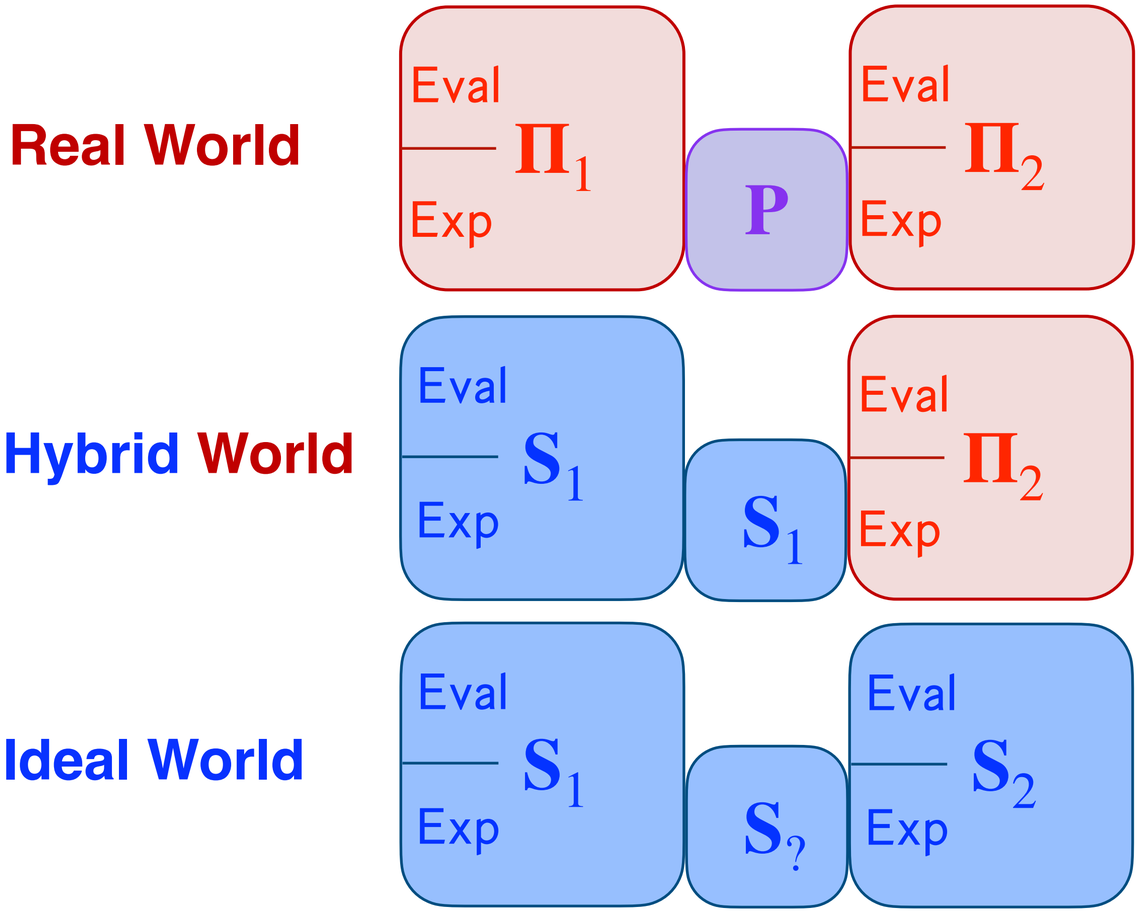


Simulator completely replacing P prevents reuse.

1. SIM-AC Shortcomings

Does single-user security → multi-user security?





Simulator completely replacing P prevents reuse.

Multiple uses of the same scheme:

- Multi-user security
- Cascade PRF
- Searchable encryption*

Multiple schemes with the same primitive:

- Searchable encryption*
- Revocable Cloud Storage*
- Enc-then-Mac*

Georgia Tech College of Computing
School of Cybersecurity and Privacy

2. SIM*-AC Solution

One “solution”, don’t re-use P.

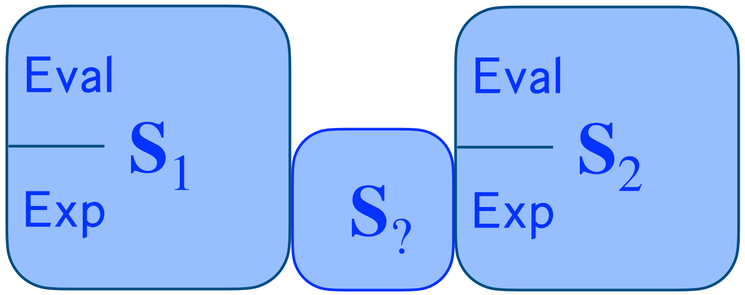
Paper 2020/241

Separate Your Domains: NIST PQC KEMs, Oracle Cloning and Read-Only Indifferentiability

Mihir Bellare, Hannah Davis, and Felix Günther

2. SIM*-AC Solution

Ideal World

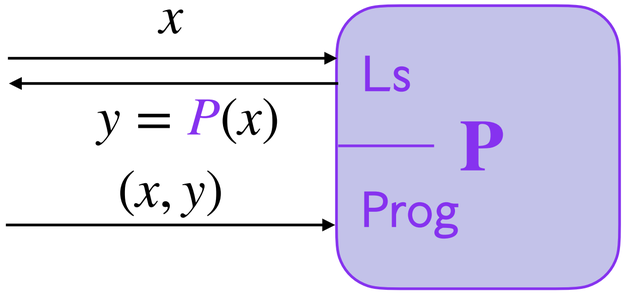


2. SIM*-AC Solution

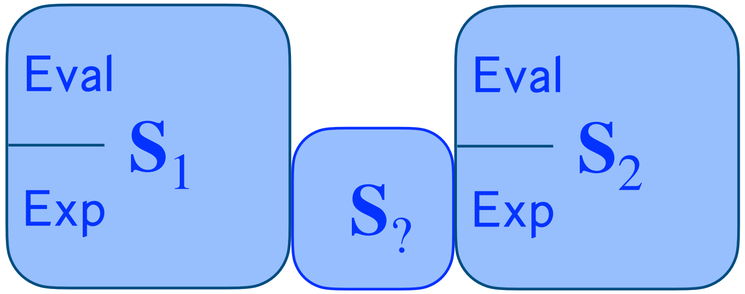
Modify ideal primitive

Lazy sampling - Define P(x) when needed.

Programmable - Give (x,y) to define P(x)=y.



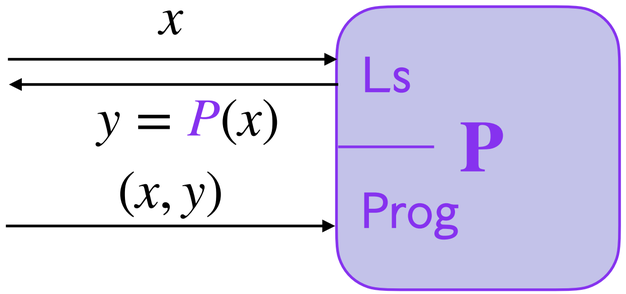
Ideal World



2. SIM*-AC Solution

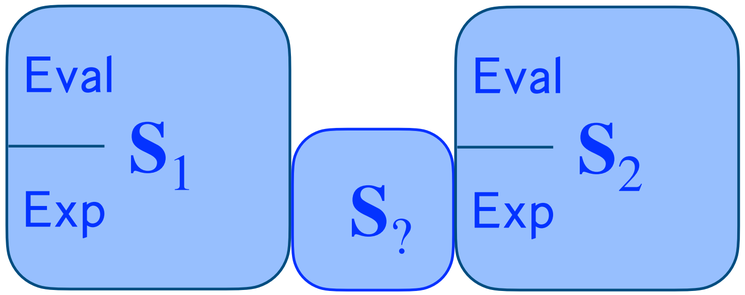
Modify ideal primitive

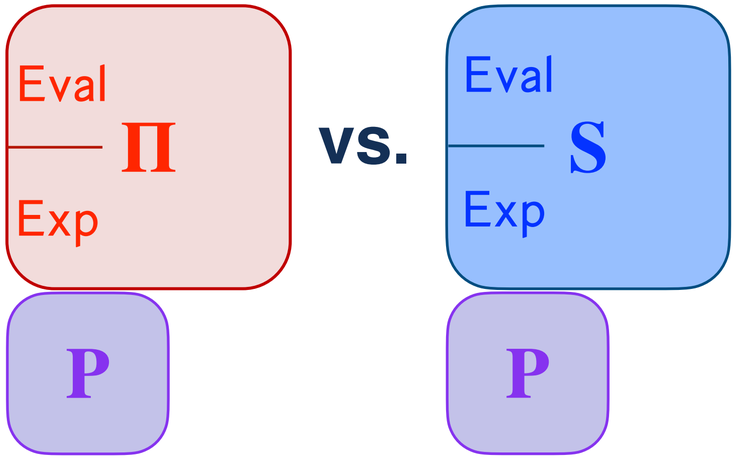
Lazy sampling - Define P(x) when needed.
Programmable - Give (x,y) to define P(x)=y.



Have S explicitly program P.

Ideal World



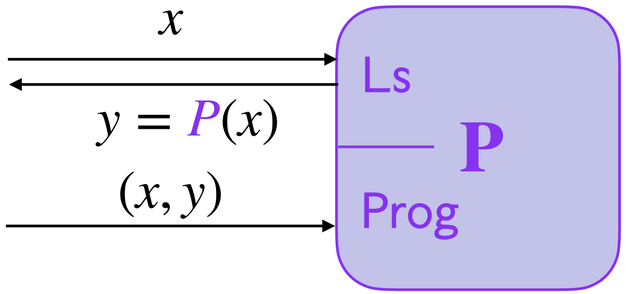


Georgia Tech College of Computing
School of Cybersecurity and Privacy

2. SIM*-AC Solution

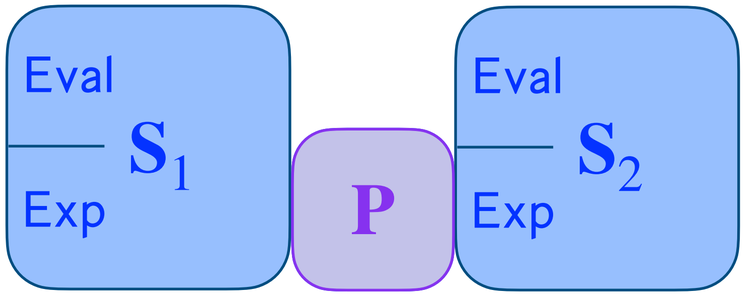
Modify ideal primitive

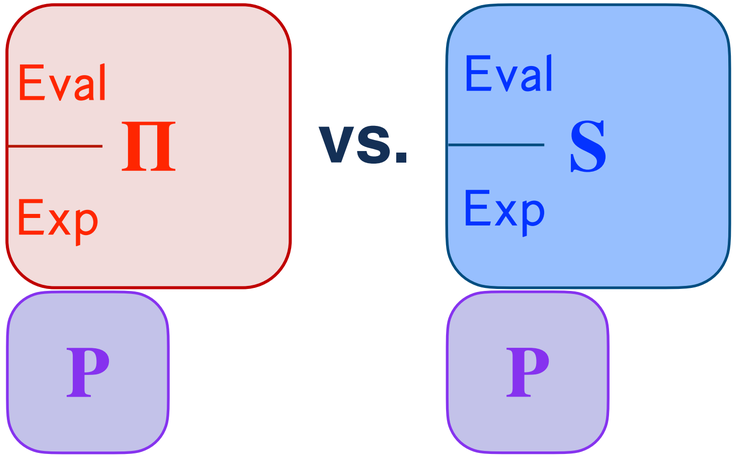
Lazy sampling - Define P(x) when needed.
Programmable - Give (x,y) to define P(x)=y.



Have S explicitly program P.

Ideal World

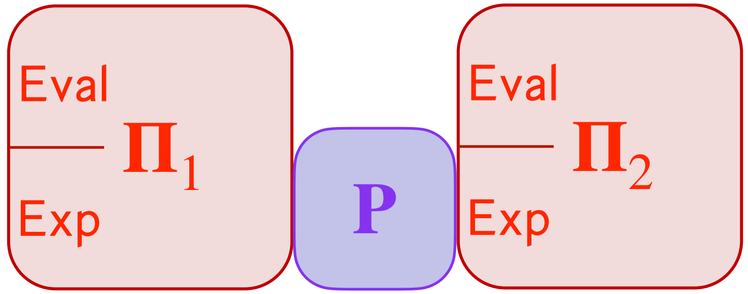




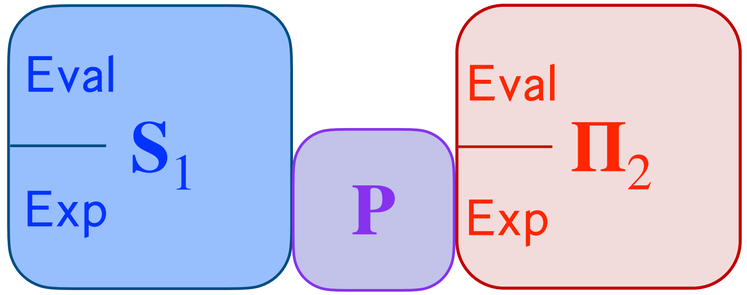
Georgia Tech College of Computing
School of Cybersecurity and Privacy

2. SIM*-AC Solution

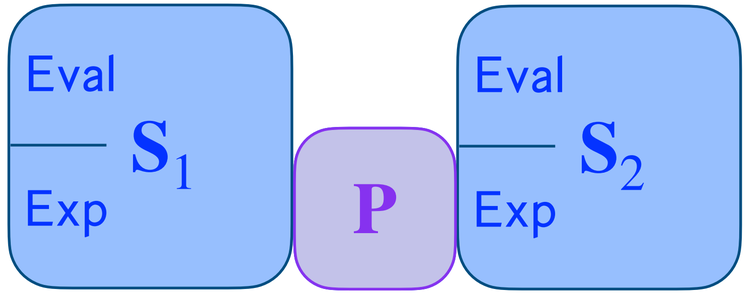
Real World



Hybrid World

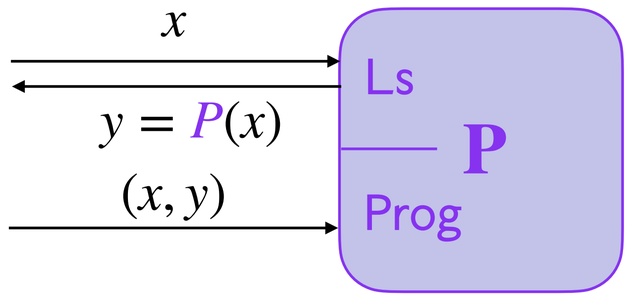


Ideal World

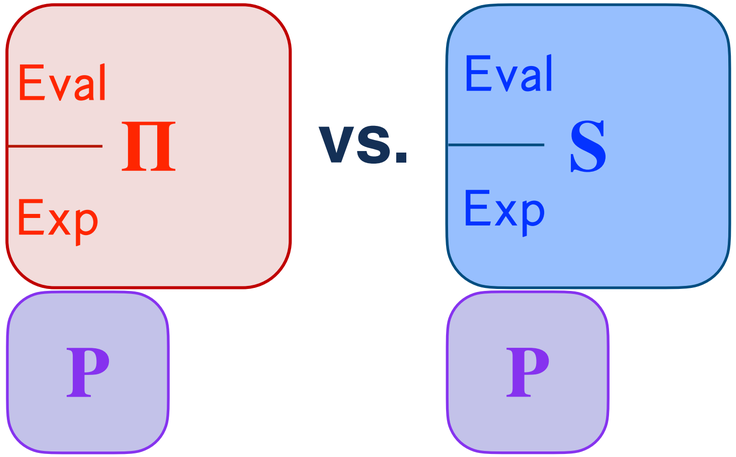


Modify ideal primitive

Lazy sampling - Define P(x) when needed.
Programmable - Give (x,y) to define P(x)=y.



Have S explicitly program P.

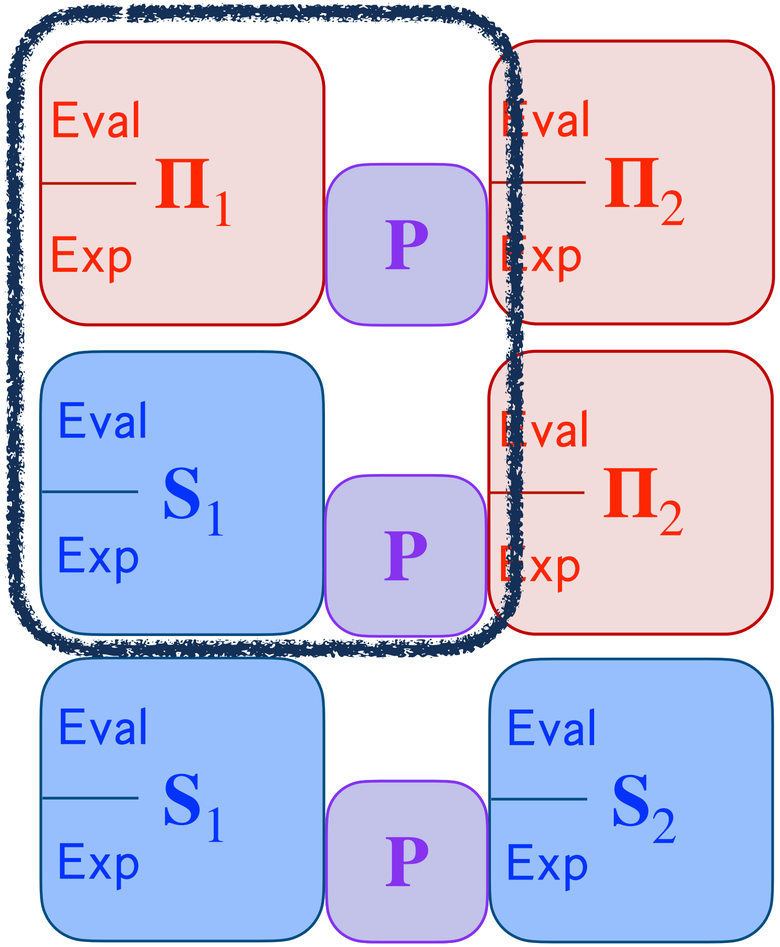


2. SIM*-AC Solution

Real World

Hybrid World

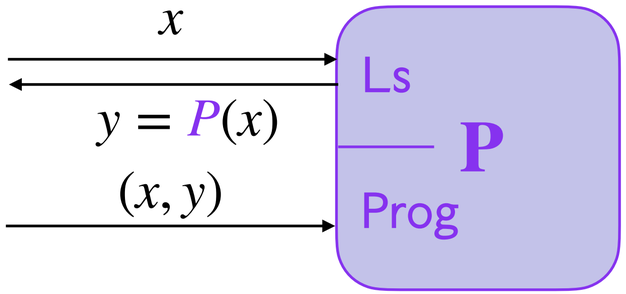
Ideal World



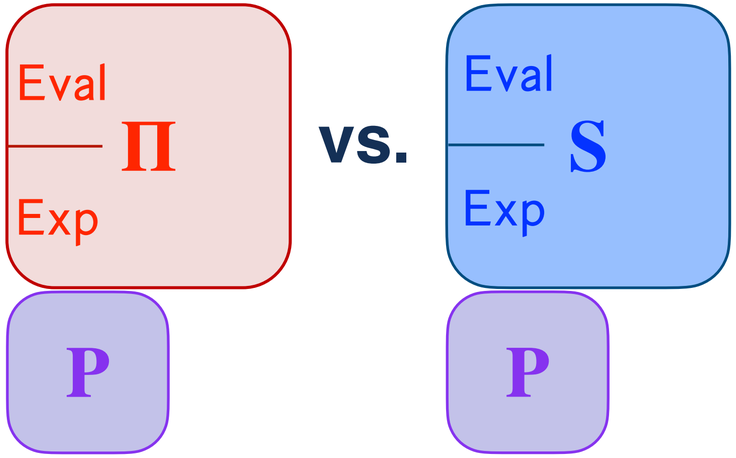
Modify ideal primitive

Lazy sampling - Define P(x) when needed.

Programmable - Give (x,y) to define P(x)=y.



Have S explicitly program P.

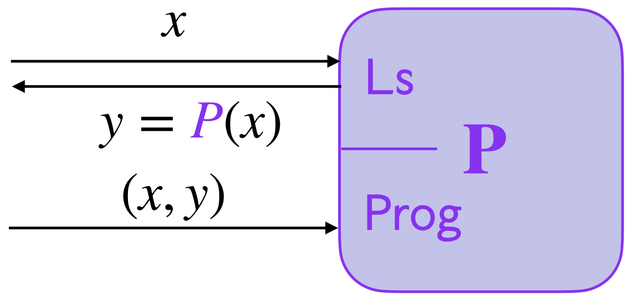


Georgia Tech College of Computing
School of Cybersecurity and Privacy

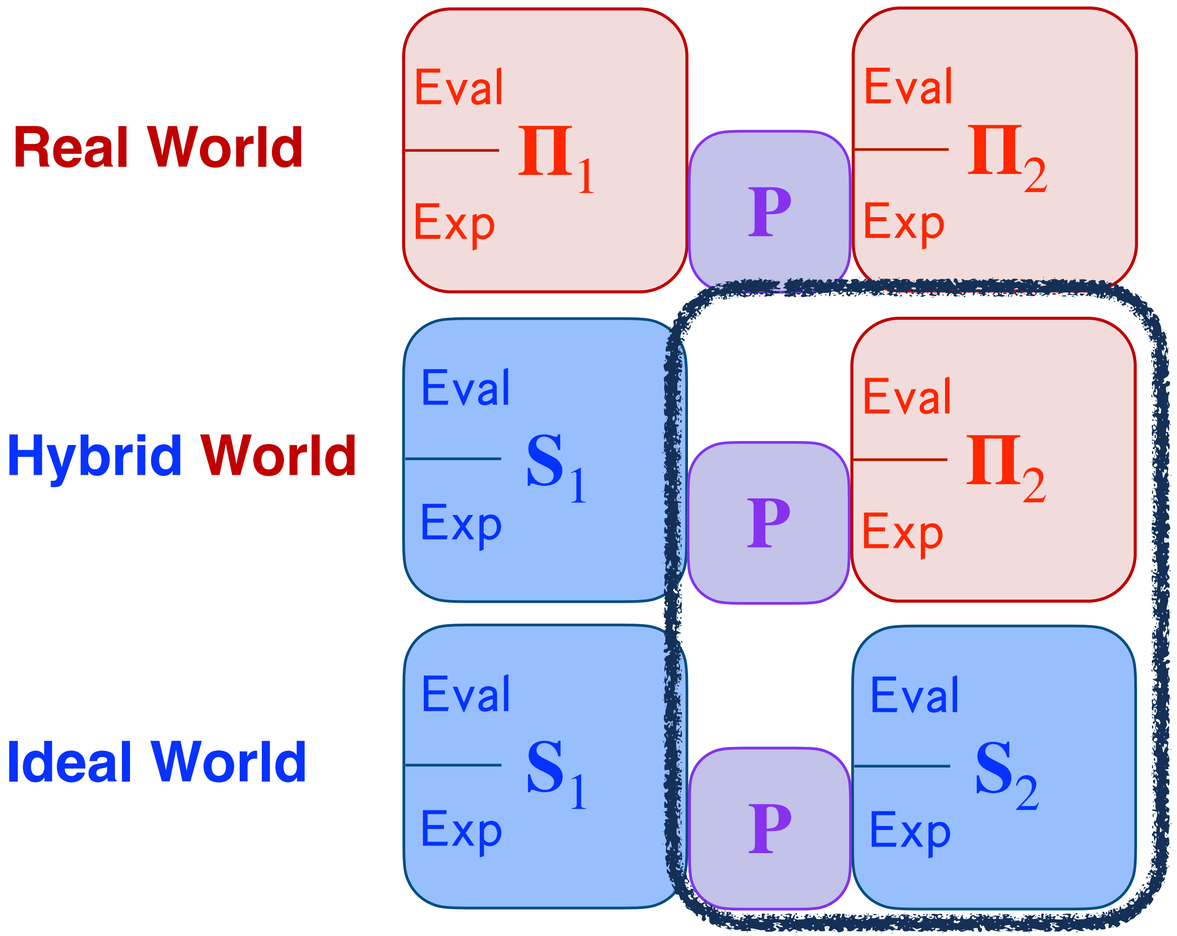
2. SIM*-AC Solution

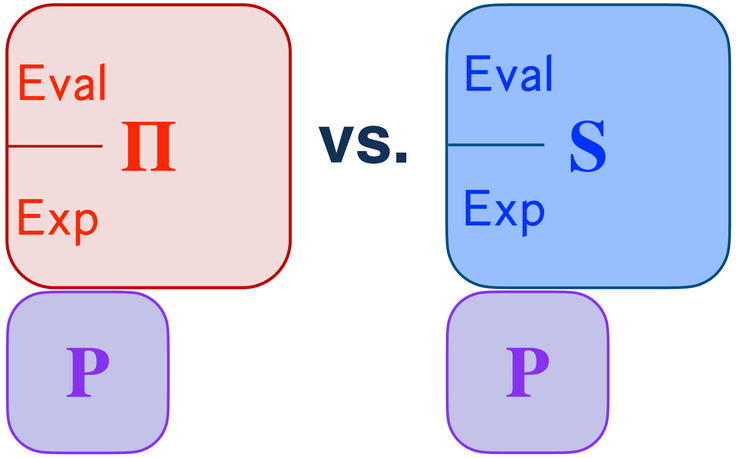
Modify ideal primitive

Lazy sampling - Define P(x) when needed.
Programmable - Give (x,y) to define P(x)=y.



Have S explicitly program P.





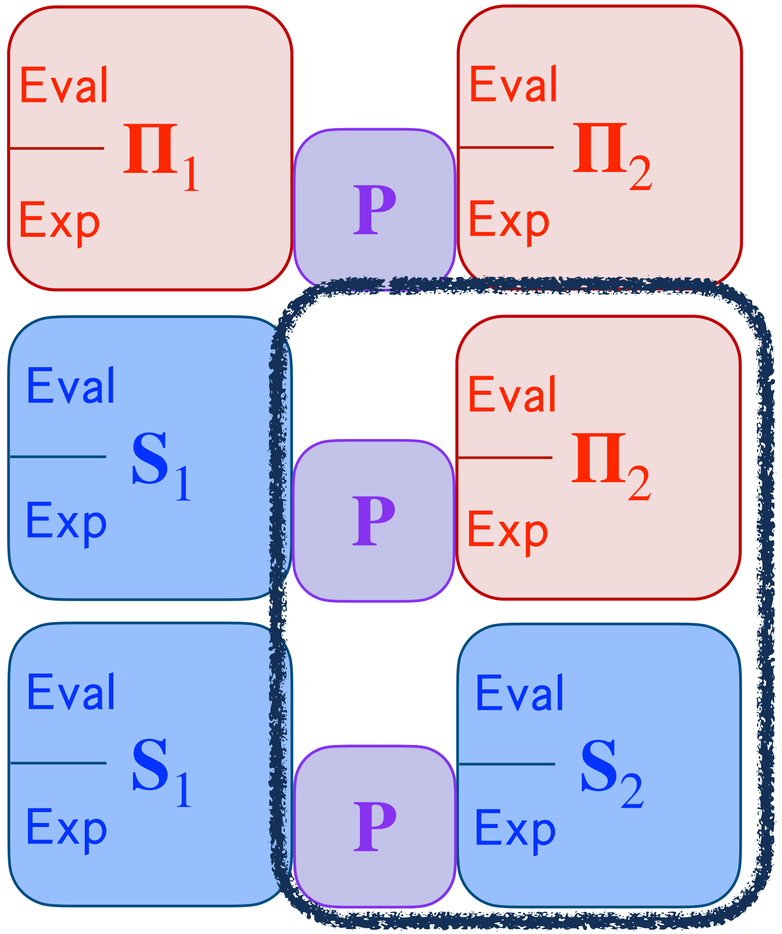
Georgia Tech College of Computing
School of Cybersecurity and Privacy

2. SIM*-AC Solution

Real World

Hybrid World

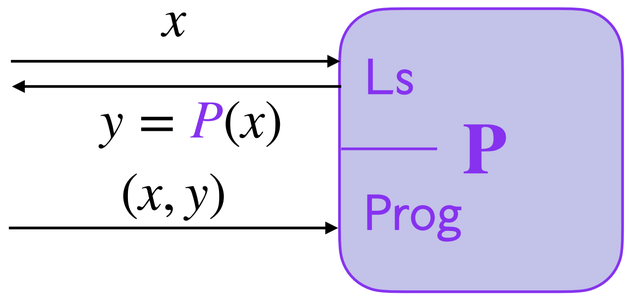
Ideal World



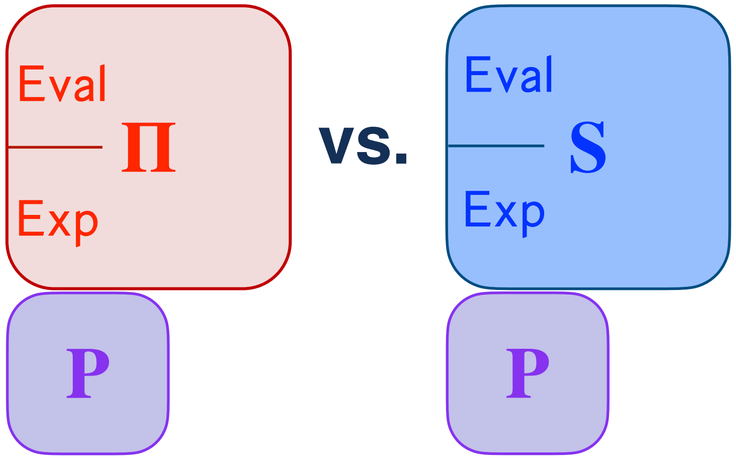
Modify ideal primitive

Lazy sampling - Define P(x) when needed.

Programmable - Give (x,y) to define P(x)=y.



Have S **and Adversary** explicitly program P.

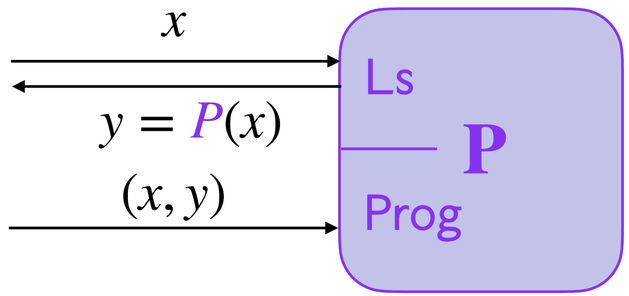


Georgia Tech College of Computing
School of Cybersecurity and Privacy

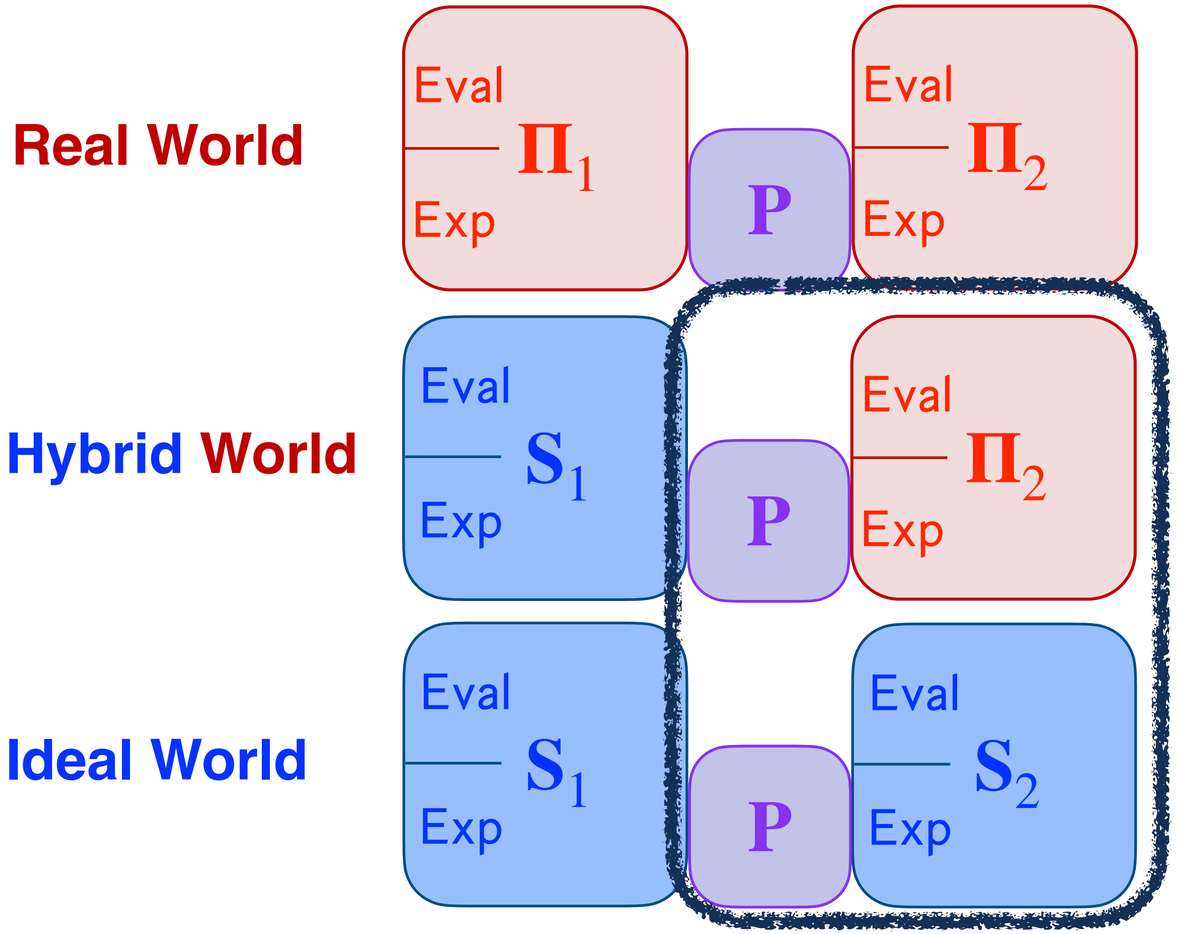
2. SIM*-AC Solution

Modify ideal primitive

Lazy sampling - Define P(x) when needed.
Programmable - Give (x,y) to define P(x)=y.



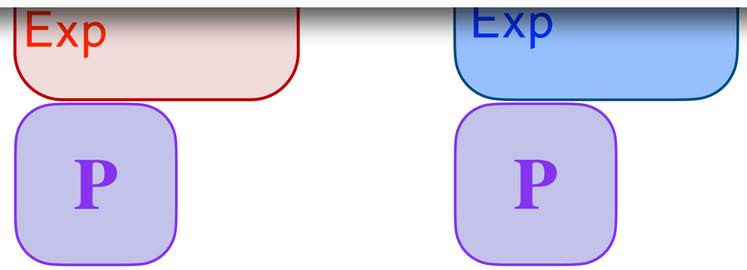
Have S **and Adversary** explicitly program P.



Paper 2018/165

The Wonderful World of Global Random Oracles

Jan Camenisch, Manu Drijvers, Tommaso Gagliardoni, Anja Lehmann, and Gregory Neven



Georgia Tech College of Computing
School of Cybersecurity and Privacy

2. SIM*-AC Solution

Multiple uses of the same scheme:

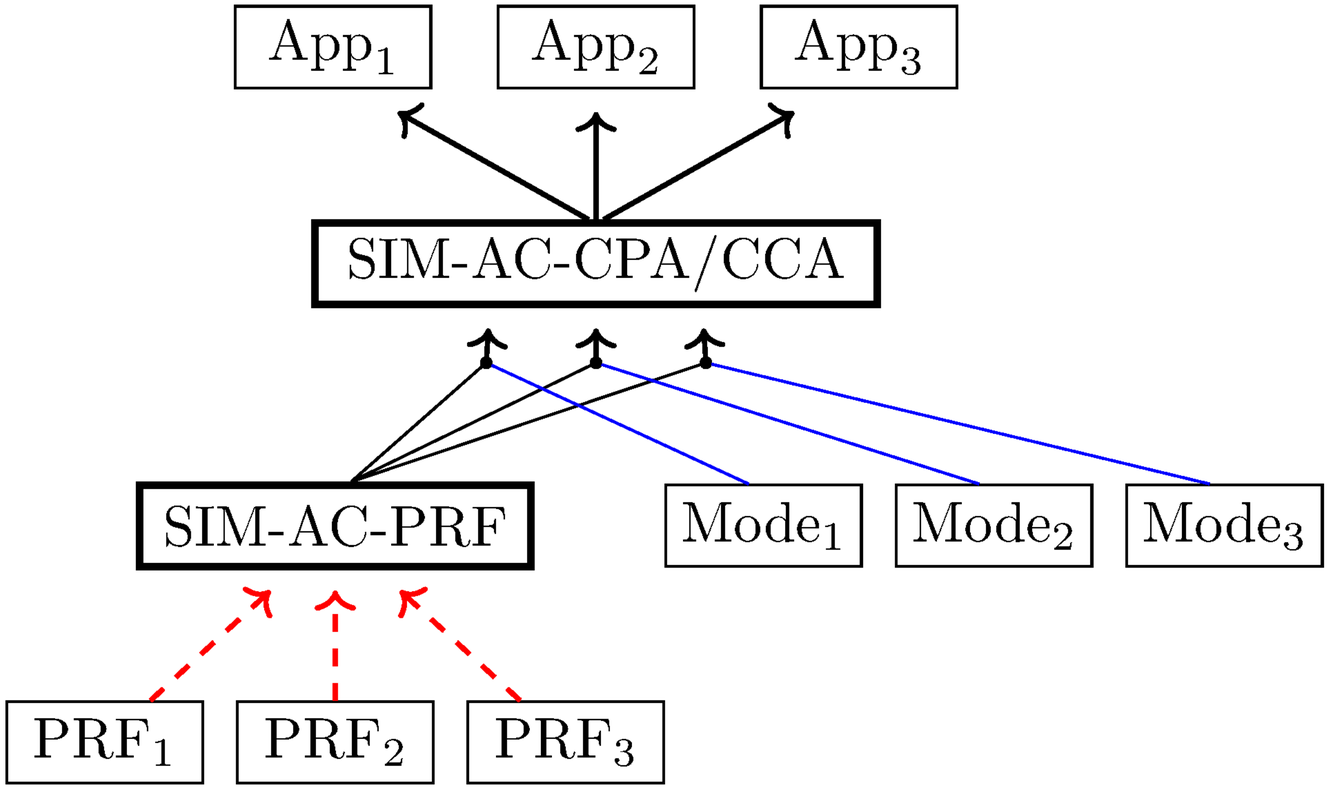
- Multi-user security
- Cascade PRF
- Searchable encryption*

New proofs for both of these.
Super-constant rounds/users needs universal simulator.

Multiple schemes with the same primitive:

- Searchable encryption*
- Revocable Cloud Storage*
- Enc-then-Mac*

3. Recovering Prior Results



High-level proofs:

Searchable encryption
Revocable Cloud Storage
OPAQUE

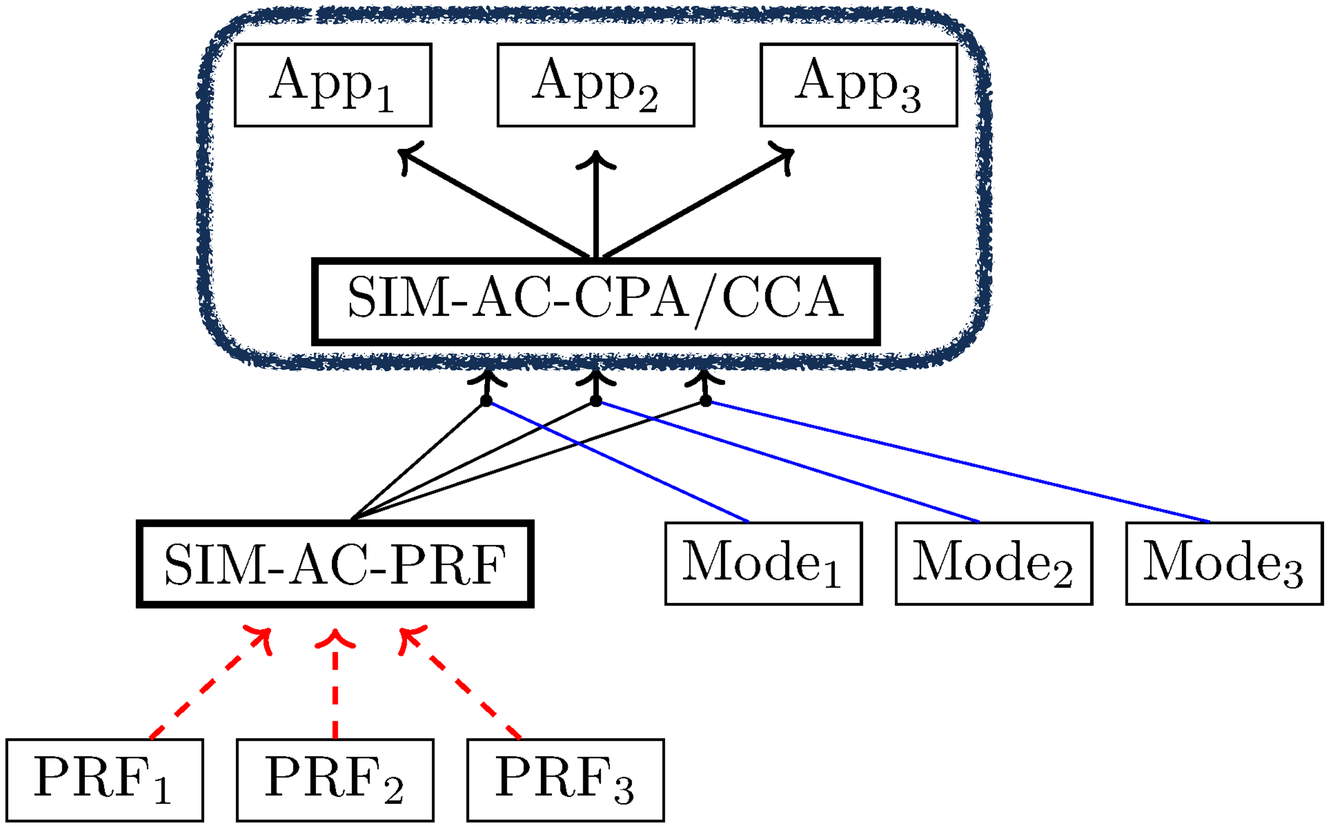
Intermediate-level proofs:

CTR, CBC, …
Enc-then-Mac

Low-level proofs:

Random oracle PRF
Ideal cipher PRF

3. Recovering Prior Results



High-level proofs:

Free!
SIM*-AC → SIM-AC

Intermediate-level proofs:

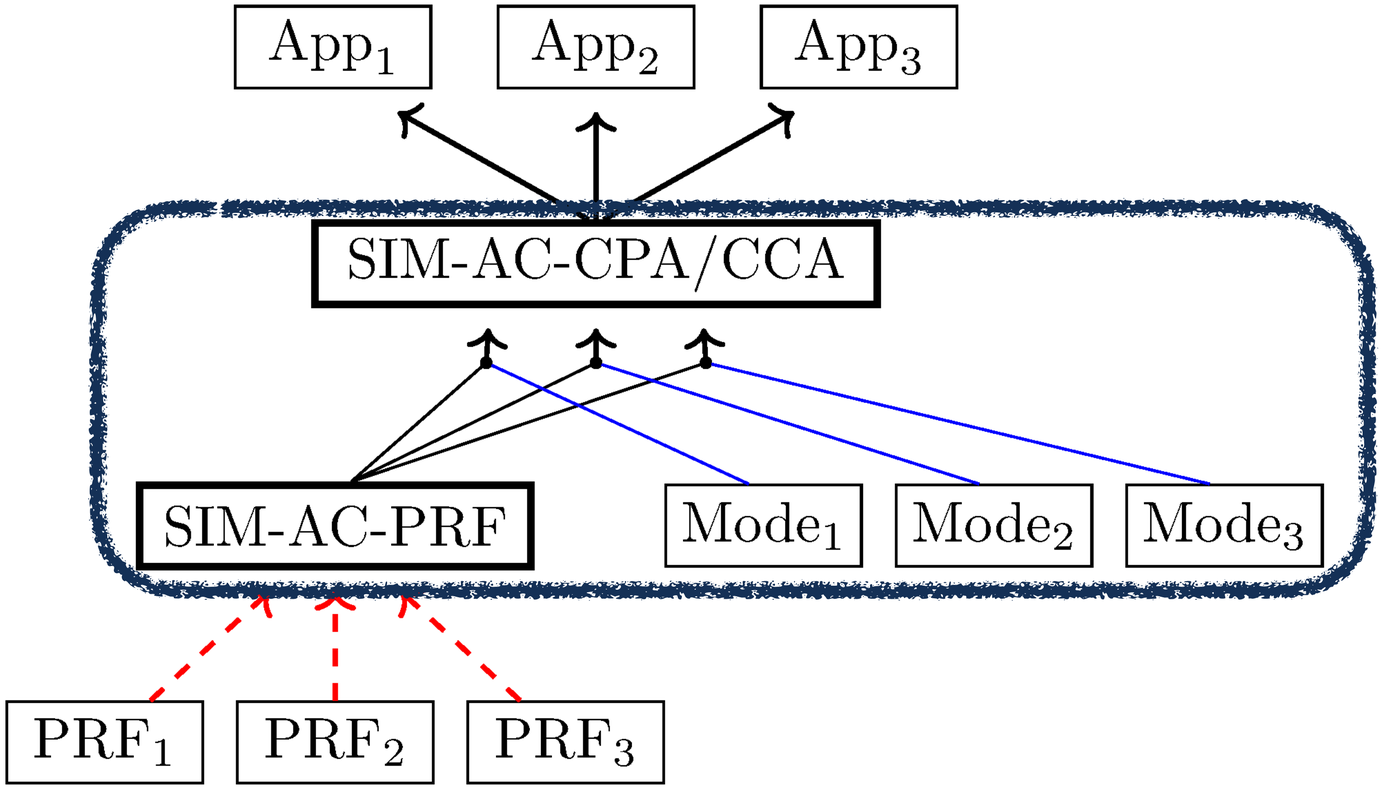
CTR, CBC, …
Enc-then-Mac

Low-level proofs:

Random oracle PRF
Ideal cipher PRF

Georgia Tech College of Computing
School of Cybersecurity and Privacy

3. Recovering Prior Results



High-level proofs:

Free!

SIM*-AC → SIM-AC

Intermediate-level proofs:

“Free”

Sufficiently blackbox

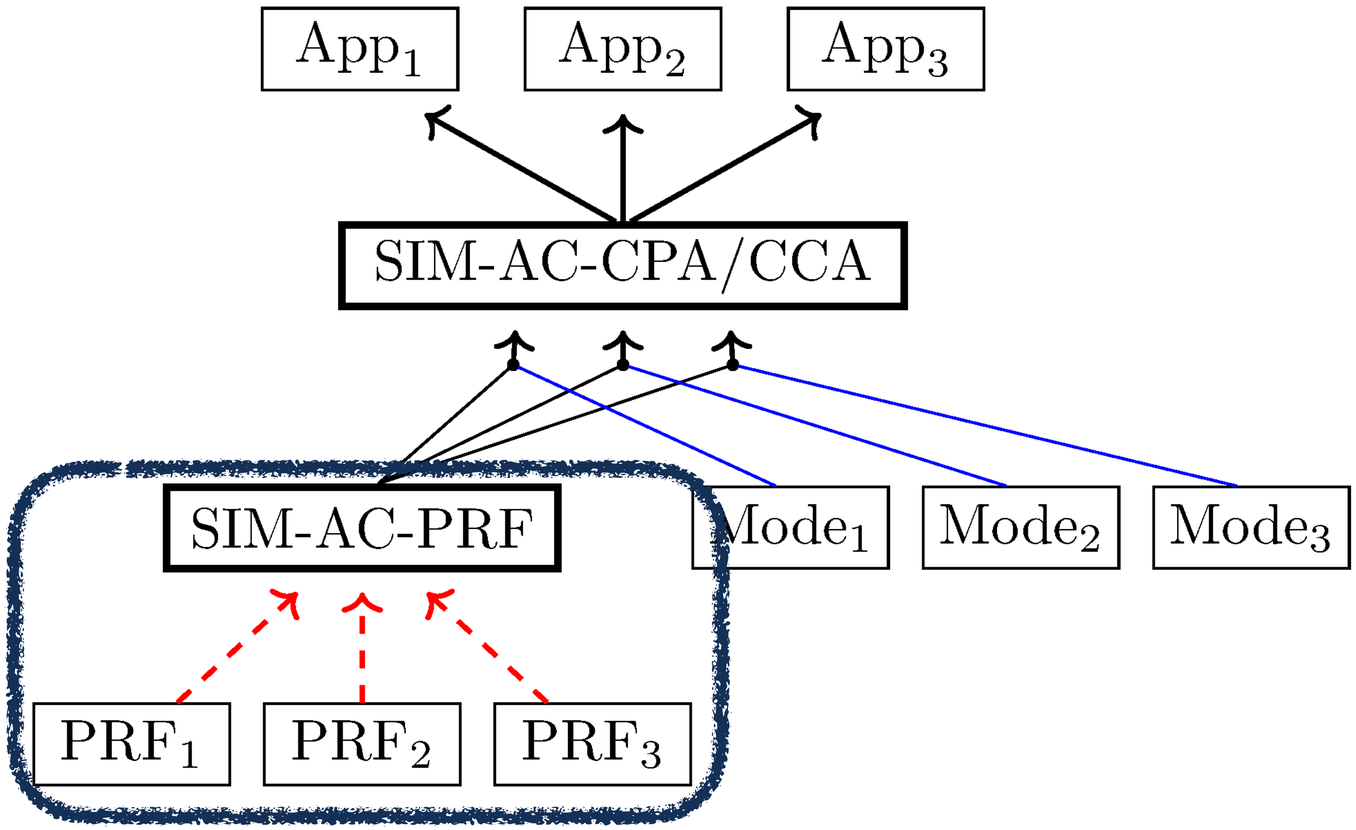
Low-level proofs:

Random oracle PRF

Ideal cipher PRF

Georgia Tech College of Computing
School of Cybersecurity and Privacy

3. Recovering Prior Results



High-level proofs:

Free!

SIM*-AC → SIM-AC

Intermediate-level proofs:

“Free”

Sufficiently blackbox

Low-level proofs:

Not free, rewrite proofs

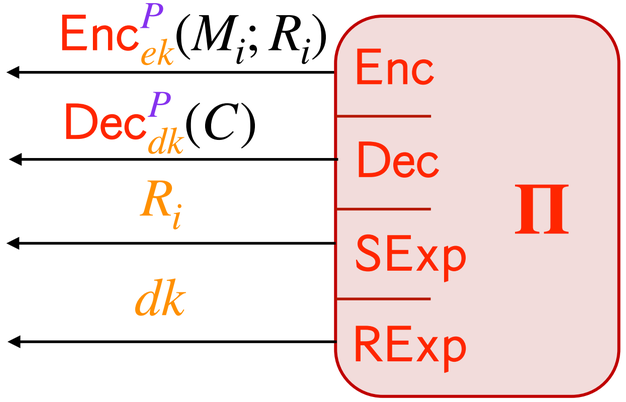
Basically same bounds

prim queries → # prim + prog

Georgia Tech College of Computing
School of Cybersecurity and Privacy

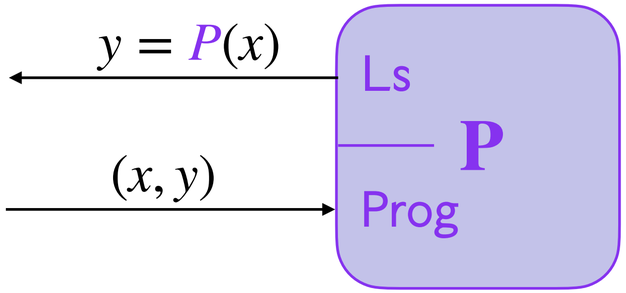
4. SIM*-AC For Asymmetric Encryption

Real World



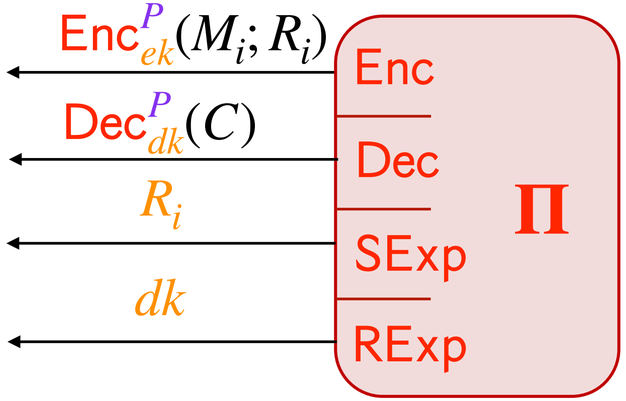
Sender Exposure: Encryption randomness
Receiver Exposure: Decryption key

SIM*-AC-CCA



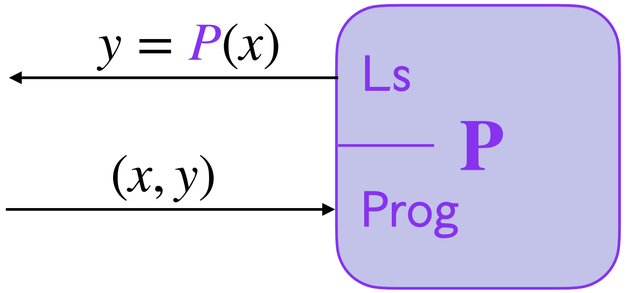
4. SIM*-AC For Asymmetric Encryption

Real World

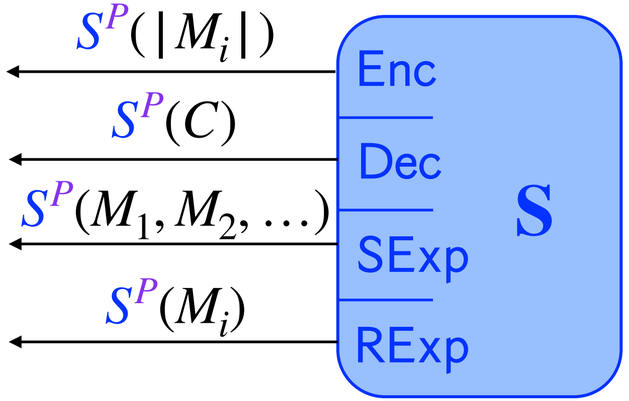


Sender Exposure: Encryption randomness
Receiver Exposure: Decryption key

SIM*-AC-CCA



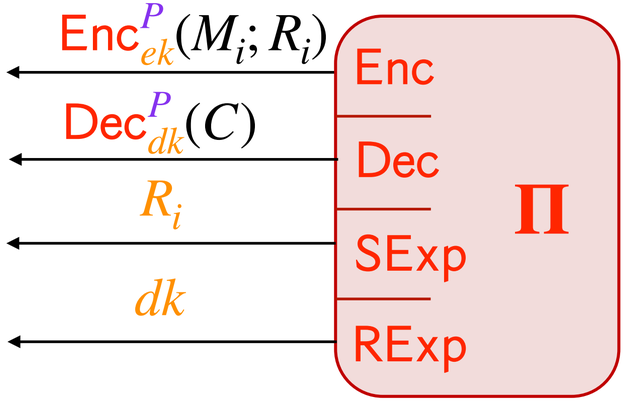
Ideal World



Georgia Tech College of Computing
School of Cybersecurity and Privacy

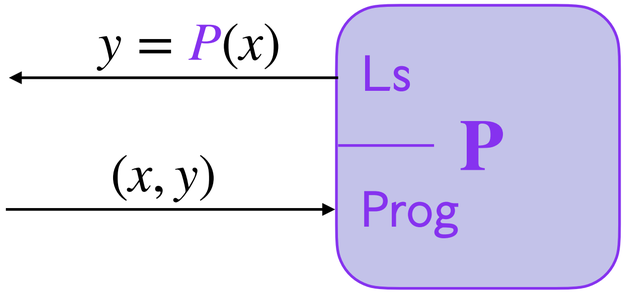
4. SIM*-AC For Asymmetric Encryption

Real World



Sender Exposure: Encryption randomness
Receiver Exposure: Decryption key

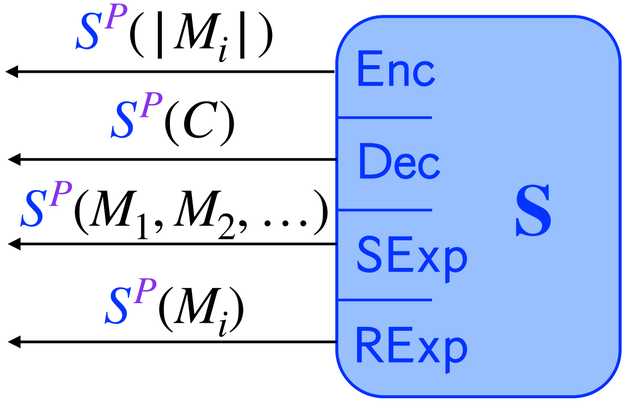
SIM*-AC-CCA



KEM definitions as well!

- Enc → Encaps
- Dec → Decaps
- Random key when ideal

Ideal World



Georgia Tech College of Computing
School of Cybersecurity and Privacy

4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

Paper 2016/845

Selective Opening Security from Simulatable Data Encapsulation

Felix Heuer and Bertram Poettering

IND-CCA **KEM** + (Perm + INT-CTXT + Simulatable) **DEM**
→
SIM-SO-CCA **PKE**

Georgia Tech College of Computing
School of Cybersecurity and Privacy

4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

Paper 2016/845

Selective Opening Security from Simulatable Data Encapsulation

Felix Heuer and Bertram Poettering

IND-CCA **KEM** + (Perm + INT-CTXT + Simulatable) **DEM**
→
SIM-SO-CCA **PKE**

Hashed KEM: SIM*-AC-CPA/CCA from forms of one-wayness + RO.

4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

Paper 2016/845

Selective Opening Security from Simulatable Data Encapsulation

Felix Heuer and Bertram Poettering

IND-CCA **KEM** + (Perm + INT-CTXT + Simulatable) **DEM**
→
SIM-SO-CCA **PKE**

Hashed KEM: SIM*-AC-CPA/CCA from forms of one-wayness + RO.

DHIES: An encryption scheme based on the Diffie-Hellman Problem

Michel Abdalla* Mihir Bellare† Phillip Rogaway‡

Paper 2017/604

A Modular Analysis of the Fujisaki-Okamoto Transformation

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz

4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

Paper 2016/845

Selective Opening Security from Simulatable Data Encapsulation

Felix Heuer and Bertram Poettering

IND-CCA **KEM** + (Perm + INT-CTXT + Simulatable) **DEM**
→
SIM-SO-CCA **PKE**

DHIES: An encryption scheme based on the Diffie-Hellman Problem

Michel Abdalla* Mihir Bellare† Phillip Rogaway‡

Hashed KEM: SIM*-AC-CPA/CCA from forms of one-wayness + RO.

Relationships:

Paper 2017/604

A Modular Analysis of the Fujisaki-Okamoto Transformation

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz

4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

Paper 2016/845

Selective Opening Security from Simulatable Data Encapsulation

Felix Heuer and Bertram Poettering

IND-CCA **KEM** + (Perm + INT-CTXT + Simulatable) **DEM**
→
SIM-SO-CCA **PKE**

DHIES: An encryption scheme based on the Diffie-Hellman Problem

Michel Abdalla* Mihir Bellare† Phillip Rogaway‡

Hashed KEM: SIM*-AC-CPA/CCA from forms of one-wayness + RO.

Relationships:

Paper 2017/604

A Modular Analysis of the Fujisaki-Okamoto Transformation

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz

SIM*-AC-CCA

Georgia Tech College of Computing
School of Cybersecurity and Privacy

4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

Paper 2016/845

Selective Opening Security from Simulatable Data Encapsulation

Felix Heuer and Bertram Poettering

IND-CCA **KEM** + (Perm + INT-CTXT + Simulatable) **DEM**
→
SIM-SO-CCA **PKE**

DHIES: An encryption scheme based on the Diffie-Hellman Problem

Michel Abdalla* Mihir Bellare† Phillip Rogaway‡

Hashed KEM: SIM*-AC-CPA/CCA from forms of one-wayness + RO.

Paper 2017/604

A Modular Analysis of the Fujisaki-Okamoto Transformation

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz

Relationships:

4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

Paper 2016/845

Selective Opening Security from Simulatable Data Encapsulation

Felix Heuer and Bertram Poettering

IND-CCA **KEM** + (Perm + INT-CTXT + Simulatable) **DEM**
→
SIM-SO-CCA **PKE**

DHIES: An encryption scheme based on the Diffie-Hellman Problem

Michel Abdalla* Mihir Bellare† Phillip Rogaway‡

Hashed KEM: SIM*-AC-CPA/CCA from forms of one-wayness + RO.

Relationships:

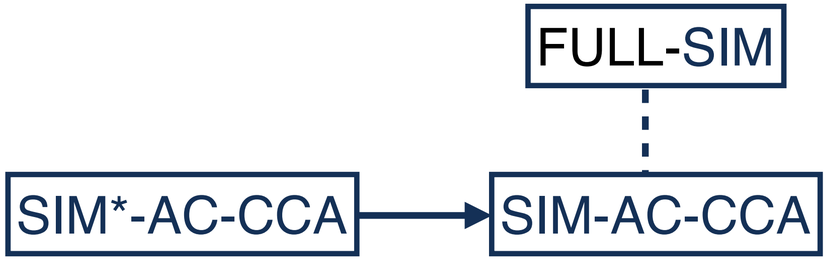
UC-Secure Non-Interactive Public-Key Encryption

Jan Camenisch*, Anja Lehmann*, Gregory Neven*, Kai Samelin*§

Paper 2017/604

A Modular Analysis of the Fujisaki-Okamoto Transformation

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz



4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

Paper 2016/845

Selective Opening Security from Simulatable Data Encapsulation

Felix Heuer and Bertram Poettering

IND-CCA **KEM** + (Perm + INT-CTXT + Simulatable) **DEM**
→
SIM-SO-CCA **PKE**

DHIES: An encryption scheme based on the Diffie-Hellman Problem

Michel Abdalla* Mihir Bellare† Phillip Rogaway‡

Hashed KEM: SIM*-AC-CPA/CCA from forms of one-wayness + RO.

Relationships:

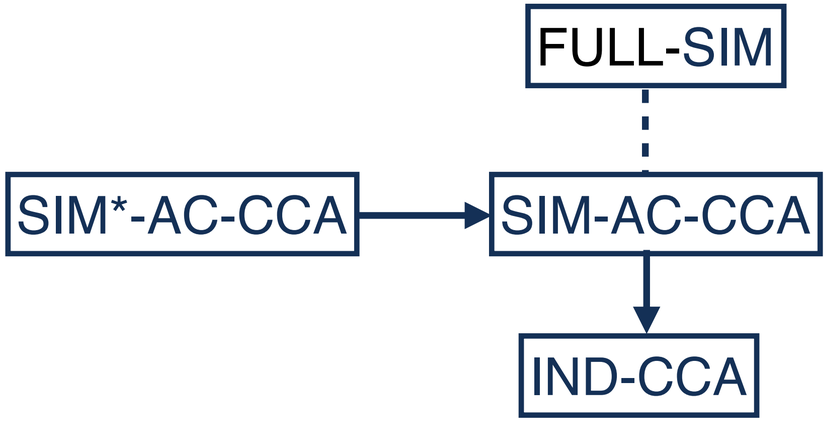
UC-Secure Non-Interactive Public-Key Encryption

Jan Camenisch*, Anja Lehmann*, Gregory Neven*, Kai Samelin*§

Paper 2017/604

A Modular Analysis of the Fujisaki-Okamoto Transformation

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz



4. SIM*-AC For Asymmetric Encryption

Positive results

KEM/DEM: SIM*-AC-X **KEM** + SIM*-AC-X **DEM** → SIM*-AC-X **PKE** for X = CPA, CCA

Paper 2016/845

Selective Opening Security from Simulatable Data Encapsulation

Felix Heuer and Bertram Poettering

IND-CCA **KEM** + (Perm + INT-CTXT + Simulatable) **DEM**
→
SIM-SO-CCA **PKE**

DHIES: An encryption scheme based on the Diffie-Hellman Problem

Michel Abdalla* Mihir Bellare† Phillip Rogaway‡

Hashed KEM: SIM*-AC-CPA/CCA from forms of one-wayness + RO.

Relationships:

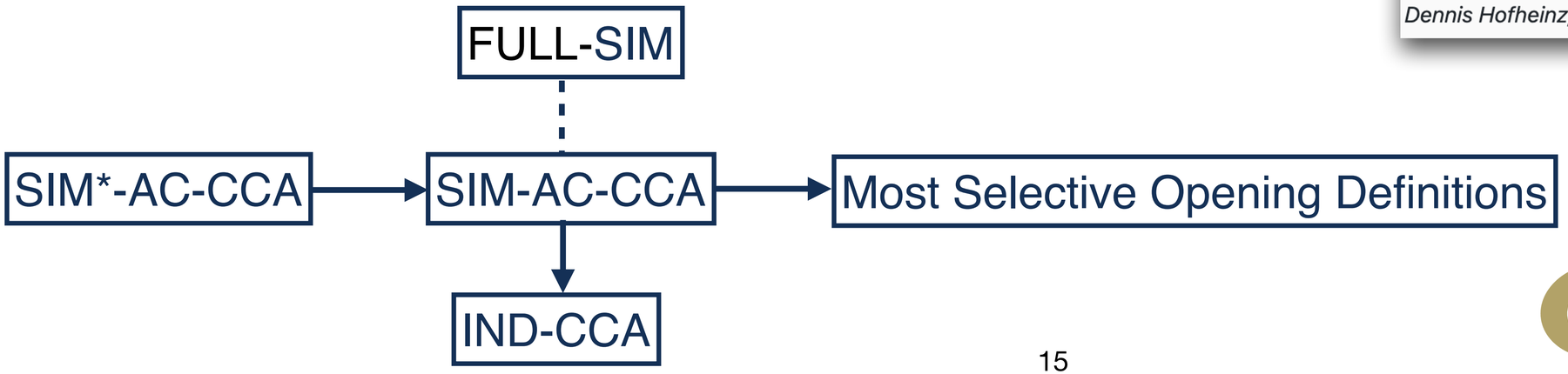
UC-Secure Non-Interactive Public-Key Encryption

Jan Camenisch*, Anja Lehmann*, Gregory Neven*, Kai Samelin*§

Paper 2017/604

A Modular Analysis of the Fujisaki-Okamoto Transformation

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz



Let Attackers Program Ideal Models

Our Contributions

1. SIM-AC and it **shortcomings**.

2. SIM*-AC and it **solution** to shortcomings.
   - Multiple schemes with same primitive
   - Multiple uses of same scheme
   - Single-user security → Multi-user security

3. **Recovering prior results:** SIM-AC results hold with SIM*-AC.

4. SIM*-AC for **asymmetric encryption**.
   - Comparisons to prior definitions
   - KEM/DEM hybrid encryption
   - Fujisaki-Okamoto style transforms