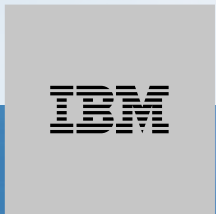


SoK: Game-based Security Models for Group Key Exchange

CT-RSA 2021

2021-06-01

Bertram Poettering



Paul Rösler



Jörg Schwenk



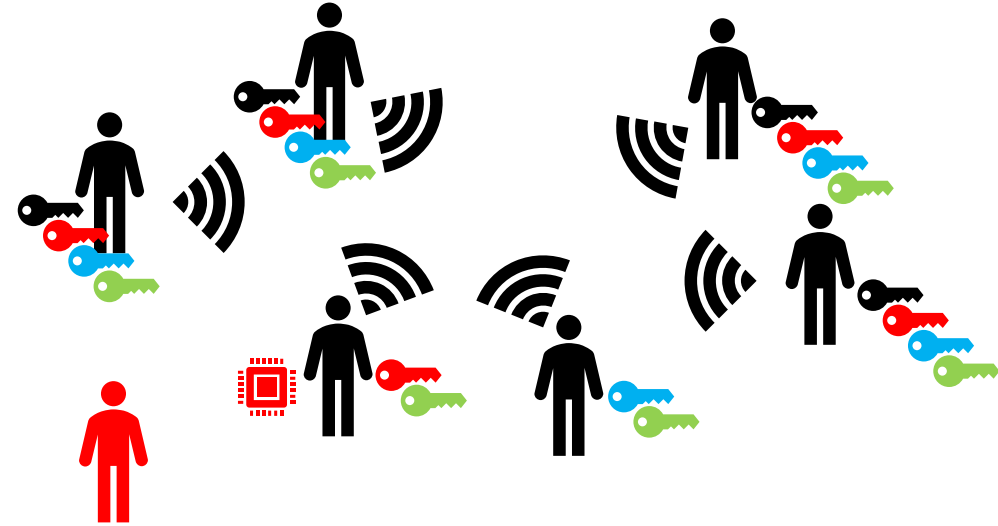
Douglas Stebila



Group Key Exchange: Idea and History

Idea: Group Key Exchange (GKE)

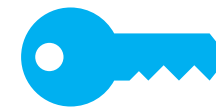
- Example: Group messaging
 - 1) Exchange key 2) Encrypt message once
 - Alternative: Encrypt to each member
- Multiple parties exchange key
 - Membership may change
 - Keys are revealed, secrets are exposed, ...
- Goal: exchanged keys look random



Literature: DBLP says >150 conference papers



- ~~1st wave: protocols with heuristic security arguments ('80s-'90s)~~
- 2nd wave: protocols with security proofs ('00s-'10s)
- 3rd wave: protocols built for secure messaging ('17-now)



Real



Random

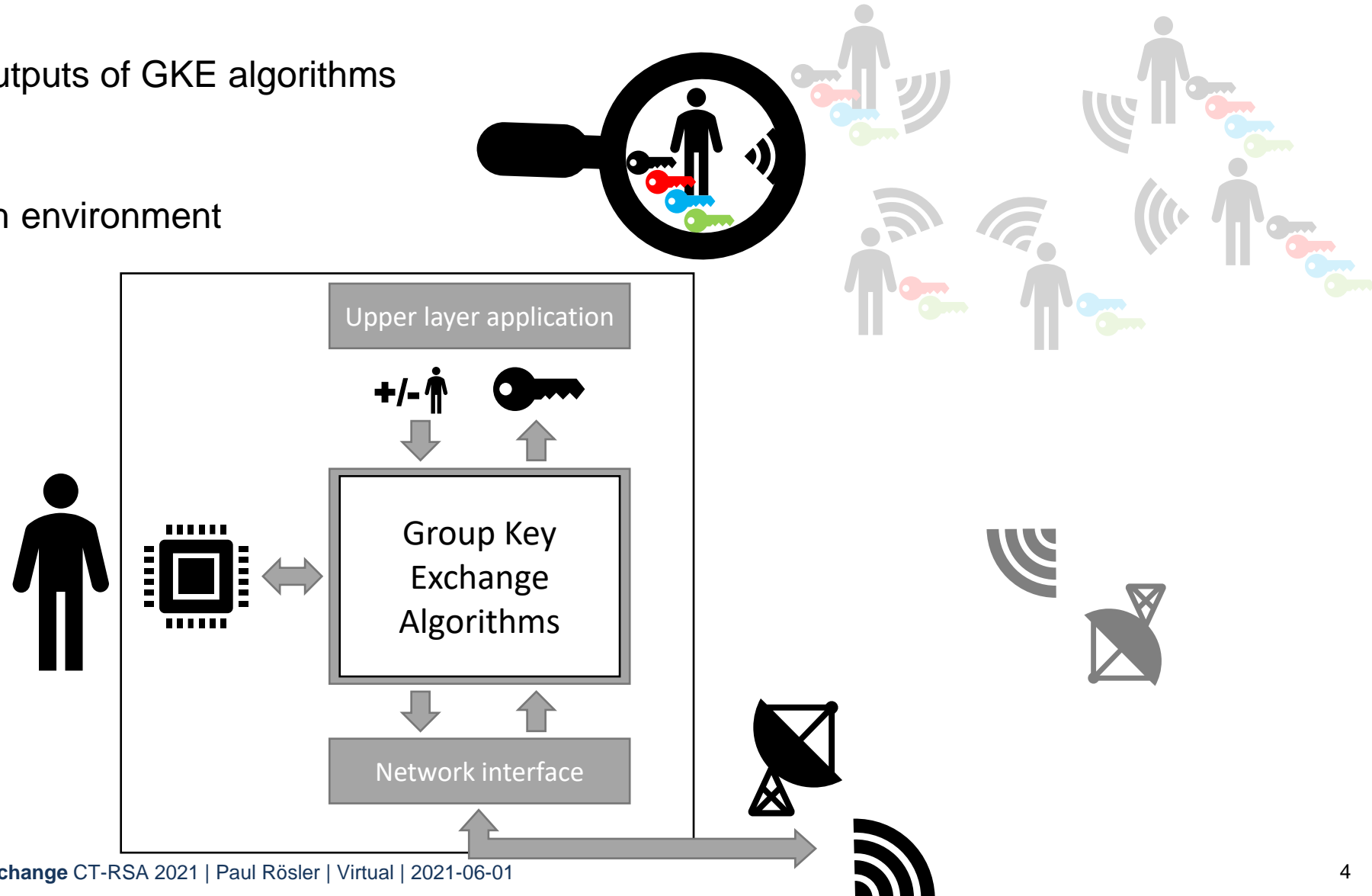
} >30 different security definitions

⇒ Systematize and unify GKE security definitions

Prerequisites: Define “GKE” and “Security”

Syntax: Abstract inputs and outputs of GKE algorithms

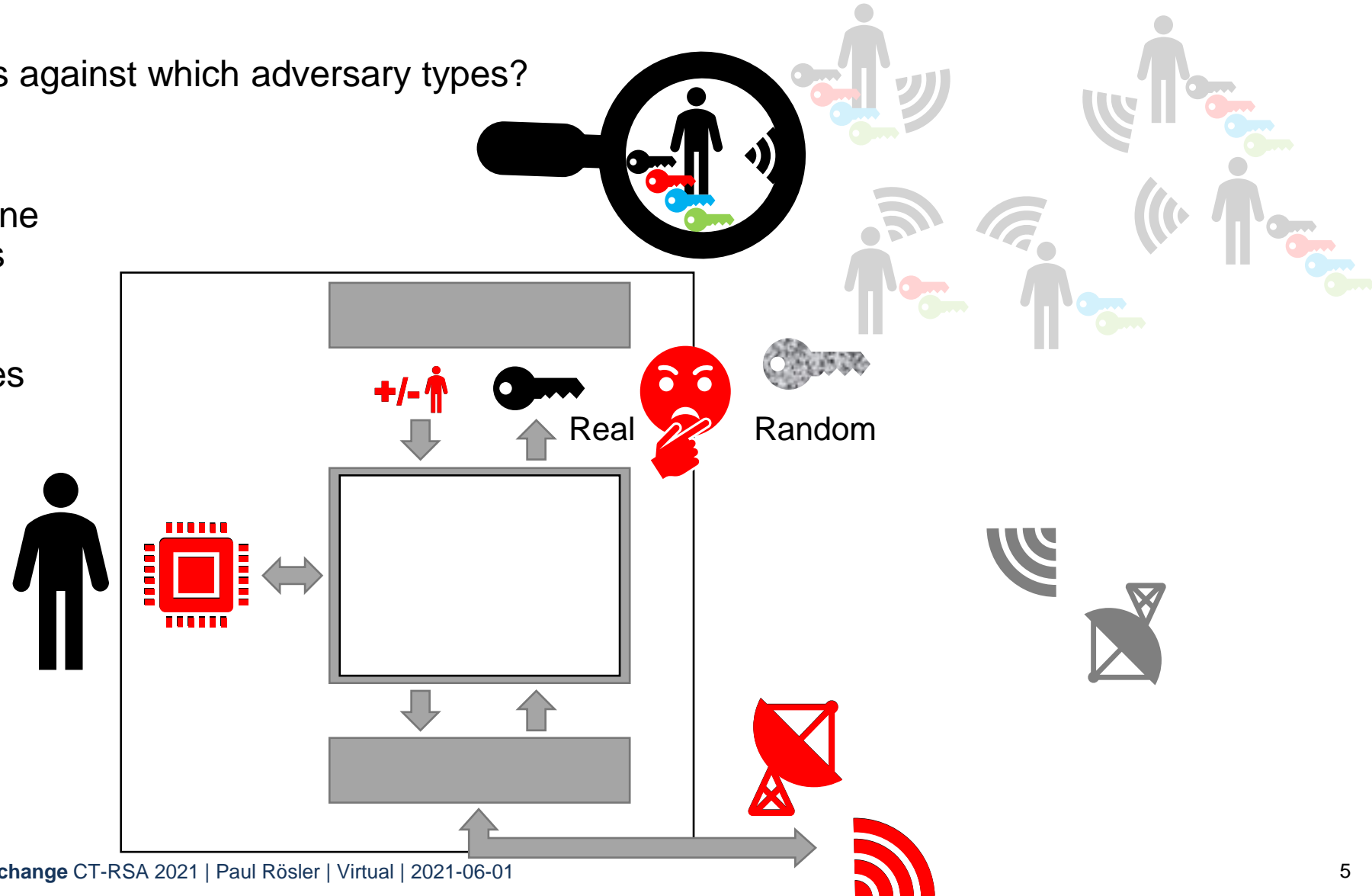
- Useful:
Offer desired interaction with environment
- Generic:
Capture many different constructions
- Unrestricted:
No unnecessary efficiency limitations



Prerequisites: Define “GKE” and “Security”

Security: Which security goals against which adversary types?

- Intuitive security goal:
Keys look random to everyone
except designated members
- Realistic adversary capabilities



Overview: Shortcomings and Implications

Paper selection: Explore GKE models

- ~~1st wave: protocols with heuristic security arguments ('80s-'90s)~~
- 2nd wave: protocols with security proofs ('00s-'10s)
- 3rd wave: protocols built for secure messaging ('17-now)
- Reduce to **"Tier-one"** OR **New model** = 9 + 3

Systematize these GKE models

Results: No generic standard model available

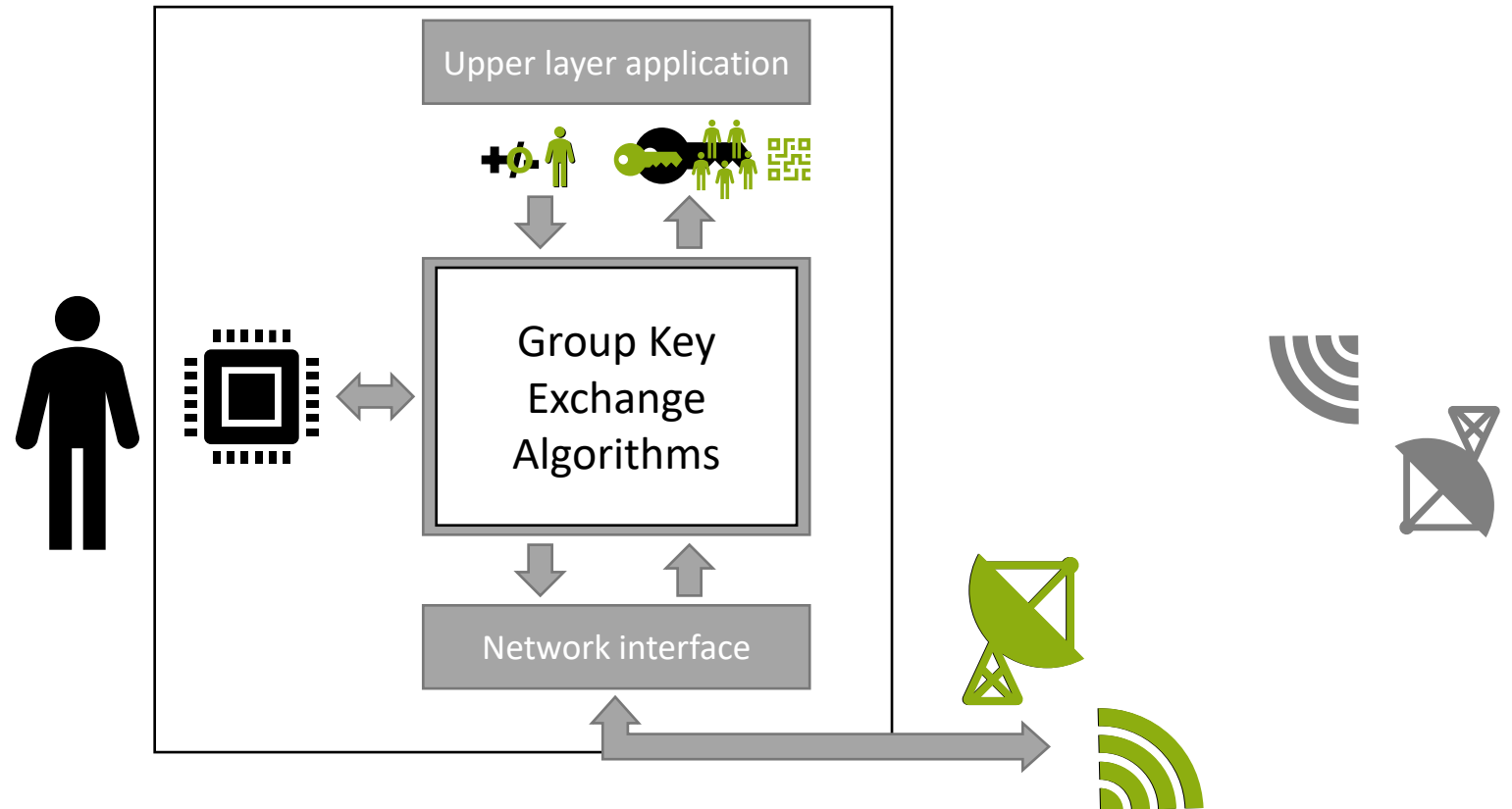
- Under-specific: some models too informal
- Overfitted: designed for single GKE constructions
- Ignoring external requirements:
 - Impractical key reporting
 - PKI required for authentication
 - Restricted to certain group operations
 - No generic composition with other protocols
 - No multi-participations per user
 - ...

		[BCP01]	[BCP02]	[KY03]	[KS05]	[CCG+18]	[ACD19]	[ACC+19]	[BCP01]	[YKLH18]	Our model
Syntax											
Quantities											
Instances											
Parties per											
Multi-part											
Setup assum											
Authenticat											
PKI											
Online adv											
Operations											
Level of sp											
Algo: Setup											
Algo: Add											
Algo: Rem											
Algo: Refr											
Abstract i											
Return value											
Group key											
Ref. for ses											
Ref. for gr											
Designated											
Ongoing o											
Status of i											
	Security										
	Security goal										
	Key indis										
	↳ Multipl										
	Explicit a										
	Partnering/										
	Defined?										
	Generic ● or P										
	Normative/P										
	↳ Tight ● (vs										
	Publicly deriva										
	Components i										
	Transcript										
	Matching tr										
	Sequence of										
	Identifiers										
	Group ident										
	Key identifi										
	Externally i										
	Group key										
	Whether partners computed a key										
	Whether group computed a key										
	Whether partners computed same key										
	Reveal of										
	↳ Always										
	Correctness										
	Defined										
	Requirements										
	Honest transcript delivery										
	Two instances are partnered										
	All group instances are partnered										
	A key is computed										
	All participating instances share \geq										
	Keys are partnered										
	Guarantees										
	Same key										
	Non-zero key										
	Keys are partnered										
	Members of the group										

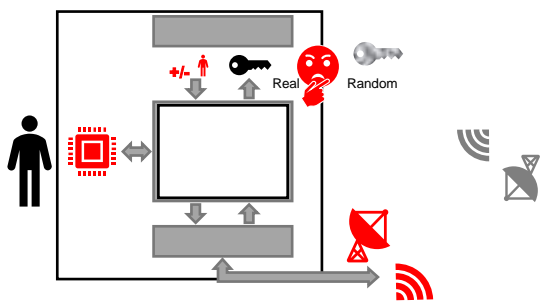
Our Enhancements

... **yet another model? No:** Learning from the past and rethinking GKE

- Precise and compact model
 - Independent of constructions
 - Pseudo-code game definition
- Indifferent to membership operations
 - Generic operations
 - Protocol reports context for keys
 - ...
- Can handle real-world settings
 - Asynchronous communication
 - Multi-participation
 - Many means of authentication
 - Easily extendable



Agenda



What is GKE abstractly?

Develop Understanding of "GKE"

Derive Systematization Framework

Syntax	Security	Partnering/	Correctness
Quantities	Security go	Defined?	Defined
Instances	Security go	Generic	Requirements
Multi-part	Key indi	Normative/P	Honest transcript delivery
Setup assum	Multi	Tight	Two instances are partnered
Authentic	Explicit	Publicly deriv	All group instances are partnered
PKI	Adversarial	Components	A key is computed
Online ad	All algor	Transcript	All participating instances share
Operations	Level of s	Corrupt	Keys are partnered
Level of s	Instances	Identifiers	Guarantees
Algo: Set	Concurr	Group ident	Same key
Algo: Add	Active co	Key identifi	Non-zero key
Algo: Rem	Adversarial	Externally	Keys are partnered
Algo: Ref	Matching	Group key	Whether partners computed a key
Abstract	Sequence of	Whether partners computed a key	Whether partners computed same key
Return value	Identifiers	Members of the group	
Group key	Group ident		
Ref. for as	Key identifi		
Ref. for gr	Externally		
Designator	Group key		
Ongoing	Whether partners computed a key		
Status of	Whether partners computed same key		
	Members of the group		

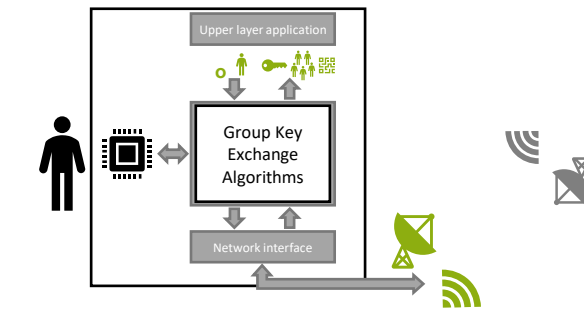
Qualities of GKE models & desirable realizations

Syntax	Security	Partnering/	Correctness
Quantities	Security go	Defined?	Defined
Instances	Security go	Generic	Requirements
Multi-part	Key indi	Normative/P	Honest transcript delivery
Setup assum	Multi	Tight	Two instances are partnered
Authentic	Explicit	Publicly deriv	All group instances are partnered
PKI	Adversarial	Components	A key is computed
Online ad	All algor	Transcript	All participating instances share
Operations	Level of s	Corrupt	Keys are partnered
Level of s	Instances	Identifiers	Guarantees
Algo: Set	Concurr	Group ident	Same key
Algo: Add	Active co	Key identifi	Non-zero key
Algo: Rem	Adversarial	Externally	Keys are partnered
Algo: Ref	Matching	Group key	Whether partners computed a key
Abstract	Sequence of	Whether partners computed a key	Whether partners computed same key
Return value	Identifiers	Members of the group	
Group key	Group ident		
Ref. for as	Key identifi		
Ref. for gr	Externally		
Designator	Group key		
Ongoing	Whether partners computed a key		
Status of	Whether partners computed same key		
	Members of the group		

Use framework to systematize models

Compare Published GKE Models

Propose Generic and Compact Model



Develop model from abstract idea of GKE

@roeslpa ia.cr/2021/305