SoK: Game-based Security Models for Group Key Exchange

CT-RSA 2021

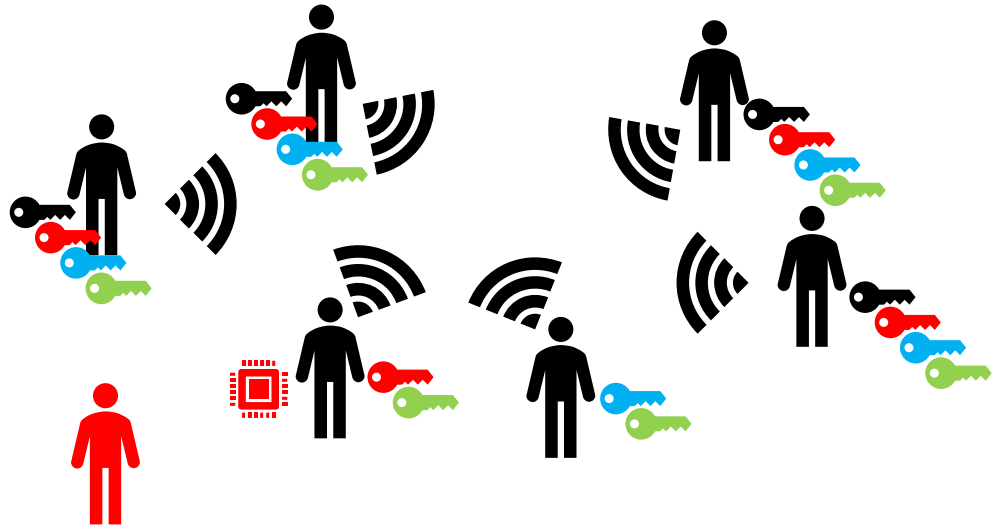
2021-06-01

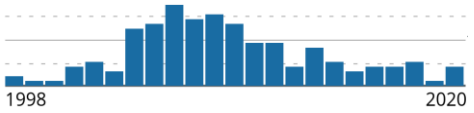
Bertram Poettering **Paul Rösler** Jörg Schwenk Douglas Stebila

Group Key Exchange: Idea and History

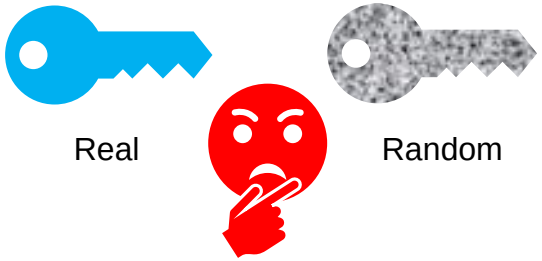
Idea: Group Key Exchange (GKE)

- 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)

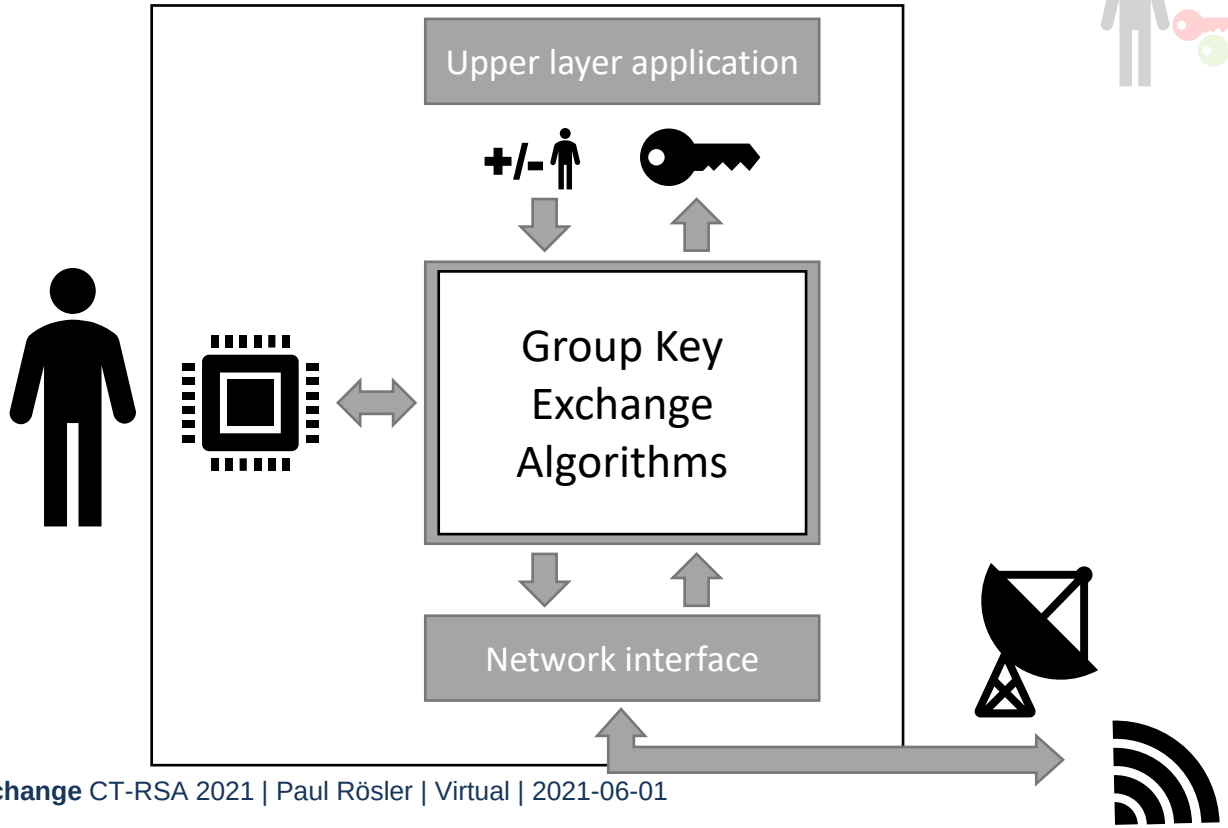
} >30 different security definitions

⇒ 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

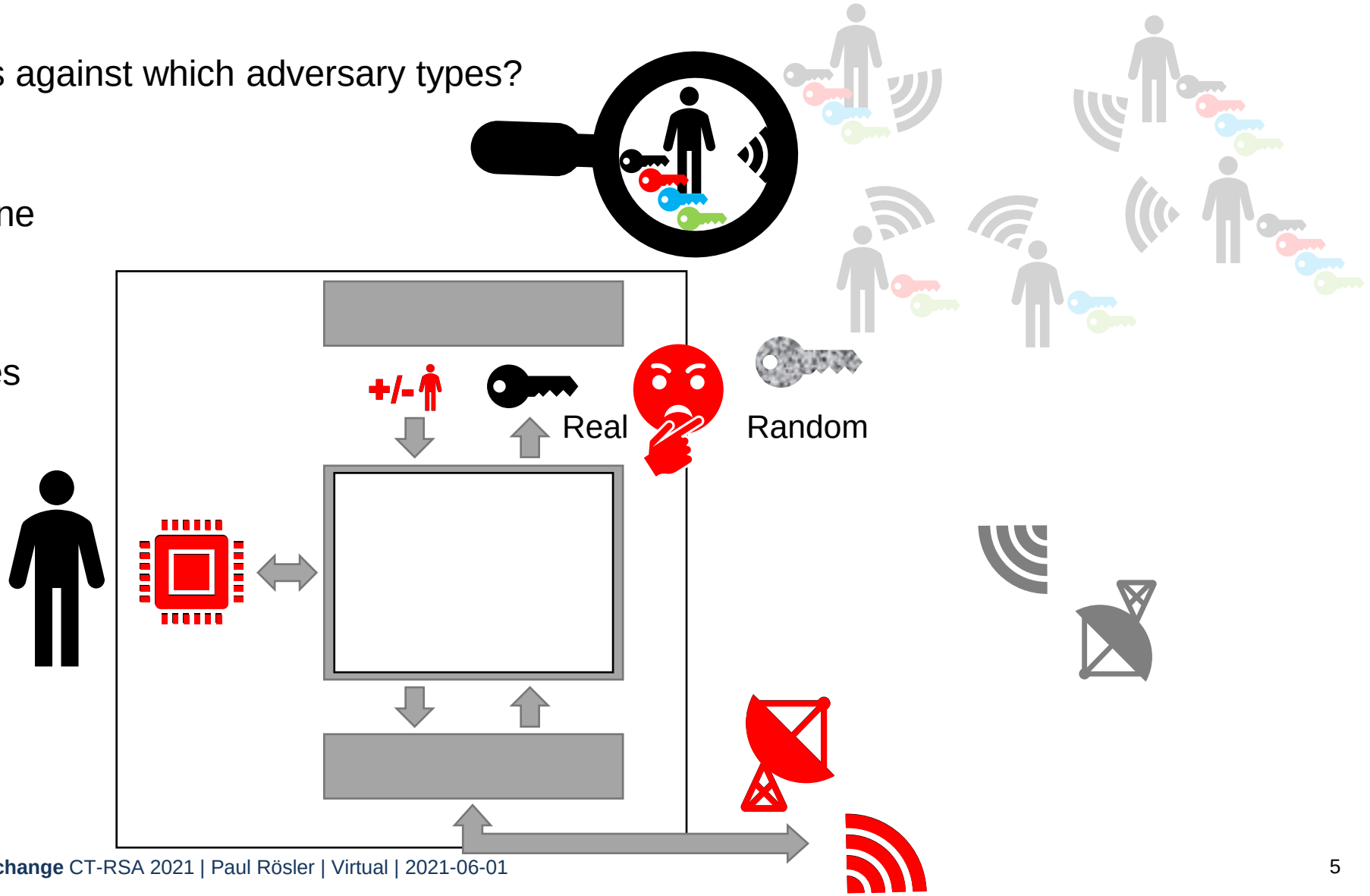


Prerequisites: Define “GKE” and “Security”

Security: Which security goals against which adversary types?

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

- Realistic adversary capabilities



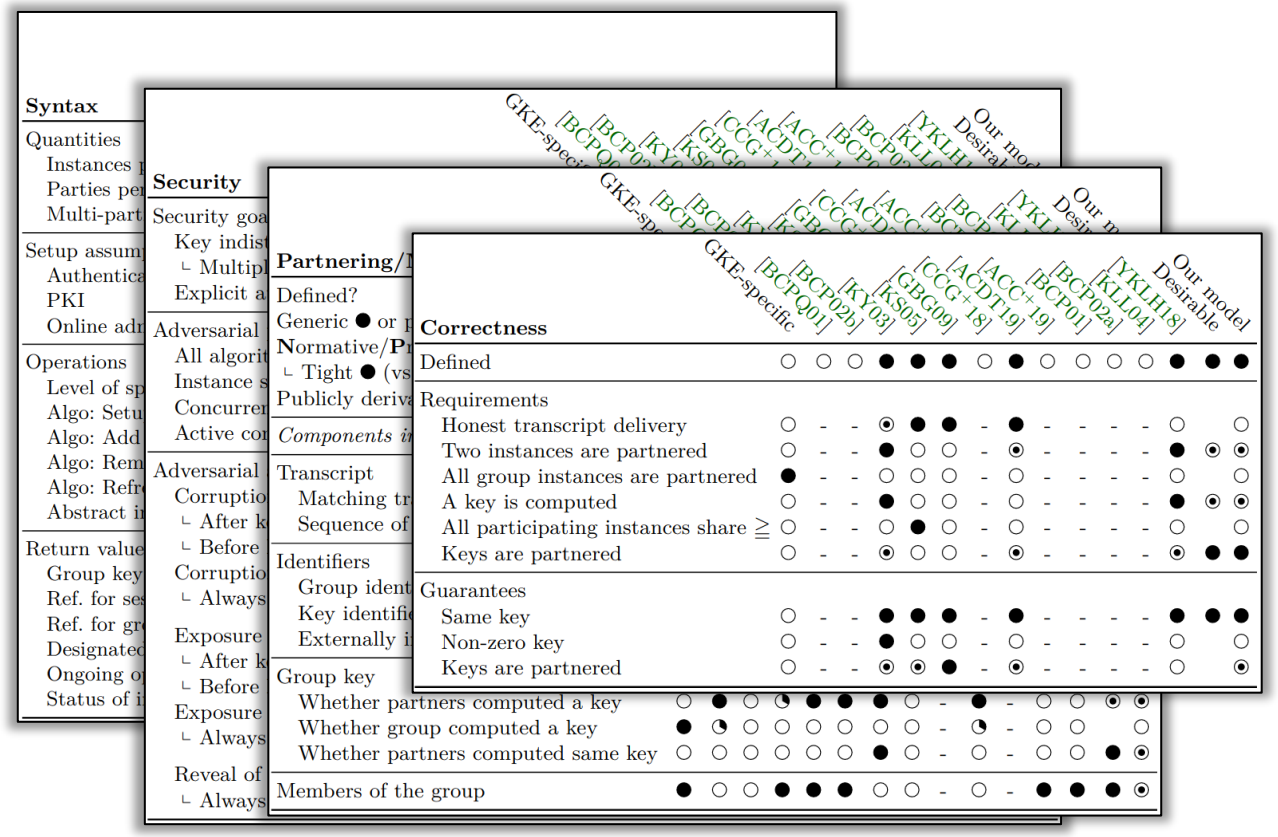
Overview: Shortcomings and Implications

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



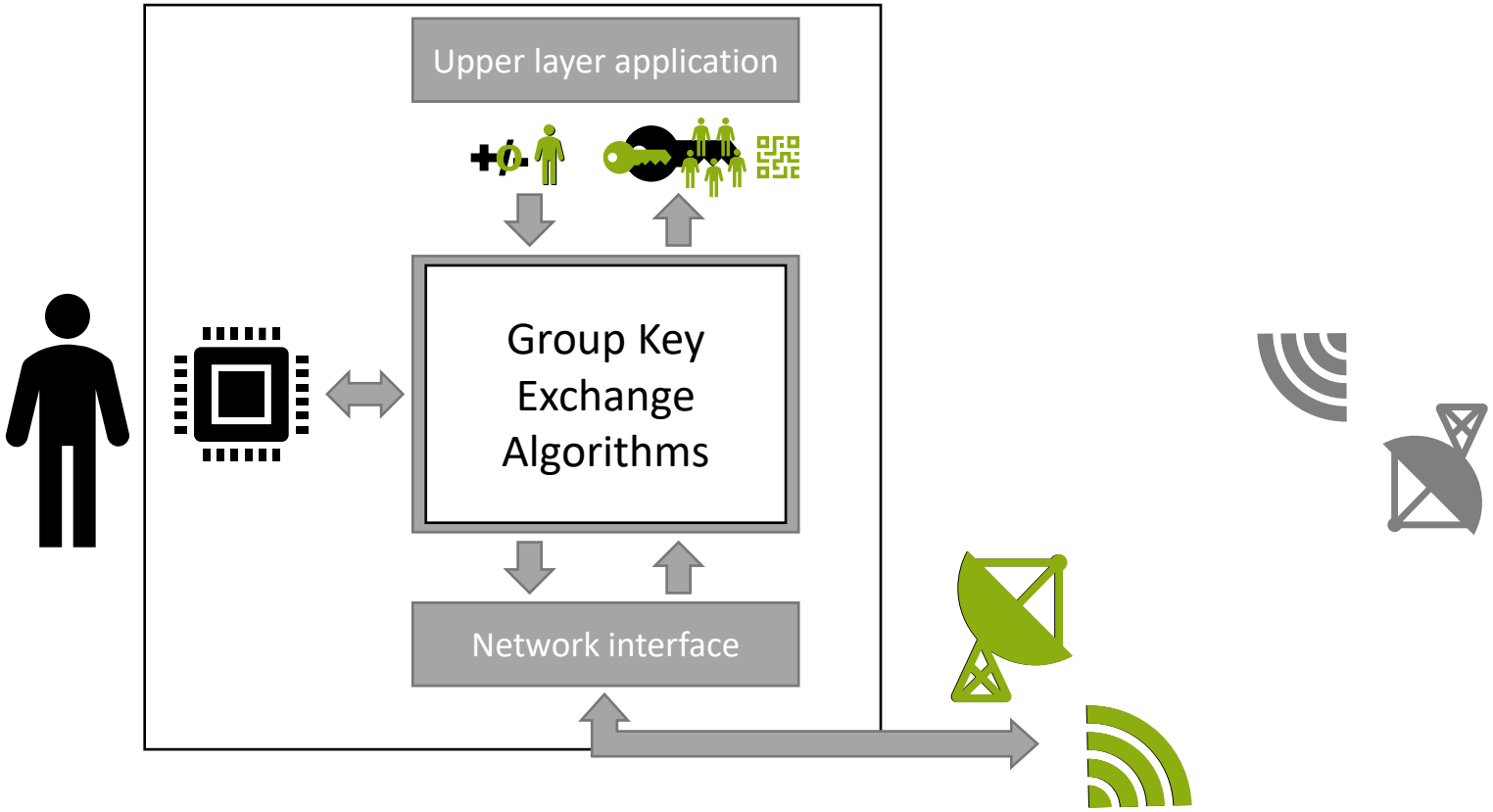
Results: No generic standard model available

- 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
  - …

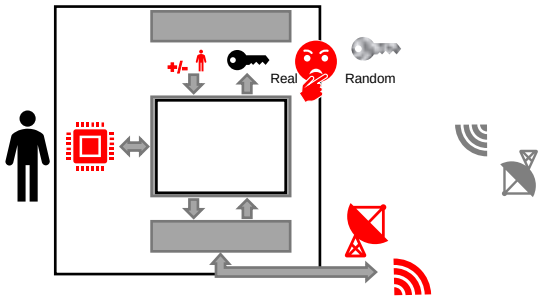
Our Enhancements

… 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



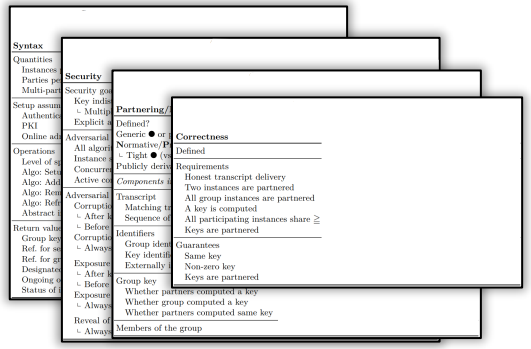
Agenda



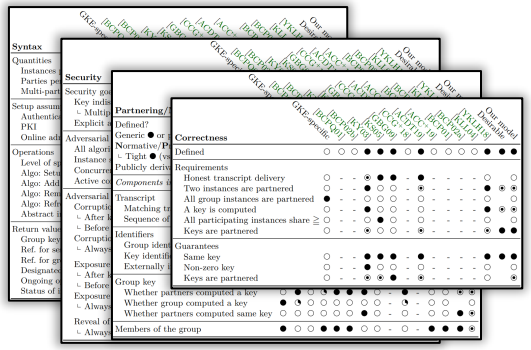
What is GKE abstractly?

Develop Understanding of "GKE"

Derive Systematization Framework



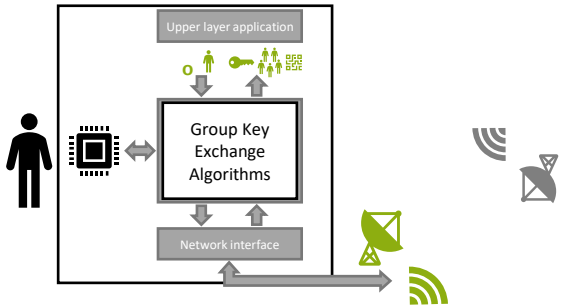
Qualities of GKE models & desirable realizations



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