T-IBE-T

Identity-Based Encryption for Inter-Tile Communication

12th European Workshop on Systems Security (EuroSec '19)
2019-03-25, Dresden, Germany

Alexander Würstlein, Wolfgang Schröder-Preikschat

Friedrich-Alexander-Universität Erlangen-Nürnberg
Chair in Distributed Systems and Operating Systems

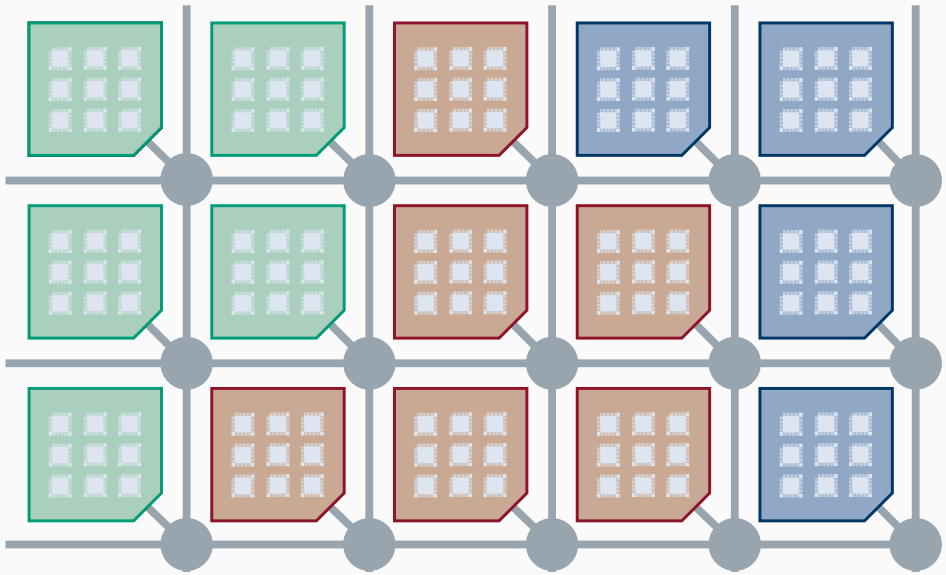
Chair in Distributed Systems
and Operating Systems

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

DFG SFB/TRR 89

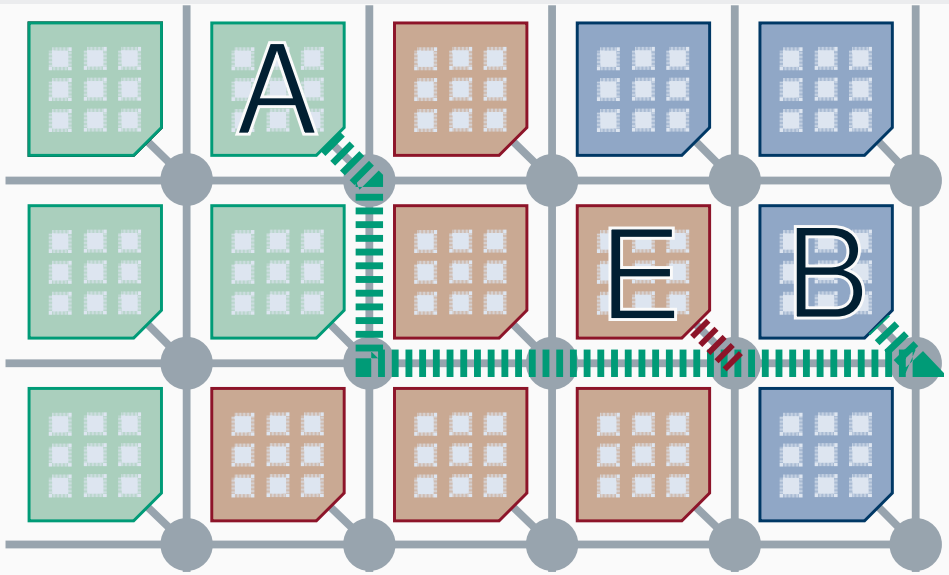
Tile-Based Architectures: Invasive Computing

- The way to 1000 cores: tiled multicore architectures
  - Tile = cores + shared mem + NoC interface
  - NoC: network on chip, grid network connecting tiles
- Needs novel approach: Invasive Computing
  - Location-awareness and regionality
  - Microparallelism
  - Flexible and on-demand



Network on Chip: Attacker model

- Tile-to-tile communication grid
- Multiple users and applications, possibly Eve
- Routing and OS are trusted
- Network interfaces (and Eve) may read messages passing them
- Needed: secure sensitive messages



Goals

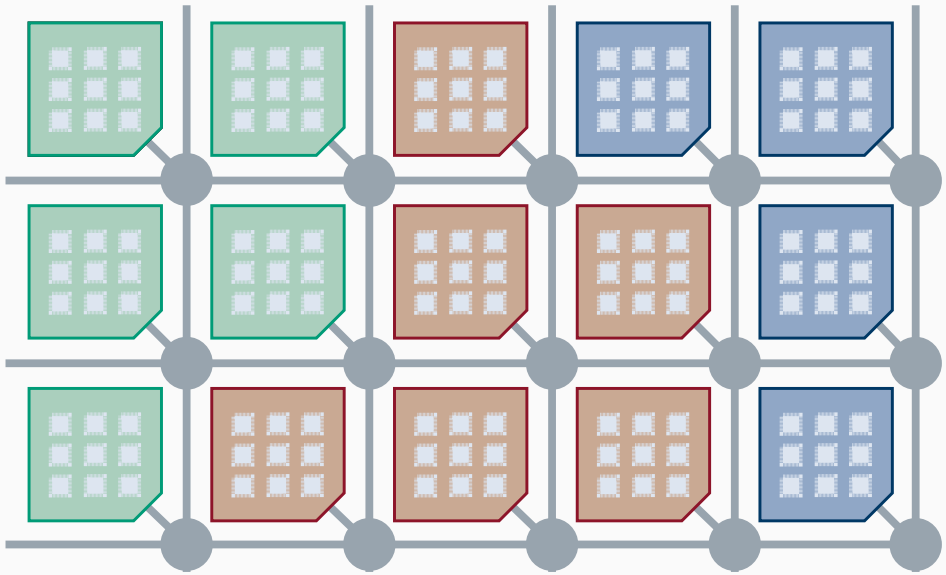
Our Goals

Frame ø contains payload

No prior connection to Bob necessary

Minimal-overhead central authority

Tailored to tiled architectures



Possible solutions

Symmetric keys

- Fast
- Pregenerated or created by Trent
- One key per pair, $\mathcal{O}(n^2)$

”Just use TLS”?

- RSA or Diffie-Hellman key exchange
- Symmetric key after key agreement
- Synchronous roundtrip before first data

Possible solutions

Symmetric keys

- Fast
- Pregenerated or created by Trent
- One key per pair, $\mathcal{O}(n^2)$

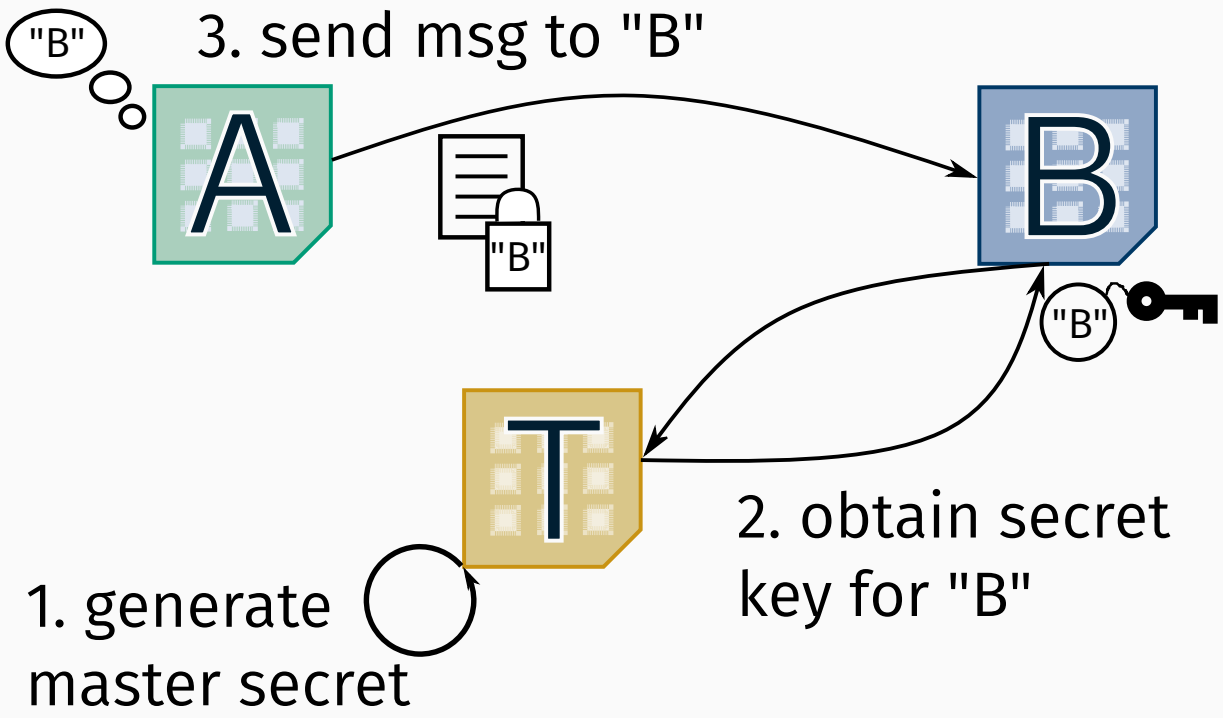
”Just use TLS”?

- RSA or Diffie-Hellman key exchange
- Symmetric key after key agreement
- Synchronous roundtrip before first data

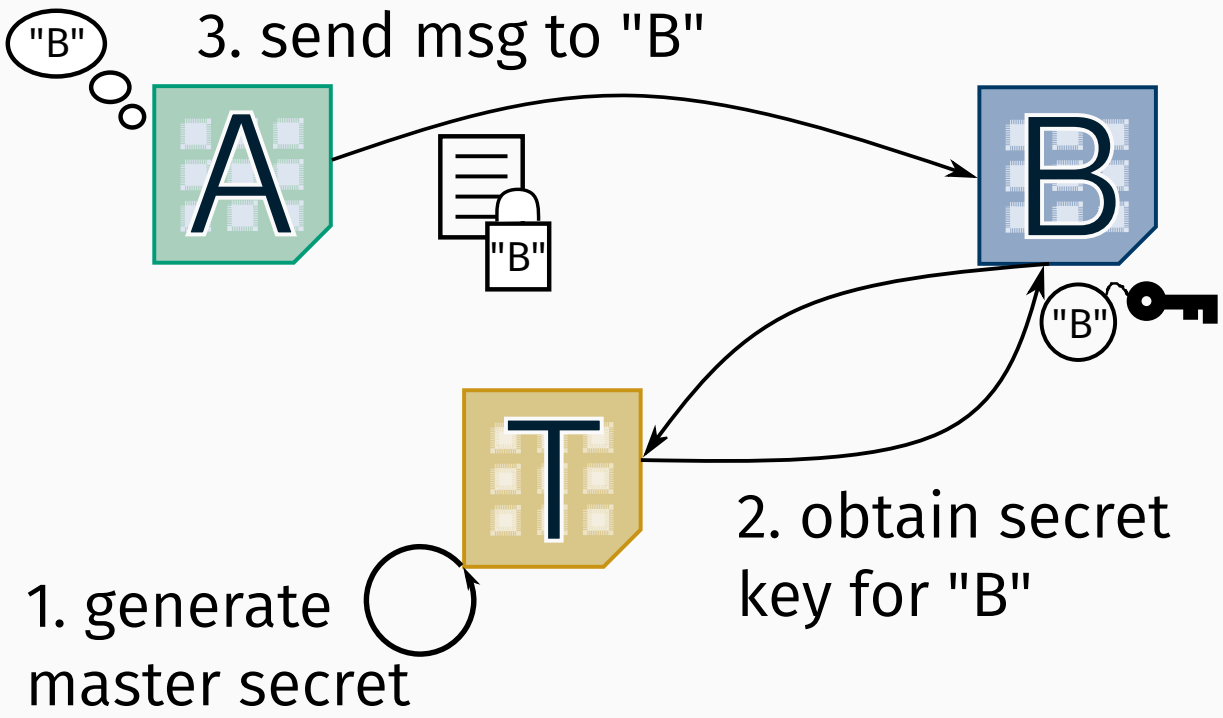
Our Answer

T-IBE-T: Identity-Based Encryption for Inter-Tile Communication

Identity-Based Encryption



Identity-Based Encryption



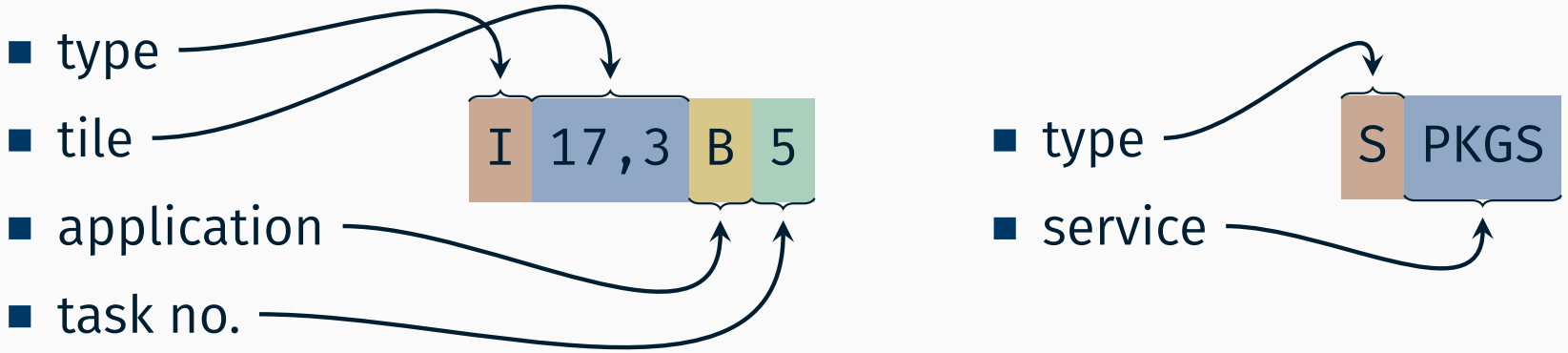
- Alice just needs Bob's name: "Bob"
- Bob's secret key only needed at decryption time
- Maximum asynchronicity: Bob need not even exist yet
- Key escrow: Trent knows secret keys

Specifics of T-IBE-T

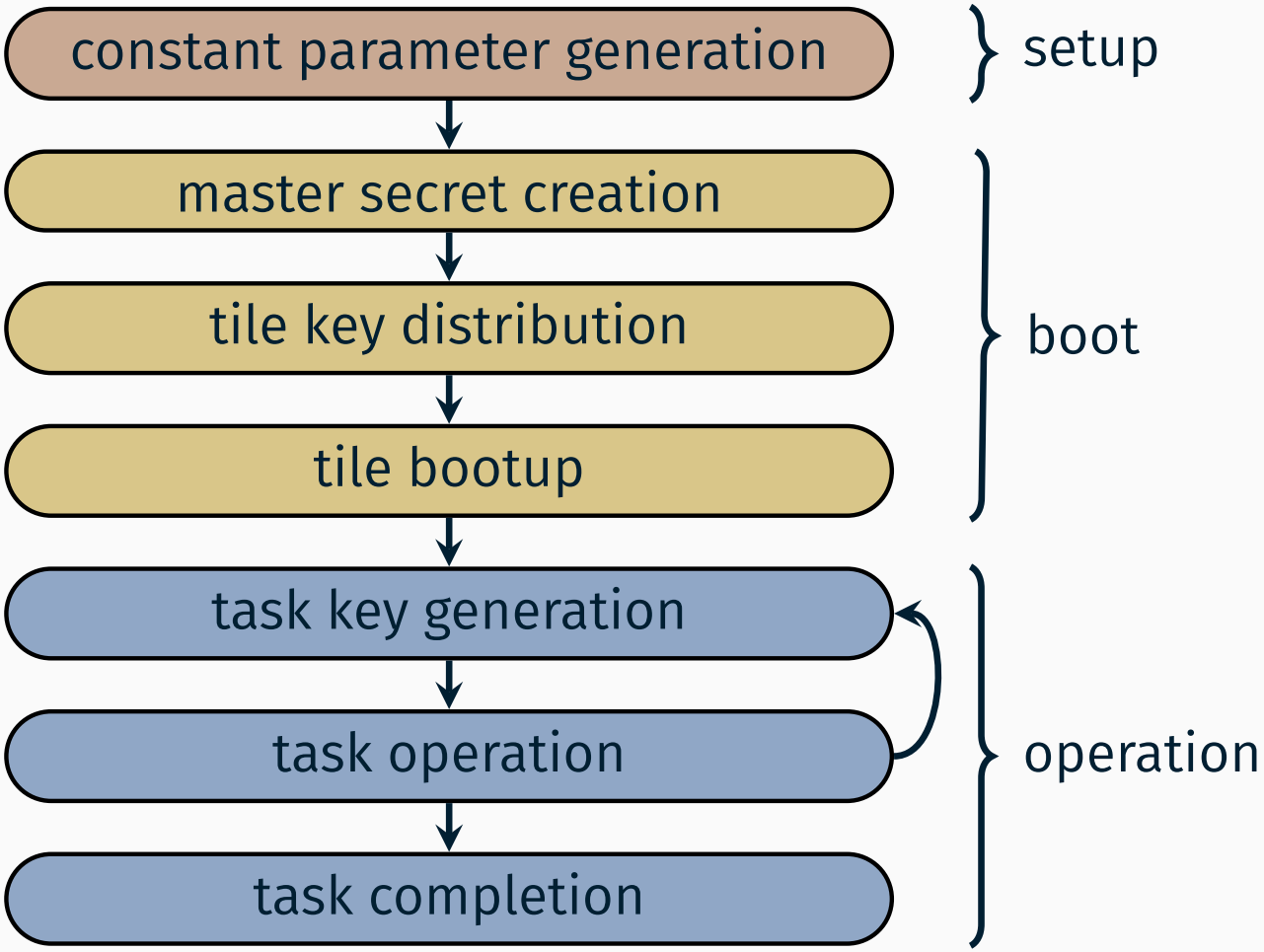
How T-IBE-T works

- Global OS service generates private keys
- Tile OS creates local task and gets task privkeys
- Hybrid: IBE encrypts symmetric message key
- Key escrow useful: debugging, tracing
- Identity/name from address

Identity Examples: task & global service



T-IBE-T system operation



Comparison of T-IBE-T with traditional solutions

	key distrib.	key dir. size	async?	# frames A ↔ T	# frames A ↔ B
symmetric	global dir.	$\mathcal{O}(n^2)$ ✗	sync ✗	2 ✗	1 ✓
symmetric	local dir.	$\mathcal{O}(n)$ ✗	async ✓	0 ✓	1 ✓
RSA	local dir.	$\mathcal{O}(n)$ ✗	async ✓	0 ✓	1 ✓
RSA	CA	$\mathcal{O}(1)$ ✓	sync ✗	0 ✓	3 ✗
DH + RSA	CA	$\mathcal{O}(1)$ ✓	sync ✗	0 ✓	3 ✗
T-IBE-T	**IBE**	$\mathcal{O}(1)$ ✓	async ✓	0 ✓	1 ✓

Next Steps

Prototype Create a prototype for evaluations

Benchmark Compare prototype with other approaches

Prove Create and prove formal definition

Improve Hierarchical IBE?

Conclusion

T-IBE-T idea:
Identity-Based Encryption for Inter-Tile Communication

- ✓ Tailored to OS and hardware
- ✓ Asynchronicity
- ✓ Data in Frame ø
- ✓ Minimal resources

Conclusion

T-IBE-T idea:
Identity-Based Encryption for Inter-Tile Communication

- ✓ Tailored to OS and hardware
- ✓ Asynchronicity
- ✓ Data in Frame ø
- ✓ Minimal resources

Questions?