Keep the Dirt: Tainted TreeKEM, Adaptively and Actively Secure Continuous Group Key Agreement

Karen Klein[1] Guillermo Pascual-Perez[1] Michael Walter[1] Chethan Kamath Margarita Capretto[2] Miguel Cueto[1] Ilia Markov[1] Michelle Yeo[1] Joël Alwen[3] Krzysztof Pietrzak[1]

IST Austria[(1)], Universidad Nacional de Rosario[(2)], Wickr Inc.[(3)]

Introduction

This work focuses on improving the efficiency of existing Continuous Group Key Agreement (CGKA) protocols, underlying efficient secure group messaging. In particular, it builds on TreeKEM, the protocol by the IETF working group on Message Layer Security (MLS). We formalize and analyze a modification named Tainted TreeKEM (TTKEM).

Continuous Group Key Agreement (CGKA)

Interactive protocol allowing a group of n users to agree on a common sequence of keys with the following characteristics:

- Dynamic membership: add and remove group members.
- Asynchronous: no assumptions on users online behaviour.
- Forward secret and Post-Compromise Secure.

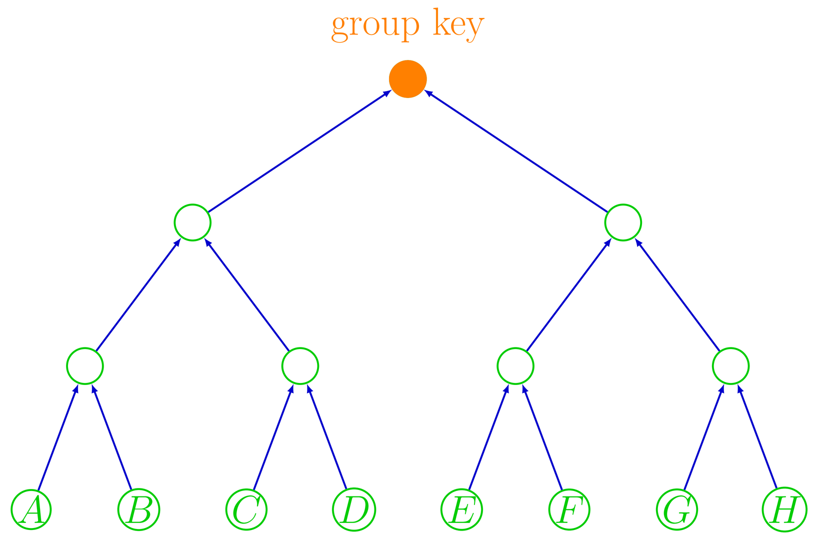
Further, efficient key updates (logarithmic in n).

Ratchet trees

Basic data structure used by TreeKEM and TTKEM.

- Leaves: associated to users.
- Nodes: associated with PKE key-pairs.
- Edges: knowledge of source secret key implies knowledge of sink secret key.

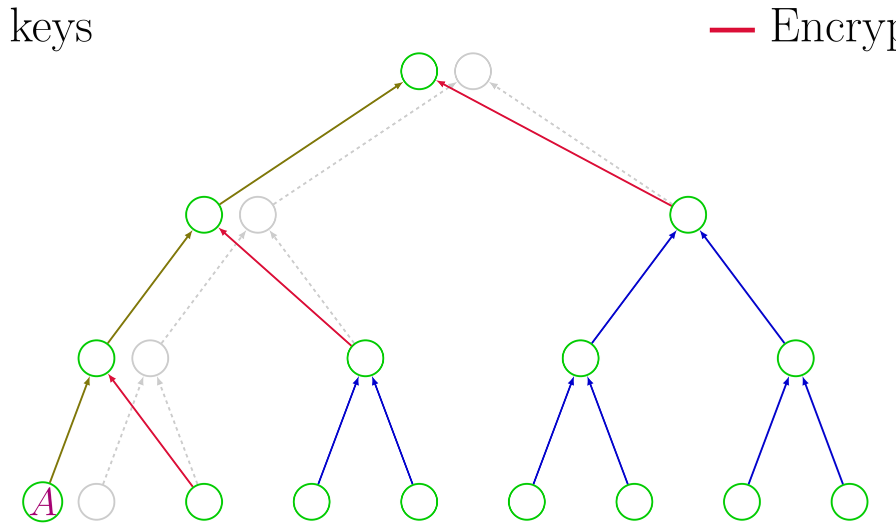
$\Rightarrow$ users know secrets keys on their *path to the root*.



Key update by party A

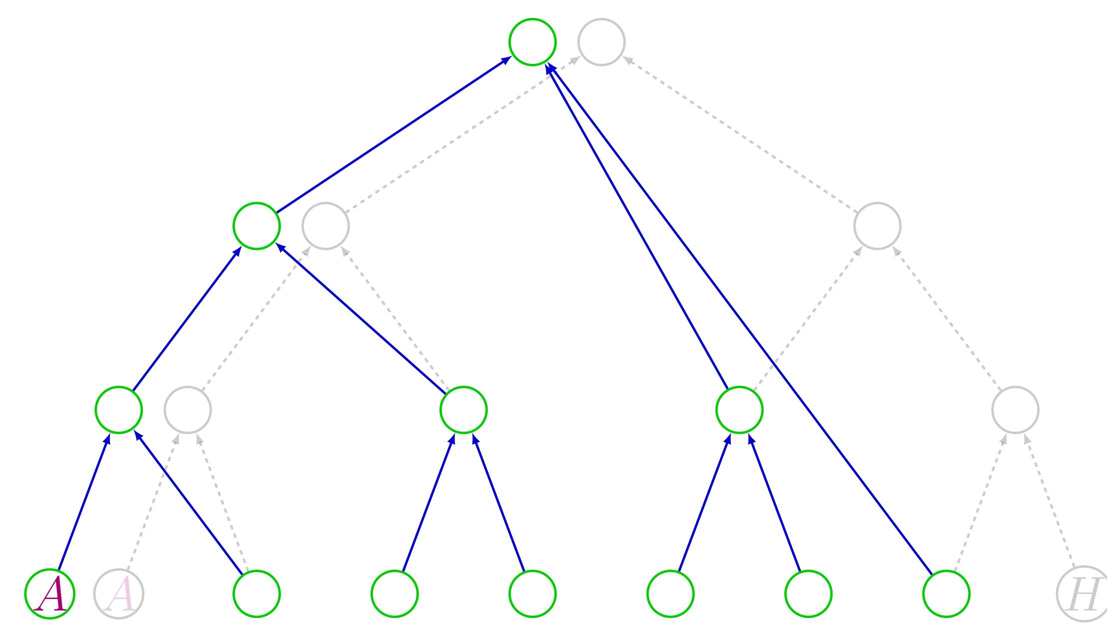
- chooses and encrypts fresh keys
- removes old keys

Hash derivation
Encryption



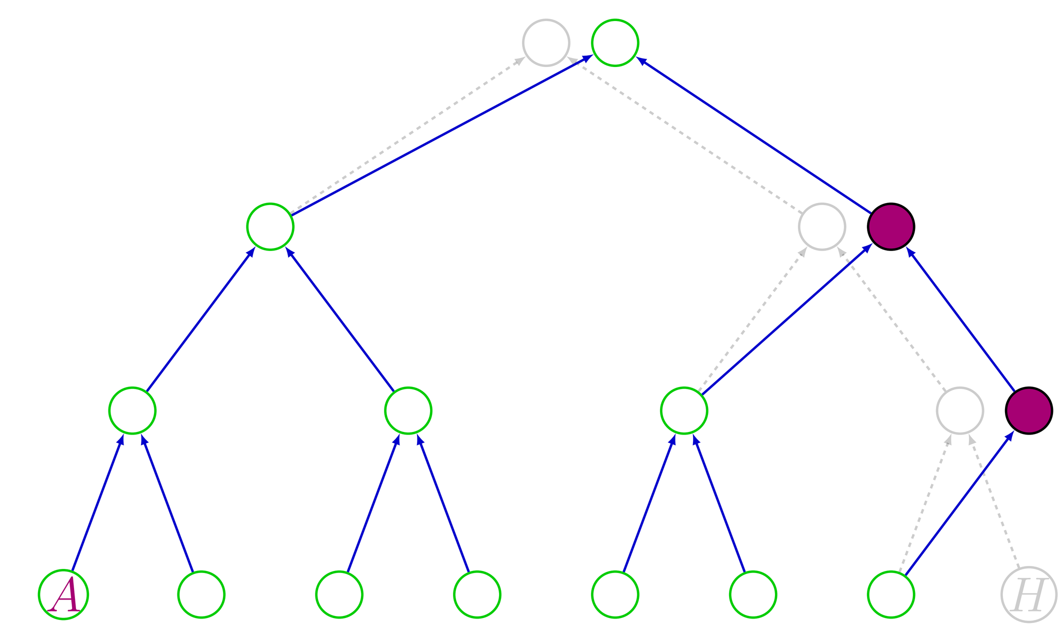
Only $\log(n)$ encryptions needed to communicate new keys to group.

TreeKEM



H is removed by A by *blanking*, i.e. deleting the keys on H's path. Blanks might induce extra encryptions in future updates.

Tainted TreeKEM (TTKEM)



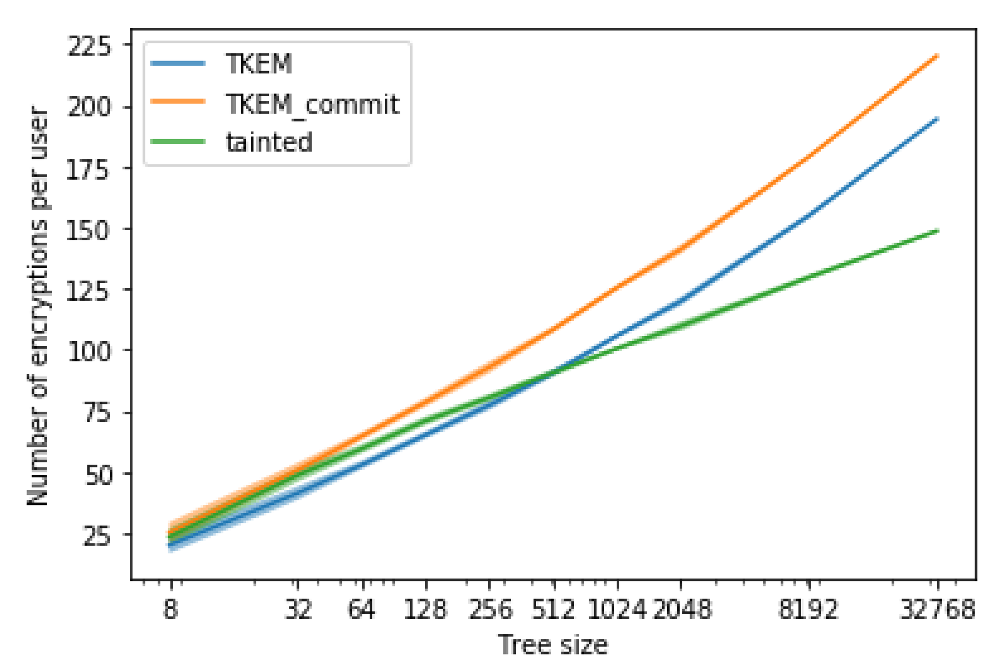
A removes H by sampling new keys for nodes on H's path. Those nodes become *tainted by A*, and have to be updated again when A updates or is removed.

Efficiency

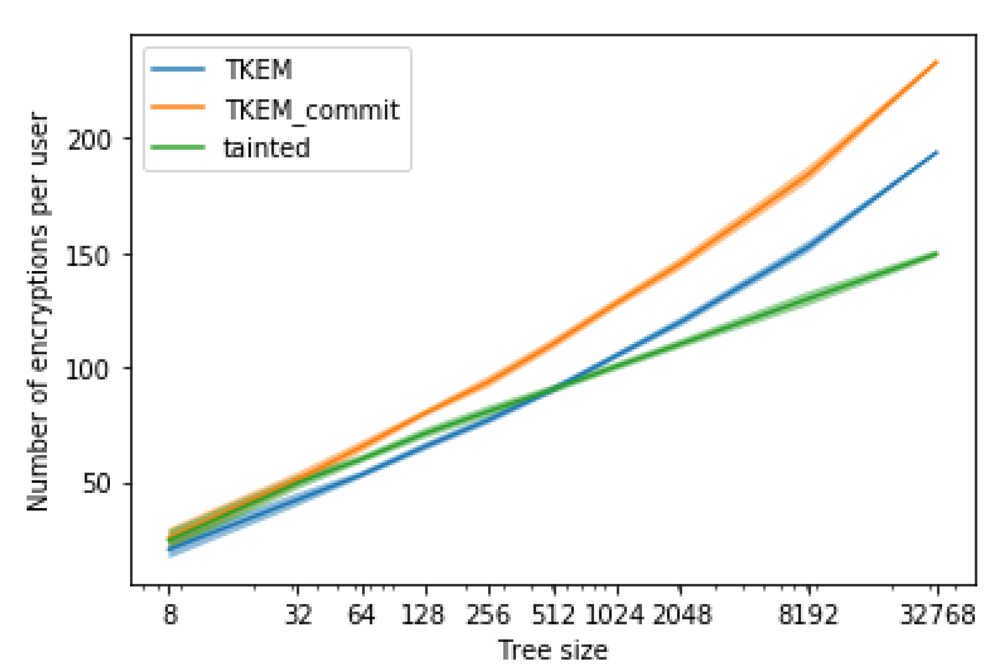
We are interested in the communication efficiency of equivalent protocol executions in TreeKEM and TTKEM. TreeKEM recent versions bundle several group operations into one. We compared TTKEM against two variants, one more and one less efficient than TreeKEM, resulting from different ways of bundling operations.

Setting I

- Adds & removes performed by all users uniformly.
- Two cases based on users updating distribution.



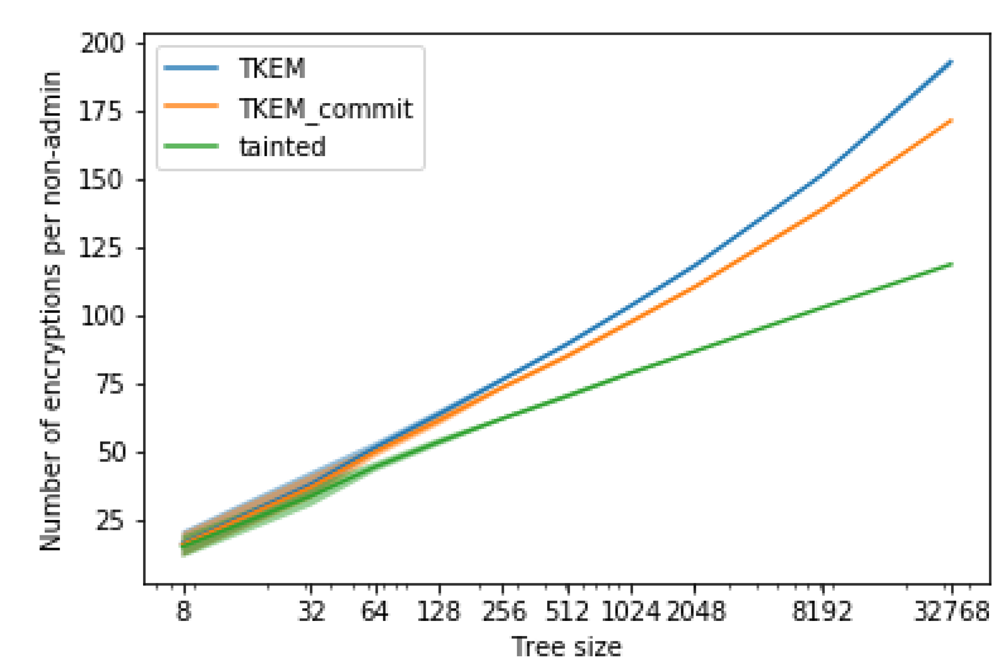
Setting I.I: Average cost with uniform updates.



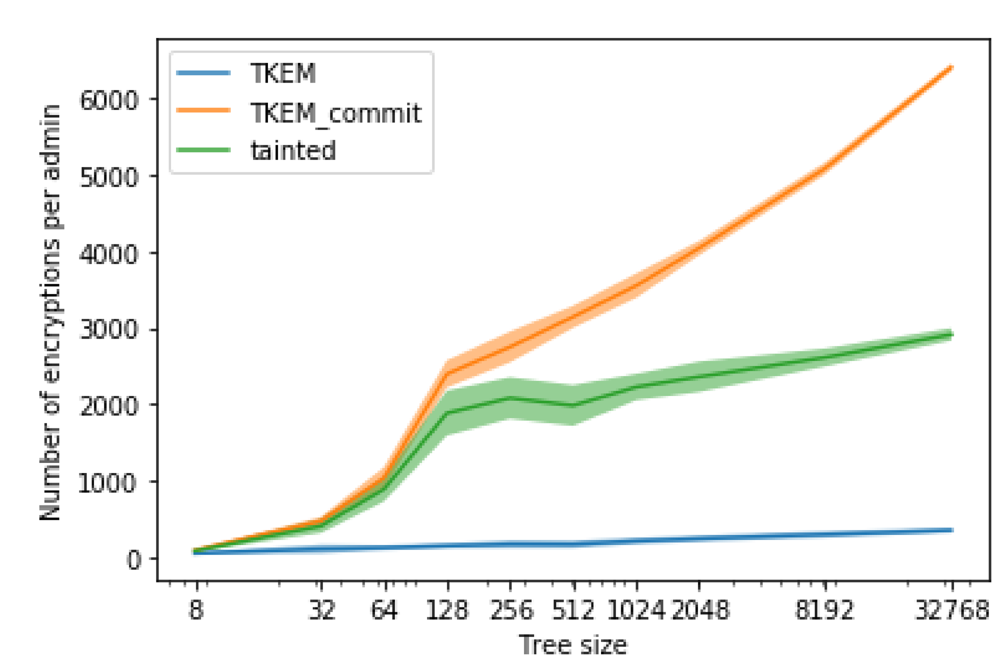
Setting I.II: Average cost with zipf updates.

Setting II

- Adds & removes only by small set of administrators.
- Trade-off between cost for admins and non-admins.



Average cost for non-administrators.



Average cost for administrators.

Security

Adversarial Model.
We consider an adversary that:

- Can control protocol execution and corrupt users *adaptively*.
- Corrupts throughout time-windows:
  - leaks all user state, including *randomness* used while corrupted.
- Is 'partially' *active*:
  - Full network control.
  - Not allowed to craft messages.
- Wins if can *distinguish* group key from random.
  - Exclude trivial challenge: define *safe* predicate.

Theorem 1 (Standard Model):

Enc ϵ-IND-CPA secure, H ϵ-pseudorandom
$\Rightarrow$ TTKEM $\epsilon \cdot Q^{\log(n)}$-CGKA-secure.

Theorem 2 (Random Oracle Model):

Enc ϵ-IND-CPA secure, H random oracle
$\Rightarrow$ TTKEM $\epsilon \cdot (Qn)^2$-CGKA-secure.

where Q - # of operations; n - # of users.

Results Overview

- Formalized Tainted TreeKEM, a CGKA protocol using *tainting* instead of *blanking*.
- Efficiency simulations showing TTKEM is *more efficient* than TreeKEM for natural distributions.
- Security proofs for TTKEM both in standard model and ROM that *extend to TreeKEM*.
- *First adaptive proof* for any CGKA with polynomial loss.

Acknowledgements

Several authors were funded by the European Research Council (ERC) under the European Union's Horizon2020 research and innovation programme, either under the TOCNeT (No. 682815) or the Marie Skłodowska-Curie (No. 665385) Grant Agreements.

IST AUSTRIA Institute of Science and Technology
wickr
European Research Council Established by the European Commission

Contact: gpascual@ist.ac.at