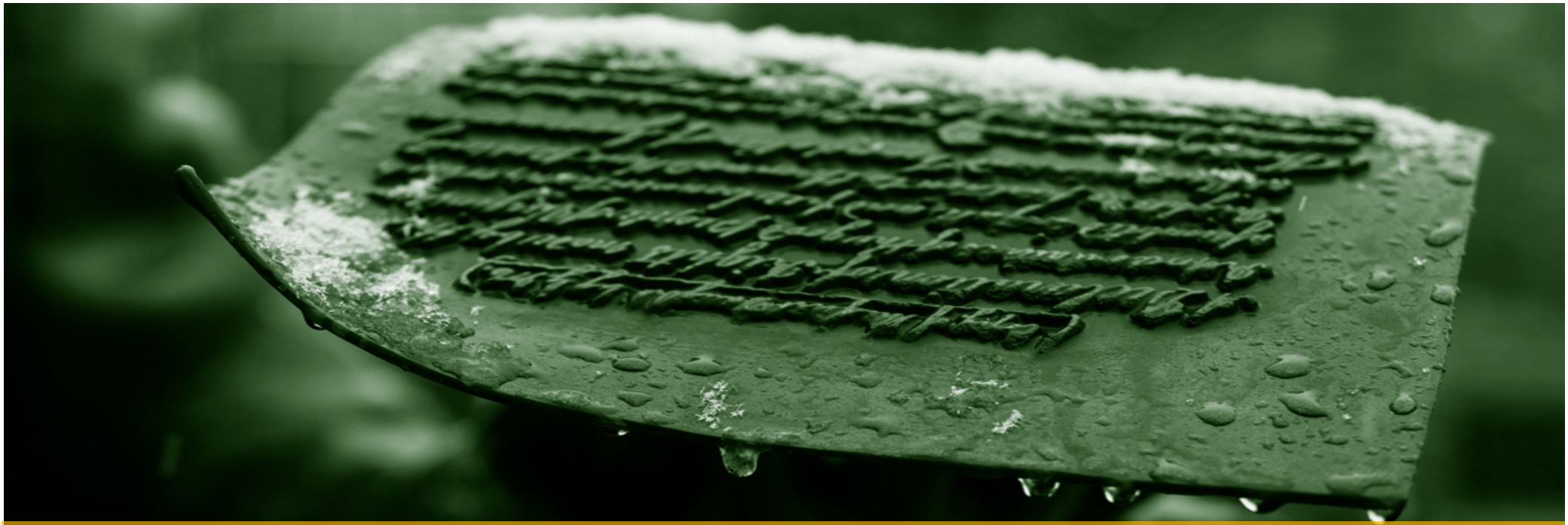


ANATOMY OF DNSSEC KEY TRANSITIONS

Eric Osterweil

Pouyan Fotouhi Tehrani -- Weizenbaum Institute / Fraunhofer FOKUS

Thomas C. Schmidt -- HAW Hamburg

Matthias Waehlisch -- Freie Universität Berlin

GEORGE MASON UNIVERSITY

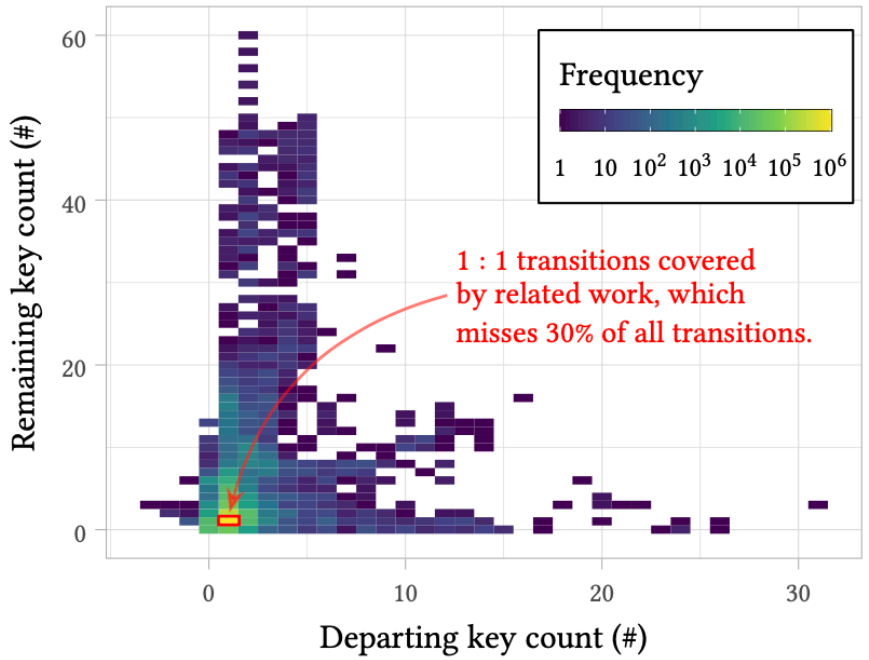
INTRODUCTION

- In 2005, we started monitoring DNSSEC with SecSpider (https://secspider.net/)
  - Not presuming we knew everything we wanted to analyze
- Recently, interest in key rollovers has emerged
  - Root zone KSK has spawned publicity and research
- But, key "rollovers" do not fully describe what we have seen in the wild for the last 15 years
- "To know the path ahead, ask those coming back"
  – Chinese proverb
- What can we learn about key rollovers by looking at how they have been conducted, and what should we formalize about *how* to conduct them going forward?

IN SEARCH OF THE ANATOMY

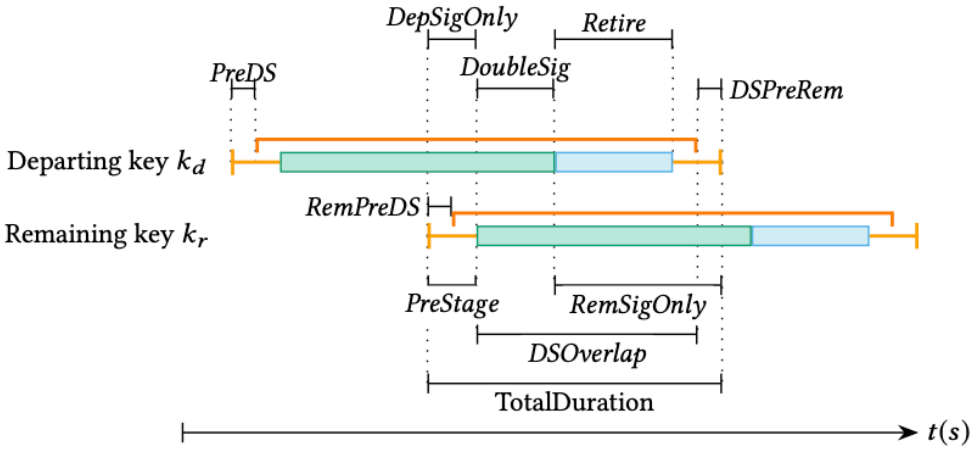
- Our first observation has been that keys often change in sets that are larger than 1:1

- Example, in a zone with *n* keys (some used to sign data):
  - If transitioning to *m* keys (some used to sign), which key(s) rolled over to which other keys?
  - Did all of departing keys rollover to each/all remaining?
  - If some keys persisted, did they also get rolled over to?



- We define changing of keys as "key transitions"
  - May be composed of multiple [simultaneous] "rollovers"
- We also defined an "anatomy" of what should be *measured* in order to quantify transitions

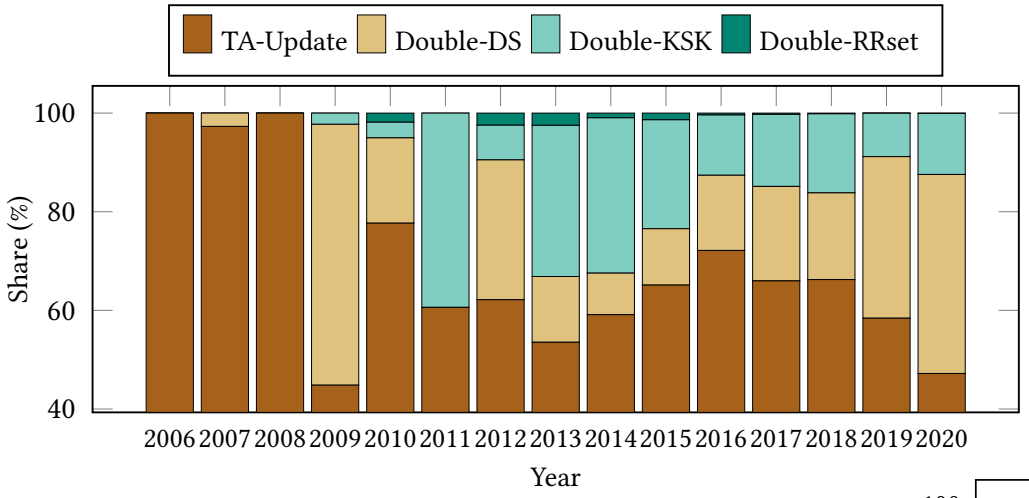
- We defined the measurable properties of timing between keys
  - We include counts of how many keys
  - if/when they were in use
  - what their relative ages are
  - etc.



- We used this to measure where keys did/did not adhere to guidance
  - RFC-5011 and RFC-7583
  - A proposal for conducting emergency key rollovers (transitions) [1]
  - Plan to use it to measure RFC-8901 (Multi-Signer)

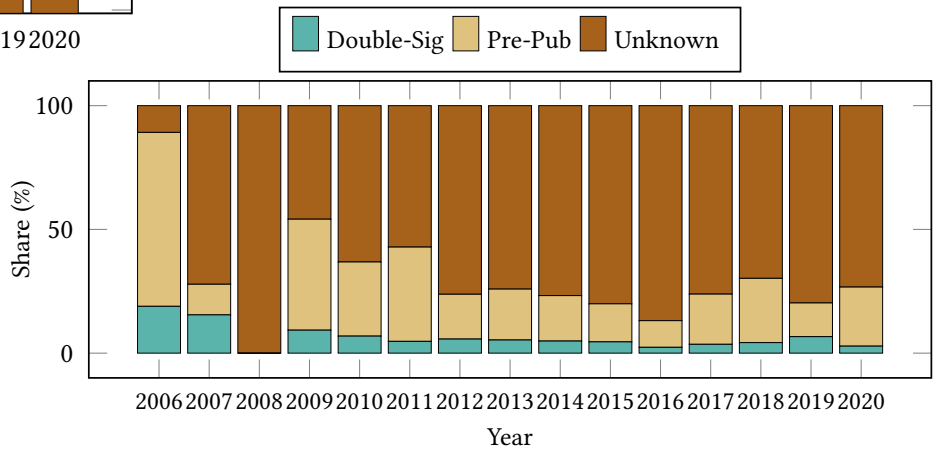
[1] Zheng Wang and Liyuan Xiao. Emergency key rollover in dnssec. In 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, pages 598–604. IEEE, 2014.

OUR ANALYSES



KSK transitions

ZSK transitions



OUR THOUGHTS…

- As operations are becoming more familiar/comfortable with DNSSEC (and as tools continue to mature), *popular* key transition processes are emerging
- With a formal anatomy, want to provide input into future key transition guidance
- Full paper of these results is under submission, but available upon request

THANK YOU