Time-Valid Security:

- \( k = 80-128, \ 2^k \approx 2^{128} \) at adversary side
- Lenstra crypto key sizes: www. cryptokeylength.com (key size?) 10^6 - 10^9 years security guarantee

Temporal Security: Guarantee lasting \( t \) unit of time

\[
\text{Trade-off:} \quad 2^k \rightarrow (|sk| = 1024, t') \\
\quad \uparrow \quad \Downarrow \quad (|sk'| = 1024, t'') \\
\quad \text{unit} \\
\]

\( |sk'| = 1024 | < |sk| = 1024, \quad t'' < t' \)

Stateful Signature → Packet loss → Resynchronize the network

High-biased
Lenpirt, HORS
\( k \rightarrow k/2 \)
Birthday Precedent

\[
\text{PK}_0 \quad \text{PK}_1 \\
\quad \text{t-unit} \quad \text{t-unit} \\
\]

\text{AFL4, obscond, generate new } \text{Rsend}

- How to keep time accurate?
- What if they are lost?

Number-theory
RSA, ECC, DH
\( k \rightarrow \text{chrestic} \)

\( k = 80, \ \text{In} = 2048 \) RSA
\( k = 90, \ \text{In} = 512 \)