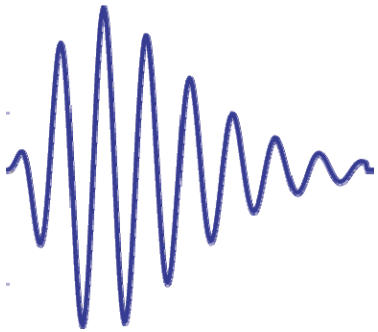
Geo-Encryption Using Loran



Stanford University
Sponsored by FAA Loran Program

Di Qiu
qiudi@stanford.edu

Digital Cinema Distribution

"Today, the film studios spend over $1 billion each year to duplicate, distribute, rejuvenate, redistribute and ultimately destroy the thousands of film reels required to bring the close to 500 films released each year to audiences across the U.S."

- "rise against the reel"
  - 35-mm print cost $ 1,200
  - limited showings
  - heavy, weighs 50 lbs
  - platter setup takes an hour
- Digital cinema
  - cost less, < $100 per screen load
  - unlimited showing
  - automatic setup

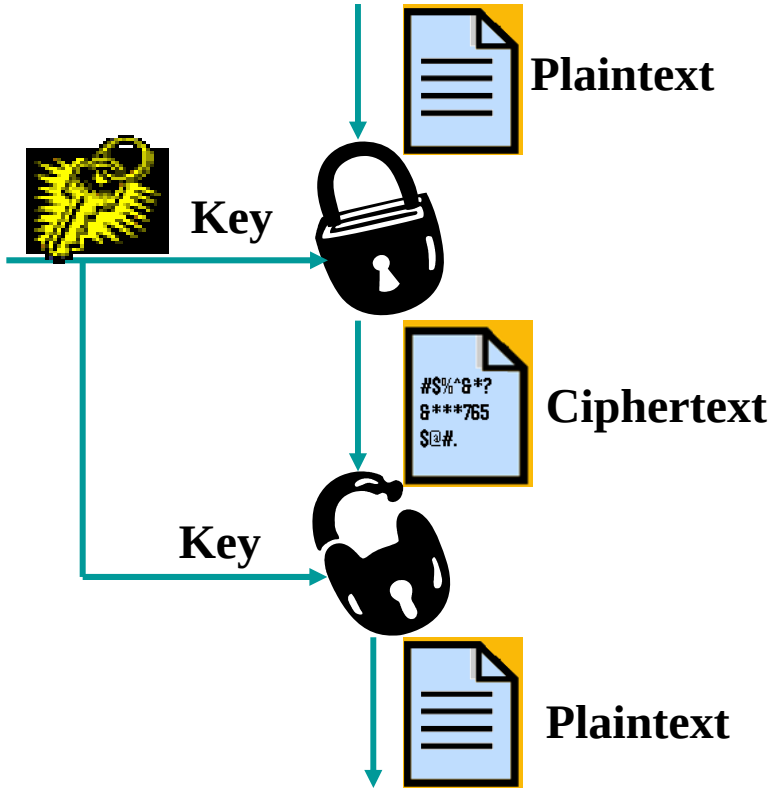
Digital Distribution Disadvantage

- **Napsterization concern**
  - Music sales are down 8%
  - Music company valuations are down 40%
- **Satellite distribution**
  - ~3 million unauthorized users

Encryption & Decryption

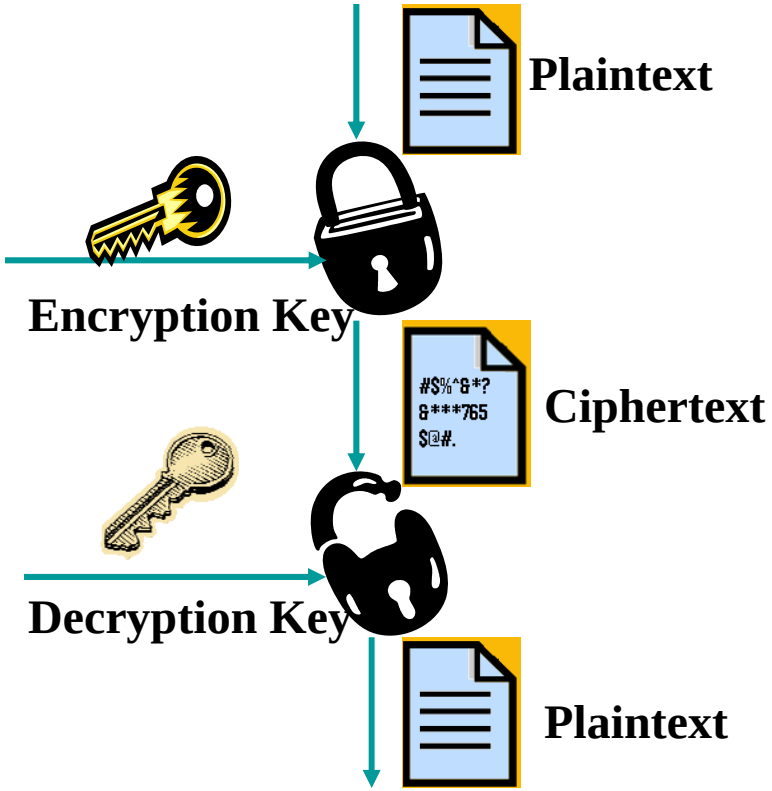
Symmetric Cipher:

Encryption key = Decryption key



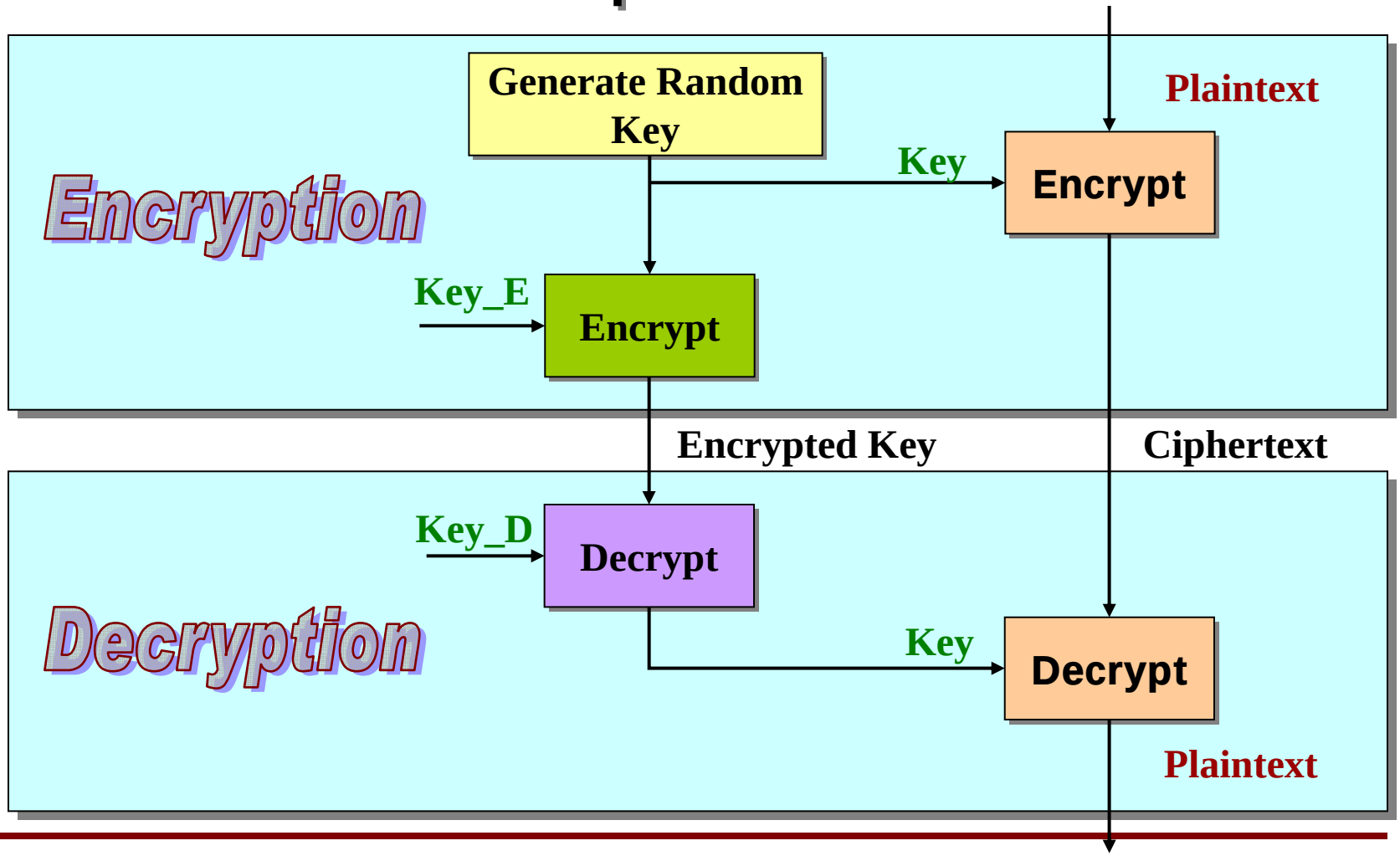
Asymmetric Cipher:

Encryption key ≠ Decryption key



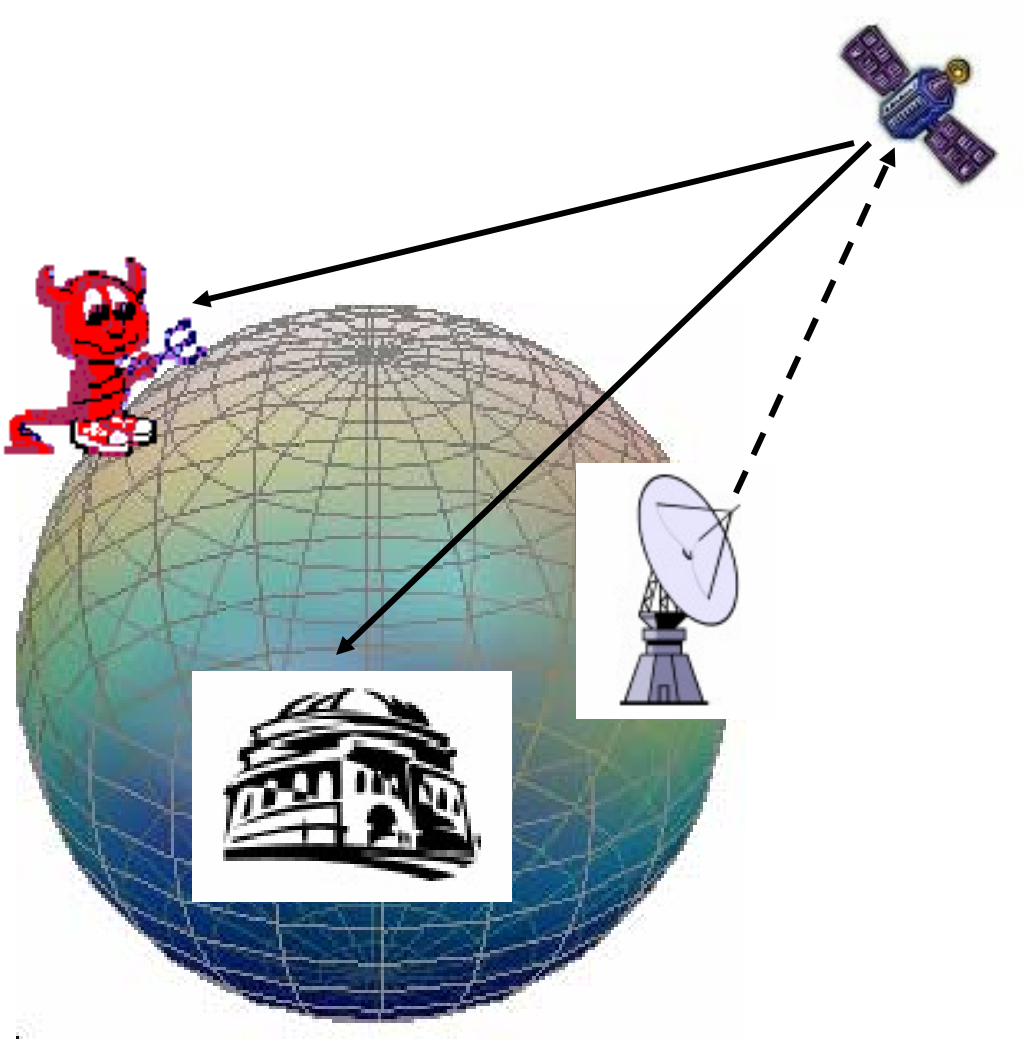
Hybrid Systems

-- a combination of asymmetric and symmetric ciphers

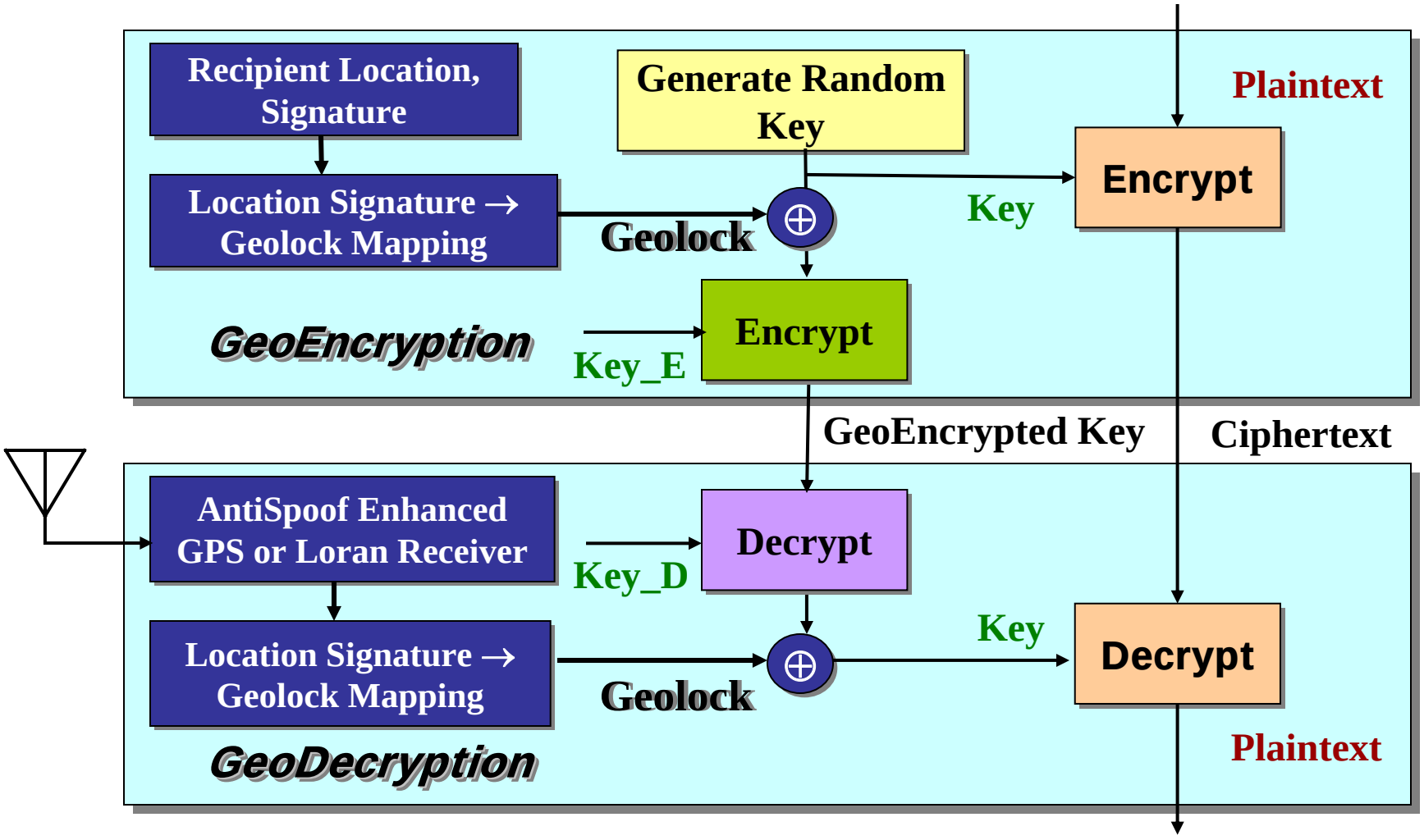


What is Geo-encryption?

- **Proposed by Dorothy Denning and Logan Scott**
- **Add another layer of security**
- **Not a replacement of the conventional crypto algorithms**



Geo-encryption Algorithm
-- Enhance the security



Comparison of the Signals
GPS v.s. LORAN

GPS

Pros
- Stable clock
- High absolute accuracy
- High repeatable accuracy
- Global coverage

Cons
- Low SNR
- Position accuracy depends on SV geometry
- LOS dependent
- Easy to spoof
- Indoor not capable

LORAN

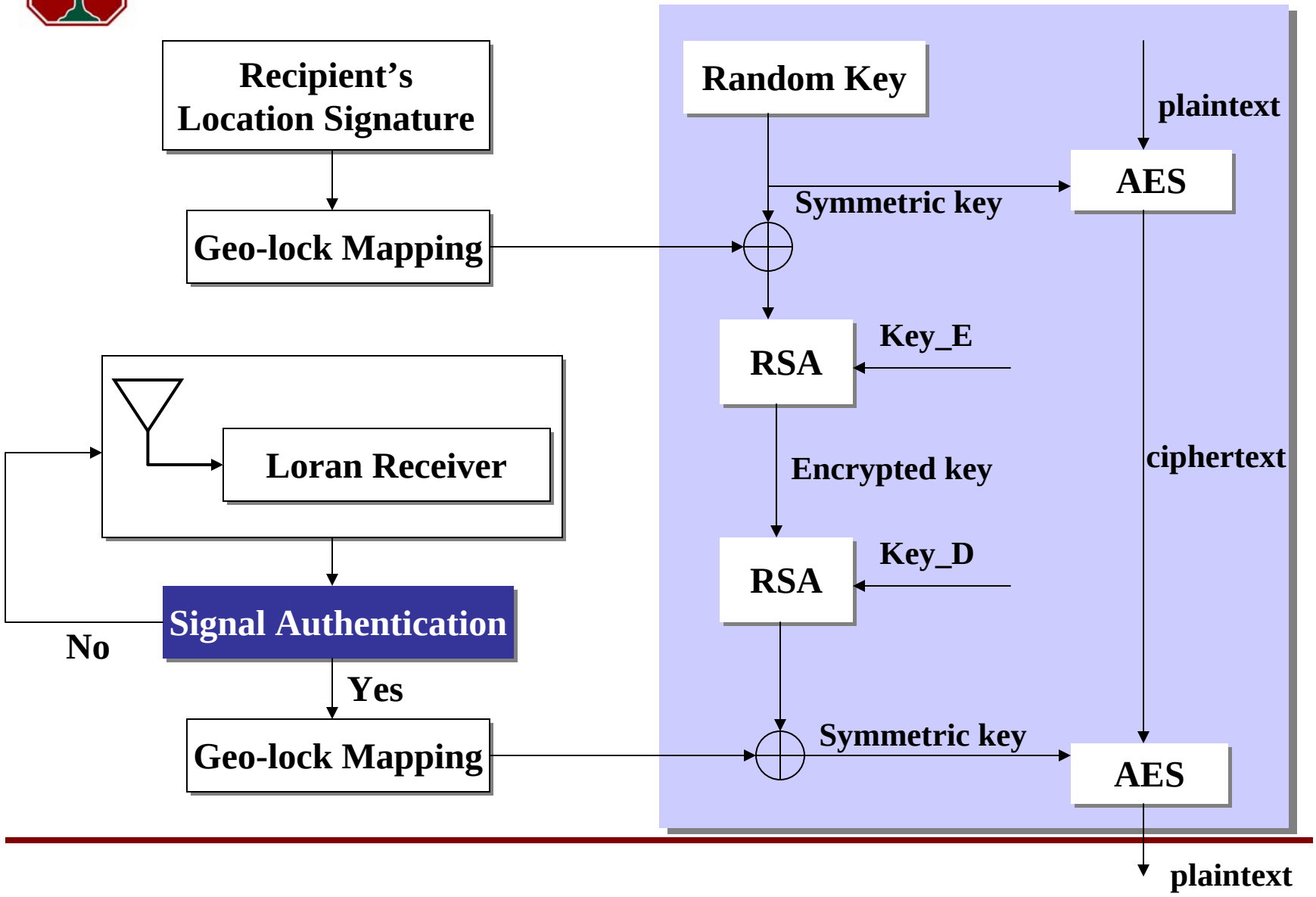
Pros
- Stationary transmitters
- Know signal shapes and SNR
- Groundwave propagation
- High signal power
- Jamming Loran is hard
- Indoors capable

Cons
- Skywave contaminations
- Signal quality depends on the transmitter distance

Research Objectives

- Signal authentication
  - Allows the receivers to ascertain its origins
  - Allows the receivers to verify that it has not been modified in transit
- Loran location signature
  - Study the consistency of Loran signal
  - Design Loran location signature
  - Map Loran location signature into geo-lock
- Build geo-encryption demonstration testbed

Modified Geo-encryption



Signal Authentication Requirements

- Low computation overhead for generation and verification of authentication
- Low communication overhead
- Buffering requirement
- Robust to packet loss
- Scales to a large number of receivers

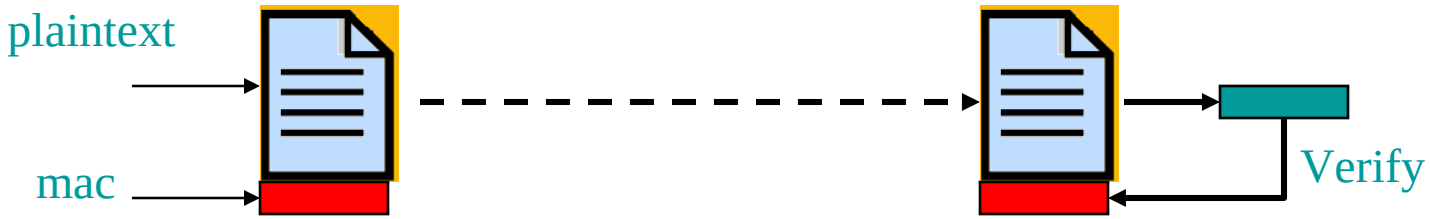
Why is Security for Broadcasts Hard?

- Symmetric authentication - not secure
- Asymmetric mechanism - not as efficient as symmetric authentication.

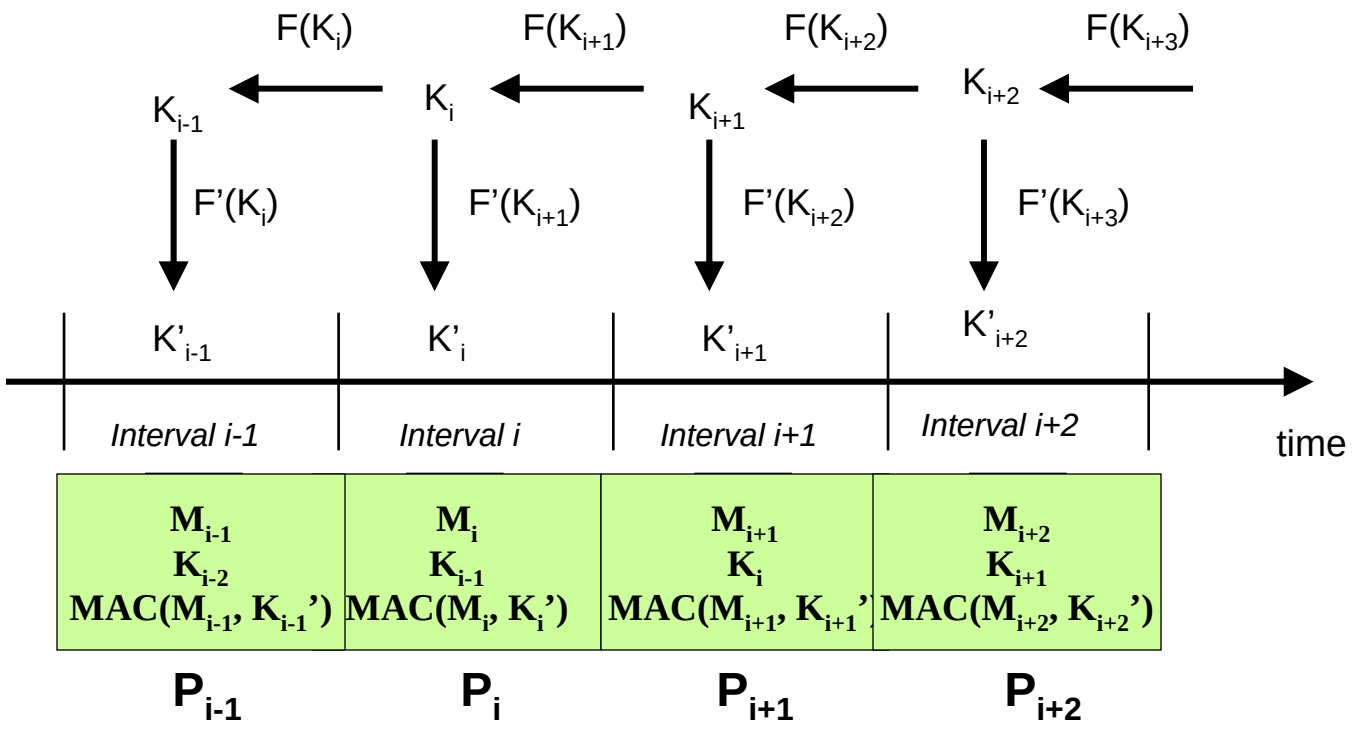
Timed Efficient Stream Loss-tolerant Authentication (TESLA)

Crypto Review

- Hash function : One way function
  - Collision resistant
  - Digest any message to a fixed hash value
  - MD5 (128 bits), SHA1 (160 bits), SHA256 (256 bits)
- Message Authentication Code (MAC)
  - Keyed hash function
  - Symmetric
  - Require to transmit the key
  - TESLA uses MAC

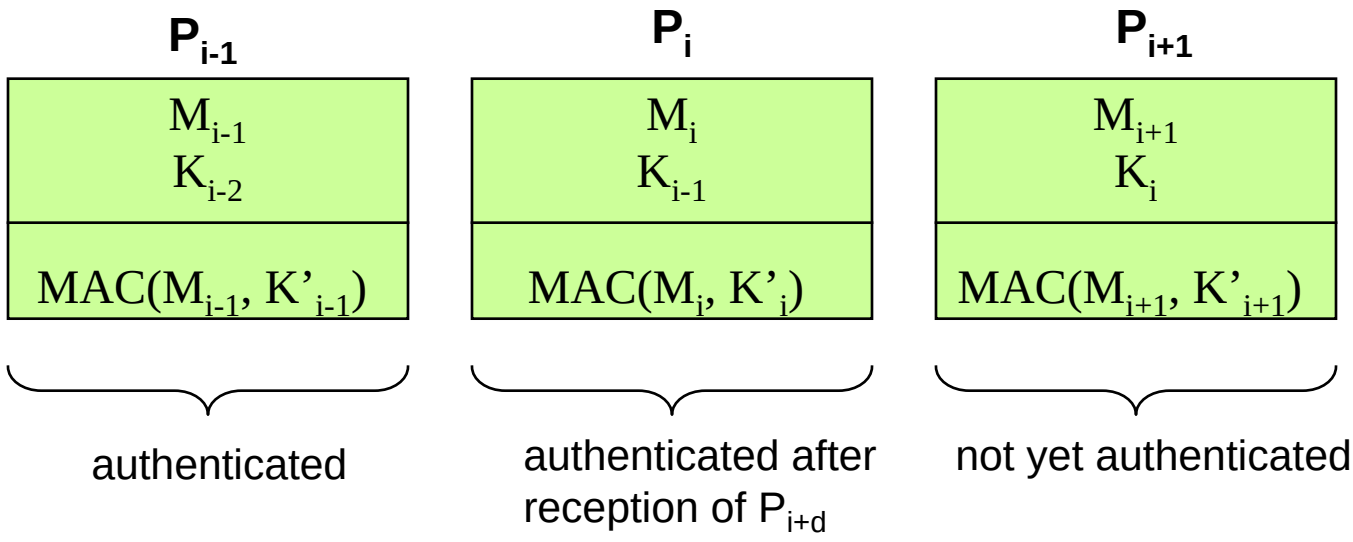


TESLA – Sender



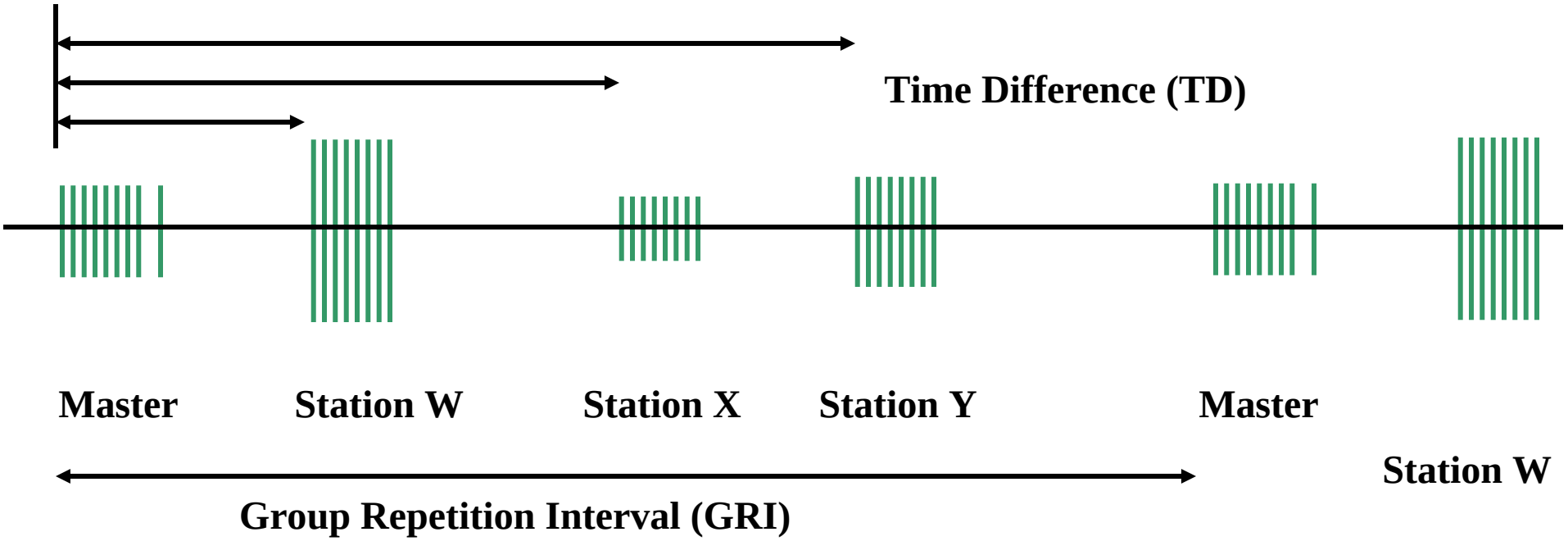
- Pre-compute a sequence of key values using one-way hash functions or pseudo-random functions. $K_n = F(K_{n-1}), \ldots, K_1 = F(K_2)$
- Use another hash function to compute K'. $K_i' = F'(K_i)$
- Generate MAC using K' and Message M
- Send packet P. $P_i = \langle M_i, K_{i-d}, MAC_i \rangle$

TESLA – Receiver



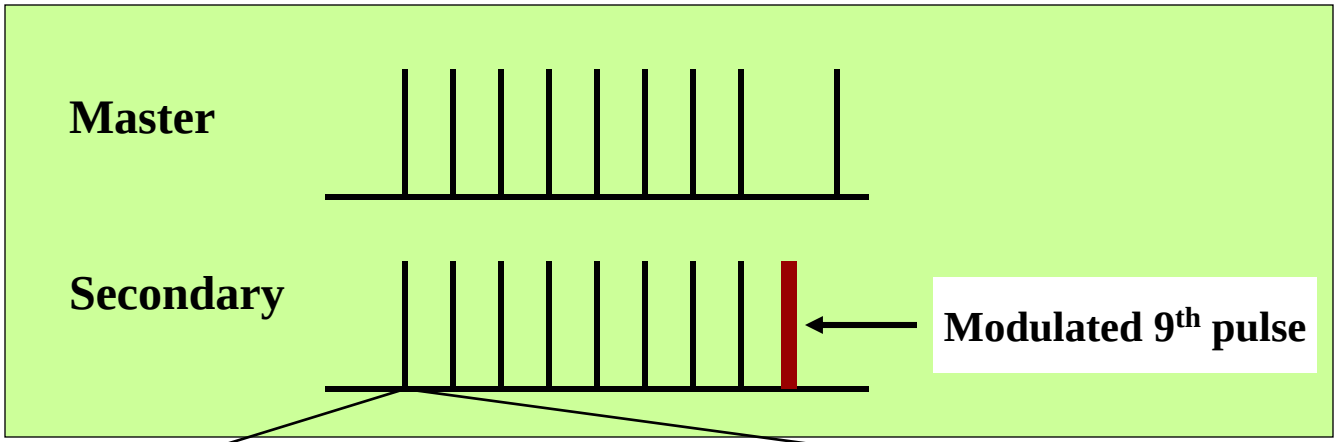
- **The receiver buffers the packet**
- **Each receiver also checks that the disclosed key is correct using self-authentication and previously released keys**
- **checks the correctness of the MAC of buffered packets that sent in the time interval of disclosed key**
- **If the MAC is correct, the receiver accepts the packet**
- **Message Sequence is arbitrary**

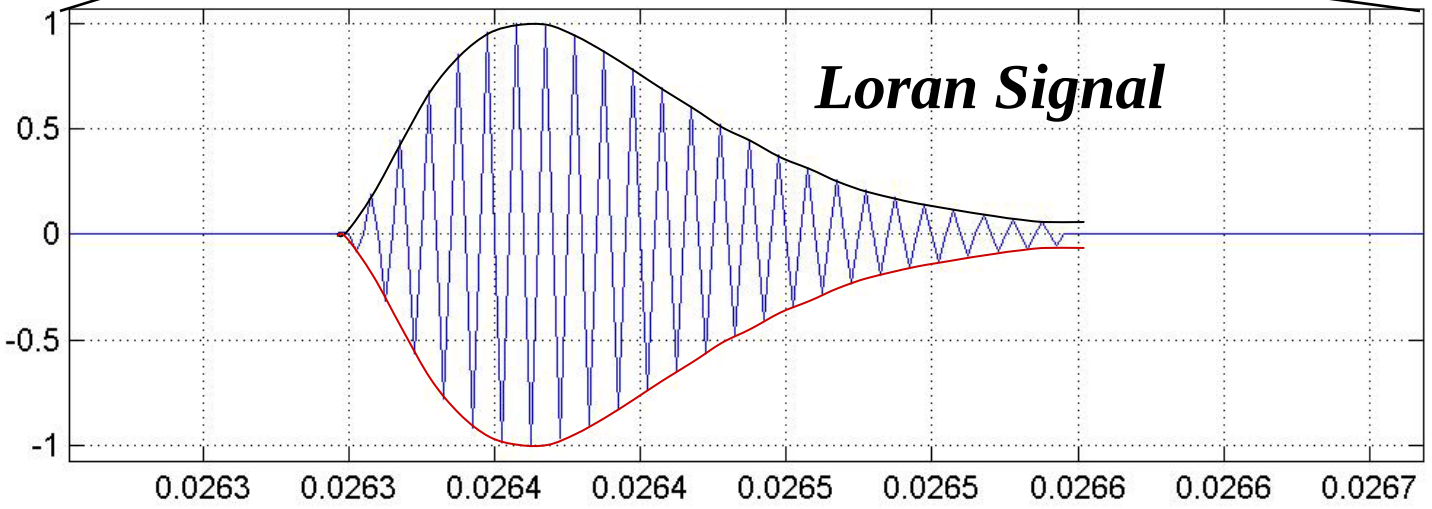
Loran Transmission



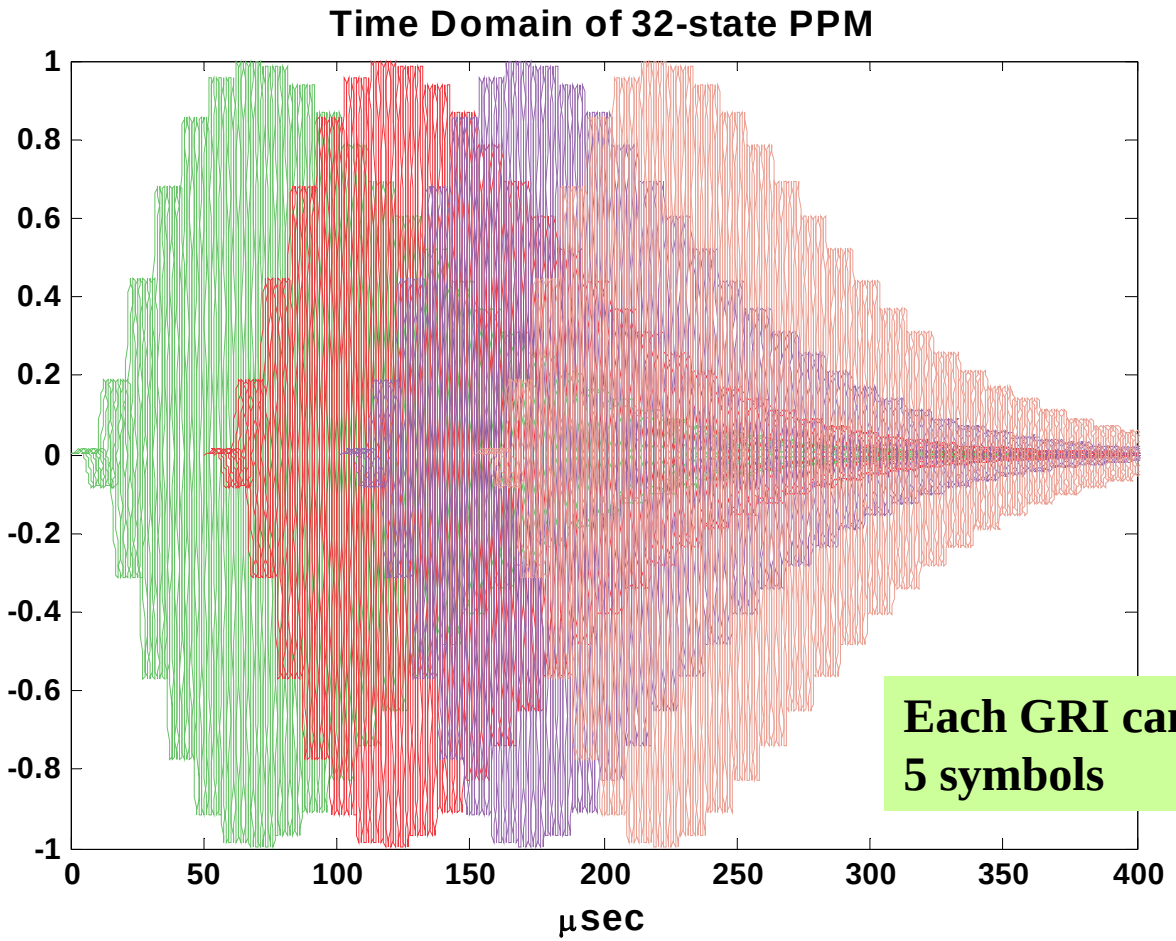
GRI range
40,000 ~ 99,990 μsec

Loran Data Channel Communication
-- Ninth-Pulse Modulation





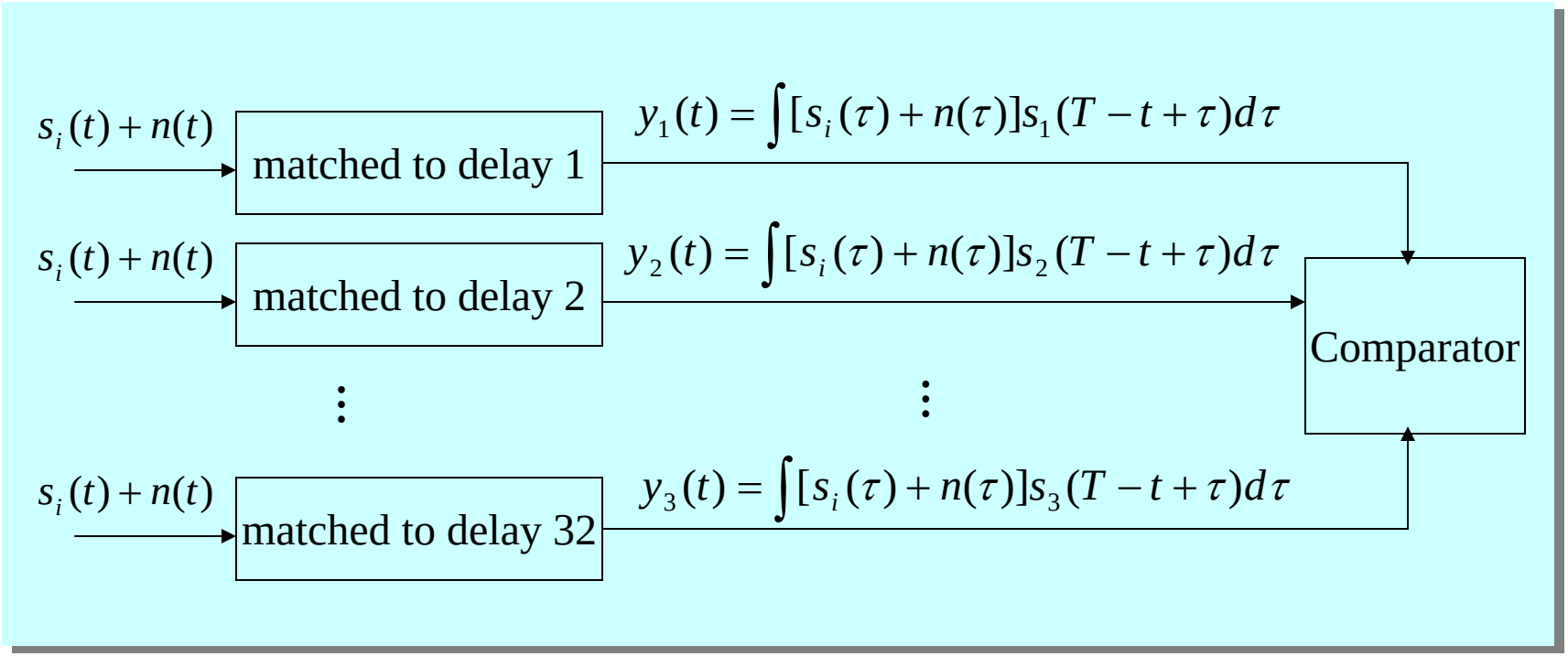
Loran Modulation Technique
-- Pulse Position Modulation



Each GRI can carry 5 symbols

Modulated Loran Pulse: $s_i(t) = (t - d_i)^2 e^{(\frac{-2(t-d_i)}{65})} \sin(0.2\pi * (t - d_i))$

Matched Filter Model

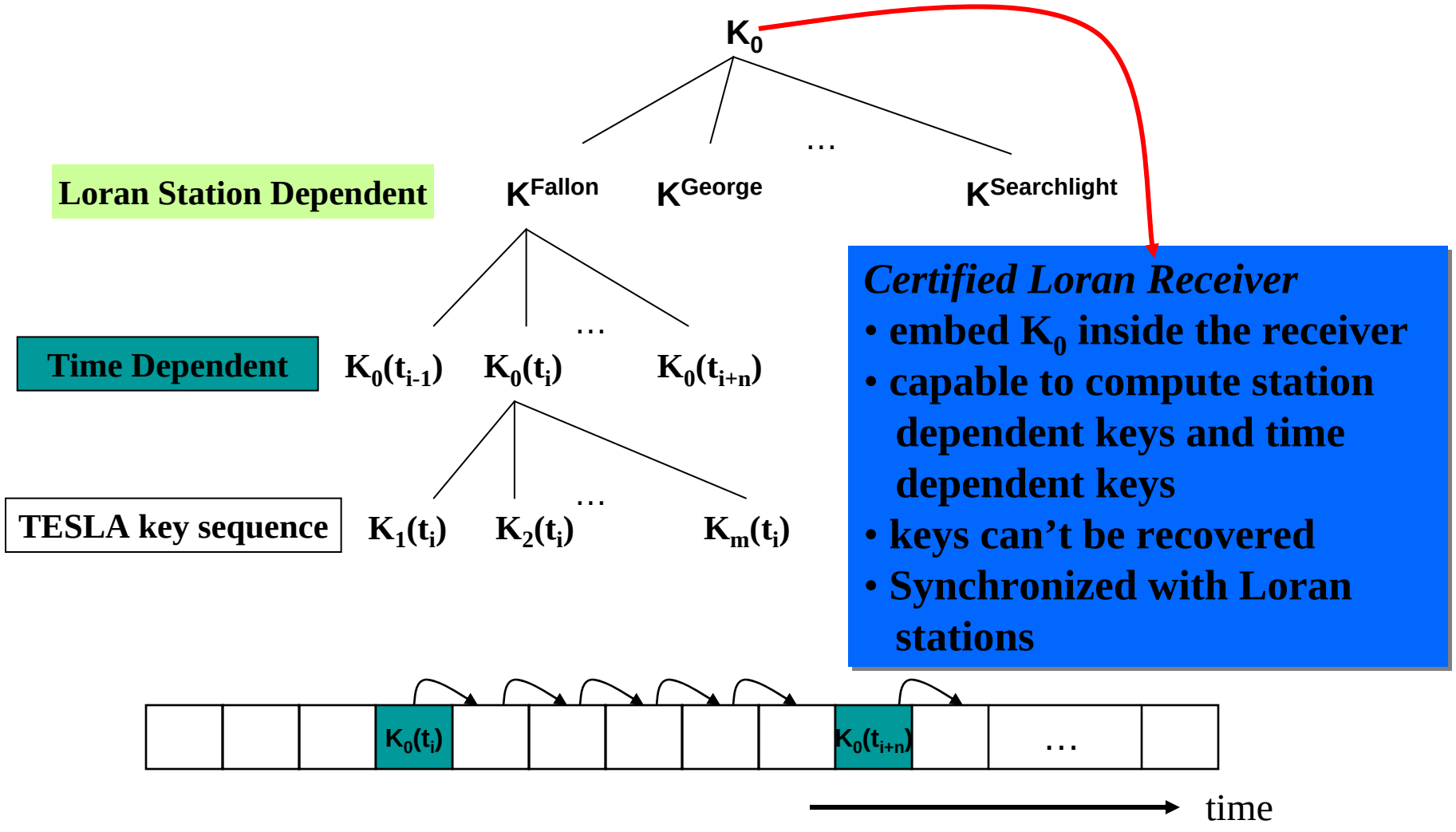


Loran Messages

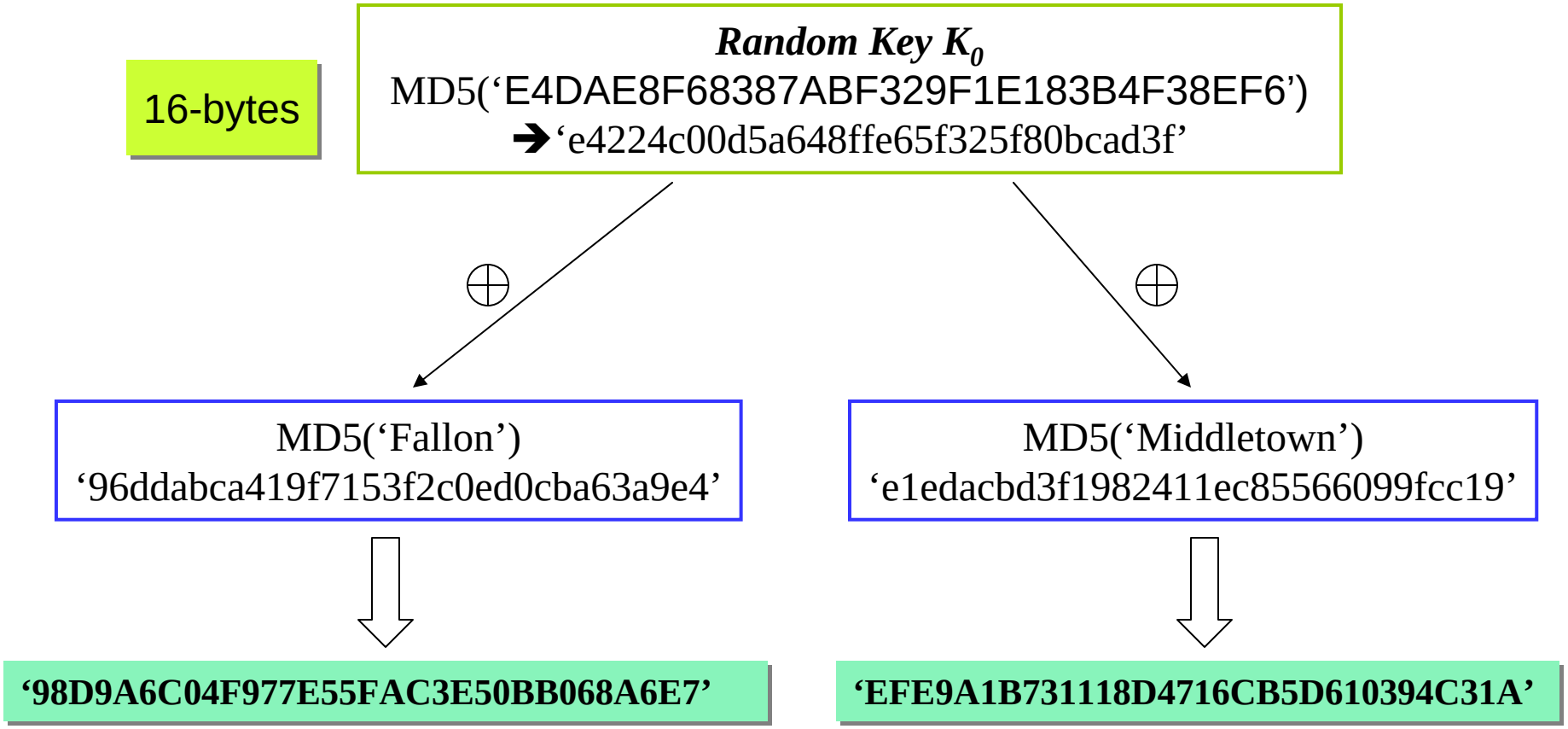
Section	Type	Payload	Parity
Length (bits)	4	41	75
Bit assignment	0…3	4…44	45…119

Type	Type code	Description
0	0000	Differential Phase Correction
1	0001	Almanac
2	0010	Message for government use only
3-14	0011 thru 1110	Undefined
15	1111	Time of day

How to Implement TESLA?

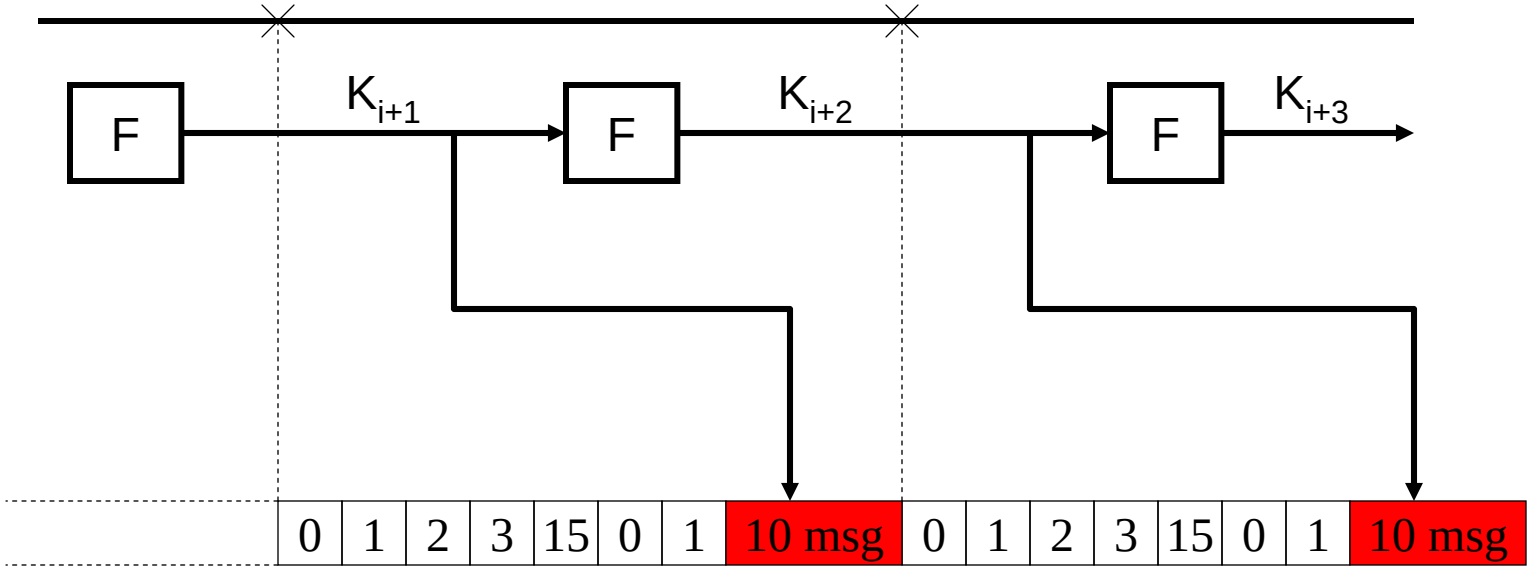


Station Dependent Keys Generation

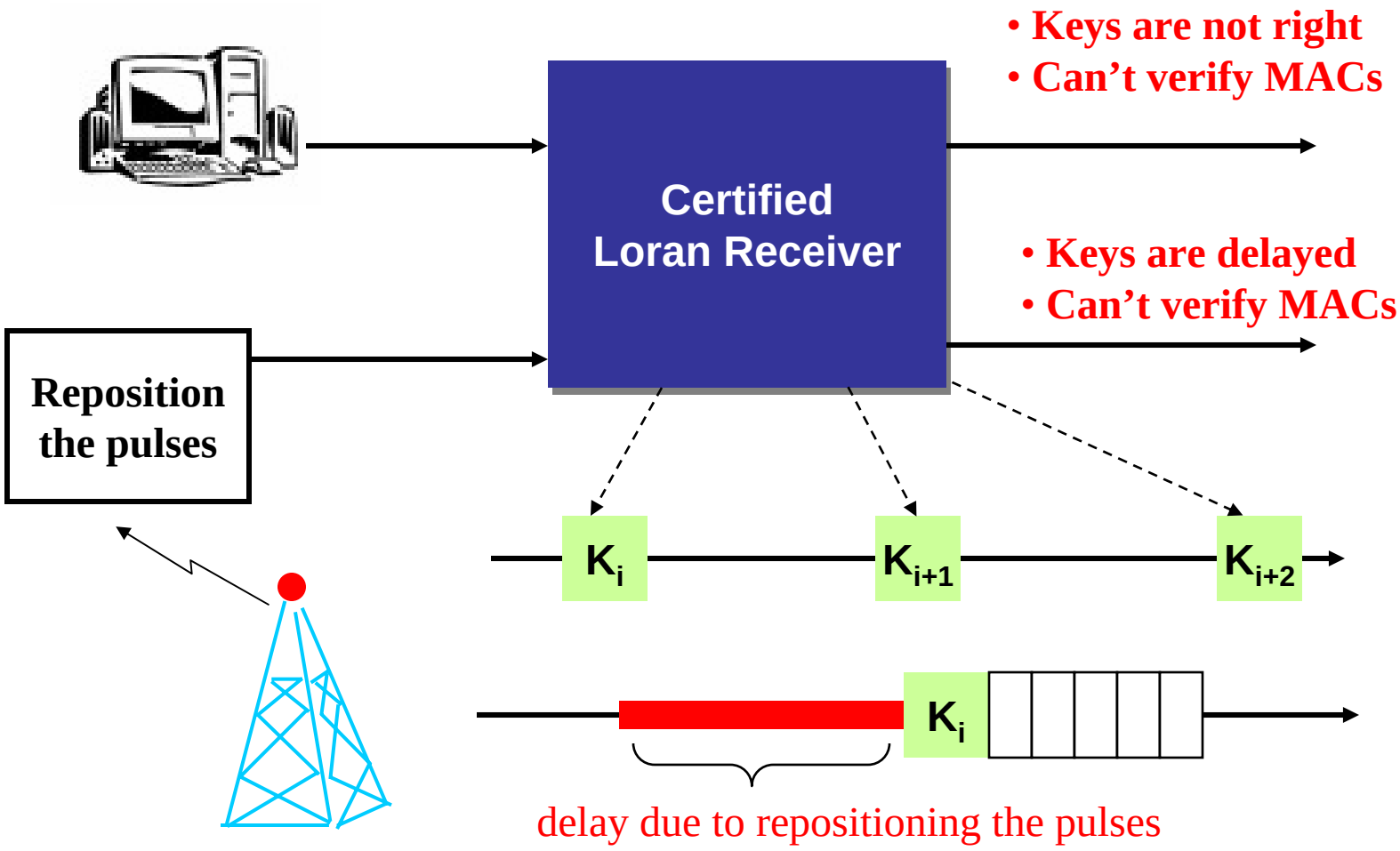


Proposed Authentication Scheme

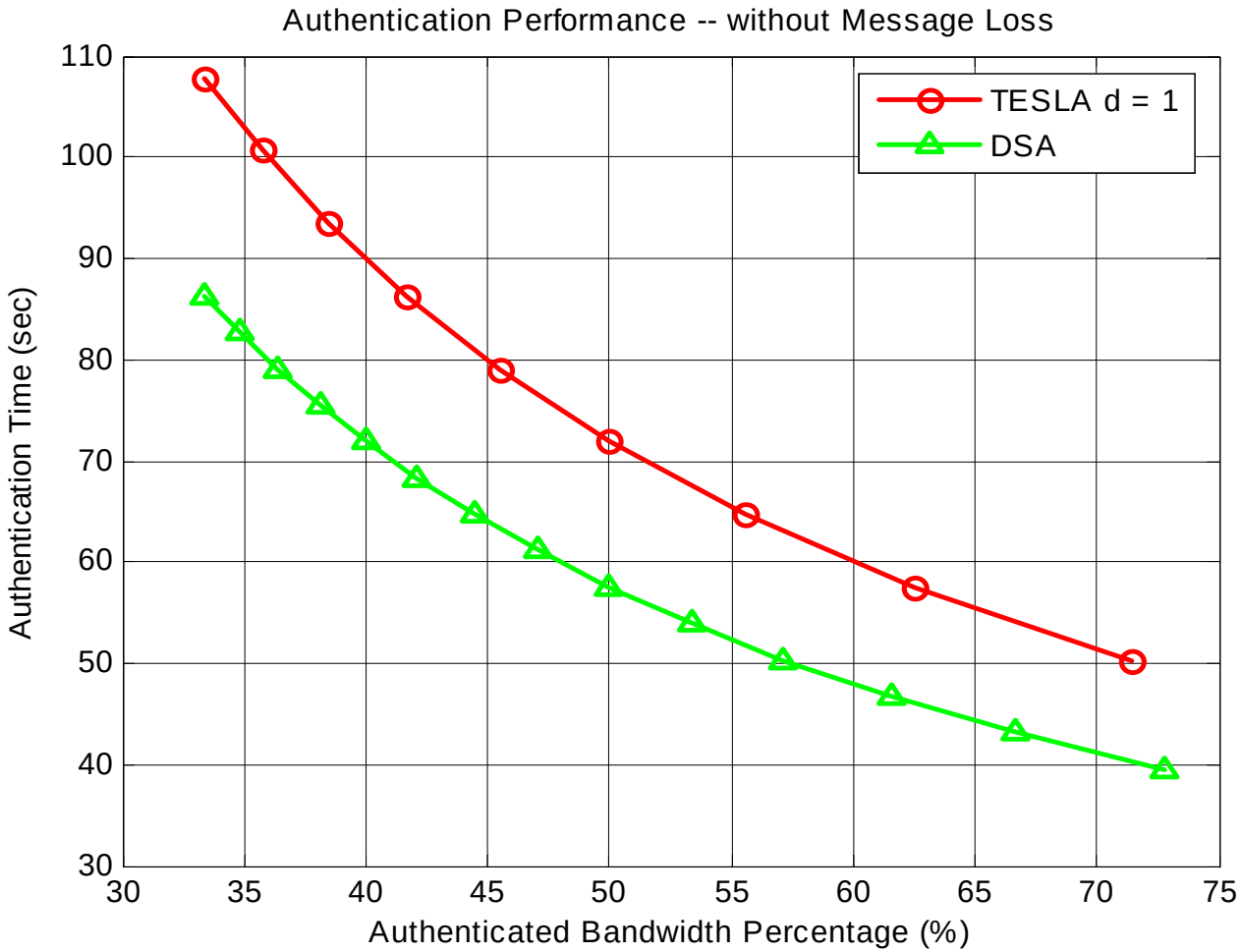
- SHA-256
- HMAC – 256-bit output, minimum key size 128 bits
- 384/41 ~ 10 messages/TESLA packet



How TESLA Enhances Security?



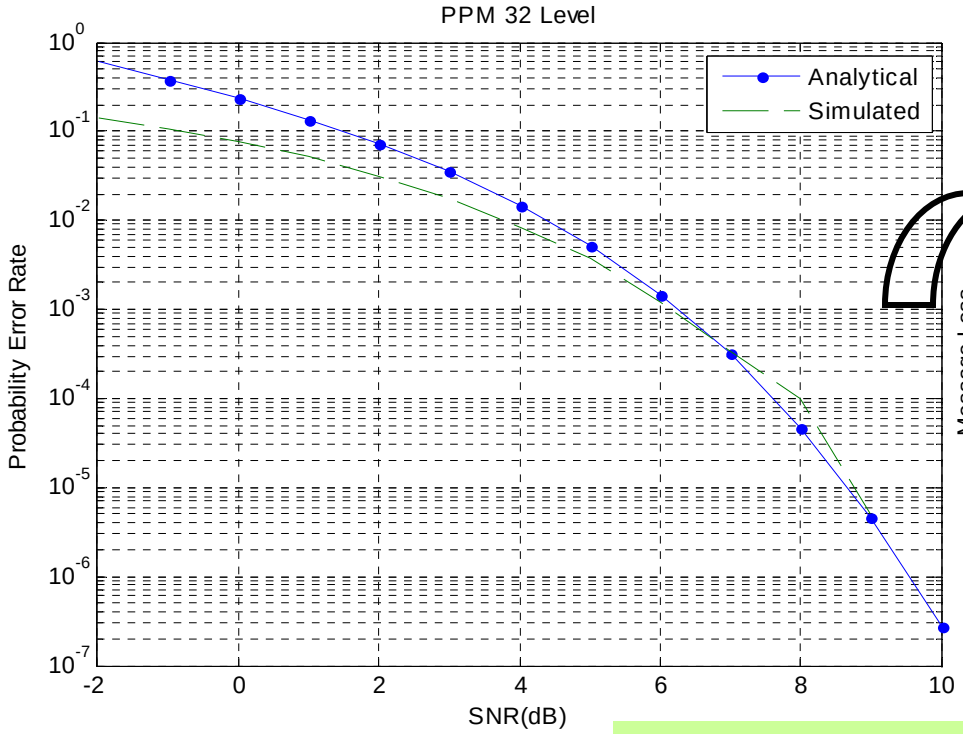
Time of Alarm



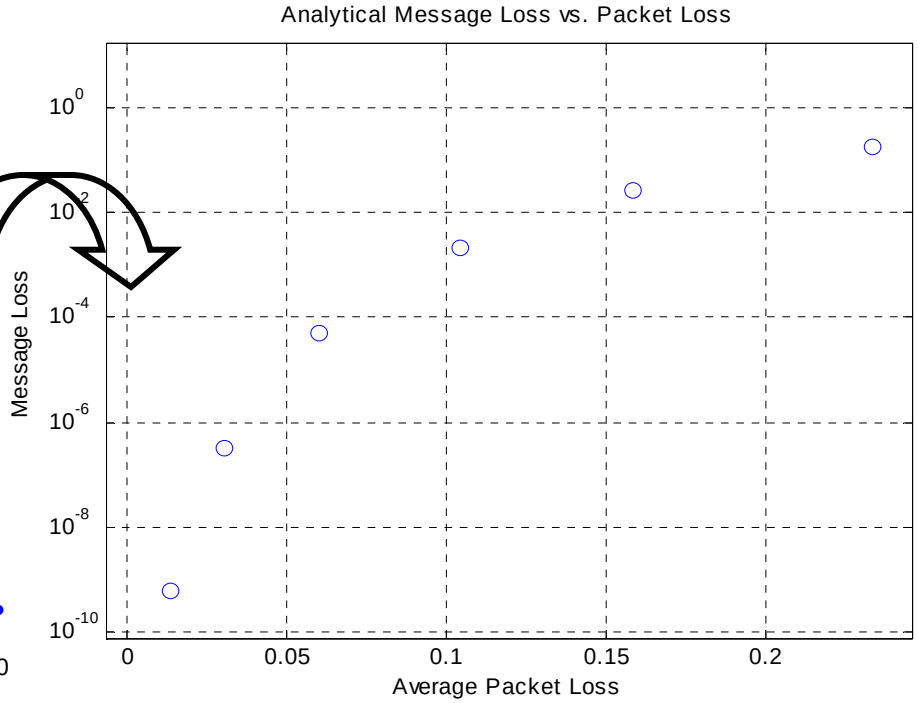
- consider GRI 9990
- DSA size > MAC size
- DSA verification has high computation overhead

TESLA Performance

PPM32 Probability of Symbol Error



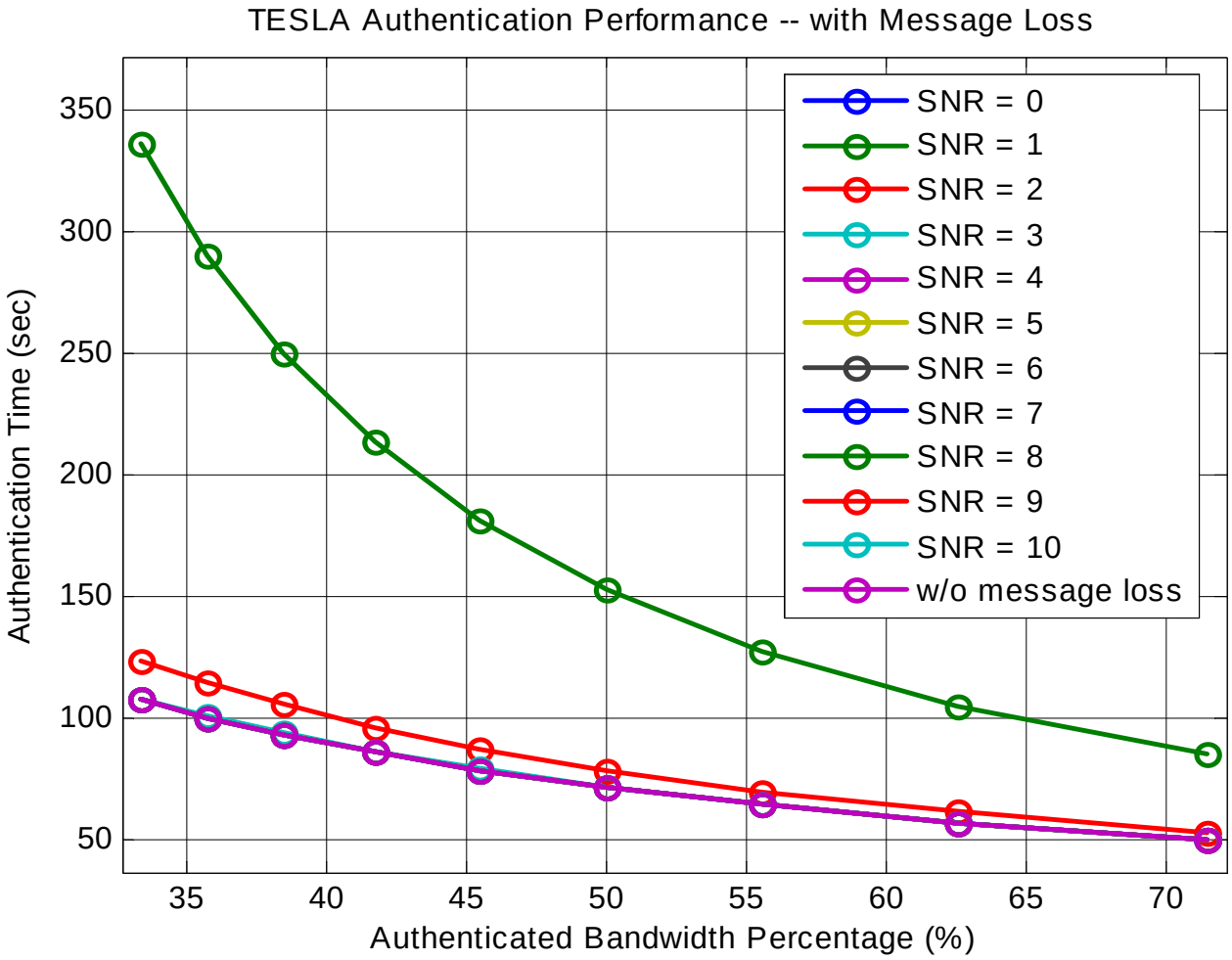
Message Loss



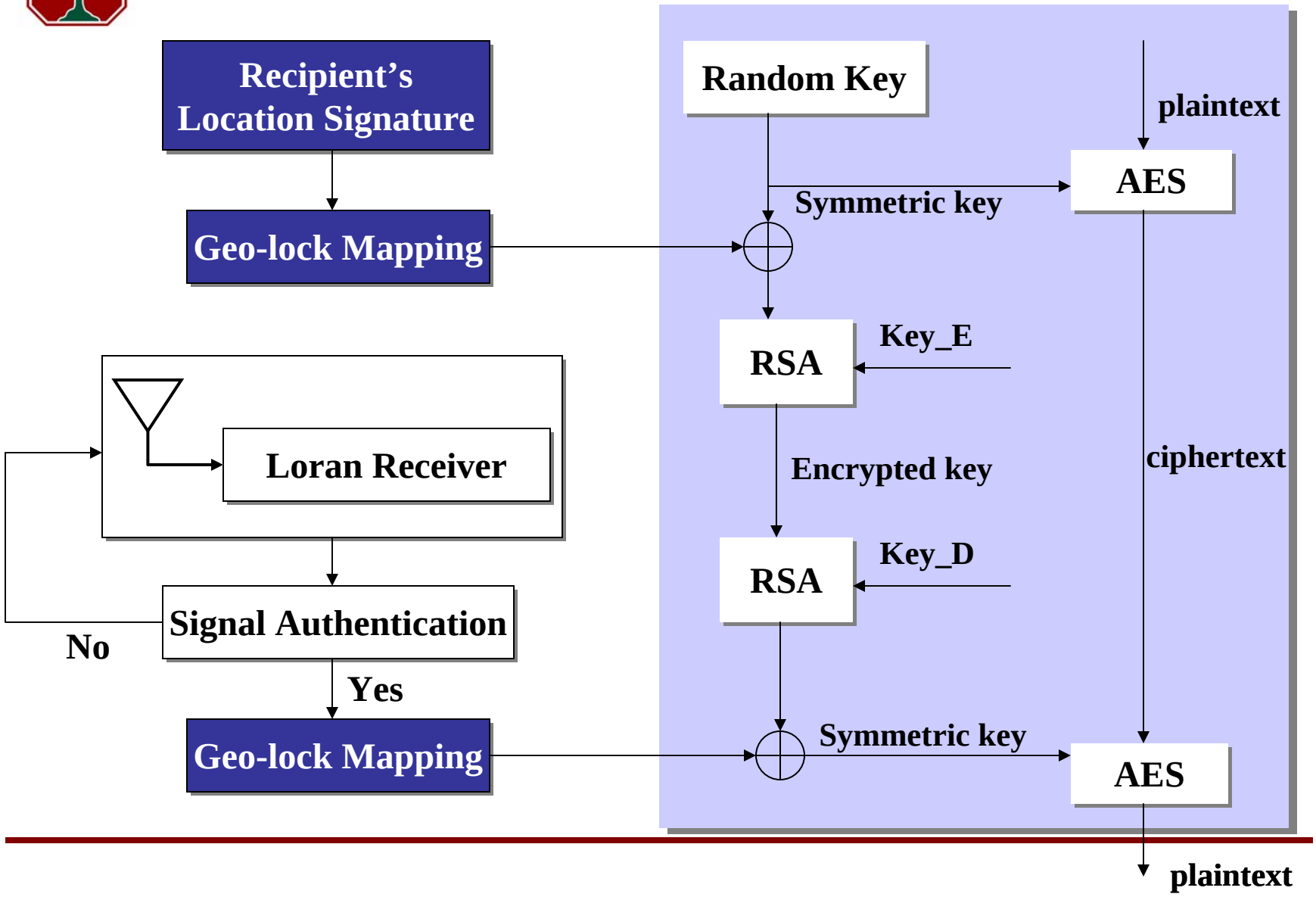
$$\Pr(error / decorder\_failure) = \sum_{j=t+1}^{n} \binom{n}{j} p^j (1-p)^{n-j}$$

$$P(undetected\_error)_{RS} = \frac{(q^k - 1)\sum_{j=0}^{t} \binom{n}{j} (q-1)^j}{q^n}$$

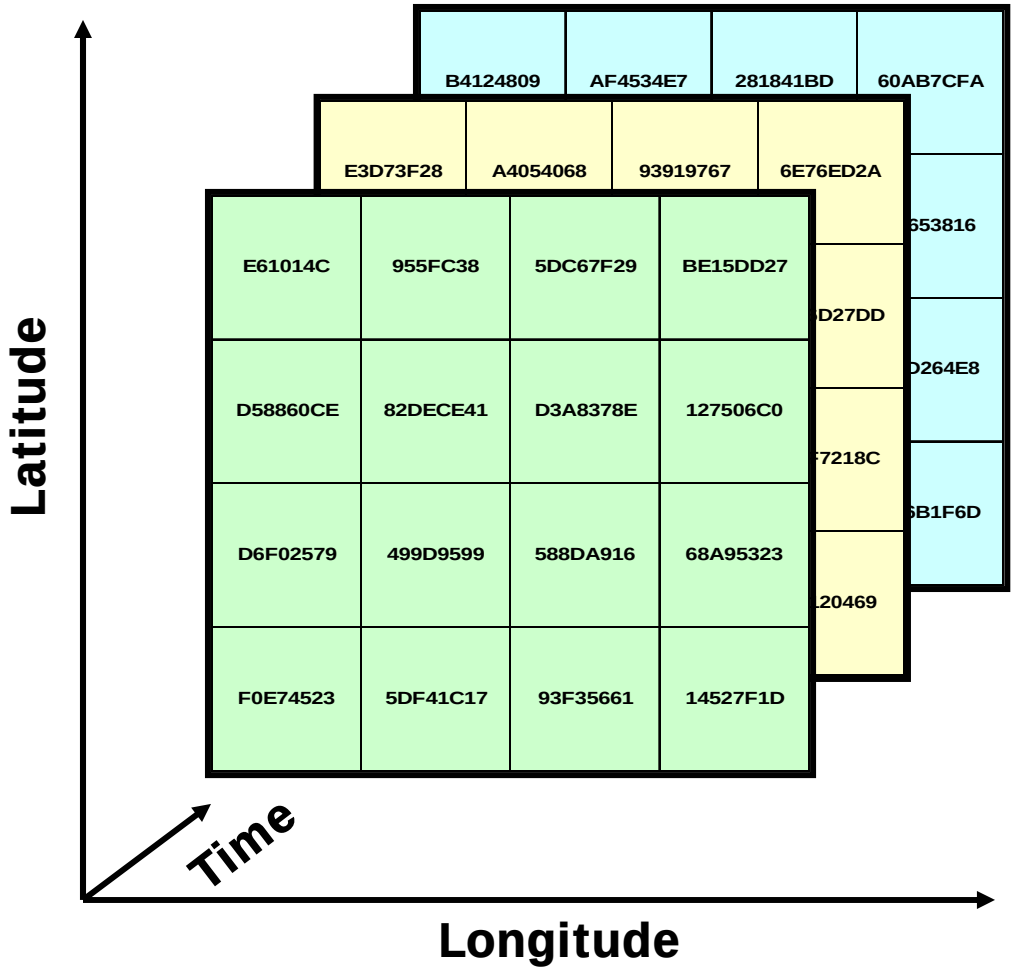
Time of Alarm with Message Loss



Next Step: Geo-lock Design



Geolock Mapping function



Possible Parameters

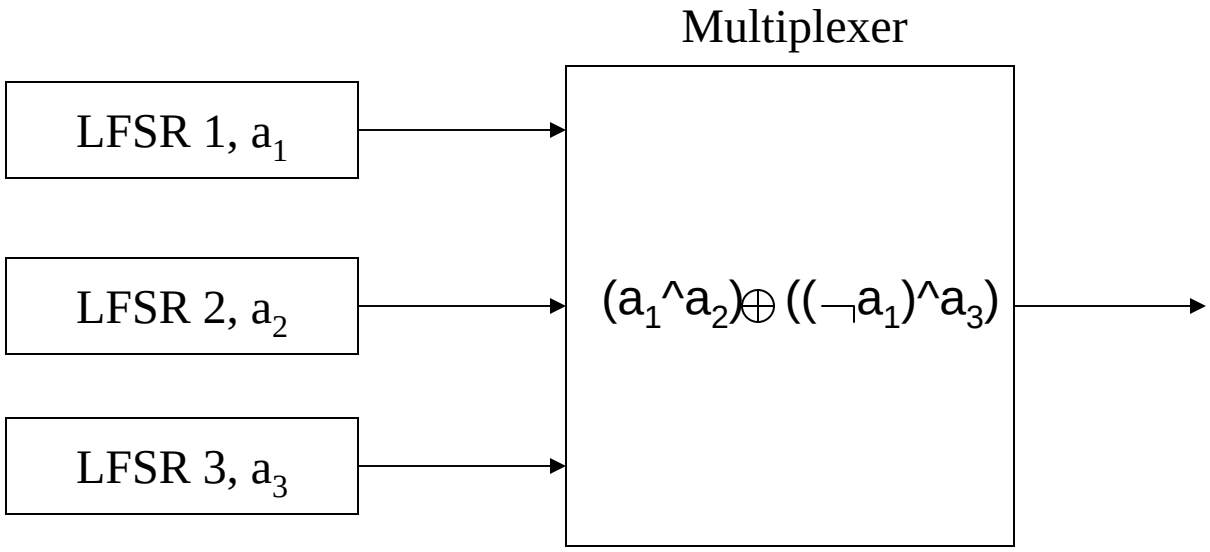
- ECD
- TD
- TDOA
- Envelope shape

Pseudo-random Sequence

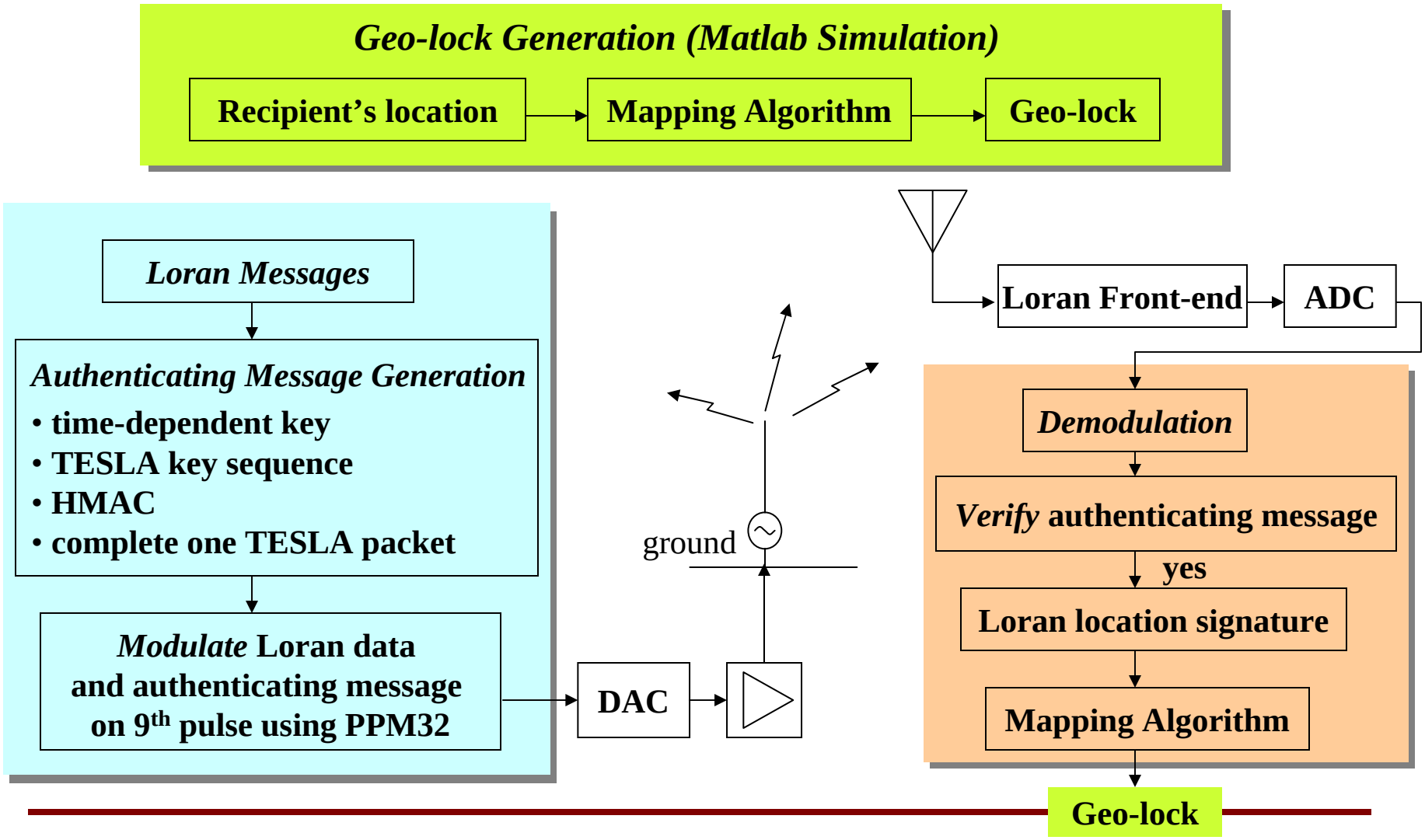
Requirement	Application area
Good auto-correlation	Range and navigation Spread spectrum communications Scrambling
Good cross-correlation	Spread spectrum communications Navigation System test and analysis
Linear complexity	cryptology

Keystream Generator

Geffe generator: a keystream generator using three LFSRs, combined in a nonlinear manner.



Steps to Build a Testbed

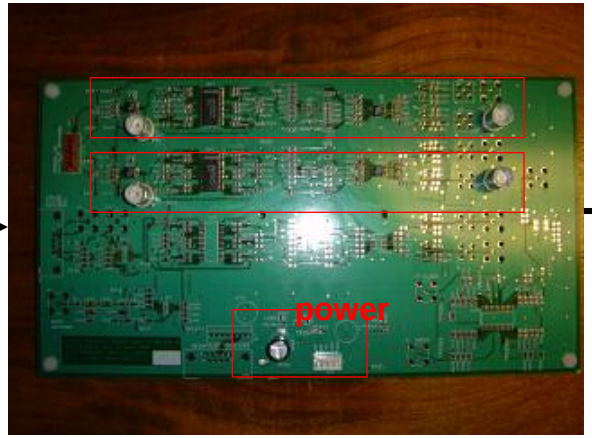


Testbed Setup

Modulated Loran Signal (MATLAB simulation)

ICS-660

Loran H-field antenna



ICS-652/
ICS-650

Thank You!