Proximity Verification for Contactless Access Control and Authentication Systems

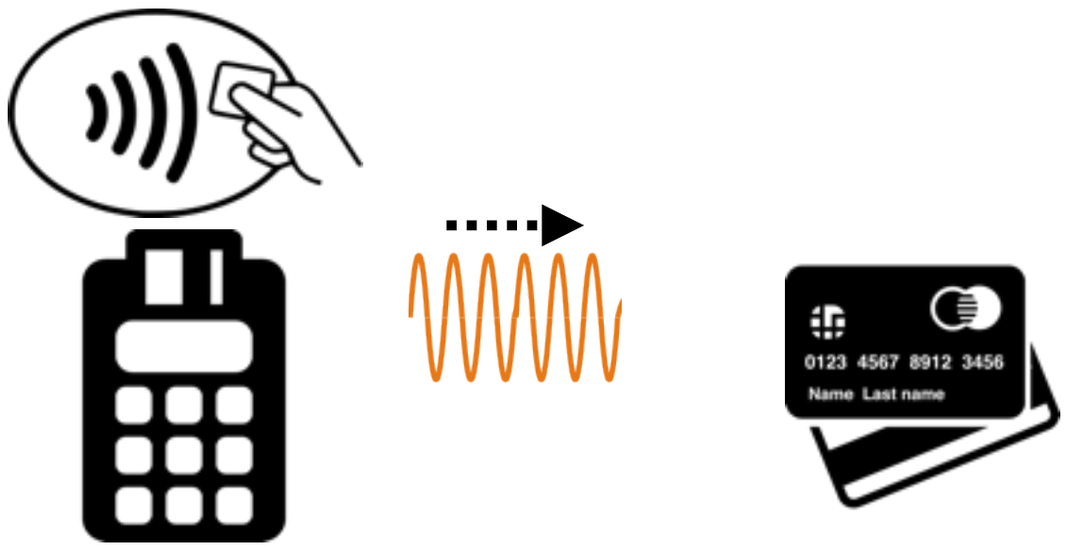
Aanjhan Ranganathan (ETH Zurich)
Boris Danev (3dB Access AG)
Srdjan Capkun (ETH Zurich)

Contactless Systems

Contactless Systems

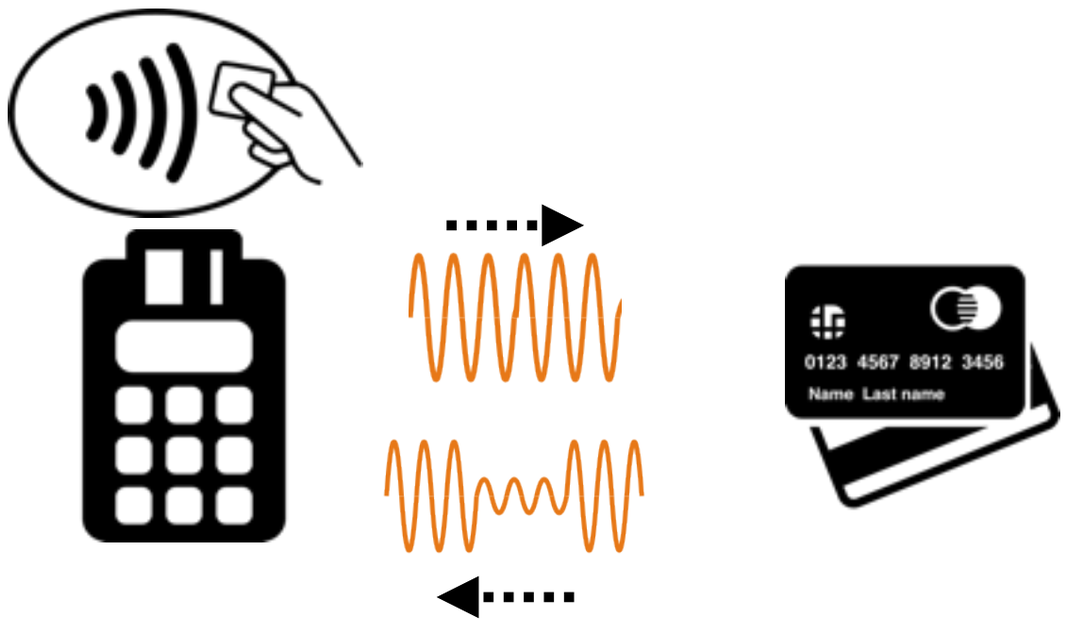
- Uses RFID technology to exchange information
- The card is fully passive i.e., no power supply of its own
- Designed for short-range applications

Contactless Systems



- Uses RFID technology to exchange information
- The card is fully passive i.e., no power supply of its own
- Designed for short-range applications

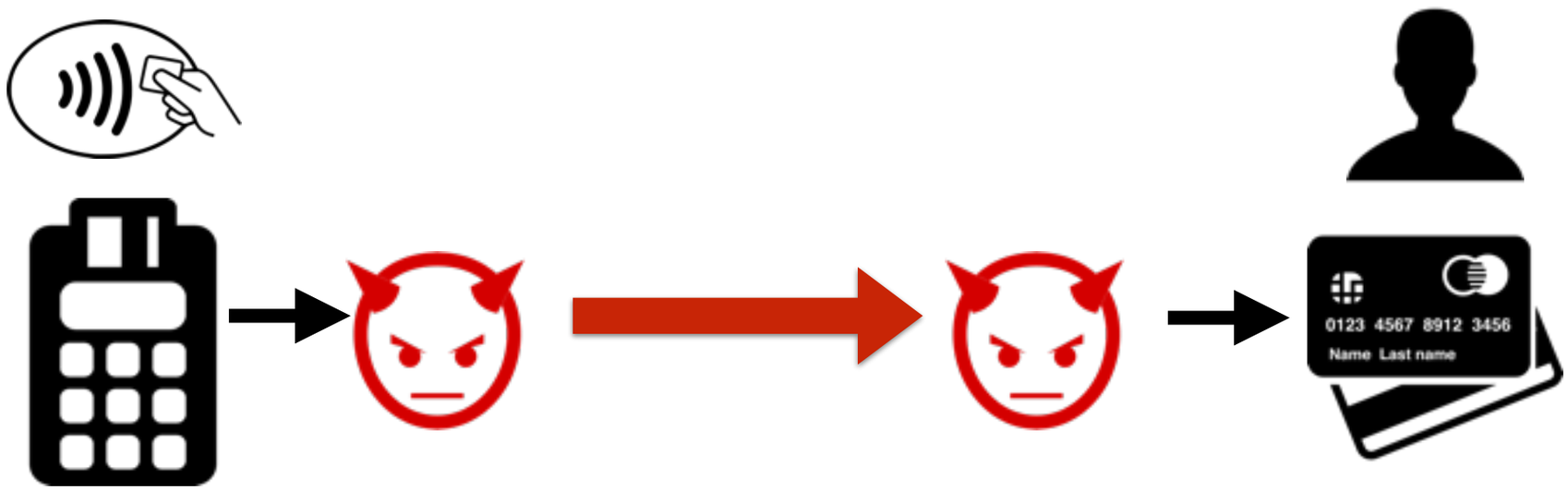
Contactless Systems



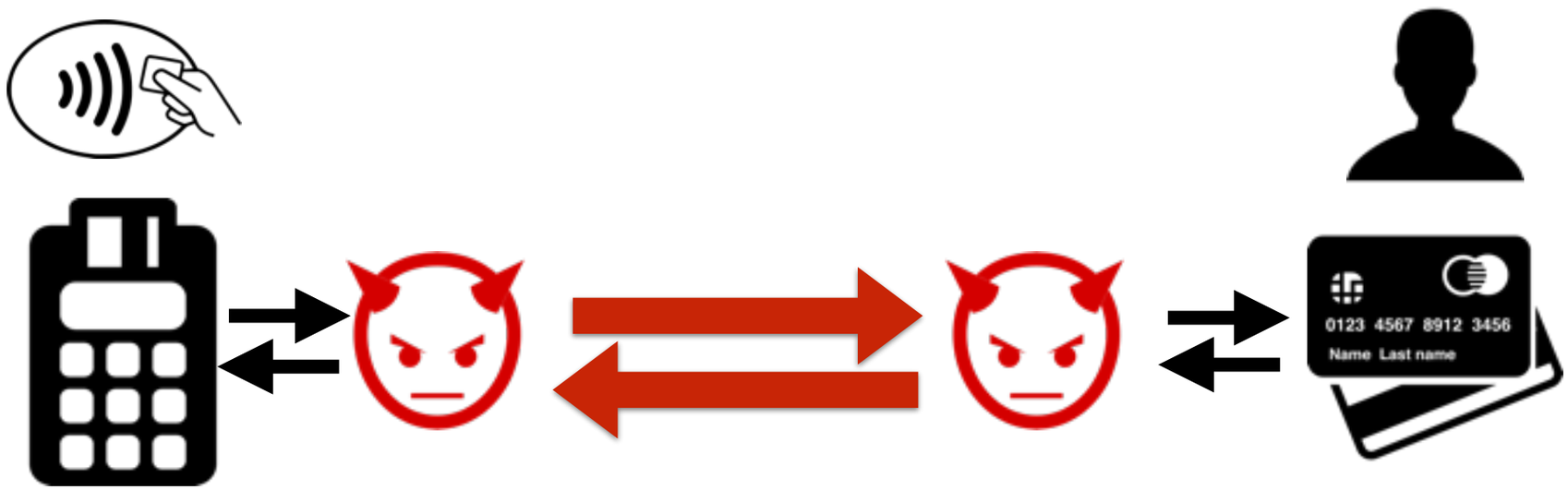
- Uses RFID technology to exchange information
- The card is fully passive i.e., no power supply of its own
- Designed for short-range applications

Relay Attacks

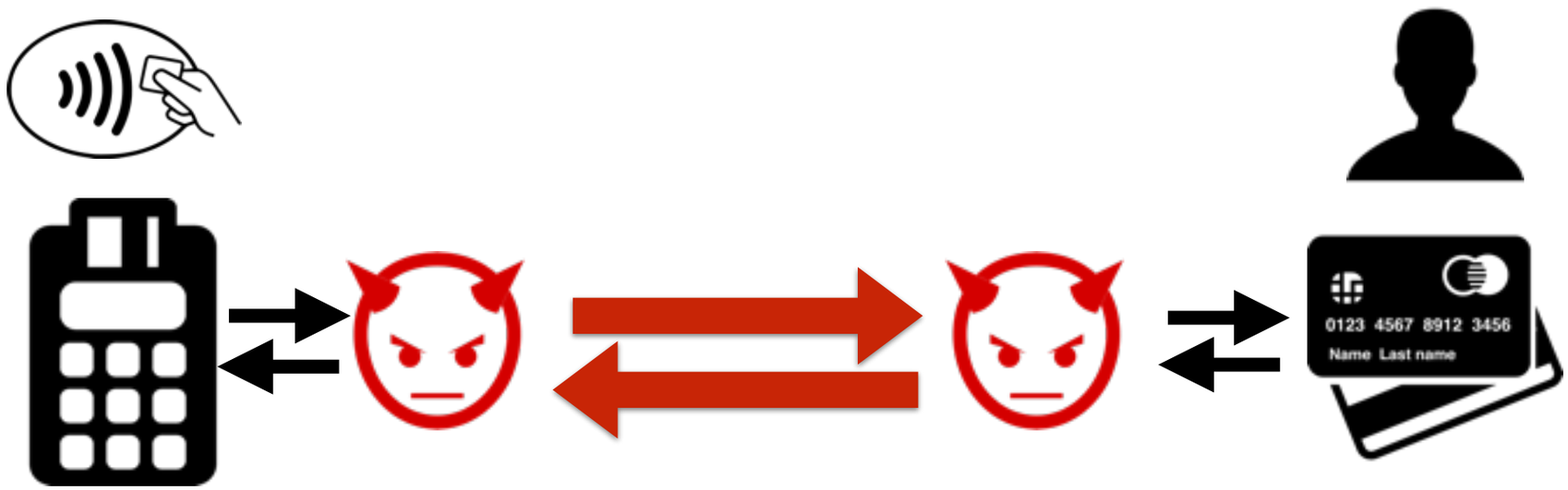
Relay Attacks



Relay Attacks

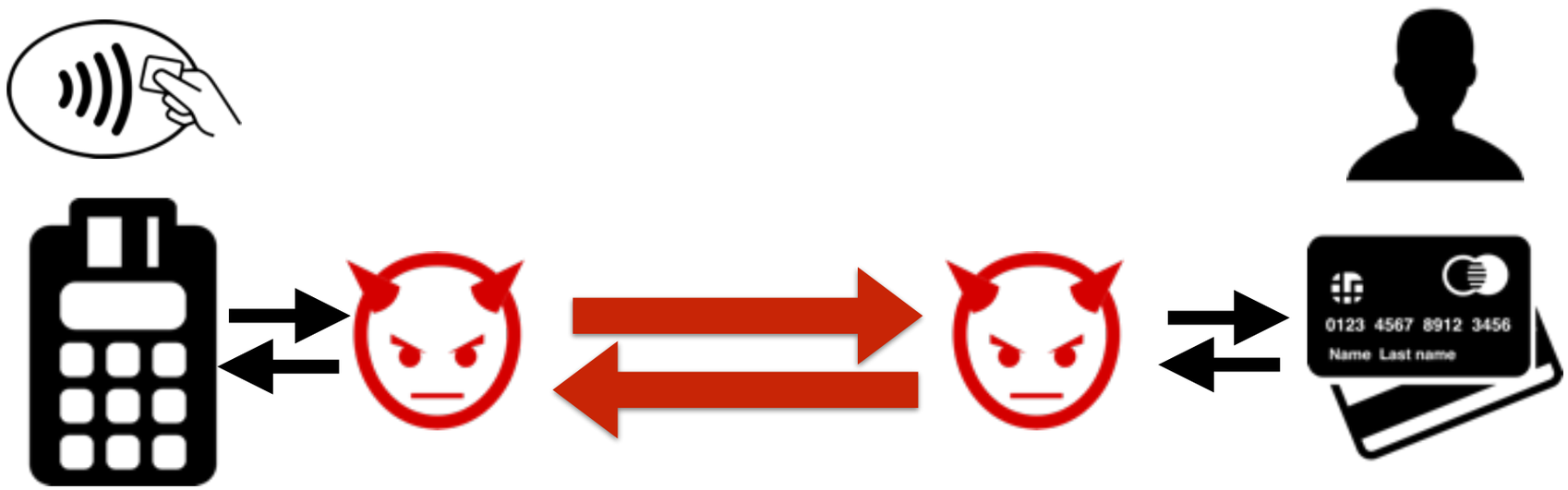


Relay Attacks



- Physical layer attack and therefore independent of any higher layer crypto

Relay Attacks



- Physical layer attack and therefore independent of any higher layer crypto
- Several practical attacks demonstrated (e.g., automobile entry systems* and Google Wallet^)

* Francillon et al. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars." *NDSS* 2011.
^ Roland et al. "Applying relay attacks to Google Wallet." *IEEE NFC Workshop 2013.*

Relay Attacks

Secure proximity verification is required to prevent such relay attacks

- Phy … any higher layer crypto
- Several practical attacks demonstrated (e.g., automobile entry systems* and Google Wallet^)

* Francillon et al. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars." *NDSS* 2011.
^ Roland et al. "Applying relay attacks to Google Wallet." *IEEE NFC Workshop 2013.*

Distance Bounding

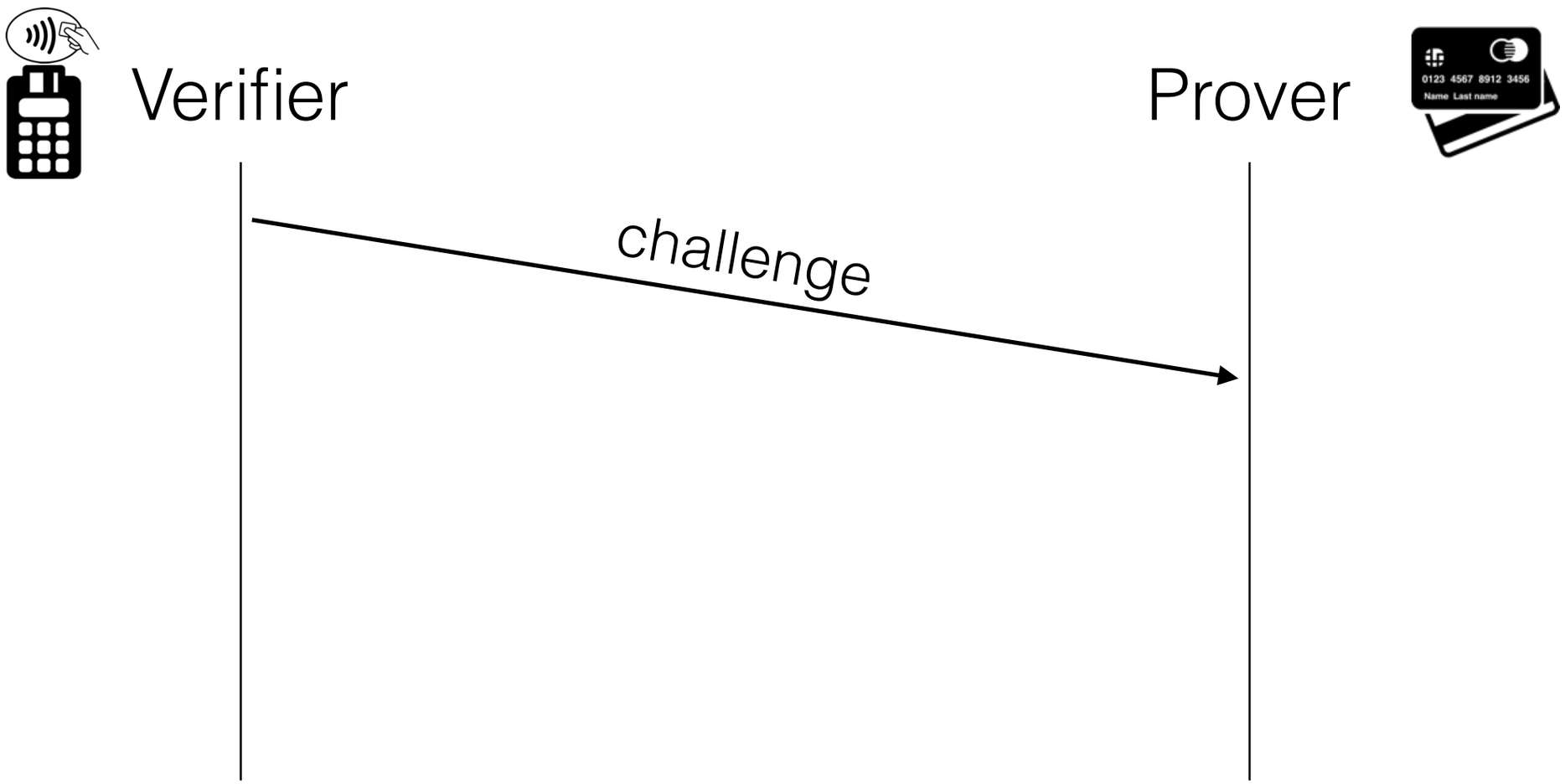
Guarantees an upper bound on the distance between two entities: a verifier and a prover

Verifier

Prover

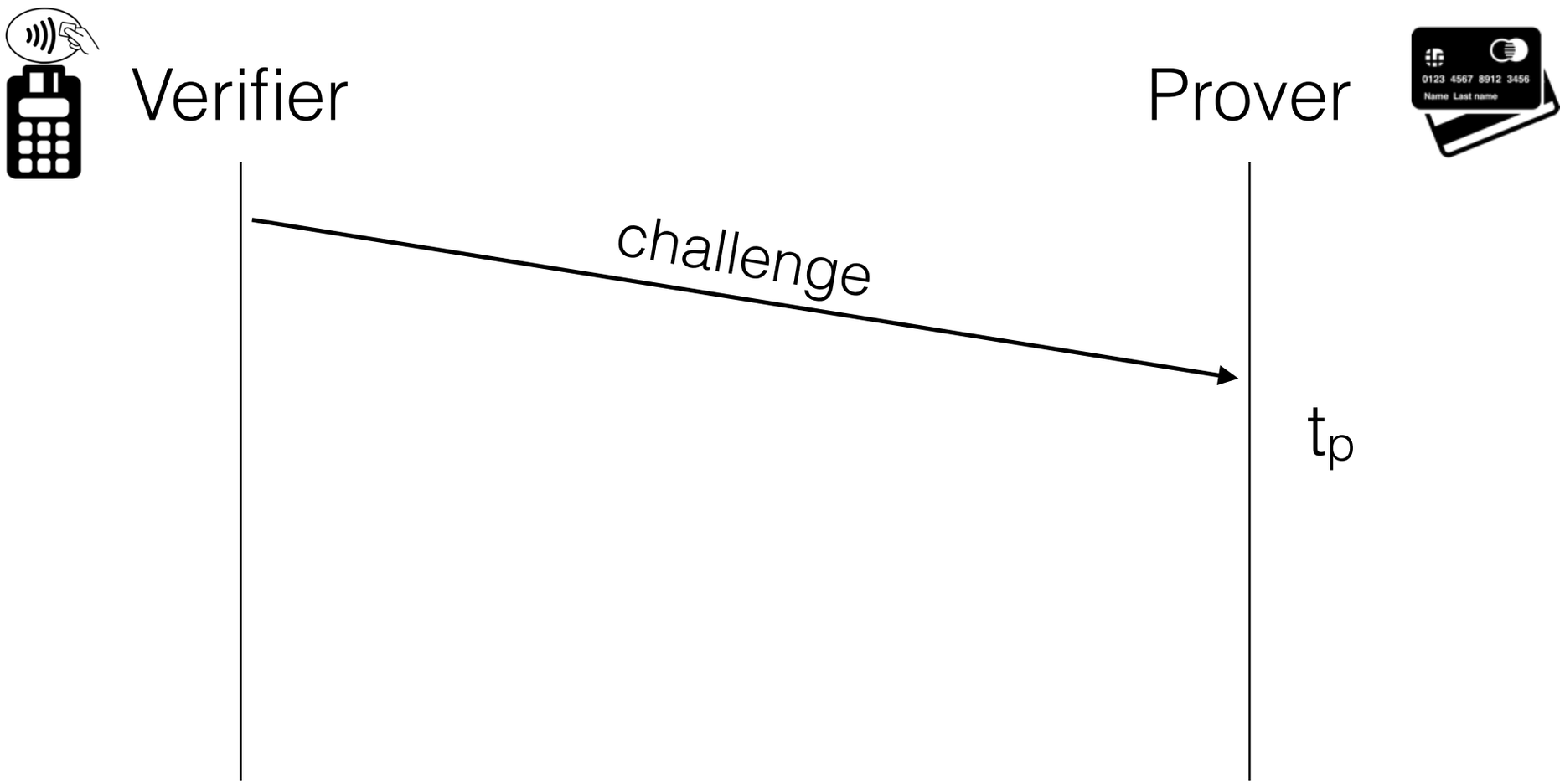
Distance Bounding

Guarantees an upper bound on the distance between two entities: a verifier and a prover



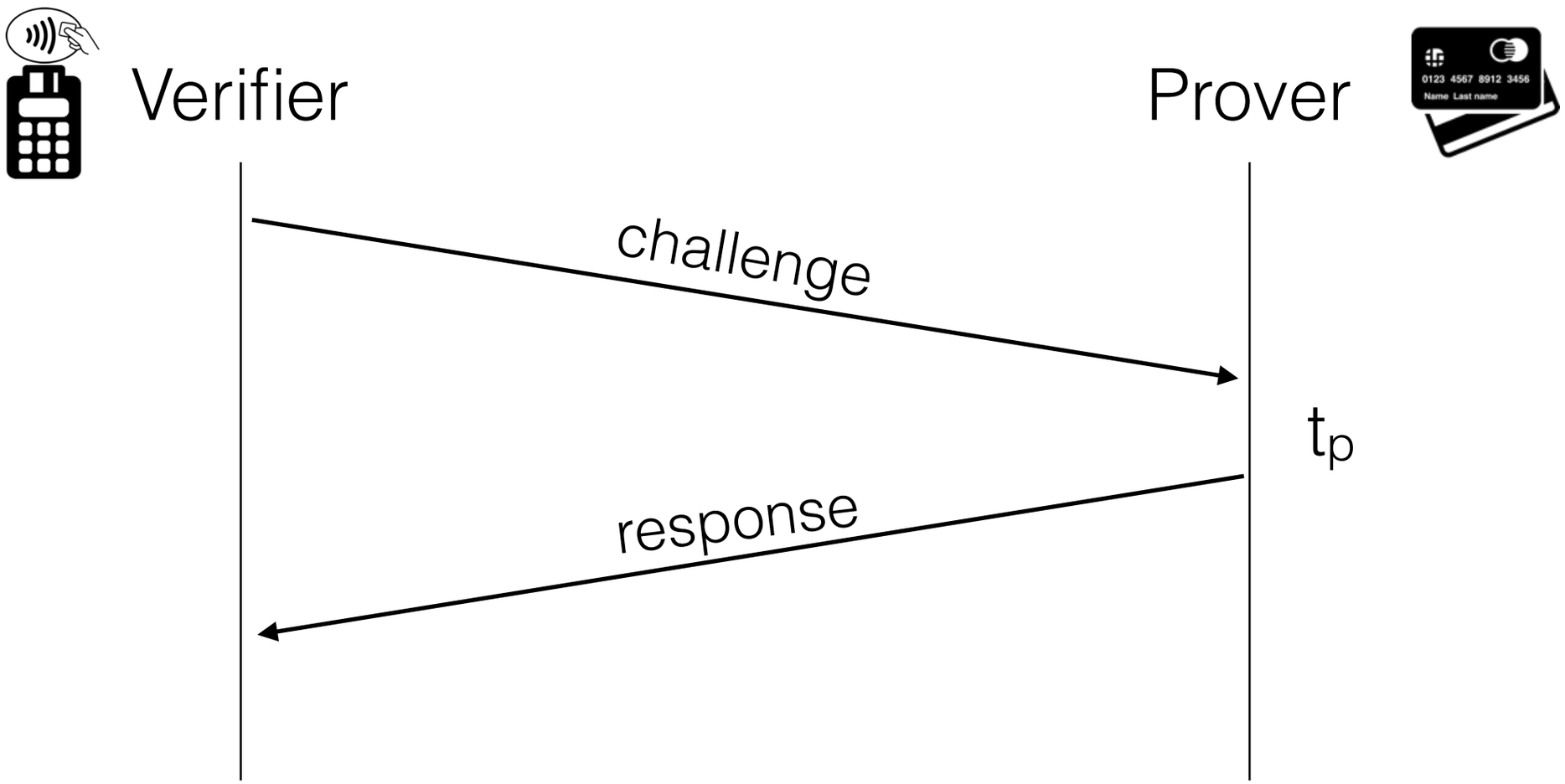
Distance Bounding

Guarantees an upper bound on the distance between two entities: a verifier and a prover



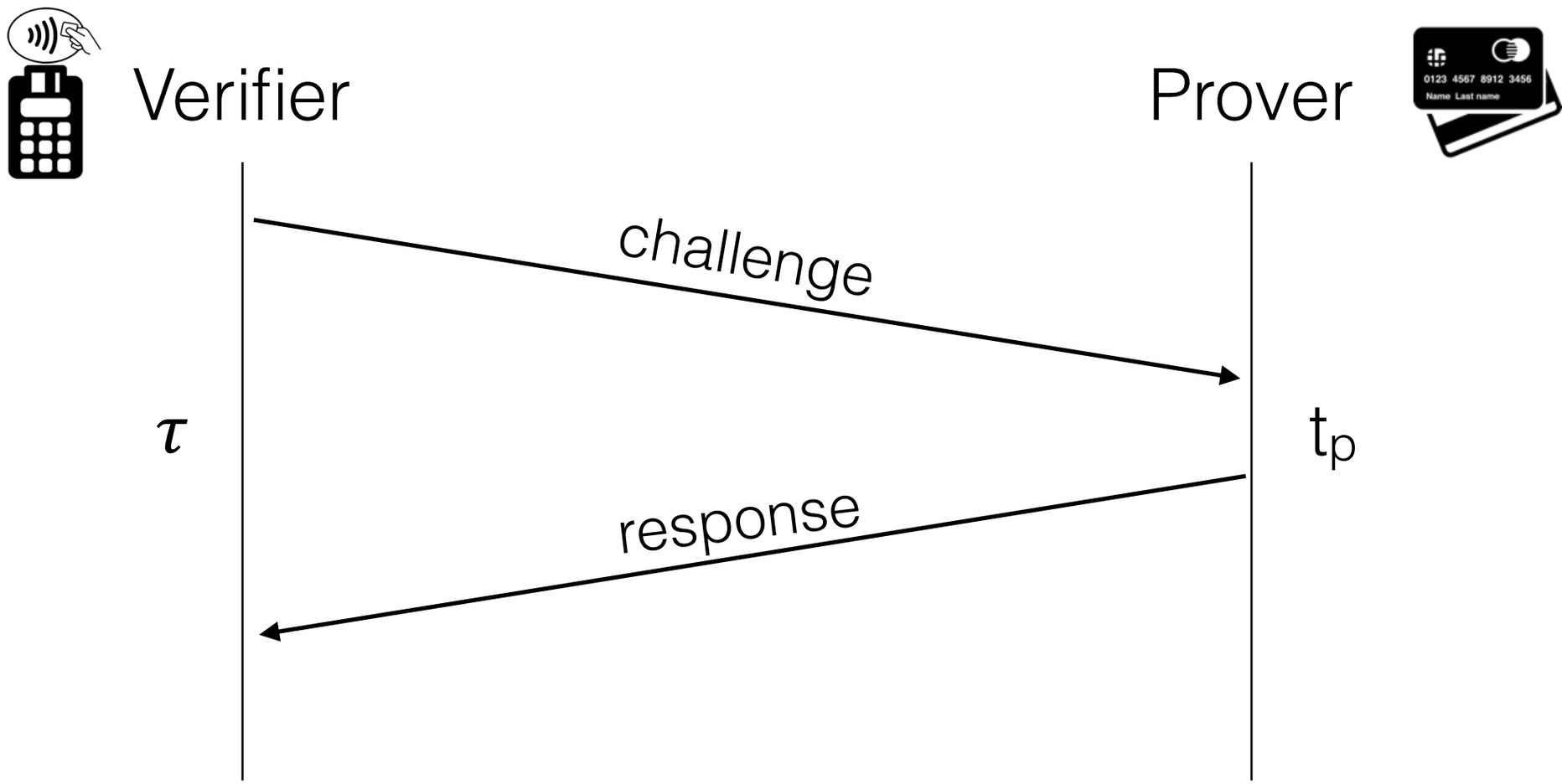
Distance Bounding

Guarantees an upper bound on the distance between two entities: a verifier and a prover



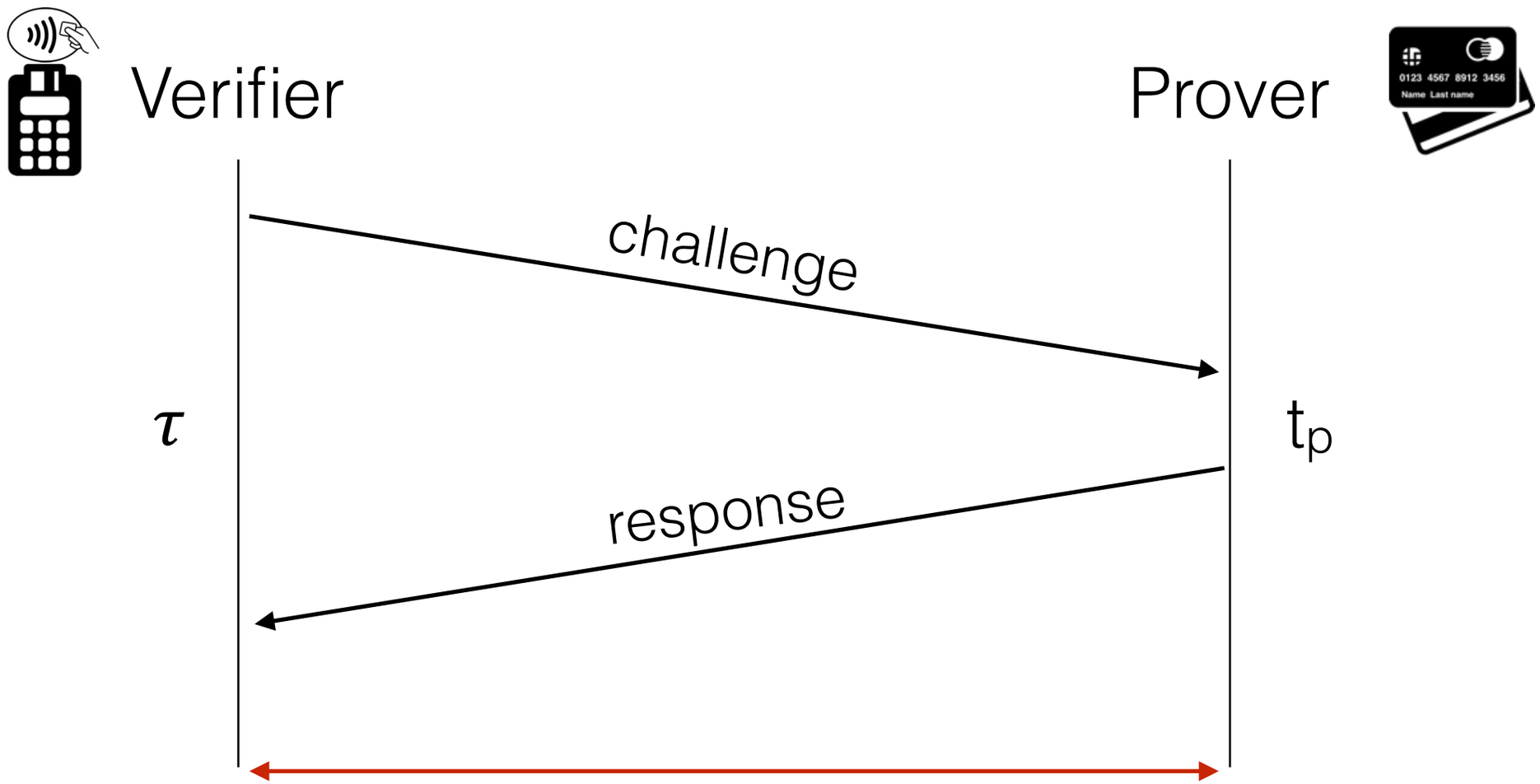
Distance Bounding

Guarantees an upper bound on the distance between two entities: a verifier and a prover



Distance Bounding

Guarantees an upper bound on the distance between two entities: a verifier and a prover



$$d = c * (\tau - t_p) / 2$$

Design Requirements

- Fully passive prover design
  - All current distance bounding implementations* use active provers
- Suitable for use in short range applications

* Ranganathan et al. "Design and Implementation of Terrorist Fraud resilient DB System" *ESORICS* 2012.
* Tippenhauer et al. "UWB Rapid-Bit-Exchange System for Distance Bounding". *WiSec 2015*
* Rasmussen et al. "Realization of RF Distance Bounding", USENIX 2010

Our Contribution

Our Contribution

- A first step towards realizing a secure proximity verification system in which the prover can be fully-passive

Our Contribution

- A first step towards realizing a secure proximity verification system in which the prover can be fully-passive
- Specifically designed for short-range contactless systems

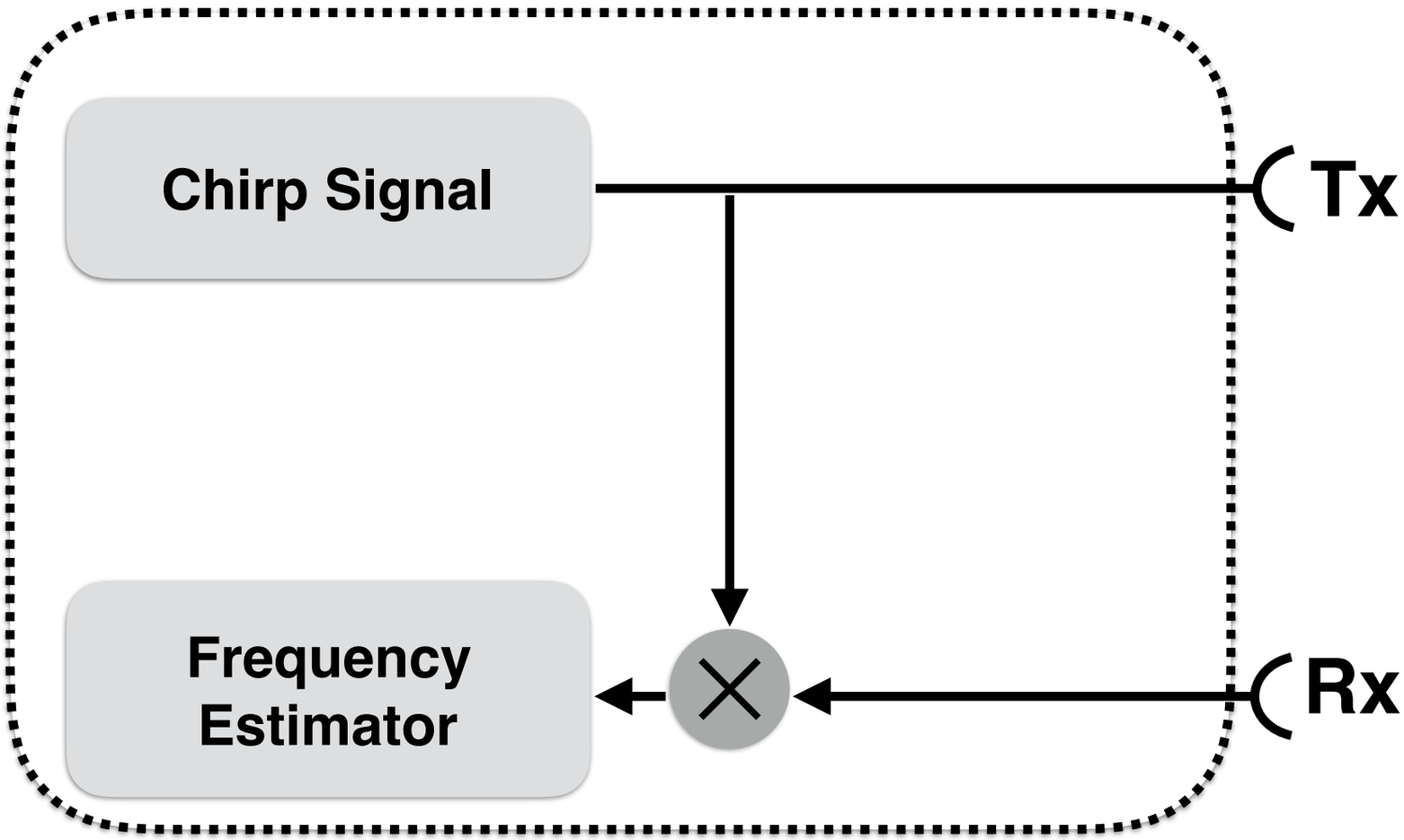
Our Contribution

- A first step towards realizing a secure proximity verification system in which the prover can be fully-passive
- Specifically designed for short-range contactless systems
- Our system is resilient against conventional relay attacks. Even an advanced attacker has to be within 1-2 m of both the victim card and the reader

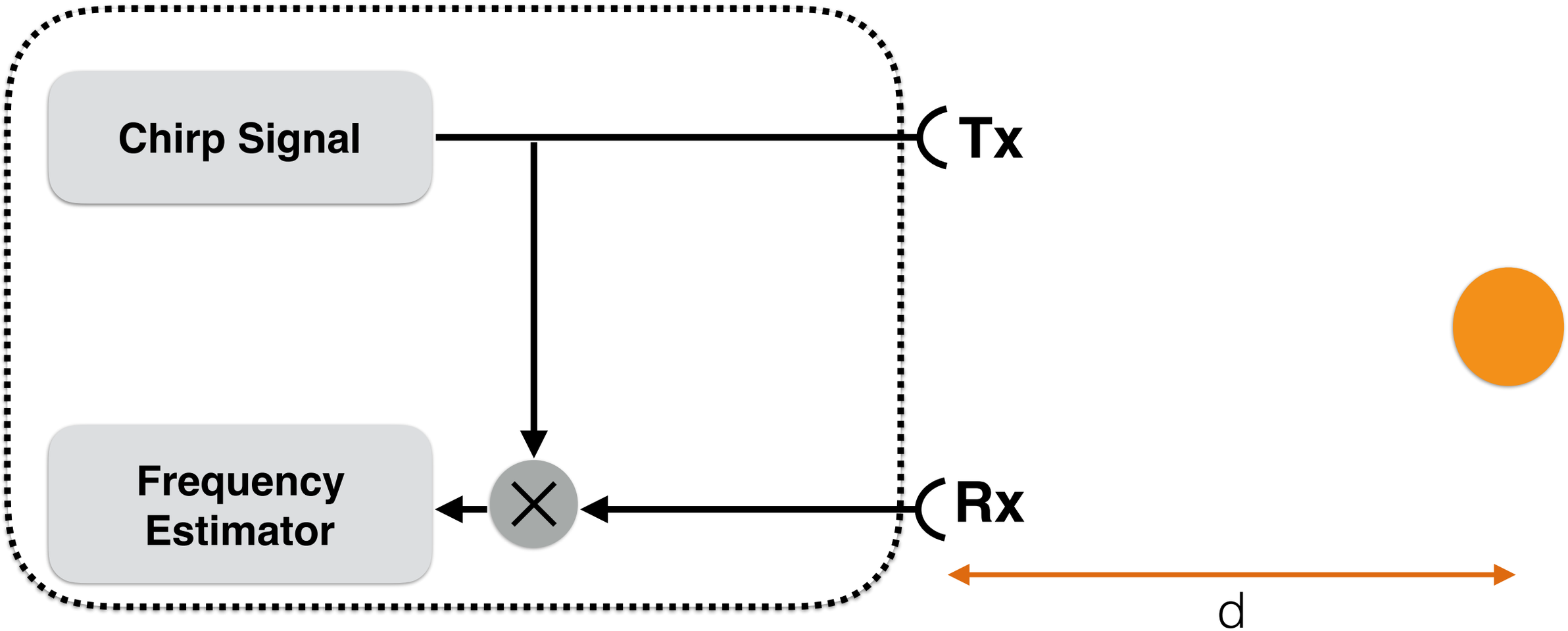
Our Contribution

- A first step towards realizing a secure proximity verification system in which the prover can be fully-passive
- Specifically designed for short-range contactless systems
- Our system is resilient against conventional relay attacks. Even an advanced attacker has to be within 1-2 m of both the victim card and the reader
- We use Frequency Modulated Continuous Wave (FMCW) for distance measurement and backscatter communication technique for data exchange

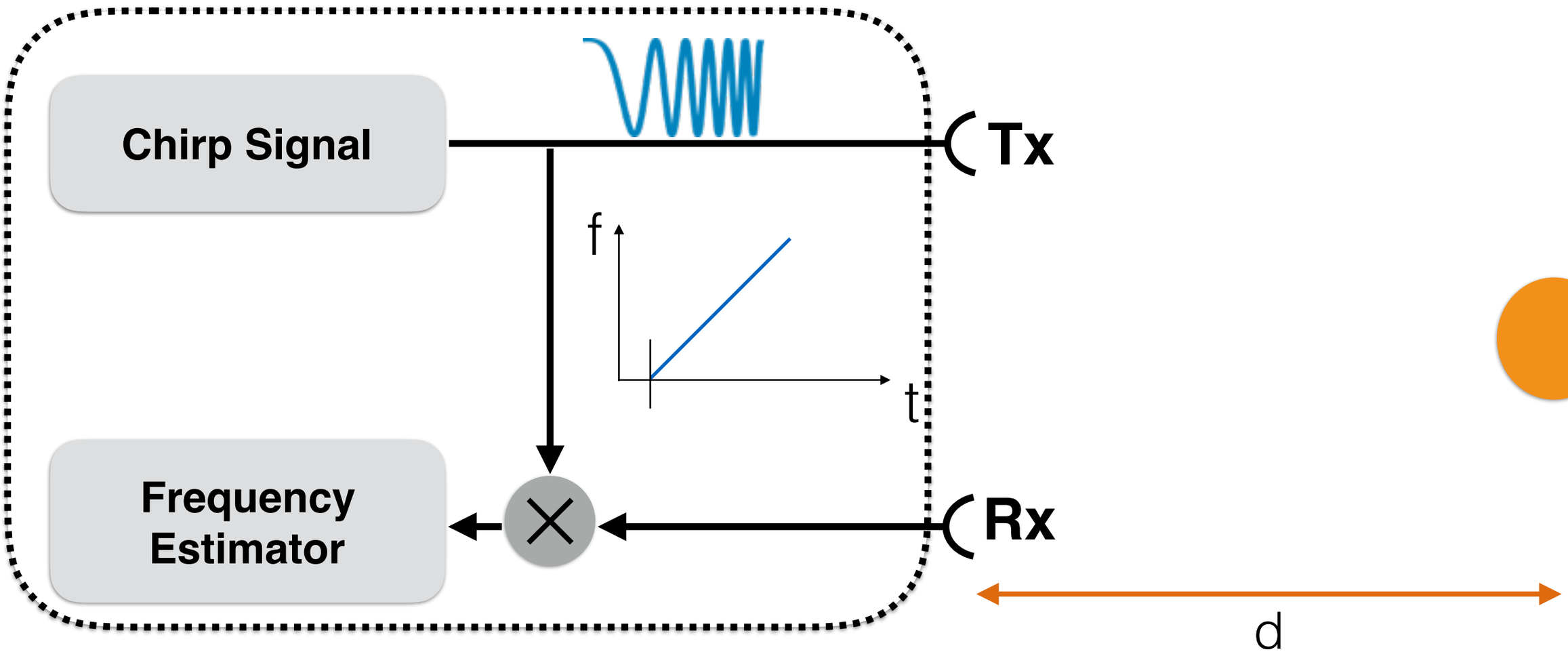
Overview of FMCW



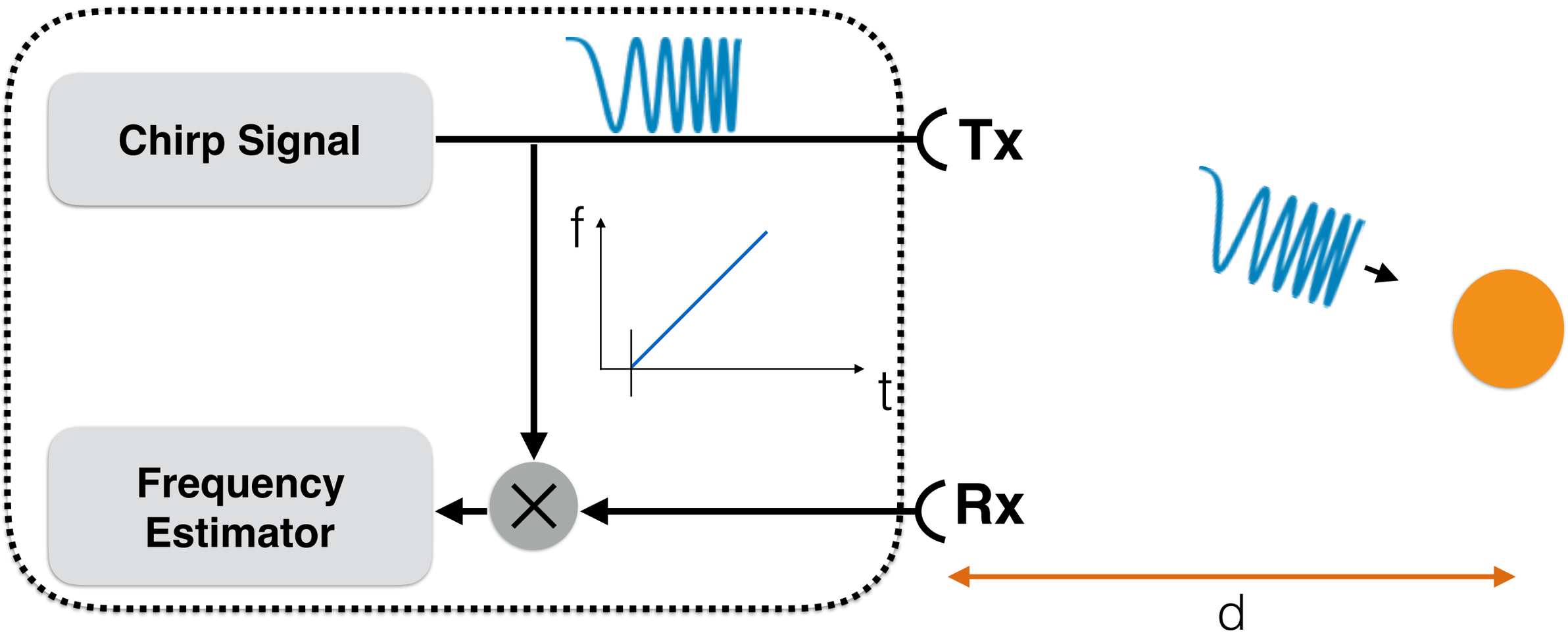
Overview of FMCW



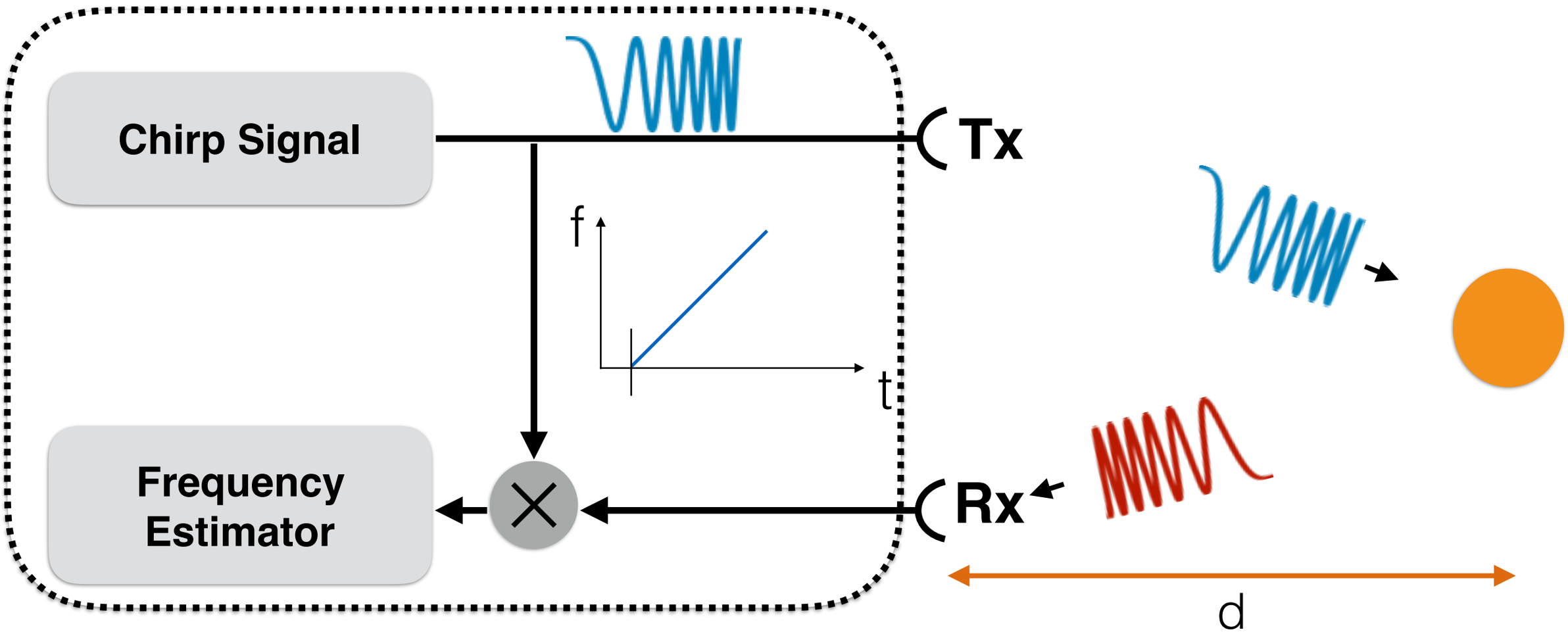
Overview of FMCW



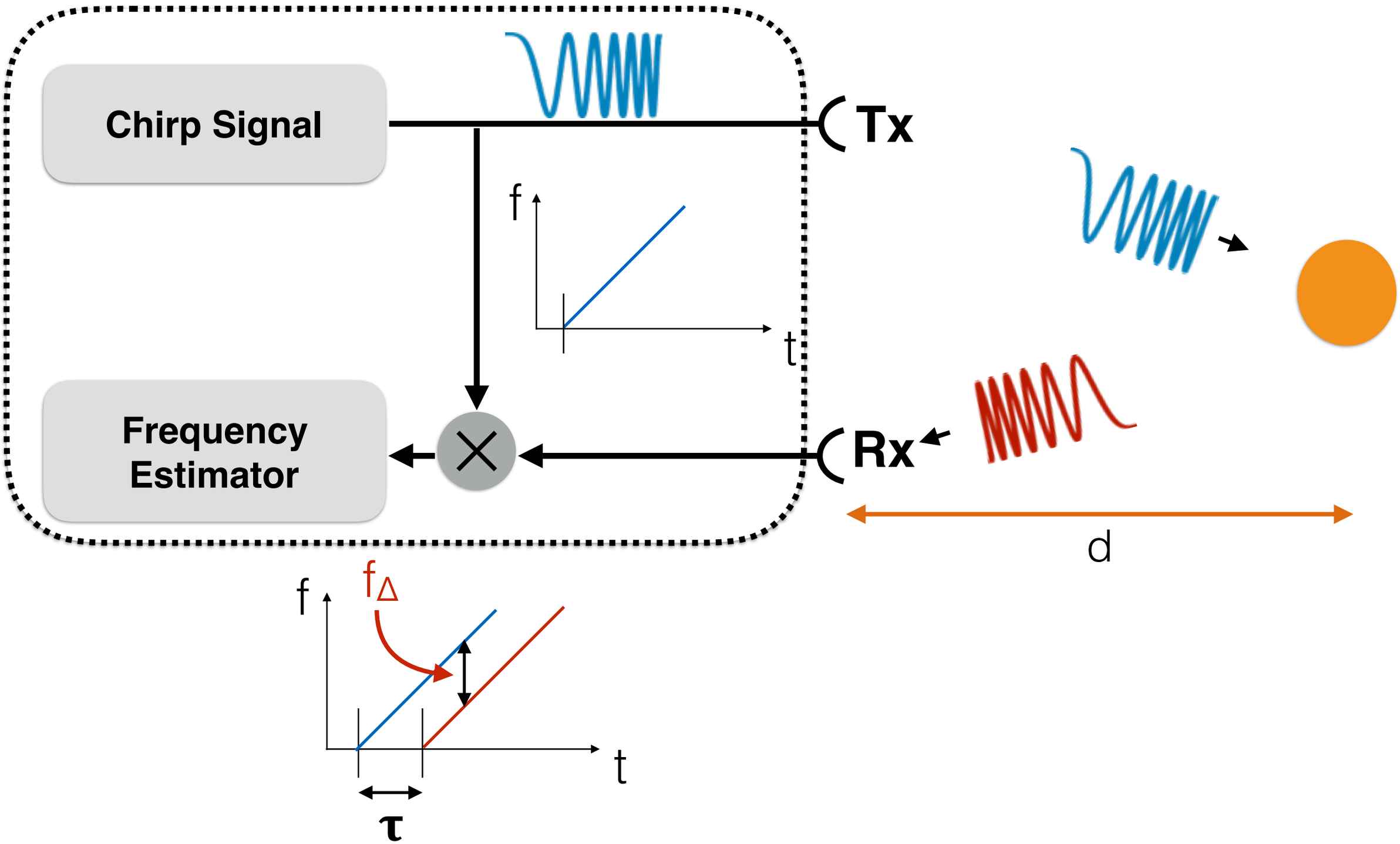
Overview of FMCW



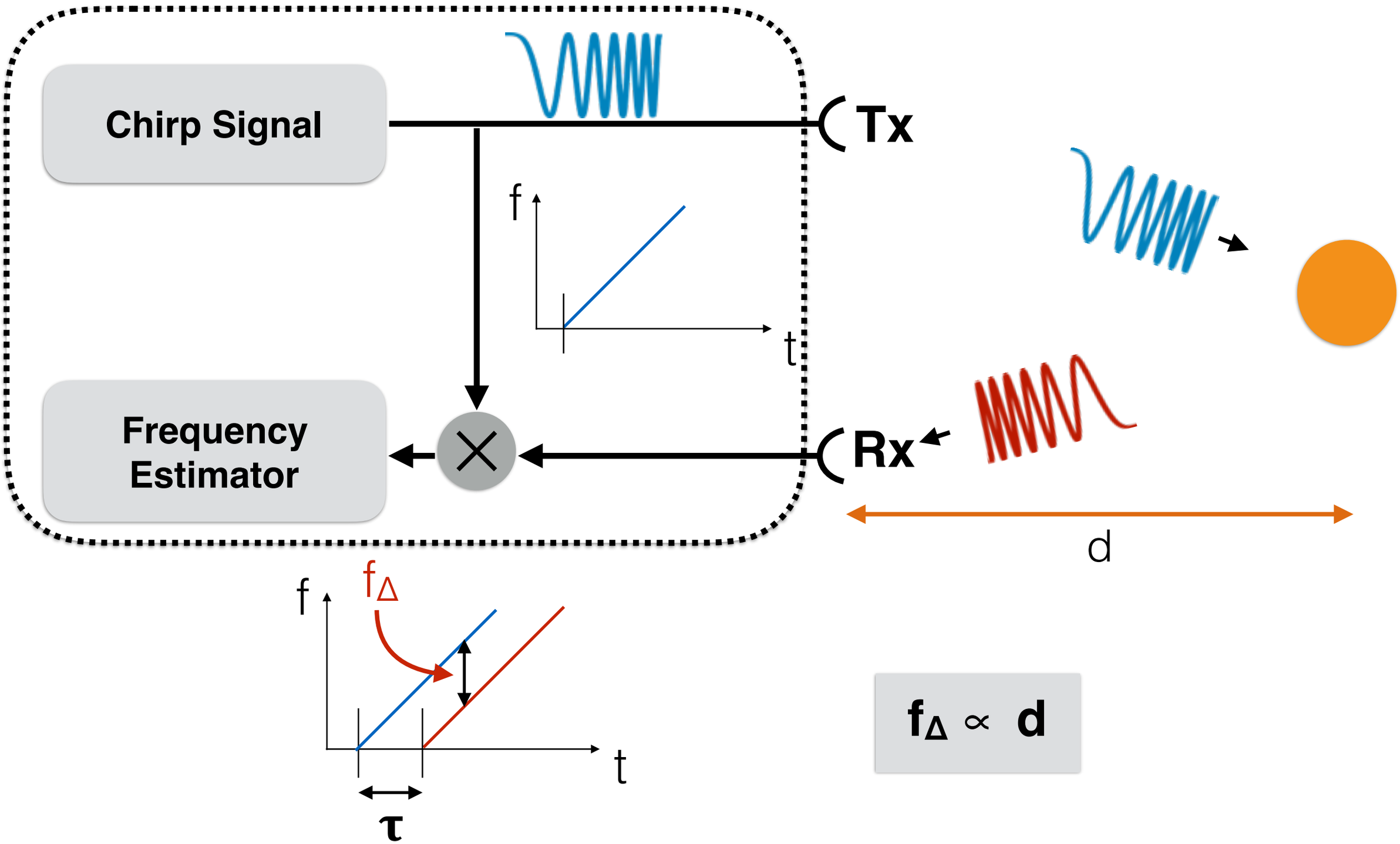
Overview of FMCW



Overview of FMCW



Overview of FMCW

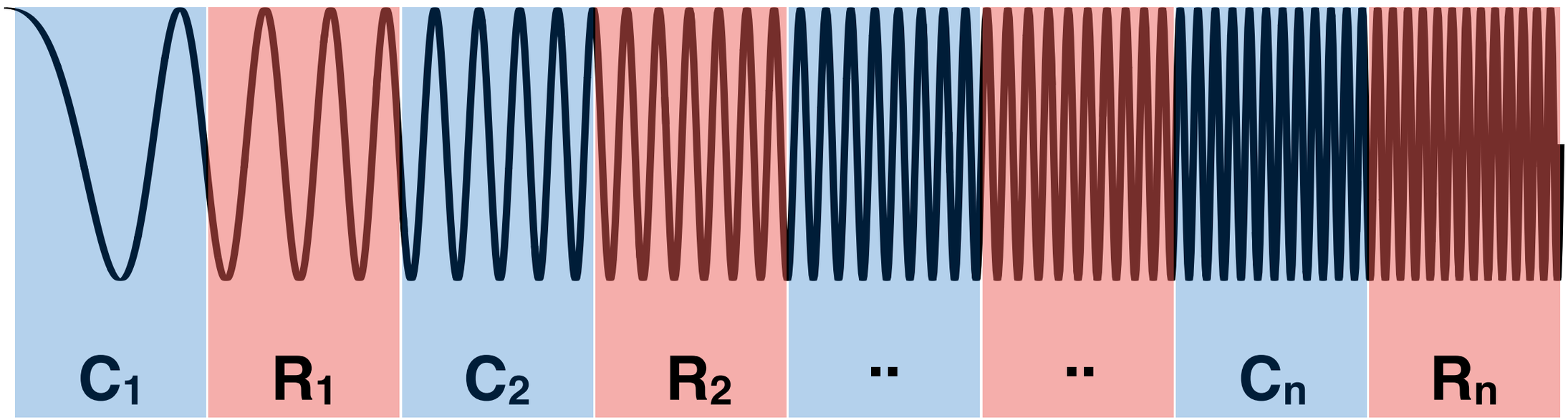


$$f_\Delta \propto d$$

FMCW-based Distance Bounding

- Conventional Radar systems do not require any data exchange.
- Exchange of data (challenges and responses) is important for secure proximity verification
- We use On-Off Keying (OOK) to modulate the challenges and responses over the FMCW chirp.

Challenge and Response Slots



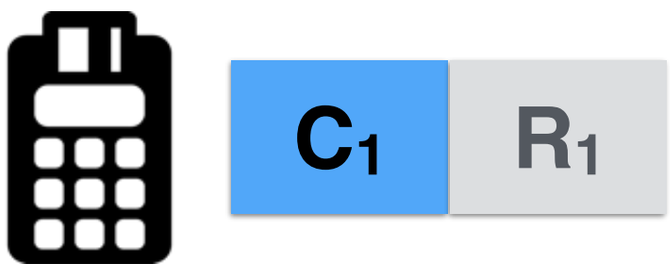
- The chirp signal is divided into challenge and response slots
- Verifier modulates challenges in the challenge slots and transmit clean (unmodulated) signal in the response slot
- The prover uses the response slots to modulate back the responses

Challenge and Response Slots

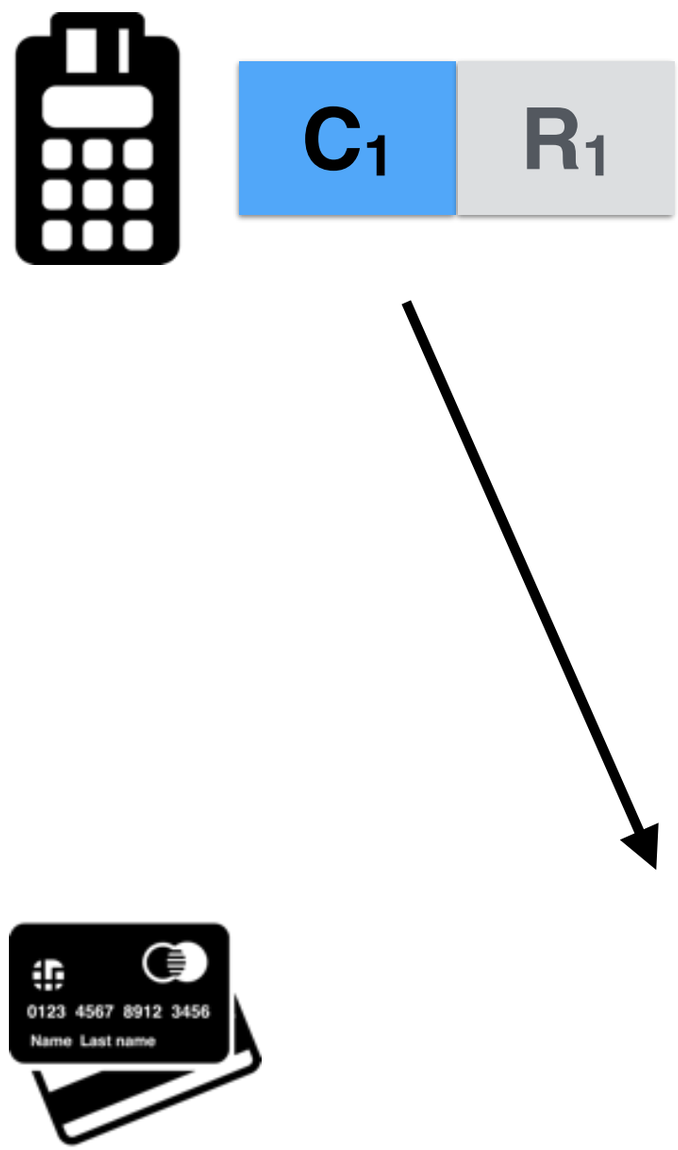
Challenge and Response Slots

C_1

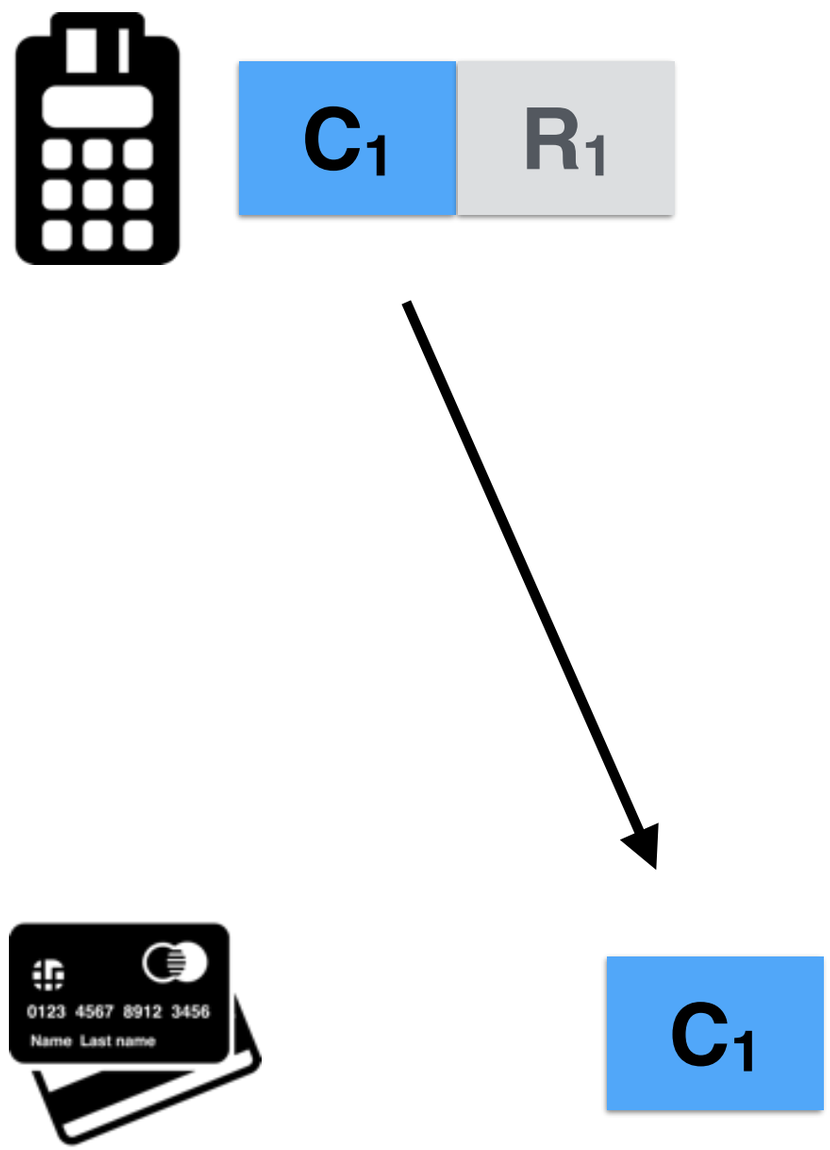
Challenge and Response Slots



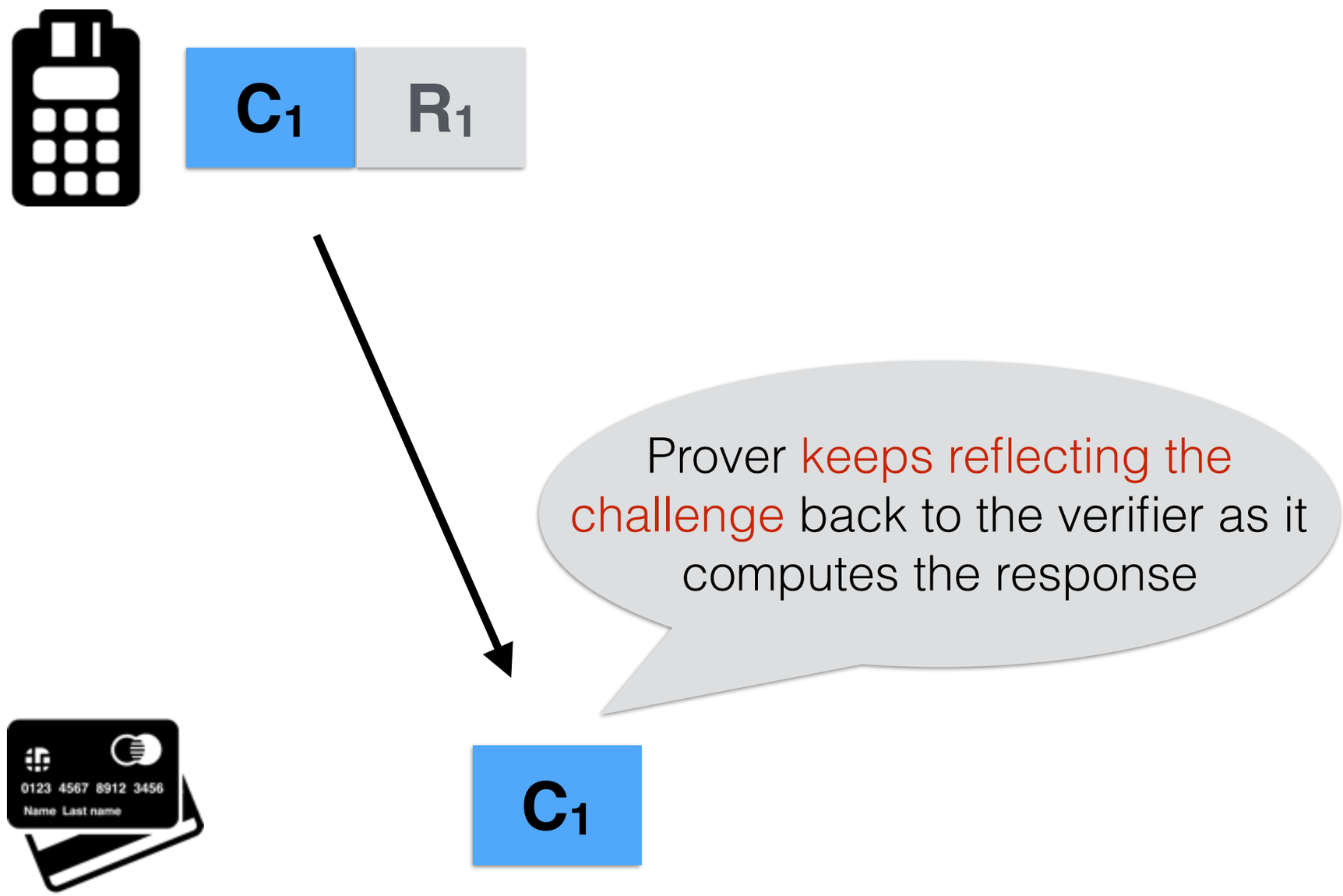
Challenge and Response Slots



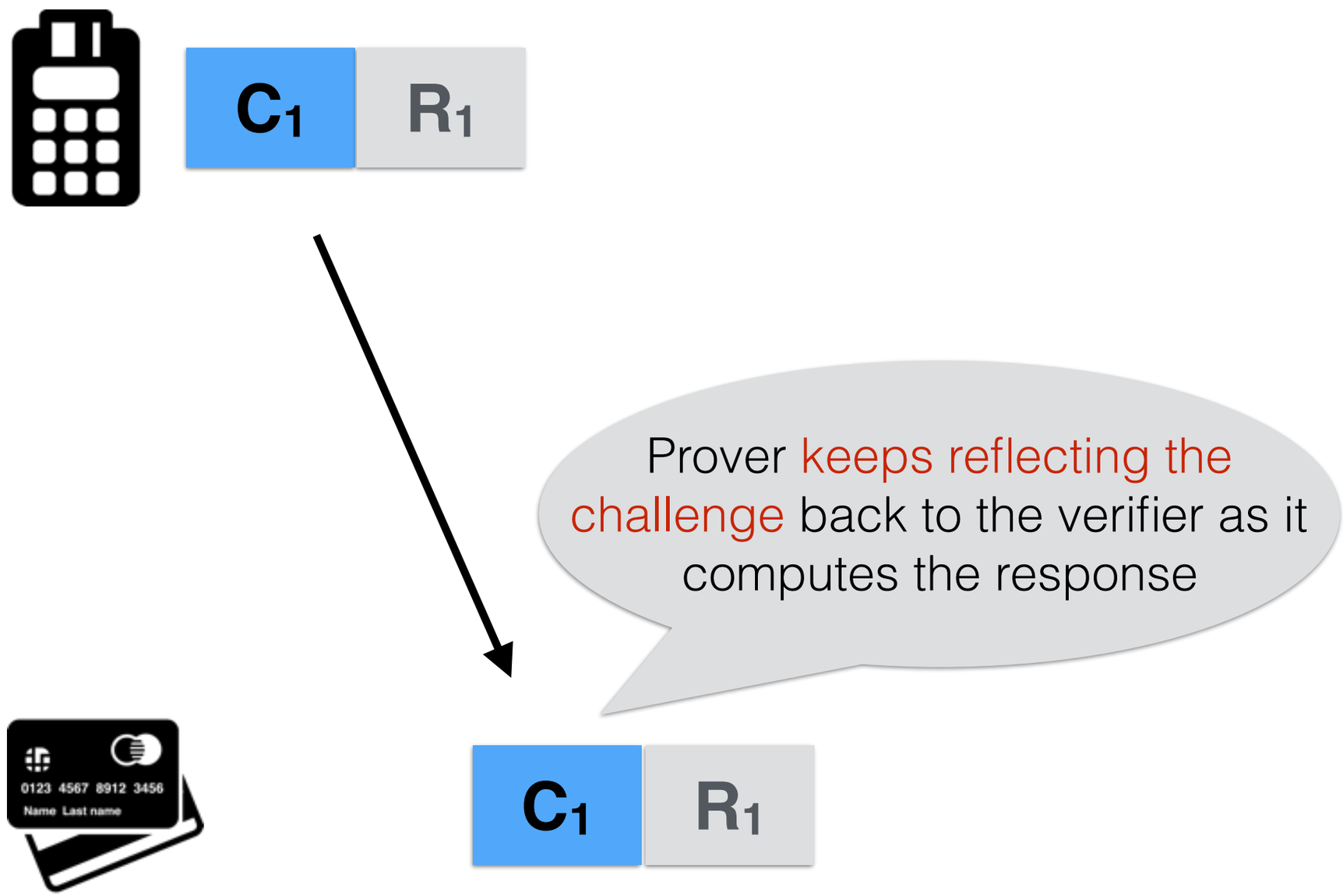
Challenge and Response Slots



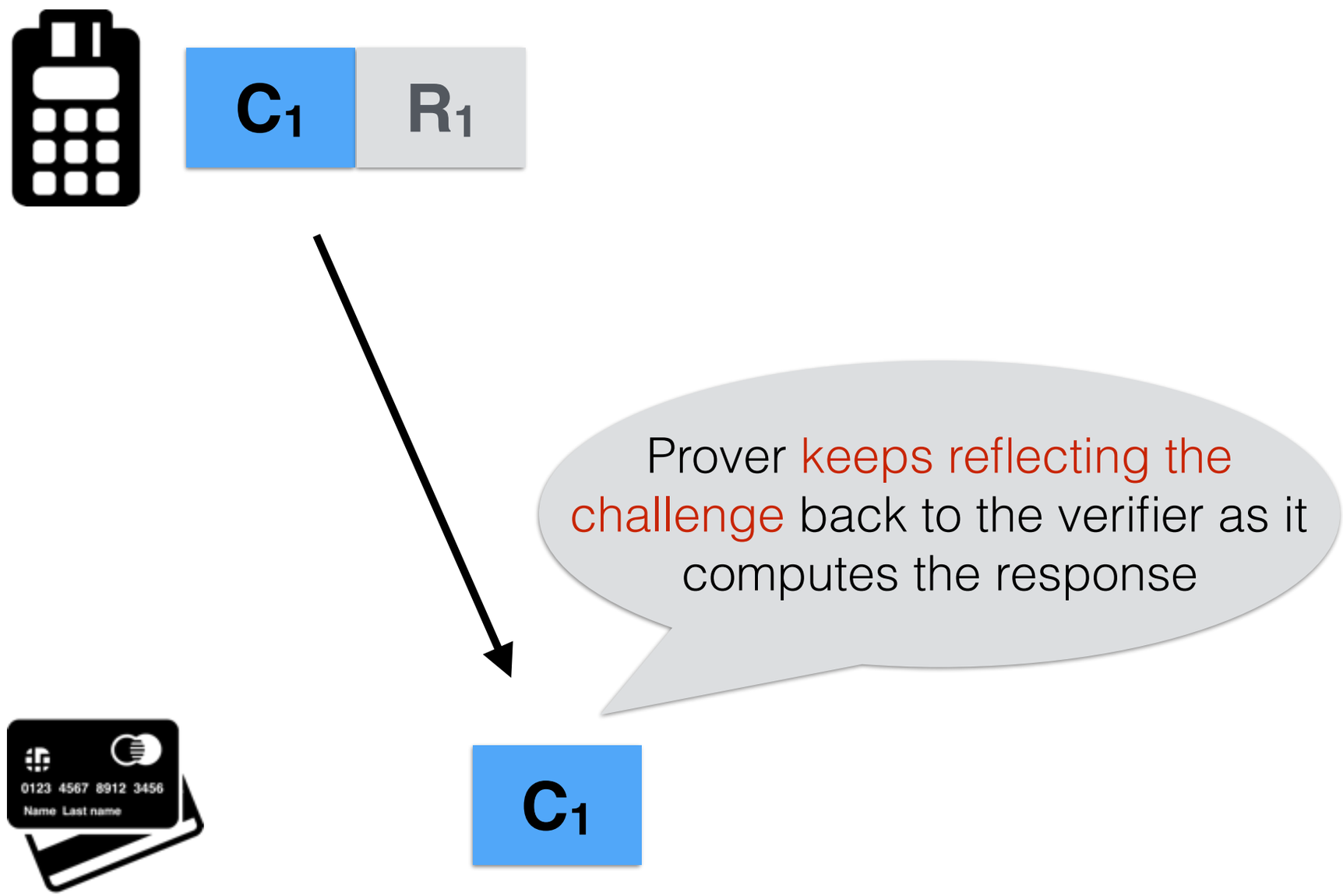
Challenge and Response Slots



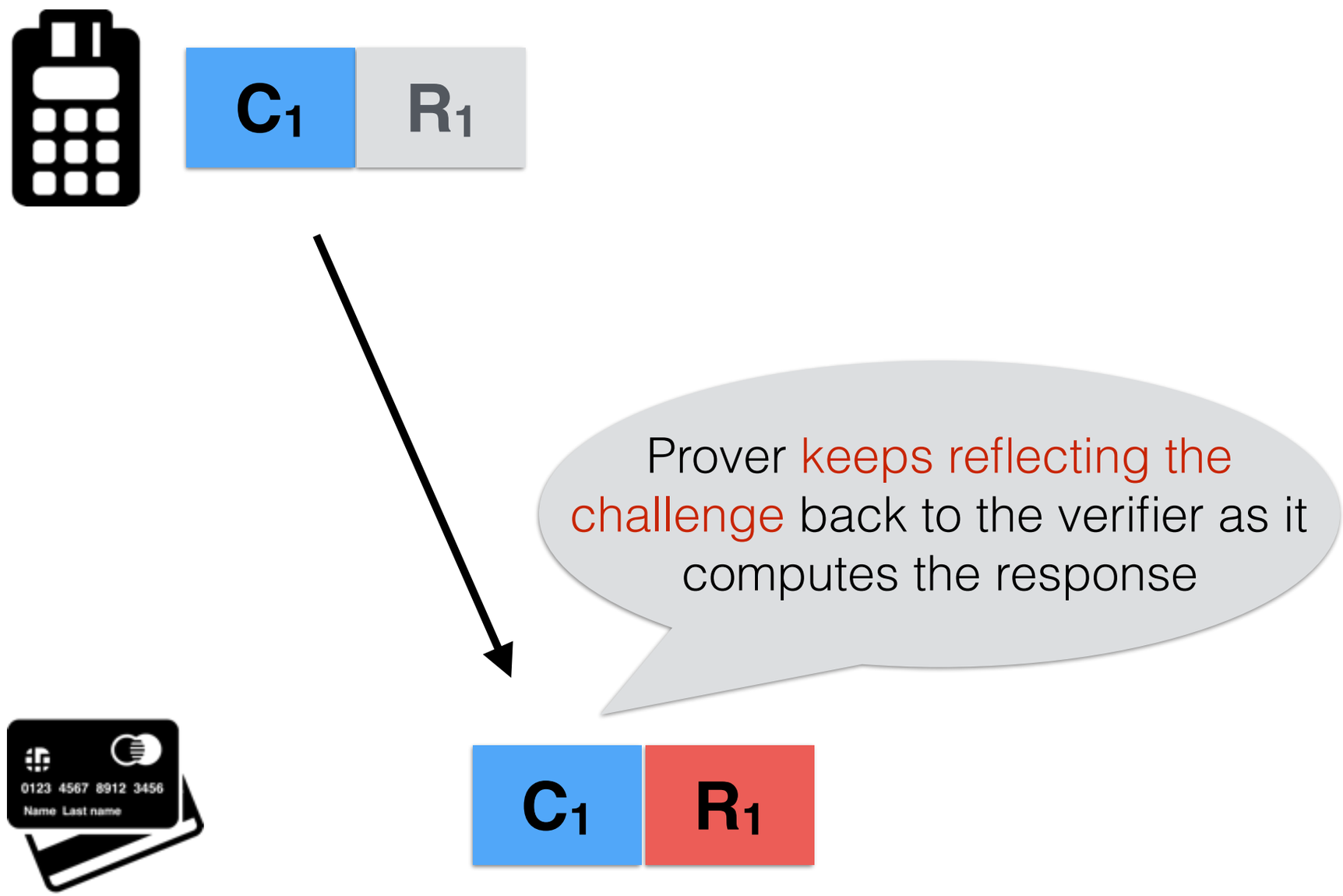
Challenge and Response Slots



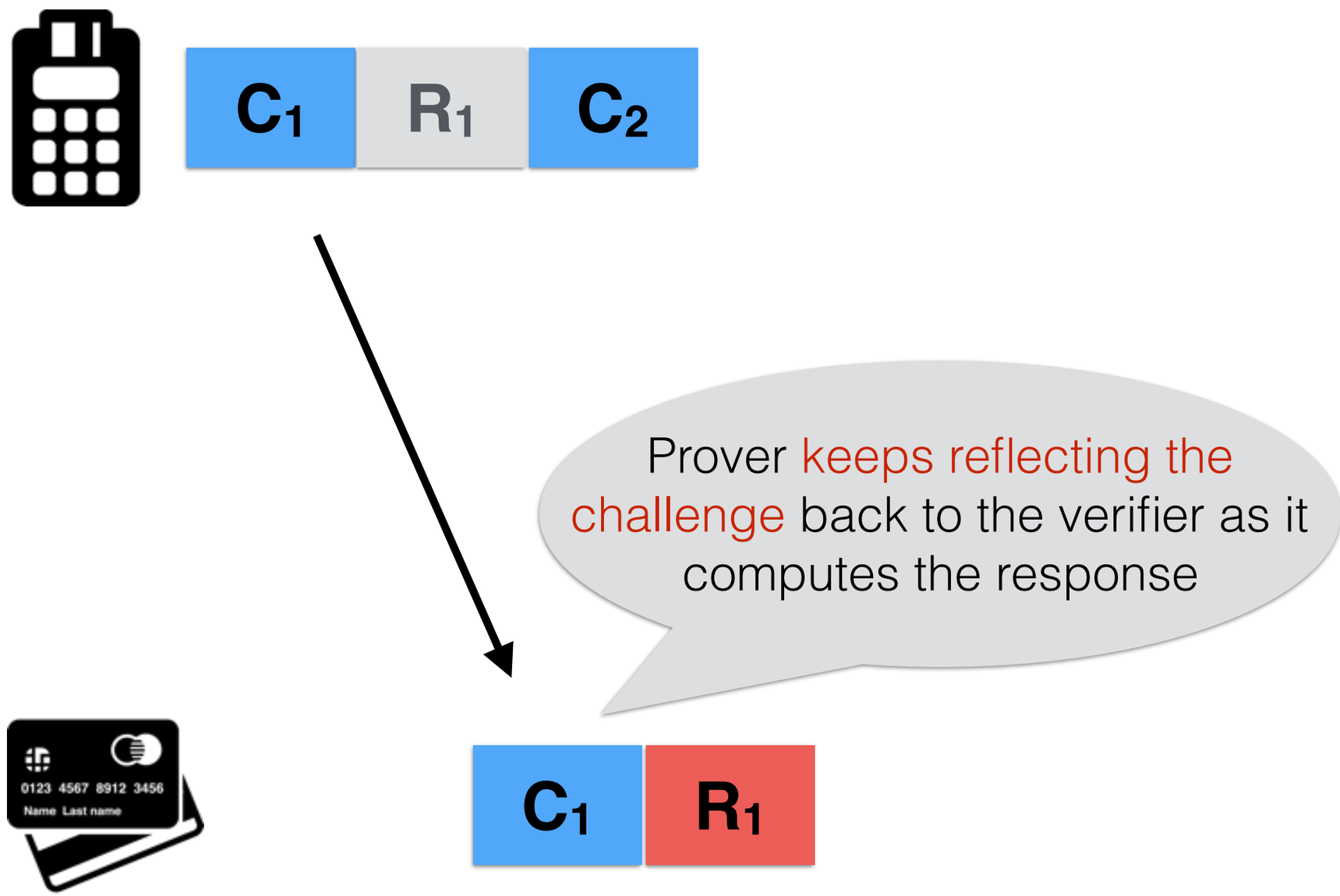
Challenge and Response Slots



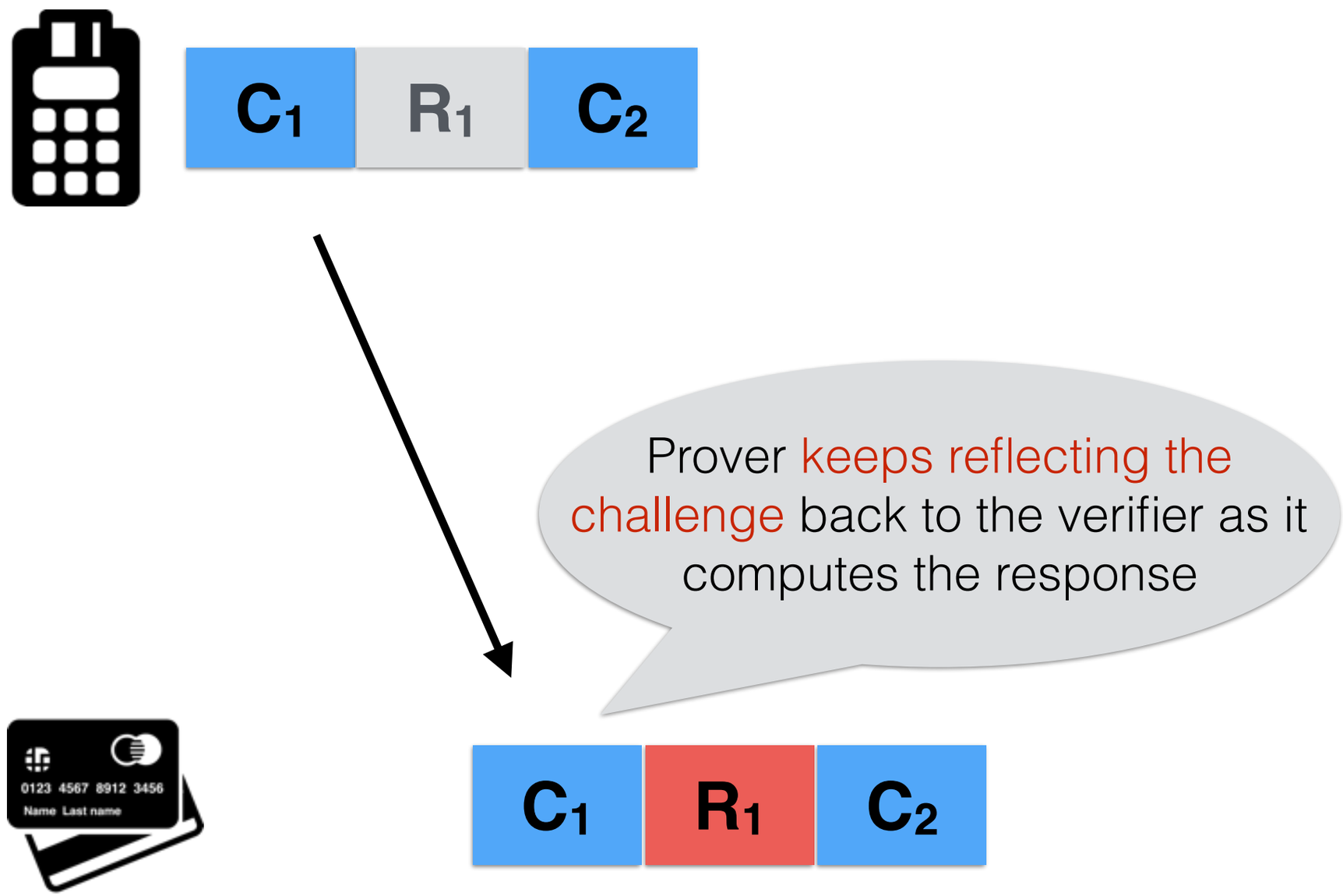
Challenge and Response Slots



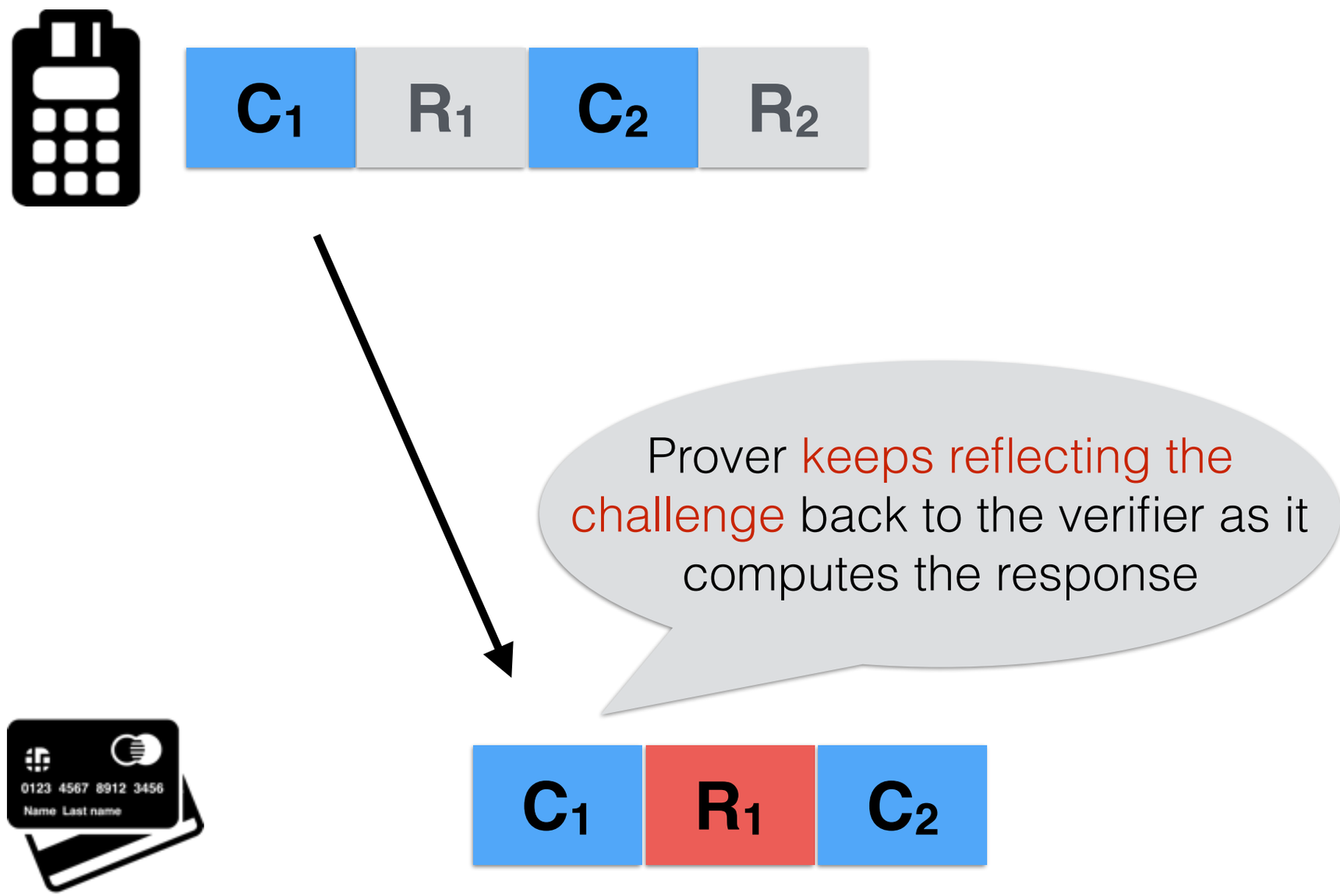
Challenge and Response Slots



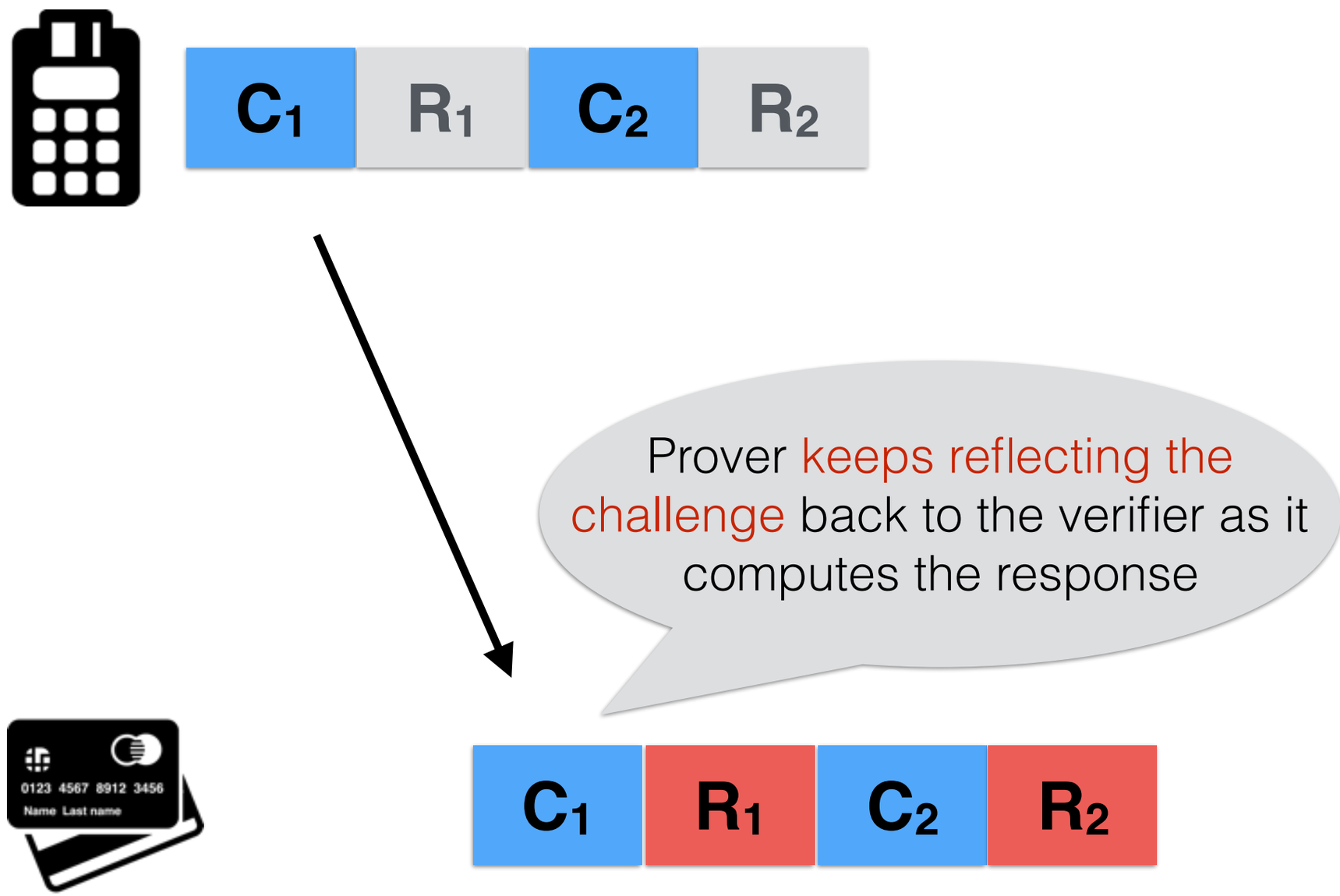
Challenge and Response Slots



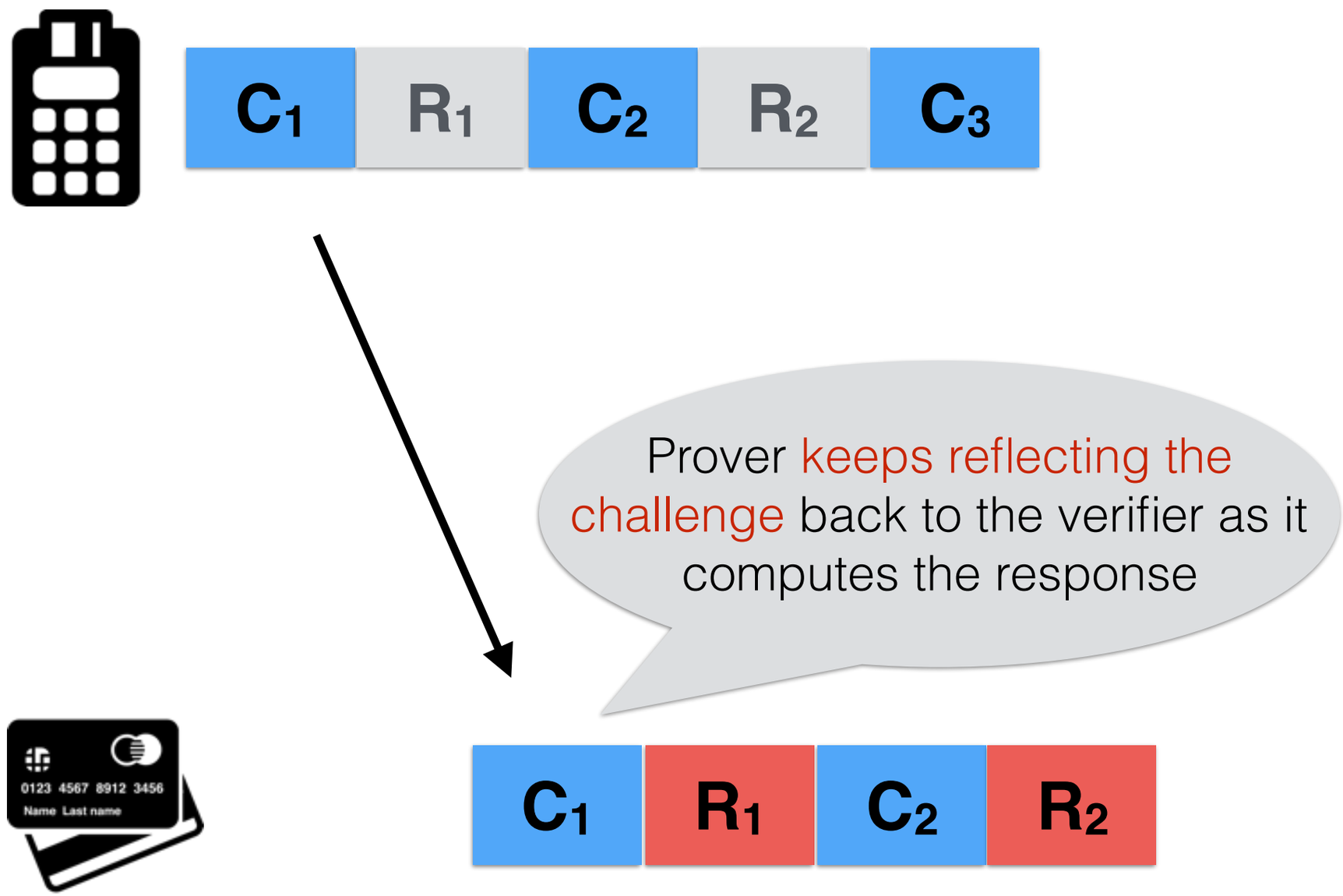
Challenge and Response Slots



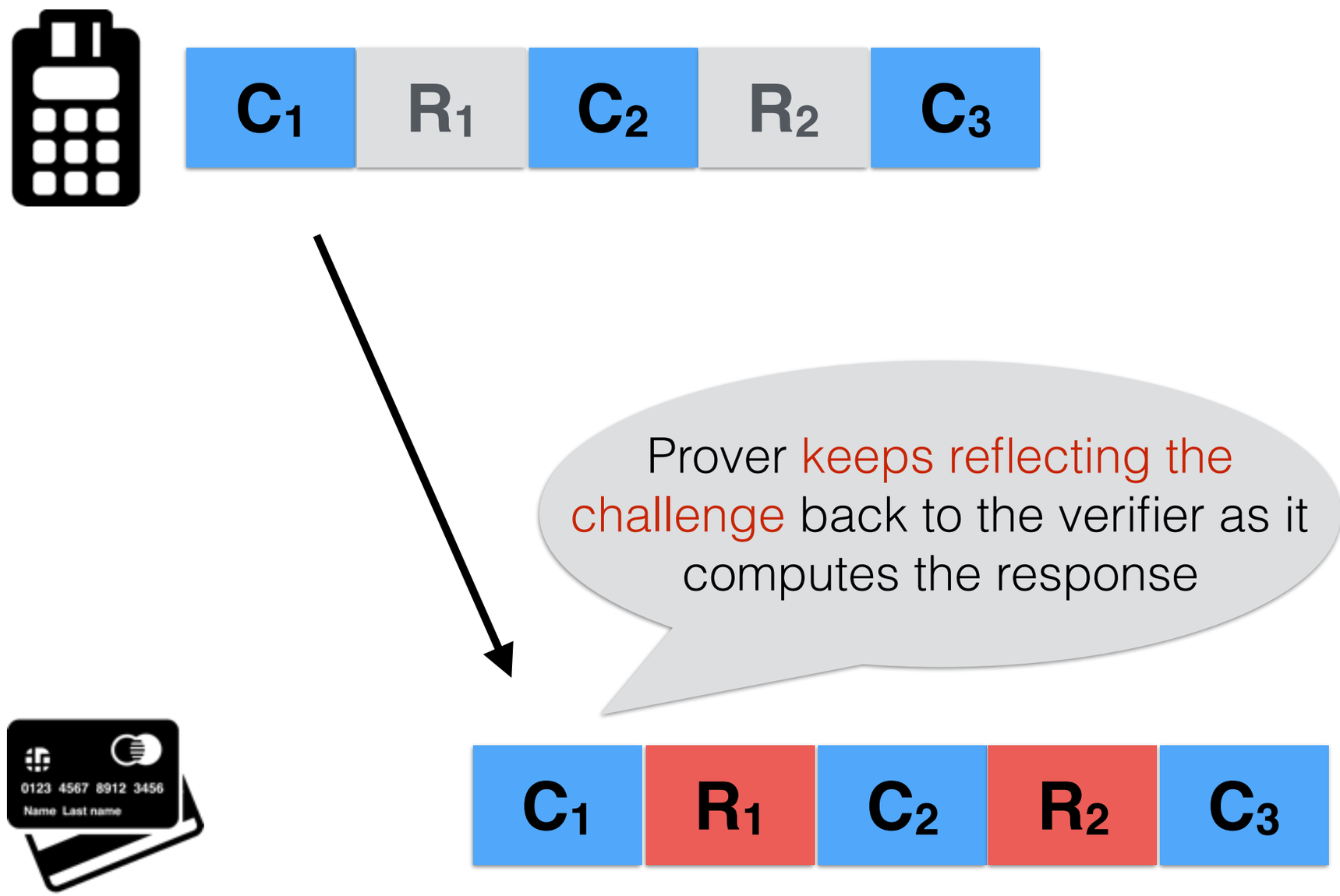
Challenge and Response Slots



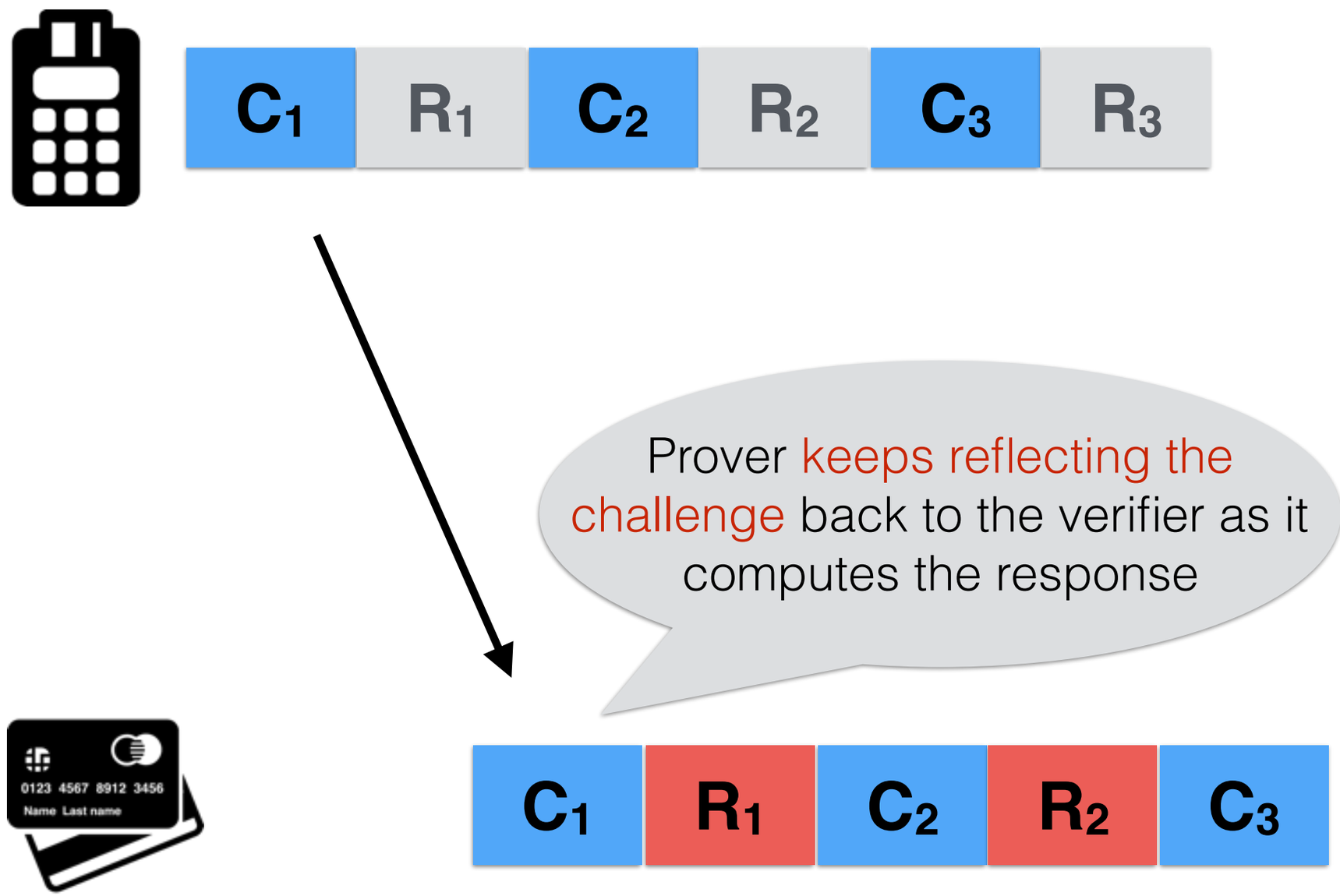
Challenge and Response Slots



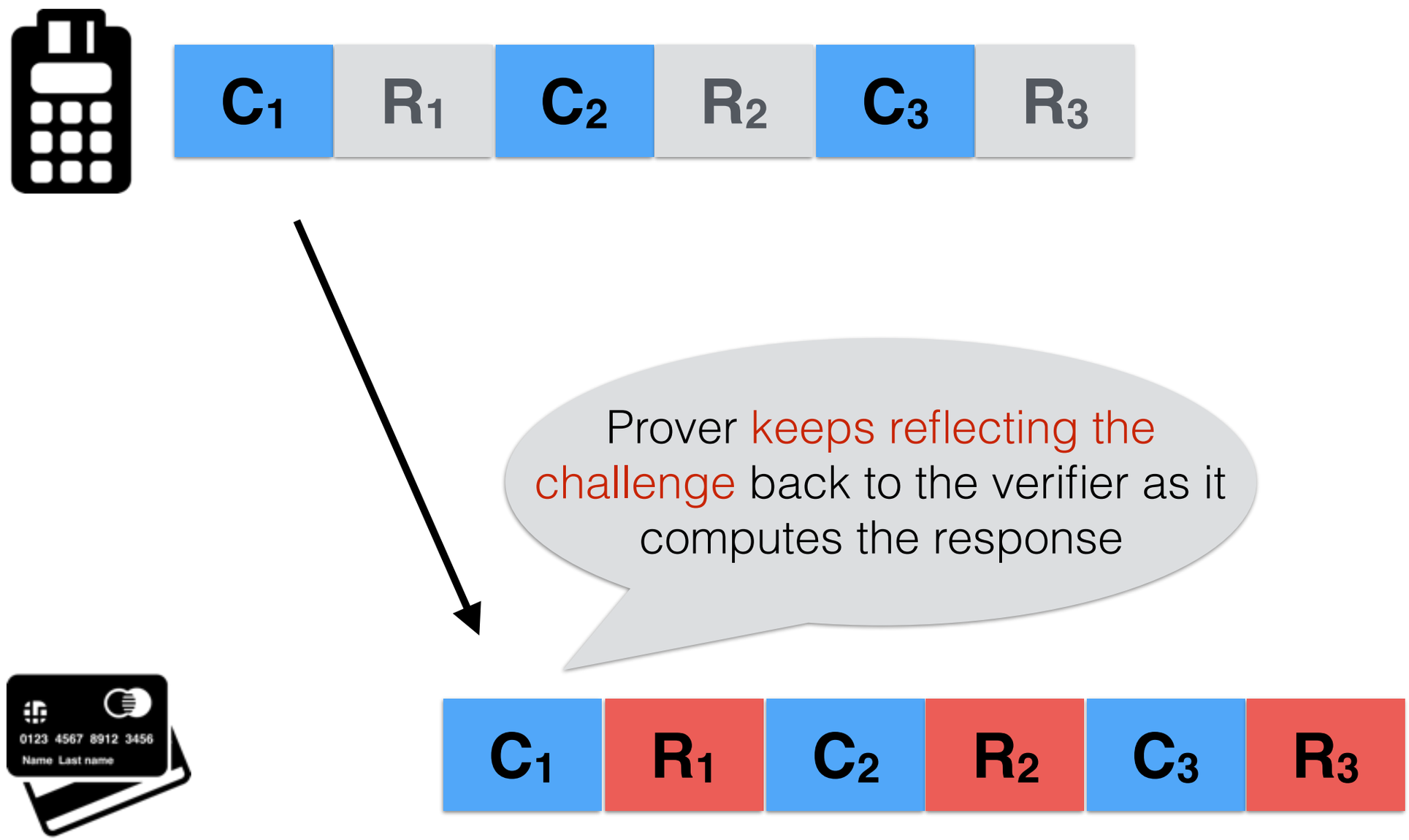
Challenge and Response Slots



Challenge and Response Slots

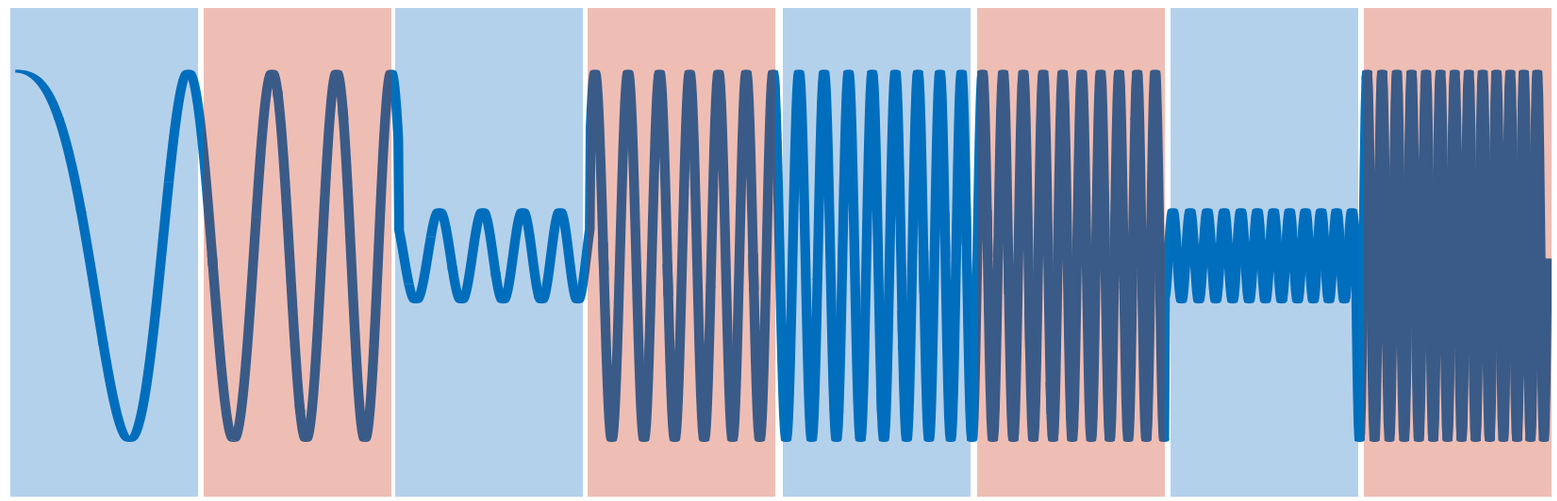


Challenge and Response Slots

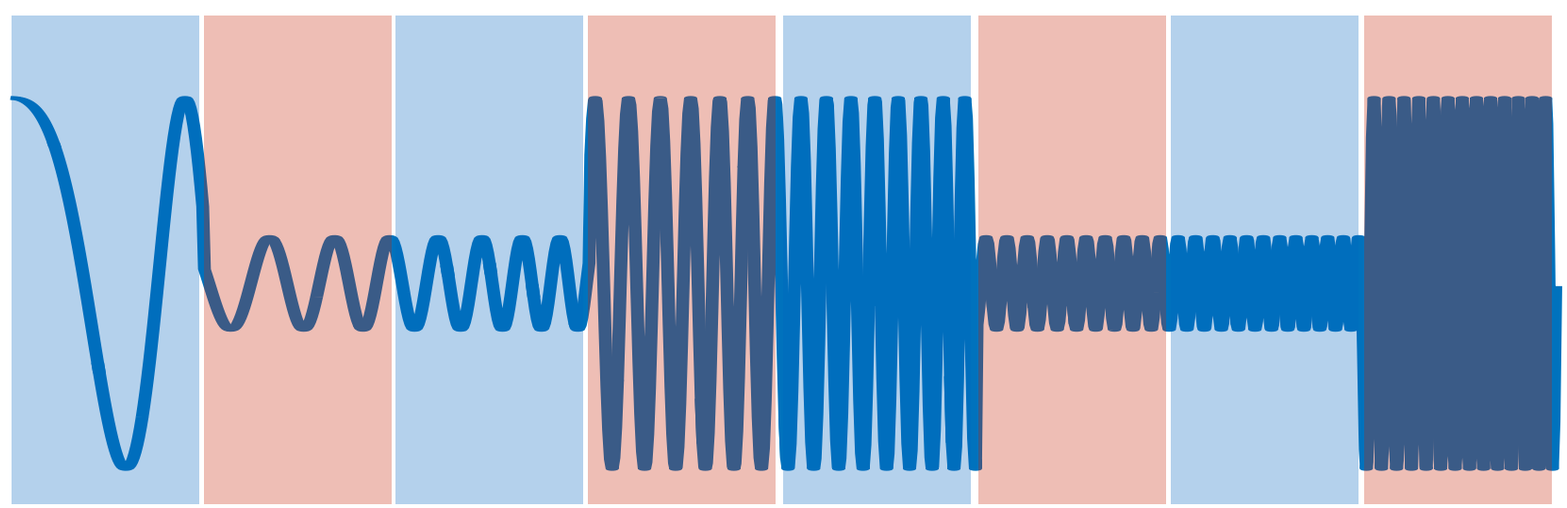


Example Challenge Response Slots

C={1,0,1,0}

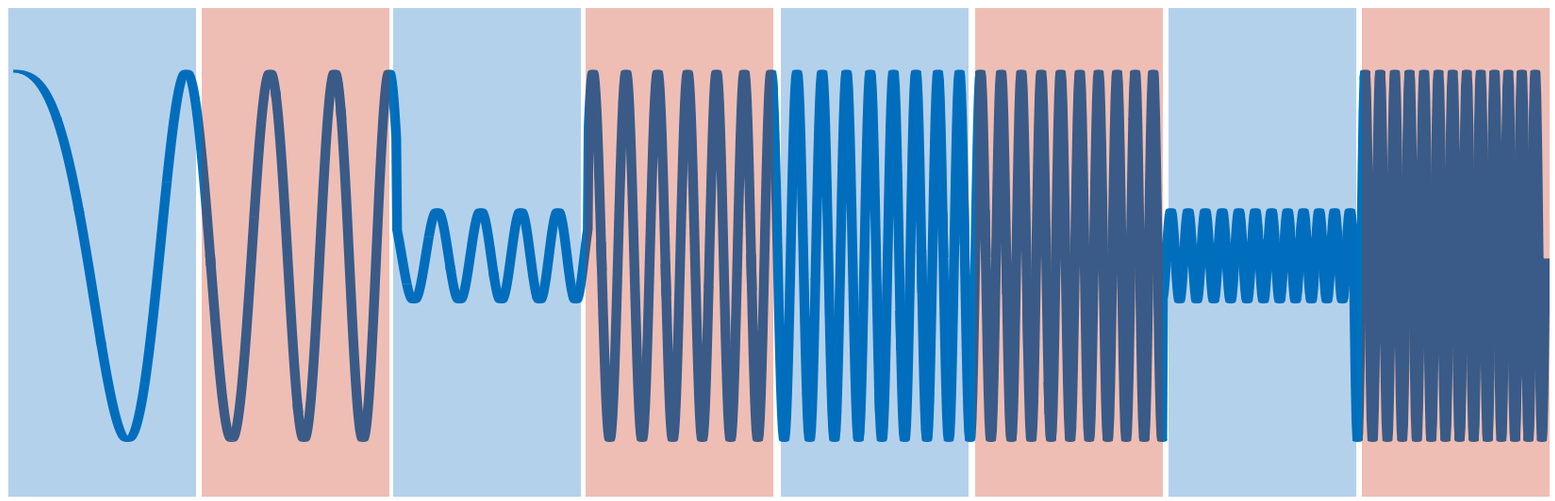


R={0,1,0,1}



Example Challenge Response Slots

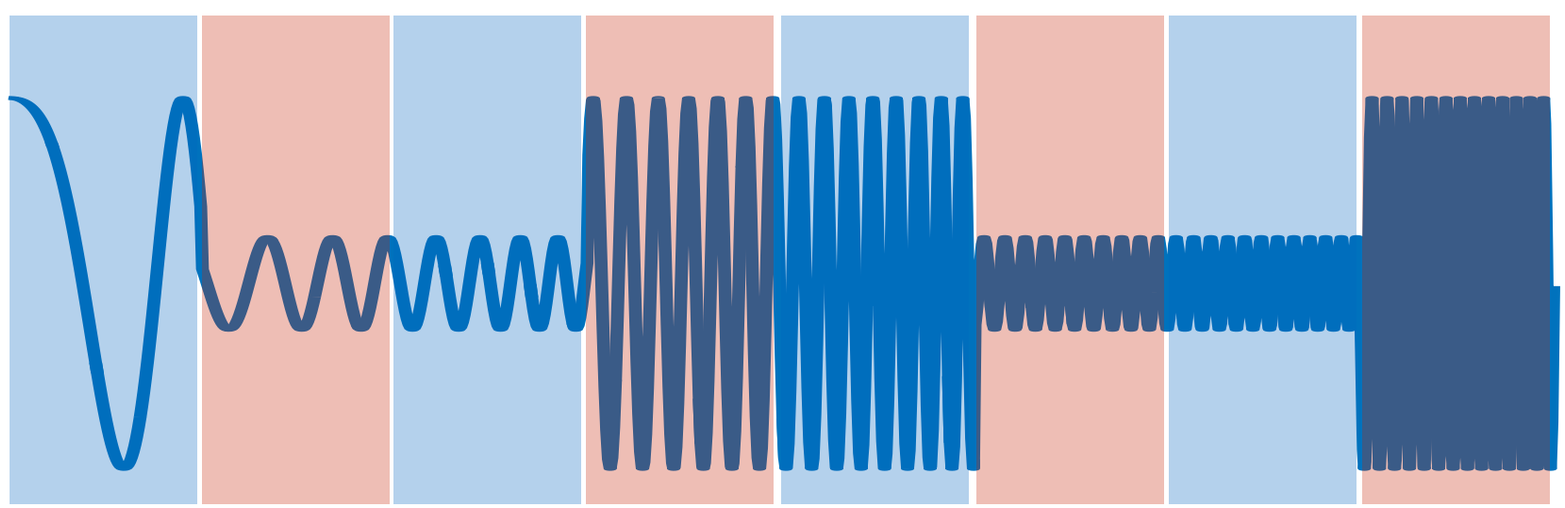
C={1,0,1,0}



C_1

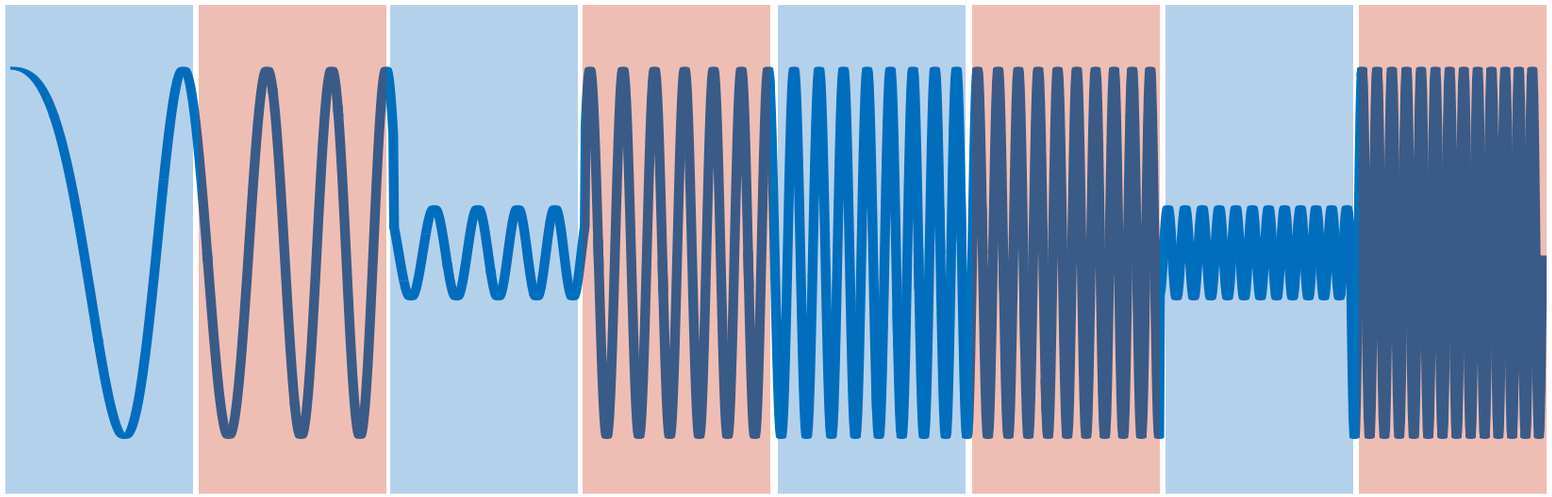
1

R={0,1,0,1}



Example Challenge Response Slots

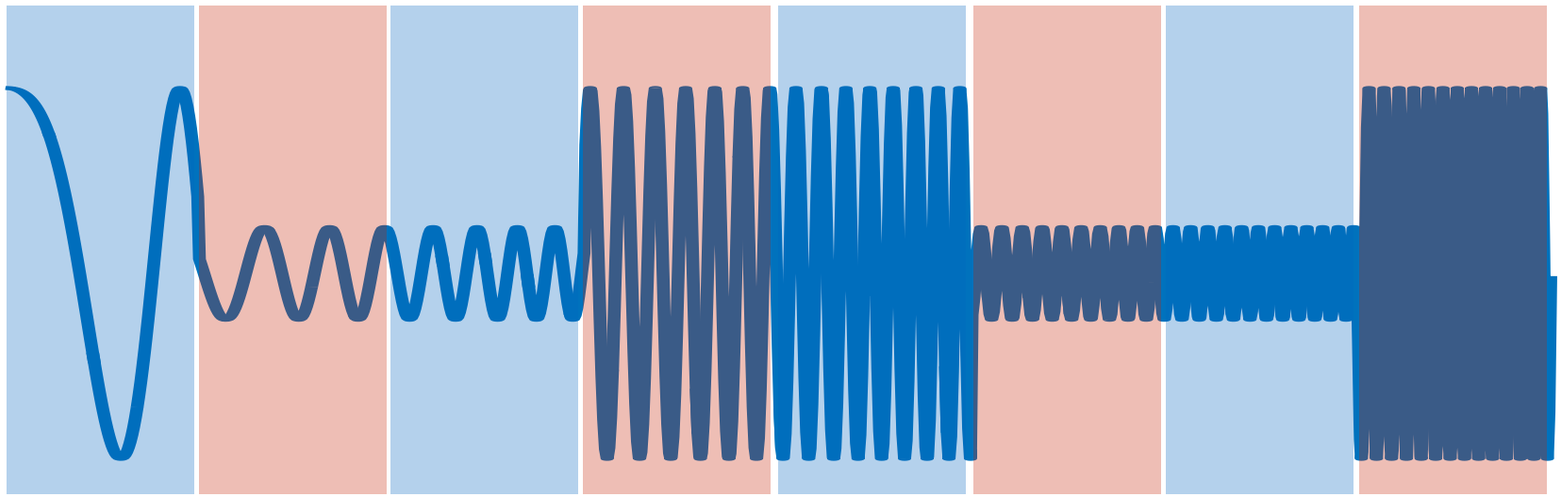
C={1,0,1,0}



C_1 R_1

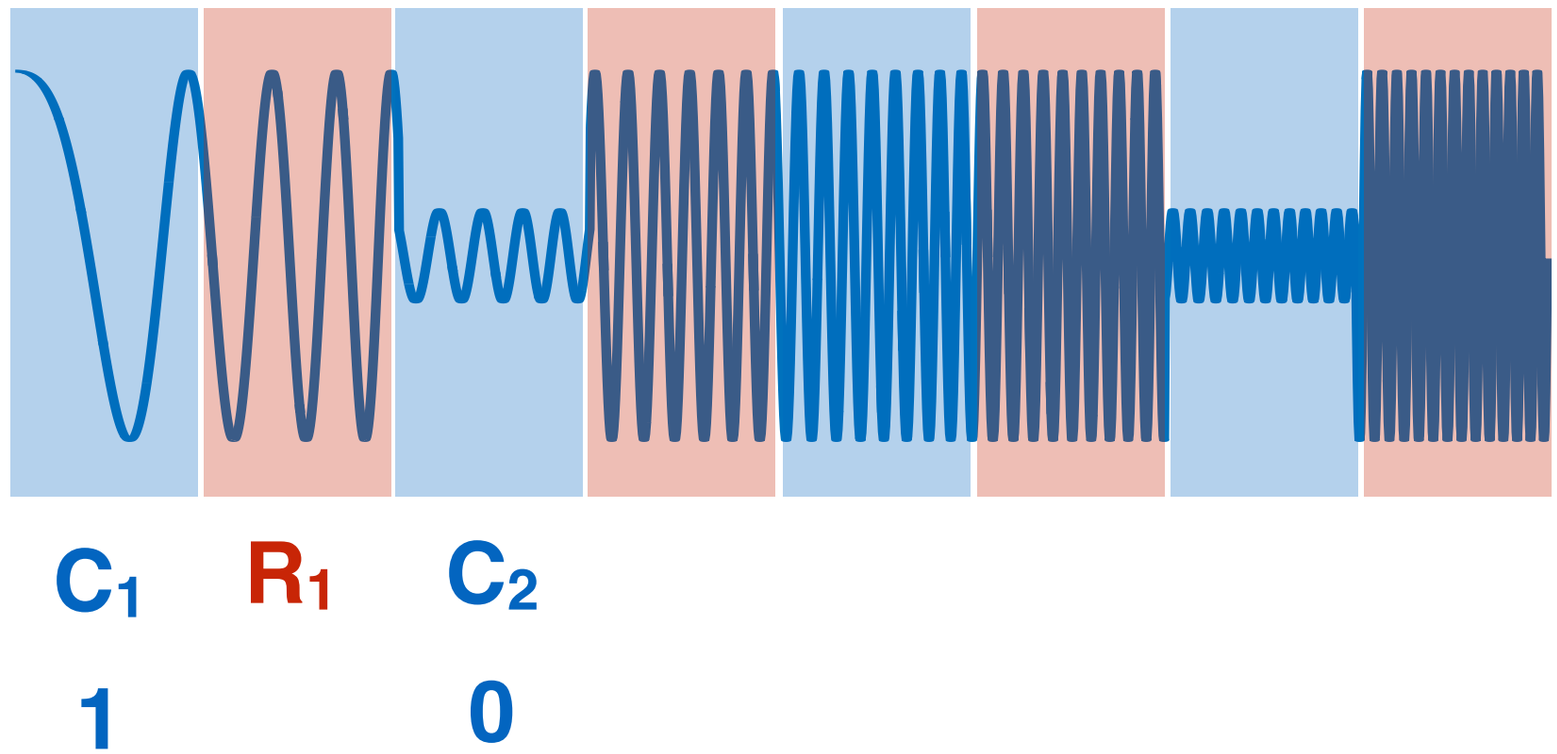
1

R={0,1,0,1}

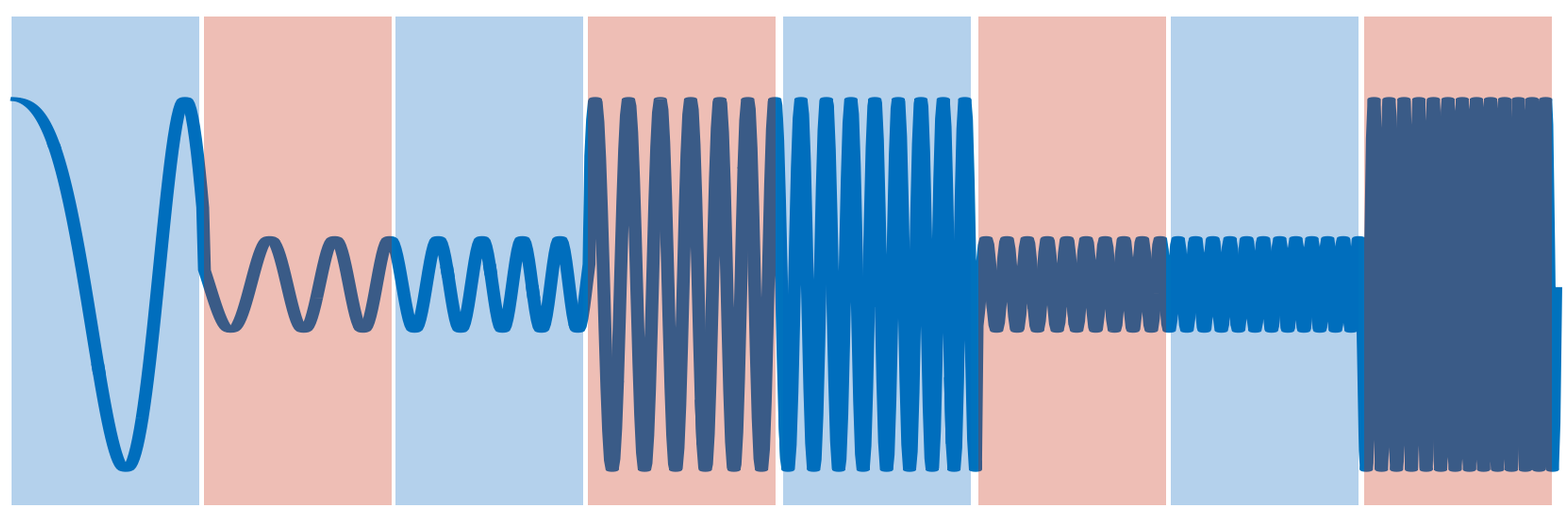


Example Challenge Response Slots

C={1,0,1,0}

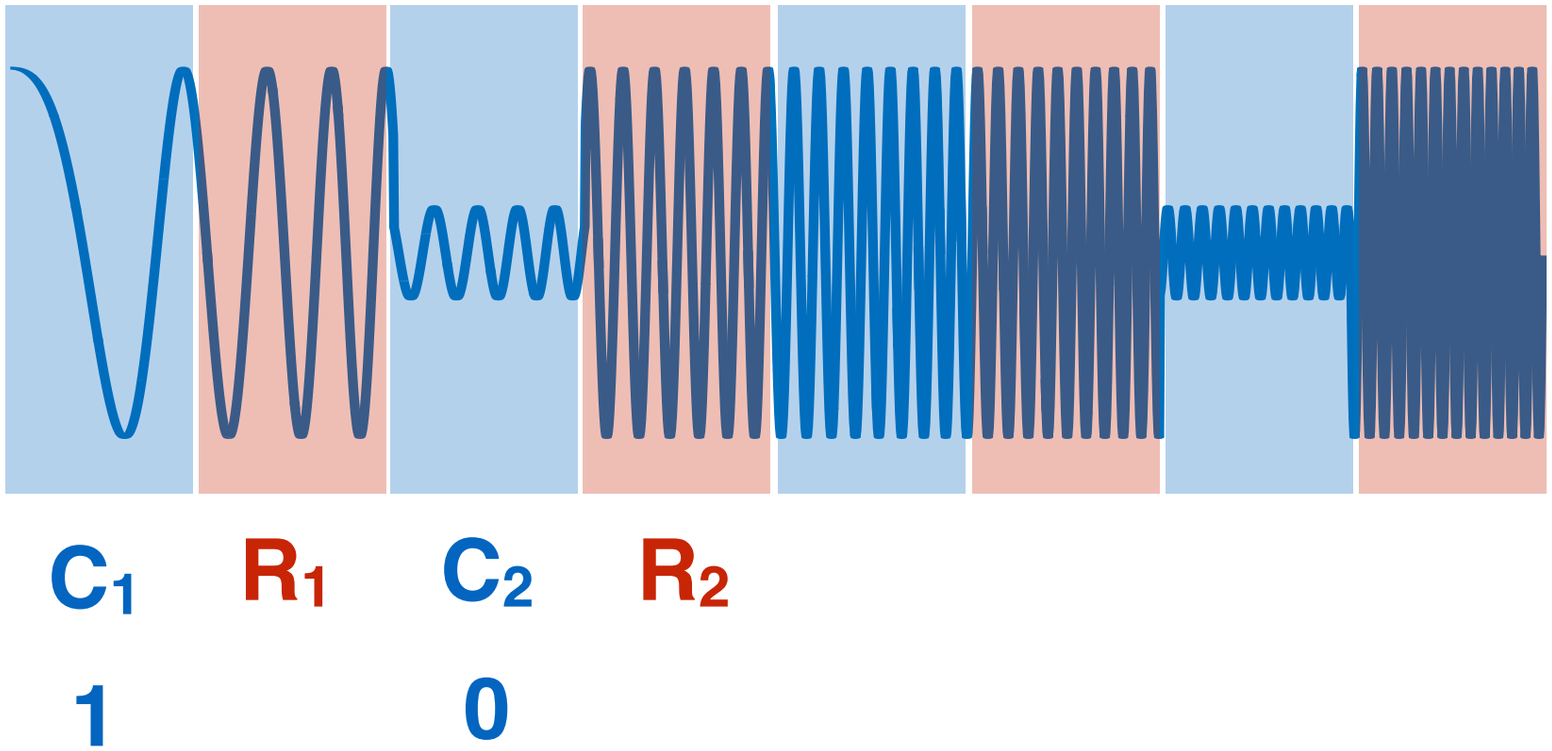


R={0,1,0,1}

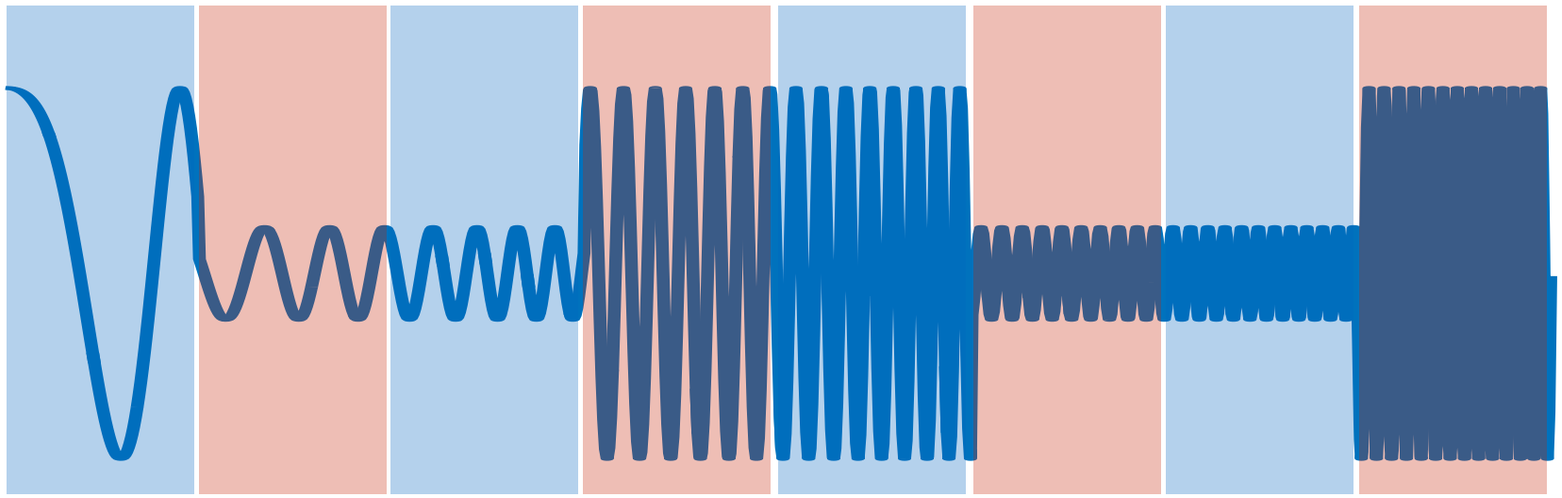


Example Challenge Response Slots

C={1,0,1,0}

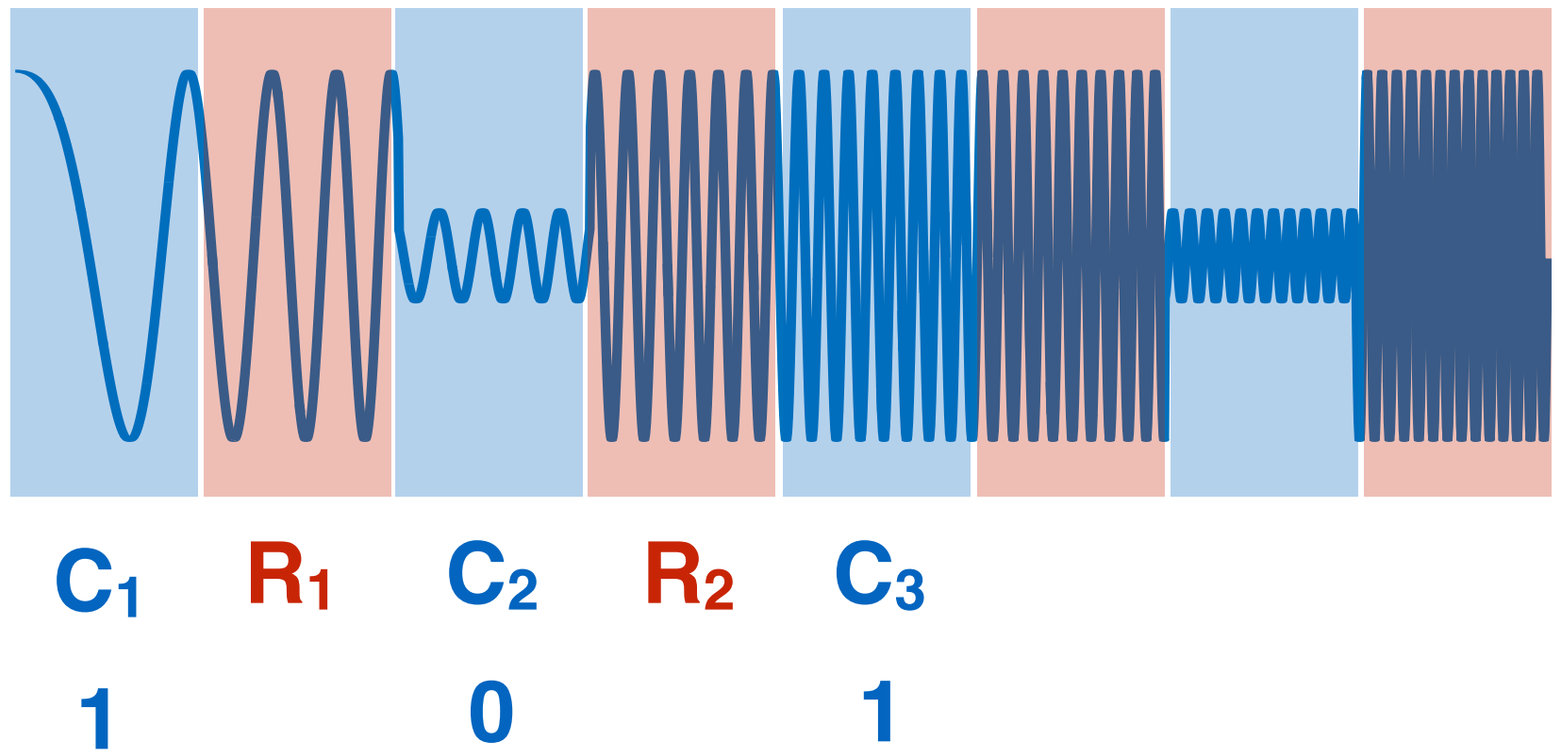


R={0,1,0,1}

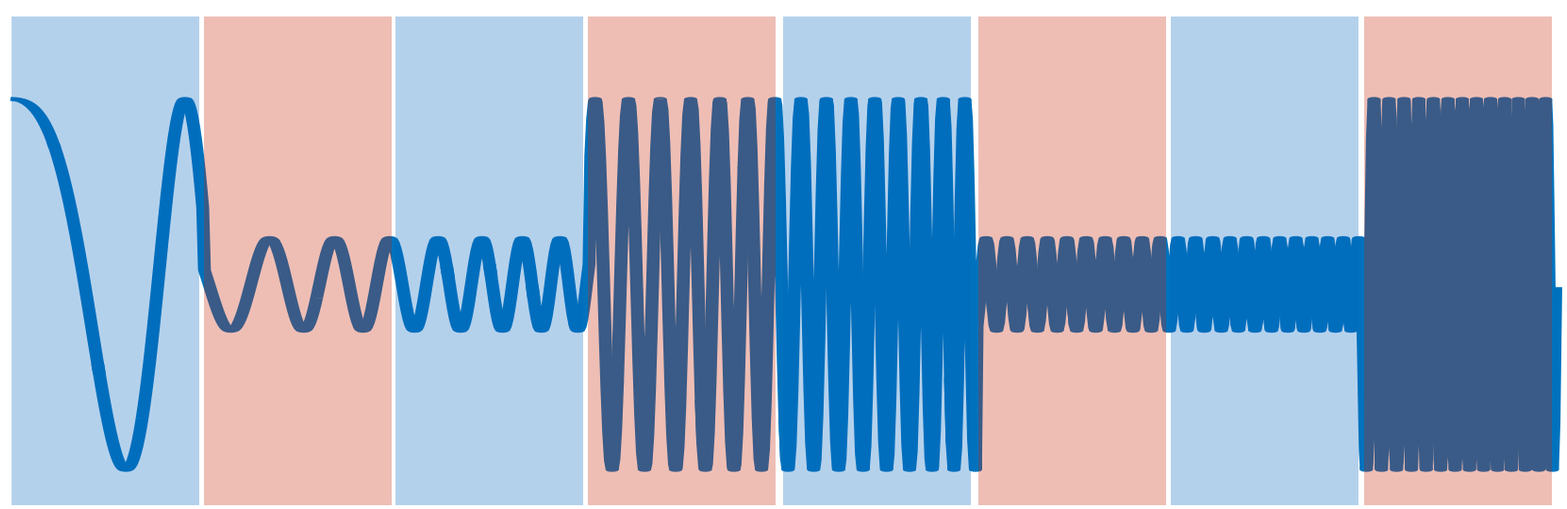


Example Challenge Response Slots

C={1,0,1,0}

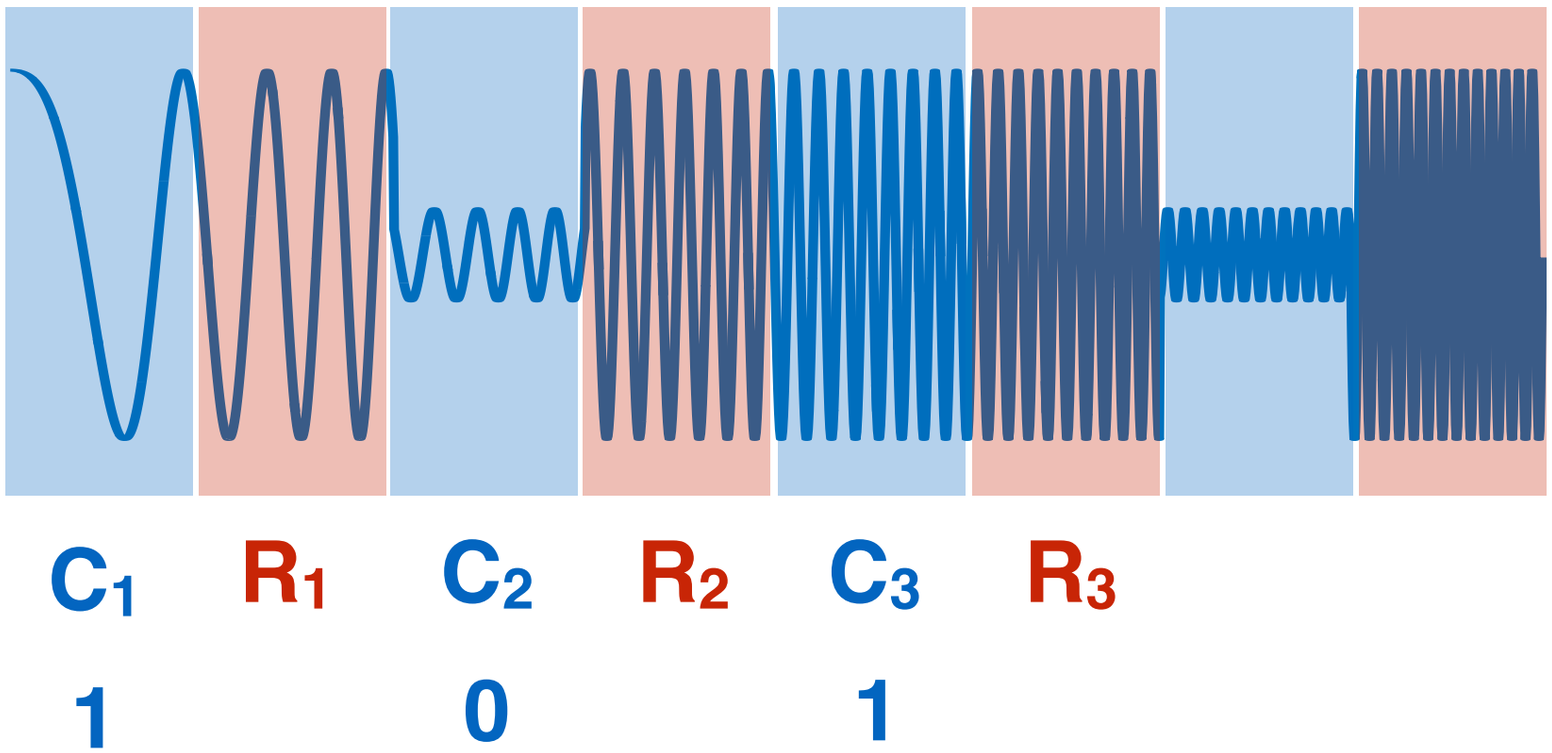


R={0,1,0,1}

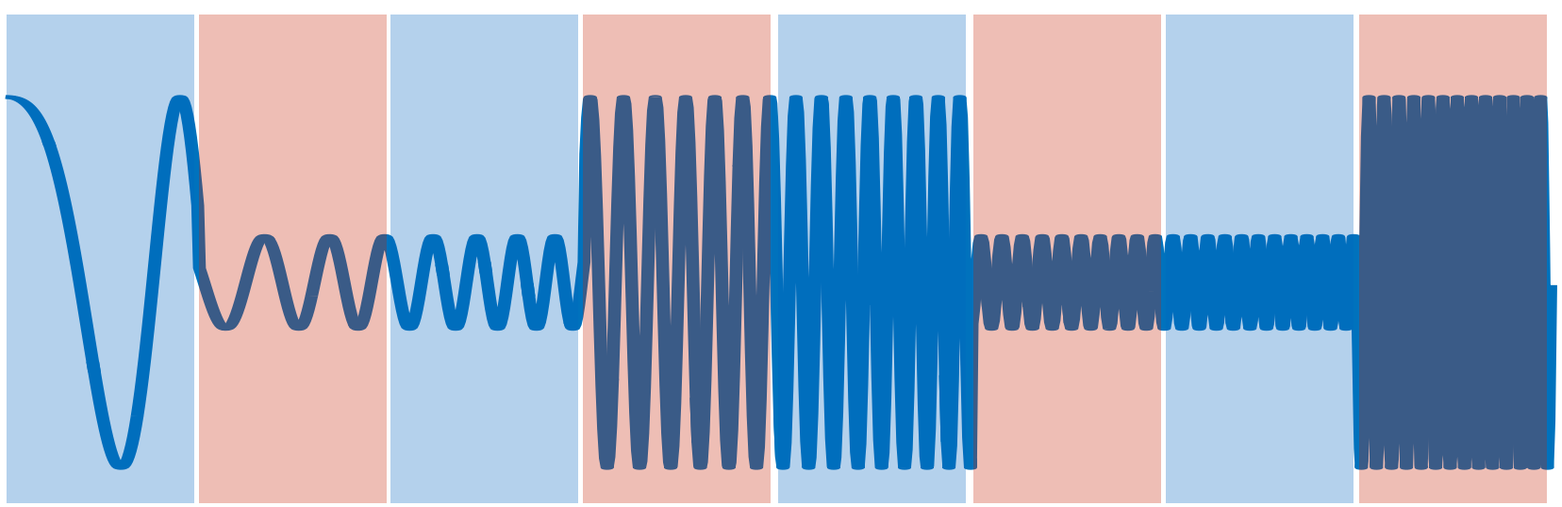


Example Challenge Response Slots

C={1,0,1,0}

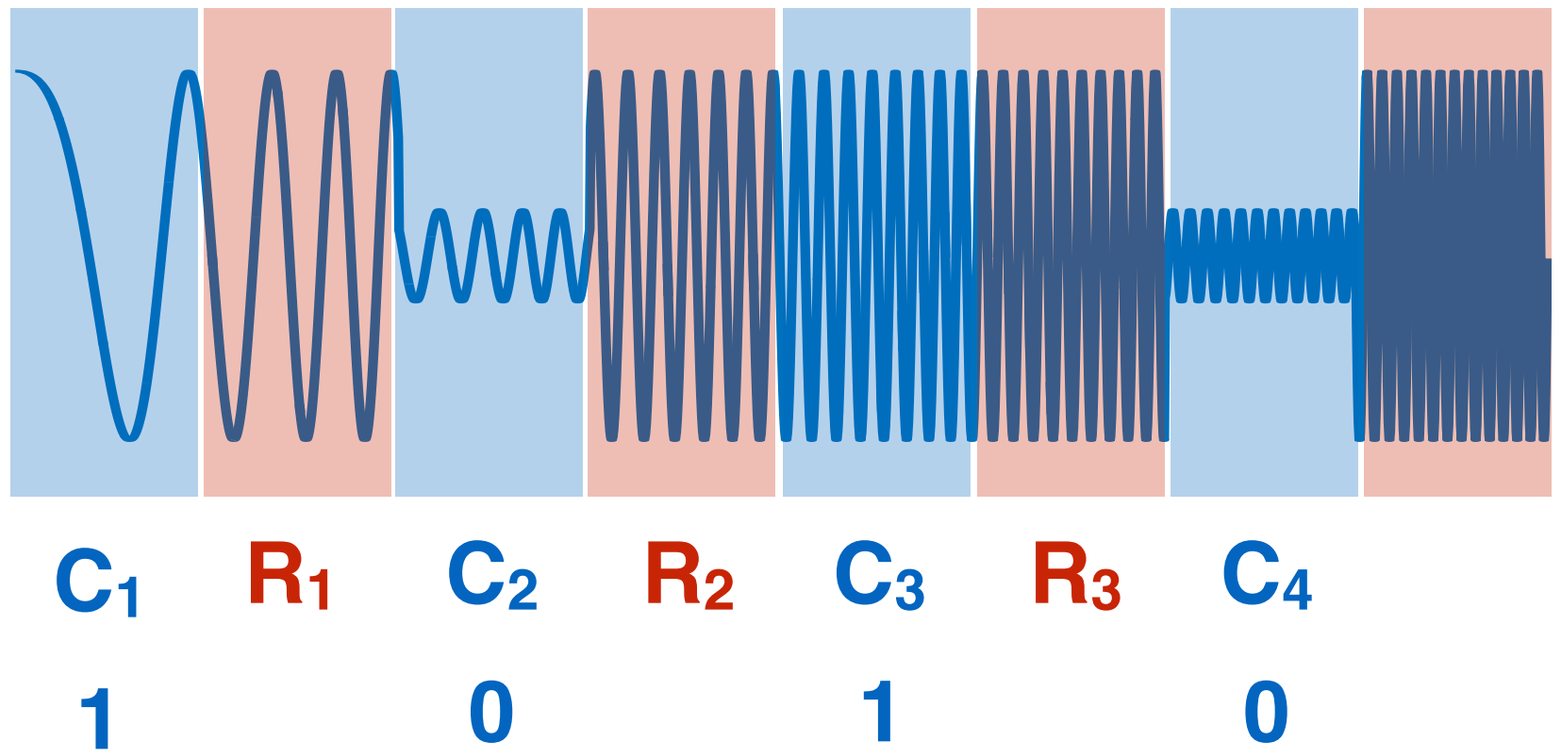


R={0,1,0,1}

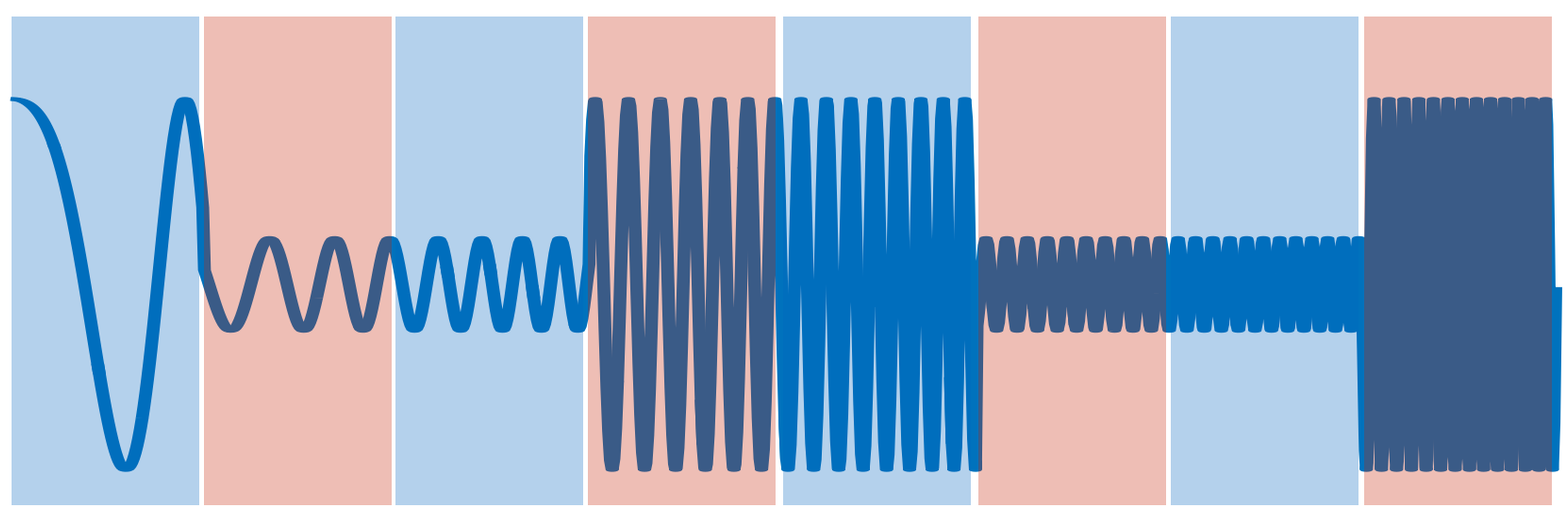


Example Challenge Response Slots

C={1,0,1,0}

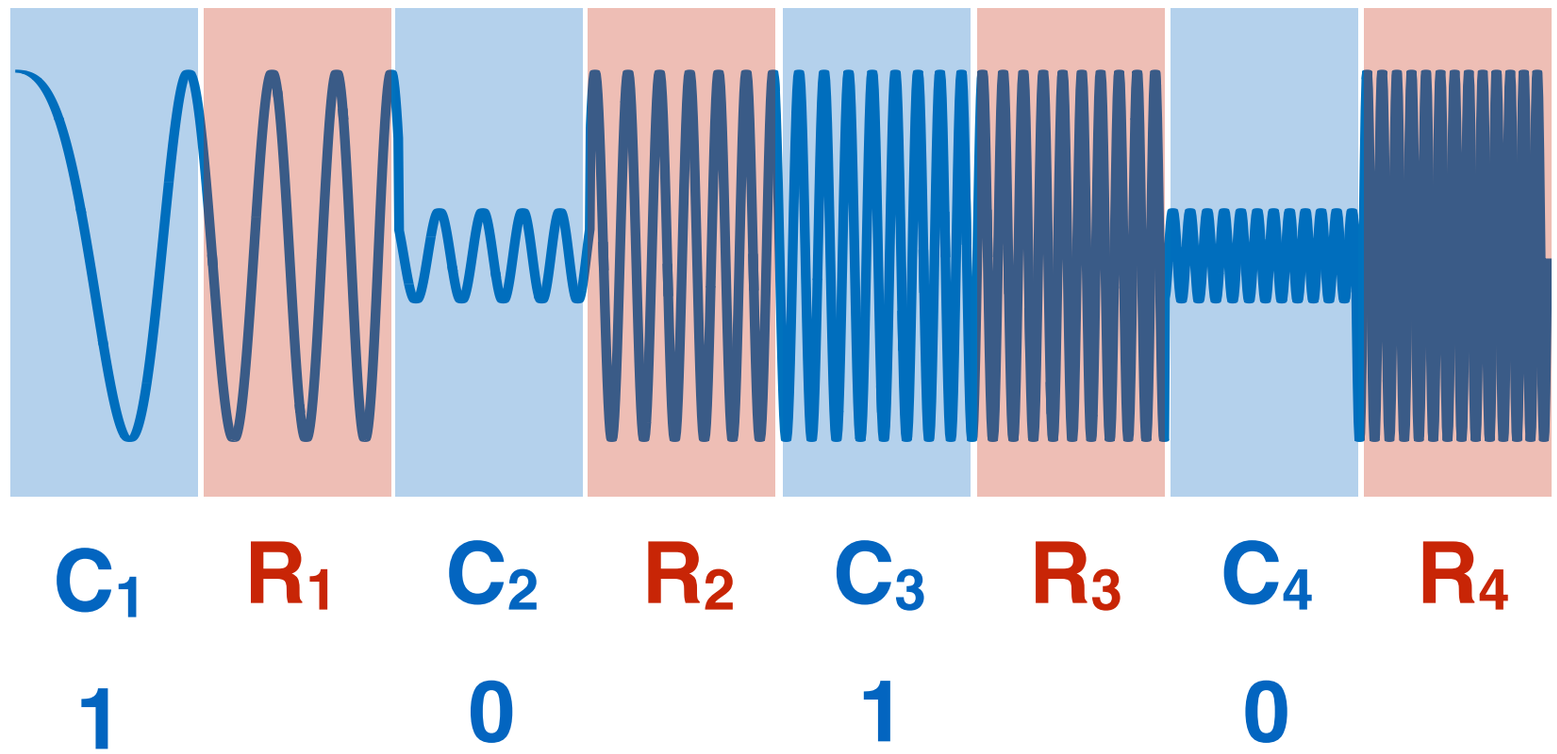


R={0,1,0,1}

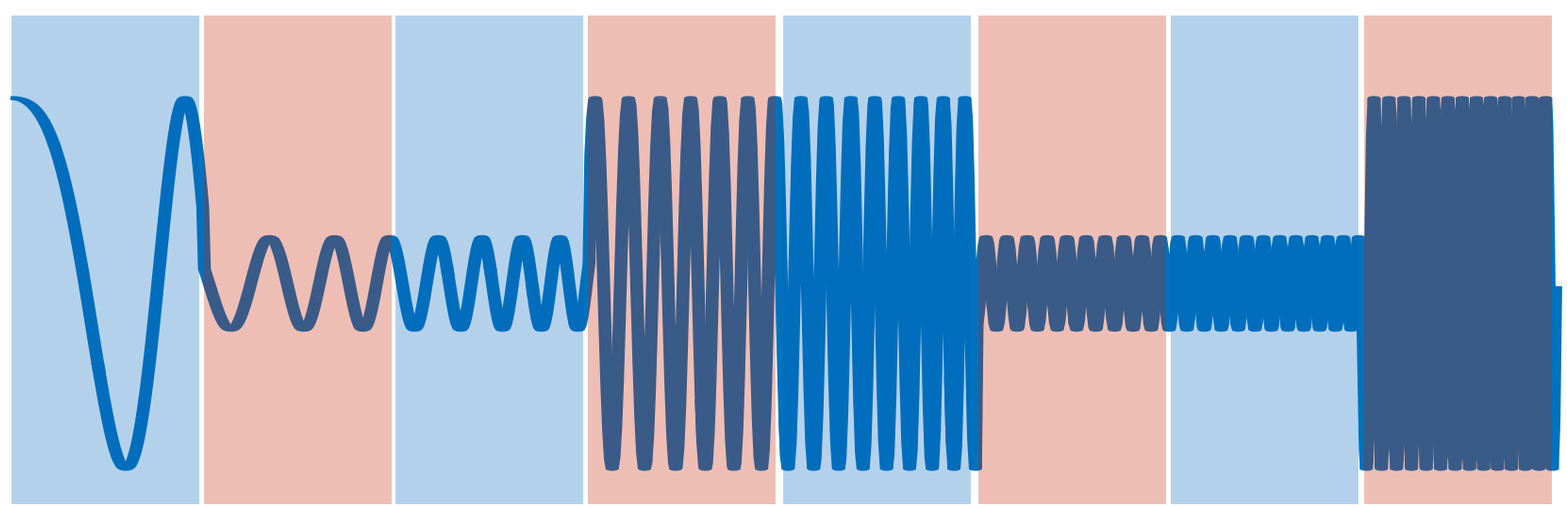


Example Challenge Response Slots

C={1,0,1,0}

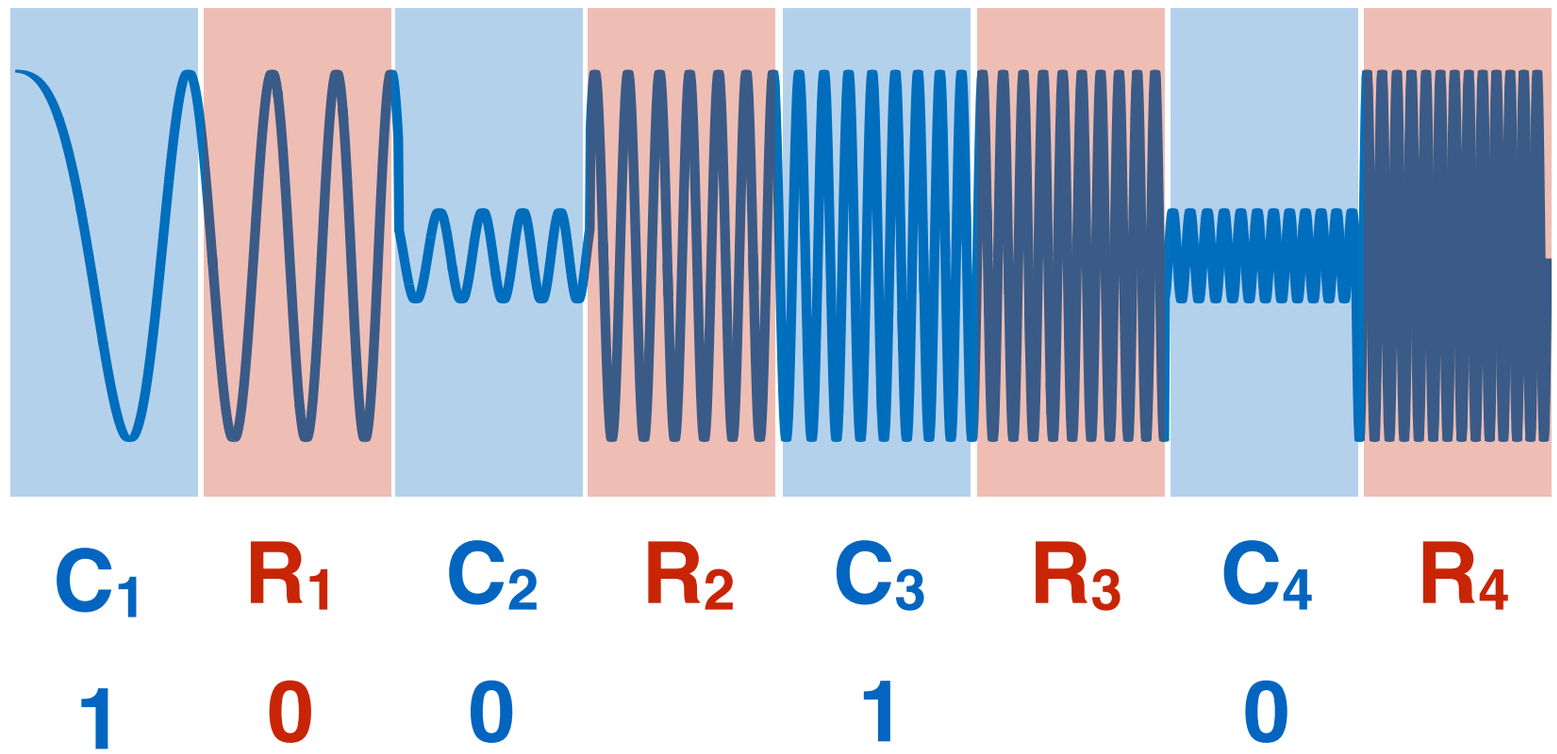


R={0,1,0,1}

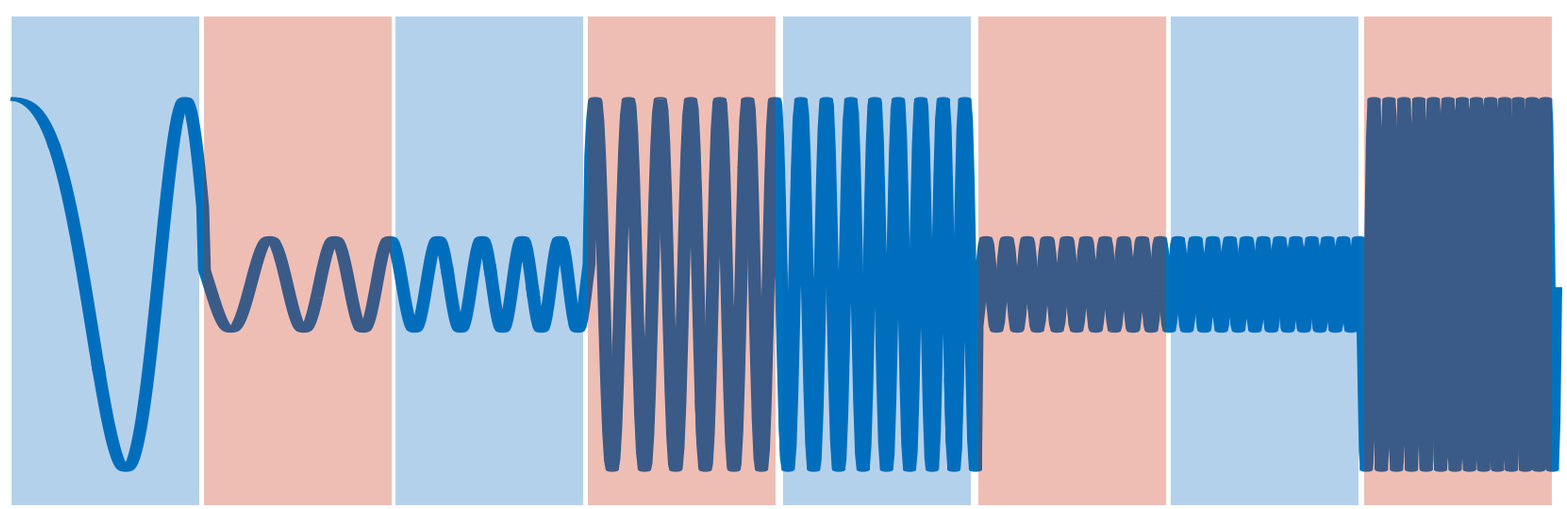


Example Challenge Response Slots

C={1,0,1,0}

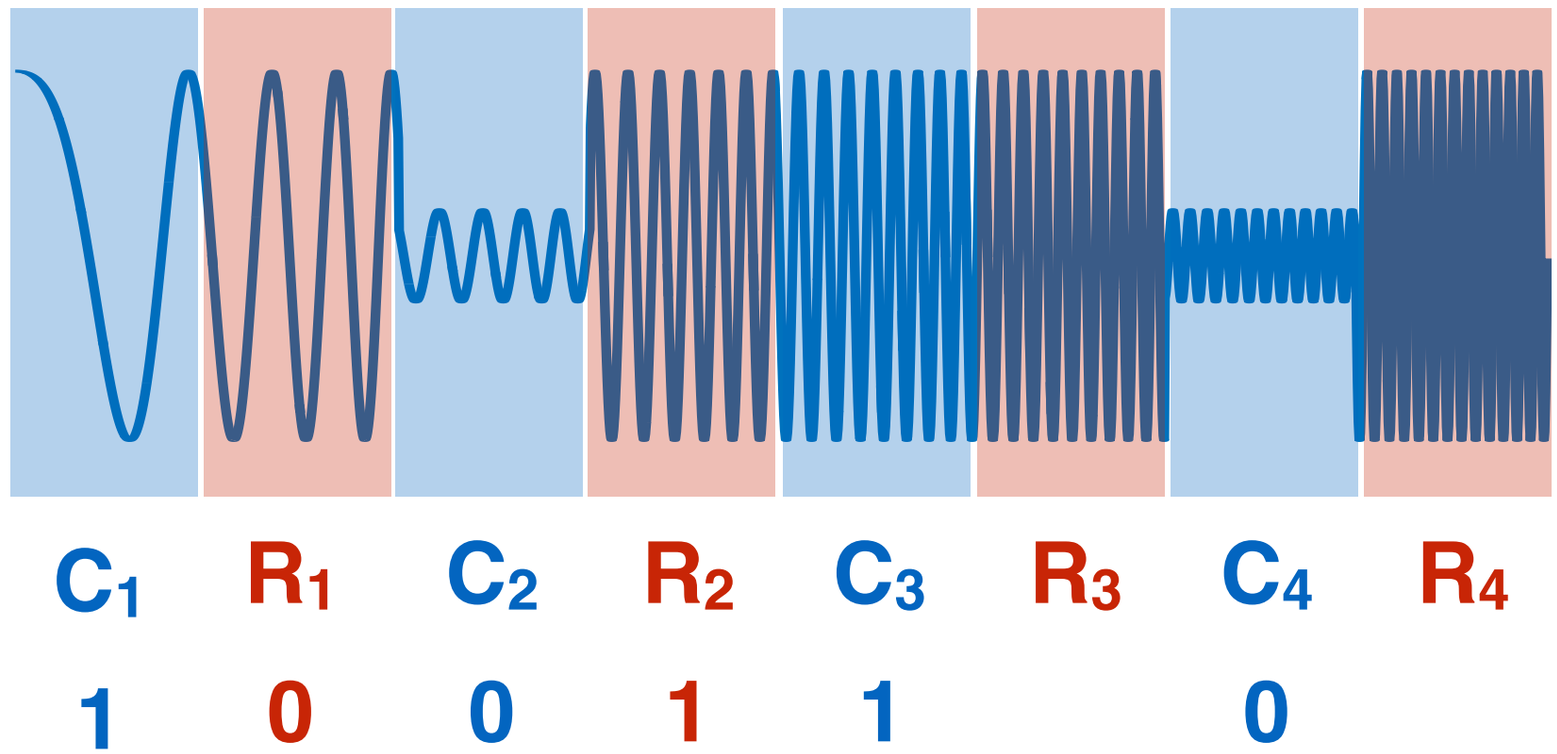


R={0,1,0,1}

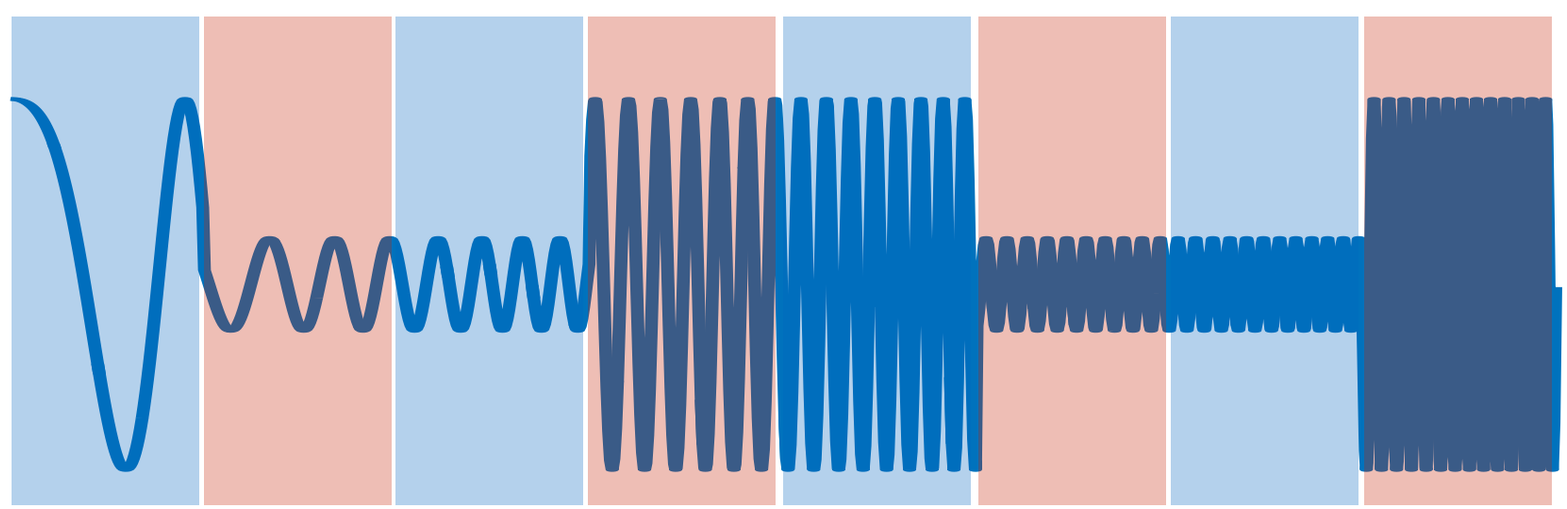


Example Challenge Response Slots

C={1,0,1,0}

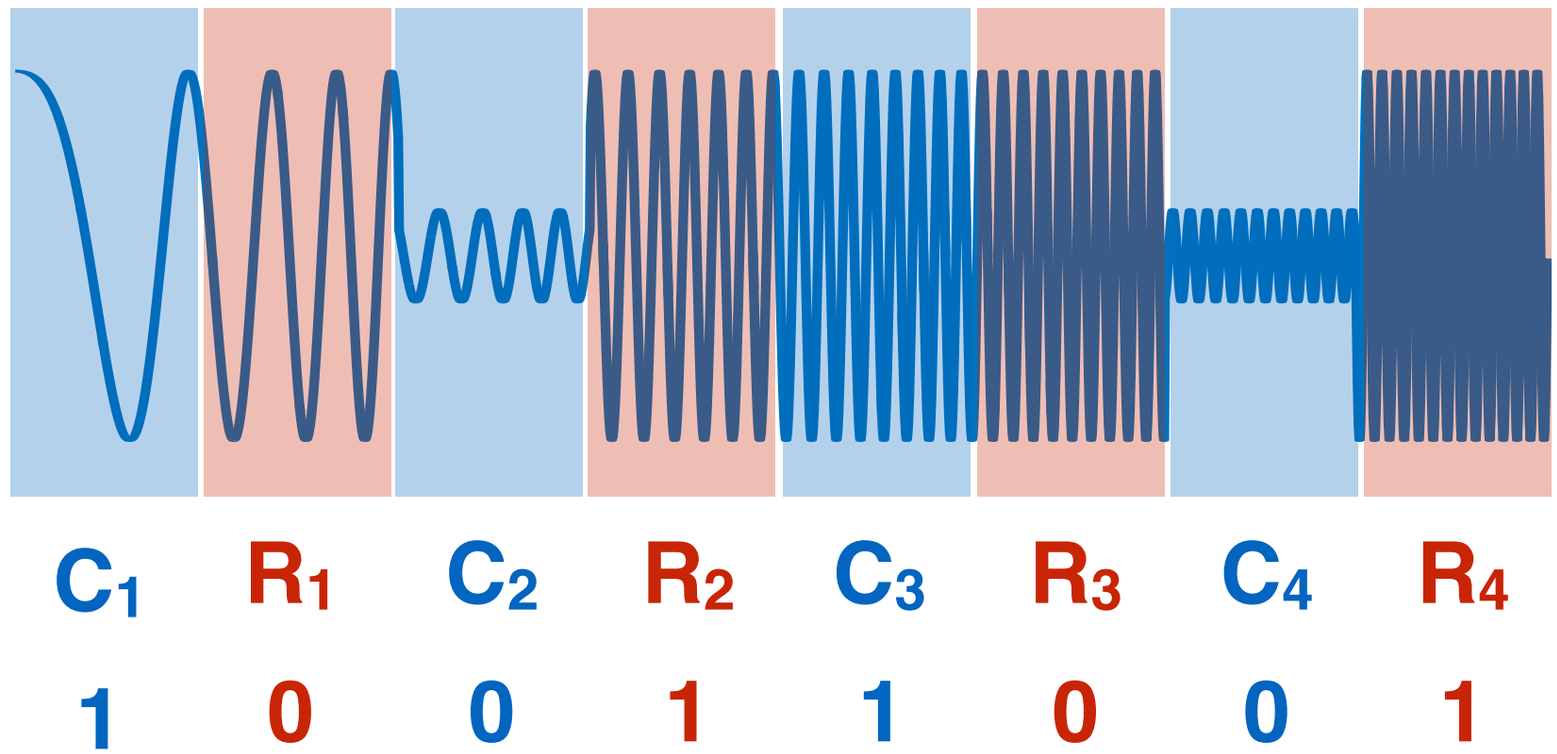


R={0,1,0,1}

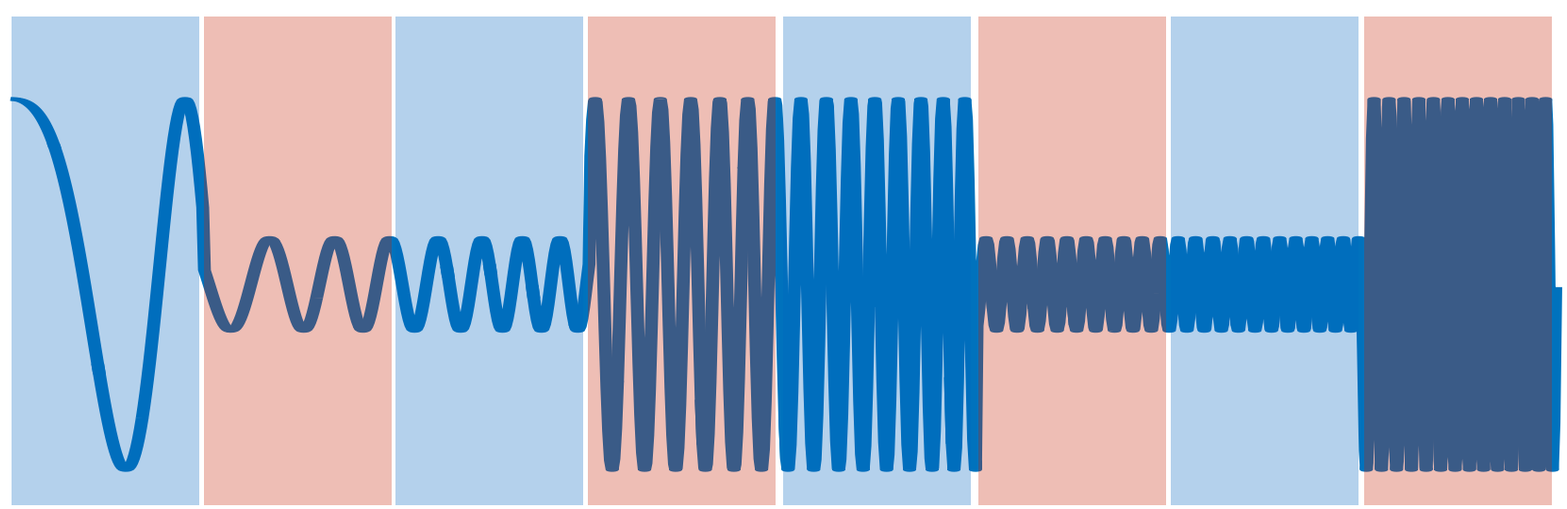


Example Challenge Response Slots

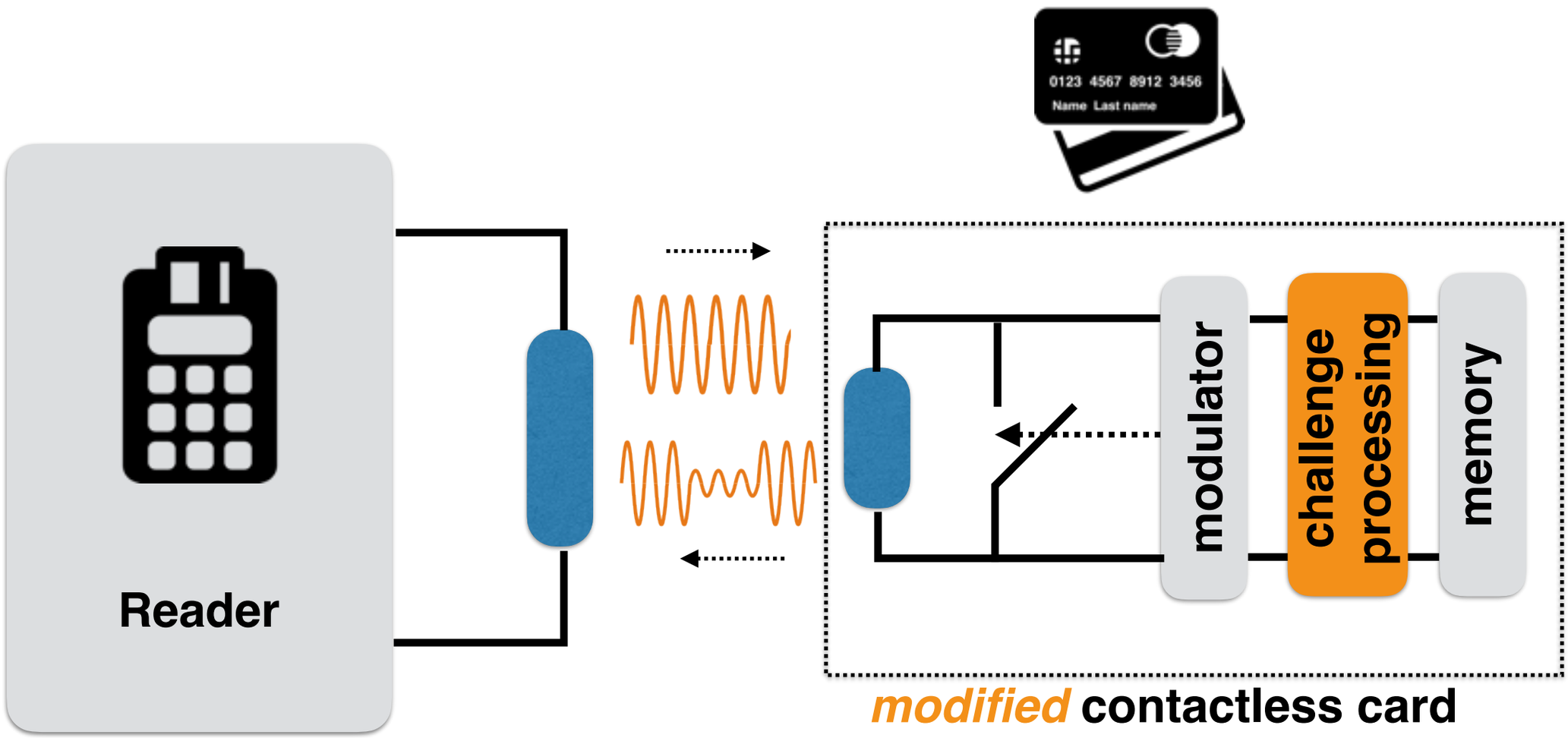
C={1,0,1,0}



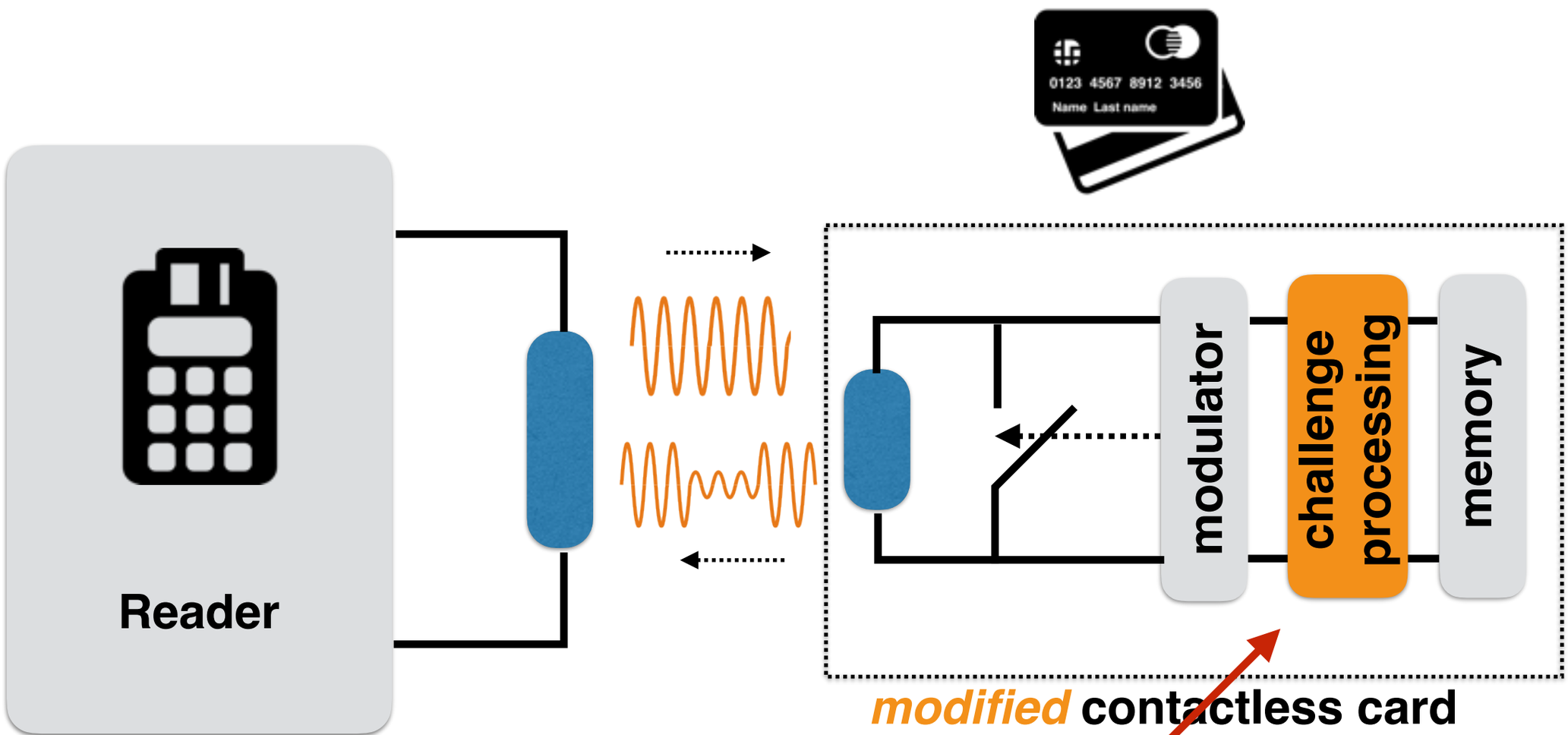
R={0,1,0,1}



Modifications to Contactless Cards



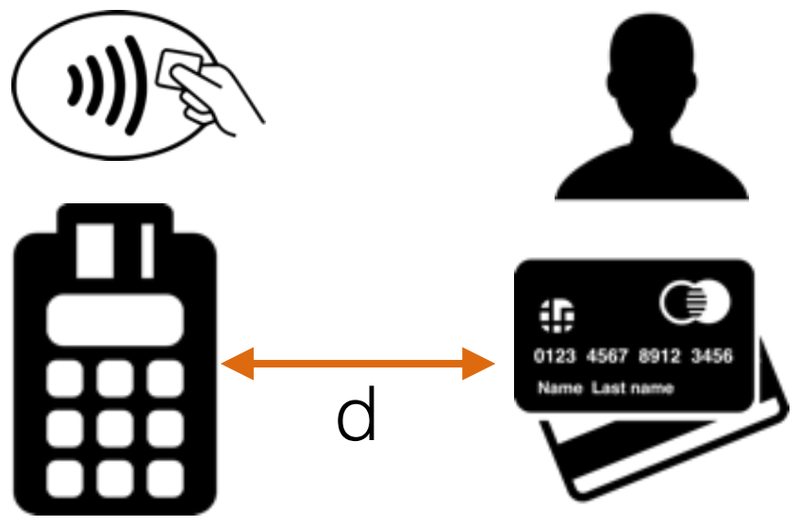
Modifications to Contactless Cards

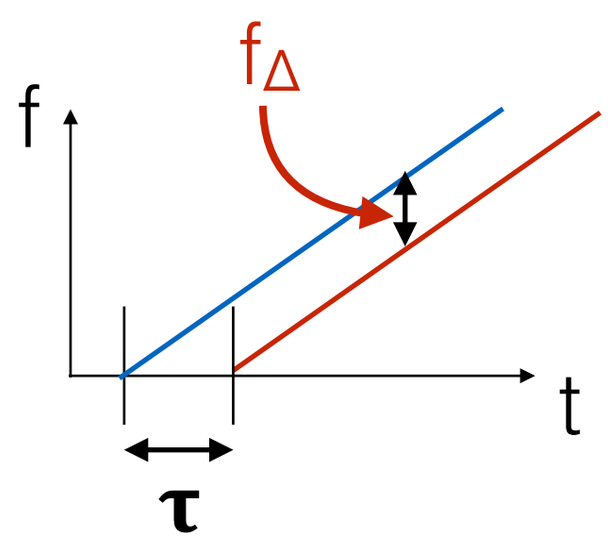


COTS energy detectors that consume less than 3 mA

Resilience against Relay Attacks

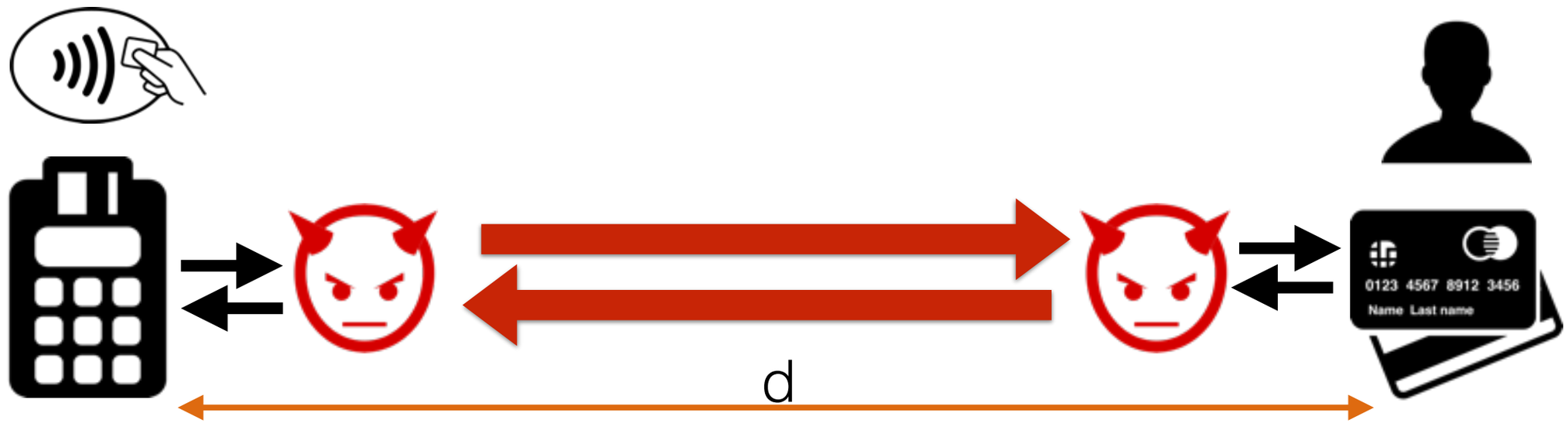
- Conventional Amplify & Forward

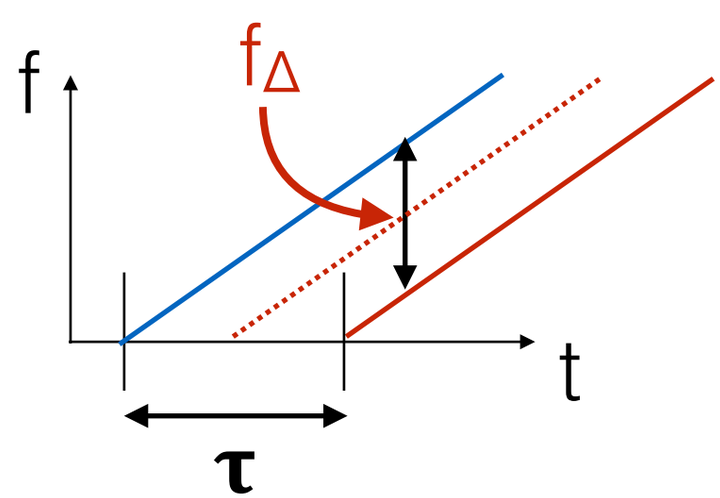




Resilience against Relay Attacks

- Conventional Amplify & Forward





Early Detect & Late Commit Attacks

* Clulow, Jolyon, et al. "So near and yet so far: Distance-bounding attacks in wireless networks." *Security and Privacy in Ad-Hoc and Sensor Networks*. 2006.

Early Detect & Late Commit Attacks

- **Early Detect:** Attacker tries to predict the bit before receiving all the signal samples

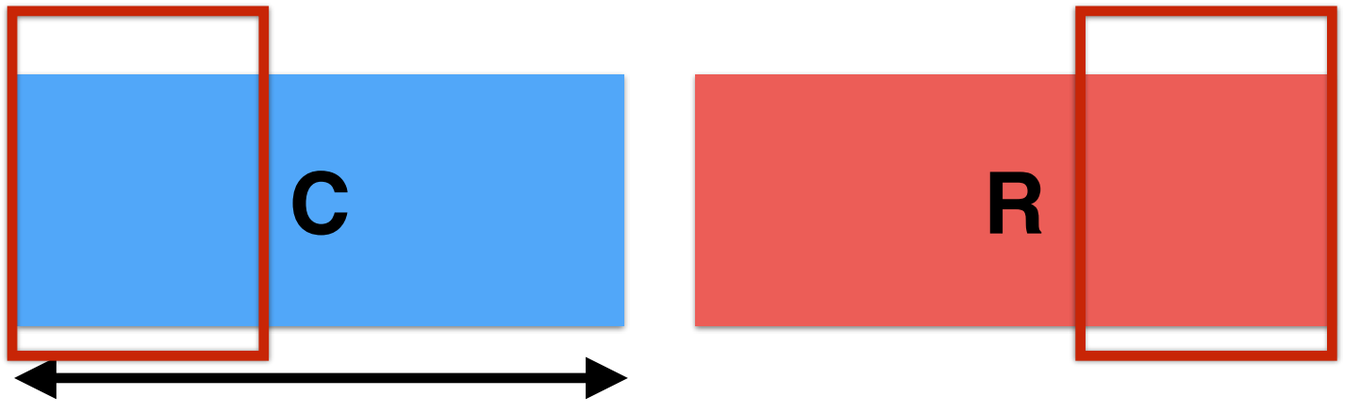
* Clulow, Jolyon, et al. "So near and yet so far: Distance-bounding attacks in wireless networks." *Security and Privacy in Ad-Hoc and Sensor Networks*. 2006.

Early Detect & Late Commit Attacks

- **Early Detect:** Attacker tries to predict the bit before receiving all the signal samples
- **Late Commit:** Leverages the ability of a receiver to decode the bit even though all the samples are not correct

* **Clulow, Jolyon, et al. "So near and yet so far: Distance-bounding attacks in wireless networks." *Security and Privacy in Ad-Hoc and Sensor Networks*. 2006.**

Early Detect & Late Commit Attacks



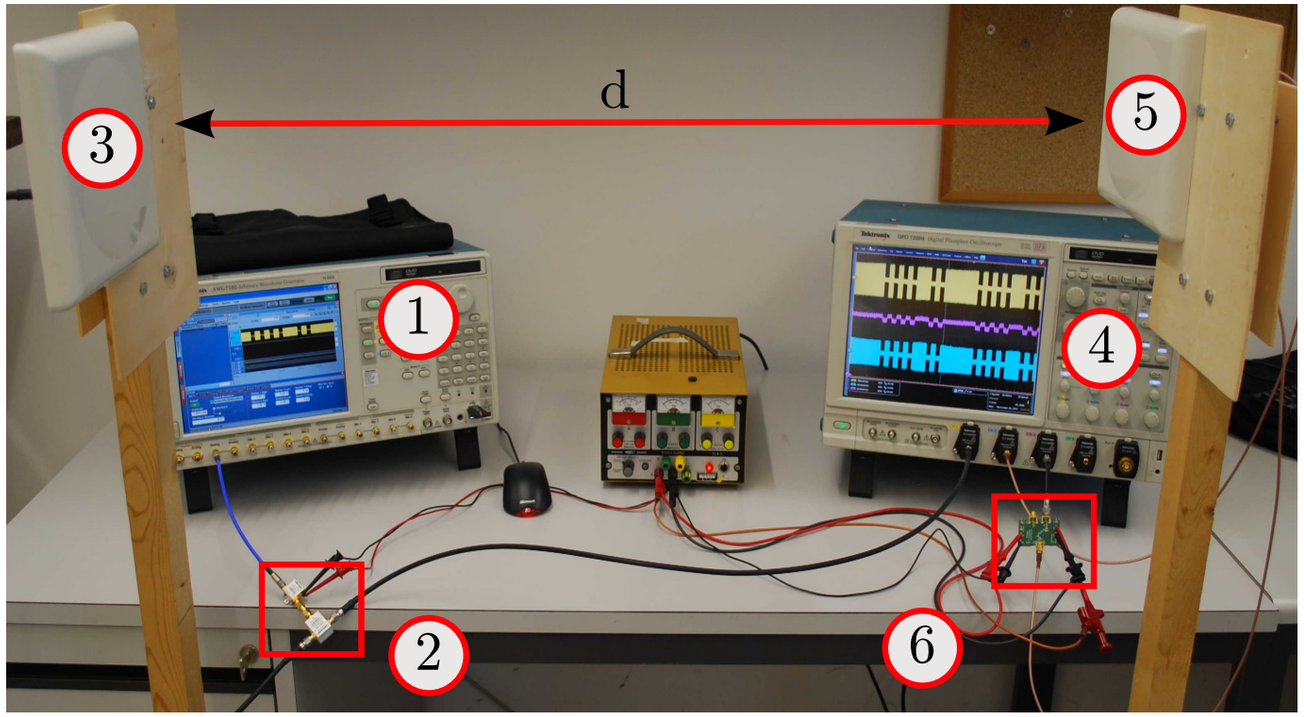
- **Early Detect:** Attacker tries to predict the bit before receiving all the signal samples
- **Late Commit:** Leverages the ability of a receiver to decode the bit even though all the samples are not correct

Success of the attack depends on the length of each slot!

* Clulow, Jolyon, et al. "So near and yet so far: Distance-bounding attacks in wireless networks." *Security and Privacy in Ad-Hoc and Sensor Networks*. 2006.

Experimental Setup

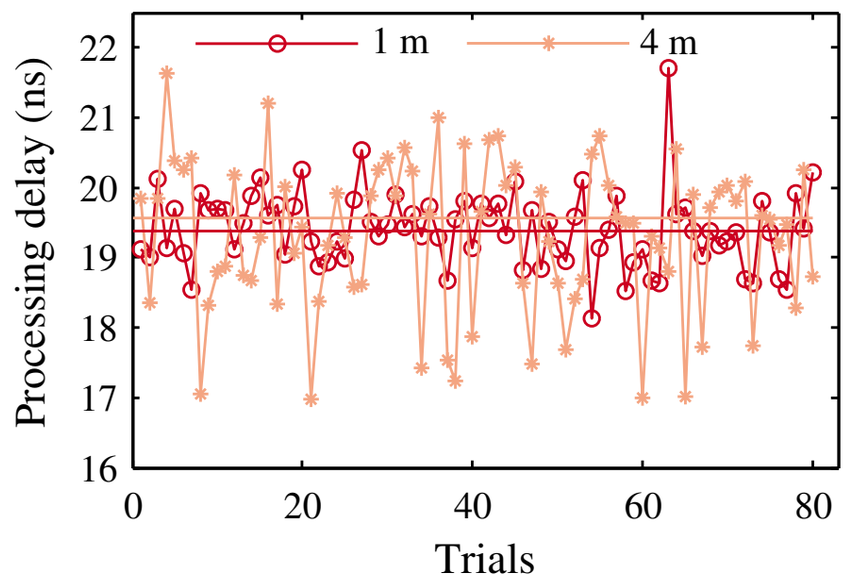
- Focus on two key parameters
    1. Challenge processing delay
    2. Ranging precision



1. Slotted chirp signal Gen
2. Amplifier
3. Tx antenna
4. Storage Oscilloscope
5. Rx Antenna
6. Challenge demodulator

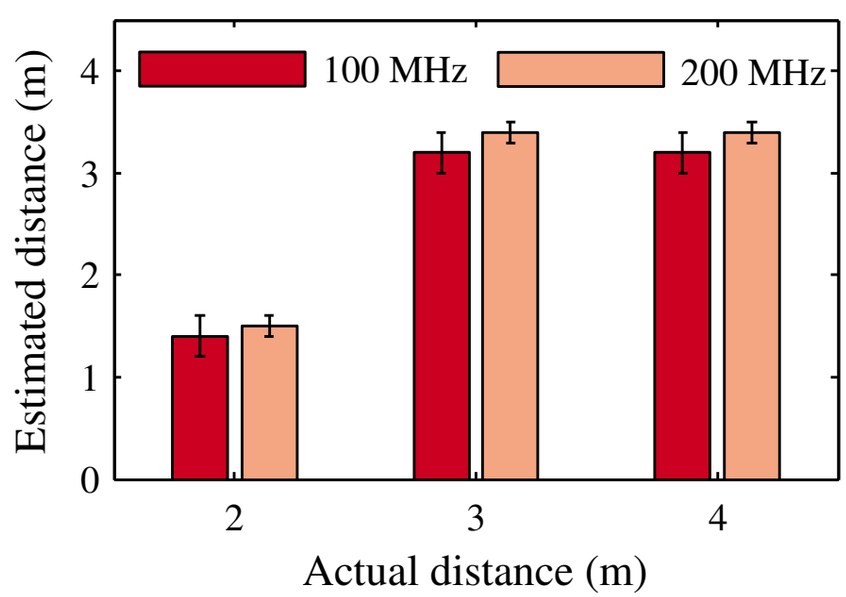
Experimental Results

Challenge processing delay



Slot length of 50 ns is very much feasible!

Ranging Precision



Ranging precision of ~ 1.5 m

Summary

Summary

- Our work makes a first step towards realizing a secure proximity verification system in which the prover can be fully-passive

Summary

- Our work makes a first step towards realizing a secure proximity verification system in which the prover can be fully-passive
- We leveraged backscatter communication technique for data exchange and Frequency Modulated Continuous Wave (FMCW) for distance measurement

Summary

- Our work makes a first step towards realizing a secure proximity verification system in which the prover can be fully-passive
- We leveraged backscatter communication technique for data exchange and Frequency Modulated Continuous Wave (FMCW) for distance measurement
- We showed that our system is resilient against conventional amplify and forward relay attacks as well as stronger early detect & late commit attacks.

Summary

- Our work makes a first step towards realizing a secure proximity verification system in which the prover can be fully-passive
- We leveraged backscatter communication technique for data exchange and Frequency Modulated Continuous Wave (FMCW) for distance measurement
- We showed that our system is resilient against conventional amplify and forward relay attacks as well as stronger early detect & late commit attacks.

Thank You!

aanjhan@inf.ethz.ch