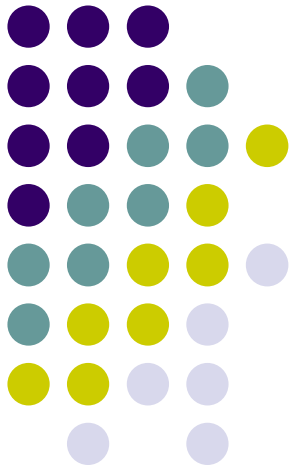
Security challenges in DNS

Philippe Camacho

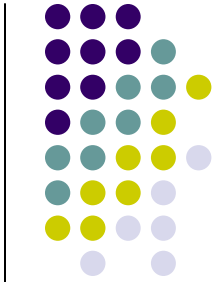
Department of Computer Science
University of Chile



Workshop on Formal Methods in Cryptography

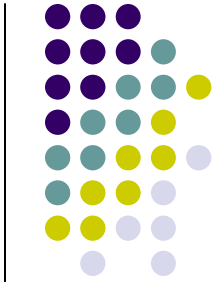
27-30 april 2009 / Campinas - Brazil

Outline



- DNS
- DNSSEC
  - Basics
  - Key Rollover
  - Problems and Limitations
- How to improve the Security of DNS?
  - Threshold Cryptography
  - Identity Based Cryptography

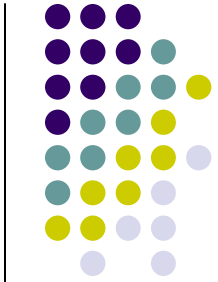
DNS
A (brief) history



- ARPANET in the 70's
  - Small, friendly network of a few hundreds of hosts.
  - A centralized HOSTS.TXT file was used to map host names to network adresses.
  - This file was updated once or twice a week.

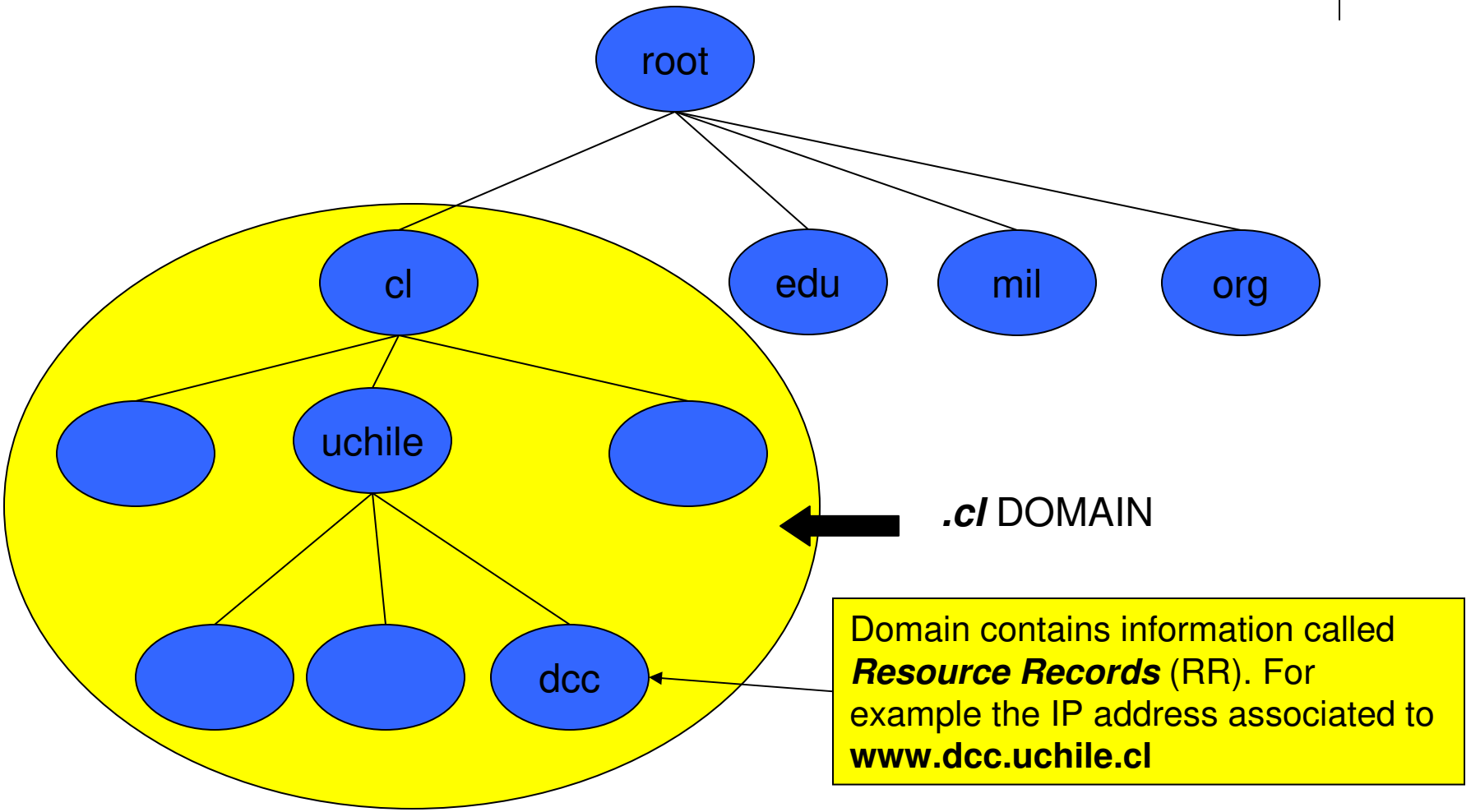
- BUT, with the growth of ARPANET this scheme became unpracticable
  - Traffic Load
  - Name Collision
  - Consistency

DNS Basics

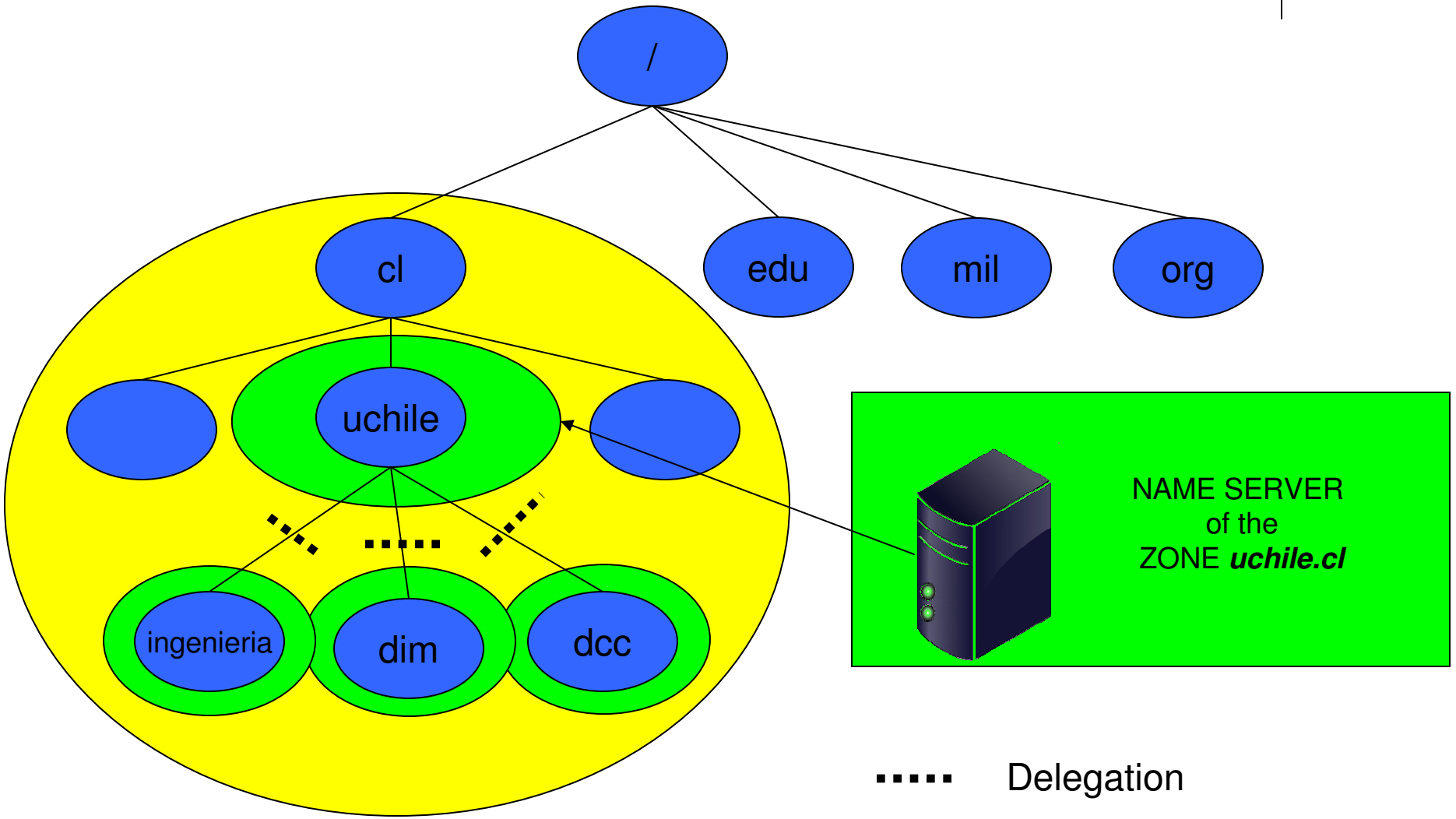


- Domain Name System (DNS)
  - Maps IP adresses to human friendly computer hostnames
    - www.google.com ⇔ 64.233.163.104
  - But also manages other type of information such as the list of mail servers associated to a domain
  - ***Distributed, Replicated, Fault Tolerant***
  - Developped by the IETF (Internet Engineering Task Force) at the beginning of 1980's

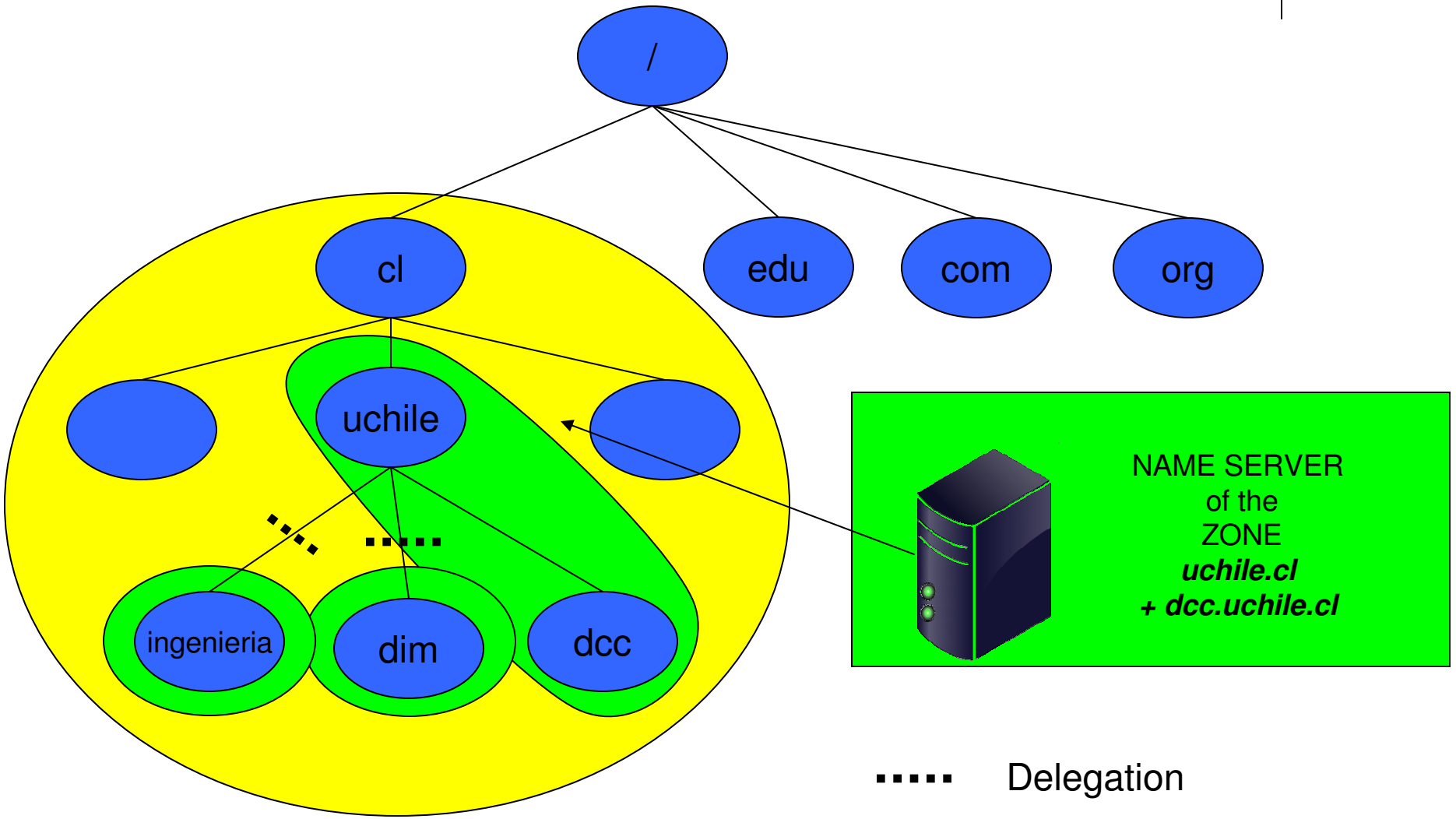
DNS
Domain Namespace



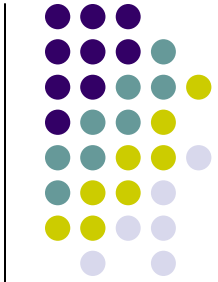
DNS
Name servers and Zones



DNS
Name servers and Zones



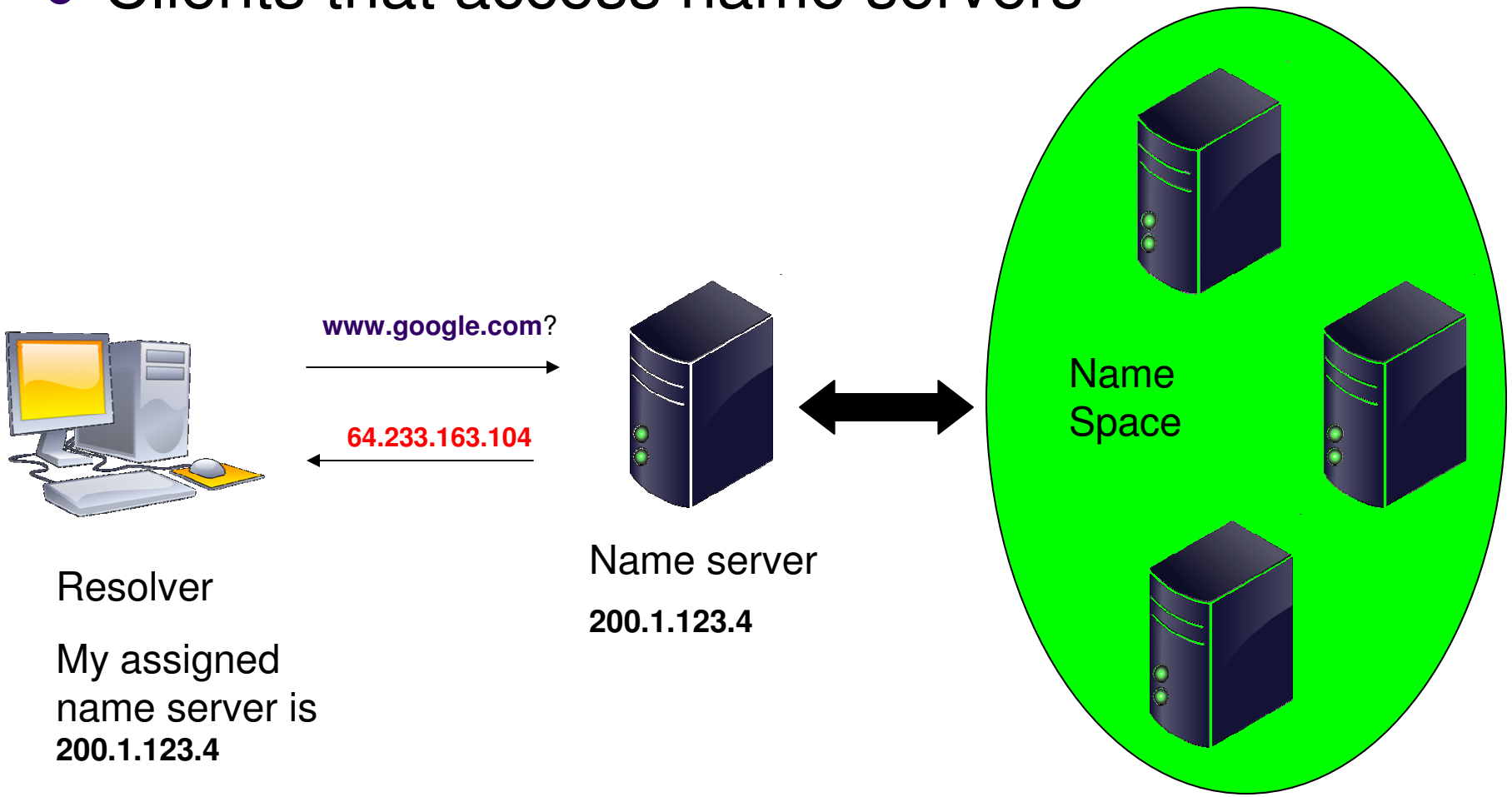
DNS
Type of Resource Records (RR)



A	Host Addresses
PTR	Reverse address name mapping
CNAME	Aliases
MX	Mail exchange for the domain
NS	Authoritative Name Servers

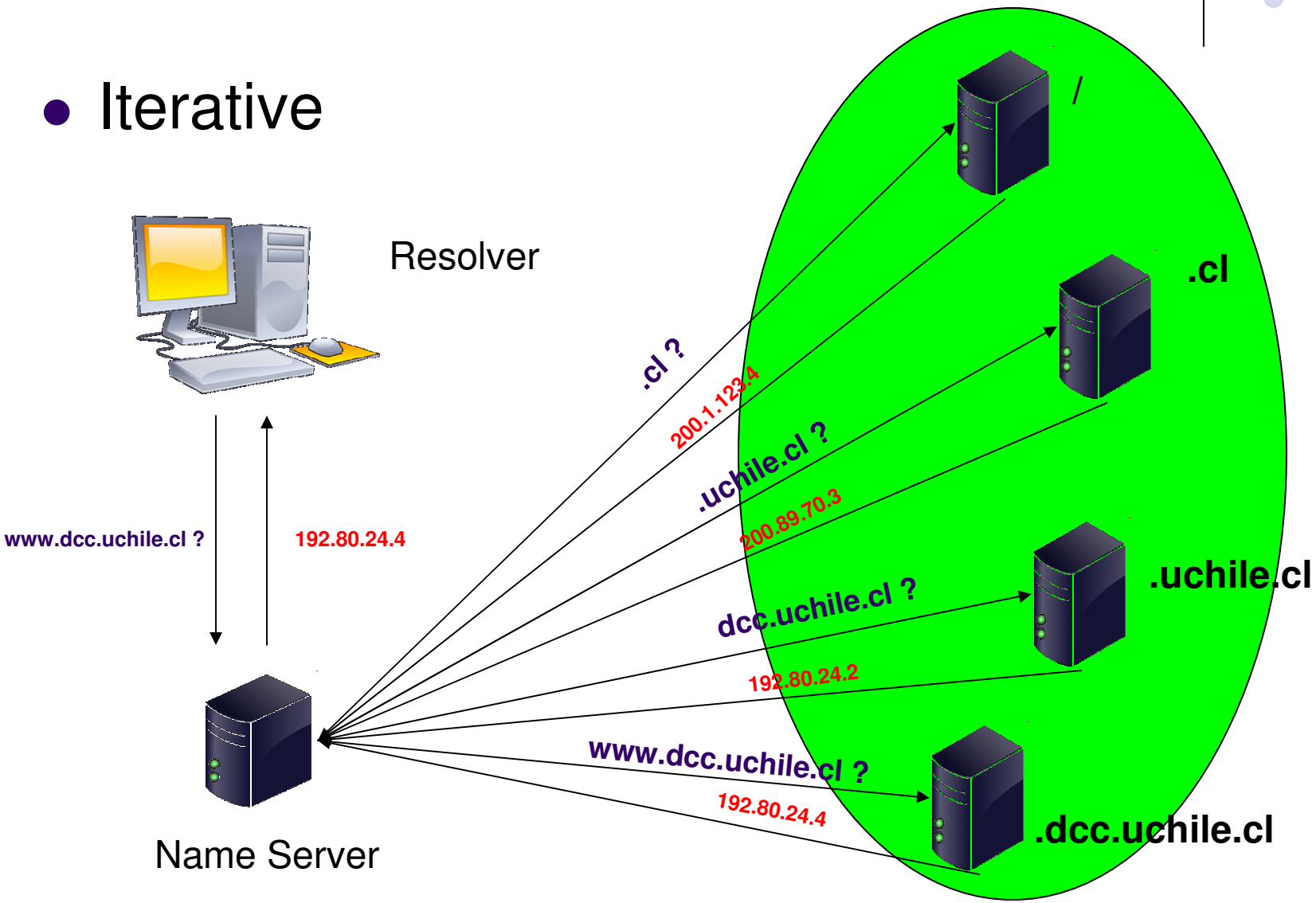
DNS
Resolvers and Name Resolution

- Clients that access name servers



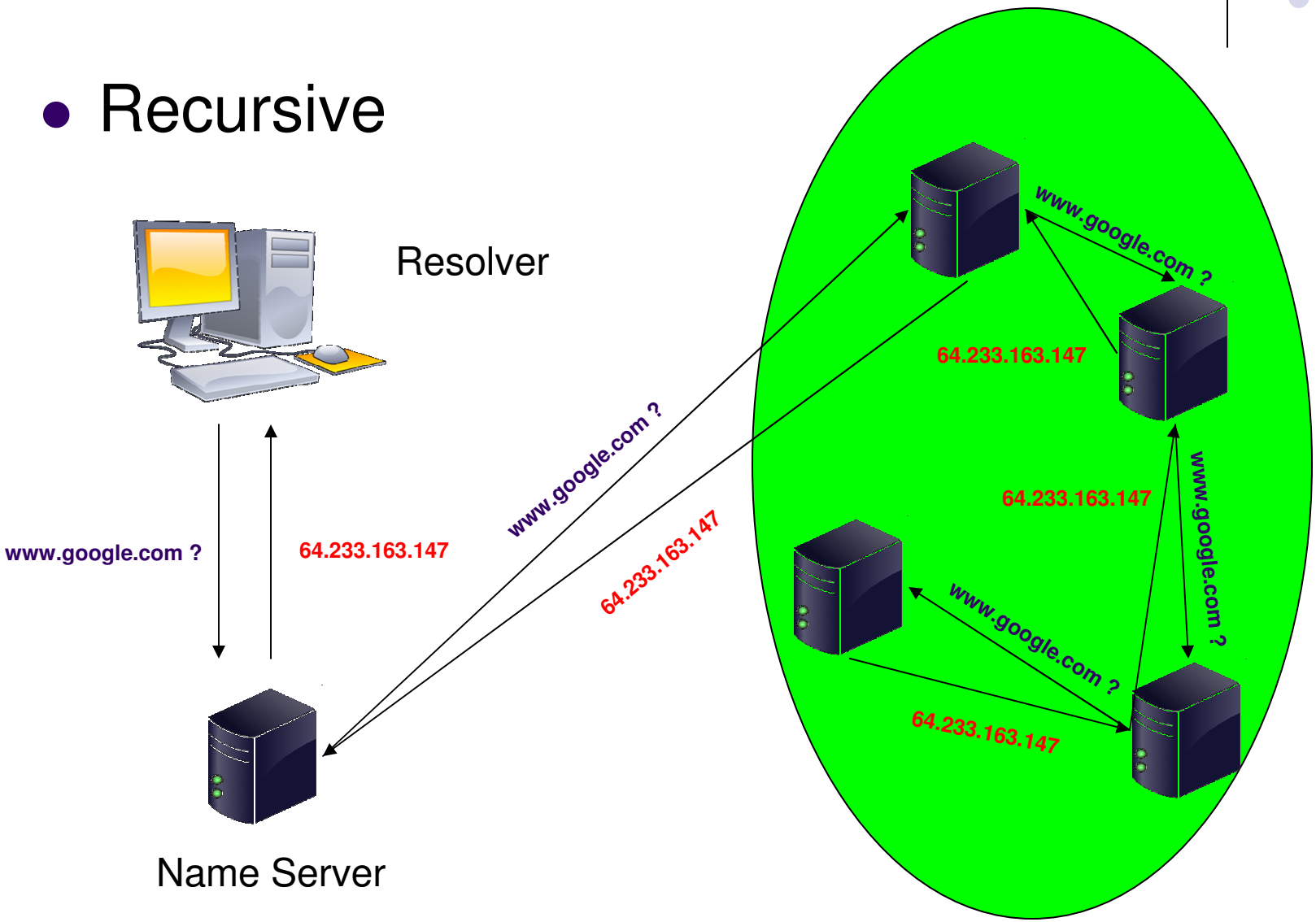
DNS
Resolving Algorithms

- Iterative

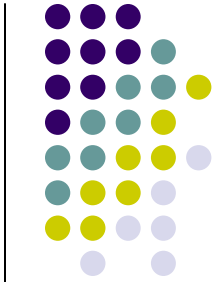


DNS
Resolving Algorithms

- Recursive



DNS Caching



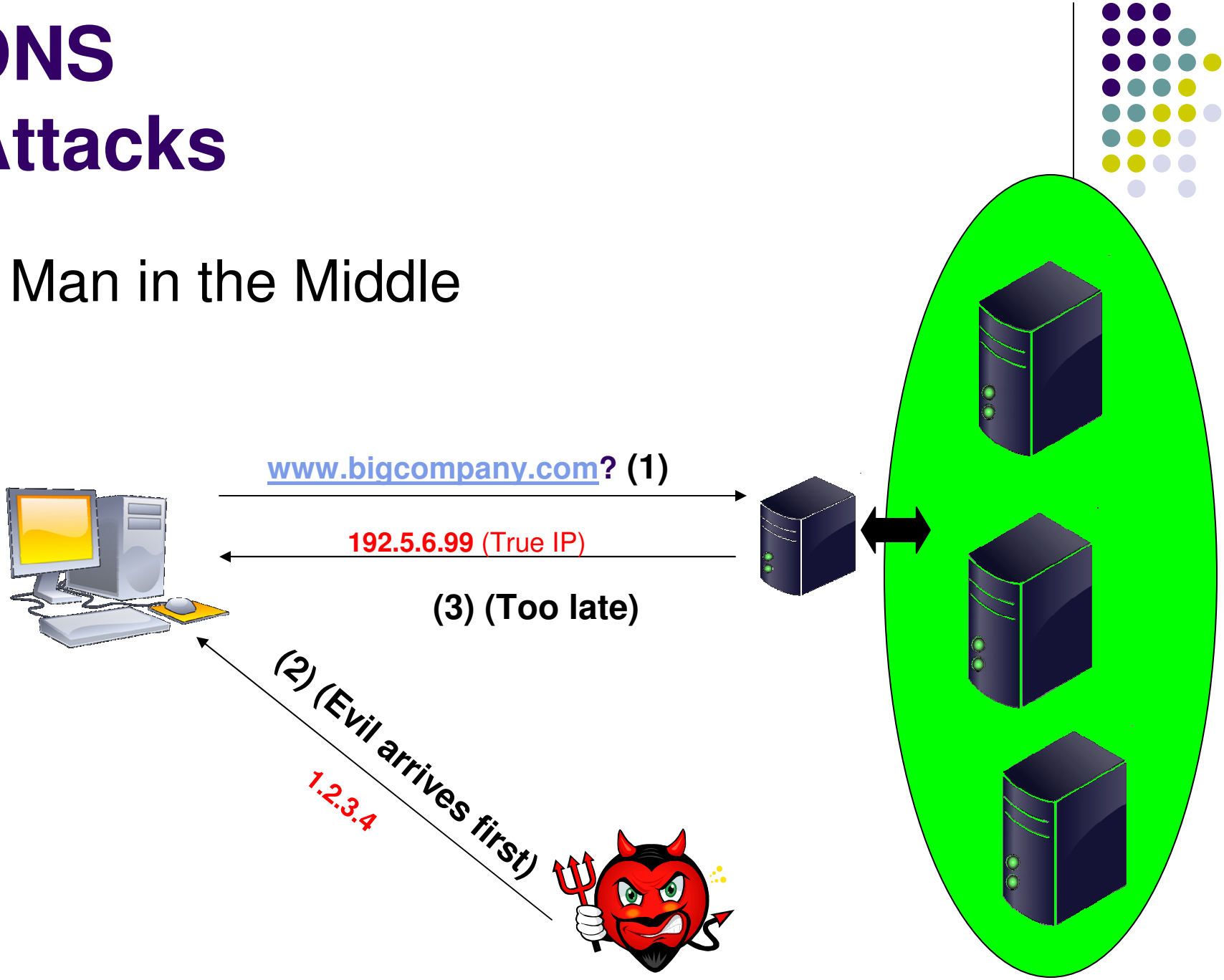
- DNS uses cache to improve performance
  - e.g: In the case of iterative resolving
    - What is the IP for www.dcc.uchile.cl?
    - I know the IP for the name server of the zone ***uchile.cl***.
    - I can ask this server directly without starting from the ***root***.
  - Time To Live (TTL)
    - Tradeoff between ***consistency*** and ***efficiency***

DNS Attacks

- Many attacks on the DNS (references)
  - Man in the Middle
  - Cache poisoning
  - (Distributed) Denial of Service
- Major problem
  - Lack of integrity / authenticity
- Consequences are **HUGE**
  - Phishing
  - Defacements
  - Internet is down

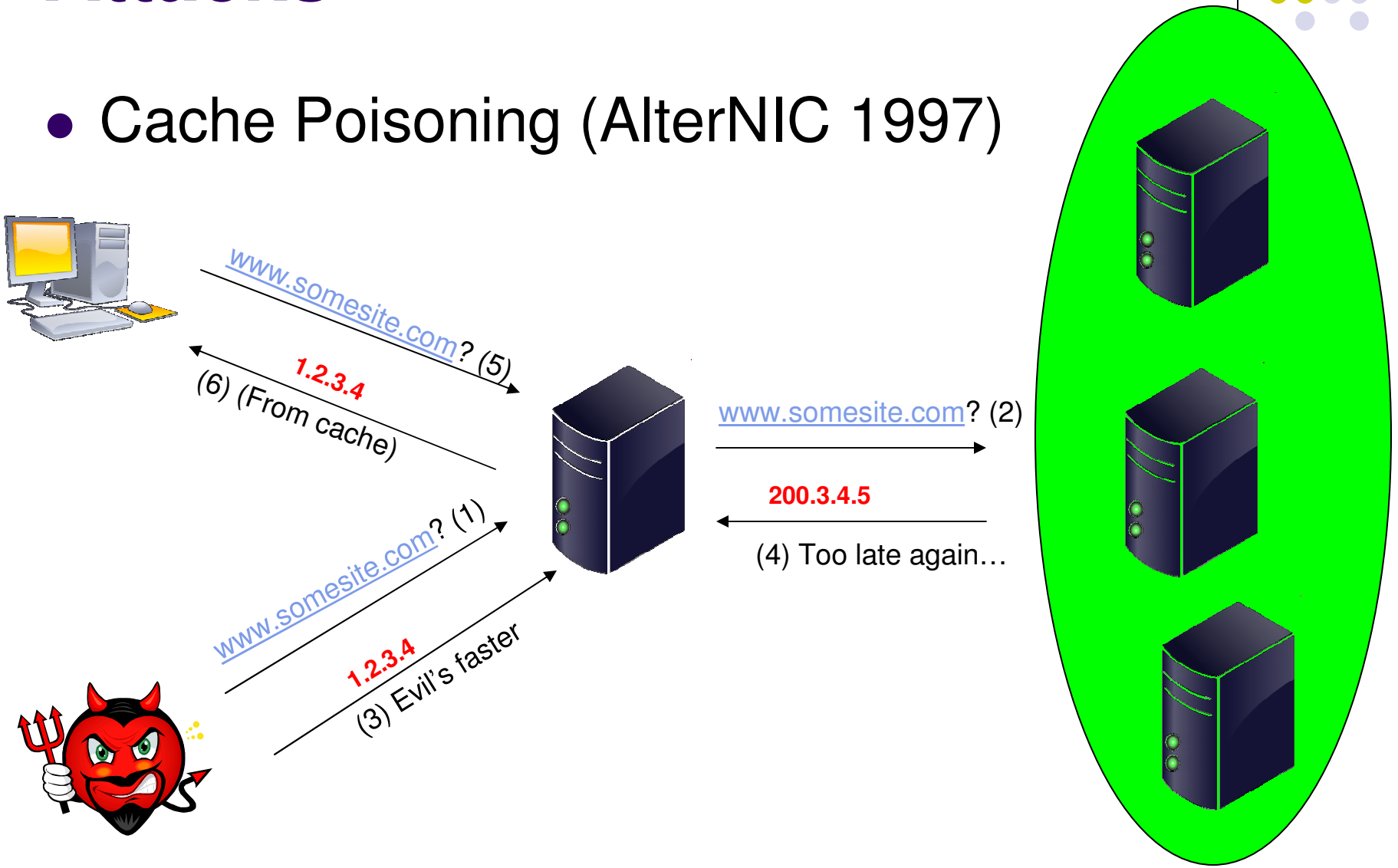
DNS Attacks

- Man in the Middle

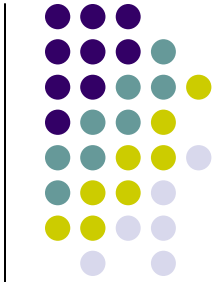


DNS Attacks

- Cache Poisoning (AlterNIC 1997)



DNS Attacks



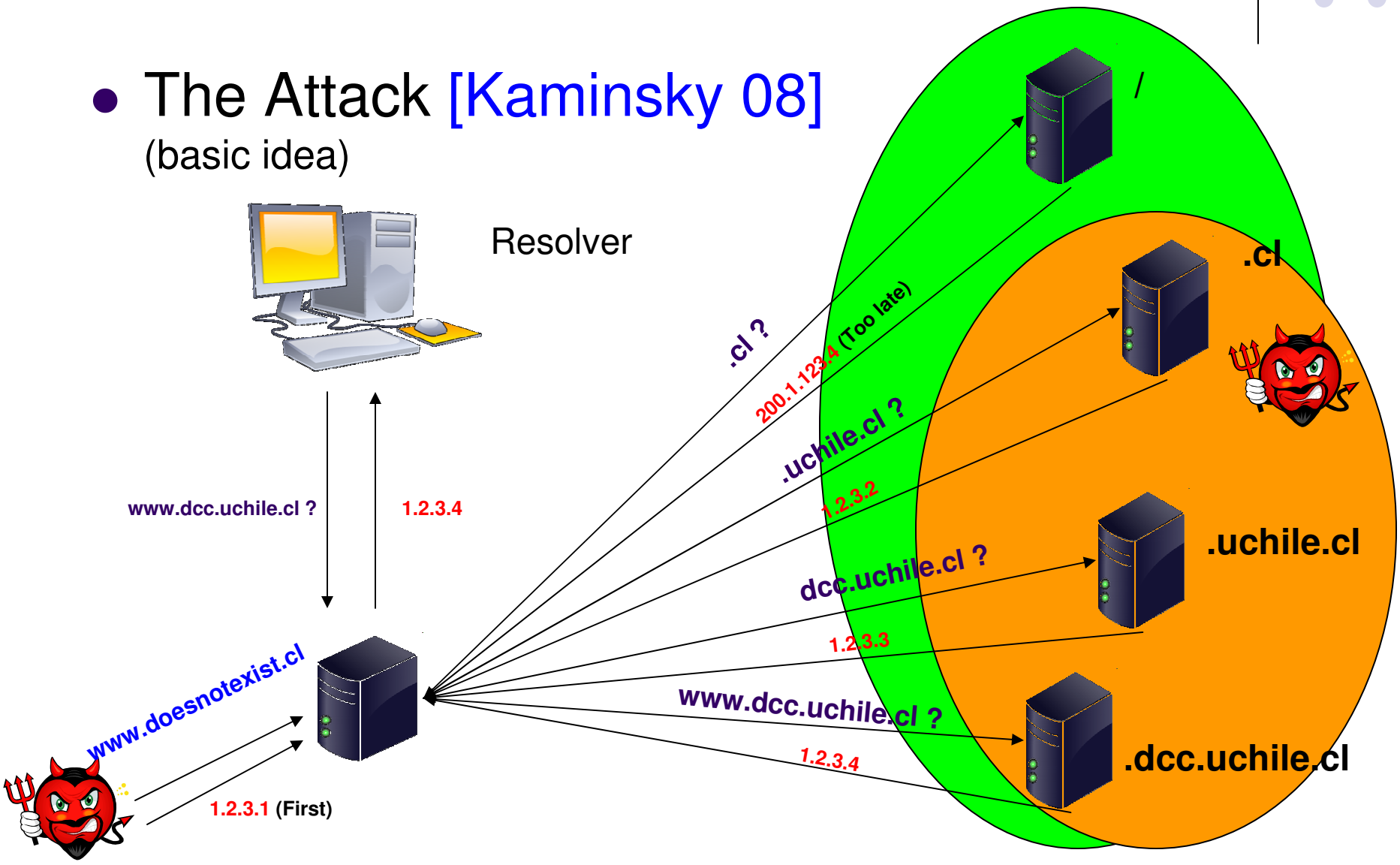
- (Distributed) Denial of Service
  - Such as every internet service, DNS is exposed to (D)DoS
  - However the specificity of the protocol allows ***amplification attacks***
  - (D)DoS is really hard to avoid
    - As we shall see DNSSEC do not pretend to solve this problem and could possibly make it worse…

DNS Attacks

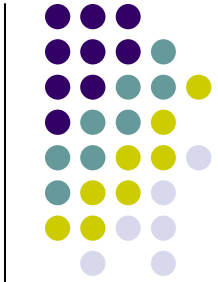
- A new attack [Kaminsky 08]
  - Presented at Black Hat 2008
  - Previous attack only allows to forge only **one (url,ip)** mapping.
  - Kaminsky's attack is far more devastating
    - Allows to control a **whole domain** (.cl)
  - This is scary…
    - Many certificate authorities validate a user's certificate by sending an email… So in this case even SSL is useless!

DNS Attacks

- The Attack [Kaminsky 08]
  (basic idea)

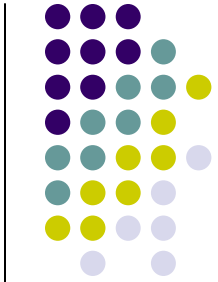


DNSSEC Basics



- What it is for?
  - **Authenticate** data exchanged between the participants of the protocol
- What it is NOT for?
  - Guarantee **privacy** (except for NSEC3)
  - Ensure **availability**

DNSSEC Basics

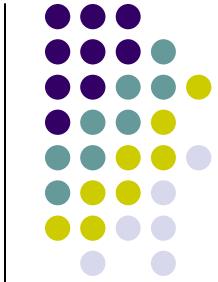


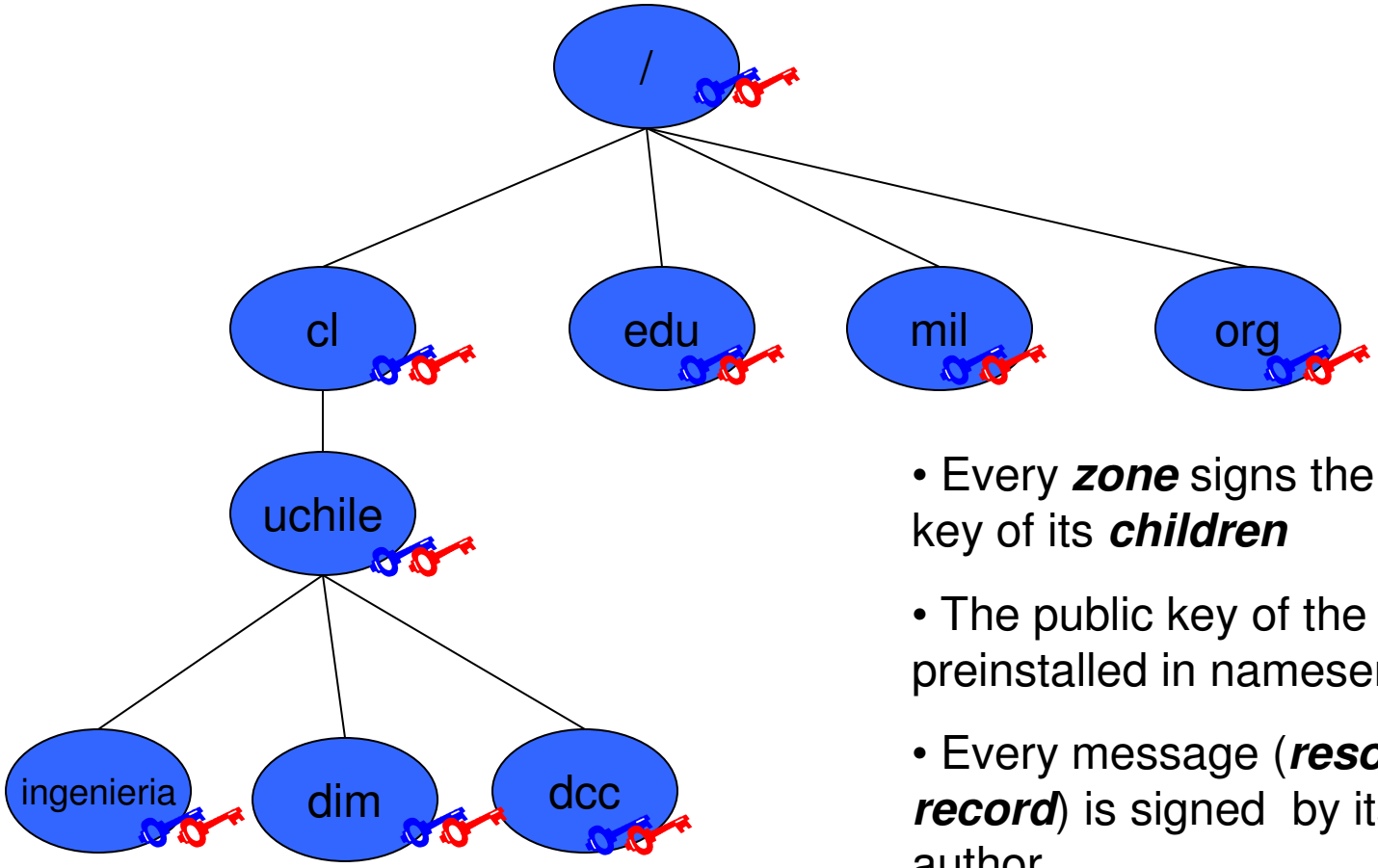
- Core RFCs that describe DNSSEC
  - DNS Security Introduction and Requirements (4033)
  - Resource Records for the DNS Security Extensions (4034)
  - Protocol Modifications for the DNS Security Extensions (4035)

- Another important RFC
  - DNSSEC Operational Practices (4641)

- Web
  - http://www.dnssec.net

DNSSEC Basics

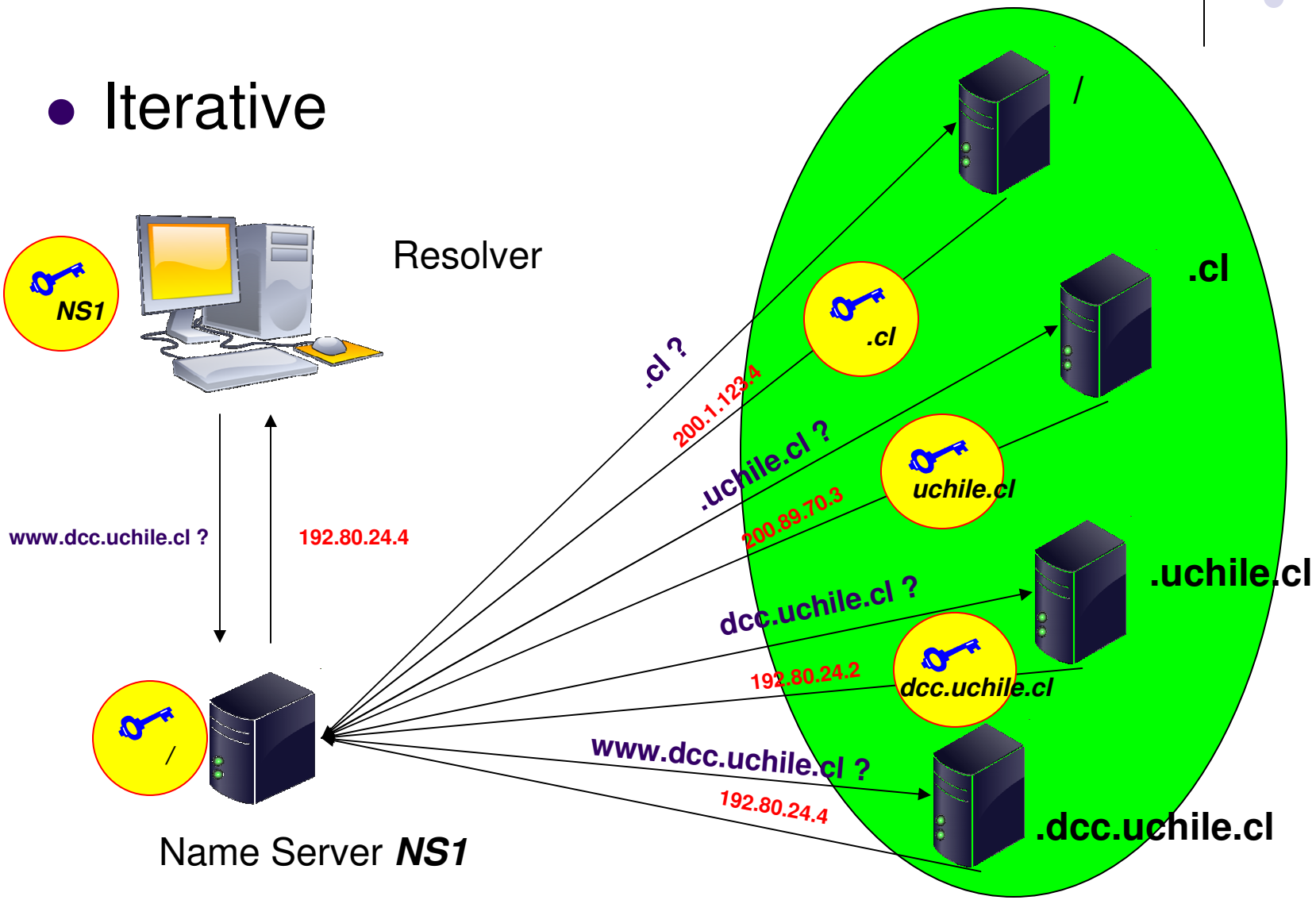




- Every ***zone*** signs the public key of its ***children***
- The public key of the ***root*** is preinstalled in nameserver.
- Every message (***resource record***) is signed by its author.

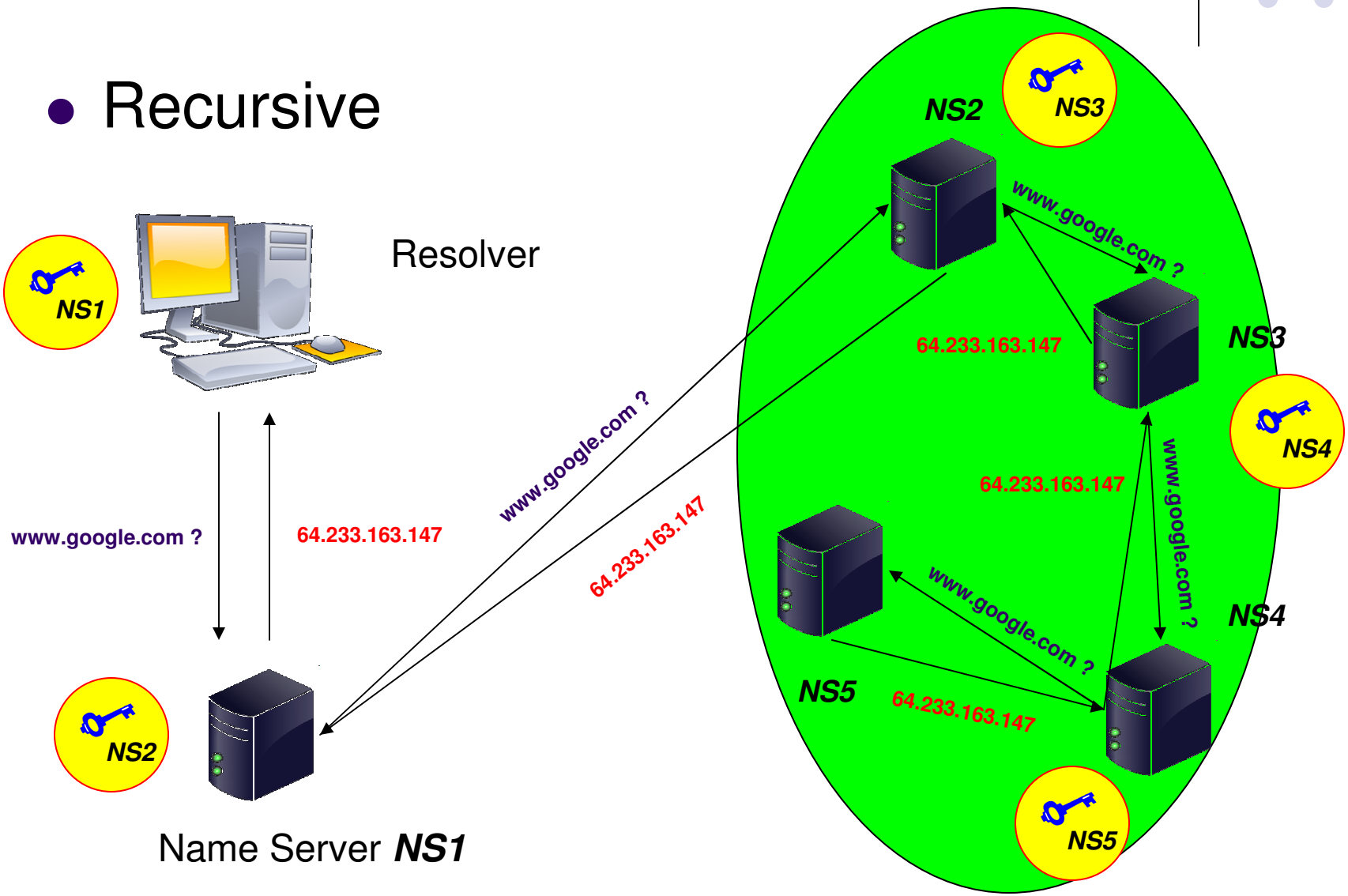
DNSSEC Resolution & Verification

- Iterative



DNSSEC Resolution & Verification

- Recursive

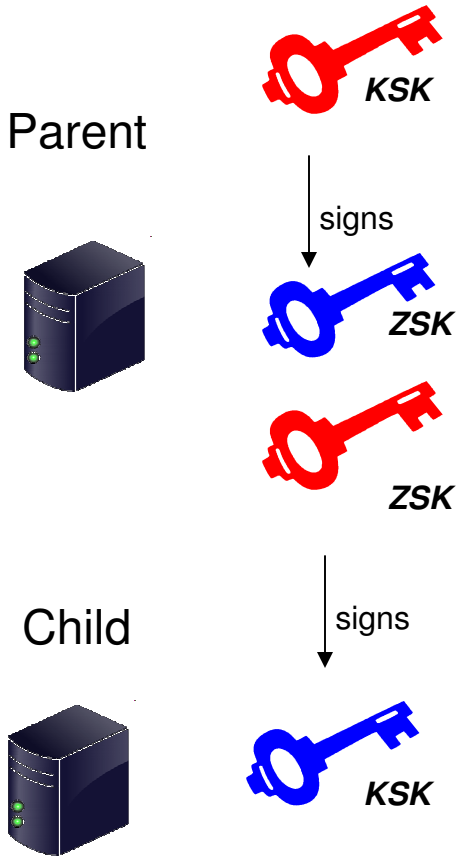


DNSSEC Operational Practices

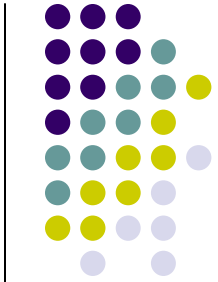
- Time
  - Assumption: ***global clock***.
  - Every signed information has a ***limited lifetime***.
  - This also applies to ***keys***.

DNSSEC Operational Practices

- Two types of Keys
  - Zone Signing Keys (ZSK)
    - Are used to sign all the information of the zone
  - Key Signing Keys (KSK)
    - Are used to sign the ZSK
  - ZSK are used to sign the KSK of the ***child***



DNSSEC Operational Practices



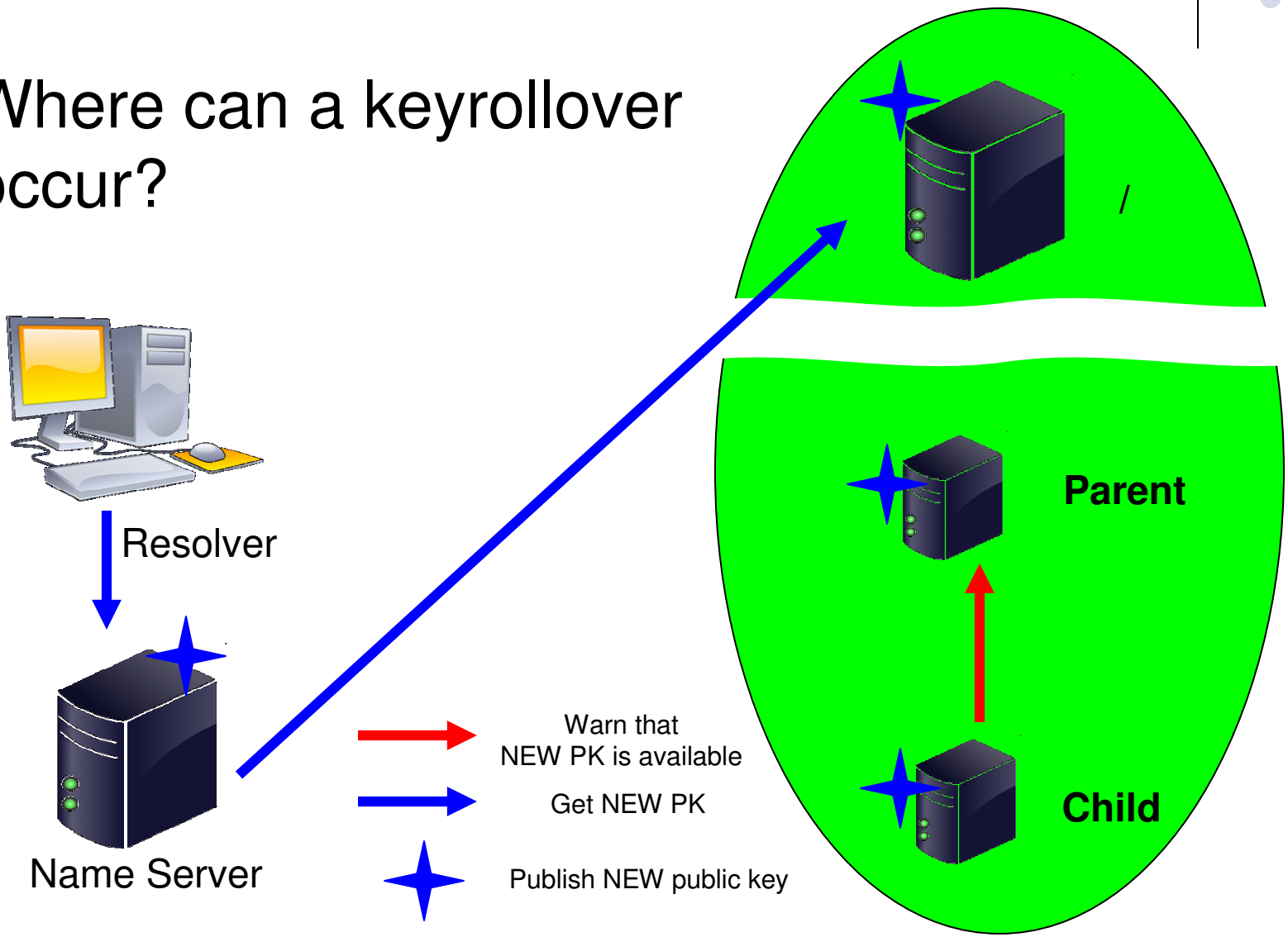
- Motivation of the use of KSK/ZSK
  - No parent/child interaction is required when ZSKs are updated.
  - The KSK can be made stronger.
  - KSK is only used to sign a set of keys. It can be stored in a safer place.
  - KSK have longer effectivity period.

DNSSEC Operational Practices

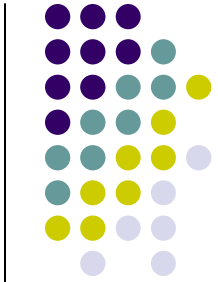
- KEY ROLLOVER
  - It is necesarry to change the keys from time to time
    - As to make cryptanalysis harder
      => Scheduled Rollover
    - Private keys may be stolen or cracked
      => Unscheduled Rollover

DNSSEC Operational Practices

- Where can a keyrollover occur?

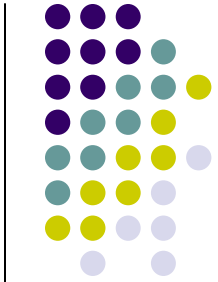


DNSSEC Operational Practices



- Scheduled Key Rollover
  - How do name servers/resolvers know this new public key?
    - Pre-Publish Key Rollover
    - Double Signature Rollover
  - ZSK Rollover
    - No interaction needed
  - KSK Rollover
    - Interaction needed between child and parent

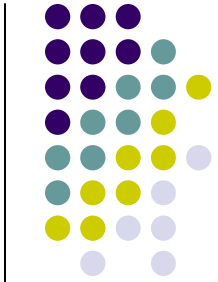
DNSSEC Operational Practices



- ZSK Prepublish Rollover

initial	New DNSKEY	New Signatures	DNSKEY Removal
KSK	KSK	KSK	KSK
ZSK1	ZSK1	ZSK1	
	ZSK2	ZSK2	ZSK2
$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	
	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$
$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK2}$	$\{ZONE\_DATA\}_{ZSK2}$

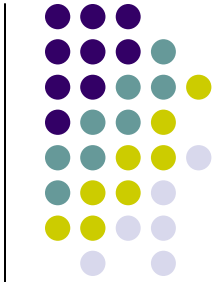
DNSSEC Operational Practices



- ZSK Prepublish Rollover

initial	New DNSKEY	New Signatures	DNSKEY Removal
KSK	KSK	KSK	KSK
ZSK1	ZSK1	ZSK1	
	ZSK2	ZSK2	ZSK2
$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	
	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$
$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK2}$	$\{ZONE\_DATA\}_{ZSK2}$

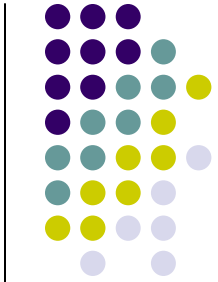
DNSSEC Operational Practices



- ZSK Prepublish Rollover

initial	New DNSKEY	New Signatures	DNSKEY Removal
KSK	KSK	KSK	KSK
ZSK1	ZSK1	ZSK1	
	ZSK2	ZSK2	ZSK2
$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	
	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$
$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK2}$	$\{ZONE\_DATA\}_{ZSK2}$

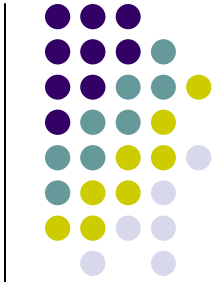
DNSSEC Operational Practices



- ZSK Prepublish Rollover

initial	New DNSKEY	New Signatures	DNSKEY Removal
KSK	KSK	KSK	KSK
ZSK1	ZSK1	ZSK1	
	ZSK2	ZSK2	ZSK2
$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	
	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$
$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK2}$	$\{ZONE\_DATA\}_{ZSK2}$

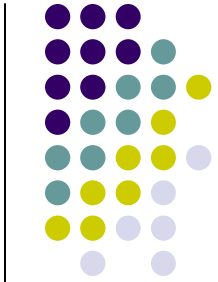
DNSSEC Operational Practices



- ZSK Double Signature Rollover

initial	New DNSKEY	DNSKEY Removal
KSK	KSK	KSK
ZSK1	ZSK1	
	ZSK2	ZSK2
$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	
	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$
$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK1}$	
	$\{ZONE\_DATA\}_{ZSK2}$	$\{ZONE\_DATA\}_{ZSK2}$

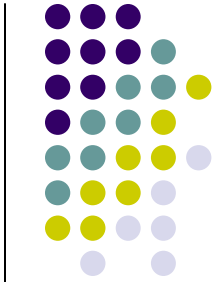
DNSSEC Operational Practices



- ZSK Double Signature Rollover

initial	New DNSKEY	DNSKEY Removal
KSK	KSK	KSK
ZSK1	ZSK1	
	ZSK2	ZSK2
$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	
	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$
$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK1}$	
	$\{ZONE\_DATA\}_{ZSK2}$	$\{ZONE\_DATA\}_{ZSK2}$

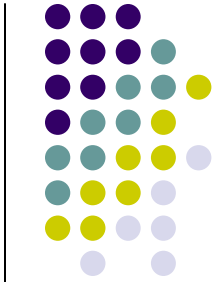
DNSSEC Operational Practices



- ZSK Double Signature Rollover

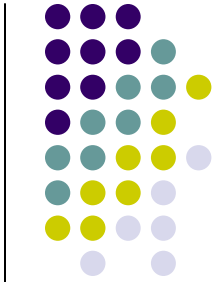
initial	New DNSKEY	DNSKEY Removal
KSK	KSK	KSK
ZSK1	ZSK1	
	ZSK2	ZSK2
$\{ZSK1\}_{KSK}$	$\{ZSK1\}_{KSK}$	
	$\{ZSK2\}_{KSK}$	$\{ZSK2\}_{KSK}$
$\{ZONE\_DATA\}_{ZSK1}$	$\{ZONE\_DATA\}_{ZSK1}$	
	$\{ZONE\_DATA\}_{ZSK2}$	$\{ZONE\_DATA\}_{ZSK2}$

DNSSEC Operational Practices



- Pros and Cons
  - Prepublish Key Rollover
    - + Does not involve signing all the zone data twice.
    - - Process requires 4 steps.
  - Double Signature
    - + Process requires 3 steps.
    - - The number of signatures in the zone doubles. Prohibitive for big zones.

DNSSEC Operational Practices



- KSK Rollover
  - Same idea
    - Now the data to sign are (zone signing) keys
  - However
    - Double Signature Rollover seems better as the data signed is only a set of key
    - The child needs to warn the parent securely that the keys have changed.
      - The way to do this is left to the DNSSEC administrators.

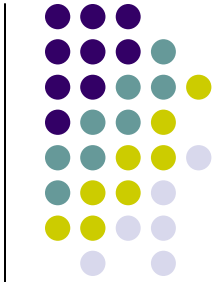
DNSSEC Operational Practices

- Unscheduled Key Rollover

  - **PANIC!**

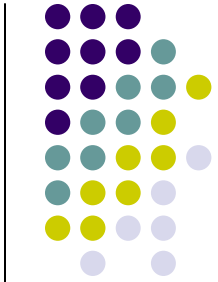
    - *"An authenticated out-of-band and secure notify mechanism to contact parent is needed in this case." (RFC 4641)*

DNSSEC Operational Practices



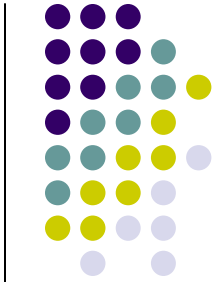
- Unscheduled Key Rollover
  - Keep the chain of trust intact
    - Resign with the compromised key the new set of keys with a very short lifetime, then make a rollover
    - **Problem:** DOMAIN DISPUTE
      - The adversary controls the compromised key, so he can also make a keyrollover…
      - At the end who should we believe?
  - Break the chain of trust
    - Say to the clients that there is a problem
    - Fix the problem
    - Interact with the clients to distribute the new public key
    - **Problem:** DNSSEC is down for a while

NSEC 3



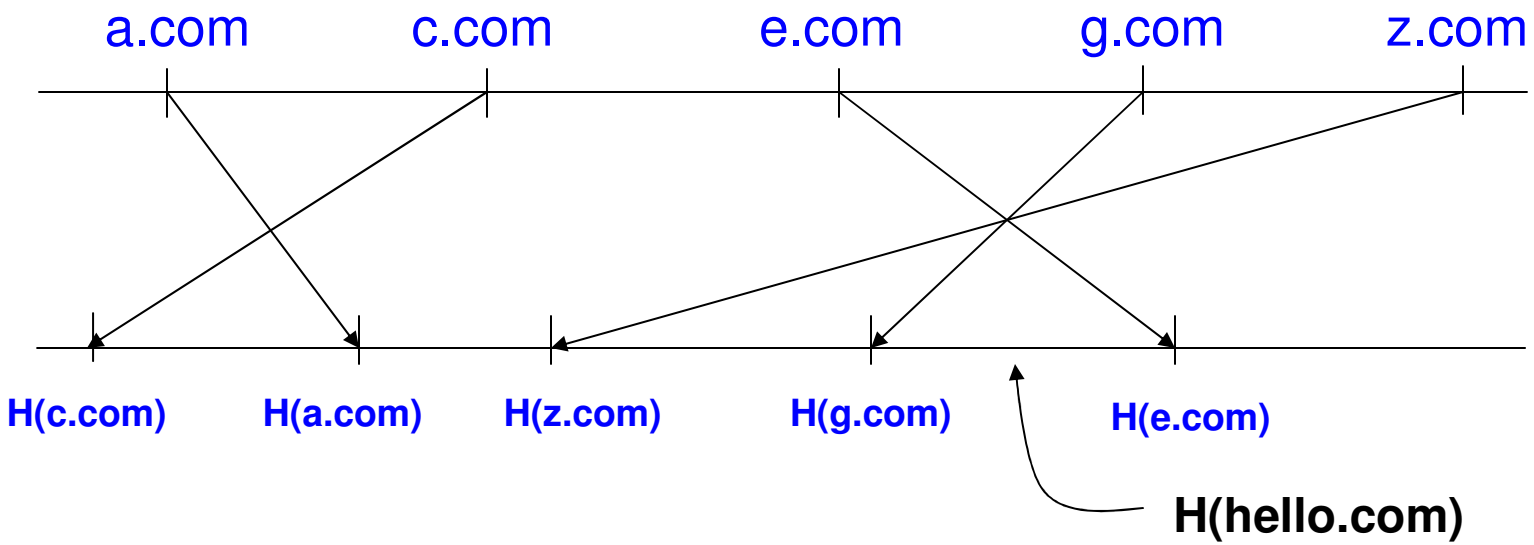
- DNSSEC
  - not only provides an authenticated mapping between IP and domains
  - but also provides proofs of non existence (membership)
    - e.g: Q: www.doesnotexist.com ?
      A: this domain does not exist
- For efficiency
  - As to avoid signing dynamically the response the consecutive pair of domains ordered in alphabetic order are signed. All proofs are ***precomputed***.
  - [a.com, c.com], [c.com, e.com], [e.com,g.com], [g.com,z.com]
  - hello.com does not exist ⇔ g.com < hello.com < z.com

NSEC 3



- Problem: Zone Walking
  - An attacker can collect all the domains of a zone, by asking for domain that lies inside of every succesive intervals.
  - Is that a problem? After all the information is public…
  - Yes but in some case knowing all the domain names for a given level can be a useful information to build an attack for example.

NSEC 3

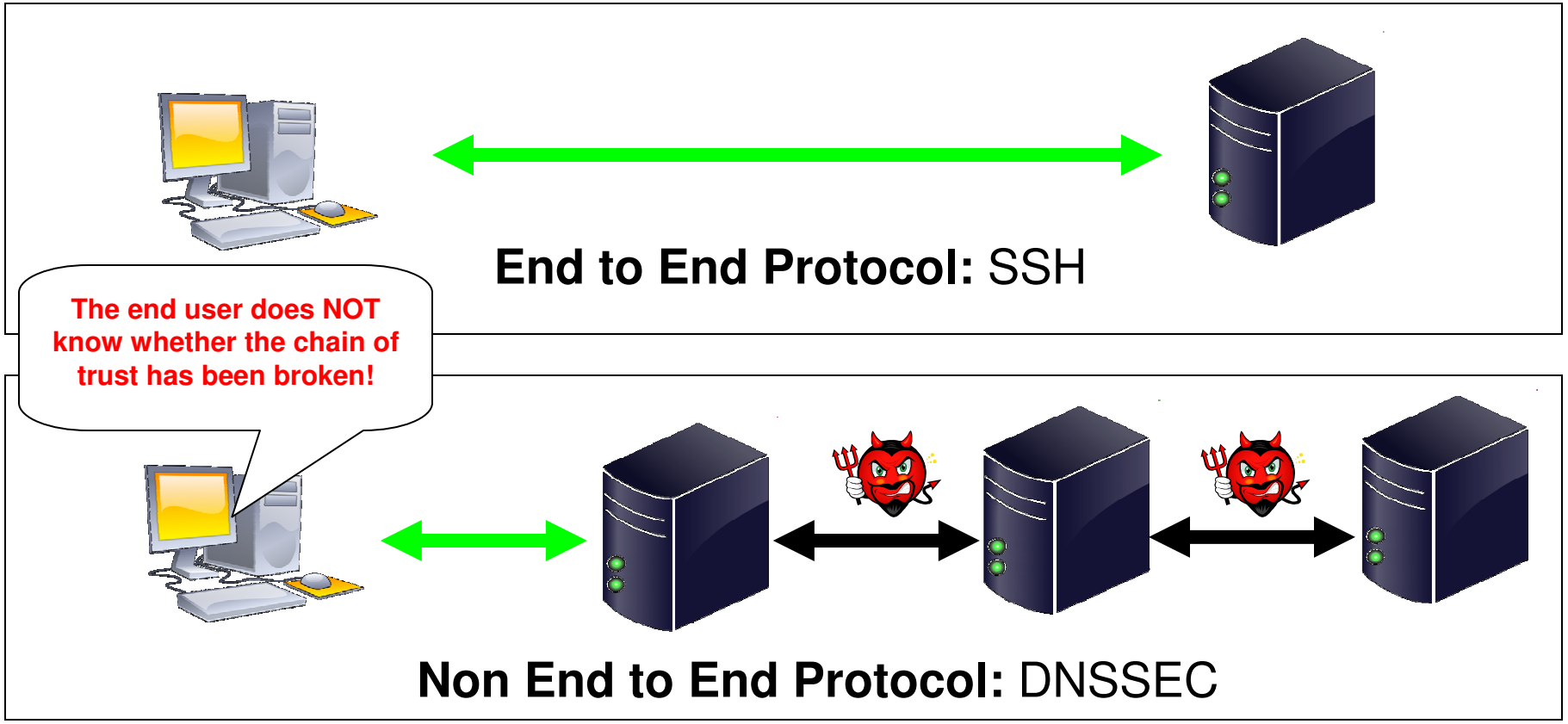
- Solution
  - Applying a hash function H to the domain names as to hide the information of the domain and still be able get nonmembership proofs.
  - 

DNSSEC
Problems and Limitations

- First proposal 1999 (RFC 2535) but still no current implementation at root level 2009
- Only a few of the Top Level Domains (.com, .org, countries…) run DNSSEC
  - Chile is working hard at this moment to implement it!
- Why?
  - Who signs the root?
  - Practical Experiences (Netherlands,…) have been painful
  - DNSSEC is complex
  - People may not see the immediate benefit
  - …

DNSSEC
Problems and Limitations

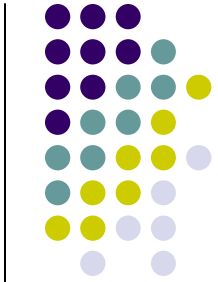
- DNSSEC is a "**Non End to End**" Protocol



DNSSEC
Problems and Limitations

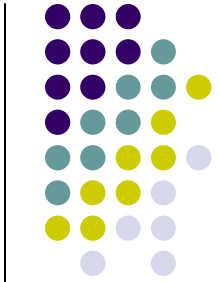
- How to set the public keys life-time?
  - Too big => gives more time to the Adversary
  - Too short => inefficient
    - Need to rollover key very often

DNSSEC
Problems and Limitations



- How to detect (automaticaly) that a private key has been stolen?
  - Users generally don't notice they have been victim of a phishing attack.
  - Defacement
    - When obtained by DNS cache poisoning, the owner of the website is not aware of it.
- ***So in practice can we really detect that a key has been compromised?***

DNSSEC
Problems and Limitations



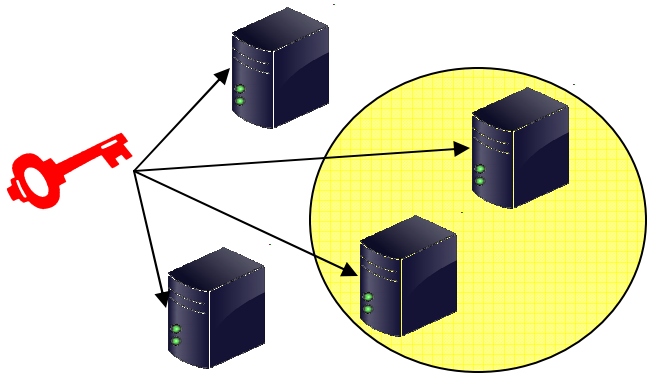
- Key Rollover/Revocation Problem
  - There is no real satisfactory solution for Key Revocation
  - Key Rollver is complex
  - Lack of specification
    - No precise procedure in case of key compromise.
    - How does the child warn its parent?

How to improve the Security of DNS?

- There is no definition for the Adversary
  - What can or cannot do the adversary
    - Steal private keys?
    - Only forge some signatures?
    - Intercept any packet?
    - Control a DNS Name Server?
    - Create a Zone / Domain?
      - Injection attack in Registrars Databases
    - …

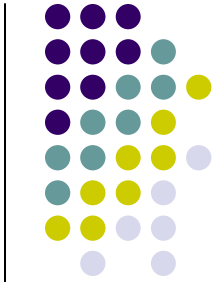
How to improve the Security of DNS?

- Use of Threshold Cryptography [Cachin, Samar 04]
  - What is Threshold Cryptography (very short)?
    - N participants
    - T participants can jointly sign
    - T-1 participant cannot do anything
      - =>Adversary must control T servers to perform an attack



N=4
T=2 participants required to sign

How to improve the Security of DNS?

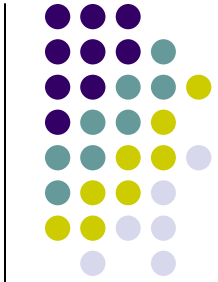


- Use of Threshold Cryptography
  [Cachin, Samar 04]
  - Concrete proposal
    - They use standard RSA signature
    - Need to change the server implementation but not the client
    - Benchmark
  - Stealing private key is harder
    - It can be effective against internal attacks.
  - However
    - If the servers that hold the share have got the same configuration, a same vulnerability can be enough to compromise all the servers.
    - More Complex

How to improve the Security of DNS?

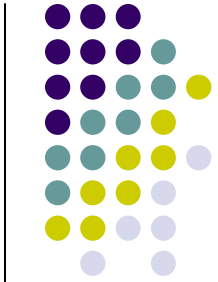
- Identity Based Cryptography [Chan 03]
  - Master Thesis work.
  - Analyzes the possibilty to use IBC to improve the security of DNS instead of using standard public key cryptography.
  - Original approach to solve this problem.

IBC



- Idea
  - A Trusted Authority (TA) generates (SK,PK) and distributes securely the private keys to every participant.
  - Then the TA publishes a public key PK
  - The public key of every participant can be computed from PK and a public information
    - Email, Name, Passport Number, Biometric data

DNS with IBC

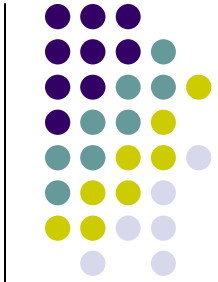


- [Shamir, 84]
  First introduction of the concept.

- [Boneh,Franklin 01]
  First efficient scheme for IBC using bilinear maps.

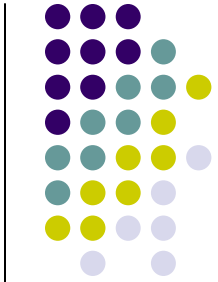
- Many other works, this is a very active field.

IBC



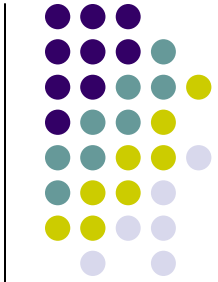
- Advantages
  - No need to store public keys
  - No need to sign/verify public keys
  - No need to manage certificates

DNS with IBC



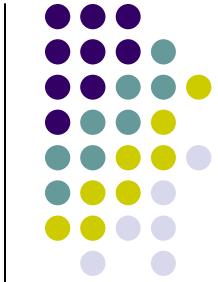
- Problem: Key Escrow
  - The TA knows (generates) all the private keys of users.
  - Is that really a problem?
  - ANSWER
    - **NO:** in our setting, a parent can always create new children with their respective private keys.

DNS with IBC



- Key Rollover
  - Add timestamp to the identity
    - **dcc.uchile.cl || 28-4-2009::29-4-2009**
- Key Revocation
  - Still hard
    - We could use a database of revocated keys but we would loose the good properties of IBC…

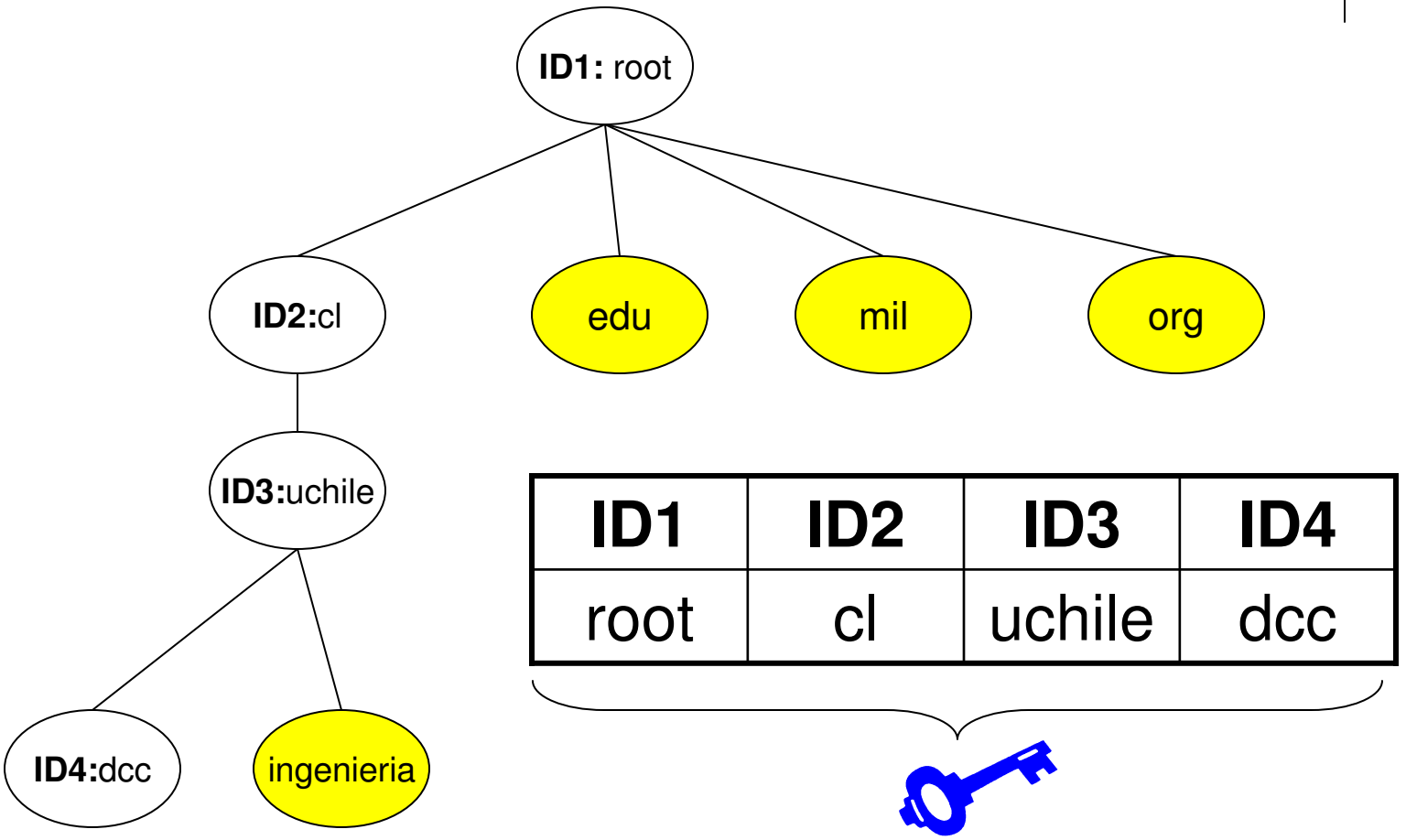
DNS with IBC



- Problem of scalability
  - A single authority has to generate all the private keys. This is not reasonable in the case of DNS.

- Solution
  - Use of Hierchical Identity Based Cryptography
    - The private key generation can be delegated to subauthorities **[Gentry, Silverberg 02]**

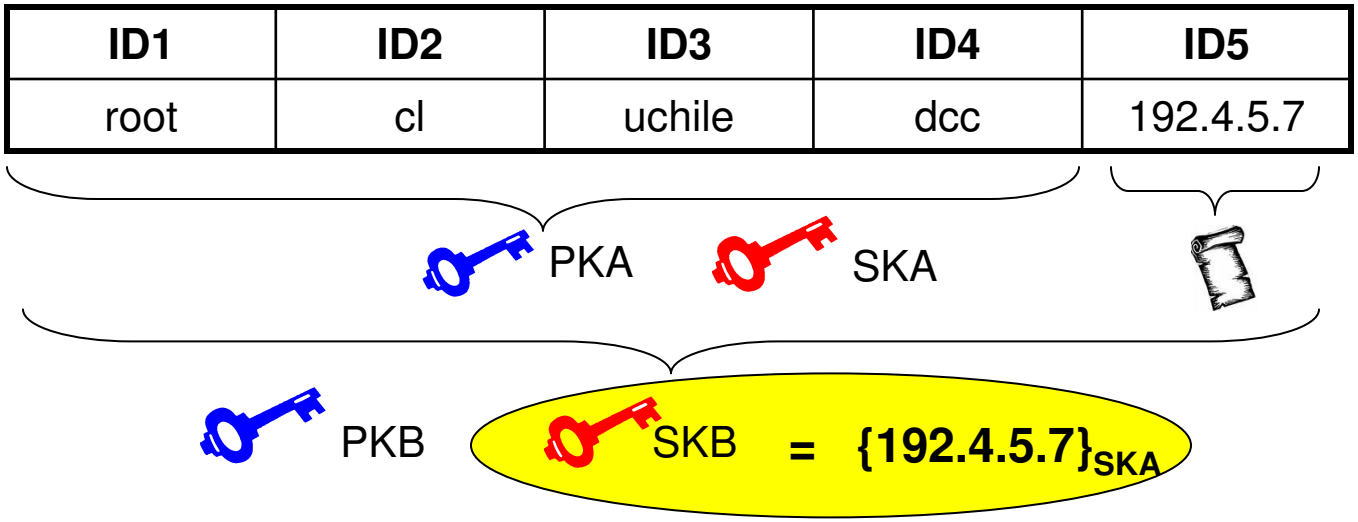
DNS with HIBC



ID1	ID2	ID3	ID4
root	cl	uchile	dcc

DNS with HIBC

- How to sign?



Verification process

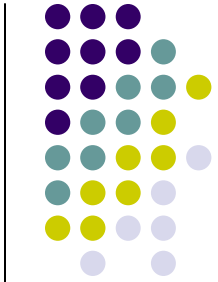
(1) R random

(2) C = Encrypt(PKB,R)

(3) R' = Decrypt(SKB,C)

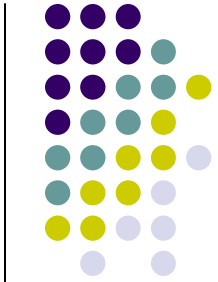
(4) R = R' ?

DNS with HIBC



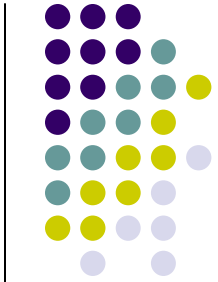
- Efficiency
  - The size of a signature grows ***linearly*** in the ***depth*** of the hierarchy.
  - So we do not win to much (even we may loose) compared to the classical DNSSEC verification procedure.

DNS with HIBC

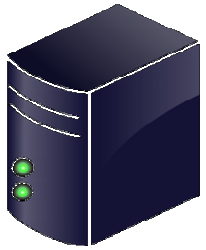


- So at the end, is HIBC useful?
  - HIBC has attractive properties
    - No need to manage public key/certificates
    - Simplifies the scheduled key rollover
  - However some problems remain unsolved
    - Key revocation (unscheduled key rollover)
    - Verification time proportional to the depth of the domain name tree.
    - Not clear that how to adapt the ***Recursive Resolving Algorithm***
    - In practice developping standards for pairings and HIBC takes time.

Conclusion



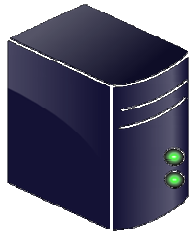
- DNS is essential for Internet
- DNS is not secure and this is a big problem
- DNSSEC adds integrity/authenticity to DNS
- DNSSEC raises some practical problems
  - Key Rollover
  - All or Nothing security / Not Point to Point
  - Administrative problem: who signs the root?
- But DNSSEC is to the date the only concrete proposal to make DNS more secure. Can we do better?

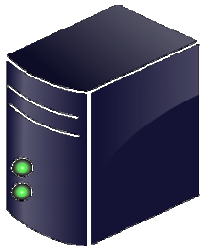


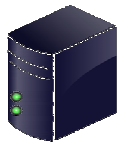











have.you.got.any.question