EncDNS: A Lightweight Privacy-Preserving Name Resolution Service

Dominik Herrmann · Karl-Peter Fuchs
Jens Lindemann · Hannes Federrath

Security in Distributed Systems
https://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

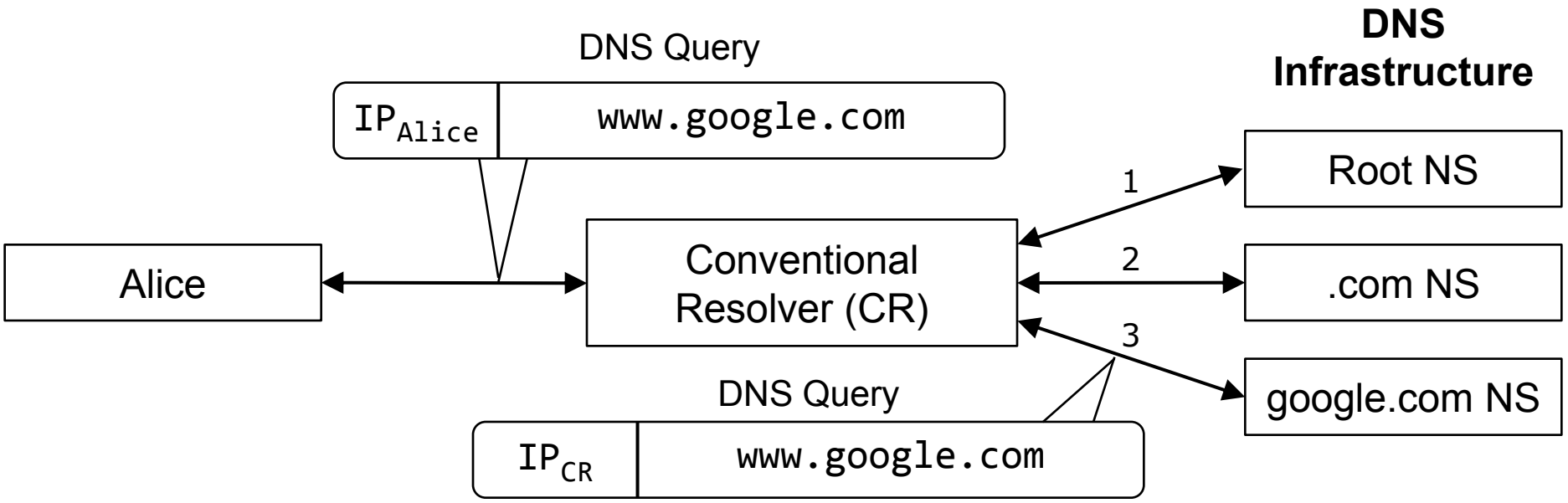
ESORICS 2014, Wroclaw
September 7, 2014

Outline

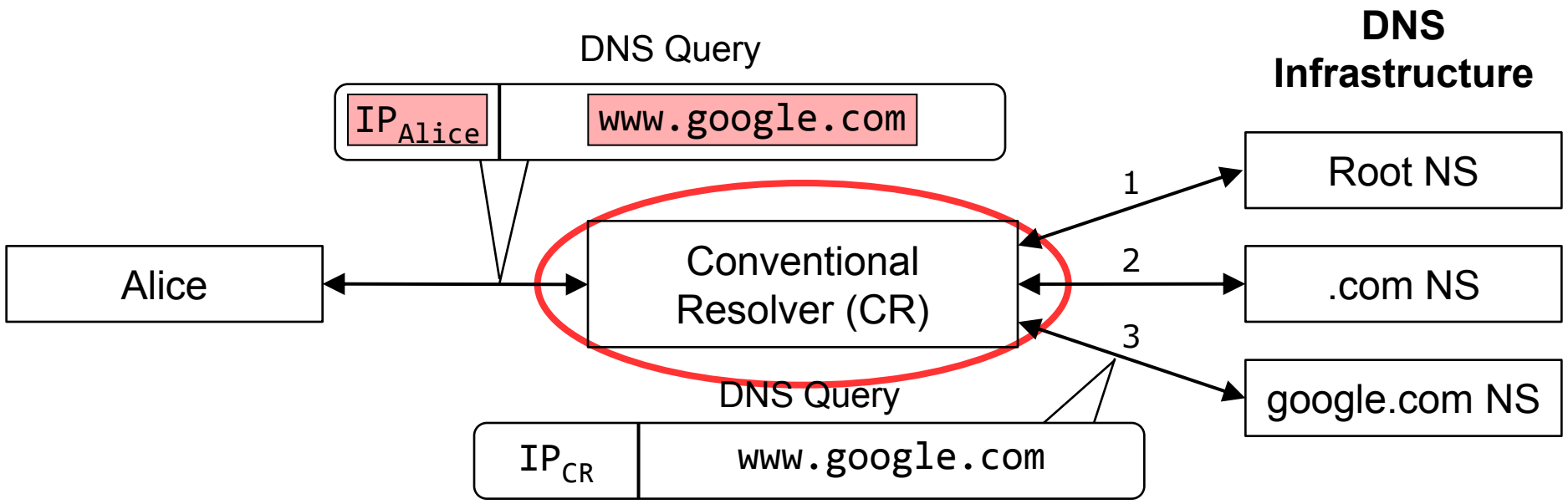
- The privacy problem in DNS
- Related work
- EncDNS
  - Design
  - Evaluation

The Domain Name System (DNS)

- Translates human-readable domain names to IP addresses



Where's the privacy problem?



CR can observe activities of its users (cf. Google Public DNS)

Related work does not solve the problem

- DNSSEC
  - Protects integrity and authenticity, but not confidentiality
- DNSCurve, DNSCrypt
  - Point-to-point encryption only
- Range queries (additional dummy queries)
  - User behaviour still detectable*
- Onion Routing (e.g. Tor)
  - Good privacy protection, but slow

* see D. Herrmann, M. Maaß, H. Federrath: "Evaluating the Security of a DNS Query Obfuscation Scheme for Private Web Surfing.", IFIP SEC 2014.

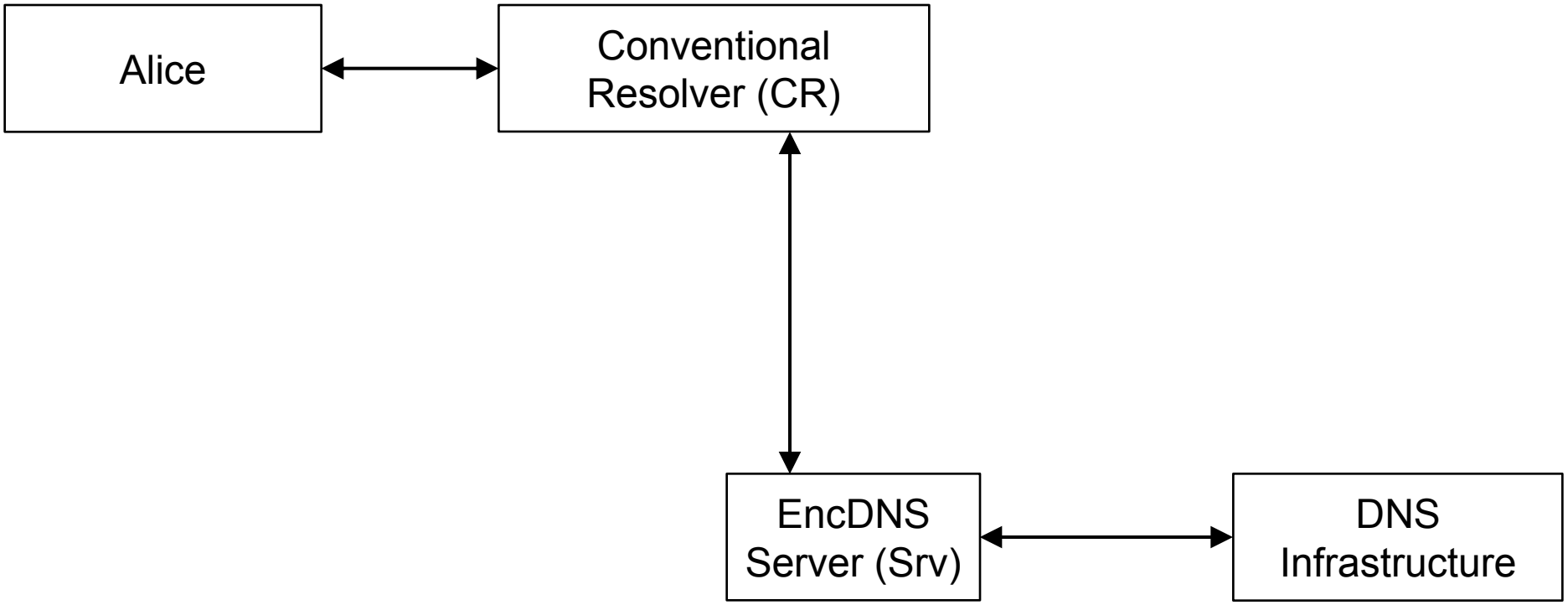
Requirements

- No linkability of sender identity and contents of query or response
- No significant delay to DNS queries
- Compatible with existing infrastructure
- Low computational burden on servers

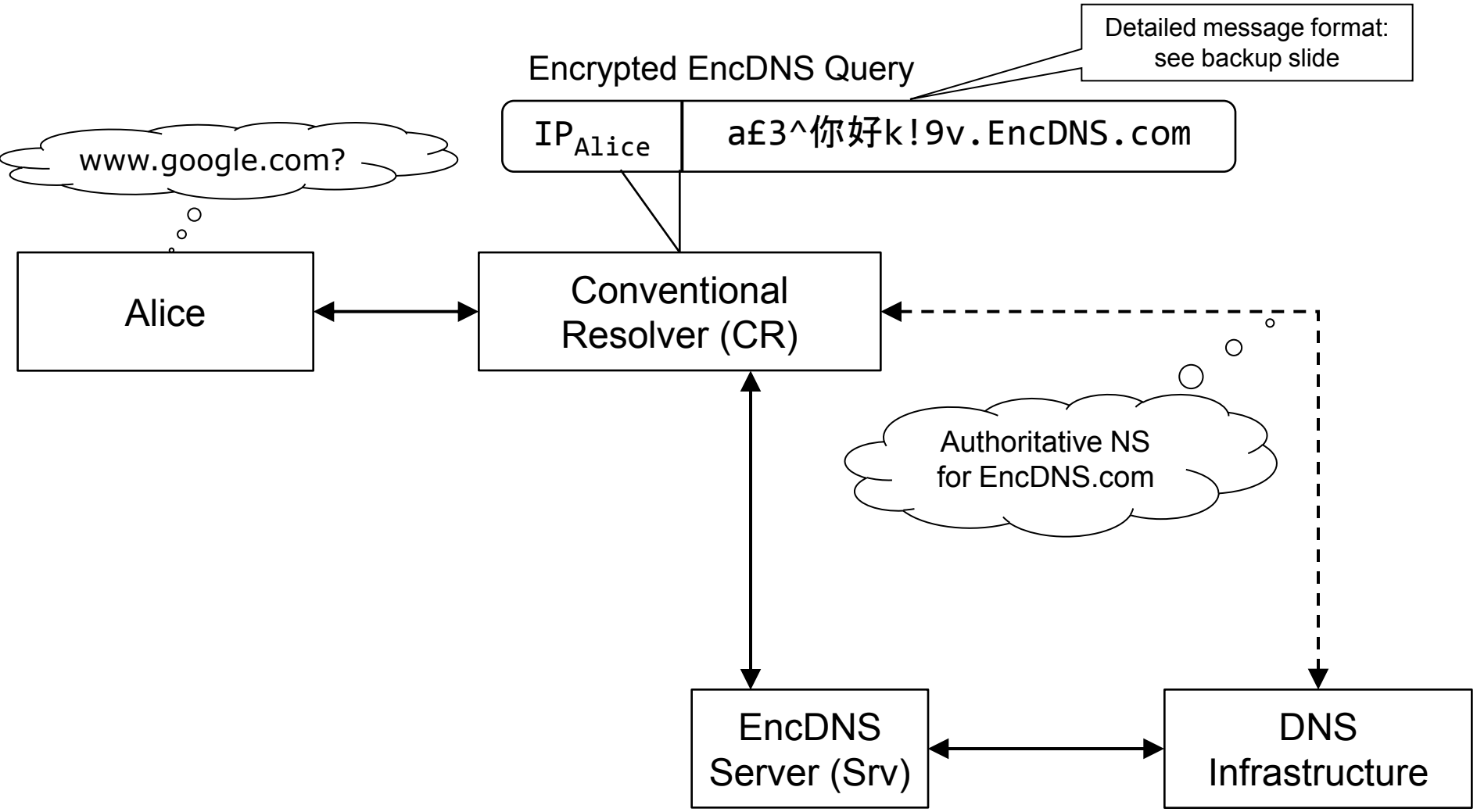
NOT: protect against distributed adversaries (traffic analysis)

→ Our solution – EncDNS: encapsulates encrypted DNS messages within standard DNS messages

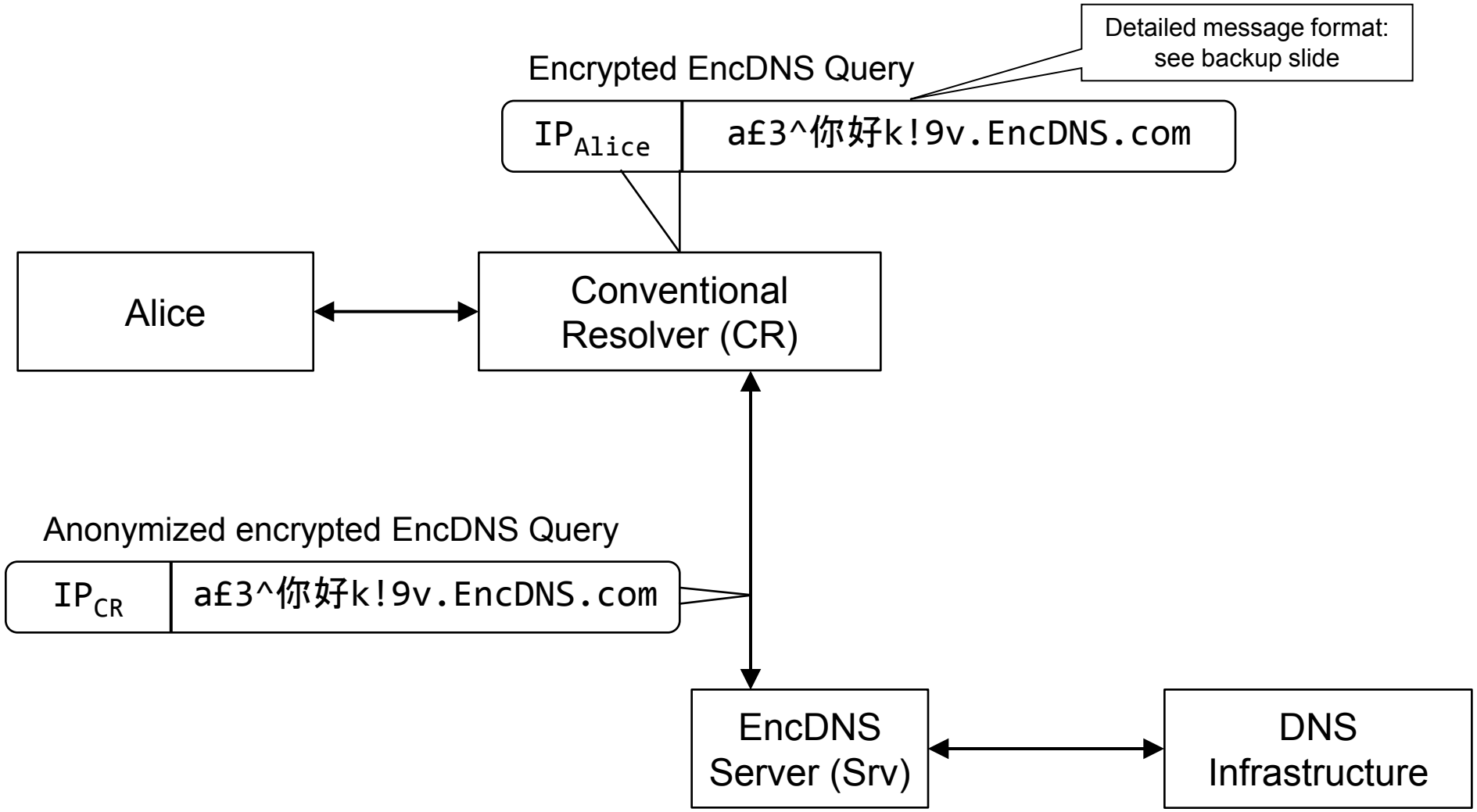
EncDNS


Alice
Conventional Resolver (CR)
EncDNS Server (Srv)
DNS Infrastructure

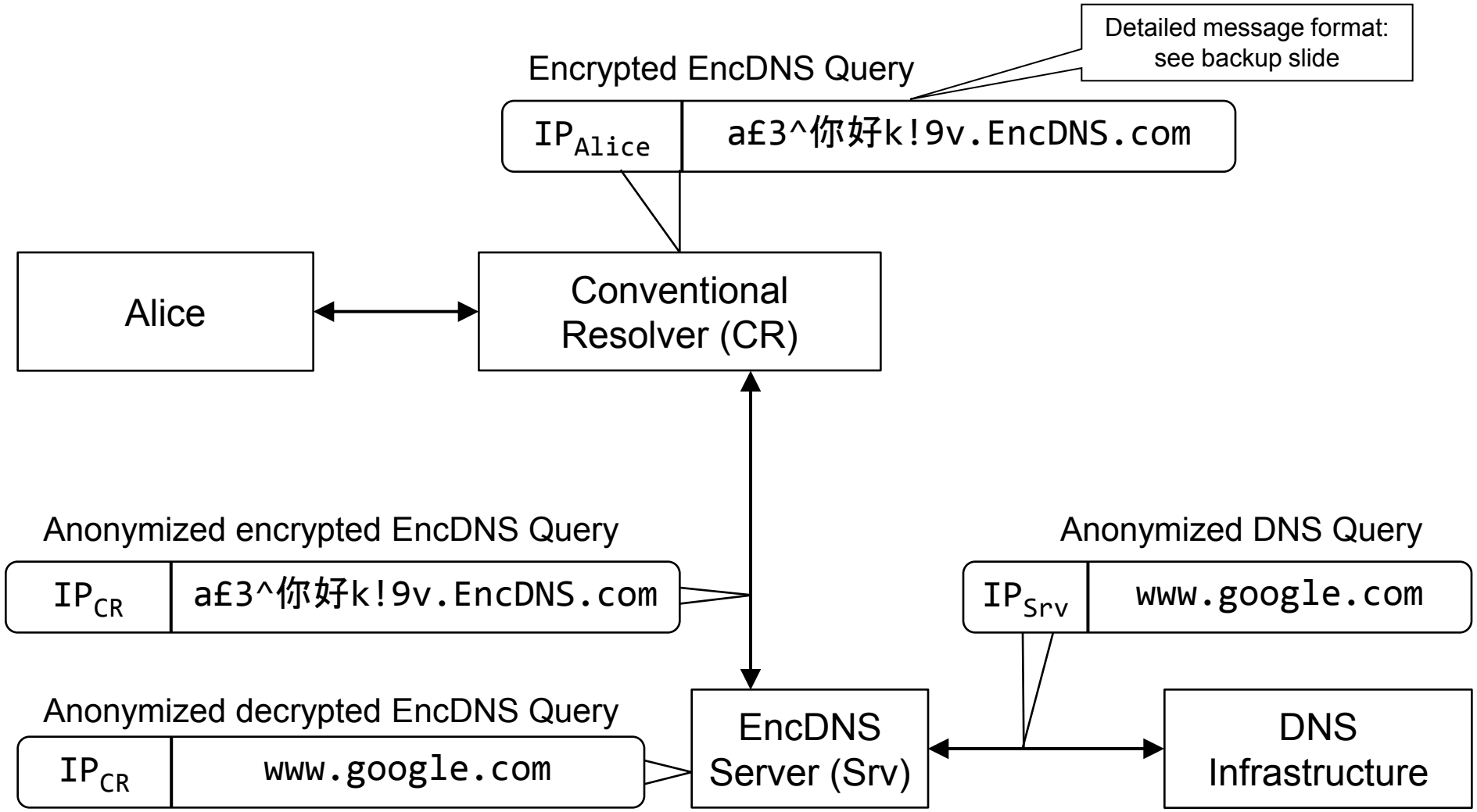
EncDNS


Detailed message format:
see backup slide
Encrypted EncDNS Query
IP_Alice
a£3^你好k!9v.EncDNS.com
www.google.com?
Alice
Conventional
Resolver (CR)
Authoritative NS
for EncDNS.com
EncDNS
Server (Srv)
DNS
Infrastructure

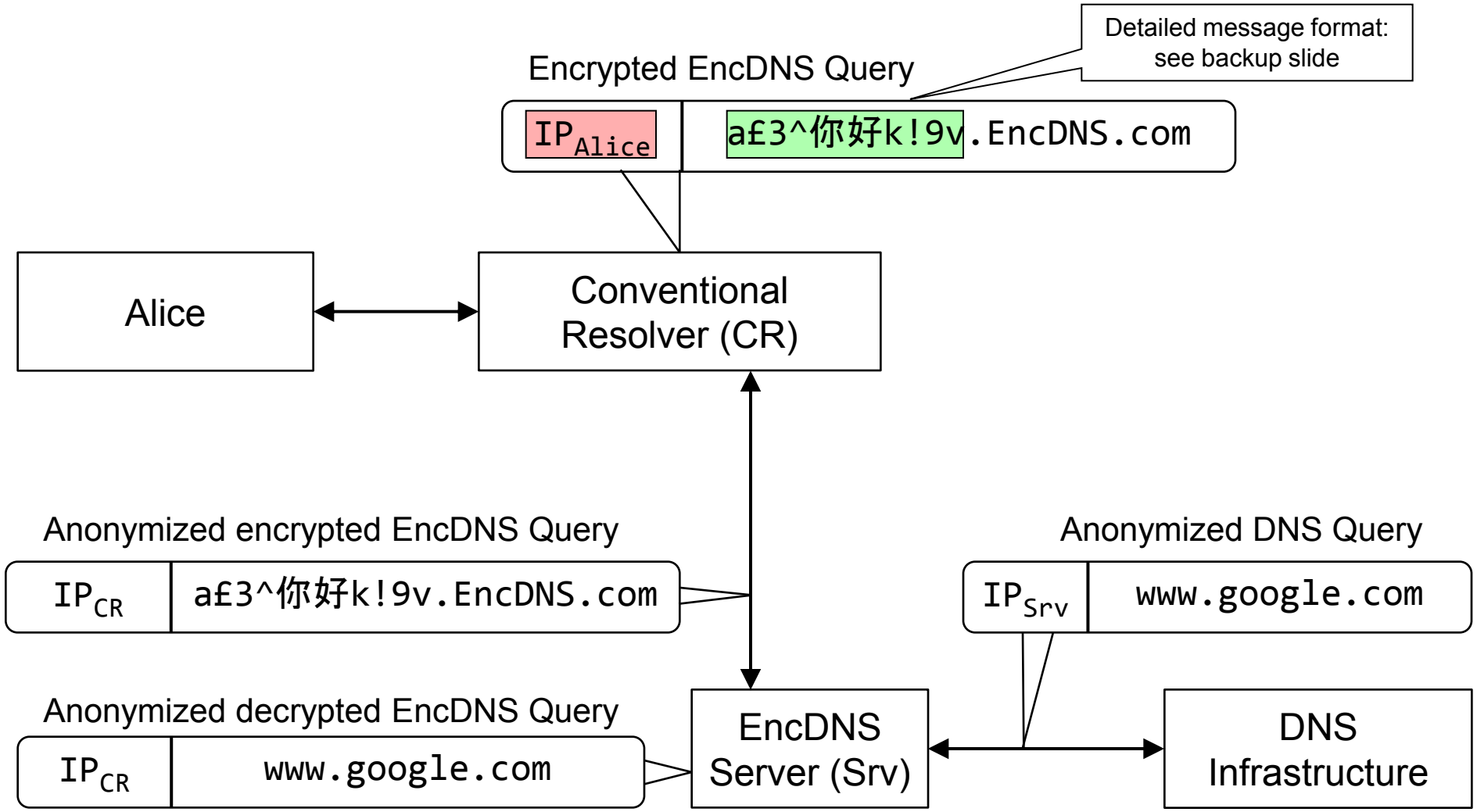
EncDNS


Detailed message format:
see backup slide
Encrypted EncDNS Query
IP_Alice
a£3^你好k!9v.EncDNS.com
Alice
Conventional
Resolver (CR)
Anonymized encrypted EncDNS Query
IP_CR
a£3^你好k!9v.EncDNS.com
EncDNS
Server (Srv)
DNS
Infrastructure

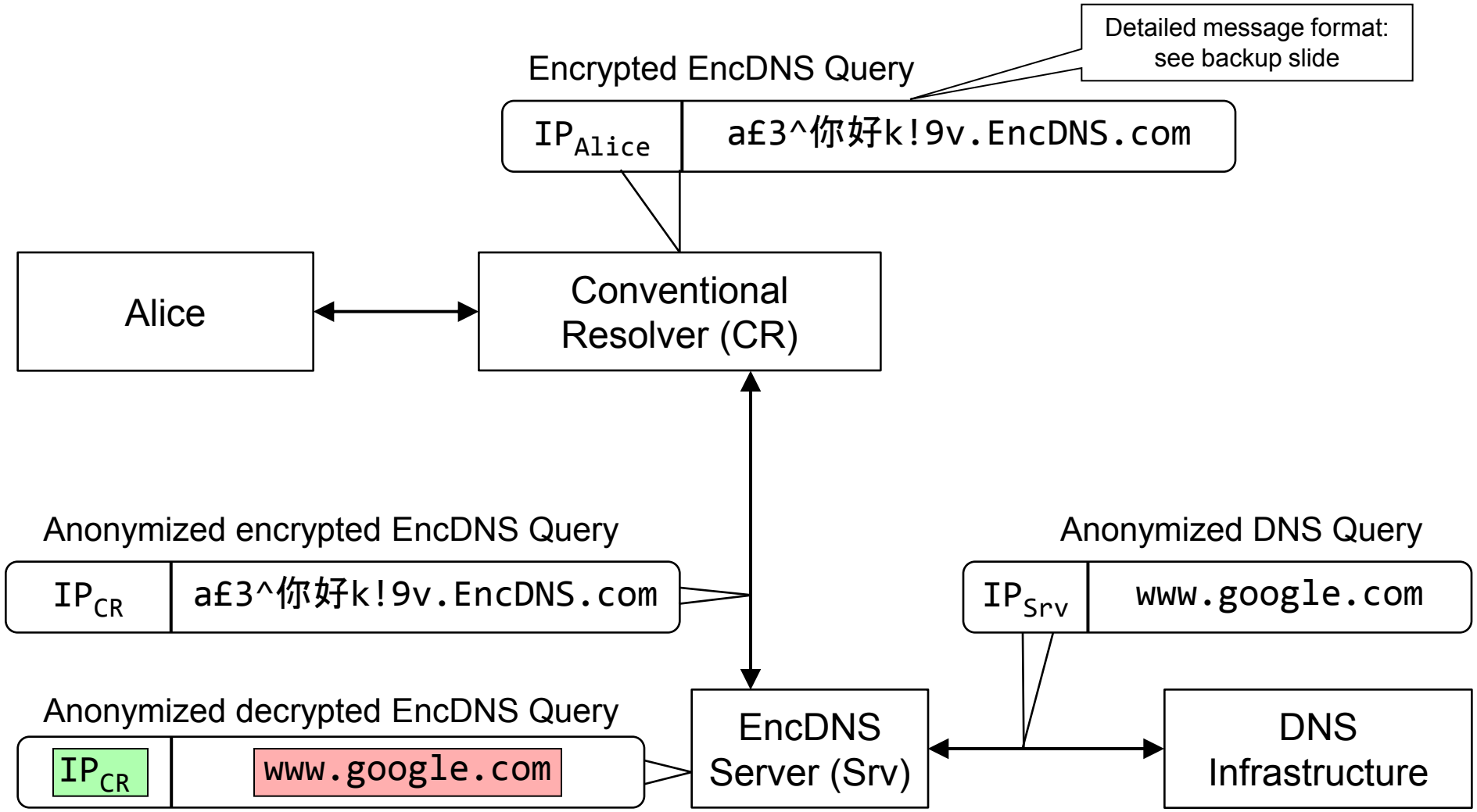
EncDNS


Detailed message format:
see backup slide
Encrypted EncDNS Query
IP_Alice
a£3^你好k!9v.EncDNS.com
Alice
Conventional
Resolver (CR)
Anonymized encrypted EncDNS Query
IP_CR
a£3^你好k!9v.EncDNS.com
Anonymized DNS Query
IP_Srv
www.google.com
Anonymized decrypted EncDNS Query
IP_CR
www.google.com
EncDNS
Server (Srv)
DNS
Infrastructure

EncDNS


Detailed message format:
see backup slide
Encrypted EncDNS Query
IP_Alice
a£3^你好k!9v.EncDNS.com
Alice
Conventional
Resolver (CR)
Anonymized encrypted EncDNS Query
IP_CR
a£3^你好k!9v.EncDNS.com
Anonymized DNS Query
IP_Srv
www.google.com
Anonymized decrypted EncDNS Query
IP_CR
www.google.com
EncDNS
Server (Srv)
DNS
Infrastructure

EncDNS


Detailed message format:
see backup slide
Encrypted EncDNS Query
IP_Alice
a£3^你好k!9v.EncDNS.com
Alice
Conventional
Resolver (CR)
Anonymized encrypted EncDNS Query
IP_CR
a£3^你好k!9v.EncDNS.com
Anonymized DNS Query
IP_Srv
www.google.com
Anonymized decrypted EncDNS Query
IP_CR
www.google.com
EncDNS
Server (Srv)
DNS
Infrastructure

Experiment 1: Scalability

How many queries can we process using off-the-shelf hardware?

	Baseline		EncDNS	
Queries/sec	Failures [%]	CPU load [%]	Failures [%]	CPU load [%]
2000	0.00	13.9	0.00	23.6
4000	0.00	22.3	0.00	47.9
6000	0.00	30.9	0.00	63.9
8000	0.00	41.6	11.82	75.4

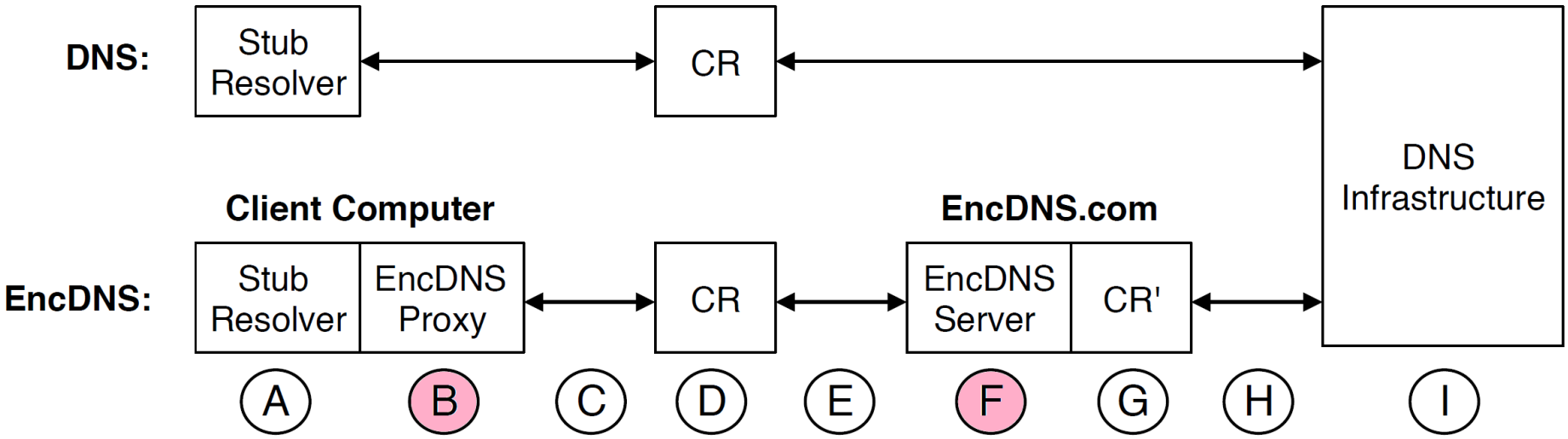
(typical users issue 0.05 queries/sec on average*)

→ computational burden on servers acceptable

* see H. Federrath, K.-P. Fuchs, D. Herrmann, C. Piosecny: "Privacy-Preserving DNS: Analysis of Broadcast, Range Queries and Mix-based Protection Methods", ESORICS 2011.

Experiment 2: User-perceived Latency

How long does the name resolution process take?



Experiment 2: User-perceived Latency

How long does the name resolution process take?

Measurement	Environment	Median latency
Baseline	LAN	1.39 ms
EncDNS		1.80 ms (+ 29.4 %)
Baseline	"real world" (simulated 130 ms network latency)	132.04 ms
EncDNS		132.49 ms (+ 0.35 %)

→ delay of cryptographic operations to queries negligible compared to typical network latency on the Internet

Experiment 3: Compatibility

Is EncDNS compatible with conventional resolvers?

Implementation	Version	Encrypted queries	Encrypted replies
BIND	9.7.3	✓	✓
MaraDNS	1.4.03	✓	✓
Unbound	1.4.6	✓	✓
PowerDNS	3.2	✓	✓
dnscache	1.05	✓	✓

Experiment 3: Compatibility

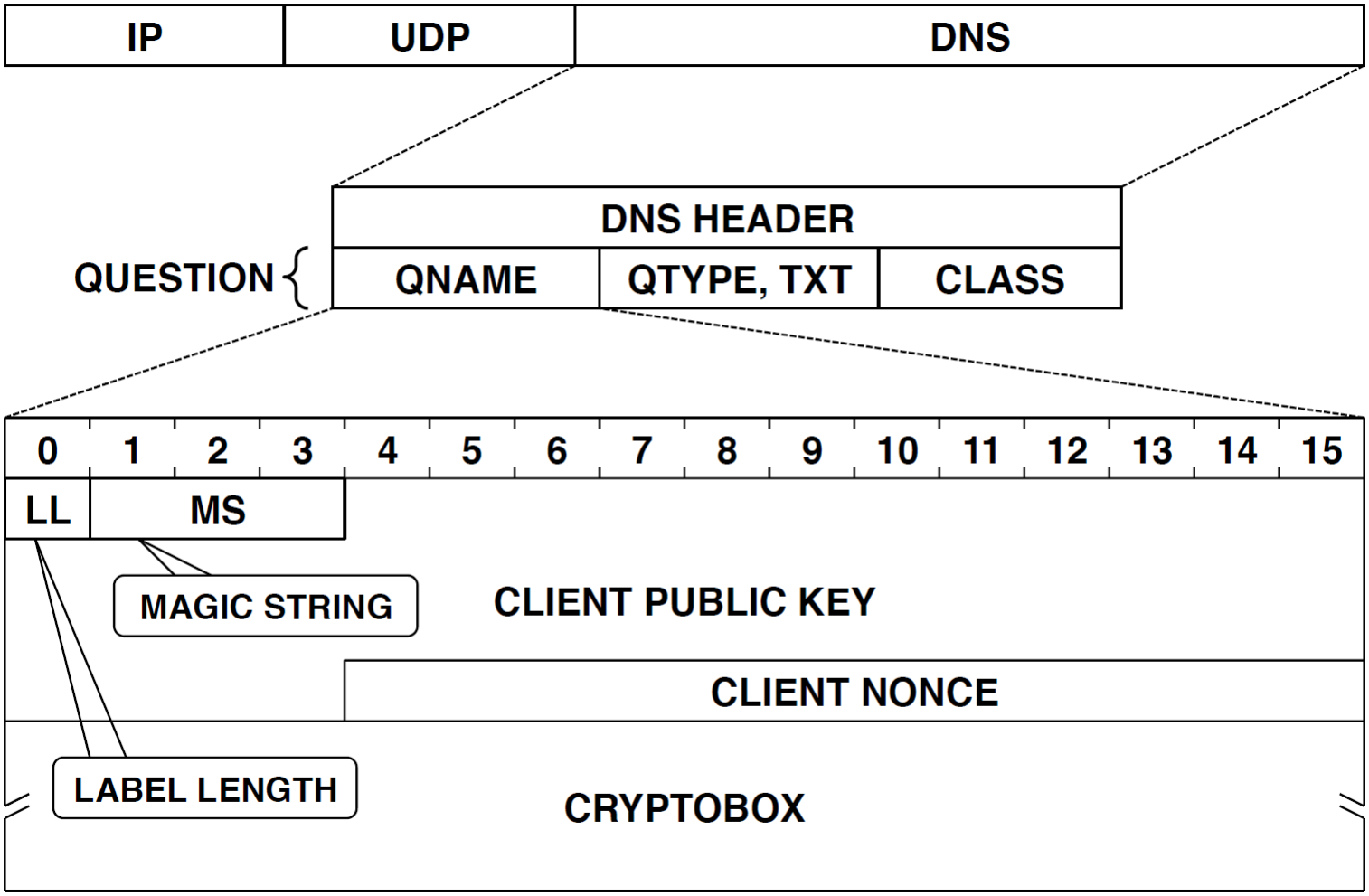
Is EncDNS compatible with conventional resolvers?

Implementation	Version	Encrypted queries	Encrypted replies
BIND	9.7.3	✓	✓
MaraDNS	1.4.03	✓	✓
Unbound	1.4.6	✓	✓
PowerDNS	3.2	✓	✓
dnscache	1.05	✓	✓
Windows Server	2012 R2	✗	✓

Conclusion

- Recursive nameservers can build user profiles → user privacy at risk
- Existing approaches
  - either do not protect privacy,
  - have a major impact on performance,
  - or are incompatible with existing infrastructure.
- EncDNS
  - encapsulates encrypted DNS messages in standard DNS messages
  - protects user privacy against recursive nameservers
  - compatible with existing infrastructure
  - negligible impact on performance
  - test deployment available for public use: https://svs.informatik.uni-hamburg.de/gmix

EncDNS Query



EncDNS Reply