National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

How to Cope with Information Leakage in The Ubiquitous Environment

Kaz Kobara[1,2] and Hideki Imai[2,1]

1: Research Center for Information Security (RCIS), Advanced Industrial Science and Technology (AIST)
2: Chuo University

National Institute of Advanced Industrial Science and Technology
AIST

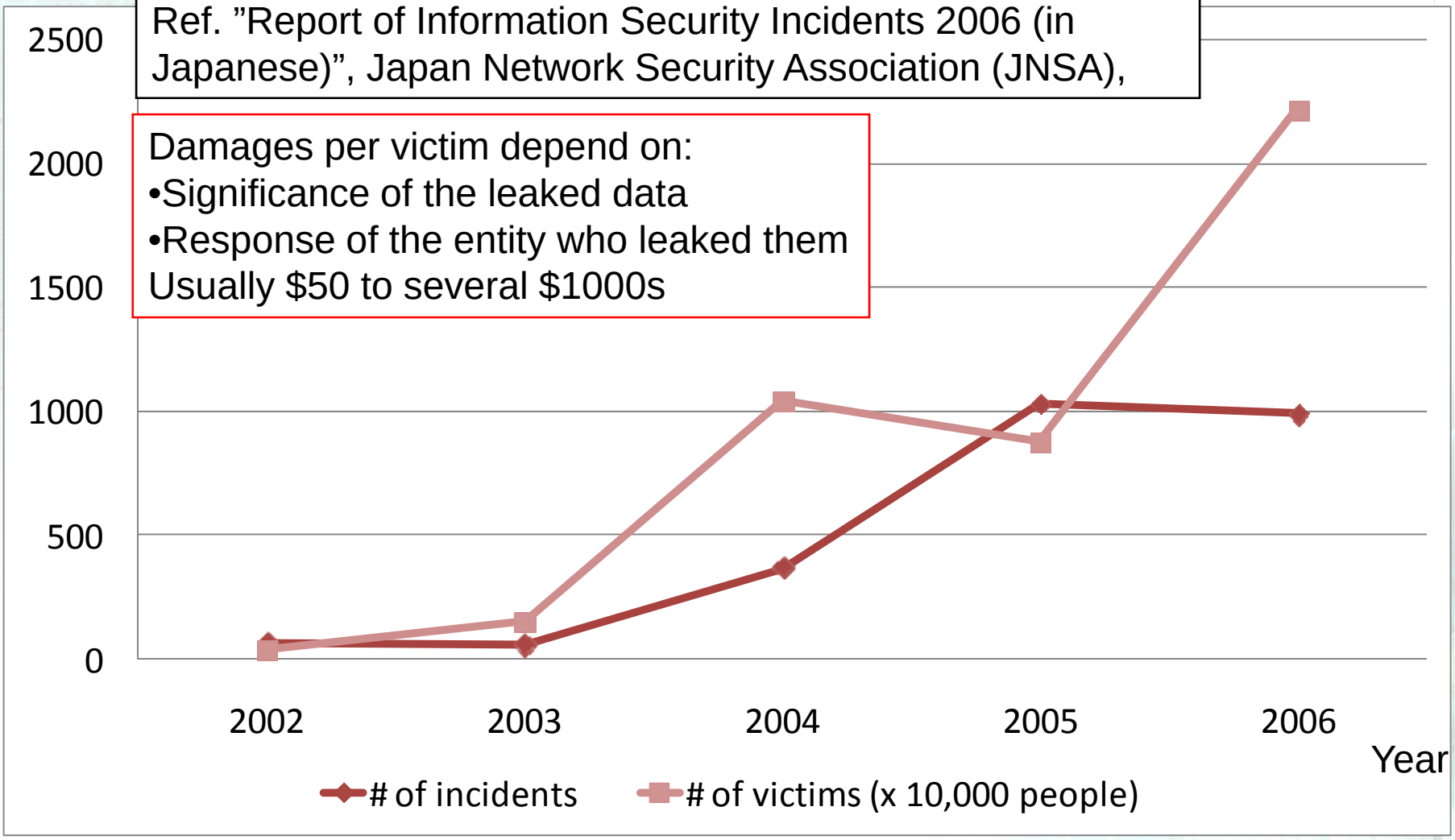
of Personal Data Leakage Incidents and Victims in Japan

Research Center for Information Security

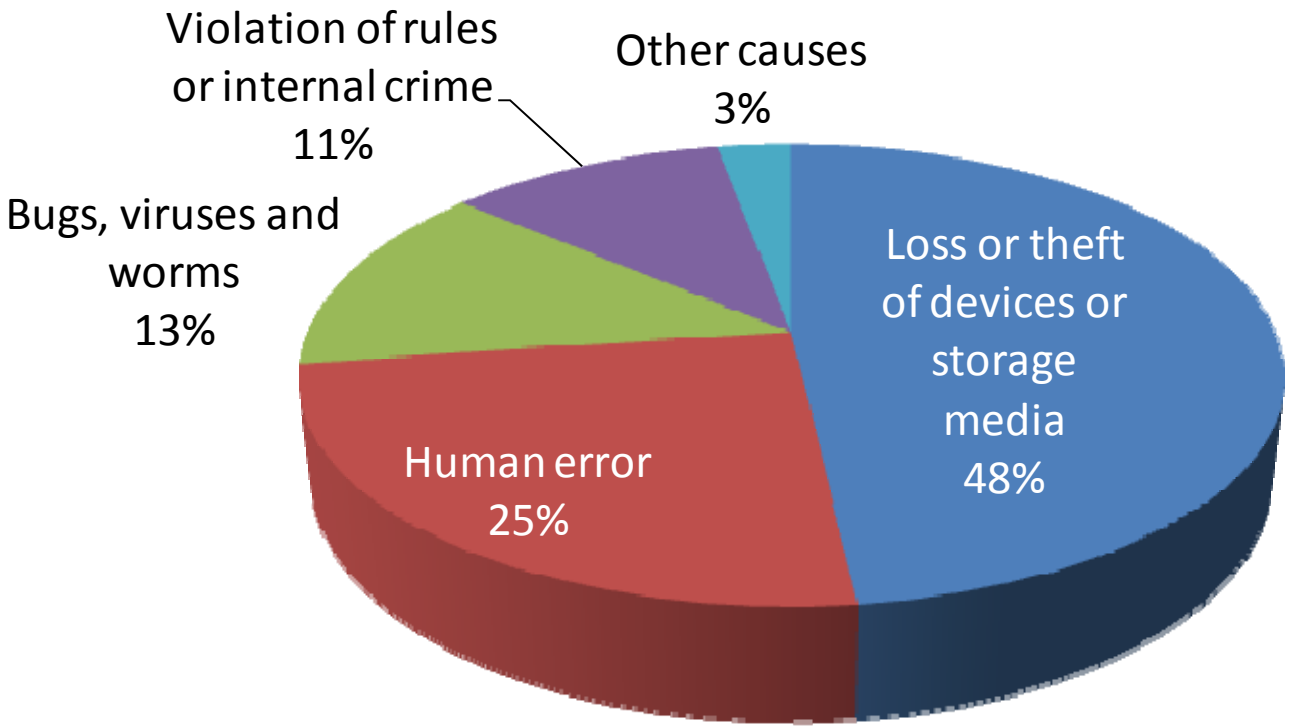
Ref. "Report of Information Security Incidents 2006 (in Japanese)", Japan Network Security Association (JNSA),

Damages per victim depend on:
- Significance of the leaked data
- Response of the entity who leaked them

Usually $50 to several $1000s



Causes of Leaks (Japan 2006)

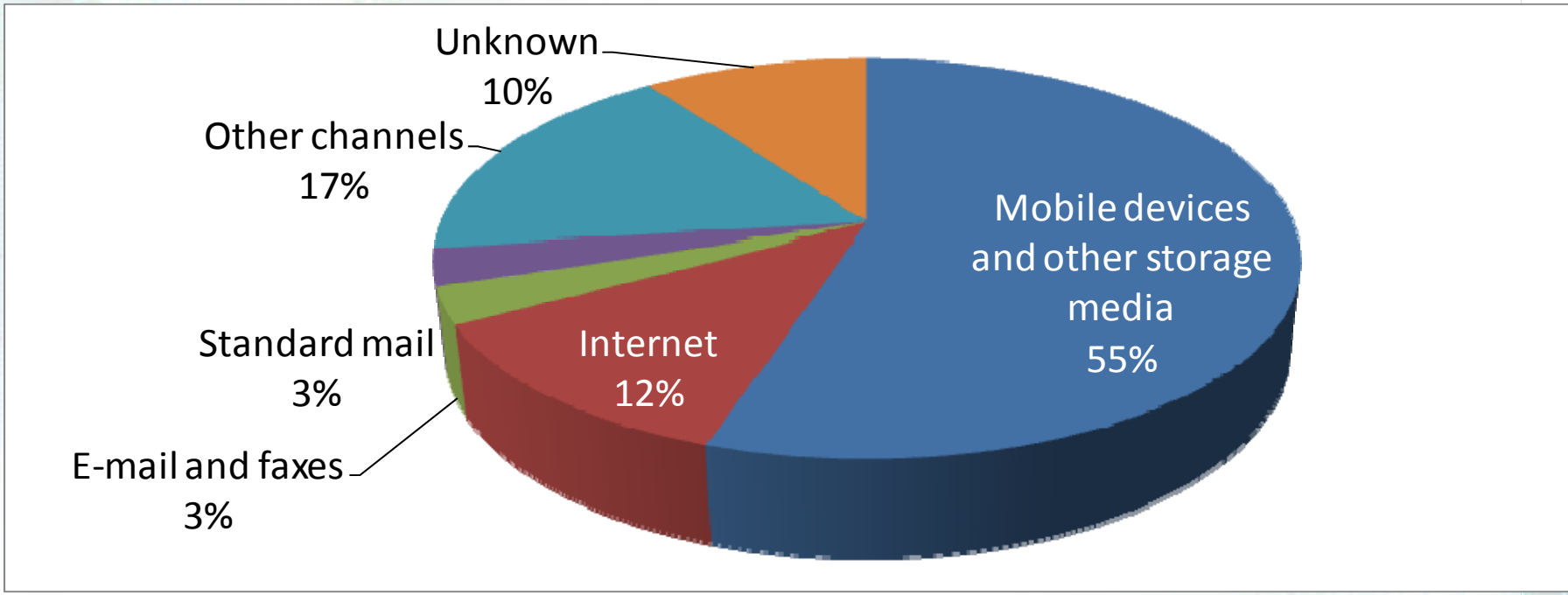


Ref. ”Report of Information Security Incidents 2006 (in Japanese)”, Japan Network Security Association (JNSA),

National Institute of Advanced Industrial Science and Technology
AIST

Channels of Leaks (Across the Globe 2006)

Research Center for Information Security



"Global Data Leakage Survey 2006," InfoWatch, http://www.infowatch.com/threats?chapter=162971949&id=207784626

These statistics show

- Protection of mobile devices and storage media is important to resist against information leakage

- Question is how to protect them?
  - One solution must be encryption but the problem is where to store the decryption key

Trivial Solutions

- How about storing it in TRM?
  - It is still hard to realize perfect TRM with low-cost due to side channel attacks, such as DPA
- How about encrypting it with a password?
  - Short passwords can easily be exhaustively searched
  - Long passwords are hard to remember

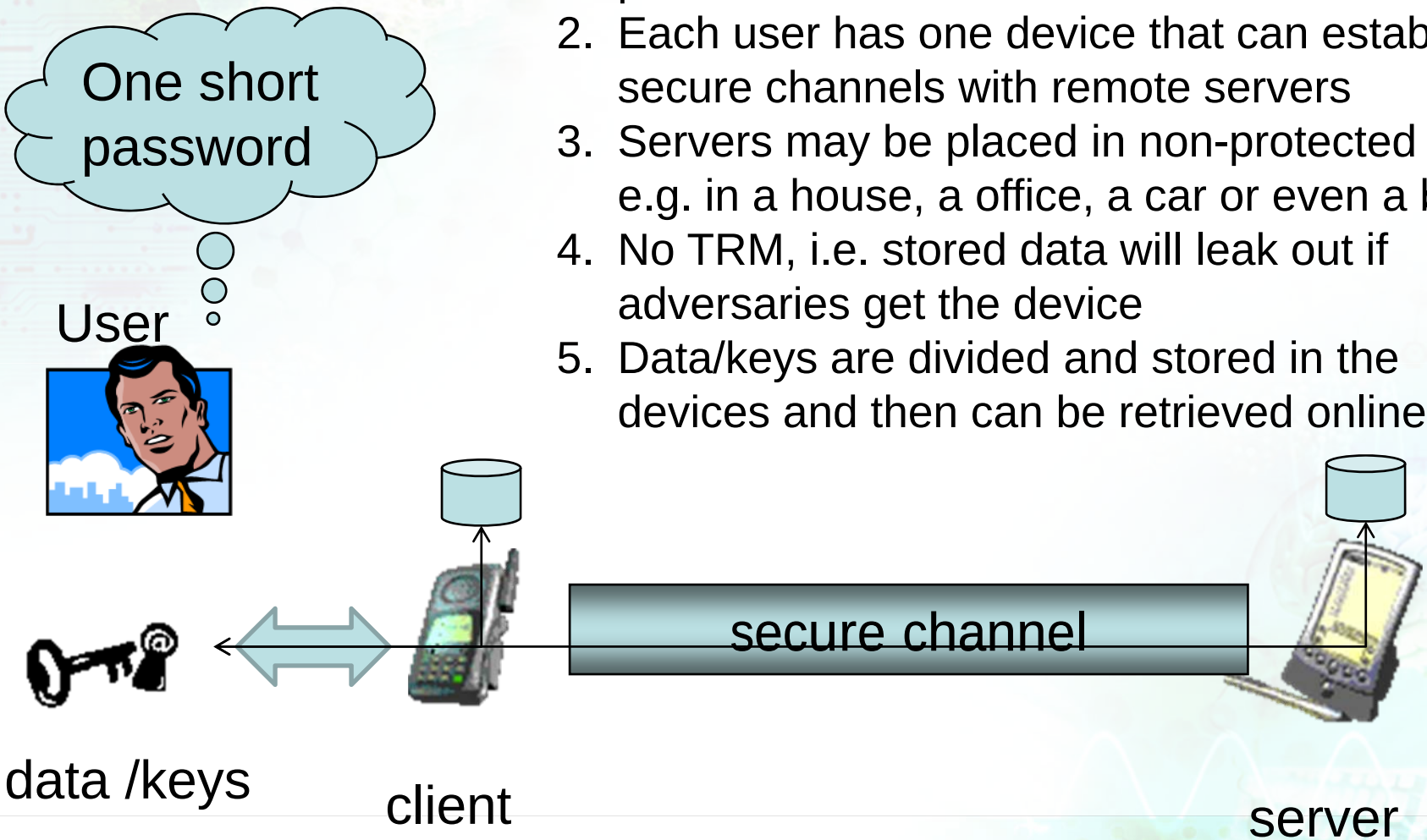
TRM: Tamper Resistant Module
DPA: Differential Power Analysis

National Institute of Advanced Industrial Science and Technology
AIST

Scenario I: Two Node Construction (2NC)

Research Center for Information Security

1. Each user remembers only one short password
2. Each user has one device that can establish secure channels with remote servers
3. Servers may be placed in non-protected area, e.g. in a house, a office, a car or even a bag
4. No TRM, i.e. stored data will leak out if adversaries get the device
5. Data/keys are divided and stored in the devices and then can be retrieved online



Problem 2

- While our scenario assumes leakage
- Most of the currently available protocols are vulnerable against information leakage
  - Since they are designed under the assumption that keys to establish secure channels are protected securely and never leak out
- So, once the keys leak out In their protocols,
  - adversaries can obtain the stored data or/and the user's personal password

National Institute of Advanced Industrial Science and Technology
AIST

Bad Example I (Hashed Password)

Research Center for Information Security

PK

SK

Short password

abduction
abnormal
abolish
absolute
...

h(“abduction”)=?S

h(“abnormal”)=?S

h(“abolish”)=?S

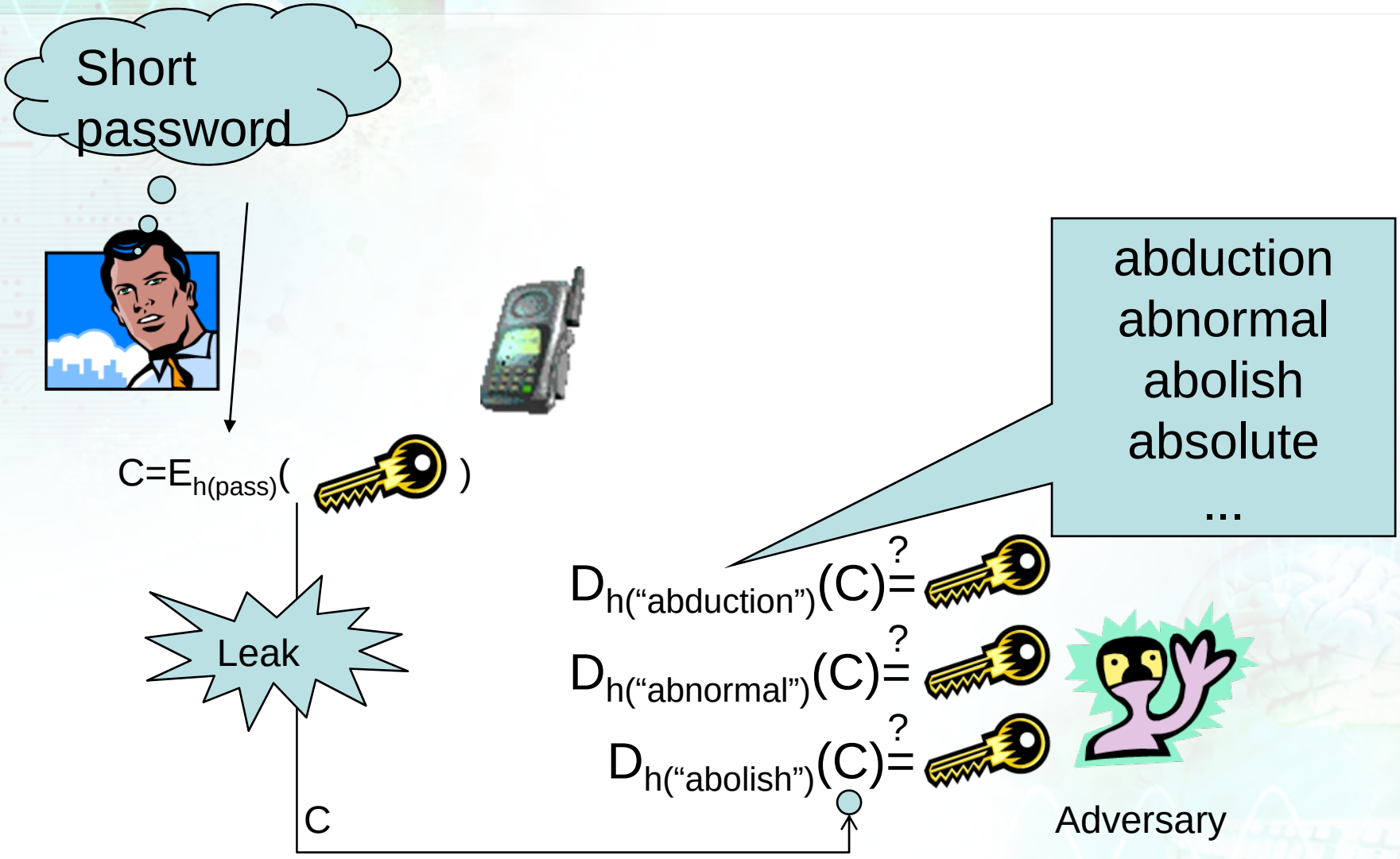
...

h(pass)=S

Leak

S

Bad Example II (PW-Protected-Keys)



Comparison among AKE Protocols

Can adversary obtain data or PW ? ○: No, ×: Yes / Protocols	Eaves dropping	Parallel On-line Attack	Resilience against Leakage			PW to remember
			From client	From server	From both with time difference	
Conventional PW-Only	×	×	○	×	×	Many
PAKE	○	×	○	×	×	Many
PKI（Server Auth.+PW）	○	×	○	×	×	Many
PKI（Server Auth.+PW+OTP）	○	○	○	×	×	Many
KPS+PW	○	○	×	×	×	One
PKI（Mutual Auth.）	○	○	×	○	×	One
LR-AKE（Our proposal）	○	○	○	○	○	One

National Institute of Advanced Industrial Science and Technology
AIST

LR-AKE (Leakage-Resilient AKE)

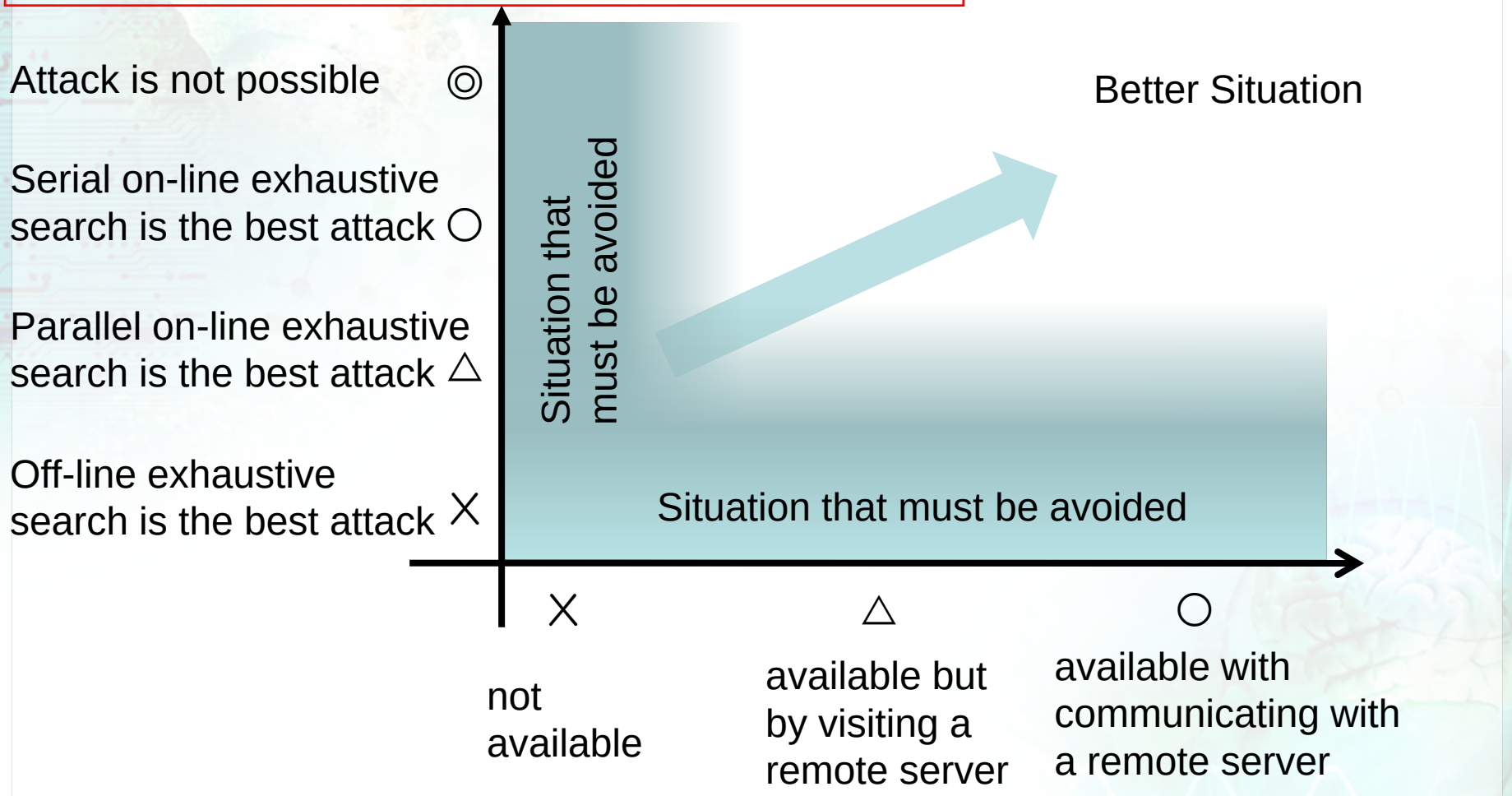
Research Center for Information Security

- New class of AKE (Authenticated Key Establishment) protocols
  - designed under the assumption that
    - Keys (more generally stored secrets) may leak out
  - can resist against information-leakage
- They fit with the scenario we consider

[SKI03] S. H. Shin, K. Kobara, and H. Imai, "Leakage-resilient authenticated key establishment protocols," Proc. of ASIACRYPT 2003, LNCS 2894, pp.166-172, 2003
[SKI07] S. H. Shin, K. Kobara, and H. Imai, "An Efficient and Leakage-Resilient RSA-Based Authenticated Key Exchange Protocol with Tight Security Reduction", IEICE Trans. Vol. E90-A, No. 2, pp. 474-490, 2007
[NGSP] "New Generation Security Project," Ministry of Economy, Trade and Industry, 2005-2007

Leakage-Resilience and Availability

Leakage-Resilience of Stored Data or Password



Availability of Stored Data

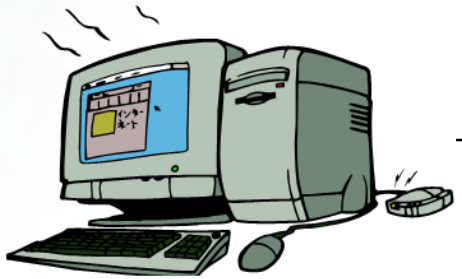
National Institute of Advanced Industrial Science and Technology
AIST

On-line Exhaustive Search

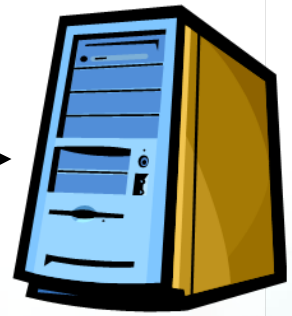
Research Center for Information Security

abduction
abnormal
abolish
absolute
...

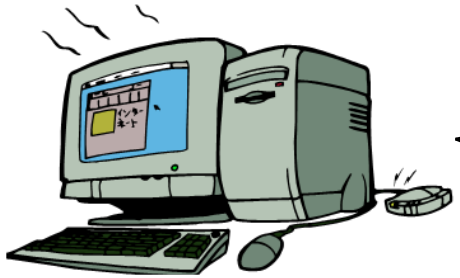
password



Alice, xxxx Alice, xxxx



Serial



Alice, xxxx

Bob, xxxx

Carol, xxxx

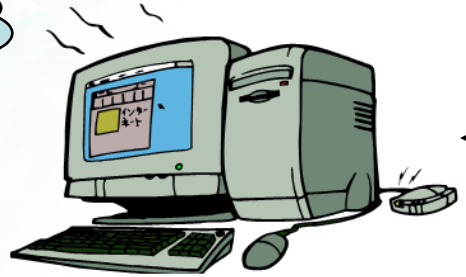
Parallel

National Institute of Advanced Industrial Science and Technology
AIST

Off-line Exhaustive Search

Research Center for Information Security

password

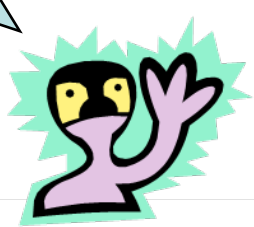


ID	PW
Alice	xxx
Bob	yyy

1. Gets the data for verifying the password
2. Tries password candidates off-line

This can be done with high speed in parallel

abduction
abnormal
abolish
absolute
...



f("abduction") $\stackrel{?}{=}$XXX

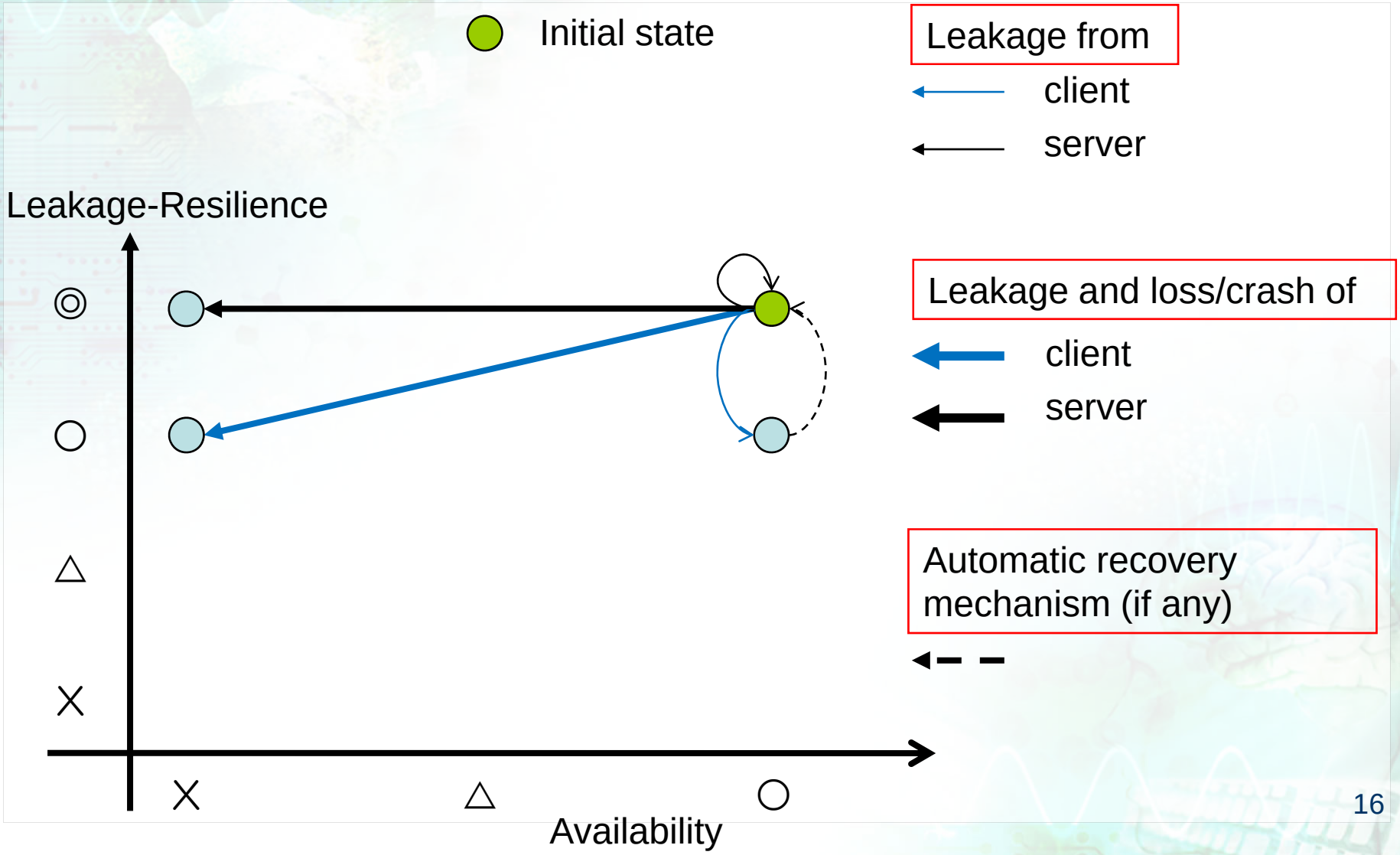
f("abnormal") $\stackrel{?}{=}$XXX

f("abolish") $\stackrel{?}{=}$XXX

...

XXX

Damage against Node Compromise



Conventional PW-Only Protocols in 2NC

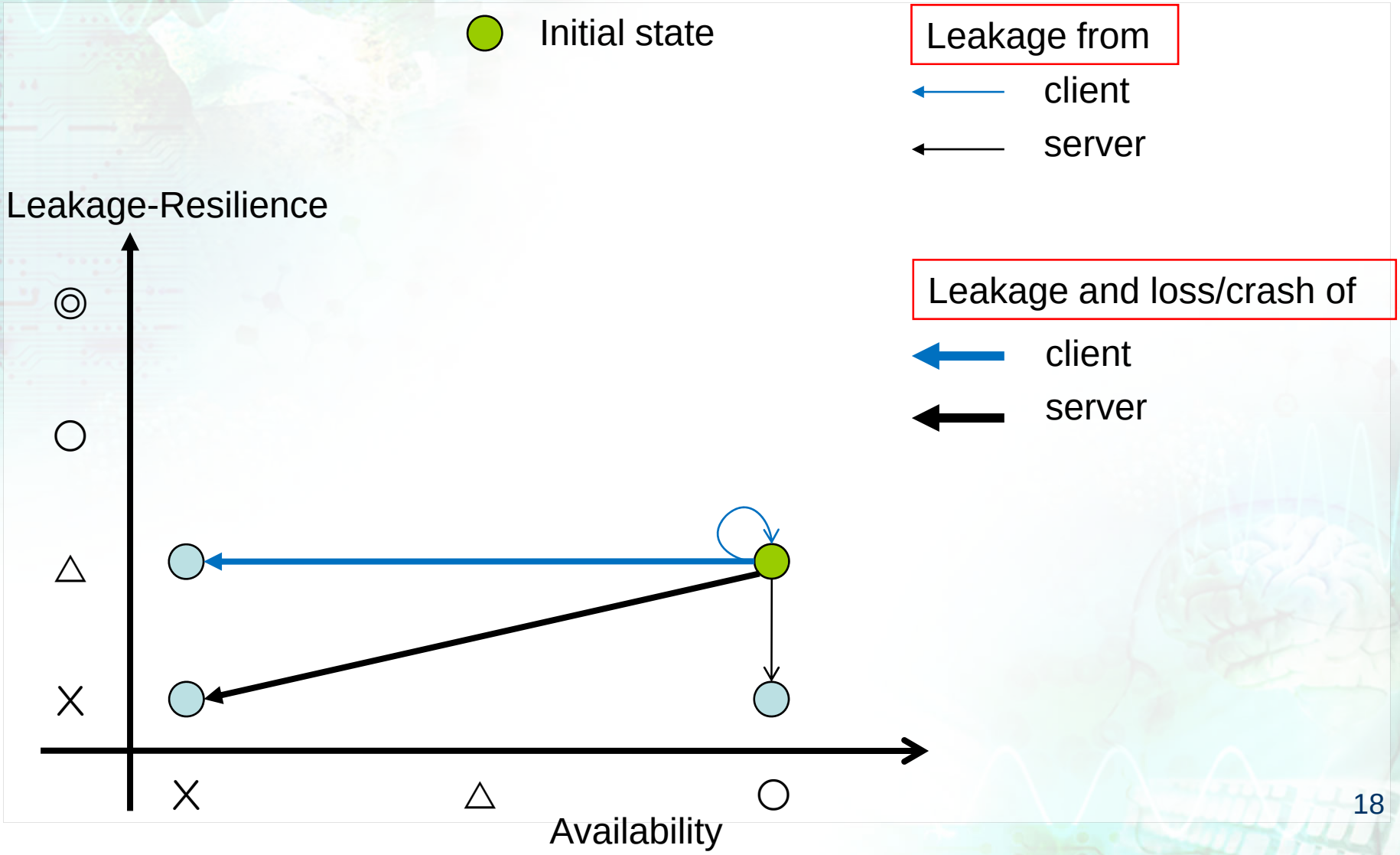
Such as CHAP, IPsec/IKE (PSK), EAP-PSK and so on

Initial state

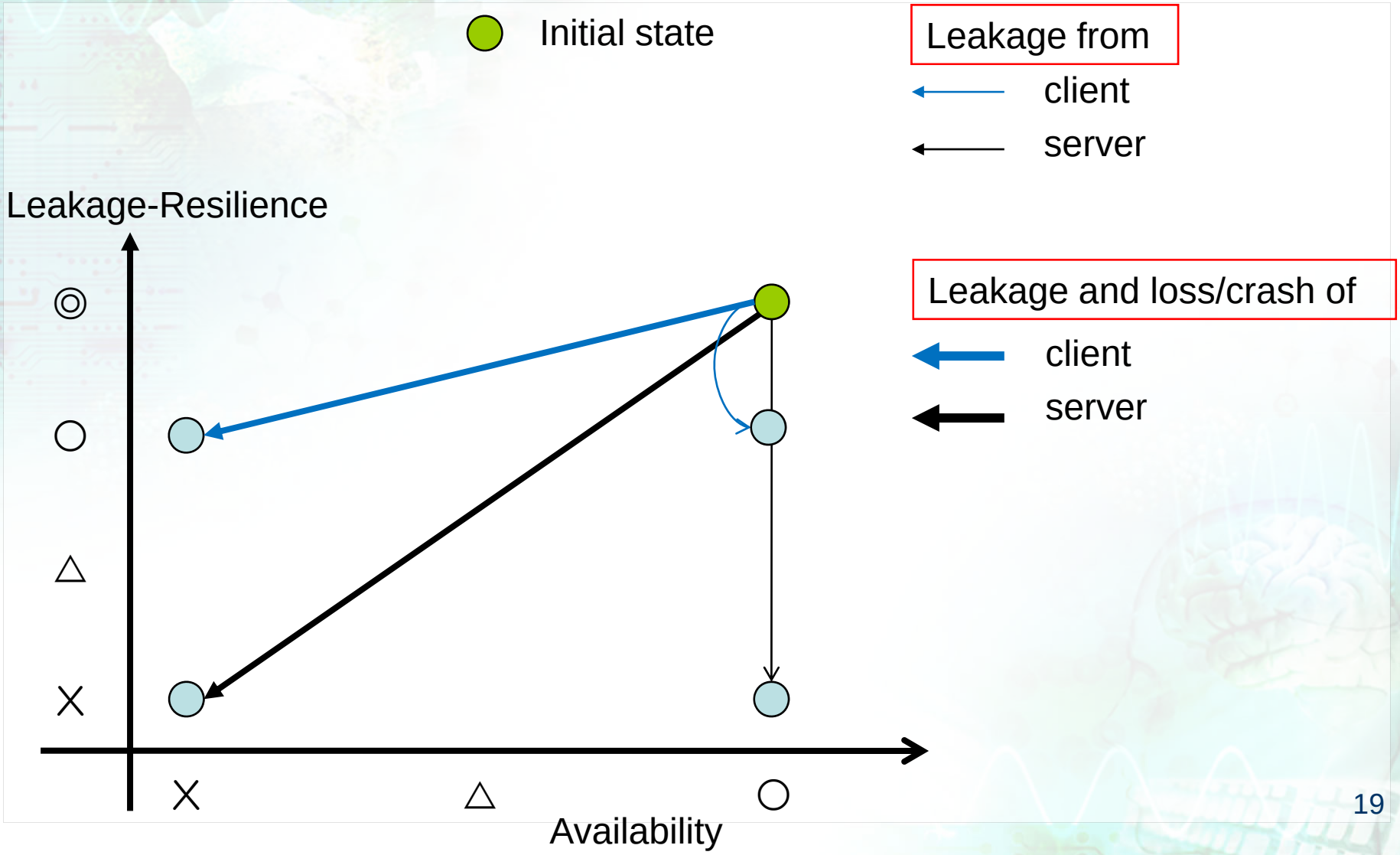
Leakage from
client
server

Leakage and loss/crash of
client
server

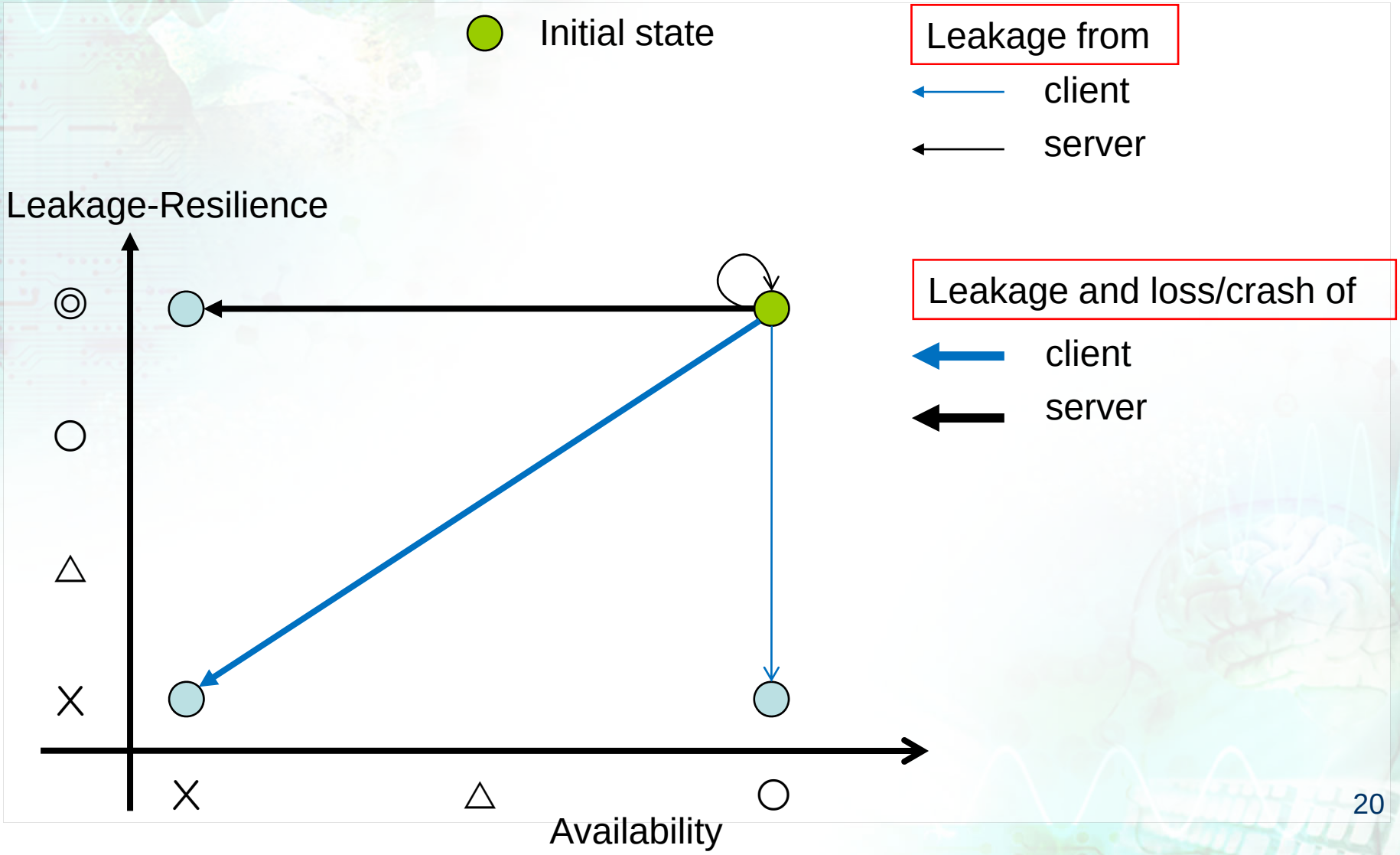
PKI (Server Auth+PW) or PAKE in 2NC



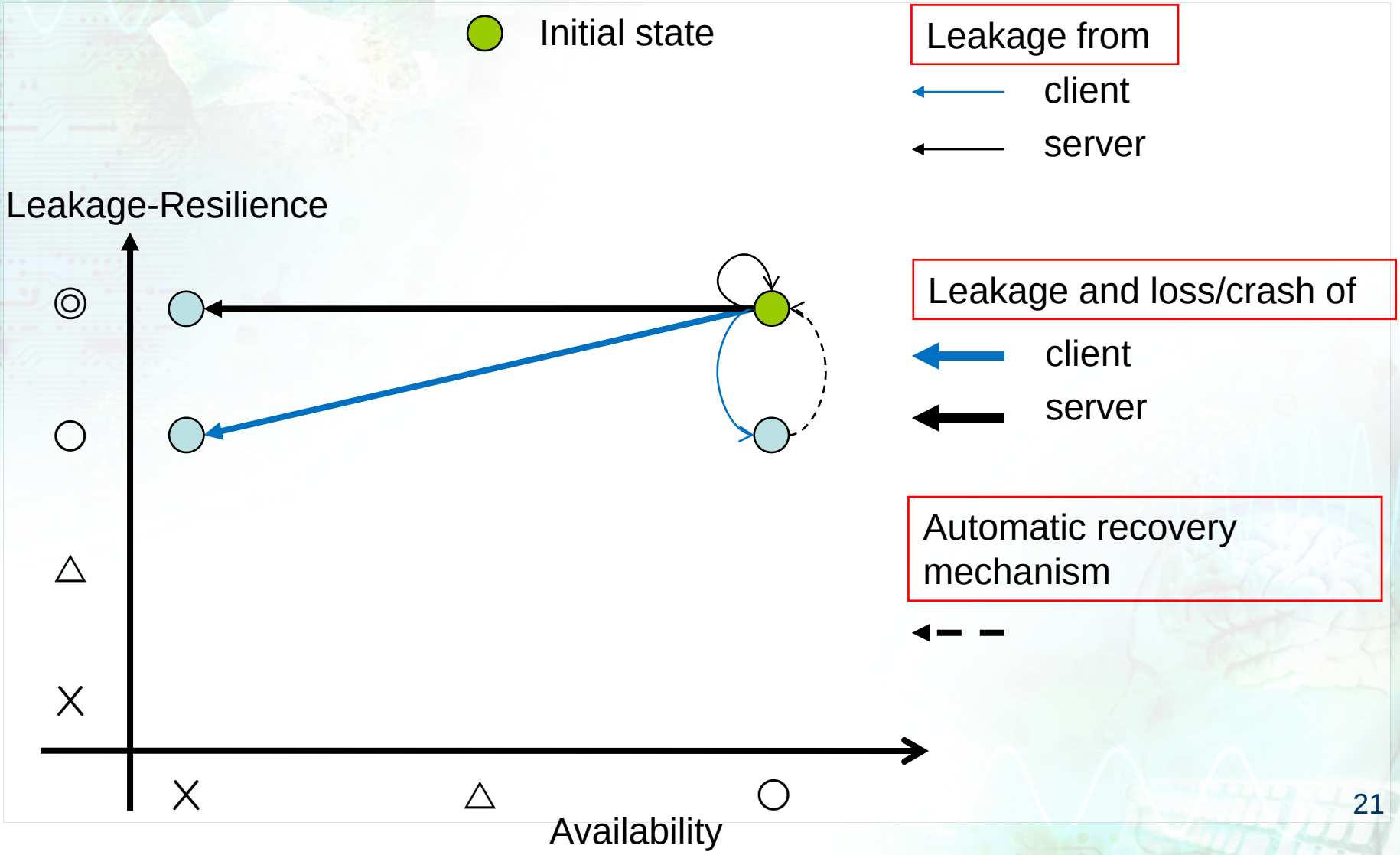
PKI (Server Auth+PW+OTP) in 2NC



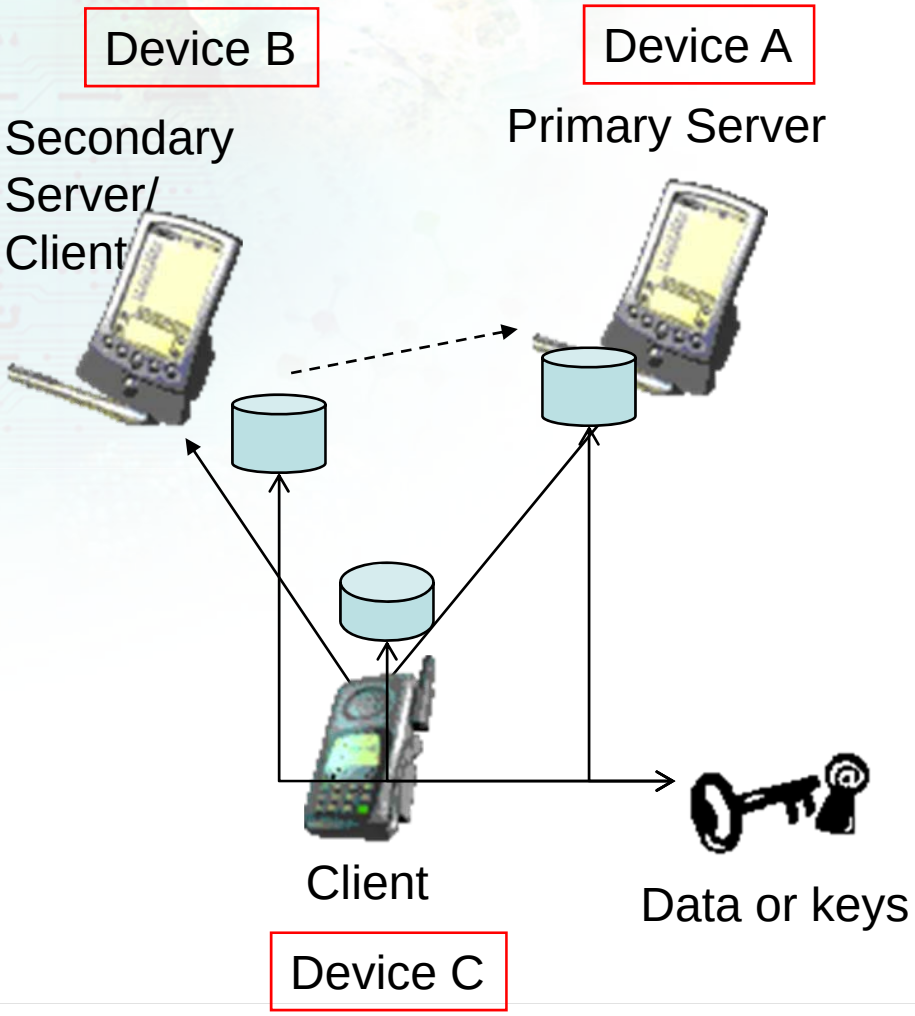
PKI (Mutual Auth) in 2NC



LR-AKE (Single Mode) in 2NC

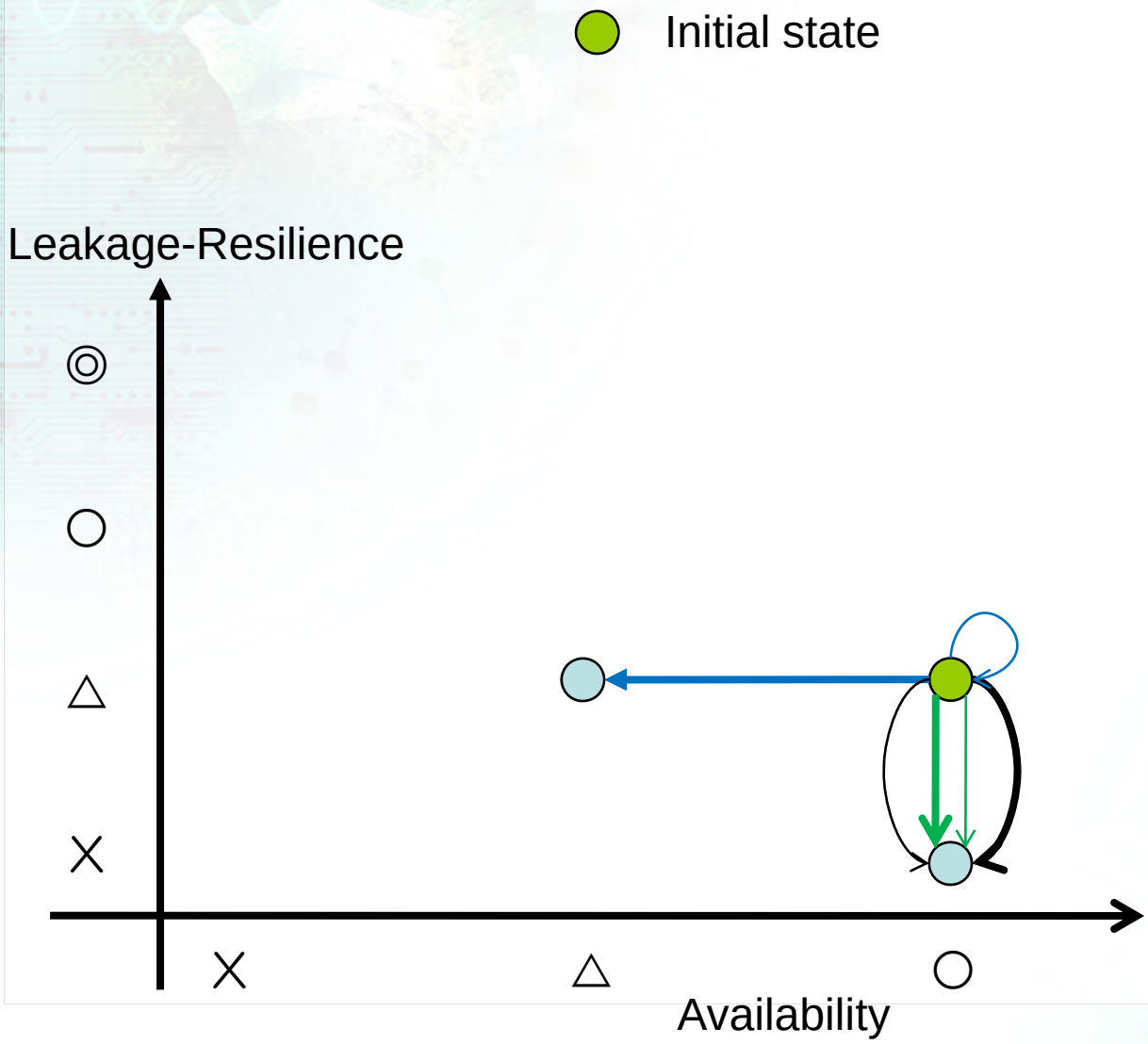


Scenario II : Three Node Construction (3NC [Type A])

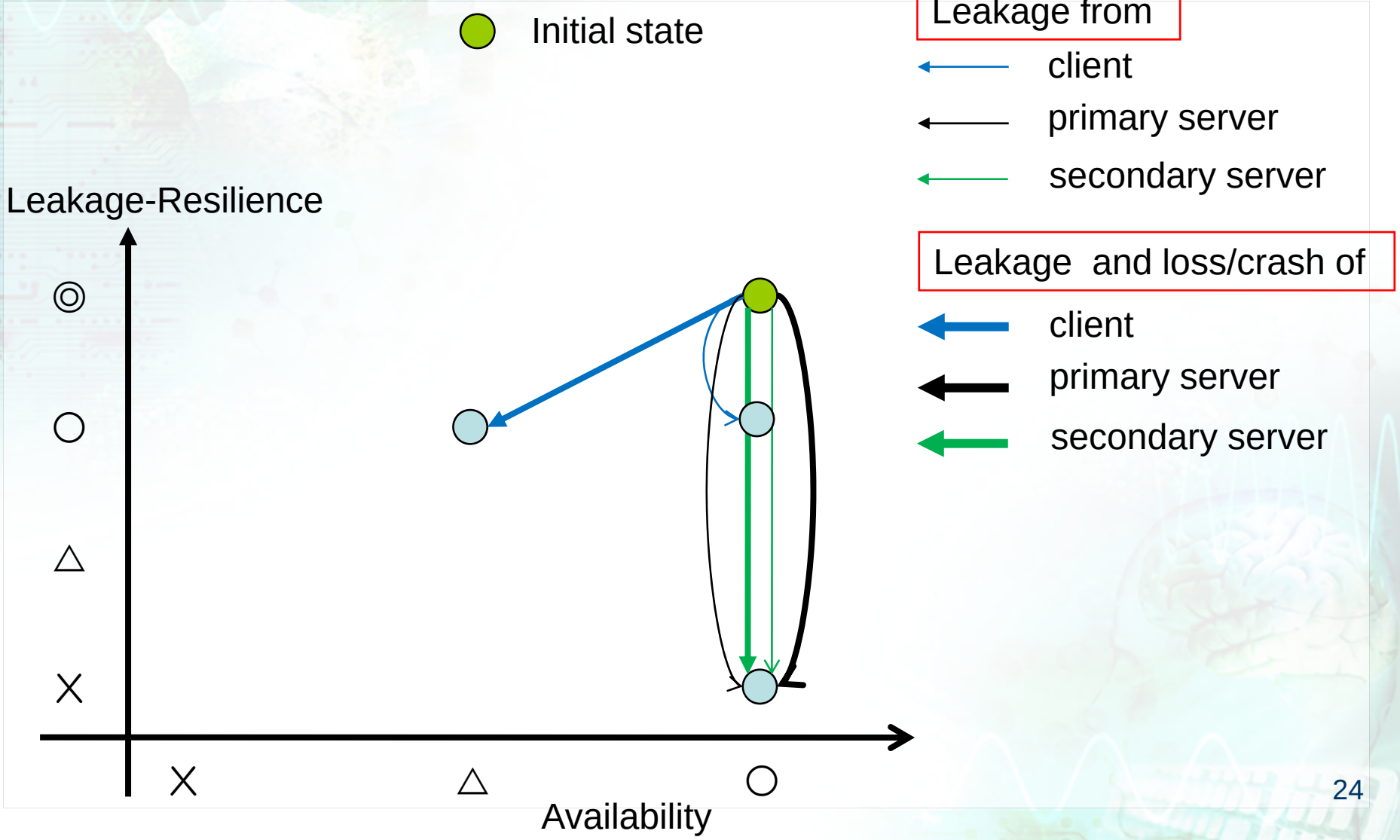


1. A user uses Device C as a client and Devices A and B as primary and secondary servers, respectively
2. When he/she lost Device C, visits at Device B and uses it as a client
3. Data/keys are divided and stored in these devices

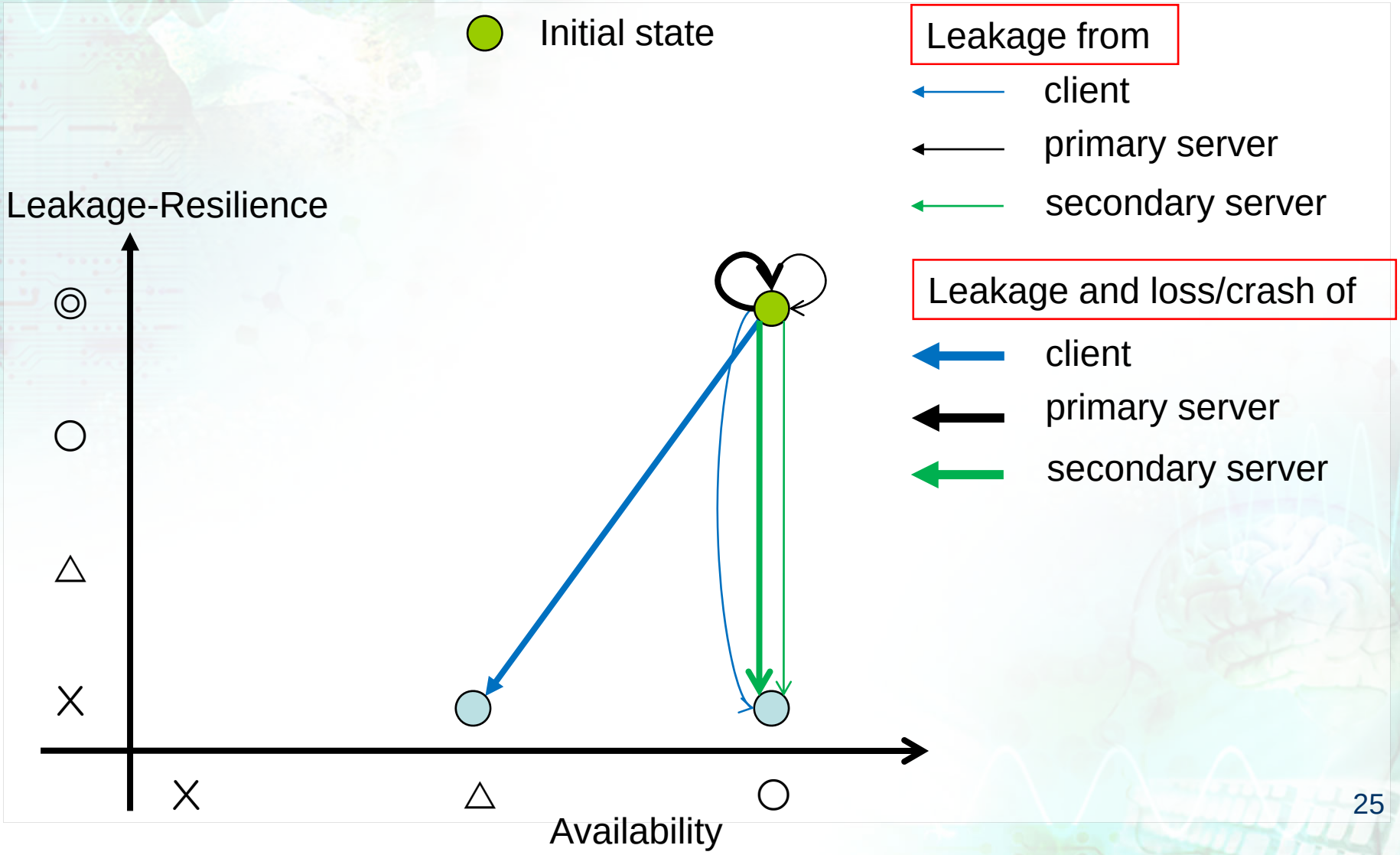
PKI(Server Auth + PW) in 3NC



PKI (Server Auth+PW+OTP) in 2NC



PKI (Mutual-Auth) in 3NC



National Institute of Advanced Industrial Science and Technology
AIST

LR-AKE (Cluster Mode) in 3NC

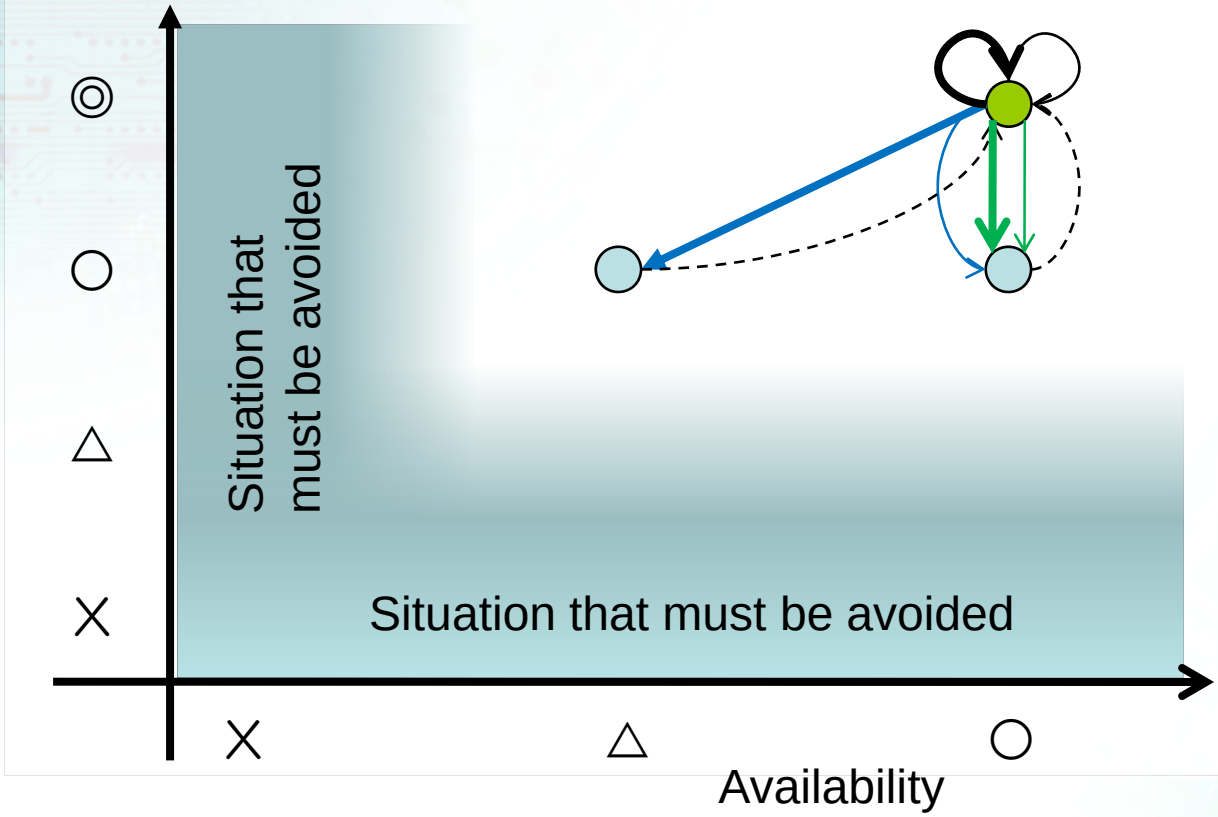
Research Center for Information Security

Initial state

Leakage from
- client
- primary server
- secondary server

Leakage and loss/crash of
- client
- primary server
- secondary server

Automatic recovery mechanism



Conclusion

- Leakage of critical information causes serious problems
- Encryption may be a solution, but the problem is where to store the decryption key
- We considered to store it in a distributed network
- And then showed the relationship of leakage resilience and availability
  - 3NC using LR-AKE has the best leakage resilience and availability