Empowered by Innovation NEC

Group Signatures

Kazue Sako

2011.12.8

k-sako@ab.jp.nec.com

Self Introduction ..Kazue Sako

- Research Fellow in NEC
- Research interest in cryptographic protocols and applied cryptography: worked on electronic voting protocols, fair lottery protocols, auction protocols, etc.
- Editor in **ISO/IEC JTC1 SC27** 'IT Security Techniques'
  - WG5 project 29191 'Partially anonymous, partially unlinkable authentication'
  - WG2 project 20008-2 'Anonymous digital signatures –Mechanisms using a group public key'
- Organizing workshops on '**Real-life Cryptographic Protocols and Standardization**' 1st in Tenerife, 2nd in St. Lucia, co-located with Financial Cryptography
- Program Co-chair for **Asiacrypt** 2012 and 2013.

My current interest

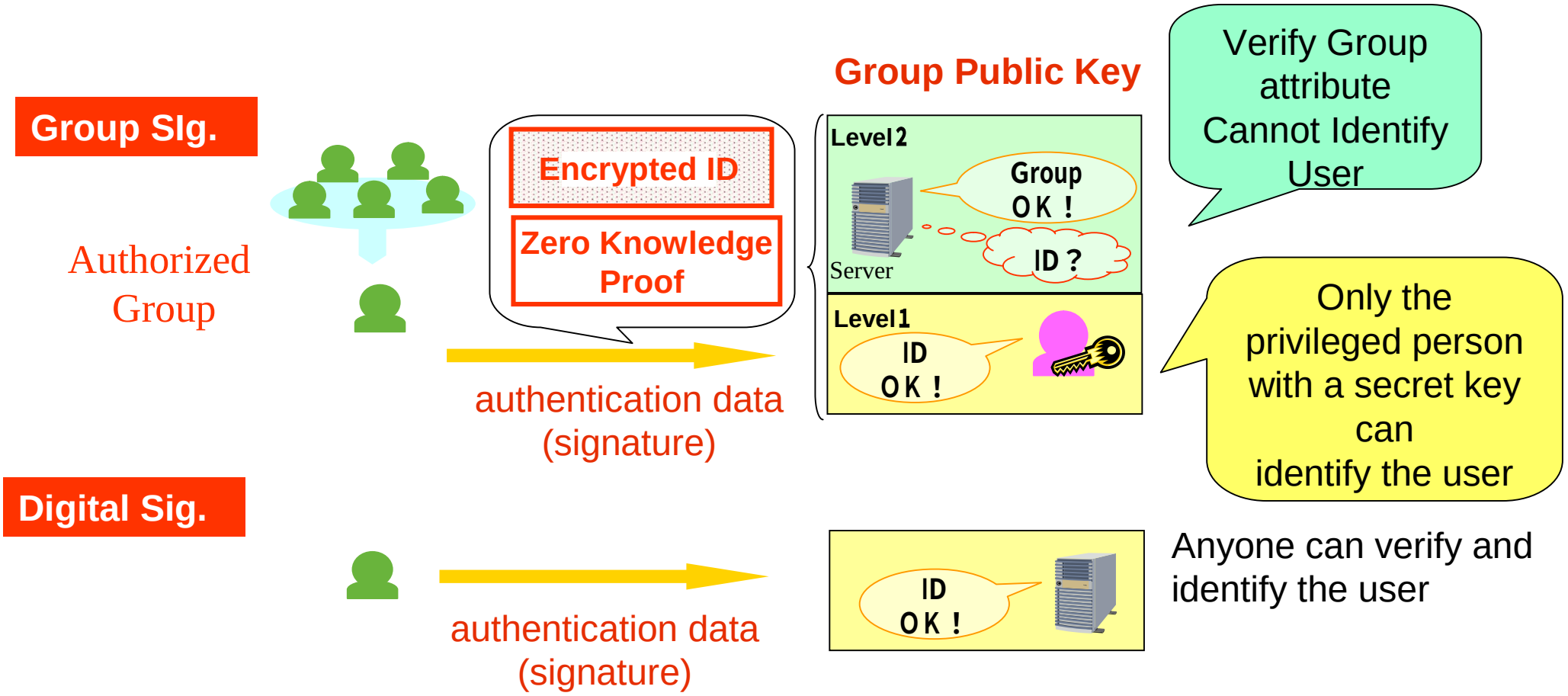
- How can cryptographic protocols can help bring better systems to the real world
  - If we can't help, are we solving a correct question?
  - Cryptography need to compete with light weight solutions with many 'trusted parties/trusted software' where people are currently satisfied with.
  - Satisfaction to the cryptography-based system must exceed the cost to implement / manage the system.
- Privacy may be a 'correct' field of question..
  - Yet there are other obstacles from legacy world such as IP address and MAC address
- We need to talk with real life engineers/ system designers in order to pursuit 'correct' question.
  - Firs step is to give them a good understanding of 'magics' brought by cryptography.

Our enthusiasm to Group Signatures

- In 1991, a wonderful notion of Group Signatures were proposed by D. Chaum and Van Heyst but it was very impractical. (computation proportion to the size of the group)
- In 1997, an improvement of Group Signatures were proposed one by J. Camenisch (ETH Zurich) et al and the other by J.Kilian (NEC Research Institute) and Petrank as Identity Escrow.
- I thought this is a wonderful technology solving the issue of security and privacy that the world should benefit more by implementing this technology

How we regard Group Signatures

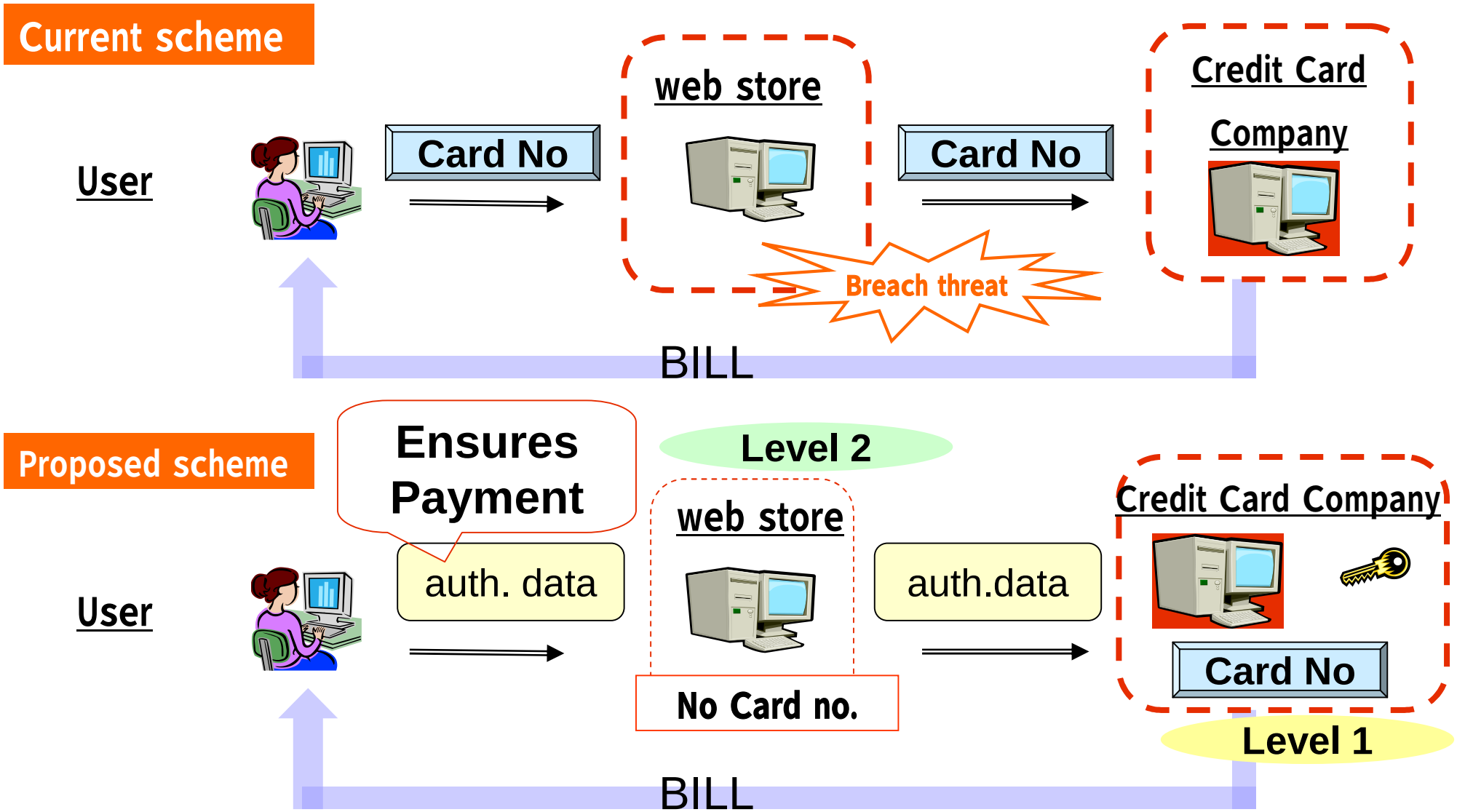
- Generating a single authentication data which provides two levels of verification



Looking for a compact application

- It would be great if Group Signature would replace PKI, but this requires too large revolution.
- Any other persuasive scenario?

Application of Group Signatures：Internet shopping



Application of Group Signatures：Outsourcing scenario

Current scheme

User

Group, ID

Entrance Gate

Group,ID

Company

Breach threat

Proposed scheme

User

Ensures Group

auth. data

Level 2

Entrance Gate

No Card no.

auth.data

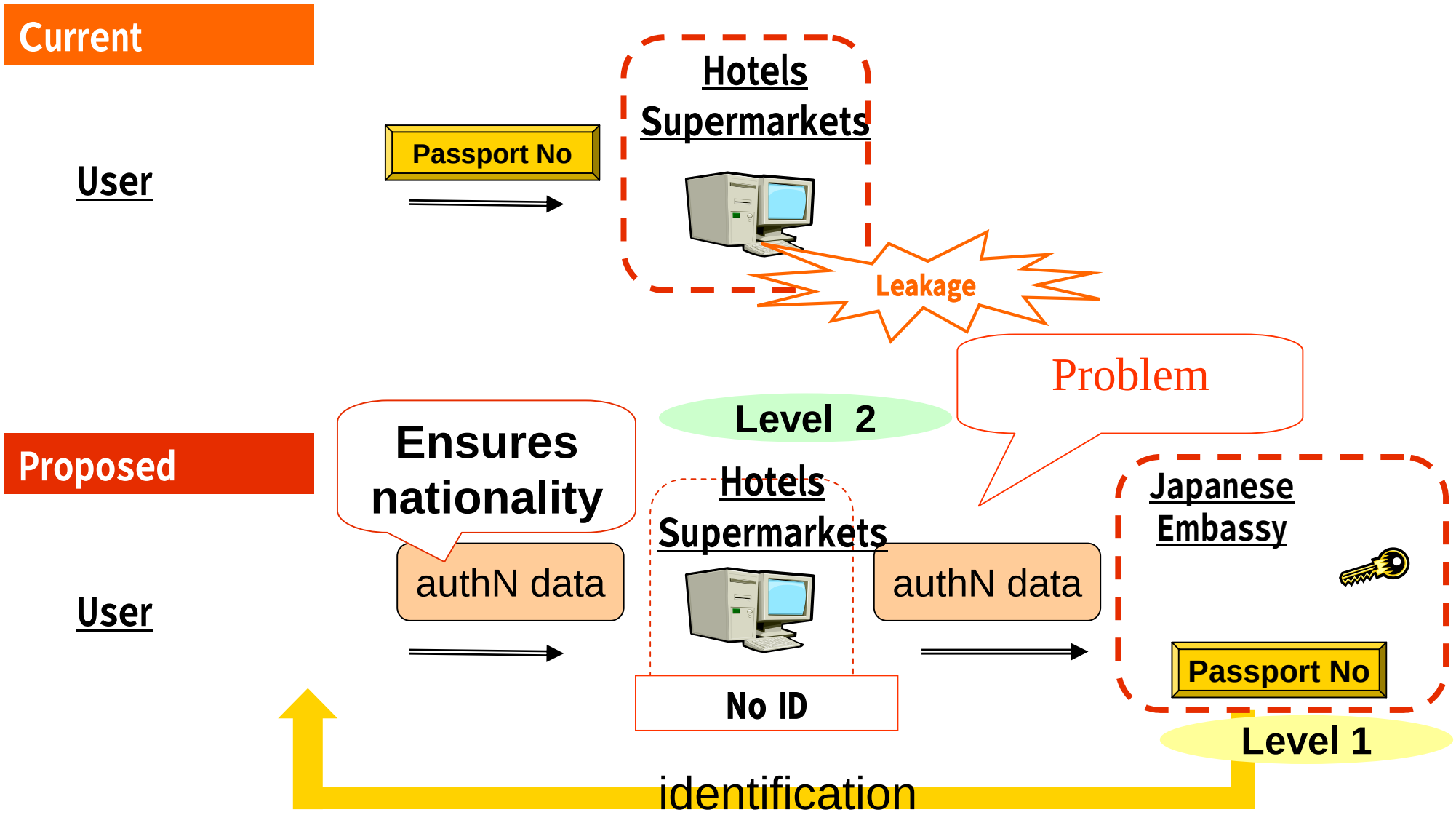
Company

ID

Work Record

Level 1

Application example : Passports



Other applications: Car to Car communication

Current

Car

Traffic Jam!

Vehicle ID

messages are broadcasted with Vehicle ID

Makes it easy to trace cars

Proposed

Car

Traffic Jam!

Authenticates message

authN data

Level 2

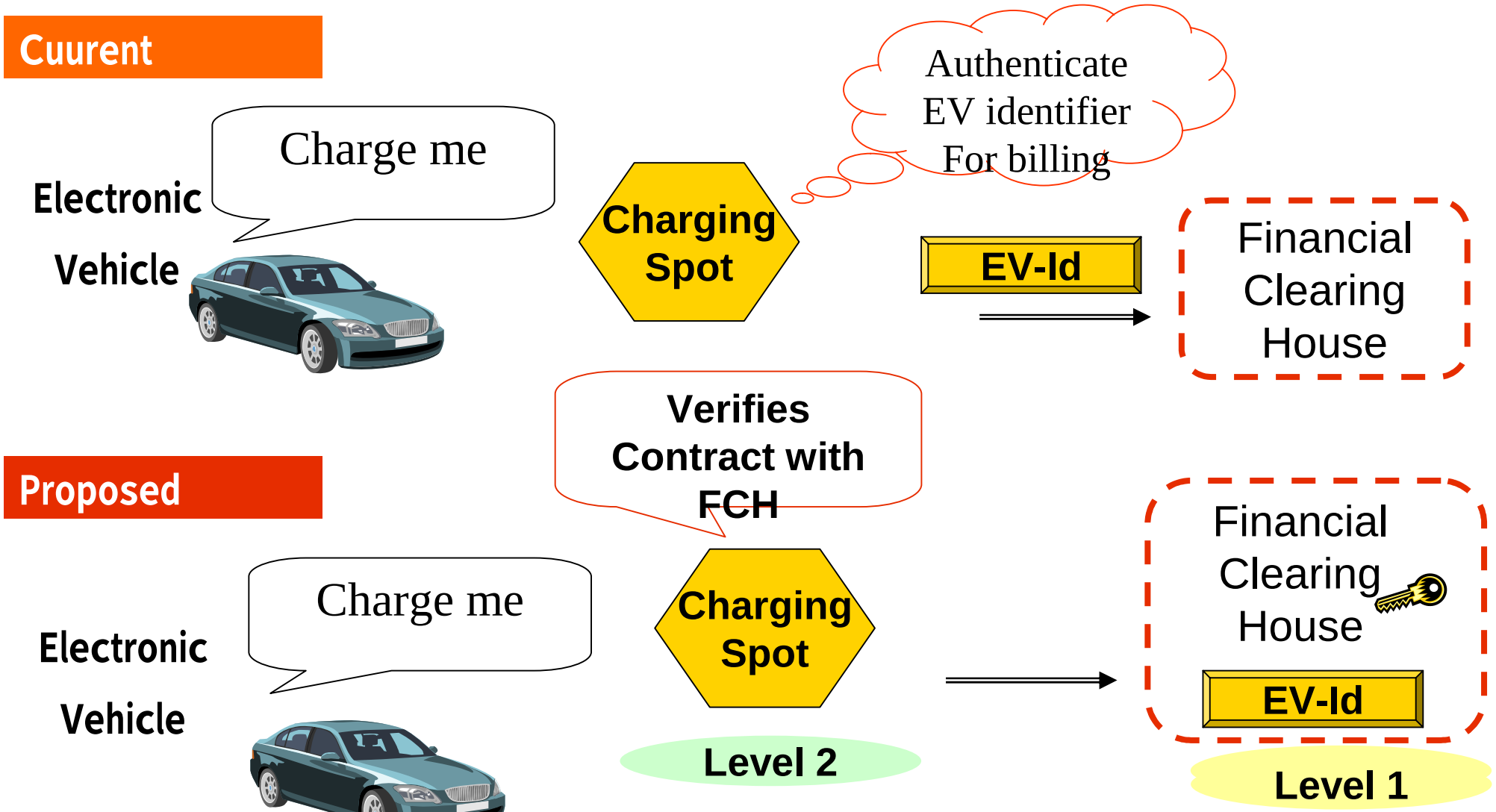
Police

Vehicle maker

Vehicle ID

Level 1

EVCharging

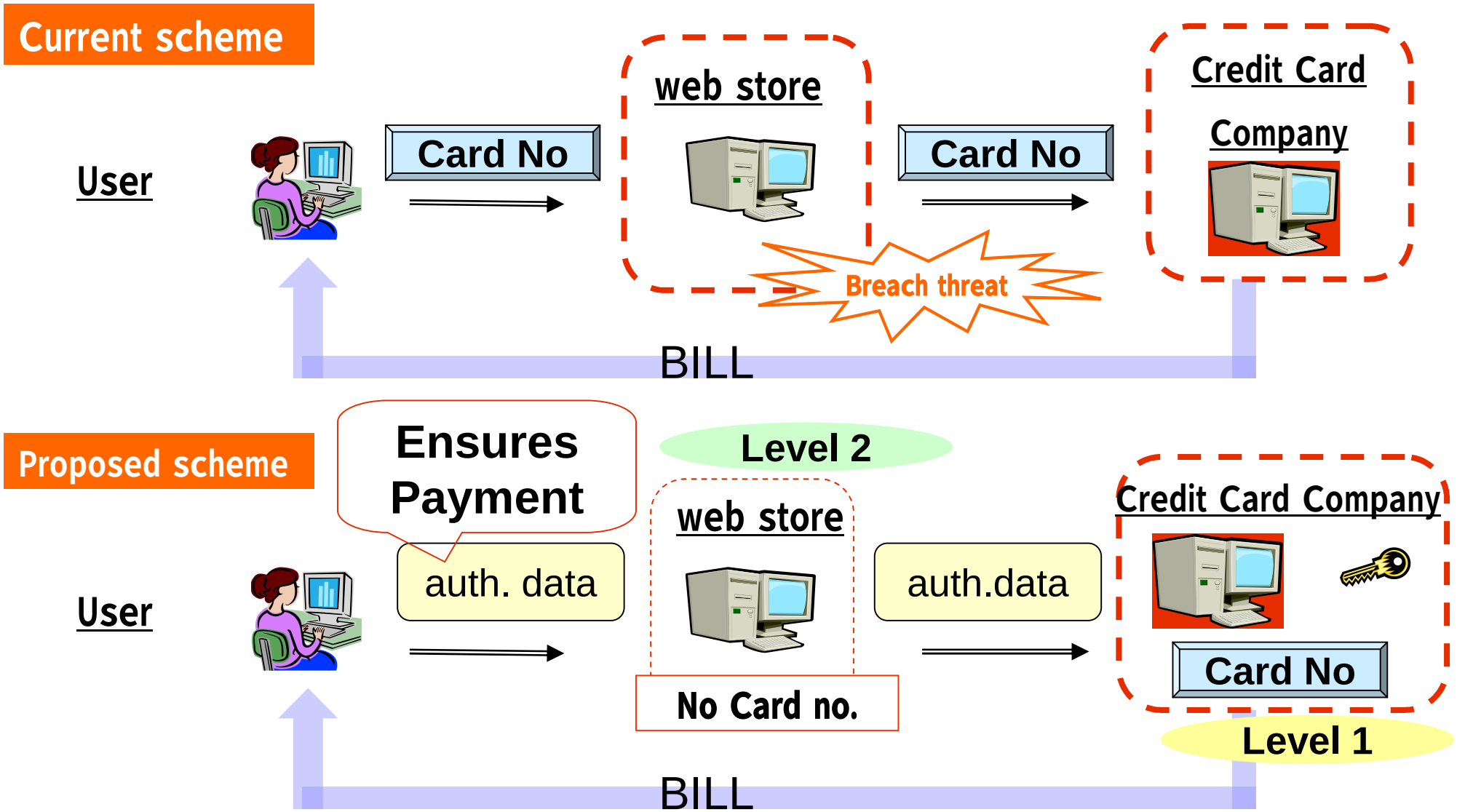


Our Observations

- Group Signature would best suit **off-line transaction**
  - As network connection is cheap in on-line transaction, one-time credential would be more powerful in on-line transaction
  - Privacy of network connection are often interfered by IP address.
  - We need NEW applications, because existing systems are designed to use identifiers.

.

Application of Group Signatures：Internet shopping



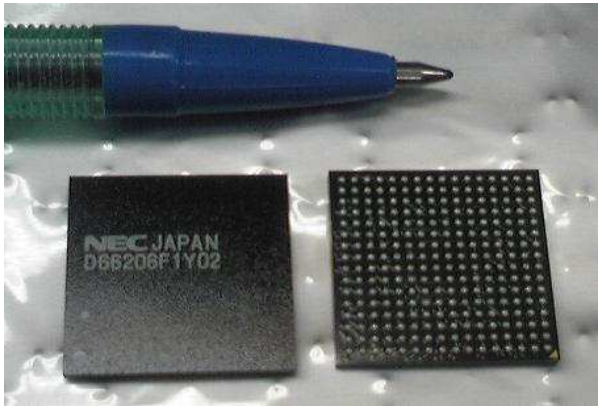
Our Observations

- Group Signature would best suit off-line transaction
  - As network connection is cheap in on-line transaction, one-time credential would be more powerful in on-line transaction
  - Privacy of network connection are often interfered by IP address.
  - We need NEW applications, because existing systems are designed to use identifiers.
- In off-line transactions, users carry small devices, such as mobile phones or smart cards.
  - If you authenticate portable devices, location privacy is often an issue.
  - How can we have small portable devices compute group signatures?
- A co-processor helped to disseminate RSA in smart cards… We need a co-processor for group signatures!!
  - It could be used not only for group signatures, but also for other cryptographic protocols as it implements modular arithmetic, hash function, ECC computation, etc.

The world's first (to our knowledge) LSI for group signatures (2010)

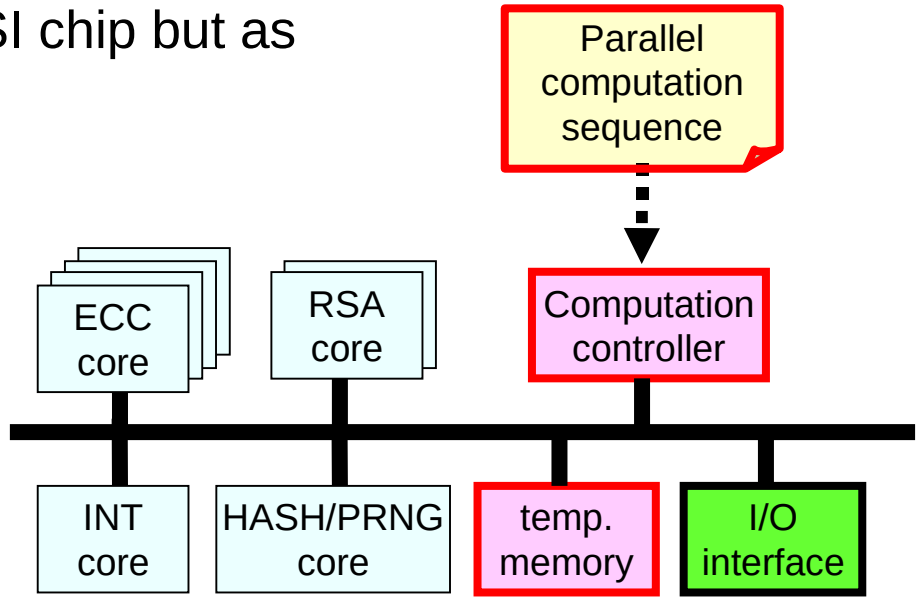
Features

- Fast signature generation/verification speed.
  - 0.1 seconds at 150MHz clock
  - Same speed with S/W on 3GHz clock PC
- Low power consumption.
  - Less than 0.6W at 150MHz clock
  - 1/100 or less power compared to PC (60W or more)
- Usable not only as an independent LSI chip but as an IP core ($2mm^2$)



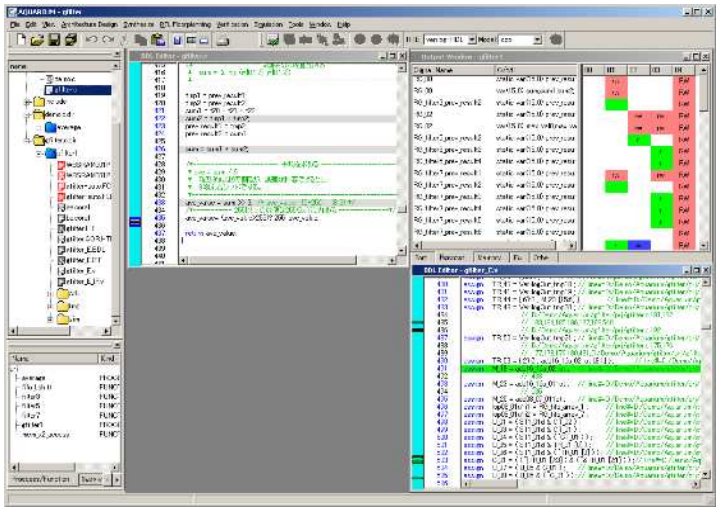
Development story

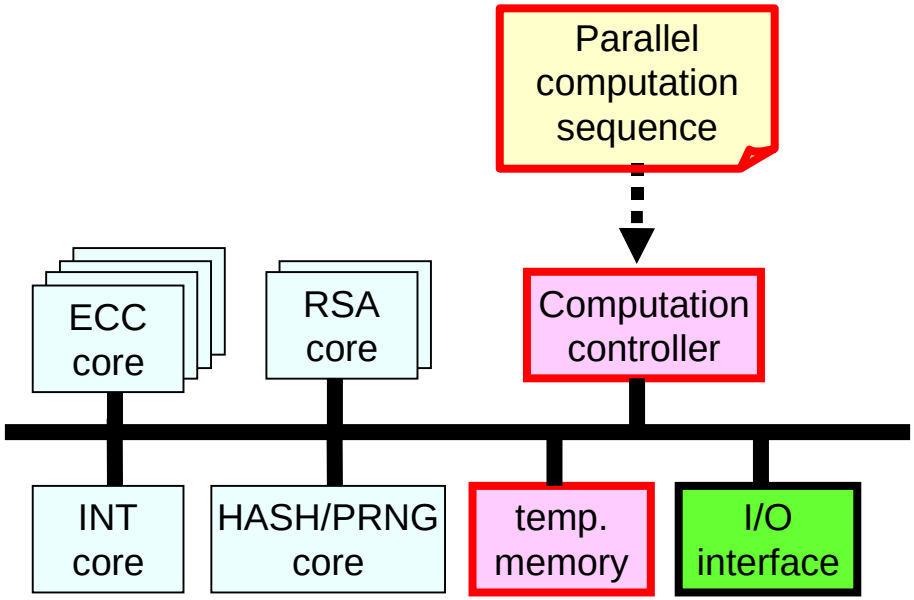
- 3 years efforts of exploring design strategy and H/W architecture.
- Achieved best trade-off balance of performance, circuit size and power consumption.



Selling point..

- NEC had a division that produces LSI… there still is a research division within NEC that designs LSI for algorithms written in C
- With the help of **NEC original behavioral synthesizer**, 10K lines of C code resulted in 800 K gates of group signature computation accelerator
- Easy to make estimations in various conditions.
- Computation controller can manage to compute other cryptographic schemes.





Our other approach

- We'd be ready to implement group signatures/ anonymous credential to small devices once they are needed… but when will it be needed?
- People may not know that there is this wonderful technology that may solve their privacy issues they are suffering!
- Have them learn that such technology exist, and is ready to be used internationally…. Why not have a international standard?(2008)
- ISO/IEC JTC 1 SC27 Security techniques
  - WG5 (Identity Management and Privacy) Convenor: Kai Rannenberg

    ‘’29191 **‘Partially anonymous, partially unlinkable authentication**’’(3rd CD)
  - WG2 (Cryptographic Mechanisms) Convenor Takeshi Chikazawa

    ‘’ 20008 **Anonymous Digital Signatures**’’ (1stCD)

    ‘’ 20009 **Anonymous Entity Authentication**’’ (1stCD)

Conclusions

- How can cryptographic protocols can help bring better systems to the real world
- Perhaps we can start talking with real life engineers how group signatures and its variants can help enhance privacy with satisfactory cost.
- We are ready for low power comsumption with LSI, what else are requirements?
- A good application is necessary for learning lessons.

Part of results presented in these slides were sponsored by Japanese Ministry of Internal Affairs and Communications.

Empowered by Innovation