Kyushu University,
Cyber Security Center
January 21st, 2015

Security Evaluation of Next-Generation Cryptography by Collaboration with Industry, Government and University

Tsuyoshi Takagi

Kyushu University
Institute Mathematics for Industry
http://imi.kyushu-u.ac.jp/~takagi/

Cryptography in Modern Society

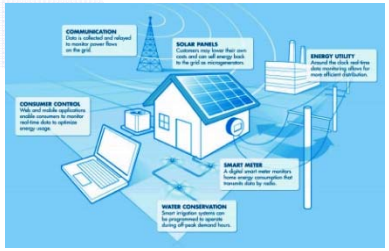
Old Cryptography

Special technology used by limited purposes

Contemporary Cryptography

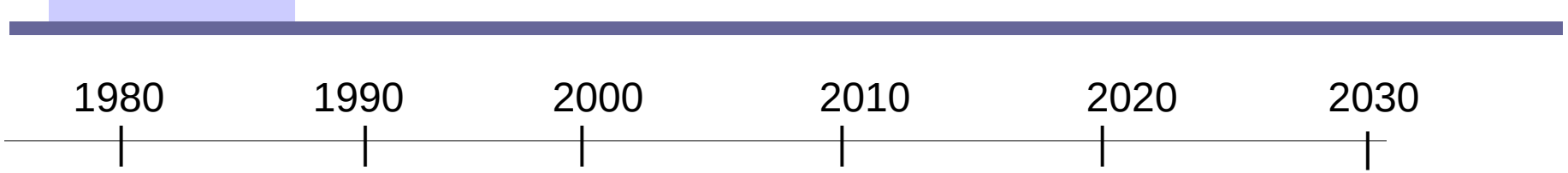
Daily used technology

http://www.e-gov.go.jp/



Cryptography is fundamental technology.

History of Public-Key Cryptography



RSA (widely used in such as SSL, integer factorization problem)

widely used

Elliptic Curve Cryptography (short keys, used in embedding devices)

Pairing-based cryptography (novel crypto protocols)

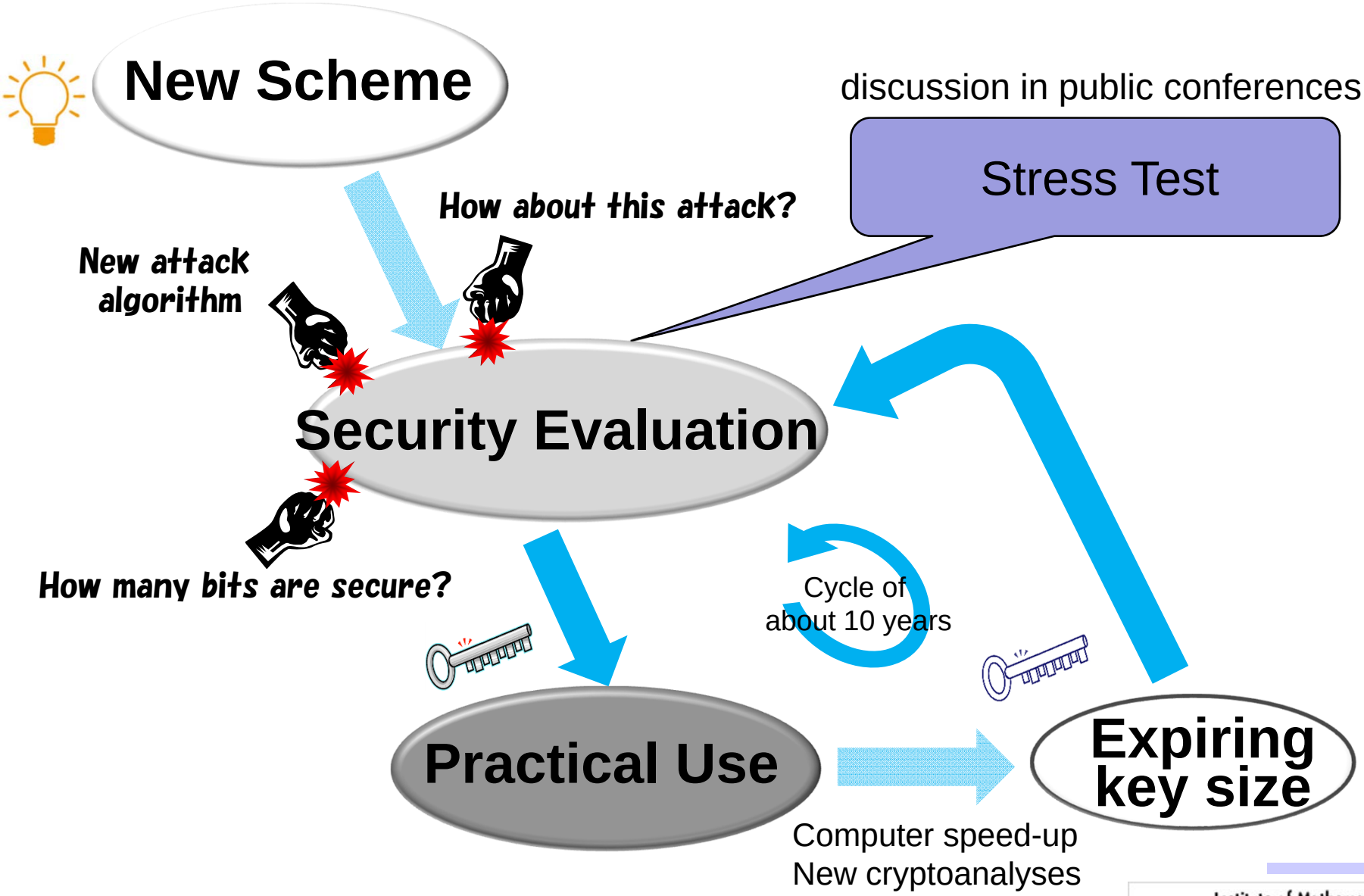
some products, some standardizations

Post-quantum cryptography
(code-based, lattice-based, multivariate polynomial based, etc)

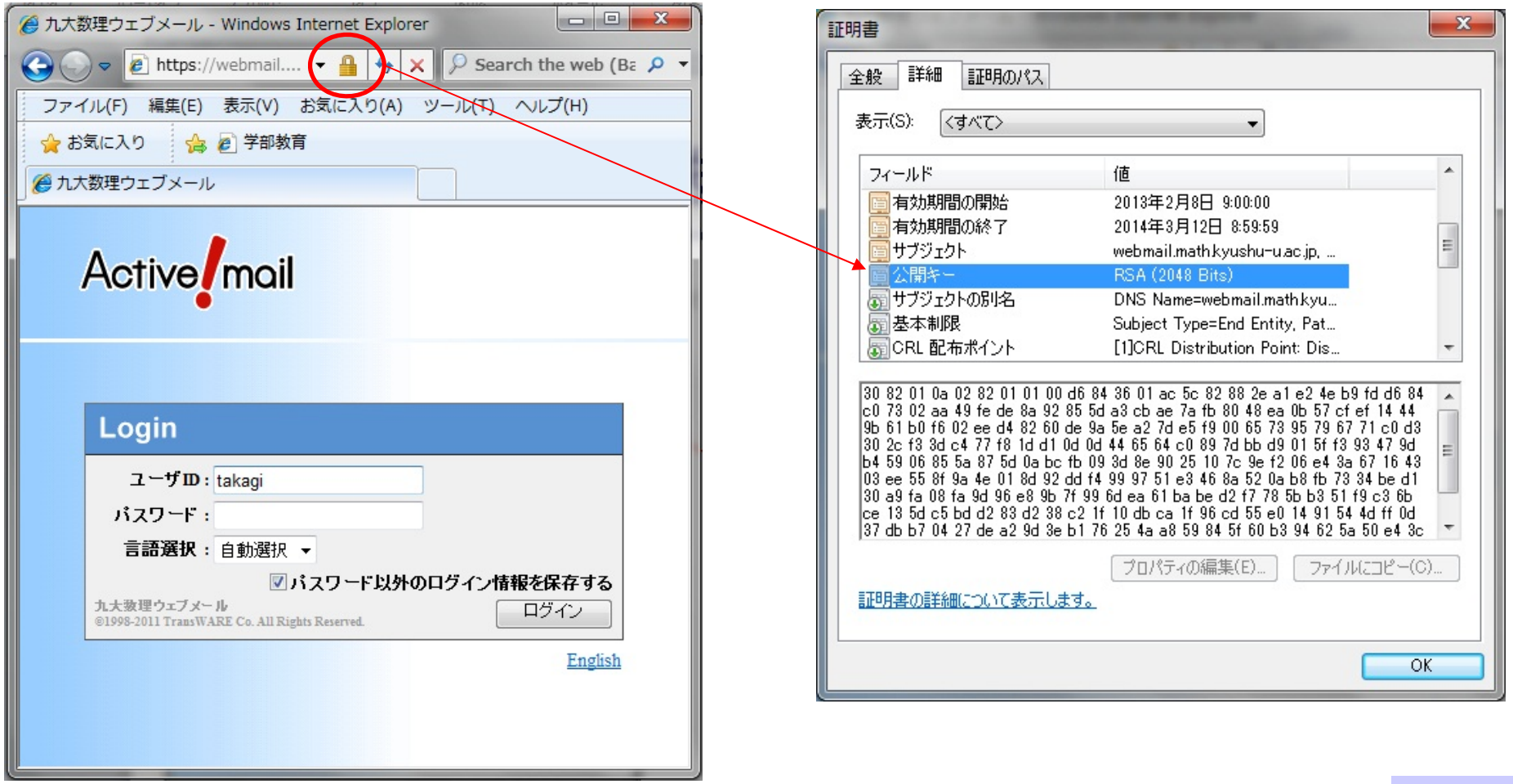
Fully homomorphic encryptions, multi-linear maps

research phase

Security Evaluation Cycle



Example of RSA public key



Current record for factoring integers

- January 2010, 768 bits, 1500 CPU years, Aoki et al.

- 123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3
  =
  334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994 89
  ×
  367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089 17

Cryptography Research and Evaluation Committees in Japan

CRYPTREC
Cryptography Research and Evaluation Committees

http://www.cryptrec.go.jp/

JAPANESE

- About CRYPTREC
- Organization of CRYPTREC
- History of CRYPTREC
- CRYPTREC Report
- Technical Report
- e-Government Recommended Ciphers List
- Specifications of e-Government Recommended Ciphers
- Guide to Related Organizations

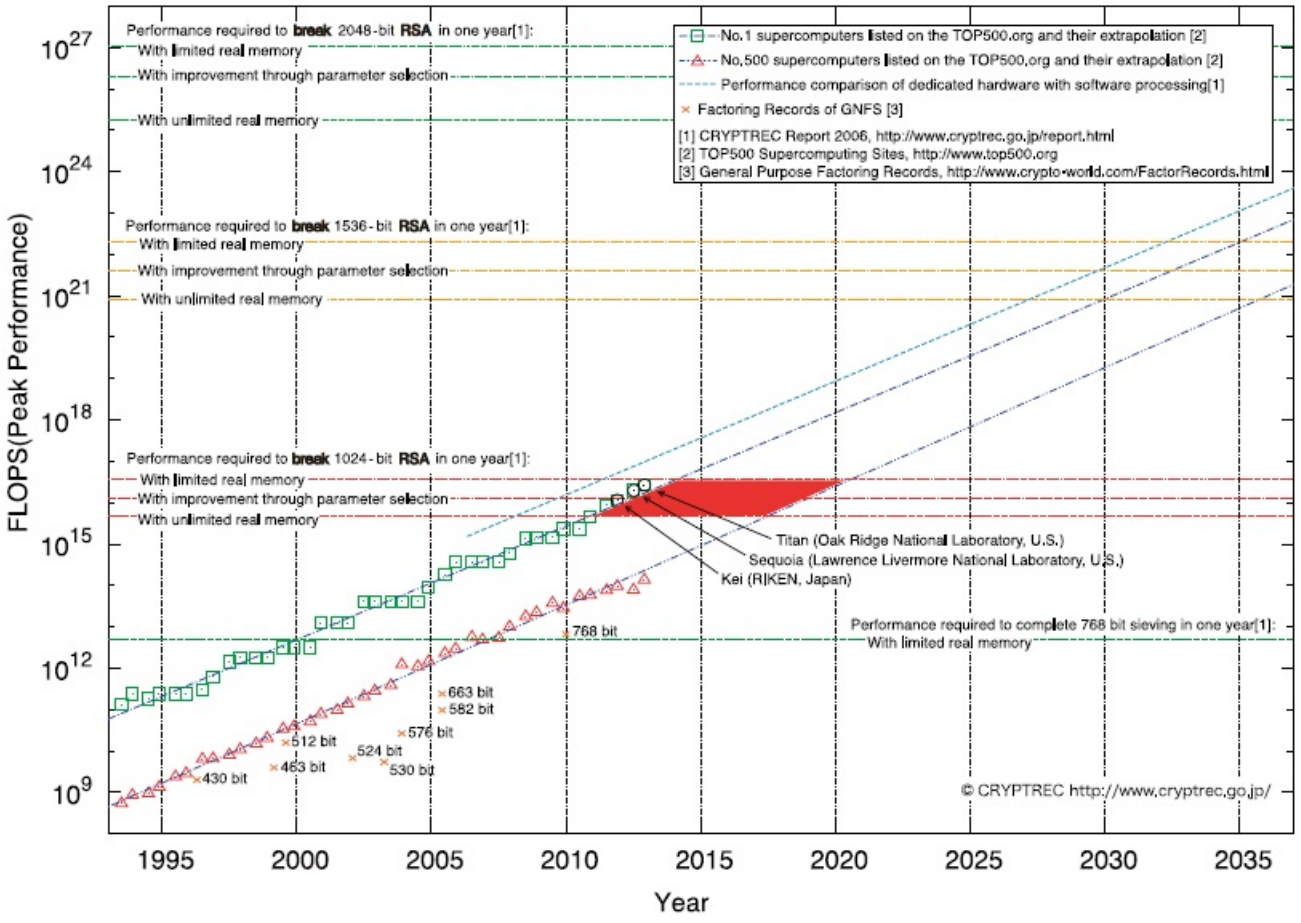
About CRYPTREC

CRYPTREC
Cryptography Research and Evaluation Committees

1. About CRYPTREC

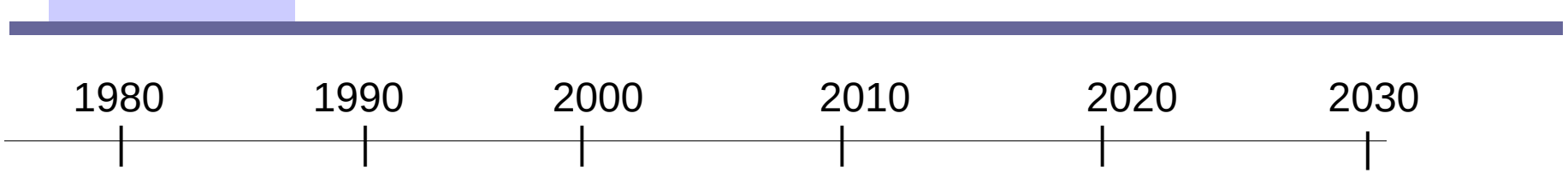
CRYPTREC is an abbreviation of Cryptography Research and Evaluation Committees, and it refers to a project to evaluate and monitor the security of e-Government recommended ciphers, as well as to examine the establishment of evaluation criteria for cryptographic modules.
It consists of the CRYPTREC Advisory Board for Cryptographic Technology (chairperson, Hideki Imai; a professor at Chuo University), which is jointly constituted by the Ministry of Internal Affairs and Communication (MIC) and the Ministry of Economy, Trade and Industry (METI); the Cryptographic Scheme Comittee (chairperson, Hideki Imai; a professor at Chuo University), the Cryptographic Module Committee (chairperson, Naofumi Honma; an associate professor at Tohoku University), and the Cryptographic Operation Committee (chairperson, Tsutomu Matsumoto; a professor at Yokohama National University), which are jointly constituted by the National Institute of Information and Communication Technology (NICT) and the Information-technology Promotion Agency, Japan (IPA).

Estimation for Key Length of RSA



Computational cost for finishing the sieving step within one year (updated Feb 2013)
(NICT NEWS No.426, 2013, http://www.nict.go.jp/en/pdf/NICT_NEWS_1303_E.pdf)

Primitives of Public-Key Cryptography



RSA (widely used in such as SSL, integer factorization problem)

widely used

Elliptic Curve Cryptography (short keys, used in embedding devices)

Pairing-based cryptography (novel crypto protocols)

some products, some standardizations

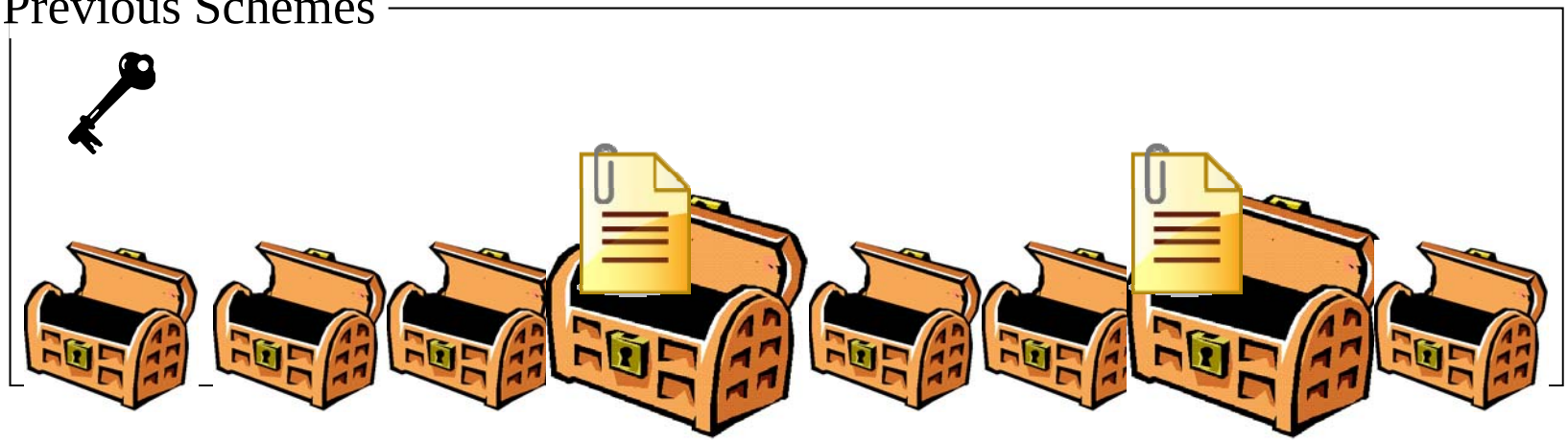
Post-quantum cryptography
(code-based, lattice-based, multivariate polynomial based, etc)

Fully homomorphic encryptions, multi-linear maps

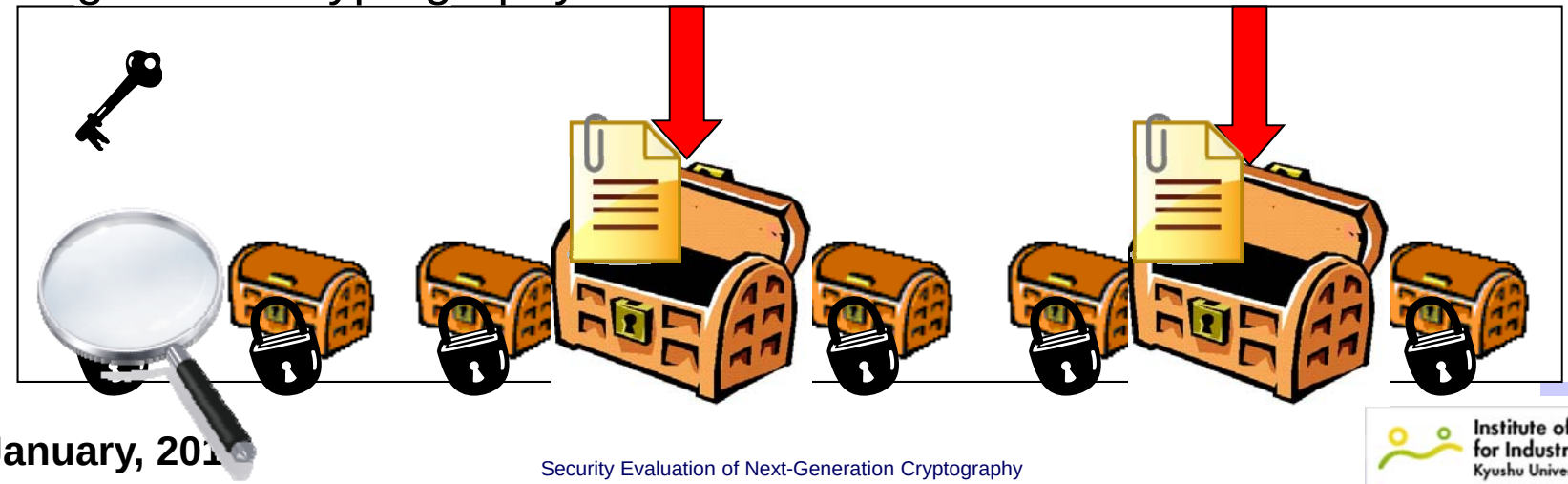
research phase

Pairing-Based Cryptography

Previous Schemes



Pairing-based Cryptography



Standardization

- IETF (Internet Engineering Task Force)
  - RFC5091 (2008): Identity-Based Cryptography Standard #1
  - RFC6508 (2012): Sakai-Kasahara Key Encryption

- IEEE (Institute of Electrical and Electronics Engineers)
  - IEEE P1363.3: Identity-Based Public Key Cryptography

- ISO/IEC JTC 1/SC27
  - ISO/IEC 15946-5:2009: part 5 Elliptic Curve Generation

Project with Industry and Government

FUJITSU　NICT 独立行政法人 情報通信研究機構　KYUSHU UNIVERSITY

How secure is pairing-based cryptography?

The discrete logarithm problem (DLP) over finite field $GF(p^n)$

"find the smallest non-zero integer such that $g^x = a$"

We solved the DLP of 923 bits.

New world record !

Computers used for our cryptanalysis

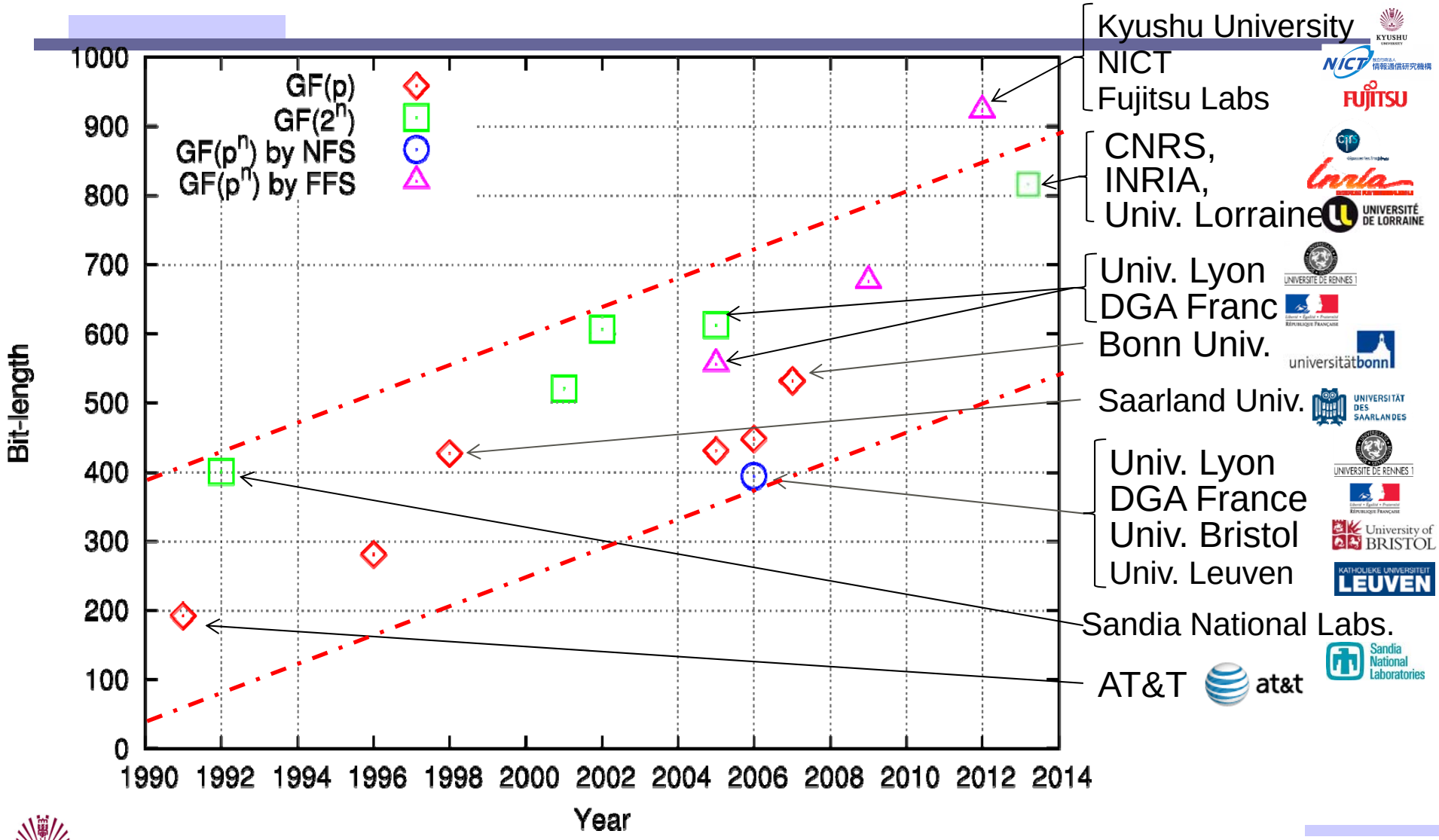
Cryptanalysis Data

- Total computation time: 148.2 days
- Intel Xeon cluster: 21 pc (252core)
- 102 years using one core.

Example of Cryptoanalysis

Rational: $(r+sm) = \prod_{p_i \in B_R} p_i^{a_i}$ Algebraic: $\langle r+sy \rangle = \sum_{\langle p_j, t_j \rangle \in B_A} b_j \langle p_j, y - t_j \rangle$

World Records of DLP



Achievements

- 6 newspapers
- 1 TV report, 1 radio interview
- More than 100 news articles on Web
- 9 invited talks, 6 invited papers

- Paper presentation at Asiacrypt 2012
  (Top-conference in crypto: acceptance ratio 0.17)
- Docomo Mobile Science Prize 2013
- IEICE Achievement Prize 2013
- JSPS Prize 2014

Yomiuri

「解けない」はずの
次世代暗号を解読

Nikkei

278桁の暗号、短期で解読
富士通研など 新技術の弱点検証

Conclusion

- Cryptography is further devolving

  - searchable encryption, privacy issue, obfuscation

- Everlasting security evaluation is required

  - computational over-limit of expected attackers

Thanks!
Q&A