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/

January, 2015

Security Evaluation of Next-Generation Cryptography



## **Cryptography in Modern Society**



### Cryptography is fundamental technology.

January, 2015

Security Evaluation of Next-Generation Cryptography



### History of Public-Key Cryptography

2010

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

2000

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

Pairing-based cryptography (novel crypto protocols)

2020

2030

some products, some standardizations

1990

Post-quantum cryptography

(code-based, lattice-based, multivariate polynomial based, etc)

Fully homomorphic encryptions, multi-linear maps

research phase



1980

Security Evaluation of Bublic-



## **Security Evaluation Cycle**





### Example of RSA public key

・       ・       ・       Search the web (B: 2 *         ・	後 九大数理ウェブメール - Windows Internet Explorer     □ □ ×	1111明書
ファイル(F) 補集(E) 表示(Y) お気に入り(A) ツー/I(F) ヘル/J(H)	🕞 🕞 🗢 🖻 https://webmail 🔽 🔒 外 🗙 🔎 Search the web (Bz 🔎 🔻	全般 詳細 証明のパス
★ お気に入り ▲ 2 学部教育 ▲ カ大教理ウェブメール 本本報題の定かす、 本本報題の こ フィールド (値) 本本報題の開始の一型の14年3月12日 85859 サブジェント、webmail.math.kyu. をなん(2018 世紀) サブジェントの別格 ・ 2018年- PGA (2018 世紀) サブジェントの別格 ・ 2018年- PGA (2018 世紀) ・ 2018年- PGA (2	ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(F) ヘルプ(H)	表示(S): <すべて>
	🚖 お気に入り 👍 🙋 学部教育	
イロジャント       イロシント       イロシント       イロシント       イロシント       イロシント	後 九大数理ウェブメール	フィールド 値 ^
Active field with a state of the state of		□ □ 有効期間の開始 2013年2月8日 9:00:00 □ ★ ★ # # # # # # # # # # # # # # # # #
Active Constant of the second of the secon		III 有効時間の称引 2014年6月12日 6:03:09 同サブジェクト webmail math kyushu=u ac in III
Login       30 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e al e2 4e b9 fd d6 84         1-ブロ:takagi       30 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e al e2 4e b9 fd d6 84         130 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e al e2 4e b9 fd d6 84         130 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e al e2 4e b9 fd d6 84         130 7-ボ         130 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e al e2 4e b9 fd d6 84         130 7-ボ:         130 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e al e2 4e b9 fd d6 84         130 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e al e2 4e b9 fd d6 84         130 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e al e2 4e b9 fd d6 84         140 85 01 06 05 ac 87 50 d0 bc fb 00 93 04 89 05 71 cd 71 10 d3         130 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e al e2 4e b9 fd d6 84         130 2c 13 3d c4 77 18 1d d1 d0 d4 45 64 4c 08 97 71 cd d3         130 2c 13 3d c4 77 18 1d d1 d0 d4 44 56 64 c0 89 71 b0 43 91 57 16 43         130 2c 13 3d c4 77 18 1d d1 d0 d4 45 64 56 40 189 71 b0 43 86 00 187 85 b3 51 16 91 68 50         130 2c 13 3d c4 77 18 1d d1 d0 d4 45 64 56 40 189 71 b0 43 86 00 187 86 b3 51 16 98 b0 60 e1 189 66 80 b7 78 91 66 e3 b1 189 61 68 50 14 91 54 4d ff 0d 197 d0 86 b0 e1 198 66 80 b7 78 91 64 e3 80 80 84 56 80 b3 94 82 5a 50 e4 3e e1 e2 e1 28 e4 38 50 84 56 80 b4 28 a0 28 50 84 56 80		国公開キー RSA (2048 Bits)
Login       30 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e at e2 4e b9 fd d6 84 4 c0 73 02 aa 49 fe de 8a 92 85 5d a3 cb ae 7a fb 80 48 ea bb 57 ct ef 14 44 4 fb c0 73 02 aa 49 fe de 8a 92 85 75 d1 ab cb e3 7a 57 71 c0 d3 30 2c f3 30 c4 77 f8 1d d1 0d dd 44 65 64 c0 89 7d bb d9 91 75 193 84 79 71 c0 d3 30 2c f3 30 c4 77 f8 1d d1 0d dd 44 65 64 c0 89 7d bb d9 91 75 193 46 ab 67 18 73 34 be d1 30 2c f3 30 c2 77 rb 11 d1 0d dd 44 65 64 c0 89 7d bb 89 75 10 ab 60 25 19 57 79 77 1 c0 d3 30 2c f3 30 c4 77 f8 1b d1 0d dd 44 65 64 c0 89 7d bb 49 91 75 16 34 88 a5 20 ab 86 fb 73 34 be d1 30 2c f3 30 c2 f1 0d bc as fr 99 6d ca f5 18 55 79 71 c0 d3 30 2c f3 30 c2 f1 0d bc as fr 99 6d ca f5 18 55 79 71 c0 d4 35 00 ce f3 35 67 91 c0 ce f4 38 25 0 ab 86 fb 73 34 be d1 10 30 e9 f5 08 fb 58 87 50 ab bc 10 93 d0 ce f3 35 70 rb 10 50 rb 19 30 42 rb 19 84 b1 81 19 cb rb 19 34 20 rb 19 94 20 ce f4 82 80 rb 19 34 e0 11 80 rb 19 34 e0 rb 19 rb 19 rb 10 rb 10 rb 10 rb 19 rb 10 rb 10 rb 10 rb 10 rb 10 rb 19 rb 10 rb		していたのの していたの しの の の の の の の の の の の の の の の の の の
Login ユーザロ:takagi パスワード: 言語選択:自動選択、 のパスワード以外のログィン情報を保存する 大大繁厚ウンプメール e1995-2011 TrasWARE Co. All Rights Reserved English		
Login ユーザロ:takagi パスワード: 言語選択:自動選択・ とり動のログイン情報を保存する た大教理ウェブメール を1998-2011 TrastWARE Co. All Rights Reserved. Brightship		GID CRL 配布ポイント     [1] CRL Distribution Point: Dis     マ
	Login ユーザD: takagi パスワード: 言語選択:自動選択 ・ 『パスワード以外のログイン情報を保存する 九大教理ウェブメール e1995-2011 TransWARE Co. All Rights Reserved	30 82 01 0a 02 82 01 01 00 d6 84 36 01 ac 5c 82 88 2e a1 e2 4e b9 fd d6 84 c0 73 02 aa 49 fe de 8a 92 85 5d a3 cb ae 7a fb 80 48 ea 0b 57 cf ef 14 44 9b 61 b0 f6 02 ee d4 82 60 de 9a 5e a2 7d e5 f9 00 65 73 95 79 67 71 c0 d3 30 2c f3 3d c4 77 f8 1d d1 0d 0d 44 65 64 c0 89 7d bb d9 01 5f f3 93 47 9d b4 59 06 85 5a 87 5d 0a bc fb 09 3d 8e 90 25 10 7c 9e f2 06 e4 3a 67 16 43 03 ee 55 8f 9a 4e 01 8d 92 dd f4 99 97 51 e3 46 8a 52 0a b8 fb 73 34 be d1 30 a9 fa 08 fa 9d 96 e8 9b 7f 99 6d ea 61 ba be d2 f7 78 5b b3 51 f9 c3 6b ce 13 5d c5 bd d2 83 d2 38 c2 1f 10 db ca 1f 96 cd 55 e0 14 91 54 4d ff 0d 37 db b7 04 27 de a2 9d 3e b1 76 25 4a a8 59 84 5f 60 b3 94 62 5a 50 e4 3c 7 つパティの編集(E) ファイルにコピー(O) 証明書の詳細について表示します。
	English	OK



January, 2015

### Current record for factoring integers

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

=

Х





### Cryptography Research and Evaluation Committees in Japan



![](_page_6_Picture_2.jpeg)

![](_page_6_Picture_4.jpeg)

### Estimation for Key Length of RSA

![](_page_7_Figure_1.jpeg)

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)

![](_page_7_Picture_3.jpeg)

Security Evaluation of Public-

![](_page_7_Picture_5.jpeg)

### Primitives of Public-Key Cryptography

2010

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

2000

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

Pairing-based cryptography (novel crypto protocols)

2020

2030

some products, some standardizations

1990

Post-quantum cryptography

(code-based, lattice-based, multivariate polynomial based, etc)

Fully homomorphic encryptions, multi-linear maps

research phase

![](_page_8_Picture_9.jpeg)

1980

Security Evaluation of Bublic-

![](_page_8_Picture_11.jpeg)

### Pairing-Based Cryptography

![](_page_9_Figure_2.jpeg)

### Pairing-based Cryptography

![](_page_9_Picture_4.jpeg)

# 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

![](_page_10_Picture_9.jpeg)

![](_page_10_Picture_10.jpeg)

![](_page_10_Picture_11.jpeg)

![](_page_10_Picture_12.jpeg)

![](_page_10_Picture_13.jpeg)

![](_page_10_Picture_14.jpeg)

# Project with Industry and Government

How secure is pairing-based cryptography? The discrete logarithm problem (DLP) over finite field GF(p<sup>n</sup>) "find the smallest non-zero integer such that g<sup>x</sup> = a"

### We solved the DLP of 923 bits. New world record !

### Cryptanalysis Data

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

![](_page_11_Figure_7.jpeg)

Computers used for our cryptanalysis

![](_page_11_Picture_9.jpeg)

# **Example of Cryptoanalysis**

Rational: $(r+sm) = \prod p_i^{a_i}$ Algebraic: $\langle r+sy \rangle = \sum_{i} b_i \langle p_i, y-t_i \rangle$
$p_i \in B_R \qquad \langle p_j, t_j \rangle \in B_A$
$p_i \in B_R$ $\langle p_j, t_j \rangle \in B_A$ $\langle p_j, t_j \rangle \in B_A$
$\begin{array}{c} 0000100001000000000000000000000000000$
$ \begin{array}{c} 03100010000000000000000000000000000000$
40010001000000000000000000000000000000
1011000000000000000000000000000000000

![](_page_12_Picture_2.jpeg)

![](_page_12_Picture_4.jpeg)

# World Records of DLP

![](_page_13_Figure_1.jpeg)

## 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	Nikkei
	<b>278 桁の暗号、短期で解読</b> 電士通研など新技術の弱点検証 電子発電の電量で放送に必要点検証 電子発電の電量で放送に必要点検証 は18日、輝くのに数十万 までの最高だったの04 は18日、輝くのに数十万 までの最高だったの04
インケンドを使ったえる。 「いい」のでないでは、 ので、 のの影響になった。 ので、 のの影響になった。 ので、 のの影響になった。 ので、 のの影響になる。 しい。 なたれての概要にする。 しい。 なたれての概要にする。 に、 のの影響になる。 に、 のの、 のの影響になる。 に、 のの、 のの影響になる。 に、 のの、 のの影響になる。 に、 のの、 のの影響になる。 に、 のの、 のの影響になる。 に、 のの、 のの影響になる。 に、 のの、 のの、 のの、 のの、 のの、 のの、 のの、	の支展だという。 つ支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展だという。 の支展でから、 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支展でたいう。 の支援でたいう、 の支援でたいう、 の支援でたいう、 の支援でたいう、 の支援でたいう、 の支援でたいう、 の支援でたいう、 の支援でたいう、 の支援でたいう、 の支援でたいう、 の の の の支援でたいう の の の の の の の の の の の の の の の の の の の

![](_page_14_Picture_10.jpeg)

![](_page_14_Picture_11.jpeg)

### Conclusion

- Cryptography is further devolving
  - searchable encryption, privacy issue, obfuscation
- Everlasting security evaluation is required
  - computational over-limit of expected attackers

![](_page_16_Picture_0.jpeg)

### Thanks! Q&A

![](_page_16_Picture_2.jpeg)