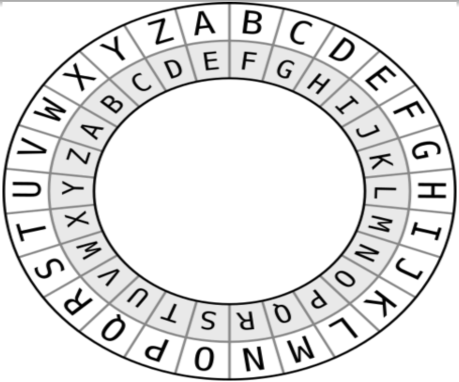
Post-quantum Key Exchanges Based on the LWE problems

Jintai Ding

Yau Center, Tsinghua & Ding Lab, BIMSA

Traditional Cryptography – Cesar's Cipher



Encryption: mapping inwards: $A \to E$, $B \to F$ ....
Decryption: mapping outwards: $E \to A$, $F \to B$ ...
Key: 4 – rotation of alphabet 4 positions
Key shared by both parties – symmetric

Cesar's Cipher

- Security:
  We can guess – 26 tries
  Random permutations ? – In English, we can use the distribution of the 26 letters. (E – the highest frequency: 12%, Next ?)

Cesar's Cipher

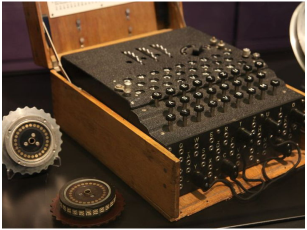
- Security:
  We can guess – 26 tries
  Random permutations ? – In English, we can use the distribution of the 26 letters. (E – the highest frequency: 12%, Next ?)

- What to do to improve?
  Mathematics: Permutation on a finite set
  Increase the size of the set – permutation on the set of 2 letters or more
  But can not too slow!

Symmetric system

Traditional symmetric systems

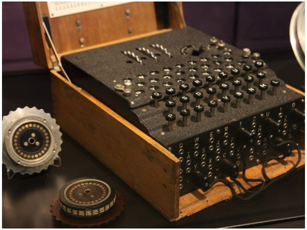
- The sender and receiver have the same keys but used on a machine:
  Enigma machines, DES, AES (Advanced Encryption Standards)



Symmetric system

Traditional symmetric systems

- The sender and receiver have the same keys but used on a machine:
  Enigma machines, DES, AES (Advanced Encryption Standards)



- The two parties must have a prior secure key exchange.
  This is acceptable for **small scale** institutional use. (German U-boats)

Symmetric system

- The mathematics behind: Working on F_q^n a vector space over a finite field F_q.
  Create a complicated permutations via simple ones.
  Encryption:
  $$E = S_1 \circ T_1 \circ S_2 \circ T_2 \cdots \circ S_m \circ T_m$$
  Decryption:
  $$E^{-1} = T_m^{-1} \circ S_m^{-1} \cdots \circ T_2^{-1} \circ S_2^{-1} \circ T_1^{-1} \circ S_1^{-1}$$
  S_i efficient nonlinear maps, T_i efficient linear maps

Symmetric system

- The mathematics behind: Create a complicated permutations via simple ones.
  S_i rotation or flipping.
  T_i a de Jonquiere (triangular) map:

$$T(x_1, x_2) = (x_1, x_2 + f(x_1))$$

where $f(x_i)$ is any efficient polynomial function.

$$T^{-1}(x_1, x_2) = (x_1, x_2 - f(x_1)).$$

Jacobian Conjecture, Tame and Wild Transformation, Nagata Conjecture

Symmetric system – security

- The Enigma machine is highly secure if used properly.
  But the start of a German Telegram?
  The Polish (Marian Rejewski 1939) started cryptanalysis and then the British (Turing 1942-43) broke the system.
  The story of NCR – National Cash Register

Symmetric system – security

- The Enigma machine is highly secure if used properly.
  But the start of a German Telegram?
  The Polish (Marian Rejewski 1939) started cryptanalysis and then the British (Turing 1942-43) broke the system.
  The story of NCR – National Cash Register
- US broke Japanese Navy Code and Japan broke US Army Code.
  Navajo code talkers
  We know this only very recently!

Symmetric system – security

- The Enigma machine is highly secure if used properly.
  But the start of a German Telegram?
  The Polish (Marian Rejewski 1939) started cryptanalysis and then the British (Turing 1942-43) broke the system.
  The story of NCR – National Cash Register
- US broke Japanese Navy Code and Japan broke US Army Code.
  Navajo code talkers
  We know this only very recently!
- The key issue is the trade-off between security and efficiency.

Symmetric system – practice

- Expensive key exchange and used by government or other institutions
- **Not scalable**
- High secrecy
  We only heard about the breaking of Enigma in 1975.
  We know some other stores in second world war on now!
  The story of Falkland war.

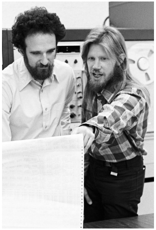
Why PKC

- The appearance of Large computer networks in 1960s.

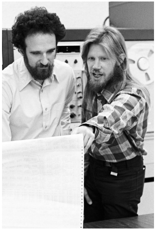
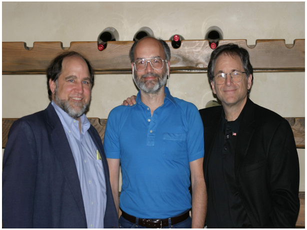
Why PKC

- The appearance of Large computer networks in 1960s.
- The cost of key agreement makes the traditional cryptography prohabative.
  We must find new solutions!!!

PKC

- Diffie-Hellman  The inventors of the idea of PKC – Turing Prize 2016

PKC

- Diffie-Hellman  The inventors of the idea of PKC – Turing Prize 2016
-  RSA – 2003 Turing prize

PKC

- Mathematics behind the RSA cryptosystem: the hardness of integer factorization

$$N = pq.$$

$$15 = 3 \times 5.$$

PKC

- Mathematics behind the RSA cryptosystem: the hardness of integer factorization

$$N = pq.$$

$$15 = 3 \times 5.$$

- The concept behind:

Public key Cryptography

PKC

- The idea was proposed in 1970s by Diffie-Hellmann

PKC

- The idea was proposed in 1970s by Diffie-Hellmann
- Traditionally the information is symmetric. PKC is asymmetric.

PKC

- The idea was proposed in 1970s by Diffie-Hellmann
- Traditionally the information is symmetric. PKC is asymmetric.
- There are two sets of keys:
  one public (N, r): $\gcd(r, (p-1)(q-1)) = 1$
  one private
  (d, p, q): $d \times r = 1 \mod (p-1)(q-1)$

PKC

- Encryption
  The public key is for encryption:
  $$e = m^r \mod N$$
  The private key for decryption:
  $$m = e^d \mod N.$$
- RSA: N is public and p,q is private.
- One knows how to factor n, one can defeat RSA.
  One can calculate d from $(p-1)(q-1)$.

PKC – Authentication

- Traditionally people meet to make key exchange – implicit authentication.

PKC – Authentication

- Traditionally people meet to make key exchange – implicit authentication.
- In the digital world (on the network or wireless), we need authentication!
  We need to make sure the message's authenticity.
  Digital Signature

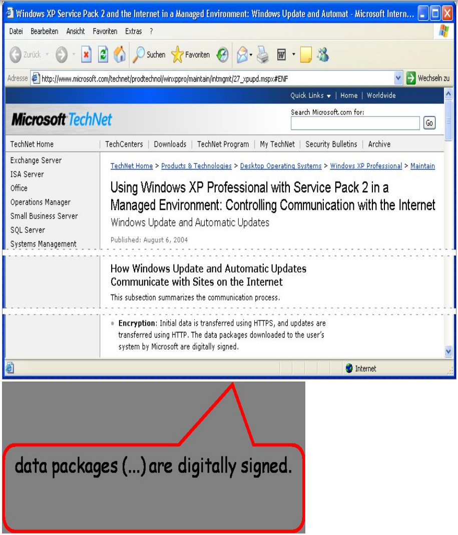
Authentications – Digital Signature

- To authenticate a message or a transaction
- The public key is to verify and anyone can verify.
- The private key is used to sign

Application: Secure Communications

- To establish a shared keys with digital signatures
- the fast communication is done using the shared keys with symmetric systems – AES
- SSL, TLS, Online shopping (sending credit card securely on the internet)

Software update: RSA signature for Microsoft update



What is this number?

2133562529 1600027351 1427593551 9420913291 4767425698
0668648182 4528580269 7571587504 8271600387 9286718814
4217660057 9559348458 0081495826 8691260056 0376434697
9087161398 8653520618 5442348052 5894942341 3033375605
8732136514 8876038644 3075342912 0129705489 0001670606
7393246389 8375697515 1734774577 2076420507 4793016726
4791679237 3351492517 3209625562 4512058040 6546060184
8036703111 8237059907 4873628794 2617311911 1255520806
0025609009 0478884806 3977173442 6254325175 1228479981
6060960213 2860929278 0435354785 7716957089 8641110787
9876456259 1930871508 8016517131 0668371684 8928958136
1754587749 9229988091 2892709869 7538006934 6521176840
9897604596 0758751

PKC

- The number for Microsoft updates

PKC

- The number for Microsoft updates
- Digital signature based on RSA

PKC

- The number for Microsoft updates
- Digital signature based on RSA
- Software update, legal document, voting

IN (the god of) MATH WE TRUST!

Bitcoin-Blockchain

- An open ledger
  Anyone can join in anytime.
- Decentralized
  No central authority
  Anyone can participate and can verify
  Good privacy and highly efficient in time
- **No encryption is used!**

Cryptocurrency?

- Fundamental building blocks:
  ECDSA, Elliptic curve digital signatur algorithm
  Hash functions
- ECDSA
  Public key (or address: the hash of public key) is to receive bitcoins
  Private key is used to send bitcoins, while the transaction cab be verified by the public key
  Only legitimate user can spend.
- Hash functions for POW
  For synchronization on a decentralized network to present double spending
  High cost of mining to present cheating (51 percent attack) .

PKC and Quantum computer

- Quantum computer: quantum mechanics for computations

R. Feynman

PKC and Quantum computer

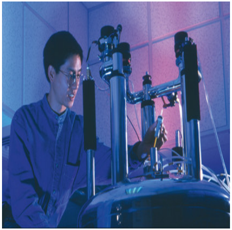
- Quantum computer: quantum mechanics for computations

R. Feynman

- In 1995, Quantum algorithm for factoring, discrete logarithm.

P. Shor

PKC and Quantum computer

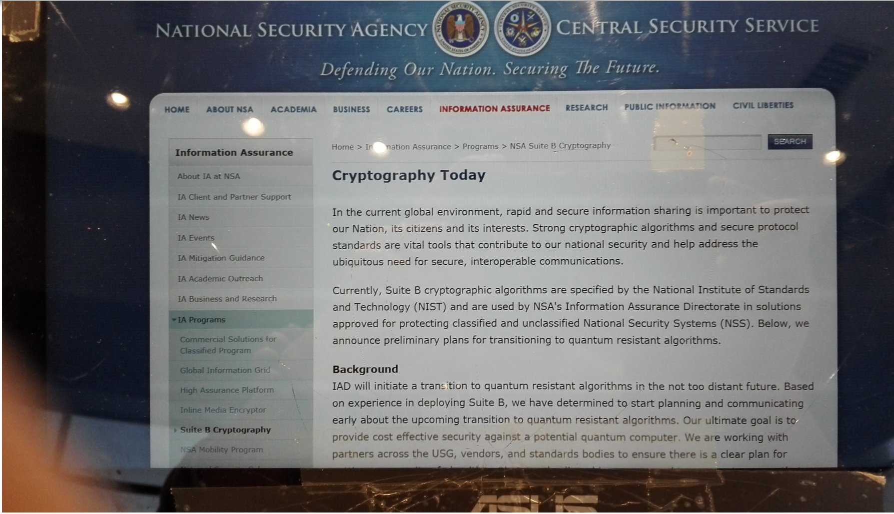
- Can quantum computer really work?
-  Isaac Chuang
  15 million dollars to show that
  $$15 = 3 \times 5.$$
- The problem of scaling
- My Gamble

The context of our work - PQC

- Shor's quantum algorithm
- **Post-quantum cryptography**

  Develop public key cryptosystems that could resist future quantum computer attacks

A commercial for PQC from NSA



Recall the story of Enigma machine!

NIST standardization

NIST standardization of PQC.
What is NIST?

NIST standardization

NIST Special Publication 800-131A
Revision 2

Transitioning the Use of Cryptographic Algorithms and Key Lengths

Elaine Barker
Allen Roginsky
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-131Ar2

March 2019

NIST standardization

NIST SP 800-131A REV. 2 — TRANSITIONING THE USE OF CRYPTOGRAPHIC ALGORITHMS AND KEY LENGTHS

Table 2: Approval Status of Algorithms Used for Digital Signature Generation and Verification

Digital Signature Process	Domain Parameters	Status
Digital Signature Generation	< 112 bits of security strength: DSA: $(L, N) \neq (2048, 224), (2048, 256)$ or $(3072, 256)$ ECDSA: **len**$(n) < 224$ RSA: **len**$(n) < 2048$	Disallowed
	≥ 112 bits of security strength: DSA: $(L, N) = (2048, 224), (2048, 256)$ or $(3072, 256)$ ECDSA or EdDSA: **len**$(n) \geq 224$ RSA: **len**$(n) \geq 2048$	Acceptable

Post Quantum Needs – Functionality

- Key Exchange – for secure communications
- Signatures – for Authentication

NIST Call for PQC Standardization

- NIST call for proposals of new, post-quantum cryptosystems (Dec 2016) with deadline Nov. 2017.
- Three criteria: Security, Cost, Algorithm and Implementation Characteristics
- $4 + 3$ in Round 3

Round 3, two are multivariate signatures, Rainbow is one of three signature finalists.

Short signatures (Rainbow: 50 bytes), fastest signing and verifying, relatively large public key size (tens of Kbs) .

Post Quantum Needs – Families

- Code-based cryptosystems – Theory of error correcting code
- Hash-based signatures
- Isogeny-based cryptosystems – Isogeny of Elliptic curves
- Lattice-based cryptosystems – Modular Forms and Geometry of numbers
- Multivariate cryptosystems – Algebraic Geometry

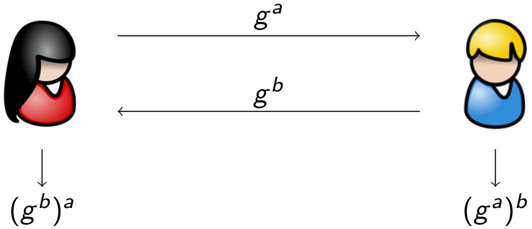
Key Exchange Applications — SSL/TLS

- RSA
- Diffie–Hellman
- Our goal – replacements for post quantum world

Forward Security

- RSA does not offer forward security since compromise of static private key allows decrypting the session keys.
- Possible to achieve forward security with RSA with ephemeral keys but expensive.
- Diffie Hellman offers forward security.
  Forward security: If static keys compromised, previous session keys remain secure.

Diffie-Hellman Key Exchange



Generalizing DH

- DH works because maps $f(x) = x^a$ and $h(x) = x^b$ commute

  $$f \circ h = h \circ f,$$

  $\circ$ – composition

  Nonlinearity

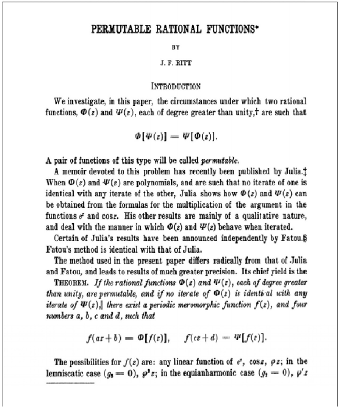
- Many attempts – Braid group etc

Generalizing DH

- When do we have commuting *nonlinear* maps?
  - Powers of x (normal DH)
  - Iterates of a polynomial
  - J. Ritt (1923) – Power polynomials, Chebychev polynomials. Elliptic curve

Who is J. Ritt: 1893-1951

Who is J. Ritt: 1923: PERMUTABLE RATIONAL FUNCTIONS



PERMUTABLE RATIONAL FUNCTIONS*

BY

J. F. RITT

INTRODUCTION

We investigate, in this paper, the circumstances under which two rational functions, $\Phi(z)$ and $\Psi(z)$, each of degree greater than unity,† are such that

$$\Phi[\Psi(z)] = \Psi[\Phi(z)].$$

A pair of functions of this type will be called *permutable*.

A memoir devoted to this problem has recently been published by Julia.‡ When $\Phi(z)$ and $\Psi(z)$ are polynomials, and are such that no iterate of one is identical with any iterate of the other, Julia shows how $\Phi(z)$ and $\Psi(z)$ can be obtained from the formulas for the multiplication of the argument in the functions e^z and $\cos z$. His other results are mainly of a qualitative nature, and deal with the manner in which $\Phi(z)$ and $\Psi(z)$ behave when iterated.

Certain of Julia's results have been announced independently by Fatou.§ Fatou's method is identical with that of Julia.

The method used in the present paper differs radically from that of Julia and Fatou, and leads to results of much greater precision. Its chief yield is the

THEOREM. *If the rational functions $\Phi(z)$ and $\Psi(z)$, each of degree greater than unity, are permutable, and if no iterate of $\Phi(z)$ is identical with any iterate of $\Psi(z)$,‖ there exist a periodic meromorphic function $f(z)$, and four numbers a, b, c and d, such that*

$$f(az+b) = \Phi[f(z)], \qquad f(cz+d) = \Psi[f(z)].$$

The possibilities for $f(z)$ are: any linear function of e^z, $\cos z$, $\wp z$; in the lemniscatic case ($g_3 = 0$), $\wp^2 z$; in the equianharmonic case ($g_2 = 0$), $\wp' z$

J. Ritt (1923) – Power polynomials, Chebychev polynomials. Elliptic curve

Generalizing DH

Our basic idea — adding "small" **noise or perturbation**:

- (Ring) LWE approximately commutes—use to build DH generalization
  From
  $$(s_1 \times a) \times s_2 = s_1 \times (a \times s_2)$$
  to
  $$(as_1 + e_1)s_2 \approx s_1 as_2 \approx (as_2 + e_2)s_1.$$

A historical Note

Our basic idea — adding "small" **noise or perturbation** is not new!!!

- GCHQ – Communications-Electronics Security Group(CESG) – James Elias – "Invention of non-secret encryption" 1969 Clifford Cocks – RSA, Malcolm Williamson – DH, 1973
- The forgotten inspiration of J. Ellis –
  "Ellis said that the idea first occurred to him after reading a paper from World War II by someone at Bell Labs describing a way to protect voice communications by the receiver adding (and then later subtracting) random noise (possibly this 1944 paper[4] or the 1945 paper co-authored by Claude Shannon)"
  – Wikipedia

James Ellias

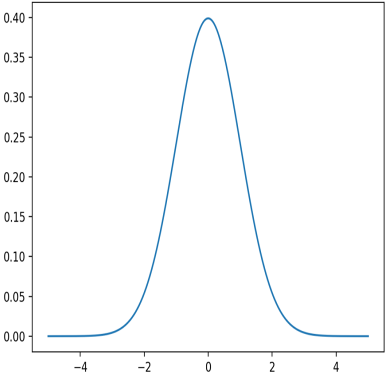
James Ellias GCHQ

Learning with Errors [2006, Regev]

$$\underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}}_{\vec{b}} = \underbrace{\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}}_{\vec{s}} + \underbrace{\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix}}_{\vec{e}}$$

- Approximate system over $\mathbb{Z}_q$
- Hard to find $\vec{s}$ from $A, \vec{b}$.
- Hard to tell if $\vec{s}$ even exists
- Reduction to lattice approximation problems

Discrete Gaussian



Ring LWE

Definition

Let n be a power of 2, $q \equiv 1 \pmod{2n}$ prime. Define the ring

$$R_q = \frac{\mathbb{Z}_q[x]}{(x^n + 1)}.$$

- Again, $b = as + e$ hard to find s
- Hard to distinguish from uniform b
- Approximation problems on *ideal* lattices
- More efficient than standard LWE

Diffie-Hellman from Ideal Lattices

$$\xrightarrow{p_A = as_A + 2e_A}$$

$$\xleftarrow{p_B = as_B + 2e_B}$$

- Public $a \in R_q$. Acts like generator g in DH.

Diffie-Hellman from Ideal Lattices

$$\xrightarrow{p_A = as_A + 2e_A}$$

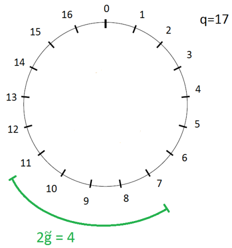
$$\xleftarrow{p_B = as_B + 2e_B}$$

$$k_A = s_A p_B + 2e'_A \quad \approx \quad k_B = p_A s_B + 2e'_B$$

$$= aS_A S_B + 2S_A e_B + 2e'_A \qquad = aS_A S_B + 2S_B e_A + 2e'_B$$

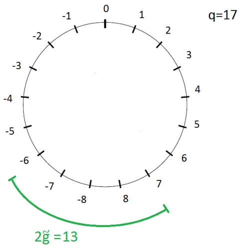
- Public $a \in R_q$. Acts like generator g in DH.
- Each side's key is only *approximately* equal to the other.
- Difference is even—same low bits.
- No authentication—MitM

Wrap-around Illustrated



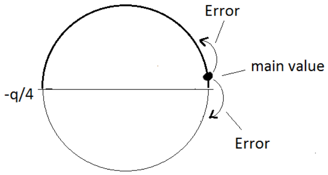
- Difference 4, both odd.

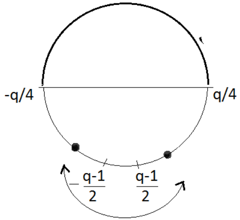
Wrap-around Illustrated



- But wait! If $q = 17$,
  $\mathbb{Z}_q = \{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$.
- 11 becomes -6, now parities disagree!

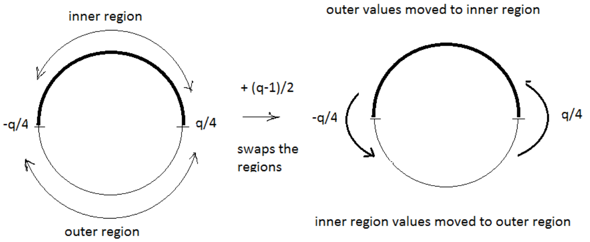
Rounding Intuition – Outer Region problem



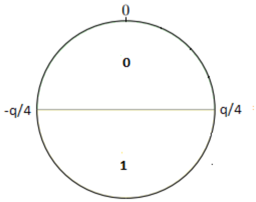


Additional modular operation

Rounding Intuition



Rounding Intuition – Region Division



Signal function Sig(.)

Compensating for Wrap-Around

- $g = 2S_A e_B - 2S_B e_A + 2e'_A - 2e'_B$.
- Recall: $|g^{(j)}| < \frac{q}{8}$
- Define $E = \{-\lfloor \frac{q}{4} \rfloor, \ldots, \lfloor \frac{q}{4} \rceil\}$. Middle half of $\mathbb{Z}_q$.
- If $k_B^{(j)} \in E$, no wrap-around occurs; $k_A^{(j)} \equiv k_B^{(j)}$.
- If $k_B^{(j)} \notin E$, then $k_B^{(j)} + \frac{q-1}{2} \in E$
- If $k_B^{(j)} \notin E$, $k_A^{(j)} + \frac{q-1}{2} \equiv k_B^{(j)} + \frac{q-1}{2}$.

Wrap-around Defeated

Define $Sig(v) = \begin{cases} 0 & v \in E, \\ 1 & v \notin E. \end{cases}$

and, $w_B^{(j)} = Sig(k_B^{(j)})$

Then $k_B^{(j)} + w_B^{(j)} \frac{q-1}{2} \in E$.

Also, $k_B^{(j)} + w_B^{(j)} \frac{q-1}{2} \equiv k_A^{(j)} + w_B^{(j)} \frac{q-1}{2} \pmod 2$.

- $k_B^{(j)} + w_B^{(j)} \frac{q-1}{2} \bmod q \bmod 2 = k_A^{(j)} + w_B^{(j)} \frac{q-1}{2} \bmod q \bmod 2$.
- Wrap-around correction $w_B = (w_B^{(0)}, w_B^{(1)}, \ldots, w_B^{(n-1)})$
- $\sigma_B = k_B + w_B \frac{q-1}{2} \bmod 2$.
- $\sigma_A = k_A + w_B \frac{q-1}{2} \bmod 2$.

Key Derivation

Obtaining shared secret from approximate shared secret:

$$\begin{aligned}
k_A &= (k_A^{(0)}, k_A^{(1)}, \ldots, k_A^{(n-1)}) \\
k_B &= (k_B^{(0)}, k_B^{(1)}, \ldots, k_B^{(n-1)}) \\
\tilde{g} &= (g^{(0)}, g^{(1)}, \ldots, g^{(n-1)}) \\
k_A - k_B &= 2\tilde{g} \\
k_A &\equiv k_B \pmod 2
\end{aligned}$$

Key Derivation

Obtaining shared secret from approximate shared secret:

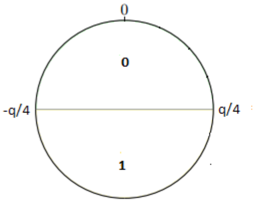
$$
\begin{aligned}
k_A &= (k_A^{(0)}, k_A^{(1)}, \ldots, k_A^{(n-1)}) \\
k_B &= (k_B^{(0)}, k_B^{(1)}, \ldots, k_B^{(n-1)}) \\
\tilde{g} &= (g^{(0)}, g^{(1)}, \ldots, g^{(n-1)}) \\
k_A - k_B &= 2\tilde{g} \\
k_A &\equiv k_B \pmod 2
\end{aligned}
$$

- Each $k_A^{(j)} = k_B^{(j)} + 2g^{(j)}$.
- Each $g^{(j)}$ is small ($|g^{(j)}| < \frac{q}{8}$).
- Matching coefficients differ by small multiple of 2
- Take each coefficient mod 2, get n bit secret

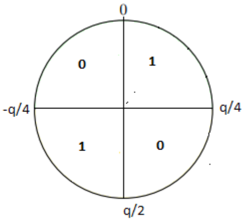
LWE KE

- Ding's paper:
  Cryptology ePrint Archive: Report 2012/688
  20121210:115748 (posted 10-Dec-2012 11:57:48 UTC)
- Cryptology ePrint Archive: Report 2014/070, C. Peikert
  Cryptology ePrint Archive: Report 2014/599, Joppe W. Bos and Craig Costello and Michael Naehrig and Douglas Stebila
  Cryptology ePrint Archive: Report 2015/1092, Erdem Alkim and Leo Ducas and Thomas Poppelmann and Peter Schwabe

Comparison of Signal



Signal function Sig(.)



cross rounding b= <.>$_2$

Proof Games

Proof proceeds by series of games:

- Begin with simulated protocol
- Adversary cannot distinguish from previous game
- Eventually, if original protocol can be distinguished from random, rLWE can be broken
- Important step to post quantum key exchange.

New Application of Lattice-based schemes - Fully Homomorphic Encryption

- The increase importance of cloud storage and computing
- Privacy concerns
- FHE allows computation on encrypted data
- Main Issue – efficiency

The new post-quantum era

- We must update all systems – a great opportunity in research and business
- Is Bitcoin OK?
  No. Due to the nature of decentralized system.
- Cryptography is needed everywhere to protect not secrecy but also **authenticity** and integrity of data and people's privacy
  MPC for data sharing (Medical data sharing, AI etc)
- A key concern – cost effectiveness.

Summary: the ubiquitous application of cryptography in the digital world

- Cryptography is used in all devices including cell phone and ubiquitous devices like RFID : subway and bus card, sensors, small medical device, ...
- Cryptography is not anymore an institutional solution but a public and civilian solution for everyone's daily use.
- Privacy is an increasing concerns
- Mathematics is the foundation of all the cryptographic algorithms.
  BIMSA – Beijing Institute of Mathematical Sciences and Applications

Privacy Protection and Blockchain Security at BIMSA

The mission of the Lab

- to apply the best mathematical ideas to develop fundamental algorithms, and apply them to ensure the long term privacy protection and the long term security of the blockchain technology,
- to discover new fundamental mathematical methods and theory to ensure the sustainable development of our applied research.

Privacy Protection and Blockchain Security Lab at BIMSA

- The lab intends to develop and apply new efficient and secure quantum-proof algorithms to ensure the long term security for our digital society.
- The lab intends to work with industry for practical applications in internet, blockchain, digital payment system, ubiquitous computer systems and other digital systems.
- The lab intends to provide technical supports and solutions for the industry to comply with privacy laws and blockchain regulations.
- The lab intends to be an open lab with a research team consisting of mathematicians, computer scientists and industry experts to work with colleagues around the world.

Thank You

Questions to jintai.ding@gmail.com