National Cyber Security Centre

Identity-based Quantum Safe Cryptography

ENISA

September 2018

National Cyber Security Centre

Background

- In 2009 CESG address the emerging UK government requirement for secure mobile voice for civil servants and emergency services
- The main challenge was to achieve security at scale. No existing commercial solution appeared to meet the challenge
- We wanted a single security solution with commercial support
- Our decision was to develop a security protocol based on published research and make this available as a free-to-use Standard
- Our technical solution was to use Identity Based Cryptography

National Cyber Security Centre

Identity based encryption (IBE)

- In traditional PKC, users select a (random) private key and then derive a public key
  - Requires a PKI for users to obtain and authenticate user public keys

- In IBE, user public keys can be meaningful, non-random identifiers e.g. a phone number, e-mail or IP address (plus any auxiliary data e.g. time/date, etc).

- User private keys are derived from their public key in an offline process by a system-wide Key Management Server (KMS)

- Some advantages of IBE over traditional PKC:
  - Lightweight key management. No need for a PKI
  - Simplex per-message transmission is much easier
  - Key revocation via identifier timestamps

National Cyber Security Centre

MIKEY-SAKKE

- MIKEY-SAKKE is an authenticated key exchange mechanism

- Elliptic curve-based IBE
  - Identifiers are user phone numbers plus date/time period

- Combination of:

  - SAKKE: Sakai-Kasahara Key Encryption, based on Elliptic Curve pairings
    - $E: y^2 = x^3 - 3x$
    - $e: E(F_P^2)[q] \times E(F_P^2)[q] \rightarrow GF(q)$
    - $e(xP,Q) = e(P,xQ) = e(P,Q)^x$

  - ECCSI: Elliptic curve certificate-less signatures
    - ECDSA adapted for identifier-based PKC (non pairings-based)

National Cyber Security Centre

Standards and industry adoption

- 3GPP Standards for E2E security for Public Safety LTE applications in 2014
- In use by UK Civil Servants. Will be adopted by UK emergency services from 2018
- Independent commercial interest for enterprise solutions
  - Trials of secure voice and non-telephony applications (encrypted e-mail, web browsing) using different identifiers (e-mail address, URL)
  - Variety of approaches proposed for KMS, enrolment, monthly key update, etc.
- Secure Chorus Industry group formed in 2014. Provides a common ecosystem for large-scale deployments. See www.securechorus.org

National Cyber Security Centre

Quantum-safe alternatives?

- What might a large-scale quantum-safe IBE network look like?

- Ideal lattices (R-LWE) seems like the most practical option for IBE today
  - Compared with ECC pairings, R-LWE gives
    - Faster encryption and decryption
    - Larger ciphertexts

- For large-scale deployments Hierarchical (HIBE) schemes would allow the Master KMS to delegate key extraction e.g. to regional networks
  - Finer-grained security
  - More efficient key distribution

- This talk will provide an overview of our investigations so far into practical ideal lattice-based HIBE

National Cyber Security Centre

Quantum Safe IBE

National Cyber Security Centre

DLP Example

- [DLP] is a good starting point. It is an efficient trapdoor IBE scheme based on NTRU + R-LWE

- Rings $R = \mathbb{Z}[x]/(x^n + 1)$ and $R_q = R/qR$. Associated discrete Gaussian distribution χ_0

- Master KMS private key is a pair of small polynomials (f, g) in R
- Master KMS public key is the quotient $A = g/f$ in R_q

- User public key ID in R_q is the hash of some identifier string
- User private key for ID is a pair of small sampled* polynomials (s_1, s_2) in R such that

$$ID = s_1 \cdot A + s_2$$

[DLP] *Efficient Identity-based Encryption over NTRU lattices.* L. Ducas, V. Lyubashevsky and T. Prest. IACR ePrint 2014/794

* Details omitted. A large part of [DLP] is devoted to showing how to set parameters and do the sampling properly.

National Cyber Security Centre

DLP Example

- We can then build a KEM using standard R-LWE techniques

- Encrypt a key $k \in \{0,1\}^n$ to the identifier ID as the pair of polynomials (u, v) in R_q where

$$u = r \cdot A + e_1,$$

$$v = r \cdot ID + e_2 + \lfloor q/2 \rfloor k$$

for ephemeral random values $r, e_1, e_2 \in \{-1,0,1\}^n$.

- Can recover k by rounding $\lfloor 2w/q \rceil$ where $w = v - s_1 \cdot u$

- DLP is a good starting point but we want to take into account advances since then and investigate whether we can find a HIBE variant

National Cyber Security Centre

Extended IBE scheme

- As a first step towards constructing a HIBE scheme we consider a variant of DLP
- Start by introducing an auxiliary public parameter *B* (uniform random in R_q)
- Master KMS private key is a pair of small polynomials (f, g) in R as before
- Master KMS public key is now a pair of polynomials (A, B) in R_q

$$A \cdot f + g = 0$$

- The user private key corresponding to ID in R_q is now the triple* of small sampled polynomials (s_1, s_2, s_3) in R_q

$$s_1 \cdot A + s_2 \cdot ID + s_3 = B$$

* Note that algebraically the NTRU/DLP lattice is a rank-2 module over a ring. Here we are extending to rank-3

National Cyber Security Centre

Extended IBE scheme

- Encrypt a key $k \in \{0,1\}^n$ to the identifier ID as the triple of polynomials in R_q

$$v_1 = s \cdot A + e_1,$$

$$v_2 = s \cdot ID + e_2,$$

$$v_3 = s \cdot B + e_3 + \lfloor q/2 \rfloor k$$

for small ephemeral polynomials s, e_1, e_2, e_3 from R

- Decrypt by rounding $\lfloor 2w/q \rceil$ where $w = v_3 - s_1 \cdot v_1 - v_2 \cdot s_2$
- Moving up to higher rank systems will allow us to incorporate more identities. In particular this variant can be used to build a HIBE scheme

National Cyber Security Centre

Hierarchical IBE (HIBE)

- [CHKP] describes an approach to HIBE via LWE called *Bonsai Trees*
  - Trees are a hierarchy of standard lattices
  - Each lattice in the tree is a higher rank super-lattice (an extension) of its parent
  - "Control" equates to knowing a trapdoor short basis for a branch
  - The master KMS controls the whole tree and the sub-KMS's control different branches
  - [CHKP] gives constructions for extending and securely delegating control of branches
  - [ABB] is another good reference

[CHKP] *Bonsai Trees, or How to Delegate a Lattice Basis.* D. Cash, D. Hofheinz, E. Kiltz and C. Peikert. IACR ePrint 2010/591

[ABB*] Efficient Lattice (H)IBE in the Standard Model* S. Agarawal, D. Boneh, and X. Boyen, EUROCRYPT 2010

National Cyber Security Centre

Hierarchical IBE (HIBE)

- We adapt the Bonsai Tree methodology to our variant DLP scheme

Master KMS	**Delegated KMS**	**User**
• Public keys		
• $L_0 = \begin{bmatrix} qI_n & 0_n \\ A & I_n \end{bmatrix}$	$L_1 = \begin{bmatrix} qI_n & 0_n & 0_n \\ A & I_n & 0_n \\ A_1 & 0_n & I_n \end{bmatrix}$	$L_2 = \begin{bmatrix} qI_n & 0_n & 0_n & 0_n \\ A & I_n & 0_n & 0_n \\ A_1 & 0_n & I_n & 0_n \\ A_2 & 0_n & 0_n & I_n \end{bmatrix}$
• Private keys		
• Short basis for L_0	Short basis for L_1	Short vector in coset B + L_2

National Cyber Security Centre

Hierarchical IBE (HIBE)

- We adapt the Bonsai Tree methodology to our variant DLP scheme

Master KMS **Delegated KMS** **User**

- Public keys
  - $L_0 = \begin{bmatrix} qI_n & 0_n \\ A & I_n \end{bmatrix}$

$$L_1 = \begin{bmatrix} qI_n & 0_n & 0_n \\ A & I_n & 0_n \\ A_k & 0_n & I_n \end{bmatrix}$$

$$L_2 = \begin{bmatrix} qI_n & 0_n & 0_n & 0_n \\ A & I_n & 0_n & 0_n \\ A_k & 0_n & I_n & 0_n \\ A_U & 0_n & 0_n & I_n \end{bmatrix}$$

- Private keys
  - Short basis for L_0 → Short basis for L_1 → Short vector in coset B + L_2

Delegate $ID_{KMS\ A(k)}$ Extract $ID_{User\ A(U)}$

National Cyber Security Centre

HIBE basis delegation

- Suppose a Master KMS wants to delegate key extraction to ID_{KMS1}
- Using its rank-2 trapdoor basis, the Master KMS can construct a good rank-3 basis over *R*

$$\begin{bmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{bmatrix}$$

- In the top two rows the x_i are constructed via sampling* using the Master KMS private basis such that each row satisfies

$$x_i \cdot A + x_{i+1} \cdot ID_{\mathrm{KMS1}} + x_{i+2} = 0$$

  and each x_i appears to have been sampled from some distribution χ_1

- The third row is constructed to satisfy a 3x3 determinantal condition
  - Other checks are needed e.g. to verify that the rows span the lattice
- This is our analogue of extending a [CHKP] trapdoor basis: we have extended the rank-2 Master KMS private basis to a rank-3 delegation basis for KMS1

*Use e.g. the randomised nearest plane algorithm from [DLP]

National Cyber Security Centre

HIBE key extraction

- KMS1 can perform delegated key extraction for the identifier ID_{User} by forming a quadruple of small sampled polynomials (s_1, s_2, s_3, s_4) in R such that

$$s_1 \cdot A + s_2 \cdot ID_{\text{KMS1}} + s_3 \cdot ID_{\text{User}} + s_4 = B$$

- Similar to previous slide, KMS1 uses its delegated trapdoor basis and sampling so that and each s_i appears to have been sampled from some χ_2

- The ciphertexts will be four instances of the R-LWE equations

$$v_1 = s \cdot A + e_1, v_2 = s \cdot ID_{\text{KMS1}} + e_2, v_3 = s \cdot ID_{\text{User}} + e_3, v_4 = s \cdot B + e_4 + \lfloor q/2 \rfloor k$$

- The above process extends to greater depths but in practice we shouldn't need too many layers

- Real-world deployments should use an actively secure transform such as Fujisaki-Okamoto

National Cyber Security Centre

Randomisation and sampling

- No additional [CHKP] obfuscation step is needed for the delegated bases since the x_i's are randomly sampled
- B separates functionality
  - B=0 for KMS delegation step
  - B ≠ 0 for user key extraction step
- Also solves some problems with management of deterministic private keys in earlier schemes
- Important to get sampling parameters right. A major contribution of [DLP] was to show how to use Gaussian sampling to find short private keys (s_1, s_2) while keeping information about the Master Secret (f, g) inaccessible. Need to verify this approach for higher rank equations to ensure that delegation methods don't leak private information
- As a starting point the standard deviations should be chosen so that

$$\sigma(\chi_0) = O\left(\sqrt{q/n}\right), \quad \sigma(\chi_1) = O\left(\sqrt{q}\right), \quad \sigma(\chi_2) = O\left(\sqrt{qn}\right)$$

National Cyber Security Centre

Preliminary security analysis and open questions

National Cyber Security Centre

Classical security analysis

- Classical attacks on lattice-based schemes are well studied
- Careful parameter selection should block most standard attacks
  - Ensure the SVP for Λ is hard. Else the Master secret (f, g) can be recovered directly
  - Ensure the CVP for Λ is hard. Else the user secret keys $s_1, s_2, s_3, \ldots$ can be recovered or forged
- Some proposed attacks on NTRU ring structure
- Active attacks need to be blocked at the protocol level e.g. via F-O transform

National Cyber Security Centre

KMS Security

- Base the KMS in a secure location and perform user key derivation off-line. Network access is only required at initial registration and then potentially at monthly or yearly intervals after that.
- The use of HIBE further limits the exposure of the central KMS as network access is only required during the provisioning of a small number of sub-KMSs
- Compromise of a sub-KMS only affects the users managed by that KMS and KMSs below it in the tree, rather than all users in the system
- There are cryptographic mechanisms that allow split generation of the user private keys. The shares of the user private key can be stored at different secure locations
- For some use cases there are valid requirements for the organisation to be able to access user private keys e.g. regulatory or audit requirements. Policies ensure that access is restricted to authorized persons

National Cyber Security Centre

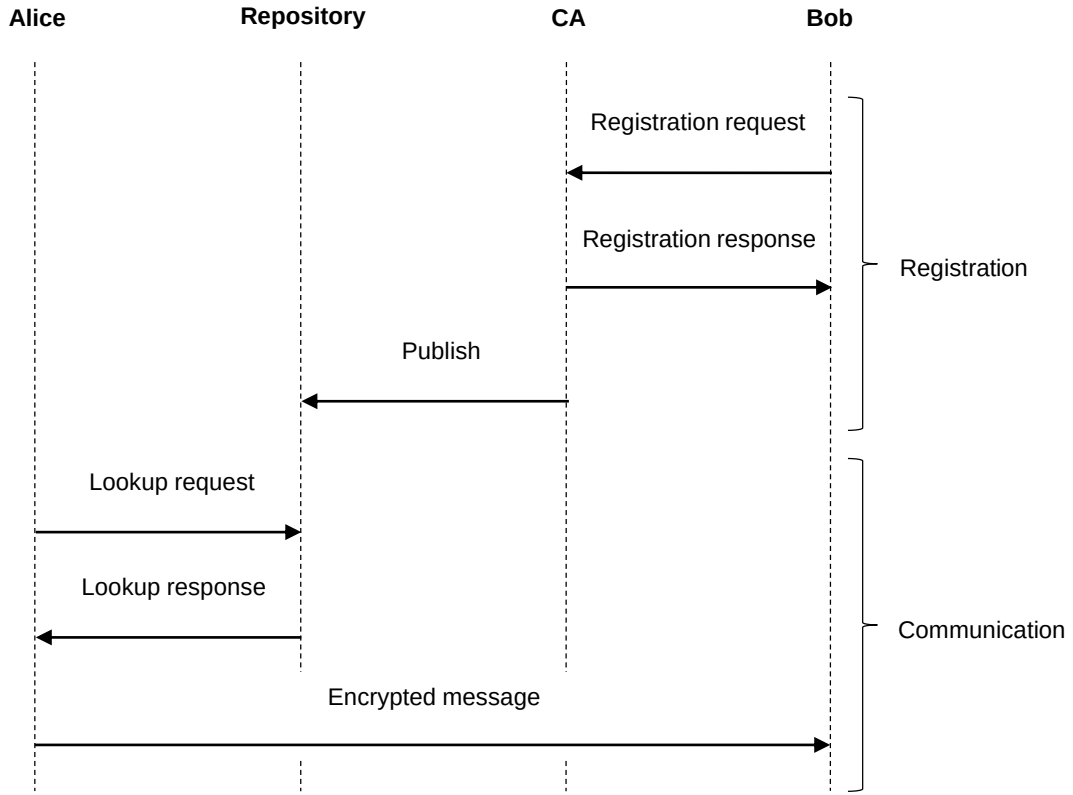
Summary

- We are investigating ideal lattice-based HIBE schemes for large scale deployments
  - Applying ideas from DLP and Bonsai trees to ideal lattices
  - Believe we can construct practical HIBE schemes
  - Variants of our HIBE scheme can support standard lattice security proofs

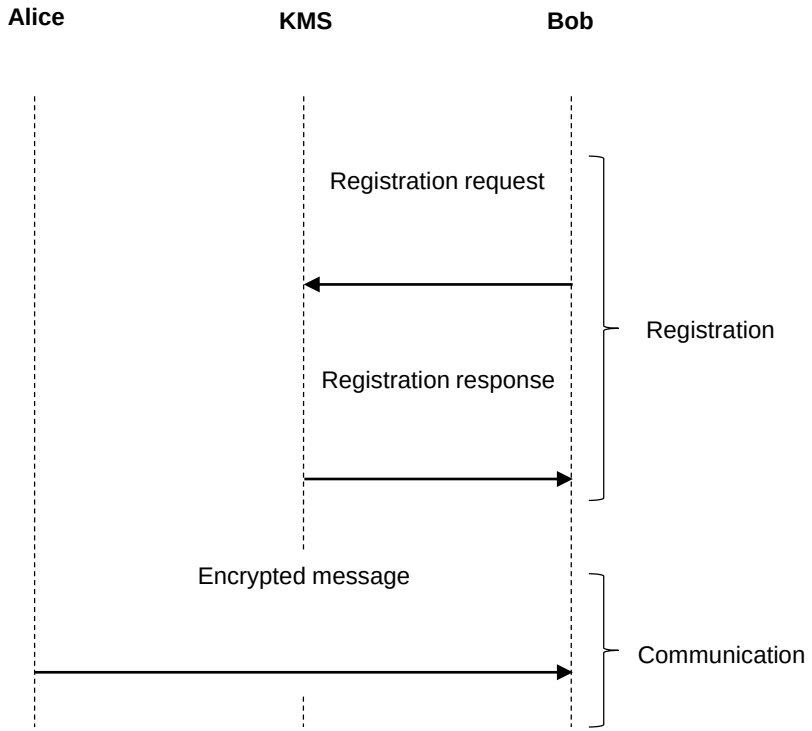
- Open questions
  - Parameter sizes and sampling methods need to be analysed very carefully
  - Implementation and efficiency issues

National Cyber Security Centre

Protocol flow



Encrypted communication with a PKI



Encrypted communication with IBE