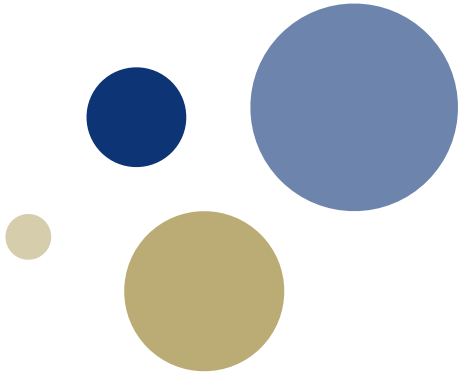
Norwegian University of
Science and Technology



PQ Key Exchange: some related problems

Bor de Kock

Norsk Kryptoseminar

January 30th, 2020

Key Exchange: the basics

Elliptic Curve Diffie-Hellman

Select point P of order n

Alice		**Bob**
Pick $d_A \in [1, n-1]$		Pick $d_A \in [1, n-1]$
$Q_A = d_A P$	$\xrightarrow{Q_A}$	$Q_B = d_B P$
	$\xleftarrow{Q_B}$	
$s = d_A Q_B$		$d_B Q_A$

Post-Quantum KEX / KEM

- Several candidates exist, some are very ‘ready’:
  - RLWE: implemented
  - SIDH: in use
- Research isn’t “done” but at least getting somewhere

Encryption-based KEM

$\mathbf{a} \leftarrow_R R_q$

Alice		Bob
$\mathbf{s}, \mathbf{e} \leftarrow_R \chi$		$\mathbf{s}', \mathbf{e}', \mathbf{e}'' \leftarrow_R \chi$
$\mathbf{b} = \mathbf{as} + \mathbf{e}$	$\xrightarrow{\mathbf{b}}$	$\mathbf{u} = \mathbf{as}' + \mathbf{e}'$
		$\mathbf{v} = \mathbf{bs}' + \mathbf{e}''$
		$\nu \in_R \{0,1\}^n$
		$\mathbf{k} = \mathrm{Encode}(\nu)$
	$\xleftarrow{\mathbf{u}, \mathbf{c}}$	$\mathbf{c} = \mathbf{v} + \mathbf{k}$
$\mathbf{v}' = \mathbf{us}$		$\mu = \mathrm{Extract}(\mathbf{k})$
$\mathbf{k}' = \mathbf{c} - \mathbf{v}'$		
$\mu = \mathrm{Extract}(\mathbf{k}')$		

In this talk

- Some Cool Things We Really Should Research More

In this talk

- Some Cool Things We Really Should Research More

- Specifically:
  - PAKE
  - Secure Remote Password
  - Group Key Exchange

PAKE?

$$
\begin{array}{lcl}
P = H_1(ID_A, ID_B, \pi) & & \\
r_A \in_R \mathbb{Z}_q & & \\
t_A = g^{r_A} & & \\
m = t_A P & \xrightarrow{\quad m \quad} & \text{Check } m \neq 0 \in G \\
 & & t_A = m/P \\
 & & r_B \in_R \mathbb{Z}_q \\
 & & t_B = g^{r_B} \\
 & & \mathbf{Z} = t_A^{r_B} \\
\mathbf{Z} = t_B^{r_A} & \xleftarrow{\quad t_B, k \quad} & k = H_2(ID_A, ID_B, m, t_B, \mathbf{Z}, P) \\
k \stackrel{?}{=} H_2(ID_A, ID_B, m, t_B, \mathbf{Z}, P) & & \\
k' = H_3(ID_A, ID_B, m, t_B, \mathbf{Z}, P) & \xrightarrow{\quad k' \quad} & k' \stackrel{?}{=} H_3(ID_A, ID_B, m, t_B, \mathbf{Z}, P) \\
\mathbf{K} = H_4(ID_A, ID_B, m, t_B, \mathbf{Z}, P) & & \mathbf{K} = H_4(ID_A, ID_B, m, t_B, \mathbf{Z}, P)
\end{array}
$$

source: 'Protocols for Authentication and Key Establishment' (Boyd, Mathuria, Stebila, 2019)

PQ-PAKE?

PQ-PAKE? Yes! RLWE!

Party i		Party j
Pre-shared password: pwd		Pre-shared password: pwd
Public key: $p_i = as_i + 2e_i \in R_q$		Public key: $p_j = as_j + 2e_j \in R_q$
Private key: $s_i \in R_q$	$\xrightarrow{p_i}$	Private key: $s_j \in R_q$
where $s_i, e_i \leftarrow D_{Z^n,\sigma}$		where $s_j, e_j \leftarrow D_{Z^n,\sigma}$
$\gamma = H_1(pwd), m = p_i + \gamma$		$\gamma' = -H_1(pwd)$
		$p'_i = m + \gamma', k_j = p'_i s_j$
$k_i = p_j s_i, \gamma' = -\gamma$		$w_j = \mathrm{Cha}(k_j) \in \{0,1\}^n$
$\sigma_i = \mathrm{Mod}_2(k_i, w_j) \in \{0,1\}^n$	$\xleftarrow{p_j, w_j, c_j}$	$\sigma_j = \mathrm{Mod}_2(k_j, w_j) \in \{0,1\}^n$
Abort if $k \neq H_2(i,j,m,p_j,\sigma,\gamma')$		$k = H_2(i,j,m,p_j,\sigma,\gamma')$
Else $k' = H_3(i,j,m,p_j,\sigma,\gamma')$		$k'' = H_3(i,j,m,p_j,\sigma,\gamma')$
		Abort if $k' \neq k''$
$sk_i = H_4(i,j,m,p_j,\sigma,\gamma')$	$\xrightarrow{k'}$	$sk_j = H_4(i,j,m,p_j,\sigma,\gamma')$

source: 'Efficient Implementation of PAKE from RLWE and Post-Quantum TLS' (Gao Ding Liu Li, 2016)

Let’s use this!

Let's use this!

US 20180302218A1

(19) **United States**

(12) **Patent Application Publication**

DING

(10) **Pub. No.: US 2018/0302218 A1**

(43) **Pub. Date: Oct. 18, 2018**

(54) **PASSWORD BASED KEY EXCHANGE FROM RING LEARNING WITH ERRORS**

(71) Applicant: **Jintai DING**, Cincinnati, OH (US)

(72) Inventor: **Jintai DING**, Cincinnati, OH (US)

(21) Appl. No.: **15/765,238**

(22) PCT Filed: **Sep. 2, 2016**

(86) PCT No.: **PCT/CN2016/097895**

§ 371 (c)(1),

Publication Classification

(51) **Int. Cl.**

H04L 9/08	(2006.01)
H04L 9/30	(2006.01)
H04L 9/32	(2006.01)
G06F 17/16	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 9/0844*** (2013.01); ***H04L 9/3013*** (2013.01); ***G06F 17/16*** (2013.01); ***H04L 9/3273*** (2013.01); ***H04L 9/3073*** (2013.01)

(57) **ABSTRACT**

Use the same basic idea of KE based on Ring LWE, this

Secure Remote Password

$a \leftarrow^{\$}$

$A = g^a$

$v =$ Password hash

$b \leftarrow^{\$}$

$B = v + g^b$

A →

← B

$p =$ "The P4s5w0rd"

$x = H(s, H(U, p))$

$S = (B - g^x)^{a+u \cdot x}$

$K = H(S)$

$S = (A \cdot v^u)^b$

$K = H(S)$

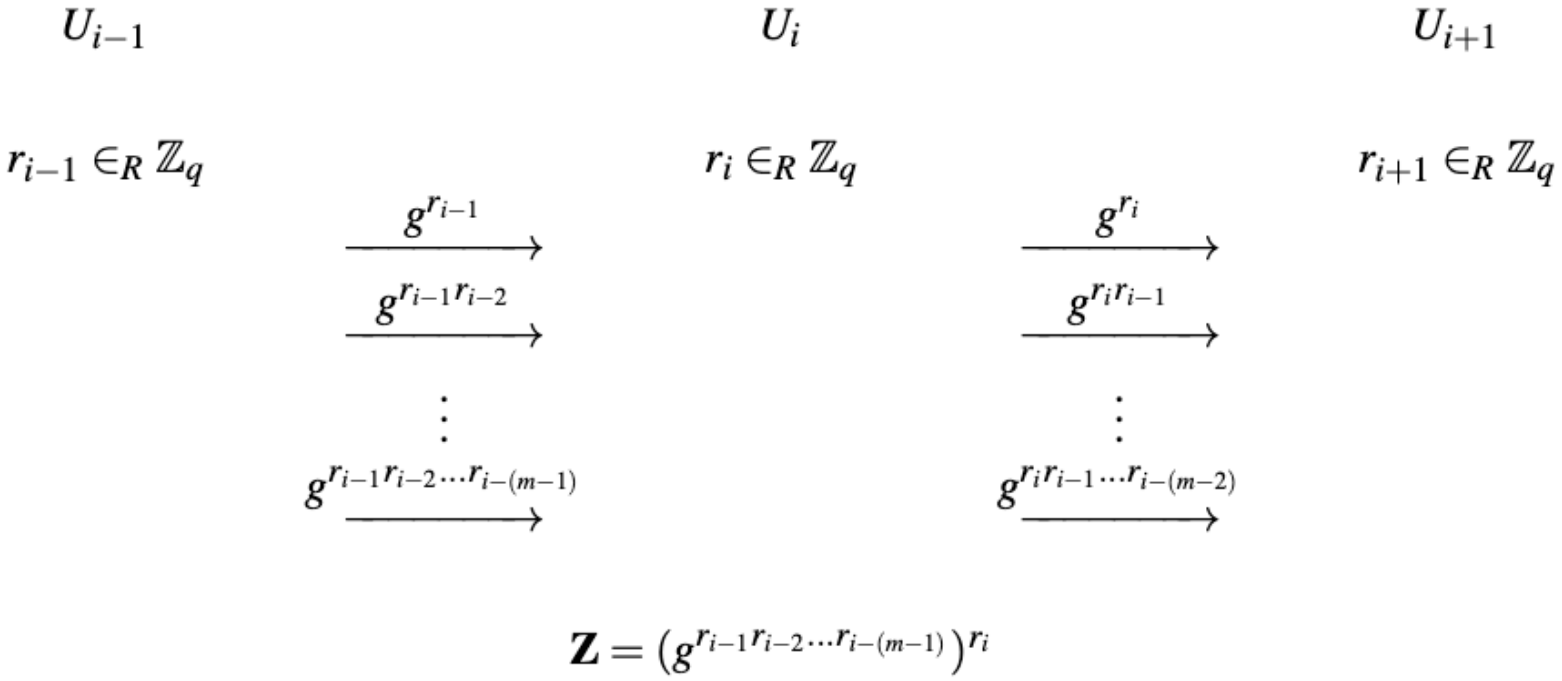
PQ-SRP?

PQ-SRP? Yes! Also RLWE!

Party i		Party j
Ephemeral public key: $p_i = as_1 + 2e_1 \in R_q$ Private key: $s_1 \in R_q$ where $s_1, e_1 \leftarrow D_{Z^n,\sigma}$	$< I, p_i >$ →	Ephemeral public key: $p_j = as'_1 + 2e'_1 + v \in R_q$ Private key: $s'_1 \in R_q$ Verifier: $v \in R_q$ where $s'_1, e'_1 \leftarrow D_{Z^n,\sigma}$
$u = XOF(H(p_i \Vert p_j)) \in R_q$ $v = as_v + 2e_v$ $k_i = (p_j - v)(s_v + s_1) + uv + 2e''_1$ where $e''_1 \leftarrow D_{Z^n,\sigma}$ $\sigma_i = \mathrm{Mod}_2(k_i, w_j) \in \{0,1\}^n$ $sk_i = \mathrm{SHA3\text{-}256}(\sigma_i)$	← $< salt, p_j, w_j >$	$u = XOF(H(p_i \Vert p_j)) \in R_q$ $k_j = (v + p_i)s'_1 + uv + 2e'''_1$ where $e'''_1 \leftarrow D_{Z^n,\sigma}$ $w_j = \mathrm{Cha}(k_j) \in \{0,1\}^n$ $\sigma_j = \mathrm{Mod}_2(k_j, w_j) \in \{0,1\}^n$ $sk_j = \mathrm{SHA3\text{-}256}(\sigma_j)$

source: 'Post-Quantum Secure Remote Password Protocol from RLWE Problem' (Gao Ding Liu Li, 2018)

Group Key Exchange



$$\mathbf{Z} = \left(g^{r_{i-1}r_{i-2}\cdots r_{i-(m-1)}}\right)^{r_i}$$

source: 'Protocols for Authentication and Key Establishment' (Boyd, Mathuria, Stebila, 2019)

PQ-GKE?

PQ-GKE? Yes! RLWE!

Public parameter: $R_q = \mathbb{Z}_q[x]/(x^n + 1)$, $a \leftarrow \mathcal{U}(R_q)$.

Round 1: Each player P_i samples $s_i, e_i \leftarrow \chi_{\sigma_1}$ and broadcasts $z_i = as_i + e_i$.
Round 2: Player P_0 samples $e'_0 \leftarrow \chi_{\sigma_2}$ and each of the other players P_i samples $e'_i \leftarrow \chi_{\sigma_1}$, broadcasts $X_i = (z_{i+1} - z_{i-1})s_i + e'_i$.
Round 3: Player P_{N-1} proceeds as follows:

1. Samples $e''_{N-1} \leftarrow \chi_{\sigma_1}$ and computes $b_{N-1} = z_{N-2}Ns_{N-1} + e''_{N-1} + X_{N-1} \cdot (N-1) + X_0 \cdot (N-2) + \cdots + X_{N-3}$.
2. Computes $(K_{N-1}, k_{N-1}) = \mathsf{recMsg}(b_{N-1})$ and broadcasts K_{N-1}.
3. Obtains session key $\mathsf{sk}_{N-1} = \mathcal{H}(k_{N-1})$.

Key Computation: Each player P_i (except P_{N-1}) proceeds as follows:

1. Computes $b_i = z_{i-1}Ns_i + X_i \cdot (N-1) + X_{i+1} \cdot (N-2) + \cdots + X_{i+N-2}$.
2. Computes $k_i = \mathsf{recKey}(b_i, K_{N-1})$, and obtains session key $\mathsf{sk}_i = \mathcal{H}(k_i)$.

source: 'Constant-round group key exchange from the RLWE assumption' (Apon, Dachman-Soled, Gong, 2019)

Summarized

- Pre-quantum crypto is more than Key Exchange, signatures and other ‘popular’ constructions.
- There are several constructions we should use more.
- Some of those are used more than you think!

Summarized

- Pre-quantum crypto is more than Key Exchange, signatures and other ‘popular’ constructions.
- There are several constructions we should use more.
- Some of those are used more than you think!

- That means a need for (more / better) PQ-variants.

Even more summarized

- There are cool research topics out there!

Even more summarized

- There are cool research topics out there!

Questions?

Contact: Bor de Kock, NTNU Trondheim
bor.dekock@ntnu.no