Ouroboros: A Simple, Secure and Efficient Key Exchange Protocol Based on Coding Theory

www.unilim.fr/pages_perso/deneuville/files/ba43bf8d80cef2999dbf4308828213ec.pdf

(paper by Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor)

Tung Chou

Post-quantum key-exchange schemes

Isogeny-based

- Similar to ECDH.

Lattice-based

- Popularized by **NewHope** (ePrint/2015/1092).
- Ephemeral, passively-secure KEMs.
- Protected by signature schemes.

Code-based

- **Ouroboros** and **CAKE** (ePrint/2017/757)
- Built from QC-MDPC codes
- *The Asiacrypt-2016 attack can't be applied.*

Preliminaries

- S_w^n: the set of weight-w vectors in $\mathbb{F}_2^n$
- H_w: hash function; hashing into S_w^n
- Vectors are often considered as element in $\mathbb{F}_2[x]/(x^n+1)$

- DSD problem (NP-complete)

  Let $H \xleftarrow{\$} \mathbb{F}_2^{(n-k)\times n}$, $x \xleftarrow{\$} S_w^n$, $y' \xleftarrow{\$} \mathbb{F}_2^{n-k}$, distinguish $(y = Hx, H)$ and (y', H)

Conjectured hard problems

- 2-DQCSD problem

  Let $h, y' \xleftarrow{\$} \mathbb{F}_2^n$, $x_1, x_2 \xleftarrow{\$} S_w^n$, distinguish

  $(y = x_1 + x_2 h, h)$ and (y', h)

$$\vec{y} = \begin{pmatrix} I & h \end{pmatrix} \vec{x}$$

- 3-DQCSD problem

  Let $g, h, y_1', y_2' \xleftarrow{\$} \mathbb{F}_2^n$, $x_1, x_2, x_3 \xleftarrow{\$} S_w^n$, distinguish

  $(y_1 = x_1 + x_3 g, y_2 = x_2 + x_3 h, g, h)$ and (y_1', y_2', g, h)

$$\vec{y} = \begin{pmatrix} I & 0 & g \\ 0 & I & h \end{pmatrix} \vec{x}$$

The Ouroboros protocol

$$x, y \xleftarrow{\$} S_w^n$$
$$\mathbf{h} \xleftarrow{\$} \mathbb{F}_2^n$$
$$\mathbf{s} \leftarrow x + \mathbf{h}y$$

$$\xrightarrow{\mathbf{h}, \mathbf{s}}$$

$$r_1, r_2 \xleftarrow{\$} S_w^n$$
$$\mathbf{s_r} \leftarrow r_1 + \mathbf{h}r_2$$
$$e_r \leftarrow H_{cw}(r_1, r_2)$$
$$\epsilon \xleftarrow{\$} S_{w_\epsilon}^n$$
$$\mathbf{s}_\epsilon \leftarrow \mathbf{s}r_2 + e_r + \epsilon$$

$$\xleftarrow{\mathbf{s_r}, \mathbf{s}_\epsilon}$$

$$\mathbf{e_c} \leftarrow \mathbf{s}_\epsilon - y\mathbf{s_r}$$
$$(r_1, r_2) \leftarrow Dec(x, y, e_c, t, w, w_\epsilon)$$
$$\epsilon \leftarrow e_\epsilon - xr_2 + yr_1 - H_{cw}(r_1, r_2)$$

The Ouroboros protocol (simplified)

$\mathbf{s} \leftarrow x + \mathbf{h}y$

$$\xrightarrow{\mathbf{h}, \mathbf{s}}$$

$\mathbf{s_r} \leftarrow r_1 + \mathbf{h}r_2$

$e_r \leftarrow H_{cw}(r_1, r_2)$

$\mathbf{s}_\epsilon \leftarrow \mathbf{s}r_2 + e_r + \epsilon$

$$\xleftarrow{\mathbf{s_r}, \mathbf{s}_\epsilon}$$

$\mathbf{e_c} \leftarrow \mathbf{s}_\epsilon - y\mathbf{s_r}$

$(r_1, r_2) \leftarrow Dec(x, y, e_c)$

$\epsilon \leftarrow e_c - xr_2 + yr_1 - H_{cw}(r_1, r_2)$

- *Can be viewed as a KEM that encrypts ϵ.*
- *The protocol is secure if the KEM satisfies IND-CPA.*

Decoding

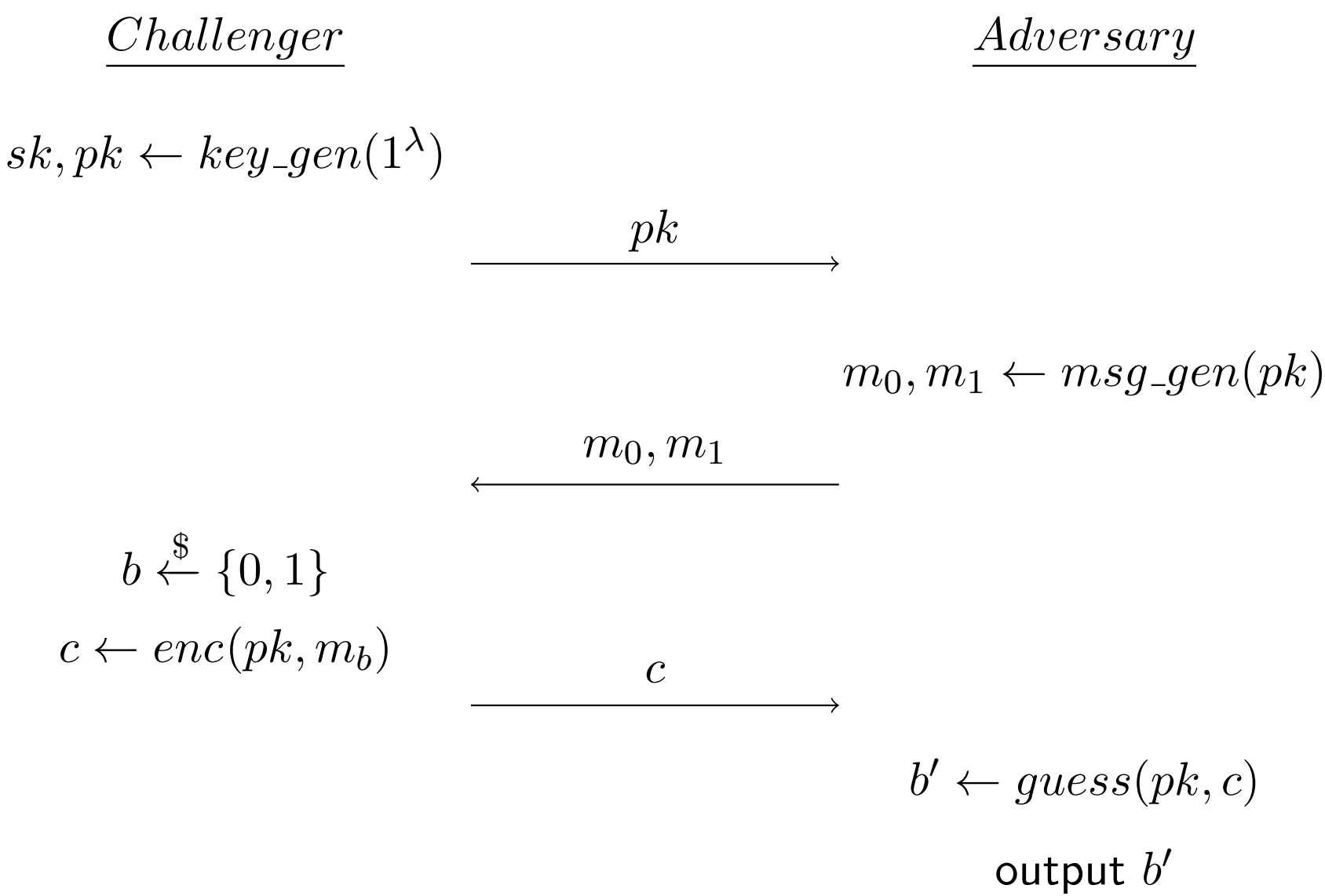
Decoding for QC-LDPC codes

- Given $x_1, \ldots, x_{n_0}$, $s = x_1 r_1 + x_2 r_2 + \cdots + x_{n_0} r_{n_0}$, $r_1, \ldots, r_{n_0}$ can be recovered using the bit-flipping algorithm.

Ouroboros

- $e_c = s_\epsilon + y s_r = x r_2 + y r_1 + (e_r + \epsilon)$.
- Claimed that given x, y, e_c, $r_1, r_2, (e_r + \epsilon)$ can be recovered.

IND-CPA


Challenger
Adversary
$sk, pk \leftarrow key\_gen(1^\lambda)$
pk
$m_0, m_1 \leftarrow msg\_gen(pk)$
m_0, m_1
$b \xleftarrow{\$} \{0,1\}$
$c \leftarrow enc(pk, m_b)$
c
$b' \leftarrow guess(pk, c)$
output b'

Hybrid argument

To prove two distributions D_0 and D_1 are indistinguishable, define

$$H_1 := D_0,\ H_2,\ \ \ldots,\ H_t := D_1$$

and show that for any PPT A

$$Adv_{H_i,H_{i+1}}(A) = \left| Pr[x \xleftarrow{\$} H_i : A(x) = 1] - Pr[x \xleftarrow{\$} H_{i+1} : A(x) = 1] \right|$$

are negligible.

IND-CPA security with hybrid argument

An alternative way to prove IND-CPA security

- $G_{b=0}$: IND-CPA game with $b = 0$
- $G_{b=1}$: IND-CPA game with $b = 1$
- Show that G_0 and G_1 are indistinguishable

With hybird argument

- Define $G_1 := G_{b=0},\ G_2,\ \ldots,\ G_t := G_{b=1}$
- Show that G_i and G_{i+1} are indistinguishable

Proof for Ouroboros

- using hybrid argument $t = 8$
- $b = 0$ for h_1, h_2, h_3, h_4; $b = 1$ for h_5, h_6, h_7, h_8
- h_i and h_{9-i} only differs in b

Security proof (G_1)

$$\mathbf{s} \leftarrow x + \mathbf{h}y$$

$$\xrightarrow{\mathbf{h}, \mathbf{s}}$$

$$\mathbf{s_r} \leftarrow r_1 + \mathbf{h}r_2$$
$$e_r \leftarrow H_{cw}(r_1, r_2)$$
$$\mathbf{s}_\epsilon \leftarrow \mathbf{s}r_2 + e_r + \epsilon^{(0)}$$

$$\xrightarrow{\mathbf{s_r}, \mathbf{s}_\epsilon}$$

Security proof (G_2)

$$\mathbf{s} \leftarrow x + \mathbf{h}y$$

$$\xrightarrow{\mathbf{h}, \mathbf{s}}$$

$$\mathbf{s_r} \leftarrow r_1 + \mathbf{h}r_2$$

~~$e_r \leftarrow H_{cw}(r_1, r_2)$~~

$$\mathbf{s}_\epsilon \leftarrow \mathbf{s}r_2 + e_r + \epsilon^{(0)}$$

$$\xrightarrow{\mathbf{s_r}, \mathbf{s}_\epsilon}$$

Indistinguishable from G_1 in the **Random Oracle** model.

Security proof (G_3)

$$\mathbf{s} \leftarrow \mathbf{x} + \mathbf{h}\mathbf{y}$$

$$\xrightarrow{\mathbf{h}, \mathbf{s}}$$

$$\mathbf{s_r} \leftarrow r_1 + \mathbf{h}r_2$$

~~$e_r \leftarrow H_{cw}(r_1, r_2)$~~

$$\mathbf{s}_\epsilon \leftarrow \mathbf{s}r_2 + e_r + \epsilon^{(0)}$$

$$\xrightarrow{\mathbf{s_r}, \mathbf{s}_\epsilon}$$

Indistinguishable from G_2 because of **2-DQCSD**.

Security proof (G_4)

$$\mathbf{s} \leftarrow \mathbf{x} + \mathbf{h}\mathbf{y}$$

$$\xrightarrow{\mathbf{h}, \mathbf{s}}$$

$$\mathbf{s_r} \leftarrow \mathbf{r_1} + \mathbf{h}\mathbf{r_2}$$

$$\cancel{e_r \leftarrow H_{cw}(r_1, r_2)}$$

$$\mathbf{s}_\epsilon \leftarrow \mathbf{s}\mathbf{r_2} + \mathbf{e_r} + \epsilon^{(0)}$$

$$\xrightarrow{\mathbf{s_r}, \mathbf{s}_\epsilon}$$

Indistinguishable from G_3 because of **3-DQCSD**.

G_3 versus G_4

3-QCSD: $\begin{pmatrix} I & 0 & h \\ 0 & I & s \end{pmatrix} \begin{pmatrix} r_1 \\ e'_r \\ r_2 \end{pmatrix}$ $\xleftrightarrow{\text{dist.}}$ $\begin{pmatrix} \$ \\ \$ \end{pmatrix}$

Adversary: $\begin{pmatrix} e_r \\ e_\epsilon \end{pmatrix} = \begin{pmatrix} I & 0 & h \\ 0 & I & s \end{pmatrix} \begin{pmatrix} r_1 \\ e'_r \\ r_2 \end{pmatrix} + \begin{pmatrix} 0 \\ \epsilon \end{pmatrix}$ $\xleftrightarrow{\text{dist.}}$ $\begin{pmatrix} \$ \\ \$ \end{pmatrix} + \begin{pmatrix} 0 \\ \epsilon \end{pmatrix}$

Security proof (G_5)

$$\mathbf{s} \leftarrow \mathbf{x} + \mathbf{h}\mathbf{y}$$

$$\xrightarrow{\mathbf{h}, \mathbf{s}}$$

$$\mathbf{s_r} \leftarrow \mathbf{r_1} + \mathbf{h}\mathbf{r_2}$$

$$\cancel{e_r \leftarrow H_{cw}(r_1, r_2)}$$

$$\mathbf{s}_\epsilon \leftarrow \mathbf{s}\mathbf{r_2} + \mathbf{e_r} + \epsilon^{(1)}$$

$$\xrightarrow{\mathbf{s_r}, \mathbf{s}_\epsilon}$$

Indistinguishable from G_4: (s_r, s_ϵ) is still **uniform random**.

Parameters

	Ouroboros Parameters					
Instance	n	w	$w_{\mathbf{e}}$	threshold	security	DFR
Low-I	$5,851$	47	94	30	80	$0.92 \cdot 10^{-5}$
Low-II	$5,923$	47	94	30	80	$2.3 \cdot 10^{-6}$
Medium-I	$13,691$	75	150	45	128	$0.96 \cdot 10^{-5}$
Medium-II	$14,243$	75	150	45	128	$1.09 \cdot 10^{-6}$
Strong-I	$40,013$	147	294	85	256	$4.20 \cdot 10^{-5}$
Strong-II	$40,973$	147	294	85	256	$< 10^{-6}$

Table 1. Parameter sets for Ouroboros

	Ouroboros Optimized Parameters					
Instance	n	w	$w_{\mathbf{e}}$	threshold	security	DFR
Low-I	$4,813$	41	123	27	80	$2.23 \cdot 10^{-5}$
Low-II	$5,003$	41	123	27	80	$2.60 \cdot 10^{-6}$
Medium-I	$10,301$	67	201	42	128	$1.01 \cdot 10^{-4}$
Medium-II	$10,837$	67	201	42	128	$< 10^{-7}$
Strong-I	$32,771$	131	393	77	256	$< 10^{-4}$
Strong-II	$33,997$	131	393	77	256	$< 10^{-7}$

Table 2. Optimized parameter sets for Ouroboros in Hamming metric