Nonabelian Cryptography

Boaz Tsaban

Bar-Ilan University

Secure Implementation of Post-Quantum Cryptography
Sep '16

Key Exchange Protocols

Alice and Bob establish a secret key over an insecure channel.

Diffie–Hellman 1976. DLP in finite fields.

Rivest-Shamir-Adleman (RSA, 1978). Factorization.

Poor performance vs security tradeoff; no long-term security.

Joux et al.: Subexp algorithms for DLP in some elliptic curves.

Quantum computers break them all.

Alternatives: (1) Lattice-based; (2) **nonabelian-based**.

Nonabelian Diffie–Hellman

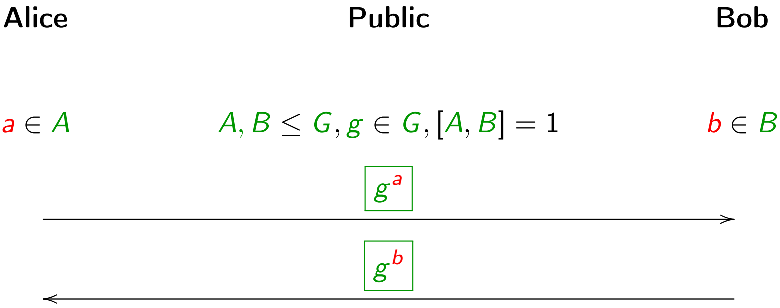
Diffie–Hellman 1976.

Alice	**Public**	**Bob**
$a \in \{0, 1, \ldots, p-1\}$	$G = \langle g \rangle, \ \lvert G \rvert = p$	$b \in \{0, 1, \ldots, p-1\}$
	$\xrightarrow{\boxed{g^{a}}}$	
	$\xleftarrow{\boxed{g^{b}}}$	
$K = \boxed{g^{b}}^{a} = g^{ab}$		$K = \boxed{g^{a}}^{b} = g^{ab}$

Nonabelian Diffie–Hellman

Ko–Lee–Cheon–Han–Kang–Park 2000. G nonabelian.

$g^x := x^{-1}gx$.



Alice **Public** **Bob**

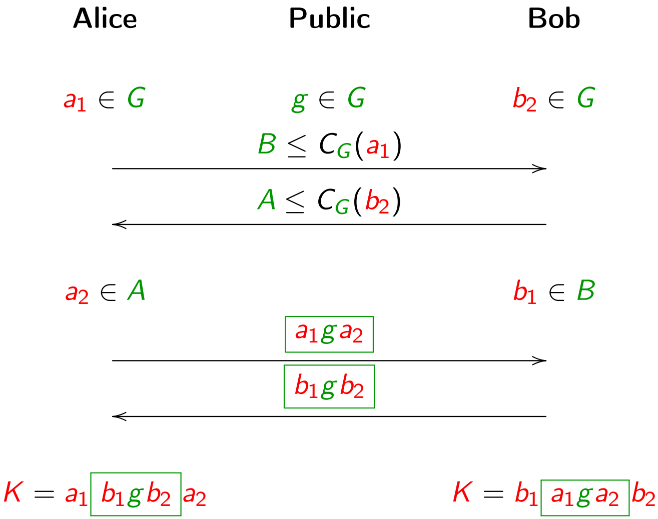
$a \in A$ $A, B \le G, g \in G, [A, B] = 1$ $b \in B$

$\xrightarrow{\boxed{g^a}}$

$\xleftarrow{\boxed{g^b}}$

$K = \boxed{g^b}^{a} = g^{ba}$ $K = \boxed{g^a}^{b} = g^{ab}$

Centralizer KE (Shpilrain–Ushakov 2006)



Alice	**Public**	**Bob**
$a_1 \in G$	$g \in G$	$b_2 \in G$
	$\xrightarrow{B \leq C_G(a_1)}$	
	$\xleftarrow{A \leq C_G(b_2)}$	
$a_2 \in A$		$b_1 \in B$
	$\xrightarrow{\boxed{a_1 g a_2}}$	
	$\xleftarrow{\boxed{b_1 g b_2}}$	
$K = a_1 \boxed{b_1 g b_2} a_2$		$K = b_1 \boxed{a_1 g a_2} b_2$

Commutator KE (Anshel–Anshel–Goldfeld 1999)

Alice	**Public**	**Bob**
$v(x_1,\dots,x_k)\in F_k$	$\langle a_1,\dots,a_k\rangle \le G$	$w(x_1,\dots,x_k)\in F_k$
$a = v(a_1,\dots,a_k)$	$\langle b_1,\dots,b_k\rangle \le G$	$b = w(b_1,\dots,b_k)$
	$\xrightarrow{\boxed{b_1{}^a},\dots,\boxed{b_k{}^a}}$	
	$\xleftarrow{\boxed{a_1{}^b},\dots,\boxed{a_k{}^b}}$	
$a^{-1}v(\boxed{a_1^b},\dots,\boxed{a_k^b})$		$w(\boxed{b_1^a},\dots,\boxed{b_k^a})^{-1}b$

$$a^{-1}v(a_1^b,\dots,a_k^b) = a^{-1}a^b = a^{-1}b^{-1}ab = (b^a)^{-1}b = w(b_1^a,\dots,b_k^a)^{-1}b$$

Triple Decomposition KE (Kurt 2005)

Alice **Public** **Bob**

a, a_1, a_2, x_1, x_2

$$\begin{array}{cccccc} A & A_1 & A_2 & X_1 & X_2 & \\ & | & | & | & | & \\ & Y_1 & Y_2 & B_1 & B_2 & B \end{array} \leq G$$

y_1, y_2, b_1, b_2, b

$$\xrightarrow{\boxed{ax_1}, \boxed{x_1^{-1}a_1x_2}, \boxed{x_2^{-1}a_2}}$$

$$\xleftarrow{\boxed{b_1y_1}, \boxed{y_1^{-1}b_2y_2}, \boxed{y_2^{-1}b}}$$

$$a\boxed{b_1y_1}a_1\boxed{y_1^{-1}b_2y_2}a_2\boxed{y_2^{-1}b} = \underbrace{ab_1a_1b_2a_2b}_{K} = \boxed{ax_1}b_1\boxed{x_1^{-1}a_1x_2}b_2\boxed{x_2^{-1}a_2}b$$

Faithful representations

All mentioned KEPs suggest using the Braid group $\mathbf{B}_N$.

Lawrence–Krammer. $\mathrm{LK}\colon \mathbf{B}_N \longrightarrow \mathrm{GL}_n(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$.

$n = \binom{N}{2}$.

Bigelow 2001 (JAMS), Krammer 2002 (Annals):
LK representation is faithful.

Cheon–Jun 2003.

1. LK Evaluation: Fast. Inversion: N^6 (acceptable).
2. $\therefore$ May work in the image of $\mathbf{B}_N$ in $\mathrm{GL}_n(\mathbb{Z}[t^{\pm 1}, \frac{1}{2}])$.
3. Take out common denominator.
4. Mod by large p and irreducible $f(t)$,
   $\mathrm{len}(\ell)$ and $d := \deg(f)$ polynomial in the security parameter.
5. Key recoverable from its image in $\mathbb{F}_{p^d}$.

$\therefore$ May work in $\mathrm{GL}_n(\mathbb{F})$; $\mathbb{F}$ a finite field.

Algebraic spans

Assume $G = \langle g_1, \dots, g_k \rangle \leq M = \mathrm{M}_n(\mathbb{F})$.

For $S \subseteq \mathrm{M}_n(\mathbb{F})$, $\mathrm{Alg}(S)$:= algebra generated by S.

$\mathrm{Alg}(G) = \mathrm{span}_{\mathbb{F}}(G)$, a vector space.

Finding a basis B of $\mathrm{Alg}(G)$ in time kn^6:

```
1. $B := (I)$, the identity matrix.
2. For $i = 1, 2, \dots$:
    2.1 $b := B(i)$.
    2.2 For $j = 1, \dots, k$: if $bg_i \notin \mathrm{span}\, B$, append it to $B$.
    2.3 Stop when reaching the end of the list.
```

Algebraic span cryptanalysis

$G_1, \ldots, G_k \leq \mathrm{GL}_n(\mathbb{F})$; $g_1 \in G_1, \ldots, g_k \in G_k$.

Given: linear equations on the entries of $g_1, \ldots, g_k$.

Need to find $f(g_1, \ldots, g_k)$.

Instead of solving subject to

$$g_1 \in G_1, \ldots, g_k \in G_k,$$

solve subject to the linear constraints

$$g_1 \in \mathrm{Alg}(G_1), \ldots, g_k \in \mathrm{Alg}(G_k).$$

Pray (or prove) that every solution $\tilde{g}_1, \ldots, \tilde{g}_k$ satisfies

$$f(\tilde{g}_1, \ldots, \tilde{g}_k) = f(g_1, \ldots, g_k).$$

This often works!

Application 1: Nonabelian Diffie–Hellman

Alice	**Public**	**Bob**
$a \in A$	$A, B \leq G, g \in G, [A, B] = 1$	$b \in B$

$$\xrightarrow{\boxed{g^{a}}}$$

$$\xleftarrow{\boxed{g^{b}}}$$

$$K = \boxed{g^{b}}^{a} = g^{ba} \qquad\qquad K = \boxed{g^{a}}^{b} = g^{ab}$$

Solve $g\,a = a \cdot \boxed{g^{a}}$, $a \in \mathrm{Alg}(A)$. $\Rightarrow$ invertible solution $\tilde{a}$.

$$\boxed{g^{b}}^{\tilde{a}} = g^{b\tilde{a}} = g^{\tilde{a}b} = (g^{\tilde{a}})^{b} = (g^{a})^{b} = g^{ab} = K.$$

Finding an invertible solution

Problem. Find an invertible matrix in a subspace of $M_n(\mathbb{F})$.

Heuristic. Pick “random” elements until invertible.

Lemma. Assume $\operatorname{span}\{A_1, \ldots, A_m\} \cap \mathrm{GL}_n(\mathbb{F}) \neq 0$. Then

$$\Pr(|x_1 A_1 + \cdots + x_m A_m| \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

Proof: $f(x_1, \ldots, x_m) := |x_1 A_1 + \cdots + x_m A_m| \in \mathbb{F}[x_1, \ldots, x_m]$, nonzero, degree n.

Schwartz–Zippel Lemma.
$f(x_1, \ldots, x_m) \in \mathbb{F}[x_1, \ldots, x_m]$ nonzero, degree n.

$$\Pr(f(x_1, \ldots, x_m) \neq 0) \geq 1 - \frac{n}{|\mathbb{F}|}.$$

In our case, $|\mathbb{F}| \gg n$.

Example 2: Centralizer KEP

$g, a_1, b_2 \in G$, $B \leq C_G(a_1)$, $A \leq C_G(b_2)$, $a_2 \in A$, $b_1 \in B$.

Need: $(a_1 g a_2, b_1 g b_2) \mapsto a_1 b_1 g a_2 b_2$.

1. Solve

$$\begin{aligned} a_1 g &= \boxed{a_1 g a_2} \cdot a_2^{-1} \\ a_1 b &= b a_1 \quad \big(b \in \text{Generators}(B)\big). \end{aligned}$$

   with $a_2^{-1} \in \text{Alg}(A)$ invertible.

2. $\exists$ solution: (a_1, a_2^{-1}). Let $(\tilde{a}_1, \tilde{a}_2^{-1})$ be one.
3. $\tilde{a}_1 \boxed{b_1 g b_2} \tilde{a}_2 \overset{!}{=} b_1 \tilde{a}_1 g \tilde{a}_2 b_2 = b_1 a_1 g a_2 b_2 = K$!

Example 3: Commutator KEP

$a \in \langle a_1, \ldots, a_k \rangle, b \in \langle b_1, \ldots, b_k \rangle \leq G \leq \mathrm{GL}_n(\mathbb{F})$.

Need: $({b_1}^a, \ldots, {b_k}^a, {a_1}^b, \ldots, {a_k}^b) \mapsto a^{-1}b^{-1}ab$.

1. Solve

$$\begin{array}{rcl} b_1 a & = & a \cdot \boxed{{b_1}^a} \\ & \vdots & \\ b_k a & = & a \cdot \boxed{{b_k}^a} \end{array} \quad ; \quad \begin{array}{rcl} a_1 b & = & b \cdot \boxed{{a_1}^b} \\ & \vdots & \\ a_k b & = & b \cdot \boxed{{a_k}^b} \end{array}$$

   with $a \in \mathrm{Alg}(a_1, \ldots, a_k)$, $b \in \mathrm{Alg}(b_1, \ldots, b_k)$, both invertible.
2. $\exists$ solution: (a, b). Let $(\tilde{a}, \tilde{b})$ be one.
3. $\tilde{a}^{\tilde{b}} = \tilde{a}^b$ since $\tilde{a} \in \mathrm{Alg}(a_1, \ldots, a_k)$. Similarly, $b^{\tilde{a}} = b^a$.
4. $\tilde{a}^{-1}\tilde{b}^{-1}\tilde{a}\tilde{b} = \tilde{a}^{-1}\tilde{a}^{\tilde{b}} = \tilde{a}^{-1}\tilde{a}^b = \tilde{a}^{-1}b^{-1}\tilde{a}b = (b^{\tilde{a}})^{-1}b = (b^a)^{-1}b = a^{-1}b^{-1}ab$!

Reminder: Triple Decomposition KE (Kurt 2005)

Alice **Public** **Bob**

a, a_1, a_2, x_1, x_2

$$\begin{array}{cccccc} A & A_1 & A_2 & X_1 & X_2 & \\ & | & | & | & | & \\ & Y_1 & Y_2 & B_1 & B_2 & B \end{array} \leq G$$

y_1, y_2, b_1, b_2, b

$$\xrightarrow{\boxed{ax_1}, \boxed{x_1^{-1}a_1x_2}, \boxed{x_2^{-1}a_2}}$$

$$\xleftarrow{\boxed{b_1y_1}, \boxed{y_1^{-1}b_2y_2}, \boxed{y_2^{-1}b}}$$

$$a\boxed{b_1y_1}a_1\boxed{y_1^{-1}b_2y_2}a_2\boxed{y_2^{-1}b} = \underbrace{ab_1a_1b_2a_2b}_{K} = \boxed{ax_1}b_1\boxed{x_1^{-1}a_1x_2}b_2\boxed{x_2^{-1}a_2}b$$

The triple products do not provide linear equations!

Without them we fail!

Cryptanalysis of Triple Dec KE (Ben Zvi-Kalka-Ts.)

$$\mathrm{Alg}(B_1)y_1 = \mathrm{Alg}(B_1)\cdot \boxed{b_1 y_1}$$

$$\mathrm{Alg}(B_2 \cup Y_2)y_1 = \mathrm{Alg}(B_2 \cup Y_2)\cdot y_2^{-1}b_2^{-1}y_1 = \mathrm{Alg}(B_2 \cup Y_2)\cdot \boxed{y_1^{-1}b_2 y_2}^{-1}$$

$$\mathrm{Alg}(A_2)x_2 = \mathrm{Alg}(A_2)\cdot a_2^{-1}x_2 = \mathrm{Alg}(A_2)\cdot \boxed{x_2^{-1}a_2}^{-1}$$

$$\mathrm{Alg}(A_1 \cup X_1)x_2 = \mathrm{Alg}(A_1 \cup X_1)\cdot \boxed{x_1^{-1}a_1 x_2}$$

Pick invertible

$$\tilde{y}_1 \in \mathrm{Alg}(Y_1) \cap \mathrm{Alg}(B_1)y_1 \cap \mathrm{Alg}(B_2 \cup Y_2)y_1;$$
$$\tilde{x}_2 \in \mathrm{Alg}(X_2) \cap \mathrm{Alg}(A_2)x_2 \cap \mathrm{Alg}(A_1 \cup X_1)x_2.$$

$$\boxed{ax_1}\cdot\boxed{b_1 y_1}\cdot\tilde{y}_1^{-1}\cdot\boxed{x_1^{-1}a_1 x_2}\cdot\tilde{x}_2^{-1}\cdot\tilde{y}_1\cdot\boxed{y_1^{-1}b_2 y_2}\cdot\tilde{x}_2\cdot\boxed{x_2^{-1}a_2}\cdot\boxed{y_2^{-1}b}$$

gives (intricate proof) $ab_1a_1b_2a_2b = K$!

(Alternatively, could check empirically.)

Intermediate (?) discussion

Not the end of nonabelian cryptography:

1. Additional nonabelian proposals (Dehornoy et al., Kalka, . . .).
2. Additional problems (CSP, Multiple CSP,. . .) to build upon.
3. Groups with no small-dim representations.
4. The application of my methods keeps getting harder as new systems emerge (cf. recent cryptanalysis of Algebraic Eraser).

∴ Psychological cryptography: We don’t break because we fail to find a polytime attack (cf. SHA3).

Part II: PILES of salt!

The shortest description ever for a hash function

$A, B \in M_n(\mathbb{F})$.

Hashing $\{0,1\}^* \to M_n(\mathbb{F})$: Replace 0 by A, 1 by B, and multiply.

Example: $h(00101) = AABAB$.

Probably more efficient than other (Lattice-based) provable hash functions.

Security of homomorphic (Cayley) hash

Focus on $|\mathbb{F}| = 2^n$.

Efficient cryptanalysis for few pairs A, B, including

$$\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} \alpha + 1 & 1 \\ 1 & 0 \end{pmatrix}$$

In general, there is a subexp attack, but *less efficient than generic ones*.

Mullan–Ts. '16: Worst-case to average-case reduction (aka random self-reducibility).

Best attack: $2^{n/2}$.

Challenge: Attack. Do QCs help?

TS Hash: How about that?

$$S(x_n, \dots, x_1) := (0, \dots, 0, x_n, \dots, x_{k+2}, x_{k+1}),$$

k minimal with $x_k = 1$.

Fix random known vectors $v, v_0, v_1 \in \{0,1\}^n$.

$$T_i(u) := u \oplus v_i.$$

$$\begin{aligned} h(b_l, b_{l-1}, \dots, b_2, b_1) &:= T_{b_l} S T_{b_{l-1}} \cdots T_{b_2} S T_{b_1} S(v) \\ &= S(\cdots(S(S(v) \oplus v_{b_1}) \oplus v_{b_2}) \cdots) \oplus v_{b_l}. \end{aligned}$$

Challenge: Break this.

Classically secure nonabelian schemes seem to be automatically QC secure.

THANK YOU!