Diffie–Hellman reductions

Lorenz Panny

Technische Universiteit Eindhoven

Ei/Ψ seminar, Eindhoven, 29 April 2019
Hardness reductions in cryptography

Recall RSA encryption (simplified special case):

- **Private key:** two big prime numbers $p, q$.
- **Public key:** their product $n = pq$.
- **Encrypt:** compute $c = m^{65537} \mod n$.
- **Decrypt:** compute $m = c^{65537-1} \mod \text{lcm}(p-1, q-1) \mod pq$.

Clearly, anyone who can factor $n$ can decrypt.
Recall RSA encryption (simplified special case):

- Private key: two big prime numbers $p, q$.
- Public key: their product $n = pq$.
- Encrypt: compute $c = m^{65537} \mod n$.
- Decrypt: compute $m = c^{65537^{-1} \mod \text{lcm}(p-1, q-1)} \mod pq$.

Clearly, anyone who can factor $n$ can decrypt.

Q: Can everyone capable of decrypting also factor $n$?
Hardness reductions in cryptography

Recall RSA encryption (simplified special case):

- Private key: two big prime numbers \( p, q \).
- Public key: their product \( n = pq \).
- Encrypt: compute \( c = m^{65537} \mod n \).
- Decrypt: compute \( m = c^{65537^{-1} \mod \text{lcm}(p-1, q-1)} \mod pq \).

Clearly, anyone who can factor \( n \) can decrypt.

Q: Can everyone capable of decrypting also factor \( n \)?

If yes:
No point attacking RSA specifically; just focus on factoring.
Diffie–Hellman key exchange (very big picture)

The magic words are Squeamish Ossifrage
Diffie–Hellman key exchange  (very big picture)

Parameters: a finite set $X$, a fixed element $x \in X$.

The magic words are Squeamish Ossifrage

$\text{ab} \quad \text{a(b(x)) b(a(x))}$

▶ Private keys: efficient functions $a, b: X \rightarrow X$ such that $a \circ b = b \circ a$.

▶ Public keys: the elements $a(x), b(x) \in X$.

▶ Shared secret: the element $a(b(x)) = b(a(x))$. 

evil eavesdropper Eve!
Diffie–Hellman key exchange

Parameters: a finite set \( X \), a fixed element \( x \in X \).

evil eavesdropper Eve!

The magic words are Squeamish Ossifrage

\[ a(b(x)) \]

\[ a(b(x)) b(a(x)) \]

Private keys: efficient functions \( a, b : X \rightarrow X \) such that \( a \circ b = b \circ a \).

Public keys: the elements \( a(b(x)), b(a(x)) \in X \).

Shared secret: the element \( a(b(x)) = b(a(x)) \).

evil eavesdropper Eve!
Diffie–Hellman key exchange (very big picture)

Parameters: a finite set $X$, a fixed element $x \in X$.

- Private keys:
  efficient functions $a, b : X \rightarrow X$. 
Diffie–Hellman key exchange (very big picture)

Parameters: a finite set $X$, a fixed element $x \in X$.

- **Private keys:**
  - efficient functions $a, b : X \to X$.
- **Public keys:** the elements $a(x), b(x) \in X$. 

$\begin{align*}
\text{a(x)} & \quad \text{???} & \quad \text{b(x)} \\
\text{a} & \quad \text{???} & \quad \text{b}
\end{align*}$
Diffie–Hellman key exchange (very big picture)

Parameters: a finite set $X$, a fixed element $x \in X$.

- Private keys: efficient functions $a, b : X \rightarrow X$ such that $a \circ b = b \circ a$.
- Public keys: the elements $a(x), b(x) \in X$.
- Shared secret: the element $a(b(x)) = b(a(x))$. 

evil eavesdropper Eve!

The magic words are Squeamish Ossifrage
This talk

Is computing $a(b(x))$ as hard as recovering $a$ or $b$?
This talk

Is computing $a(b(x))$ as hard as recovering $a$ or $b$?

- Standard proof technique:
  Use a black-box ‘oracle’
  
  $\mathcal{O} : (x, a(x), b(x)) \mapsto a(b(x))$

  to construct an efficient algorithm
  
  $A(\mathcal{O}) : a(x) \mapsto a$.

  (The oracle formalizes an attack that we don’t know yet.)
Group-based Diffie–Hellman

The only reasonable Diffie–Hellman instantiations 1976–2017:

\((G, \cdot)\) a finite group; \(a, b\) exponents.
Group-based Diffie–Hellman

The only reasonable Diffie–Hellman instantiations 1976–2017: 
$(G, \cdot)$ a finite group; $a, b$ exponentiations.

- Private keys: $a, b \in \mathbb{Z}/\text{ord } g$.
- Public keys: $g^a, g^b$.
- Shared secret: $(g^a)^b = (g^b)^a = g^{ab}$.

Examples:
- Multiplicative groups of finite fields $(F^*_q, \cdot)$.
- Elliptic curves $E$: $y^2 = x^3 + Ax^2 + x$ with 'weird' addition.
Group-based Diffie–Hellman

The only reasonable Diffie–Hellman instantiations 1976–2017: $(G, \cdot)$ a finite group; $a, b$ exponentiations.

- Private keys: $a, b \in \mathbb{Z}/\text{ord } g$.
- Public keys: $g^a, g^b$.
- Shared secret: $(g^a)^b = (g^b)^a = g^{ab}$.

Examples:
- Multiplicative groups of finite fields $(\mathbb{F}_q^*, \cdot)$.
- Elliptic curves $E: y^2 = x^3 + Ax^2 + x$ with ‘weird’ addition.
Problems from Diffie–Hellman

Discrete-logarithm problem (DLP)
Compute $a$ from $g^a$.

Computational Diffie–Hellman problem (CDH)
Compute $g^{ab}$ from $g^a$, $g^b$. 
Problems from Diffie–Hellman

- **Discrete-logarithm problem (DLP)**
  Compute $a$ from $g, g^a$.
Problems from Diffie–Hellman

- **Discrete-logarithm problem (DLP)**
  Compute $a$ from $g, g^a$.

- **Computational Diffie–Hellman problem (CDH)**
  Compute $g^{ab}$ from $g, g^a, g^b$. 
Generic complexity of DLP (Pohlig–Hellman 1978)

- Upshot: If the factorization of $|G|$ is $p_1^{e_1} \cdots p_r^{e_r}$, then one can solve DLP in $O\left(\sum_{i=1}^{r} e_i \cdot (\log |G| + \sqrt{p_i})\right)$ group operations.
  
  $\implies$ Cost dominated by the biggest prime factor of $|G|$.

  $\implies$ DLP is easy if $|G|$ is smooth (i.e., no big prime factors).
Upshot: If the factorization of $|G|$ is $p_1^{e_1} \cdots p_r^{e_r}$, then one can solve DLP in $O(\sum_{i=1}^{r} e_i \cdot (\log |G| + \sqrt{p_i}))$ group operations.

$\implies$ Cost dominated by the biggest prime factor of $|G|$.

$\implies$ DLP is easy if $|G|$ is smooth (i.e., no big prime factors).

!! There are many groups where one can solve DLP faster.
Anyone can...

- **encode** numbers $x$ in the exponents: compute $g^x$.
Diffie–Hellman’s algebraic properties

Anyone can...

- **encode** numbers $x$ in the exponents: compute $g^x$.
- **add** in the exponents: $g^{a+b} = g^a \cdot g^b$.
- **negate** exponents: $g^{-a} = (g^a)^{-1}$.
Diffie–Hellman’s algebraic properties

Anyone can...

- **encode** numbers \( x \) in the exponents: compute \( g^x \).
- **add** in the exponents: \( g^{a+b} = g^a \cdot g^b \).
- **negate** exponents: \( g^{-a} = (g^a)^{-1} \).

Anyone who can solve CDH can...

- **multiply** exponents: \( g^{a\cdot b} = \text{shared}_\text{secret}(g, g^a, g^b) \).
Diffie–Hellman’s algebraic properties

Anyone can...

- **encode** numbers $x$ in the exponents: compute $g^x$.
- **add** in the exponents: $g^{a+b} = g^a \cdot g^b$.
- **negate** exponents: $g^{-a} = (g^a)^{-1}$.

Anyone who can solve CDH can...

- **multiply** exponents: $g^{a \cdot b} = \text{shared}_\text{secret}(g, g^a, g^b)$.
- **exponentiate** exponents: square-and-multiply using $\uparrow$. 
Diffie–Hellman’s algebraic properties

Anyone can...

- **encode** numbers $x$ in the exponents: compute $g^x$.
- **add** in the exponents: $g^{a+b} = g^a \cdot g^b$.
- **negate** exponents: $g^{-a} = (g^a)^{-1}$.

Anyone who can solve CDH can...

- **multiply** exponents: $g^{a \cdot b} = shared\_secret(g, g^a, g^b)$.
- **exponentiate** exponents: square-and-multiply using $\mathcal{C}$.
- **invert** exponents: $g^{1/a} = g^{a \cdot \varphi(|G|)^{-1}}$ if $\gcd(a, |G|) = 1$ using $\mathcal{C}$.
Black-box rings

- We interpret $g^a$ as labels for the hidden elements $a$.
- With a CDH oracle we can perform arbitrary ring operations ($+, -, \cdot, /$) on these hidden representations.
- **Notation:** Write $[a]$ for the hidden element $g^a$. 
Black-box rings

- We interpret \( g^a \) as **labels** for the **hidden** elements \( a \).
- With a CDH oracle we can perform **arbitrary ring operations** \((+,-,\cdot,/)\) on these hidden representations.
- **Notation:** Write \([a]\) for the hidden element \( g^a \).

The elements \( g^a \) form a **black-box ring** isomorphic to \( \mathbb{Z}/\text{ord } g \).
Black-box rings

- We interpret $g^a$ as labels for the hidden elements $a$.
- With a CDH oracle we can perform arbitrary ring operations ($+, -, \cdot, /$) on these hidden representations.
- **Notation**: Write $\lceil a \rceil$ for the hidden element $g^a$.

The elements $g^a$ form a **black-box ring** isomorphic to $\mathbb{Z}/\text{ord } g$.

We mostly care about **black-box fields**: For discrete logarithms, it’s sufficient to consider prime-order $g$. 
First result: den Boer (1988)

Let $G = \mathbb{F}_p^*$, write $R = \mathbb{Z}/|G| = \mathbb{Z}/(p - 1)$, and suppose $|R^*| = \varphi(p - 1)$ is smooth. Then CDH is polynomial-time equivalent to DLP in $\mathbb{F}_p^*$. 

Proof idea:
Solve a DLP in the exponents $R^*$ to find a representation of $\lceil a \rceil$ as a power of some known $\lceil g \rceil$, then recompute $a$ in the clear.
First result: den Boer (1988)

Let $G = \mathbb{F}_p^*$, write $R = \mathbb{Z}/|G| = \mathbb{Z}/(p - 1)$, and suppose $|R^*| = \varphi(p - 1)$ is smooth. Then CDH is polynomial-time equivalent to DLP in $\mathbb{F}_p^*$.

Proof idea:
Solve a DLP in the exponents $R^*$ to find a representation of $\lceil a \rceil$ as a power of some known $\lceil g \rceil$, then recompute $a$ in the clear.
First result: den Boer (1988)

Let $G = \mathbb{F}_p^*$, write $R = \mathbb{Z}/|G| = \mathbb{Z}/(p - 1)$, and suppose $|R^*| = \varphi(p - 1)$ is smooth. Then CDH is polynomial-time equivalent to DLP in $\mathbb{F}_p^*$.

**Proof idea:**
Solve a DLP in the exponents $R^*$ to find a representation of $[a]$ as a power of some known $[g]$, then recompute $a$ in the clear.

**Proof:**

- Suppose (for simplicity) that $R^*$ is cyclic and find a generator $g$.
- Encode $g$ to a black-box element $[g]$ of $R$.
- Solve the DLP $([g], [a])$ in the hidden version of $R^*$ using Pohlig–Hellman. We get $k \in \mathbb{Z}$ such that $g^a = g^{g^k}$.
- Simply compute $a$ as the power $g^k \in R^*$. 
Observation:
There is nothing special about using $R^*$ in the exponents; in principle anything expressible as field operations works.
Observation:
There is nothing special about using $R^*$ in the exponents; in principle anything expressible as field operations works.

This is known as an auxiliary group:
A smooth-order algebraic group over the black-box field.
Observation:
There is nothing special about using $R^*$ in the exponents; in principle anything expressible as field operations works.

This is known as an auxiliary group:
A smooth-order algebraic group over the black-box field.

Example: For $|G| = p$ with $p^d - 1$ smooth, we can use $\mathbb{F}_{p^d}^*$. 
Second result: Maurer (1994)

Let $G$ be of prime order $p$, write $R = \mathbb{F}_p$, and suppose $E : y^2 = x^3 + Ax^2 + x \mod \mathbb{F}_p$ has smooth order. Then CDH is polynomial-time equivalent to DLP in $G$. 
Let $G$ be of prime order $p$, write $R = \mathbb{F}_p$, and suppose $E: y^2 = x^3 + Ax^2 + x \mod \mathbb{F}_p$ has smooth order. Then CDH is polynomial-time equivalent to DLP in $G$.

**Proof:**

- Find a generator point $G$ on $E$.
- Hope that $\alpha$ is an $x$-coordinate on the curve ($\text{Pr} \approx 1/2$). Compute (black-box) the corresponding $y$-coordinate $\lceil \eta \rceil$, giving a **black-box elliptic-curve point** $\lceil P \rceil = (\lceil \alpha \rceil, \lceil \eta \rceil)$.
  (If $\lceil \eta \rceil^2 \neq \lceil \alpha \rceil^3 + \lceil A \rceil \lceil \alpha \rceil^2 + \lceil \alpha \rceil$, then randomize $\lceil \alpha \rceil$ as $\lceil \alpha' \rceil = \lceil \alpha \rceil + \lceil \delta \rceil$ and retry.)
- Solve the (black-box) DLP $(\lceil G \rceil, \lceil P \rceil)$ via Pohlig–Hellman. We get $k \in \mathbb{Z}$ such that $(\alpha, \eta) = [k]G$.
- Simply compute $\alpha$ as the $x$-coordinate of $[k]G$. 
Let $G$ be of prime order $p$, write $R = \mathbb{F}_p$, and suppose $E : y^2 = x^3 + Ax^2 + x \mod \mathbb{F}_p$ has smooth order. Then CDH is polynomial-time equivalent to DLP in $G$.

Are there always such $E$?  
Unknown in general, but likely. People have constructed some for many ‘common’ groups $G$.

$\implies$ For all practical purposes, DLP is equivalent to CDH.
Let $G$ be of prime order $p$, write $R = \mathbb{F}_p$, and suppose $E : y^2 = x^3 + Ax^2 + x / \mathbb{F}_p$ has smooth order. Then CDH is polynomial-time equivalent to DLP in $G$.

Are there always such $E$?
Unknown in general, but likely.
People have constructed some for many ‘common’ groups $G$.

$\implies$ For all practical purposes, DLP is equivalent to CDH.

...and they lived happily ever after??
Shor’s algorithm (1994)

Shor’s algorithm **breaks** all group-based DH instantiations.
Shor’s algorithm (1994)

...is a quantum algorithm for period finding.
Shor’s algorithm (1994)

...is a quantum algorithm for **period finding**.

Let $S$ be some finite set and

$$f: \mathbb{Z}^n \rightarrow S$$

a map with an **unknown period lattice** $\Lambda \subseteq \mathbb{Z}^n$, such that

$$f(\nu + \tau) = f(\nu)$$

if and only if $\tau \in \Lambda$. 
Shor’s algorithm (1994)

...is a quantum algorithm for **period finding**.

Let $S$ be some finite set and

$$f: \mathbb{Z}^n \longrightarrow S$$

a map with an **unknown period lattice** $\Lambda \subseteq \mathbb{Z}^n$, such that

$$f(v + \tau) = f(v)$$

if and only if $\tau \in \Lambda$.

Given such $f$ and some size constraints on $\Lambda$, Shor’s algorithm recovers a **basis of** $\Lambda$ in polynomial time.
Shor’s algorithm (1994)

...is a quantum algorithm for **period finding**.

**Application:**

For $G$ be a cyclic group and $(g, h = g^k)$ a DLP instance in $G$, the (publicly computable) function

$$f : \mathbb{Z}^2 \rightarrow G$$

$$(x, y) \mapsto g^x \cdot h^y$$

has period lattice $\Lambda = \langle (k, -1) \rangle \subseteq \mathbb{Z}^2$, which Shor can recover.
And now...
For something totally different.
Let $G$ be a group, $X$ a set. A **group action** of $G$ on $X$ is a map

$$\ast : G \times X \longrightarrow X$$

such that $\text{id} \ast x = x$ and $$(g \cdot h) \ast x = g \ast (h \ast x).$$
Diffie–Hellman from group actions (2006)

Let $G$ be a group, $X$ a set. A group action of $G$ on $X$ is a map

$$*: G \times X \longrightarrow X$$

such that $\text{id} * x = x$ and $(g \cdot h) * x = g * (h * x)$.

This suggests an evident Diffie–Hellman scheme:
Let $G$ be finite and commutative and fix $x \in X$.
- **Private keys:** group elements $a, b \in G$.
- **Public keys:** the elements $a * x, b * x \in X$.
- **Shared secret:** the element $a * (b * x) = b * (a * x)$.

This is not broken in general by Shor!

Example: CSIDH (2018) [joint w/ Castryck, Lange, Martindale, Renes]
Let $G$ be a group, $X$ a set. A group action of $G$ on $X$ is a map

$$*: G \times X \rightarrow X$$

such that $\text{id} * x = x$ and $(g \cdot h) * x = g * (h * x)$.

This suggests an evident Diffie–Hellman scheme:

Let $G$ be finite and commutative and fix $x \in X$.

- **Private keys**: group elements $a, b \in G$.
- **Public keys**: the elements $a * x, b * x \in X$.
- **Shared secret**: the element $a * (b * x) = b * (a * x)$.

This is not broken in general by Shor!
**Diffie–Hellman from group actions** (2006)

Let $G$ be a group, $X$ a set. A **group action** of $G$ on $X$ is a map

$$*: G \times X \to X$$

such that $\text{id} * x = x$ and $(g \cdot h) * x = g * (h * x)$.

This suggests an evident **Diffie–Hellman scheme**:

Let $G$ be finite and commutative and fix $x \in X$.

- **Private keys**: group elements $a, b \in G$.
- **Public keys**: the elements $a * x, b * x \in X$.
- **Shared secret**: the element $a * (b * x) = b * (a * x)$.

This is not broken in general by Shor!

**Example:** CSIDH [ˈsiːˌsaɪd] (2018) [joint w/ Castryck, Lange, Martindale, Renes]
The implicit group

Just like before, we get an implicit structure on the public keys.
The implicit group

Just like before, we get an *implicit structure* on the public keys. However, crucially, the ‘pairing’ \( g^x \cdot g^y = g^{x+y} \) is lost.

\( \Rightarrow \) We only get a **black-box group** rather than a ring or field.
The implicit group

Just like before, we get an implicit structure on the public keys. However, crucially, the ‘pairing’ $g^x \cdot g^y = g^{x+y}$ is lost.

$\implies$ We only get a **black-box group** rather than a ring or field.

Anyone can...

- **encode** elements $a$: compute $\lceil a \rceil = a \ast x$.
- **translate** by cleartext elements: $a \ast \lceil b \rceil = \lceil a \cdot b \rceil$. 
The implicit group

Just like before, we get an **implicit structure** on the public keys. However, crucially, the ‘pairing’ \( g^x \cdot g^y = g^{x+y} \) is lost.

\[ \Rightarrow \] We only get a **black-box group** rather than a ring or field.

Anyone can...

- **encode** elements \( a \): compute \( \lceil a \rceil = a \cdot x \).
- **translate** by cleartext elements: \( a \cdot \lceil b \rceil = \lceil a \cdot b \rceil \).

Anyone who can solve CDH can...

- **compose**: \( \lceil a \rceil \cdot \lceil b \rceil = shared\_secret(x, a \cdot x, b \cdot x) \).
The implicit group

Just like before, we get an implicit structure on the public keys. However, crucially, the ‘pairing’ \( g^x \cdot g^y = g^{x+y} \) is lost.

\[ \Rightarrow \] We only get a black-box group rather than a ring or field.

Anyone can...

- **encode** elements \( a \): compute \( \lceil a \rceil = a \cdot x \).
- **translate** by cleartext elements: \( a \cdot \lceil b \rceil = \lceil a \cdot b \rceil \).

Anyone who can solve CDH can...

- **compose**: \( \lceil a \rceil \cdot \lceil b \rceil = \text{shared} \text{-secret}(x, a \cdot x, b \cdot x) \).
- **exponentiate**: square-and-multiply using \( \pmod{\cdot} \).
The implicit group

Just like before, we get an implicit structure on the public keys. However, crucially, the ‘pairing’ \( g^x \cdot g^y = g^{x+y} \) is lost.

\[ \Rightarrow \] We only get a black-box group rather than a ring or field.

Anyone can...

- **encode** elements \( a \): compute \( \lceil a \rceil = a \ast x \).
- **translate** by cleartext elements: \( a \ast \lceil b \rceil = \lceil a \cdot b \rceil \).

Anyone who can solve CDH can...

- **compose**: \( \lceil a \rceil \cdot \lceil b \rceil = shared\_secret(x, a \ast x, b \ast x) \).
- **exponentiate**: square-and-multiply using \( \cdot \).
- **invert**: \( \lceil a^{-1} \rceil = \lceil a \rceil^{G-1} \) using \( \cdot \).
Our result (2018) [joint w/ Galbraith, Smith, Vercauteran]

**Theorem.** There is a polynomial-time quantum equivalence between the CDH and DLP problems for group actions.
Theorem. There is a polynomial-time quantum equivalence between the CDH and DLP problems for group actions.

Proof:

- Compute a set of generators \( g_1, \ldots, g_r \in G \).
- Apply Shor’s algorithm to the map

\[
f: \mathbb{Z}^r \times \mathbb{Z} \rightarrow X
\]

\[
(x_1, \ldots, x_r, y) \mapsto (g_1^{x_1} \cdots g_r^{x_r}) \ast \left\lfloor a \right\rfloor^y.
\]

- Any period vector of the form \((x_1, \ldots, x_r, 1)\) yields the desired element \(a = g_1^{-x_1} \cdots g_r^{-x_r}\).
An open question

- Can we get similar results if the CDH oracle $(x, a \cdot x, b \cdot x) \mapsto ab \cdot x$ is unreliable?

Classical case: Yes, by repeatedly blinding the inputs, unblinding the outputs, and using majority vote.

Here: Exponentially many queries in superposition; do we need all of them to be correct?
An open question

- Can we get similar results if the CDH oracle $(x, a \times x, b \times x) \mapsto ab \times x$ is unreliable?

Classical case: Yes, by repeatedly blinding the inputs, unblinding the outputs, and using majority vote.

Here: Exponentially many queries in superposition; do we need all of them to be correct?

Thank you!