Entropoids: Groups in Disguise

Lorenz Panny

Academia Sinica, Taipei, Taiwan

MathCrypt, online, 15 August 2021

poster presentation (no actual poster exists)

Summary

Summary

- Someone invented a new post-quantum cryptosystem.

Summary

- Someone invented a new post-quantum cryptosystem.
- It's broken.* ☺

Summary

- Someone invented a new post-quantum cryptosystem.
- It's broken.* ☺

* All proposed instantiations are dead, and the attack strategy is fairly generic (but no proof).

Entropic magmas

Entropoid-based cryptography [Gligoroski, ePrint 2021/469]:

Entropic magmas

Entropoid-based cryptography [Gligoroski, ePrint 2021/469]:

- Goal: Make Diffie–Hellman "work" with less structure.

Entropic magmas

Entropoid-based cryptography [Gligoroski, ePrint 2021/469]:

- Goal: Make Diffie–Hellman "work" with less structure.
- Suggestion: Use entropic magmas.

Entropic magmas

Entropoid-based cryptography [Gligoroski, ePrint 2021/469]:

- Goal: Make Diffie–Hellman "work" with less structure.
- Suggestion: Use entropic magmas.
  - A magma is a set G with a binary operation $*\colon G \times G \to G$.

Entropic magmas

Entropoid-based cryptography [Gligoroski, ePrint 2021/469]:

- Goal: Make Diffie–Hellman "work" with less structure.
- Suggestion: Use entropic magmas.
  - A magma is a set G with a binary operation $*\colon G \times G \to G$.
  - The entropic property is $(a * b) * (c * d) = (a * c) * (b * d)$.

Entropic magmas

Entropoid-based cryptography [Gligoroski, ePrint 2021/469]:

- Goal: Make Diffie–Hellman "work" with less structure.
- Suggestion: Use entropic magmas.
  - A magma is a set G with a binary operation $*\colon G \times G \to G$.
  - The entropic property is $(a * b) * (c * d) = (a * c) * (b * d)$.
  - $\Longrightarrow$ non-assocative exponentiation satisfies $(x^{\mathbf{A}})^{\mathbf{B}} = (x^{\mathbf{B}})^{\mathbf{A}}$.

Entropic magmas

Entropoid-based cryptography [Gligoroski, ePrint 2021/469]:

- Goal: Make Diffie–Hellman "work" with less structure.
- Suggestion: Use entropic magmas.
  - A magma is a set G with a binary operation $*\colon G \times G \to G$.
  - The entropic property is $(a * b) * (c * d) = (a * c) * (b * d)$.
  - $\Longrightarrow$ non-assocative exponentiation satisfies $(x^{\mathbf{A}})^{\mathbf{B}} = (x^{\mathbf{B}})^{\mathbf{A}}$.

Non-associative exponents are

$-$, $\square$, $\square\square$, $(\square\square)\square$, $\square(\square\square)$, $\square(\square(\square\square))$, $\square((\square\square)\square)$, $(\square\square)(\square\square)$, $((\square\square)\square)\square$, $(\square(\square\square))\square$, ...

and so on. You get the idea.

Structure theorem

Murdoch/Toyoda/Bruck (1939–1944):

Structure theorem

Murdoch/Toyoda/Bruck (1939–1944):

Theorem. For every entropic quasigroup $(G, *)$, there exists an abelian group $(G, \cdot)$, commuting automorphisms σ, τ of $(G, \cdot)$, and an element $c \in G$, such that

$$x * y = x^\sigma \cdot y^\tau \cdot c\,.$$

Structure theorem

Murdoch/Toyoda/Bruck (1939–1944):

Theorem. For every entropic quasigroup $(G, *)$, there exists an abelian group $(G, \cdot)$, commuting automorphisms σ, τ of $(G, \cdot)$, and an element $c \in G$, such that

$$x * y = x^{\sigma} \cdot y^{\tau} \cdot c\,.$$

$\Longrightarrow$ All non-associative powers of an element x are of the form

$$x^{\mathbf{A}} = x^{\xi} \cdot c^{\gamma}$$

with $\xi, \gamma \in \mathbb{Z}[\sigma, \tau]$.

Structure theorem

Murdoch/Toyoda/Bruck (1939–1944):

Theorem. For every entropic quasigroup $(G, *)$, there exists an abelian group $(G, \cdot)$, commuting automorphisms σ, τ of $(G, \cdot)$, and an element $c \in G$, such that

$$x * y = x^{\sigma} \cdot y^{\tau} \cdot c\,.$$

$\Longrightarrow$ All non-associative powers of an element x are of the form

$$x^{\mathbf{A}} = x^{\xi} \cdot c^{\gamma}$$

with $\xi, \gamma \in \mathbb{Z}[\sigma, \tau]$. Recovering ξ, γ reduces to DLP in $(G, \cdot)$.

Ambiguous equivalent keys

Previous slide: Recover $\xi, \gamma \in \mathbb{Z}[\sigma, \tau]$ such that $g^{\mathbf{A}} = g^{\xi} \cdot c^{\gamma}$.
Idea: (ξ, γ) is an *equivalent key* for $\mathbf{A}$.

Ambiguous equivalent keys

Previous slide: Recover $\xi, \gamma \in \mathbb{Z}[\sigma, \tau]$ such that $g^{\mathbf{A}} = g^{\xi} \cdot c^{\gamma}$.
Idea: (ξ, γ) is an *equivalent key* for $\mathbf{A}$.

However, (ξ, γ) are non-unique given just one pair $(g, g^{\mathbf{A}})$, and different solutions yield different $x \mapsto x^{\xi} \cdot c^{\gamma}$.

Ambiguous equivalent keys

Previous slide: Recover $\xi, \gamma \in \mathbb{Z}[\sigma, \tau]$ such that $g^{\mathbf{A}} = g^{\xi} \cdot c^{\gamma}$.
Idea: (ξ, γ) is an *equivalent key* for $\mathbf{A}$.

However, (ξ, γ) are non-unique given just one pair $(g, g^{\mathbf{A}})$, and different solutions yield different $x \mapsto x^{\xi} \cdot c^{\gamma}$.

Solution (me, 2021):

Lemma. The correct solution (ξ, γ) satisfies $\xi = 1 + (\sigma + \tau - 1) \cdot \gamma$. Any such (ξ, γ) computes $x \mapsto x^{\mathbf{A}}$ correctly for all x in $\langle g \rangle_*$.

$\Longrightarrow$ Have only one unknown γ instead of two (ξ, γ).

Finding the group

Given an algorithm for $*$, how to recover $\cdot$ and σ, τ, c?

Finding the group

Given an algorithm for $*$, how to recover $\cdot$ and σ, τ, c?

Generally: Unclear.

Finding the group

Given an algorithm for $*$, how to recover $\cdot$ and σ, τ, c?

Generally: Unclear.

Less generally: If one-sided divisions are efficient, can construct $\cdot$ and σ, τ, c from that. (Mimic proof of structure theorem.)

Finding the group

Given an algorithm for $*$, how to recover $\cdot$ and σ, τ, c?

Generally: Unclear.

Less generally: If one-sided divisions are efficient, can construct $\cdot$ and σ, τ, c from that. (Mimic proof of structure theorem.)

In ePrint 2021/469: Everything is algebraic, and with a little work we find an isomorphism $(G, \cdot) \cong (\mathbb{F}_p^\times)^2$.

Is it kapot?

Attack cost for 128-bit post-quantum secure parameters:

Is it kapot?

Attack cost for 128-bit post-quantum secure parameters:

< 10 minutes on a laptop.

Thanks!

https://ia.cr/2021/583