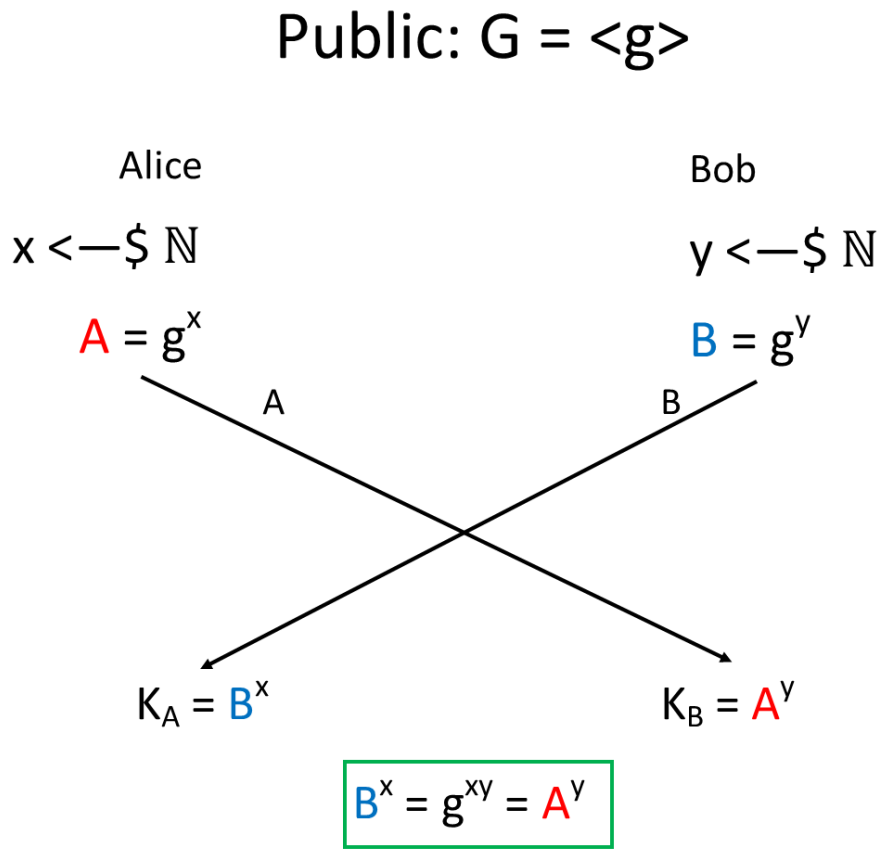
Semidirect Product Key Exchange - the State of Play

Christopher Battarbee
University of York

Delaram Kahrobaei
CUNY

Siamak F. Shahandashti
University of York

Diffie-Hellman Key Exchange[1]



[1] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

DHKE Security

- **Assumption:** it is computationally difficult to recover the integer a from g, g^x (DLP)
- **Assumption:** it is computationally difficult to recover g^{xy} from g, g^x, g^y (CDH)

Oh no!

Consider set $G \times End(G)$ with multiplication

$$(g, \phi)(g', \psi) = (\psi(g)g', \rho \circ \psi)$$

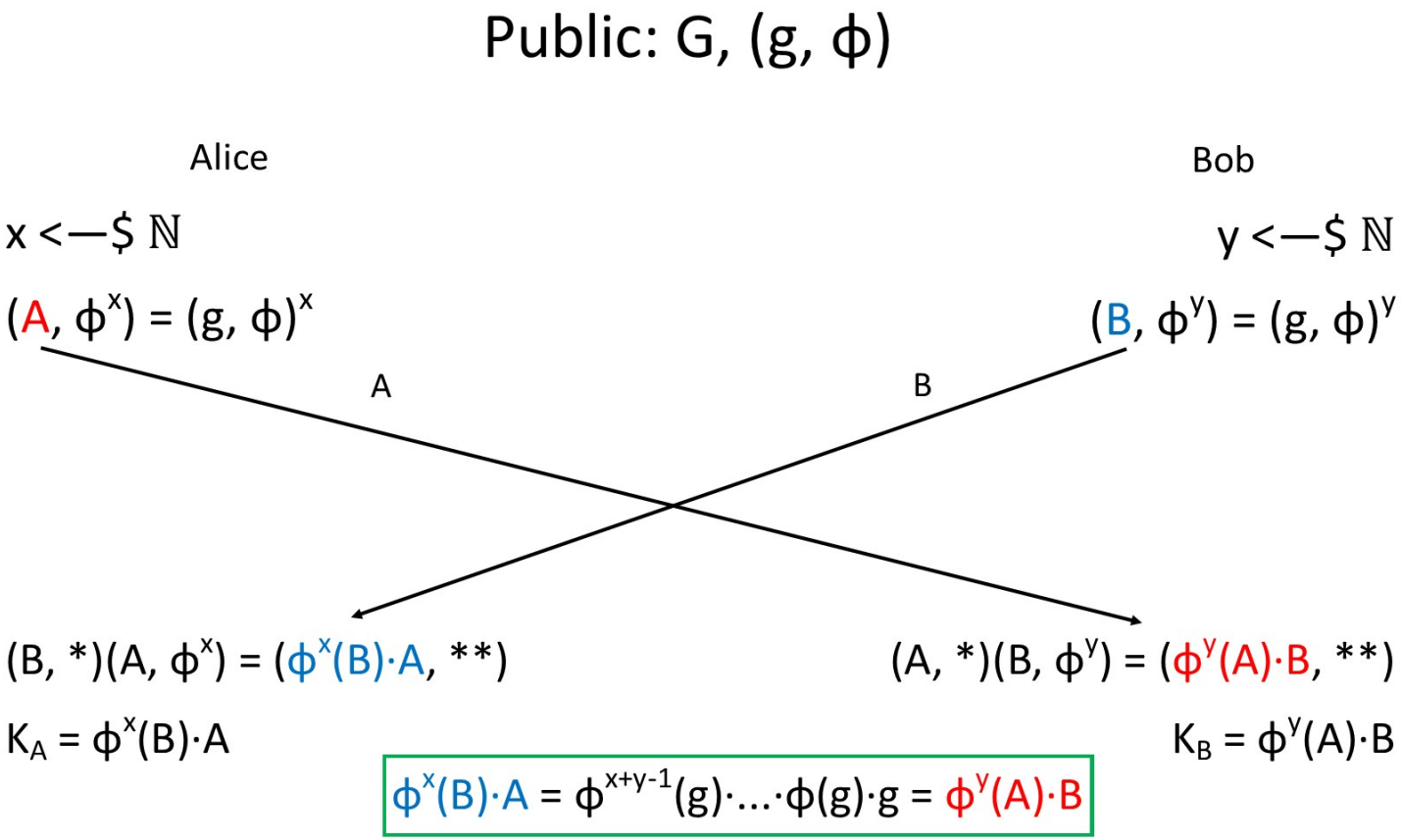
Note:

$$\begin{aligned}(g, \phi)^2 &= (\phi(g)g, \phi^2) \\ (g, \phi)^3 &= (\phi^2(g)\phi(g)g) \\ &\dots \\ (g, \phi)^n &= (\phi^{n-1}(g)...\phi(g)g, \phi^n)\end{aligned}$$

- **Assumption:** it is computationally difficult to recover integer x from $\phi^{x-1}(g)...\phi(g)g$
- **Useful Property:**

$$\begin{aligned}\phi^{x+y-1}(g) &= \phi^{x}\left(\phi^{y-1}(g)...g\right)\phi^{x-1}(g)...g \\ &= \phi^{y}\left(\phi^{x-1}(g)...g\right)\phi^{y-1}(g)...g\end{aligned}$$

Semidirect Product Key Exchange (SDPKE)[2]



[2] Habeeb, Kahrobaei, Koupparis, and Shpilrain. "Public key exchange using semidirect product of (semi) groups". In: *ACNS*. Springer.

Proposed Platforms

Consider $n \times n$ matrices in $M_n(R)$ with R a (semi)ring. We can

- **Scale:** component-wise with multiplication in R
- **Add:** component-wise with addition in R
- **Multiply:** in the usual manner with arithmetic in R

- Dima Grigoriev and Vladimir Shpilrain. "Tropical cryptography II: extensions by homomorphisms". In: *Communications in Algebra* 47.10 (2019), pp. 4224–4229
- Steve Isaac and Delaram Kahrobaei. "A closer look at the tropical cryptography". In: *International Journal of Computer Mathematics: Computer Systems Theory* (2021), pp. 1–6
- Dylan Rudy and Chris Monico. "Remarks on a tropical key exchange system". In: *Journal of Mathematical Cryptology* 15.1 (2021), pp. 280–283

R a ring, G a group, then

$$R[G] = \left\{ \sum_{g \in G} a_g.g : a_g \in R, g \in G \right\}$$

Arithmetic defined by

$$\sum_{g \in G} a_g.g + \sum_{g \in G} b_g.g = \sum_{g \in G} (a_g + b_g).g$$

$$\left(\sum_{g \in G} a_g.g \right) \left(\sum_{h \in G} b_h.h \right) = \sum_{g,h \in G} (a_g b_h).(gh)$$

Choose parameters $G = A_5$, $R = \mathbb{Z}_7$ to get matrix algebra $M_3(\mathbb{Z}_7[A_5])$.

Pick $H \in M_3(\mathbb{Z}_7[A_5])$ invertible:

$$\phi_H(M) = H^{-1}MH$$

- Closed form of product:

$$\phi_H^{x-1}(M)...\phi_H(M)M = H^{-x}(HM)^x$$

- Experimental evidence of computational indistinguishability from random values

[3] Habeeb, Kahrobaei, Koupparis, and Shpilrain. "Public key exchange using semidirect product of (semi) groups". In: *ACNS*. Springer.

Cryptanalysis[4][5]

- Exchange values can be given as a linear decomposition which allows key recovery
- Possible since the platform embeds as multiplicative semigroup of an algebra and ϕ preserves addition
- Attack is polynomial in the dimension of such an algebra

[4] Vitaliĭ Roman'kov. "Linear decomposition attack on public key exchange protocols using semidirect products of (semi) groups". In: *arXiv preprint arXiv:1501.01152* (2015).

[5] Alexei Myasnikov and Vitaliĭ Roman'kov. "A linear decomposition attack". In: *Groups Complexity Cryptology* 7.1 (2015), pp. 81–94.

Free Nilpotent p-Groups[6],[7]

- F_r free group on r generators
- F_r^p generated by all elements g^p
- $\gamma_c(F_r)$ generated by all elements $[g_1, ..., g_c]$

Propose platform $F_r/(F_r^{p^2}.\gamma_{c+1}(F_r))$ with conjugation endomorphism to enforce p-group with element order p^2 (security) and low nilpotency class (efficiency).

Janusz: such a p-group has minimum dimension of representation $1 + p$

Parameters: $p \sim 2^{100}, c = 2$ or 3.

[6] Delaram Kahrobaei and Vladimir Shpilrain. "Using semidirect product of (semi) groups in public key cryptography". In: *CiE*. Springer LNCS.

[7] GJ Janusz. "Faithful Representations of p-Groups at Characteristic p". In: *Representation Theory of Finite Groups and Related Topics* 21 (1971), p. 89.

Matrix Action Key Exchange (MAKE)[8]

$(M_n(\mathbb{Z}_p), +)$ with endomorphism $\phi_{H_1,H_2}(M) = H_1 M H_2$

- Good diffusion from mixing operations
- Formal reduction proof that related security problem is at least as hard as DLP
- Reasonably efficient

[8] Nael Rahman and Vladimir Shpilrain. "MAKE: A Matrix Action Key Exchange". In: *Journal of Mathematical Cryptology* 16.1 (2022), pp. 64–72.

Note that $(M, \phi_{H_1,H_2})^2 = (H_1MH_2 + M, \phi^2_{H_1,H_2})$ so exchange values look like

$$A = \sum_{i=0}^{x-1} H_1^i M H_2^i \quad B = \sum_{i=0}^{y-1} H_1^i M H_2^i$$

Note that $(M, \phi_{H_1,H_2})^2 = (H_1MH_2 + M, \phi^2_{H_1,H_2})$ so exchange values look like

$$A = \sum_{i=0}^{x-1} H_1^i M H_2^i \quad B = \sum_{i=0}^{y-1} H_1^i M H_2^i$$

We have

$$\sum_{i=1}^{x} H_1^i M H_2^i + M = H_1^x M H_2^x + \sum_{i=0}^{n-1} H_1^i M H_2^i$$

so

$$\phi_{H_1,H_2}(A) + M = \phi^x_{H_1,H_2}(M) + A$$

[9] Daniel RL Brown, Neal Koblitz, and Jason T LeGrow. "Cryptanalysis of "MAKE"". In: *Journal of Mathematical Cryptology* 16.1 (2022), pp. 98–102.

Clearly the value $\phi^x_{H_1,H_2}(M)$ encodes some information about private exponent x in a different way than novel exponentiation

In fact (not true in general) by exploiting linearity we can recover $\phi^x_{H_1,H_2}(B)$ which suffices for key recovery.

Theorem (Cayley-Hamilton)

Every $n \times n$ square matrix M over a commutative ring is such that $\lambda = M$ is admissible in the equation

$$det(\lambda I - M) = 0$$

Corollary

There are ring coefficients $r_0, ..., r_{n-1}$ such that

$$A^x = \sum_{i=0}^{n-1} r_i M^i$$

for any $x \in \mathbb{Z}$.

Linearity approach possible by Cayley-Hamilton theorem which only applies when underlying ring is commutative.

Lemma (Our contribution)

Suppose there is an injective ring homomorphism $\phi : R \to M_m(S)$ *for some* $m \in \mathbb{N}$ *and a commutative ring* S*. For any* $n \in \mathbb{N}$ *define*

$$\begin{aligned} \psi : & M_n(R) \to M_{mn}(S) \\ & (\psi(A))_{im+g,jm+h} = (\phi(A_{i,j}))_{g,h} \end{aligned}$$

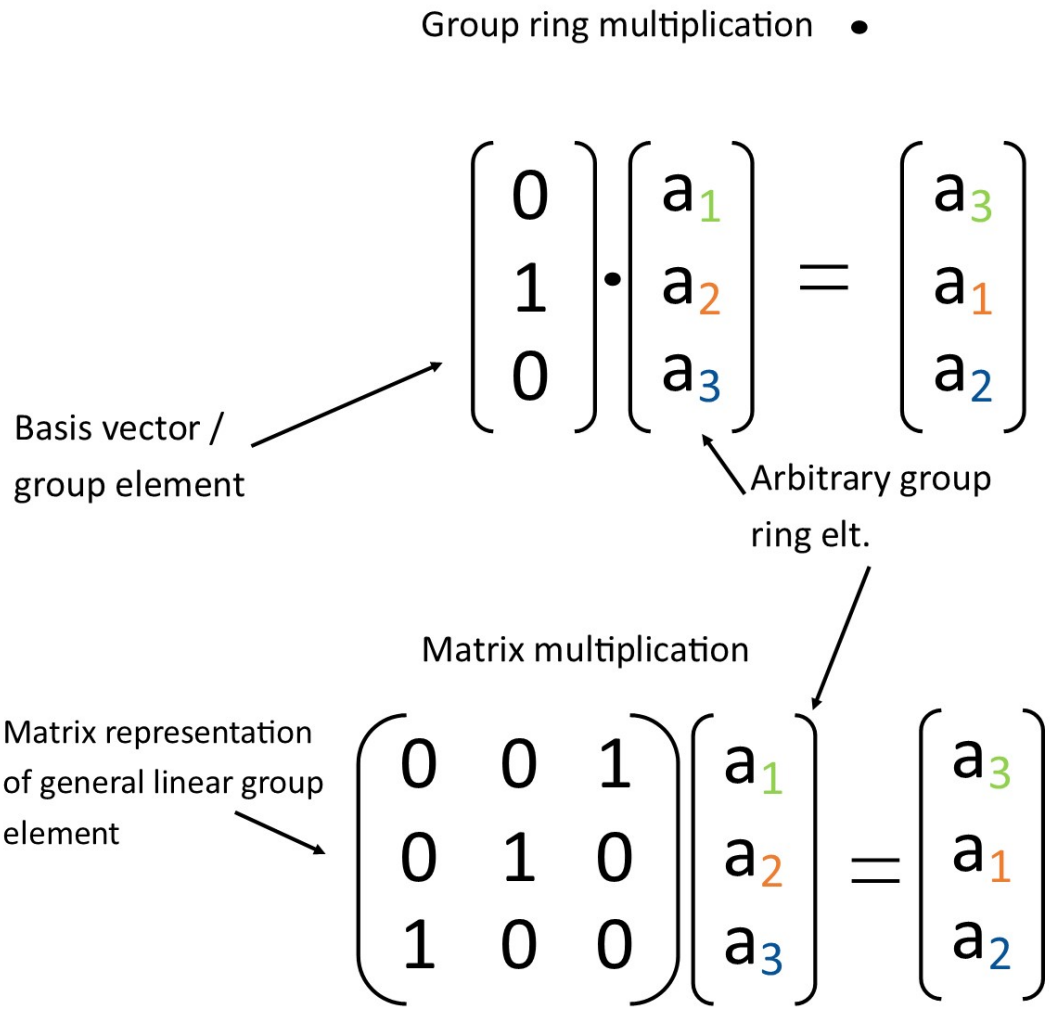
where $0 \leq i, j \leq n-1$, $0 \leq g, h \leq m-1$*. Then* ψ *is an injective ring homomorphism.*

[10] Battarbee, Kahrobaei, and Shahandashti. "Cryptanalysis of Semidirect Product Key Exchange Using Matrices Over Non-Commutative Rings". In: *Mathematical Cryptology* (2022).

Lemma (Our contribution)

Let $\mathbb{F}$ a finite field , G a finite non-abelian group of order m. The group ring $\mathbb{F}[G]$ admits an injective ring homomorphism into $M_m(\mathbb{F})$.

Example: Group Rings



$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} a_3 \\ a_1 \\ a_2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} a_3 \\ a_1 \\ a_2 \end{pmatrix}$$

Matrices Over Bitstrings (MOBS)[11]

Consider the semiring $\{0, 1\}$ with Boolean operations:

- *Addition:* $a \vee b = max\{a, b\}$
- *Multiplication:* $a \wedge b = min\{a, b\}$

Extend these operations component wise on bitstrings; e.g.

$$0110 \vee 1100 = 1110 \quad 0110 \wedge 1100 = 0100$$

Matrices over k-bit ring, denoted B_n^k; endomorphism constructed by applying high-order permutation to each bitstring entry. Call the endomorphism h.

[11] Nael Rahman and Vladimir Shpilrain. "MOBS: Matrices Over Bit Strings public key exchange". In: *https://eprint.iacr.org/2021/560* (2021).

This time

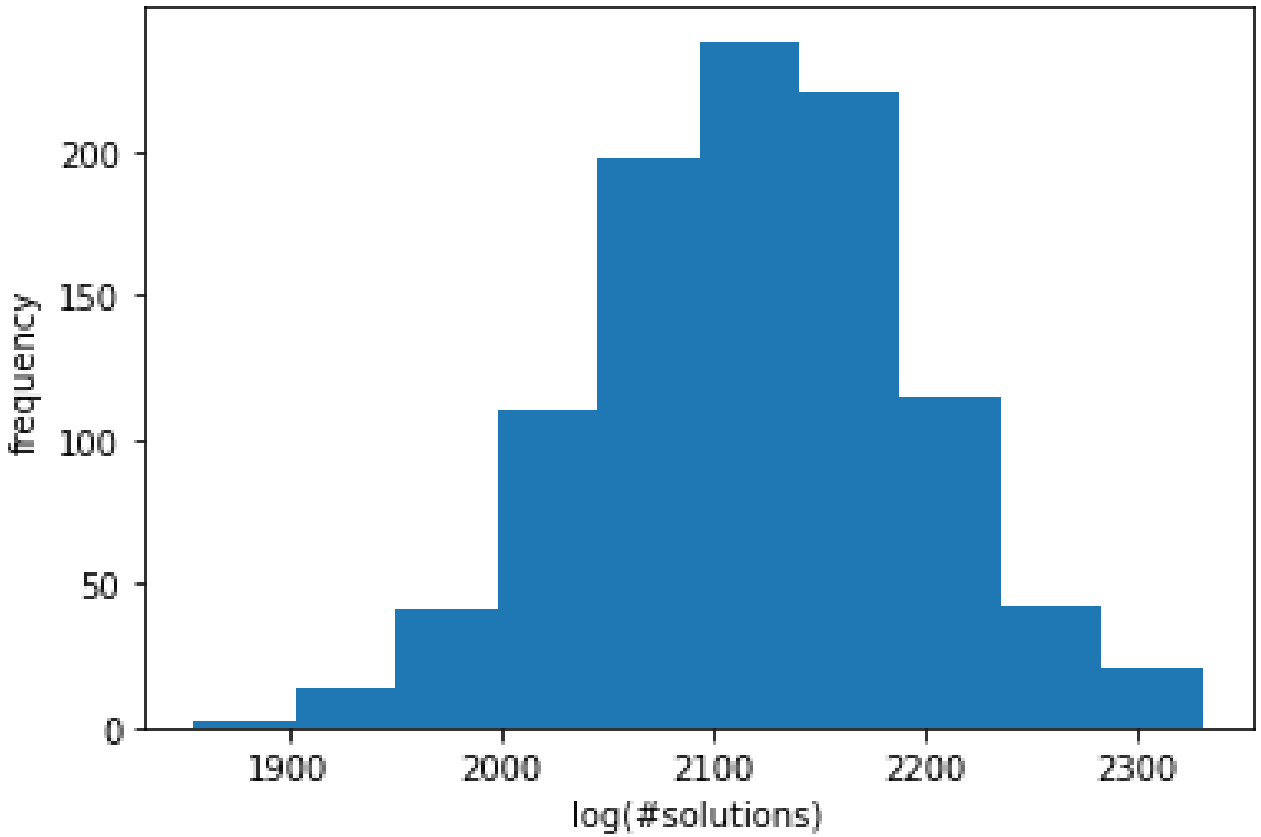
$$h(A)M = h^x(M)\,A$$

If we know $h^x(M)$ we can recover permutation h^x by inspection.

- **Question:** how many Boolean matrices Y are admissible in the equation

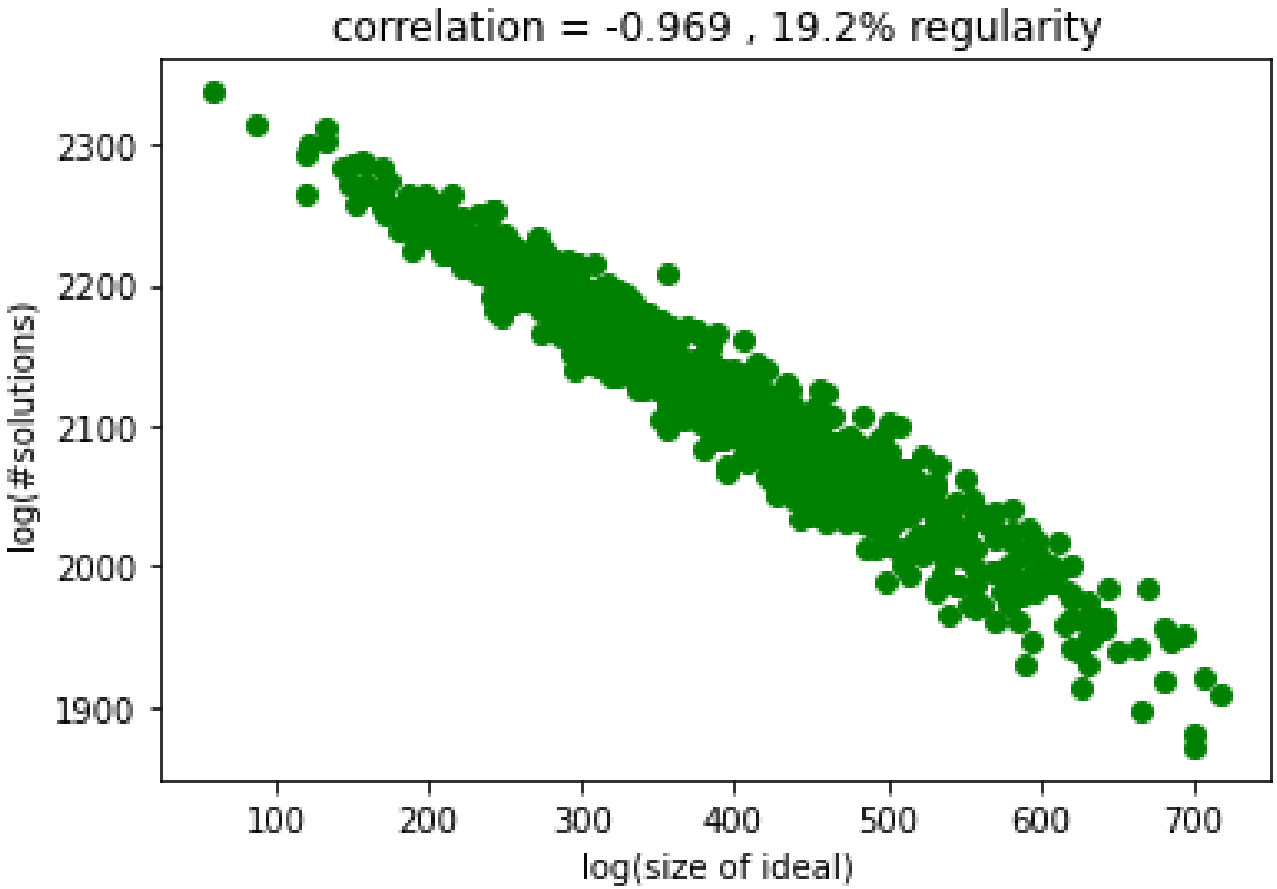
$$h(A)M = YA\ ?$$

- **Answer:** astronomically many!



[12] Battarbee, Kahrobaei, Tailor, and Shahandashti. "On the efficiency of a general attack against the MOBS cryptosystem". In: *to appear in Journal of Mathematical Cryptology* (2021).

Size of ideal generated by $A = \#\{MA : M \in B_n^k\}$



Can achieve key recovery provided:

- Platform embeds as multiplicative subgroup of algebra over a field
- Endomorphism ϕ extends to linear function on this algebra

Can achieve key recovery provided:

- Feasible to recover $\phi^x(M)$ from the equation

$$\phi(A)M = \phi^x(M)A$$

- Information about the secret key can be efficiently deduced from $\phi^x(M)$

Summary

Platform	Dimension Attack		Telescoping Attack	
	Embeds in algebra	Linear endomorphism	Recovery of value	Key Recovery
Group Rings	✓	✓	✗	✗
p-Groups	✓	✓	✓	✗
MAKE	✗	✓	✓	✓
MOBS	✓	✗	✗	✓

Thank you.

Secret Backup Slide

Let $a_0 = M$, $a_i = H^{-i}(HM)^i$. We achieve key recovery as follows:

- By a general result the set $\{a_0, a_1, ..., a_l, ...\}$ has a basis $\{a_0, ..., a_k\}$
- We use this basis to get group ring coefficients η_i such that

$$a_x = \sum_{i=0}^{k} \eta_i a_i$$

- We have

$$K = \phi^y(a_x)a_y = \phi^y\left(\sum_{i=0}^{k} \eta_i a_i\right) a_y$$
$$= \sum_{i=0} \eta_i \phi^y(a_i)a_y = \sum_{i=0} \eta_i \phi^i(a_y)a_i$$

Secret Backup Slide 2

Suppose we have functions f, g such that

1. Equation $f(Y)s = g(H_1^x Y H_2^x)$ has constant solution vector s for all $Y \in M_n(\mathbb{Z}_p)$
2. $f(A+B) = f(A) + f(B)$
3. $f(Y)u = 0 \Rightarrow f(H_1^i Y H_2^i)u = 0$

Solve $f(M)v = g(H_1^x M H_2^x)$ to get vector t. In fact t satisfies $f(B)t = g(H_1^x B H_2^x)$ since:

- $f(M)u = f(M)(t - s) = 0$
- Therefore $f(H_1^i M H_2^i)u = 0$ for all $i \in \mathbb{N}$ by property 3
- We have

$$0 = \sum_{i=0}^{y-1} f(H_1^i M H_2^i)u = f\left(\sum_{i=0}^{y-1} H_1^i M H_2^i\right) u = f(B)u$$

  by property 2
- Therefore $f(B)t = f(B)s = g(H_1^x B H_2^x)$ by property 1.