Multilinear Cryptography using Nilpotent Groups

Maria Tota
(joint work with D. Kahrobaei and A. Tortora)

Università degli Studi di Salerno
Dipartimento di Matematica

"SandGAL 2019" - Cremona, June 2019

Let n be a positive integer and G and G_T arbitrary groups. A map

$$e : G^n \to G_T$$

is said to be a (symmetric) *n-linear map* (or a multilinear map) if for any $a_1, \ldots, a_n \in \mathbb{Z}$ and $g_1, \ldots, g_n \in G$, we have

$$e(g_1^{a_1}, \ldots, g_n^{a_n}) = e(g_1, \ldots, g_n)^{a_1 \cdots a_n}.$$

Notice that the map e is not necessarily linear in each component.

In addition, we say that e is *non-degenerate* if there exists $g \in G$ such that $e(g, \ldots, g) \neq 1$.

Let n be a positive integer and G and G_T cyclic groups of prime order. A map

$$e : G^n \to G_T$$

is said to be a (symmetric) *n-linear map* (or a multilinear map) if for any $a_1, \ldots, a_n \in \mathbb{Z}$ and $g_1, \ldots, g_n \in G$, we have

$$e(g_1^{a_1}, \ldots, g_n^{a_n}) = e(g_1, \ldots, g_n)^{a_1 \ldots a_n}$$

and further e is non-degenerate in the sense that $e(g, \ldots, g)$ is a generator of G_T for any generator g of G.

D. Boneh and A. Silverberg, *Applications of Multilinear Forms to Cryptography, Contemporary Mathematics* **324**, American Mathematical Society, (2003) 71–90.

From Diffie - Hellman to multilinear maps...

Let n be a positive integer and G and G_T cyclic groups of prime order. A map

$$e : G^n \to G_T$$

is said to be a (symmetric) *n-linear map* (or a multilinear map) if for any $a_1, \dots, a_n \in \mathbb{Z}$ and $g_1, \dots, g_n \in G$, we have

$$e(g_1^{a_1}, \dots, g_n^{a_n}) = e(g_1, \dots, g_n)^{a_1 \dots a_n}$$

and further e is non-degenerate in the sense that $e(g, \dots, g)$ is a generator of G_T for any generator g of G.

D. Boneh and A. Silverberg, *Applications of Multilinear Forms to Cryptography, Contemporary Mathematics* **324**, American Mathematical Society, (2003) 71–90.

Motivation

Motivation

A. Mahalanobis and P. Shinde, *Bilinear Cryptography Using Groups of Nilpotency Class* 2, Cryptography and Coding, 16th IMA Int. Conf., IMACC 2017, Oxford, UK (2017), 127–134.

Motivation

A. Mahalanobis and P. Shinde, *Bilinear Cryptography Using Groups of Nilpotency Class* 2, Cryptography and Coding, 16th IMA Int. Conf., IMACC 2017, Oxford, UK (2017), 127–134.

Idea

Find an n-linear map starting from a nilpotent group of class n.

The definition

A group G is said to be *nilpotent* if it has a finite series

$$\{1\} = G_0 < G_1 < \cdots < G_n = G$$

which is central, that is, each G_i is normal in G and G_{i+1}/G_i is contained in the center of G/G_i.

The length of a shortest central series is the *(nilpotency) class* of G.

The definition

A group G is said to be *nilpotent* if it has a finite series

$$\{1\} = G_0 < G_1 < \cdots < G_n = G$$

which is central, that is, each G_i is normal in G and G_{i+1}/G_i is contained in the center of G/G_i.

The length of a shortest central series is the *(nilpotency) class* of G.

Examples

The definition

A group G is said to be *nilpotent* if it has a finite series

$$\{1\} = G_0 < G_1 < \cdots < G_n = G$$

which is central, that is, each G_i is normal in G and G_{i+1}/G_i is contained in the center of G/G_i.

The length of a shortest central series is the *(nilpotency) class* of G.

Examples

Abelian groups

The definition

A group G is said to be *nilpotent* if it has a finite series

$$\{1\} = G_0 < G_1 < \cdots < G_n = G$$

which is central, that is, each G_i is normal in G and G_{i+1}/G_i is contained in the center of G/G_i.

The length of a shortest central series is the *(nilpotency) class* of G.

Examples

Abelian groups
Finite p-groups

Let $g_1, \ldots, g_n$ be elements of a group G. We will use the following commutator notation:

$$[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2.$$

More generally, a simple commutator of weight $n \geq 2$ is defined recursively by the rule

$$[g_1, \ldots, g_n] = [[g_1, \ldots, g_{n-1}], g_n],$$

where by convention $[g_1] = g_1$.

A useful shorthand notation is

$$[x,_n g] = [x, \underbrace{g, \ldots, g}_{n}].$$

A group G is abelian if and only if the identity $[g_1, g_2] = 1$ is satisfied in G.

A group G is abelian if and only if the identity $[g_1, g_2] = 1$ is satisfied in G.

A characterization

A group G is nilpotent of class at most $n \geq 1$ if and only if the identity $[g_1, \ldots, g_{n+1}] = 1$ is satisfied in G.

A generalization

A group G is called *n-Engel* if $[x,_n y] = 1$ for all $x, y \in G$.

If G is nilpotent of class n, then G is n-Engel.

BUT: Liebeck

There are nilpotent groups of class n which are not $(n-1)$-Engel: Given a prime p, the wreath product $G = \mathbb{Z}_p \wr \mathbb{Z}_p$ is nilpotent of class p but not $(p-1)$-Engel.

Let G be a nilpotent group of class $n > 1$ and $g_1, \ldots, g_n \in G$. Then, for any $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$, we have

$$[g_1^{a_1}, \ldots, g_n^{a_n}] = [g_1, \ldots, g_n]^{\prod_{i=1}^{n} a_i}.$$

Hence, $e : G^n \to G$ given by

$$e(g_1, \ldots, g_n) = [g_1, \ldots, g_n]$$

is a multilinear map.

Let G be a nilpotent group of class $n > 1$ and $g_1, \ldots, g_n \in G$. Then, for any $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$, we have

$$[g_1^{a_1}, \ldots, g_n^{a_n}] = [g_1, \ldots, g_n]^{\prod_{i=1}^n a_i}.$$

Hence, $e : G^n \to G$ given by

$$e(g_1, \ldots, g_n) = [g_1, \ldots, g_n]$$

is a multilinear map.

Similarly, given $x \in G$, we can consider the multilinear map $e' : G^{(n-1)} \to G$ given by

$$e'(g_1, \ldots, g_{n-1}) = [x, g_1, \ldots, g_{n-1}].$$

Moreover, if G is not $(n-1)-$Engel, one can take $x \in G$ such that e' is non-degenerate.
In fact there exists $g \in G$ such that $[x,_{n-1} g] \neq 1$.

Protocol I (Kahrobaei, Tortora, T.)

Let G be a public nilpotent group of class $n > 1$ and let $g_1, \ldots, g_n$ elements of G. Let $\mathcal{A}_1, \ldots, \mathcal{A}_{n+1}$ be $n+1$ users with private exponents $a_1, \ldots, a_{n+1}$, respectively.

The user $\mathcal{A}_1$ transmits in public channel ${g_1}^{a_1}$.
The users $\mathcal{A}_j$ $(j = 2, \ldots, n)$ transmit ${g_i}^{a_j}$, for $j-1 \leq i \leq j$.
The user $\mathcal{A}_{n+1}$ transmits in public channel ${g_n}^{a_{n+1}}$.

The key exchange works as follows:

- The user $\mathcal{A}_1$ can compute $[{g_1}^{a_2}, \ldots, {g_n}^{a_{n+1}}]^{a_1}$.
- The user $\mathcal{A}_j$ $(j = 2, \ldots, n)$ can compute

$$[{g_1}^{a_1}, \ldots, {g_{j-1}}^{a_{j-1}}, {g_j}^{a_{j+1}}, {g_{j+1}}^{a_{j+2}}, \ldots, {g_n}^{a_{n+1}}]^{a_j}.$$

- The user $\mathcal{A}_{n+1}$ can compute $[{g_1}^{a_1}, \ldots, {g_n}^{a_n}]^{a_{n+1}}$.

The common key is $[g_1, \ldots, g_n]^{\prod_{j=1}^{n+1} a_j}$.

Protocol II (Kahrobaei, Tortora, T.)

Let G be a public nilpotent group of class $n+1$ which is not n-Engel ($n \geq 1$). Then there exist $x, g \in G$ such that $[x,_n g] \neq 1$.

Suppose that $n+1$ users $\mathcal{A}_1, \ldots, \mathcal{A}_{n+1}$ want to agree on a shared secret key.

Each user $\mathcal{A}_j$ selects a private non-zero integer a_j, computes g^{a_j} and sends it to the other users. Then:

- The user $\mathcal{A}_1$ computes $[x^{a_1}, g^{a_2}, \ldots, g^{a_{n+1}}]$.
- The user $\mathcal{A}_j$ ($j = 2, \ldots, n$), computes $[x^{a_j}, g^{a_1}, \ldots, g^{a_{j-1}}, g^{a_{j+1}}, \ldots, g^{a_{n+1}}]$.
- The user $\mathcal{A}_{n+1}$ computes $[x^{a_{n+1}}, g^{a_1}, \ldots, g^{a_n}]$.

Each user obtains $[x,_n g]^{\prod_{j=1}^{n+1} a_j}$ which is the shared key.

Security and Platform Group

Shamir: "Absolutely secure systems do not exist."

We have to wonder whether or not our systems are secure enough.

Security and Platform Group

Shamir: "Absolutely secure systems do not exist."

We have to wonder whether or not our systems are secure enough.

The key exchange is broken if one can find a_i from g^{a_i}. This is the discrete logarithm problem (DLP).
The security of our protocols is based on the DLP.

Security and Platform Group

Shamir: "Absolutely secure systems do not exist."

We have to wonder whether or not our systems are secure enough.

The key exchange is broken if one can find a_i from g^{a_i}. This is the discrete logarithm problem (DLP).
The security of our protocols is based on the DLP.

The ideal platform group for our protocols must be a non-abelian nilpotent group of large order such that the nilpotency class is not too large and the DLP in such a group is hard.

A. Mahalanobis, *The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups*, Israel J. Math. 165 (2008), 161–187.

A. Mahalanobis and P. Shinde, *Bilinear Cryptography Using Groups of Nilpotency Class* 2, Cryptography and Coding, 16th IMA International Conference, IMACC 2017, Oxford, UK (2017), 127–134.

A. Mahalanobis, *The MOR cryptosystem and finite p-groups*, Algorithmic problems of group theory, their complexity, and applications to cryptography, 81–95, Contemp. Math. **633**, Amer. Math. Soc., Providence, RI, 2015.

A. Mahalanobis, *The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups*, Israel J. Math. 165 (2008), 161–187.

A. Mahalanobis and P. Shinde, *Bilinear Cryptography Using Groups of Nilpotency Class* 2, Cryptography and Coding, 16th IMA International Conference, IMACC 2017, Oxford, UK (2017), 127–134.

A. Mahalanobis, *The MOR cryptosystem and finite p-groups*, Algorithmic problems of group theory, their complexity, and applications to cryptography, 81–95, Contemp. Math. **633**, Amer. Math. Soc., Providence, RI, 2015.

Any contribution in this direction is welcome!

THANK YOU!

D. Kahrobaei, A. Tortora and M. Tota,
Multilinear Cryptography using nilpotent groups, submitted.