A New Approach on Bilinear Pairings and Its Applications

Tatsuaki Okamoto

Who Used Bilinear Pairings in Cryptography for the First Time?

Are Alfred Menezes, O. and Scott Vanstone such persons by their attack to ECC in 1990?

No, it is not true!

Unsung Hero in Pairing-Based Cryptography

Burt Kaliski

In his PhD thesis in 1988, he did a pioneer work on bilinear pairings for a cryptographic application.

Elliptic Curves and Cryptography:
A Pseudorandom Bit Generator and Other Tools

by

Burton S. Kaliski, Jr.

S.B., Computer Science and Engineering, June 1984
Massachusetts Institute of Technology

S.M., Electrical Engineering and Computer Science, February 1987
Massachusetts Institute of Technology

SUBMITTED TO THE DEPARTMENT OF
ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE
DEGREE OF

DOCTOR OF PHILOSOPHY
IN COMPUTER SCIENCE

at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
February 1988

Signature of Author Burton S. Kaliski, Jr.
Department of Electrical Engineering and Computer Science
January 1, 1988

Certified by Ronald L. Rivest
Ronald Linn Rivest
Thesis Supervisor

Accepted by

Contents

- A general construction of pseudo-random generators over general Abelian groups.
- A typical example: construction on general elliptic curves.
- It is necessary to determine the group structure of the underlying curve.

⇒ Weil pairing is employed.

6 A new pseudorandom bit generator **129**
6.1 Embedding messages on elliptic curves 130
6.1.1 Simple class 131
6.1.2 General class 132
6.2 Finding generating pairs for elliptic curves 134
6.2.1 Weil pairing and equivalence classes 135
6.2.2 Group structure and testing generating pairs 137
6.3 Definition of the generators 138
6.3.1 Simple class 139
6.3.2 General class 141

7 Conclusion **145**

A Implementation of Weil pairing **147**
A.1 Definition of the Weil pairing 147
A.2 Implementation 149

Bibliography **167**

6.2.1 Weil pairing and equivalence classes

The Weil pairing, defined simply as a "correspondence" by Weil [Wei40], takes an integer m as parameter and is a rational function on pairs of points of order dividing m in the group $E(\overline{\mathbf{F}_q})$:

$$e_m\colon E(\overline{\mathbf{F}_q})[m] \times E(\overline{\mathbf{F}_q})[m] \to \overline{\mathbf{F}_q}. \qquad (6.11)$$

The pairing has several useful properties:

(i) *Identity.* For all points $P \in E(\overline{\mathbf{F}_q})[m]$, $e_m(P,P) = 1$.

(ii) *Alternation.* For all points $P_1, P_2 \in E(\overline{\mathbf{F}_q})[m]$, $e_m(P_1,P_2) = e_m(P_2,P_1)^{-1}$.

(iii) *Bilinearity.* For all points $P_1, P_2, P_3 \in E(\overline{\mathbf{F}_q})[m]$, $e_m(P_1+P_2,P_3) = e_m(P_1,P_3)e_m(P_2,P_3)$ and $e_m(P_1,P_2+P_3) = e_m(P_1,P_2)e_m(P_1,P_3)$.

(iv) *Nondegeneracy.* For all points $P_1 \in E(\overline{\mathbf{F}_q})[m]$, if $e_m(P_1,P_2) = 1$ for all points $P_2 \in E(\overline{\mathbf{F}_q})[m]$ then $P_1 = O$.

Miller recently developed a probabilistic polynomial time algorithm for computing the Weil pairing [Mil85]. The algorithm is essential to the results which follow in this section. Indeed most of the results have been suggested in some form by Miller [Mil87], although the use of partial factorization is new. The definition of the Weil pairing and a MACSYMA implementation of Miller's algorithm are included in Appendix A.

Equivalence classes

The properties of the Weil pairing provide a method of partitioning elements into equivalence classes. The partitioning can be done for points of order dividing m on the elliptic curve over the algebraic closure, or for points on the elliptic curve over the finite field. The following lemma shows how this is done.

Lemma 6.7 *Let $E(\mathbf{F}_q)$ be an elliptic curve with group structure (n_1, n_2) and let G_1 be an element of maximum order. Let h denote a homomorphism modulo the subgroup generated by G_1.*

[Mil85] V. Miller. Short programs for functions on curves. 1985. Unpublished manuscript.

[Mil86] V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology: Proceedings of Crypto'85*, pages 417–426, 1986.

[Mil87] V. Miller. 1987. Personal communication.

[Nam84] M. Namba. *Geometry of Projective Algebraic Curves*. Volume 88 of *Pure and Applied Mathematics*, Marcel Dekker Inc., 1984.

[Odl85] A. Odlyzko. Discrete logarithms and their cryptographic significance. In *Advances in Cryptology: Proceedings of Eurocrypt'84*, pages 224–314, 1985.

[Plu82] J. Plumstead. Inferring a sequence generated by a linear congruence. In *Proceedings of the Twenty-third Annual Symposium on Foundations of Computer Science*, pages 153–159, 1982.

[Pol74] J. Pollard. Theorems on factorization and primality testing. *Proc. Cambridge Philos. Soc.*, 76:521–528, 1974.

[Pom85a] C. Pomerance. Analysis and comparison of some integer factorization algorithms. In *Computational Methods in Number Theory*, Mathematisch Centrum, 1985.

[Pom85b] C. Pomerance. How to factor a number. Seminar, MIT Laboratory for Computer Science, 1985.

[Pra75] V. Pratt. Every prime has a succinct certificate. *SIAM J. Comput.*, 4:214–220, 1975.

[Rab80] M. Rabin. Probabilistic algorithms in finite fields. *SIAM J. Comput.*, 9:273–280, 1980.

[RS62] J. Rosser and L. Schoenfield. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6:64–94, 1962.

[RSA78] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[SA84] C. Schnorr and W. Alexi. RSA bits are $0.5 + \epsilon$ secure. In *Advances in Cryptology: Proceedings of Eurocrypt'84*, pages 113–126, 1984.

MOV Reduction

- 1988: PhD Thesis of B. Kaliski
- 1990: Menezes, O. and Vanstone read his thesis and learnt the cryptographic application of the Weil pairing and Miller's algorithm. We then found the reduction of ECDL to MDL by using the Weil pairing.

Reply message from Kaliski

- Victor Miller visited Ron Rivest when I was a graduate student, and he met with me about my research. If I recall correctly, I asked him if he knew a way to determine whether an elliptic curve group was cyclic, and he suggested the Weil pairing. He also gave me a copy of his algorithm for computing the Weil pairing, and agreed that I could implement it for my thesis.

A New Approach on Bilinear Pairings and Its Applications

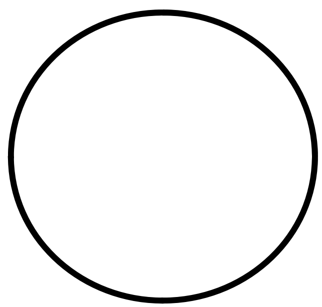
Joint Work with Katsuyuki Takashima (Mitsubishi Electric)

Pairing-Based Cryptography

Why Did Pairing-Based Cryptography So Succeed?

Mathematically Richer Structure

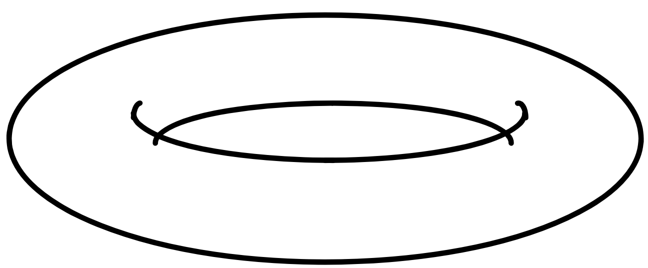
- Traditional Crypto: genus 0



F_p^* (e.g., Multiplicative group)

- Pairing-Based Crypto:

genus 1



$$E[n] \cong Z_n \oplus Z_n \subset E\left(\overline{F}_p\right)$$

(e.g., pairing-friendly elliptic curve group)

Additional Math Structure with Pairings

- Traditional Techniques over Cyclic Groups
  - $h = g^x$: One-way (hard to compute x from (g, h)).
  - $(g^x)^y = (g^y)^x$: Commutativity
  - $g^{x+y} = g^x g^y$: Homomorphism
- Pairing ➔ Additional Structure as well as the Above Properties
  - $h = g^x$: One-way (hard to compute x from (g, h).
  - $(g^x)^y = (g^y)^x$: Commutativity
  - $g^{x+y} = g^x g^y$: Homomorphism:
  - $e(g^x, g^y) = e(g, g)^{xy}$: Bilinearity

New Approach on Pairings:

Constructing a Richer Structure from Pairing Groups

Pairing Groups

- $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T), \quad |\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = q$ (prime)

  ($\mathbb{G}_1, \mathbb{G}_2$: additive form expression)
  ($\mathbb{G}_T$: multiplicative form expression)

  $G_1 \in \mathbb{G}_1,\ G_2 \in \mathbb{G}_2 \quad (G_1, G_2 \neq \mathbf{0})$

- $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

  - $g_T := e(G_1, G_2) \neq 1$ (nondegenerate)
  - $e(xG_1, yG_2) = e(G_1, G_2)^{xy}$ (bilinear)

The Most Natural Way to Make a Richer Algebraic Structure from Pairing Groups

Direct Product of Pairing Groups

$$\mathbb{V} := \overbrace{\mathbb{G}_1 \times \cdots \times \mathbb{G}_1}^{N}$$

$$\mathbb{V}^* := \overbrace{\mathbb{G}_2 \times \cdots \times \mathbb{G}_2}^{N}$$

$$\boldsymbol{x} \in \mathbb{V}, \qquad \boldsymbol{y} \in \mathbb{V}^*$$

$$\boldsymbol{x} := (x_1 G_1, \ldots, x_N G_1), \qquad \boldsymbol{y} := (y_1 G_2, \ldots, y_N G_2)$$

$$(x_i,\ y_i\ \in \mathbb{F}_q \text{ for } i = 1, \ldots, N).$$

N-Dimensional Vector Spaces:

$$\mathbb{V} = \mathbb{G}_1 \times \cdots \times \mathbb{G}_1, \quad \mathbb{V}^* = \mathbb{G}_2 \times \cdots \times \mathbb{G}_2$$

- Vector Addition

For $\boldsymbol{x} := (x_1 G_1, \ldots, x_N G_1) \in \mathbb{V}$ and $\boldsymbol{y} := (y_1 G_1, \ldots, y_N G_1) \in \mathbb{V}$,

$$\begin{aligned}\boldsymbol{x} + \boldsymbol{y} &:= (x_1 G_1 + y_1 G_1, \ldots, x_N G_1 + y_N G_1) \\ &= ((x_1 + y_1) G_1, \ldots, (x_N + y_N) G_1) \in \mathbb{V}\end{aligned}$$

Similarly defined for $\mathbb{V}^*$.

- Scalar multiplication

For $\boldsymbol{x} := (x_1 G_1, \ldots, x_N G_1) \in \mathbb{V}$ and $c \in \mathbb{F}_q$,

$$c\boldsymbol{x} := (c x_1 G_1, \ldots, c x_N G_1) \in \mathbb{V}$$

Similarly defined for $\mathbb{V}^*$.

N-Dimensional Vector Spaces:

$$\mathbb{V} = \mathbb{G}_1 \times \cdots \times \mathbb{G}_1, \ \ \mathbb{V}^* = \mathbb{G}_2 \times \cdots \times \mathbb{G}_2$$

Canonical Bases

$$\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N) \text{ for } \mathbb{V}, \quad \mathbb{A}^* := (\boldsymbol{a}_1^*, \ldots, \boldsymbol{a}_N^*) \text{ for } \mathbb{V}^*,$$

$$\boldsymbol{a}_1 := (G_1, \boldsymbol{0}, \ldots, \boldsymbol{0}),\ \boldsymbol{a}_2 := (\boldsymbol{0}, G_1, \boldsymbol{0}, \ldots, \boldsymbol{0}), \ldots, \boldsymbol{a}_N := (\boldsymbol{0}, \ldots, \boldsymbol{0}, G_1)$$

$$\boldsymbol{a}_1^* := (G_2, \boldsymbol{0}, \ldots, \boldsymbol{0}),\ \boldsymbol{a}_2^* := (\boldsymbol{0}, G_2, \boldsymbol{0}, \ldots, \boldsymbol{0}), \ldots, \boldsymbol{a}_N^* := (\boldsymbol{0}, \ldots, \boldsymbol{0}, G_2)$$

Element Expression on Canonical Basis

$$\begin{aligned} \boldsymbol{x} &:= (x_1 G_1, \ldots, x_N G_1) = x_1 \boldsymbol{a}_1 + \cdots + x_N \boldsymbol{a}_N \\ &= (x_1, \ldots, x_N)_{\mathbb{A}} = (\overrightarrow{x})_{\mathbb{A}} \in \mathbb{V} \end{aligned}$$

$$\begin{aligned} \boldsymbol{y} &:= (y_1 G_2, \ldots, y_N G_2) = y_1 \boldsymbol{a}_1^* + \cdots + y_N \boldsymbol{a}_N^* \\ &= (y_1, \ldots, y_N)_{\mathbb{A}^*} = (\overrightarrow{y})_{\mathbb{A}^*} \in \mathbb{V}^* \end{aligned}$$

$$\boldsymbol{a}_1 = (1, 0, \ldots, 0)_{\mathbb{A}},\ \boldsymbol{a}_2 = (0, 1, 0, \ldots, 0)_{\mathbb{A}}, \ldots, \boldsymbol{a}_N = (0, \ldots, 0, 1)_{\mathbb{A}},$$

$$\boldsymbol{a}_1^* = (1, 0, \ldots, 0)_{\mathbb{A}^*},\ \boldsymbol{a}_2^* = (0, 1, 0, \ldots, 0)_{\mathbb{A}^*}, \ldots, \boldsymbol{a}_N^* = (0, \ldots, 0, 1)_{\mathbb{A}^*}$$

Duality

Inner-Products between $\mathbb{V}$ and $\mathbb{V}^*$

For $\boldsymbol{x} := (\overrightarrow{x})_{\mathbb{A}} \in \mathbb{V}$, $\boldsymbol{y} := (\overrightarrow{y})_{\mathbb{A}^*} \in \mathbb{V}^*$,

$$\boldsymbol{x} \cdot \boldsymbol{y} := \sum_{i=1}^{N} x_i y_i = \overrightarrow{x} \cdot \overrightarrow{y} \in \mathbb{F}_q$$

Dual Spaces

For $\boldsymbol{y} \in \mathbb{V}^*$,

Linear map $\quad \boldsymbol{y} : \quad \mathbb{V} \longrightarrow \mathbb{F}_q$

$\qquad\qquad\qquad \boldsymbol{y} : \quad \boldsymbol{x} \longmapsto \boldsymbol{x} \cdot \boldsymbol{y}$

$\mathbb{V}^*$ is the dual space of $\mathbb{V}$.

Pairing between $\mathbb{V}$ and $\mathbb{V}^*$ $\quad e : \mathbb{V} \times \mathbb{V}^* \to \mathbb{G}_T$

$$e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^{N} e(x_i G_1, y_i G_2) = e(G_1, G_2)^{\sum_{i=1}^{N} x_i y_i}$$

$$= g_T^{\overrightarrow{x} \cdot \overrightarrow{y}} = g_T^{\boldsymbol{x} \cdot \boldsymbol{y}} \in \mathbb{G}_T$$

$$\boxed{\begin{array}{l} \boldsymbol{x} := (x_1 G_1, \ldots, x_N G_1) \in \mathbb{V} \\ \qquad\quad \updownarrow e \qquad\qquad \updownarrow e \\ \boldsymbol{y} := (y_1 G_2, \ldots, y_N G_2) \in \mathbb{V}^* \end{array}}$$

Orthonormality

$(\mathbb{A}, \mathbb{A}^*)$: dual orthonormal bases of $\mathbb{V}$ and $\mathbb{V}^*$, since

$$\boldsymbol{a}_i \cdot \boldsymbol{a}_j^* = \delta_{i,j} := \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}$$

$$e(\boldsymbol{a}_i, \boldsymbol{a}_j^*) = g_T^{\delta_{i,j}}$$

Base Change

$\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$: basis of $\mathbb{V}$

s.t. $X := (\chi_{i,j}) \xleftarrow{\mathsf{U}} GL(N, \mathbb{F}_q)$,

$\boldsymbol{b}_i = \sum_{j=1}^{N} \chi_{i,j} \boldsymbol{a}_j$ for $i = 1, \ldots, N$.

$$\mathbb{A} \overset{X}{\downarrow} \mathbb{B}$$

$\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$: basis of $\mathbb{V}^*$

s.t. $(\vartheta_{i,j}) := (X^T)^{-1}$,

$\boldsymbol{b}_i^* = \sum_{j=1}^{N} \vartheta_{i,j} \boldsymbol{a}_j^*$ for $i = 1, \ldots, N$.

$$\mathbb{A}^* \overset{(X^T)^{-1}}{\downarrow} \mathbb{B}^*$$

$(\mathbb{B}, \mathbb{B}^*)$: dual orthonormal bases of $\mathbb{V}$ and $\mathbb{V}^*$,

since $\boldsymbol{b}_i \cdot \boldsymbol{b}_j^* = \delta_{i,j}$

i.e., $e(\boldsymbol{b}_i, \boldsymbol{b}_j^*) = g_T^{\delta_{i,j}}$

Base Change

$(\mathbb{A}, \mathbb{A}^*)$: dual orthonormal bases of $(\mathbb{V}, \mathbb{V}^*)$, i.e., $e(\boldsymbol{a}_i, \boldsymbol{a}_j^*) = g_T^{\delta_{i,j}}$

Base change by $X \overset{\cup}{\leftarrow} GL(N, \mathbb{F}_q)$,

$(\mathbb{B}, \mathbb{B}^*)$: dual orthonormal bases of $(\mathbb{V}, \mathbb{V}^*)$, i.e., $e(\boldsymbol{b}_i, \boldsymbol{b}_j^*) = g_T^{\delta_{i,j}}$

For $\boldsymbol{x} := x_1\boldsymbol{b}_1 + \cdots + x_N\boldsymbol{b}_N = (x_1, \ldots, x_N)_{\mathbb{B}} = (\overrightarrow{x})_{\mathbb{B}} \in \mathbb{V}$
and $\boldsymbol{y} := y_1\boldsymbol{b}_1^* + \cdots + y_N\boldsymbol{b}_N^* = (y_1, \ldots, y_N)_{\mathbb{B}^*} = (\overrightarrow{y})_{\mathbb{B}^*} \in \mathbb{V}^*$,
$e(\boldsymbol{x}, \boldsymbol{y}) = \prod_{i=1}^N e(x_i\boldsymbol{b}_i, y_i\boldsymbol{b}_i^*) = e(g, g)^{\sum_{i=1}^N x_i y_i} = g_T^{\overrightarrow{x} \cdot \overrightarrow{y}} \in \mathbb{G}_T$.

Trapdoor

$$\begin{tikzcd}[column sep=large] (\mathbb{B},\ \mathbb{A},\ \mathbb{A}^*) \arrow[r, shift left=2, "\text{hard}", "\times" marking] \arrow[r, shift right=2, "\text{easy}"', "X"' below] & \mathbb{B}^* \end{tikzcd}$$

Special Case: Self-Duality

Symmetric pairing group $(\mathbb{G}_1 = \mathbb{G}_2)$:

$(\mathbb{G}, \mathbb{G}, \mathbb{G}_T)$ with $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$

$$\mathbb{V} = \mathbb{V}^* := \mathbb{G} \times \cdots \times \mathbb{G}$$

$\mathbb{A}$: (self-dual) orthonormal basis of $\mathbb{V}$, i.e., $e(\boldsymbol{a}_i, \boldsymbol{a}_j) = g_T^{\delta_{i,j}}$

$\Downarrow$ Base change by $X \xleftarrow{\cup} GL(N, \mathbb{F}_q)$,

$(\mathbb{B}, \mathbb{B}^*)$: (self-dual) orthonormal bases of $\mathbb{V}$, i.e., $e(\boldsymbol{b}_i, \boldsymbol{b}_j^*) = g_T^{\delta_{i,j}}$

$$(\mathbb{B},\ \mathbb{A}) \not\longrightarrow \mathbb{B}^*$$

$$(\mathbb{B},\ \mathbb{A}) \xrightarrow[X]{} \mathbb{B}^*$$

Abstraction: Dual Pairing Vector Spaces (DPVS)

$(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*)$:

q: prime, $\mathbb{V}$ and $\mathbb{V}^*$: N-dimensional vector spaces over $\mathbb{F}_q$, $\mathbb{G}_T$: cyclic group of order q (g_T: generator), $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$ and $\mathbb{A}^* := (\boldsymbol{a}_1^*, \ldots, \boldsymbol{a}_N^*)$: canonical bases of $\mathbb{V}$ and $\mathbb{V}^*$. There are efficient algorithms for e, $\phi_{i,j}$ and $\phi_{i,j}^*$ such that:

1. [Non-degenerate bilinear pairing] $e : \mathbb{V} \times \mathbb{V}^* \to \mathbb{G}_T$ i.e., $e(s\boldsymbol{x}, t\boldsymbol{y}) = e(\boldsymbol{x}, \boldsymbol{y})^{st}$ and if $e(\boldsymbol{x}, \boldsymbol{y}) = 1$ for all $\boldsymbol{y} \in \mathbb{V}$, then $\boldsymbol{x} = \boldsymbol{0}$.
2. [Dual orthonormal bases] $e(\boldsymbol{a}_i, \boldsymbol{a}_j^*) = g_T^{\delta_{i,j}}$ for all i and j.
3. [Canonical maps] Endomorphisms $\phi_{i,j}$ of $\mathbb{V}$ s.t. $\phi_{i,j}(\boldsymbol{a}_j) = \boldsymbol{a}_i$ and $\phi_{i,j}(\boldsymbol{a}_k) = \boldsymbol{0}$ if $k \neq j$. Endomorphisms $\phi_{i,j}^*$ of $\mathbb{V}^*$ s.t. $\phi_{i,j}^*(\boldsymbol{a}_j^*) = \boldsymbol{a}_i^*$ and $\phi_{i,j}^*(\boldsymbol{a}_k^*) = \boldsymbol{0}$ if $k \neq j$. We call $\phi_{i,j}$ and $\phi_{i,j}^*$ "canonical maps".

(Example of canonical maps on $\mathbb{V} = \mathbb{G}_1 \times \cdots \times \mathbb{G}_1$)

$$\phi_{i,j}(\boldsymbol{x}) := (\overbrace{\boldsymbol{0}, \ldots, \boldsymbol{0}}^{i-1}, x_j G_1, \overbrace{\boldsymbol{0}, \ldots, \boldsymbol{0}}^{N-i}) \text{ for } \boldsymbol{x} := (x_1 G_1, \ldots, x_j G_1, \ldots, x_N G_1)$$

Construction of Dual Pairing Vector Spaces:

- Direct product of pairing groups

$$\mathbb{V} = \mathbb{G}_1 \times \cdots \times \mathbb{G}_1 \text{ and } \mathbb{V}^* = \mathbb{G}_2 \times \cdots \times \mathbb{G}_2$$

(e.g., product of elliptic curves)

- Jocobian of supersingular hyperelliptic curves

$\mathbb{V} = \mathbb{V}^* := \mathrm{Jac}_C[q] \cong (\mathbb{F}_q)^{2g}$:
q-torsion point group of the Jacobian variety of some specific supersingular hyperelliptic curves C of genus g.

[Takashima, ANTS'08]

Intractable Problems in DPVS Suitable for Cryptographic Applications

- Vector Decomposition Problem (VDP)
- Decisional VDP (DVDP)
- Decisional Subspace Problem (DSP)

Vector Decomposition Problem (VDP)

$\mathbb{V}, \mathbb{V}^*, \mathbb{A}, \mathbb{A}^*, \mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{N_1})$ $\qquad \begin{array}{c} \mathbb{A} \\ \big\downarrow X := (\chi_{i,j}) \\ \mathbb{B} \end{array}$

$$\boldsymbol{v} := \boxed{v_1 \boldsymbol{b}_1 + \cdots + v_{N_2} \boldsymbol{b}_{N_2}} + \boxed{v_{N_2+1} \boldsymbol{b}_{N_2+1} + \cdots + v_{N_1} \boldsymbol{b}_{N_1}}$$

$$\left(\sum_{j=1}^{N_1} v_j \chi_{j,1} G_1, \ldots, \sum_{j=1}^{N_1} v_j \chi_{j,N_1} G_1\right)$$

hard $\quad \cancel{\Downarrow} \quad$ $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{N_2} \rangle$.

$$\boldsymbol{u} := \boxed{v_1 \boldsymbol{b}_1 + \cdots + v_{N_2} \boldsymbol{b}_{N_2}}$$

$$\left(\sum_{j=1}^{N_2} v_j \chi_{j,1} G_1, \ldots, \sum_{j=1}^{N_2} v_j \chi_{j,N_1} G_1\right)$$

Special Case of Vector Decomposition Problem (VDP)

$\mathbb{V}, \mathbb{V}^*, \mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{N_1}), \mathbb{A}^*$

$$\boldsymbol{v} := \boxed{v_1\boldsymbol{a}_1 + \cdots + v_{N_2}\boldsymbol{a}_{N_2}} + \boxed{v_{N_2+1}\boldsymbol{a}_{N_2+1} + \cdots + v_{N_1}\boldsymbol{a}_{N_1}}$$

$$(v_1 G_1, \ldots, v_{N_2} G_1, v_{N_2+1} G_1, \ldots, v_{N_1} G_1)$$

easy

$\mathsf{span}\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{N_2} \rangle.$

$$\boldsymbol{u} := \boxed{v_1\boldsymbol{a}_1 + \cdots + v_{N_2}\boldsymbol{a}_{N_2}}$$

$$(v_1 G_1, \ldots, v_{N_2} G_1, \boldsymbol{0}, \ldots, \boldsymbol{0})$$

History of Vector Decomposition Problem (VDP)

[Yoshida, Mitsunari and Fujiwara 2003], [Yoshida 2003]

Introduced VDP on elliptic curves.

History of Vector Decomposition Problem (VDP)

[Duursma and Kiyavash 2005], [Duursma and Park 2006],

VDP on hyperelliptic curves, higher dimensional ElGamal-type signatures

History of Vector Decomposition Problem (VDP)

[Galbraith and Verheul, PKC 2008]

Introduced "distortion eigenvector basis" for VDP on elliptic curves.

History of Vector Decomposition Problem (VDP)

O. and Takashima (Pairing 2008):

Introduced more general notion, “distortion eigenvector spaces”, for higher dimensional spaces, and showed several cryptographic applications.

We also extended the concept to “dual pairing vector spaces” (Aisiacrypt 2009) for VDP and other problems, and showed an application to predicate encryption.

Trapdoor of VDP: Algorithm Deco

$\mathbb{V}, \mathbb{V}^*, \mathbb{A}, \mathbb{A}^*, \mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{N_1})$

$\mathbb{A} \xrightarrow{X} \mathbb{B}$

$\boldsymbol{v} := \boxed{v_1\boldsymbol{b}_1 + \cdots + v_{N_2}\boldsymbol{b}_{N_2}} + \boxed{v_{N_2+1}\boldsymbol{b}_{N_2+1} + \cdots + v_{N_1}\boldsymbol{b}_{N_1}}$

$\Downarrow (X, \mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{N_2} \rangle, \mathbb{B})$

Deco

$(t_{i,j}) := X^{-1}$,

$\boldsymbol{u} := \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} \sum_{\kappa=1}^{N_1} t_{i,j} x_{j,\kappa} \phi_{\kappa,i}(\boldsymbol{v})$

$\Downarrow$

$\boldsymbol{u} := \boxed{v_1\boldsymbol{b}_1 + \cdots + v_{N_2}\boldsymbol{b}_{N_2}}$

Decisional VDP (DVDP)

$$\mathbb{V}, \mathbb{V}^*, \mathbb{A}, \mathbb{A}^*, \mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{N_1})$$

$$\boldsymbol{v} := \boxed{v_1 \boldsymbol{b}_1 + \cdots + v_{N_2} \boldsymbol{b}_{N_2}} + \boxed{v_{N_2+1} \boldsymbol{b}_{N_2+1} + \cdots + v_{N_1} \boldsymbol{b}_{N_1}}$$

$$\boldsymbol{u} := \boxed{v_1 \boldsymbol{b}_1 + \cdots + v_{N_2} \boldsymbol{b}_{N_2}}$$

$$\boldsymbol{u}' := \boxed{r_1 \boldsymbol{b}_1 + \cdots + r_{N_2} \boldsymbol{b}_{N_2}} \qquad (r_1, \ldots, r_{N_2}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{N_2}$$

DVDP Assumption

$\forall$ Adv

$$\Pr\left[(\boldsymbol{v}, \boldsymbol{u}) \to \boxed{\text{Adv}} \to 1 \right] \approx \Pr\left[(\boldsymbol{v}, \boldsymbol{u}') \to \boxed{\text{Adv}} \to 1 \right]$$

Decisional Subspace Problem (DSP)

$$\mathbb{V}, \mathbb{V}^*, \mathbb{A}, \mathbb{A}^*, \mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{N_1})$$

$$\boldsymbol{v} := \boxed{v_1\boldsymbol{b}_1 + \cdots + v_{N_2}\boldsymbol{b}_{N_2}} + \boxed{v_{N_2+1}\boldsymbol{b}_{N_2+1} + \cdots + v_{N_1}\boldsymbol{b}_{N_1}}$$

i.e., $\boldsymbol{v} \xleftarrow{\mathsf{U}} \mathbb{V}$

$$\boldsymbol{v}' := \boxed{r_1\boldsymbol{b}_1 + \cdots + r_{N_2}\boldsymbol{b}_{N_2}} \qquad (r_1, \ldots, r_{N_2}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{N_2}$$

i.e., $\boldsymbol{v}' \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{N_2} \rangle \subset \mathbb{V}$

DSP Assumption

$\forall$ Adv

$$\Pr\left[\begin{array}{c} \boldsymbol{v} \\ \Downarrow \\ \boxed{\mathsf{Adv}} \\ \Downarrow \\ 1 \end{array}\right] \approx \Pr\left[\begin{array}{c} \boldsymbol{v}' \\ \Downarrow \\ \boxed{\mathsf{Adv}} \\ \Downarrow \\ 1 \end{array}\right]$$

Relations with DDH and DLIN Problems

Decisional s-linear assumption:

$G, G_1, \ldots, G_s \xleftarrow{\mathsf{U}} \mathbb{G}, \quad x_1, \ldots, x_s, x_{s+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q$

Given $(G, G_1, \ldots, G_s)$, it is hard to distinguish

$\boldsymbol{v} = (x_1 G_1, \ldots, x_s G_s, x_{s+1} G)$ and

$\boldsymbol{v}' = (x_1 G_1, \ldots, x_s G_s, (\sum_{i=1}^{s} x_i) G)$.

Decisional 1-linear assumption (=DDH assumption):

It is hard to distinguish

$(G, G_1, x_1 G_1, x_2 G)$ and

$(G, G_1, x_1 G_1, x_1 G)$.

$(\kappa_1 G, \ldots, \kappa_s G) := (G_1, \ldots, G_s)$,

$\boldsymbol{b}_1 := (\kappa_1 G, \boldsymbol{0}, \ldots, \boldsymbol{0}, G) = \kappa_1 \boldsymbol{a}_1 + \boldsymbol{a}_{s+1}$,

$\boldsymbol{b}_2 := (\boldsymbol{0}, \kappa_2 G, \boldsymbol{0}, \ldots, \boldsymbol{0}, G) = \kappa_2 \boldsymbol{a}_2 + \boldsymbol{a}_{s+1},$,

$\vdots$

$\boldsymbol{b}_s := (\boldsymbol{0}, \ldots, \boldsymbol{0}, \kappa_s G, G) = \kappa_s \boldsymbol{a}_s + \boldsymbol{a}_{s+1}$,

$\boldsymbol{b}_{s+1} := (\boldsymbol{0}, \ldots, \boldsymbol{0}, G) = \boldsymbol{a}_{s+1}$

$\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{s+1})$

$$X := \begin{pmatrix} \kappa_1 & & 0 & 1 \\ & \ddots & & \vdots \\ & & \kappa_s & 1 \\ 0 & & & 1 \end{pmatrix}$$

$\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{s+1})$

It is hard to distinguish

$\boldsymbol{v} = x_1 \boldsymbol{b}_1 + \ldots + x_s \boldsymbol{b}_s + x'_{s+1} \boldsymbol{b}_{s+1} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_s, \boldsymbol{b}_{s+1} \rangle = \mathbb{V}$ and

$\boldsymbol{v}' = x_1 \boldsymbol{b}_1 + \ldots + x_s \boldsymbol{b}_s \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_s \rangle$

Trapdoors for DVDP and DSP

- Algorithm Deco with X
- Pairing with $\mathbb{B}^*$

  DSP can be efficiently solved by using *trapdoor*

  $\boldsymbol{t}^* \in \mathrm{span}\langle \boldsymbol{b}^*_{N_2+1}, \ldots, \boldsymbol{b}^*_{N_1} \rangle$

  $$e(\boldsymbol{v}, \boldsymbol{t}^*) \neq 1 \quad \text{with high probability}$$

  $$e(\boldsymbol{v}', \boldsymbol{t}^*) = 1$$

- Hierarchy of trapdoors

$$X \;\underset{\cancel{\longleftarrow}}{\longrightarrow}\; \mathbb{B}^* \;\underset{\cancel{\longleftarrow}}{\longrightarrow}\; \boldsymbol{t}^* \in S^* \subset \mathbb{V}^*$$

(Top level trapdoor)

Related Works and Properties

Higher dimensional vector treatment of bilinear pairing groups have been already employed in literature especially in the areas of IBE, ABE and BE

To the best of our knowledge, however, the base change and dual space framework have not been presented in an explicit manner.

Our key properties of our appraoch are
the hard decomposability and indistinguishability
on DPVS $\mathbb{V}$ with basis $\mathbb{B}$ and its trapdoors via X and $\mathbb{B}^*$.

Application to Cryptography

Multivariate Homomorphic Encryption

$\mathsf{Gen}(1^k)$:

$\mathbb{V} \xleftarrow{\mathsf{R}} \mathbb{G}(1^k)$ with canonical basis $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{N_1})$

$X := (x_{i,j}) \xleftarrow{\mathsf{U}} \ \boldsymbol{b}_i := \sum_{j=1}^{N_1} x_{i,j}\boldsymbol{a}_j, \ \mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{N_1})$.

$\boxed{\mathsf{sk} := X,} \quad \mathsf{pk} := (\mathbb{V}, \mathbb{A}, \mathbb{B})$.

return sk, pk.

$\mathsf{Enc}(\mathsf{pk}, (m_1, \ldots, m_{N_2}) \in \{0, \ldots, \tau - 1\}^{N_2})$:

$(r_{N_2+1}, \ldots, r_{N_1}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{N_1 - N_2}$,

$\boldsymbol{c} := (m_1\boldsymbol{b}_1 + \cdots + m_{N_2}\boldsymbol{b}_{N_2}) + (r_{N_2+1}\boldsymbol{b}_{N_2+1} + \cdots + r_{N_1}\boldsymbol{b}_{N_1})$

return ciphertext $\boldsymbol{c}$.

$\mathsf{Dec}(\mathsf{sk}, \boldsymbol{c})$:

$\boxed{\boldsymbol{c}'_i := \mathsf{Deco}(\boldsymbol{c}, \mathsf{span}\langle \boldsymbol{b}_i \rangle, X, \mathbb{B}).} \quad m'_i := \mathrm{Dlog}_{\boldsymbol{b}_i}(\boldsymbol{c}'_i) \quad$ for $i = 1, \ldots, N_2$.

return plaintext $(m'_1, \ldots, m'_{N_2})$.

Homomorphic property

$$\mathsf{Enc}(\mathsf{pk}, (m_1, \ldots, m_{N_2}) + \mathsf{Enc}(\mathsf{pk}, (m'_1, \ldots, m'_{N_2})$$
$$= \mathsf{Enc}(\mathsf{pk}, (m_1 + m'_1, \ldots, m_{N_2} + m'_{N_2})$$

Multivariate Homomorphic Encryption

$\mathsf{Gen}(1^k)$:

$\mathbb{V} \xleftarrow{\mathsf{R}} \mathbb{G}(1^k)$ with canonical basis $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{N_1})$

$X := (x_{i,j}) \xleftarrow{\mathsf{U}}$ $\boldsymbol{b}_i := \sum_{j=1}^{N_1} x_{i,j}\boldsymbol{a}_j$, $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{N_1})$.

$\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$: basis of $\mathbb{V}^*$ s.t. $(\vartheta_{i,j}) := (X^T)^{-1}$,

$\boldsymbol{b}_i^* = \sum_{j=1}^{N} \vartheta_{i,j}\boldsymbol{a}_j^*$ for $i = 1, \ldots, N$.

$\boxed{\mathsf{sk} := \mathbb{B}^*,}$ $\mathsf{pk} := (\mathbb{V}, \mathbb{A}, \mathbb{B})$.

return sk, pk.

$\mathsf{Enc}(\mathsf{pk}, (m_1, \ldots, m_{N_2}) \in \{0, \ldots, \tau - 1\}^{N_2})$:

$(r_{N_2+1}, \ldots, r_{N_1}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{N_1 - N_2}$,

$\boldsymbol{c} := (m_1\boldsymbol{b}_1 + \cdots + m_{N_2}\boldsymbol{b}_{N_2}) + (r_{N_2+1}\boldsymbol{b}_{N_2+1} + \cdots + r_{N_1}\boldsymbol{b}_{N_1})$

return ciphertext $\boldsymbol{c}$.

$\mathsf{Dec}(\mathsf{sk}, \boldsymbol{c})$:

$\boxed{c_i' := e(\boldsymbol{c}, \boldsymbol{b}_i^*)}$ $m_i' := \mathrm{Dlog}_{g_T}(c_i')$ for $i = 1, \ldots, N_2$.

return plaintext $(m_1', \ldots, m_{N_2}')$.

Predicate Encryption Scheme

- Setup : $(\mathsf{param}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, n+2)$

  $\mathsf{pk} := (\mathsf{param}, \mathbb{B}), \quad \mathsf{sk} := \mathbb{B}^*$

- $\mathsf{GenKey}(\mathsf{sk}, \vec{v} := (v_1, \ldots, v_n))$:

  $\mathsf{sk}_{\vec{v}} := \boldsymbol{k}^* := \sigma(v_1 \boldsymbol{b}_1^* + \cdots + v_n \boldsymbol{b}_n^*) + \boldsymbol{b}_{n+1}^*$

  $= (\sigma \vec{v}, 1, 0)_{\mathbb{B}^*}$

- $\mathsf{Enc}(\mathsf{pk}, \vec{x} := (x_1, \ldots, x_n), m)$:

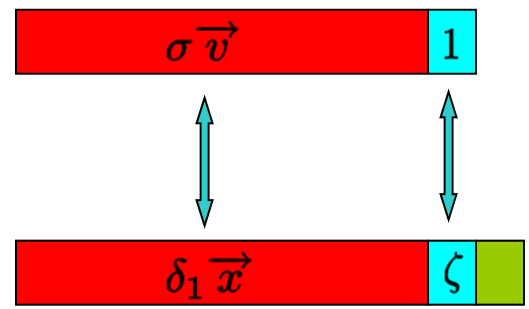
  $\boldsymbol{c}_1 := \delta_1(x_1 \boldsymbol{b}_1 + \cdots + x_n \boldsymbol{b}_n) + \zeta \boldsymbol{b}_{n+1} + \delta_{n+2} \boldsymbol{b}_{n+2}$

  $= (\delta_1 \vec{x}, \zeta, \delta_{n+2})_{\mathbb{B}}$

  $c_2 := g_T^{\zeta} \cdot m$

- $\mathsf{Dec}(\mathsf{pk}, \boldsymbol{k}^*, (\boldsymbol{c}_1, c_2))$:

  $m' := c_2 / e(\boldsymbol{c}_1, \boldsymbol{k}^*)$



$\delta_1 \sigma (\vec{x} \cdot \vec{v}) \quad + \quad \zeta$

$= \zeta$ if $\vec{x} \cdot \vec{v} = 0$,

random if $\vec{x} \cdot \vec{v} \neq 0$.

Summary

- A new approach on bilinear pairing: Dual pairing vector spaces

  - enjoy richer algebraic structures

- Cryptographic applications:

  - predicate encryption for inner-products

  - more...

Thank you!