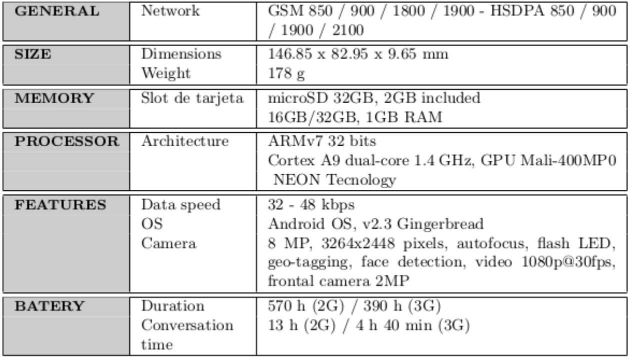
ABE implementation on ARM Processors

Ana Helena Sánchez Ramírez, Francisco Rodríguez Henríquez

CINVESTAV-IPN

ECC Rump Session

Samsung Galaxy Note



GENERAL	Network	GSM 850 / 900 / 1800 / 1900 - HSDPA 850 / 900 / 1900 / 2100
SIZE	Dimensions Weight	146.85 x 82.95 x 9.65 mm 178 g
MEMORY	Slot de tarjeta	microSD 32GB, 2GB included 16GB/32GB, 1GB RAM
PROCESSOR	Architecture	ARMv7 32 bits Cortex A9 dual-core 1.4 GHz, GPU Mali-400MP0 NEON Tecnology
FEATURES	Data speed OS Camera	32 - 48 kbps Android OS, v2.3 Gingerbread 8 MP, 3264x2448 pixels, autofocus, flash LED, geo-tagging, face detection, video 1080p@30fps, frontal camera 2MP
BATERY	Duration Conversation time	570 h (2G) / 390 h (3G) 13 h (2G) / 4 h 40 min (3G)

Ingredients

BN Curves

Ingredients

BN Curves

Pairings

Ingredients

BN Curves

Pairings

Faster formulas

Ingredients

BN Curves

Pairings

Faster formulas

ABE protocol

Receta

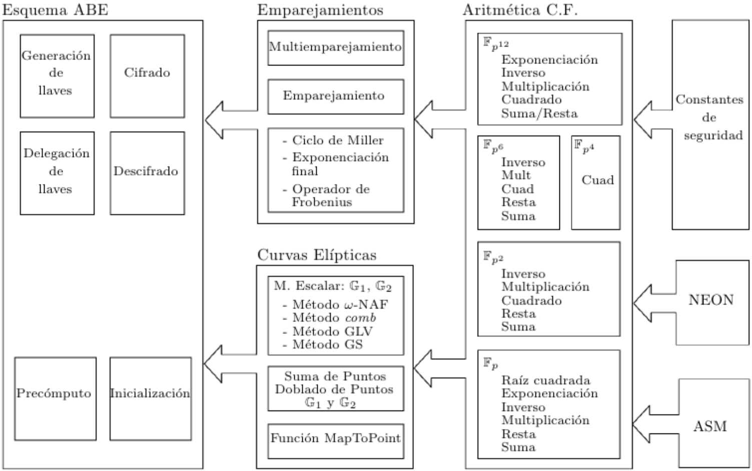
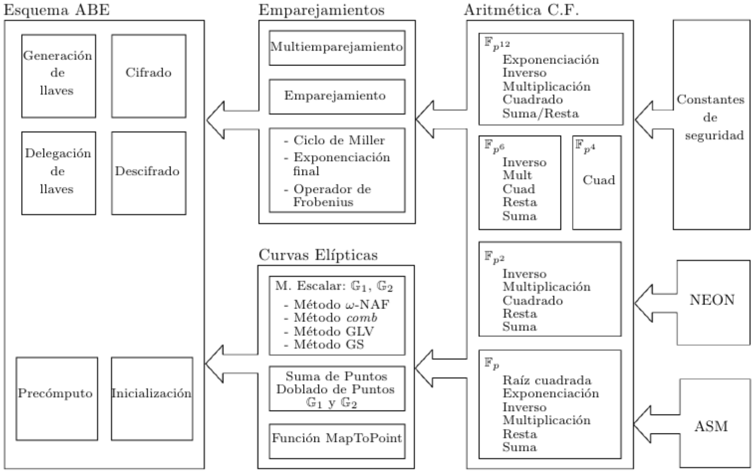


Figure: Modelo de implementación

Receta



Esquema ABE

Generación de llaves

Cifrado

Delegación de llaves

Descifrado

Precómputo

Inicialización

Emparejamientos

Multiemparejamiento

Emparejamiento

- Ciclo de Miller
- Exponenciación final
- Operador de Frobenius

Curvas Elípticas

M. Escalar: $\mathbb{G}_1$, $\mathbb{G}_2$

- Método ω-NAF
- Método *comb*
- Método GLV
- Método GS

Suma de Puntos
Doblado de Puntos
$\mathbb{G}_1$ y $\mathbb{G}_2$

Función MapToPoint

Aritmética C.F.

$\mathbb{F}_{p^{12}}$
Exponenciación
Inverso
Multiplicación
Cuadrado
Suma/Resta

$\mathbb{F}_{p^6}$
Inverso
Mult
Cuad
Resta
Suma

$\mathbb{F}_{p^4}$
Cuad

$\mathbb{F}_{p^2}$
Inverso
Multiplicación
Cuadrado
Resta
Suma

$\mathbb{F}_p$
Raíz cuadrada
Exponenciación
Inverso
Multiplicación
Resta
Suma

Constantes de seguridad

NEON

ASM

Figure: Modelo de implementación

Results

		ARMv7 Cortex A9 Dual Core		
Field	Operation	Galaxy Tab 10.1 nVidia Tegra 2	Galaxy Note Exynos 4	
		@1.0Ghz	@1.4Ghz	@1.4Ghz NEON
$\mathbb{F}_{p^2}$	mul	3.410	2.443	1.811
	cua	2.405	1.720	1.433
	inv	39.25	28.01	26.85
Miller Loop		8313	5963	4807
Final Exponentiation		5269	3291	2891
Pairing		13582	9727	7698

Table: Times in μs

Results

	Miller Loop	**Final Exponentiation**	**Pairing**
[Acar et all., 2012]	$26,320$	$24,690$	$51,010$
[Grewal et all., 2012] (ASM)	$7,376$	$4,510$	$11,886$
This work (NEON)	$6,730$	$4,047$	$10,777$

Table: Aprox. cpu cycles (1×10^3)

Attribute-Based Encryption (ABE)

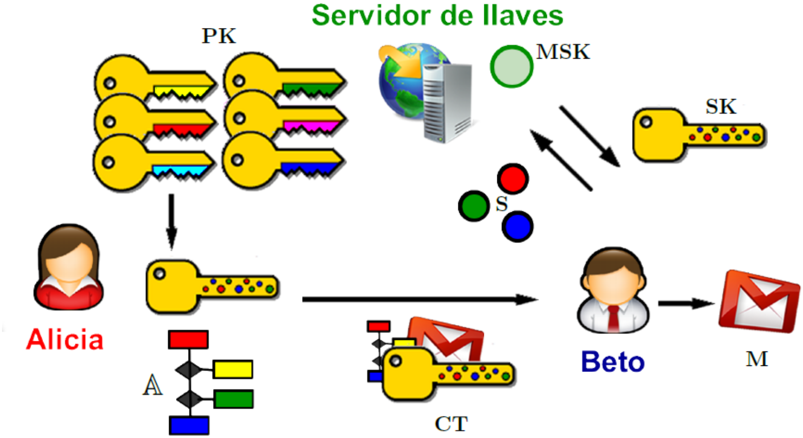
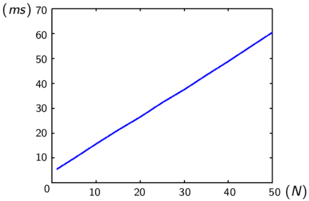
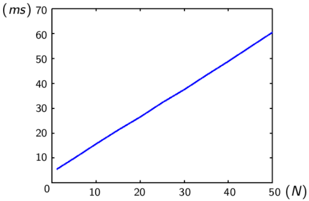


Figure: Attribute-Based Encryption

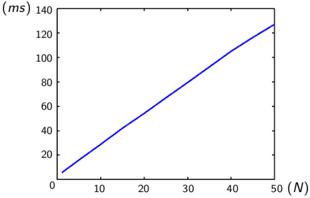
Results ABE



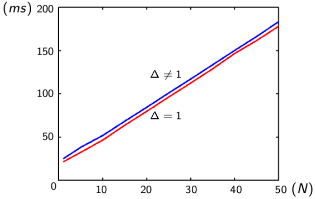
Key Generation



Delegation



Encrypt



Decrypt

Summary

1. We implement a cryptographic library for pairings
2. NEON gave us an improvement of 20%
3. ABE was implemented using the library
4. Buy a Samsung Galaxy Note

Summary

1. We implement a cryptographic library for pairings
2. NEON gave us an improvement of 20%
3. ABE was implemented using the library
4. Buy a Samsung Galaxy Note

Summary

1. We implement a cryptographic library for pairings
2. NEON gave us an improvement of 20%
3. ABE was implemented using the library
4. Buy a Samsung Galaxy Note

Summary

1. We implement a cryptographic library for pairings
2. NEON gave us an improvement of 20%
3. ABE was implemented using the library
4. Buy a Samsung Galaxy Note

¡GRACIAS!