# BGN-F-CF: a pairing-based SHE scheme

Vincent Herbert

## Contents

# 1 Settings

Let $\lambda = 128$ be the security parameter.

$x_0 = v^3$ and $v = 1868033$

$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$

$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$

$t(x) = 6x^2 + 1$

$p = p(x_0), r = r(x_0), t = t(x_0)$

$p$ and $r$ are 256-bits prime integers , $t$ is a 128-bits integer. Let $E$ be a curve of equation $y^2 = x^3 + 3$ defined over $\mathbb{F}_p$. 12 is the embedding degree of $r$ or the one of subgroup $E(\mathbb{F}_p)[r]$ of $E(\mathbb{F}_p)$. The operator $\xleftarrow{\$}$ refers to a random draw according to an uniform distribution.

$i_1, j_1, k_1, l_1, i_2, j_2, k_2, l_2 \xleftarrow{\$} \mathbb{F}_p : i_1 l_1 - j_1 k_1 = i_2 l_2 - j_2 k_2 = 1$

$g \xleftarrow{\$} E(\mathbb{F}_p)[r] : \mathrm{ord}(g) = r$

$$\begin{aligned} \pi \colon E &\to E \\ (x, y) &\mapsto (x^p, y^p) \end{aligned}$$

$h \xleftarrow{\$} E[r] \cap \mathrm{Ker}(\pi - p) : \mathrm{ord}(h) = r$

$u_1 \xleftarrow{\$} <(i_1 g, j_1 g)> \leq E(\mathbb{F}_p)[r]^2$

$v_1 \xleftarrow{\$} <(i_2 h, j_2 h)> \leq (E[r] \cap \mathrm{Ker}(\pi - p))^2$

$u = (u[0], u[1]) \xleftarrow{\$} E(\mathbb{F}_p)[r]^2$, $v = (v[0], v[1]) \xleftarrow{\$} (E[r] \cap \mathrm{Ker}(\pi - p))^2$

# 2 Encryption and decryption of a bit

$m \in \mathbb{F}_2$ $b \xleftarrow{\$} \mathbb{F}_2$

$a = m - b$

$c = \mathrm{Enc}(m) = (a, bu + u_1, bv + v_1) \in \mathbb{F}_2 \times E(\mathbb{F}_p)[r]^2 \times (E[r] \cap \mathrm{Ker}(\pi - p))^2$

To evaluate with this ciphertext, we need the first and one of the two last components. We decrypt with the two remaining components.

$\pi_1 \in \mathrm{End}(E(\mathbb{F}_p)[r]^2), \pi_2 \in \mathrm{End}(\mathrm{Ker}(\pi - p))^2)$

$\pi_1(x, y) = (-j_1 k_1 x + i_1 k_1 y, -j_1 l_1 x + i_1 l_1 y)$

$\pi_2(x, y) = (-j_2 k_2 x + i_2 k_2 y, -j_2 l_2 x + i_2 l_2 y)$

$m = \mathrm{Dec}(c) = a + \dfrac{\pi_1(bu + u_1)}{\pi_1(u)}$[1] if $c \in \mathbb{F}_2 \times E(\mathbb{F}_p)[r]^2$

$m = \mathrm{Dec}(c) = a + \dfrac{\pi_2(bv + v_1)}{\pi_2(v)}$ if $c \in \mathbb{F}_2 \times (E[r] \cap \mathrm{Ker}(\pi - p))^2$

The encryption function takes a bit on input. It outputs :

- an element of $\mathbb{F}_2$,

[1] The ratio is well-defined if the numerator is a multiple of the denumerator. Its value is the scalar factor between the two points, modulo 2.

- two group elements in $E(\mathbb{F}_p)[r]$ of order $r$, that is four elements of $\mathbb{F}_p$
- two group elements in $E[r] \cap \mathrm{Ker}(\pi - p)$ of order $r$, that is four elements of $\mathbb{F}_{p^{12}} \cong \mathbb{F}_p[X]/(X^{12} + 3)$

We simplify groups expressions. We have $E(\mathbb{F}_p)[r] = E(\mathbb{F}_p)$ since we have $\#E(\mathbb{F}_p) = r$ with $r$ prime. We also have $E[r] \cap \mathrm{Ker}(\pi - p) = E(\mathbb{F}_{p^{12}})[r]$. $E(\mathbb{F}_p)[r]$ and $E[r] \cap \mathrm{Ker}(\pi - p)$ are commutative groups of order $r$. They are isomorph to $(\mathbb{Z}/r\mathbb{Z}, +)$. Two elements of $E(\mathbb{F}_p)[r]$ can be represented by two elements of $\mathbb{F}_p$ plus 2 bits (x-coordinates and y-signs), that is $2\log_2(p)+2 = 514$ bits. The curve $E$ admits a twist of degree 6. With twist, elements of $\mathbb{F}_{p^{12}}$ can be represented using elements of $\mathbb{F}_{p^2}$. Two elements of $E[r] \cap \mathrm{Ker}(\pi - p)$ can be represented by two elements of $\mathbb{F}_p^2$ plus 2 bits, that is $4\log_2(p) + 2 = 1026$ bits. We employ $E' : y^2 = x^3 + 3/\xi$, a sextic twist of $E$ defined over $\mathbb{F}_p^2$, with $\xi$ chosen such that $r \mid \#E'(\mathbb{F}_p^2)$.

We reformulate. The encryption of a bit consists in:

- an element of $\mathbb{F}_2$,
- two group elements in $E(\mathbb{F}_p)$
- two group elements in $E'(\mathbb{F}_p^2)$

# 3 Multiply level-1 ciphertexts

A level-1 ciphertext $\in \mathbb{F}_2 \times E(\mathbb{F}_p)[r]^2 \times (E[r] \cap \mathrm{Ker}(\pi - p))^2$. To obtain the product of two level-1 ciphertexts, we remove the second component of first ciphertext and the third component of second ciphertext. We proceed in this way because we use an asymmetric pairing. The result is a level-2 ciphertext.

$c_1 = (a_1, \beta_1) \in \mathbb{F}_2 \times E(\mathbb{F}_p)[r]^2, c_2 = (a_2, \beta_2) \in \mathbb{F}_2 \times (E[r] \cap \mathrm{Ker}(\pi - p))^2$.

$\mathrm{Mult}^{(2)}(c_1, c_2) \coloneqq c = (a, \beta) \in \mathbb{F}_2 \times \mu_r^4$

$b_1, b_2, s \xleftarrow{\$} \mathbb{F}_2$

For $i = 1$ and $i = 2$, $c_i$ is an encryption of $m_i \in \mathbb{F}_2$ and $a_i = m_i - b_i$.

$a = a_1 a_2 - s$

We redo a random uniform draw for $u_1$ and $v_1$.

$$u_1 \xleftarrow{\$} <(i_1 g, j_1 g)>,\ v_1 \xleftarrow{\$} <(i_2 h, j_2 h)>$$

We split up the computation of $\beta$ in order to explain how the formula is obtained. We can jump this paragraph and only retain the final formula for a practical usage. The operator $\oplus$ refers to an homomorphic addition with the scheme BGN-F[2]. Let $e_{OA}$ be the optimal Ate pairing. The notation, $\mathrm{Enc}^{(l)}(s)$ refers to a level-$l$ ciphertext of bit $s$, with the scheme BGN-F. If no level is indicated, *e.g.* $\mathrm{Enc}(s)$, we consider a level-1 ciphertext.

[2]The addition operator, in the scheme BGN-F-CF, is denoted $\boxplus$

$$e\colon E(\mathbb{F}_p)[r]^2 \times (E[r] \cap \mathrm{Ker}(\pi - p))^2 \to \mu_r^4$$
$$e((g_1, g_2)(h_1, h_2)) \mapsto (e_{OA}(g_1, h_1), e_{OA}(g_1, h_2), e_{OA}(g_2, h_1), e_{OA}(g_2, h_2))$$

$$\beta = e(\beta_1, \beta_2)e(u, v_1)e(u_1, v) \oplus a_1\beta_2 \oplus a_2\beta_1 \oplus \mathrm{Enc}^{(2)}(s)$$

Let $\mu_r$ be the subgroup of $r^{\text{th}}$-roots of unity in $\mathbb{F}_{p^{12}}$. The first term belongs to $\mu_r^4$. Note, the level should be the same for all terms [3].

$u_2, u_3, u_4 \xleftarrow{\$} <(i_1 g, j_1 g)>$

$v_2, v_3, v_4 \xleftarrow{\$} <(i_2 h, j_2 h)>$

$\beta = e(\beta_1, \beta_2)e(u, v_1)e(u_1, v) \oplus e(\mathrm{Enc}(1), a_1\beta_2)e(u, v_2)e(u_2, v) \oplus e(a_2\beta_1, \mathrm{Enc}(1))e(u, v_3)e(u_3, v) \oplus e(\mathrm{Enc}(1), \mathrm{Enc}(s))e(u, v_4)e(u_4, v)$

Using bilinearity, we can simplify this expression. In practice, it is not useful to define $u_2, u_3, u_4, v_2, v_3, v_4$. On the other hand, it is useful to understand how we obtain the following formula.

$$\beta = e(\beta_1, \beta_2)e(\mathrm{Enc}(1), a_1\beta_2 + \mathrm{Enc}(s))e(a_2\beta_1, \mathrm{Enc}(1))e(u, v_1)e(u_1, v)$$

We compute $5 \times 4$ pairings to get a level-2 ciphertext.

# 4 Add level-$l$ ciphertexts with $1 \leq l \leq 2$

On input, there are two ciphertexts $(a_1, \beta_1)$ and $(a_2, \beta_2)$, with the same level $1 \leq l \leq 2$ and $a_1, a_2 \in \mathbb{F}_2$. On output, there is one level-$l$ ciphertext $(a, \beta)$ The three ciphertexts are in the same space.

Three configurations are possible.

- $\beta_1, \beta_2 \in E(\mathbb{F}_p)[r]^2$
- $\beta_1, \beta_2 \in (E[r] \cap \mathrm{Ker}(\pi - p))^2$
- $\beta_1, \beta_2 \in \mu_r^4$

$$a = a_1 + a_2$$

We redo a random uniform draw for $u_1$ and $v_1$.

$$u_1 \xleftarrow{\$} <(i_1 g, j_1 g)>,\ v_1 \xleftarrow{\$} <(i_2 h, j_2 h)>$$

$$\beta = \beta_1 + \beta_2 + u_1 \text{ if } \beta_1, \beta_2 \in E(\mathbb{F}_p)[r]^2$$

[3] If it is not the case, we multiply homomorphically the other terms by Enc(1), an encryption of bit 1. More generally, this is applied several times when we compute the sum of ciphertexts with several levels of difference.

$$\beta = \beta_1 + \beta_2 + v_1 \text{ if } \beta_1, \beta_2 \in (E[r] \cap \mathrm{Ker}(\pi - p))^2$$

$$\beta = \beta_1 \beta_2 e(u, v_1) e(u_1, v) \text{ if } \beta_1, \beta_2 \in \mu_r^4$$

# 5 Decrypt level-2 ciphertext

We define a notation used by Freeman, more compact than the usual one.

Let $\mathcal{M} = (m_{i,j})$ be an $n$-order matrix over $\mathbb{F}_p$

$\gamma^{\mathcal{M}} \coloneqq (\prod_{i=1}^n \gamma_i^{m_{i1}}, \cdots, \prod_{i=1}^n \gamma_i^{m_{in}})$ with $\gamma$ in a product group.

$\mathcal{A} = \begin{pmatrix} -j_1 k_1 & -j_1 l_1 \\ i_1 k_1 & i_1 l_1 \end{pmatrix}$, $\mathcal{B} = \begin{pmatrix} -j_2 k_2 & -j_2 l_2 \\ i_2 k_2 & i_2 l_2 \end{pmatrix}$

$\mathcal{A} \otimes \mathcal{B}$ is a matrix of order 4. We can divide it into 4 matrices of order 2. The $(i,j)^{\text{th}}$ block is equal to $a_{i,j}\mathcal{B}$ with $\mathcal{A} = (a_{i,j})_{i,j \in \{1,2\}}$.

$\pi_T \in \mathrm{End}(\mu_r^4)$

$\pi_T(\beta) = (\beta_1, \beta_2, \beta_3, \beta_4)^{\mathcal{A} \otimes \mathcal{B}}$

$m = \mathrm{Dec}(c) = a + \log_{\pi_T(e(u,v))}(\pi_T(\beta))$ if $c \in \mathbb{F}_2 \times \mu_r^4$

## 5.1 Public-key and private-key

At this stage, we have used all the material needed to encrypt and decrypt. We can explicit the keys in BGN-F-CF scheme.

- Public-key is $((E(\mathbb{F}_p)[r])^2, (i_1 g, j_1 g), (E[r] \cap \mathrm{Ker}(\pi - p))^2, (i_2 h, j_2 h), \mu_r, e, u, v)$.
- Private-key is $(\pi_1, \pi_2, \pi_T)$.

# 6 Multiply ciphertexts to obtain a level-$l$ ciphertext with $3 \leq l \leq 4$

On input, there are two ciphertexts $(a_1, \beta_1)$ and $(a_2, \beta_2)$, with levels $l_1, l_2 \in [\![1, 2]\!]$, $3 \leq l_1 + l_2 \leq 4$ and $a_1, a_2 \in \mathbb{F}_2$. On output, there is one level-$l$ ciphertext $(\alpha, \beta)$ with $l = l_1 + l_2$[4]. As previously said, $\oplus$ refers to an homomorphic addition with the scheme BGN-F.

$$\alpha = \mathrm{Enc}(a_1 a_2) \oplus \beta_2^{a_1} \oplus \beta_1^{a_2} \quad [5]$$

$$\beta = (\beta_1, \beta_2)$$

We can only add ciphertexts of same level, see Section 4. To compute $\alpha$, we should get level-2 terms.

[4] We can obtain level-4 ciphertexts but no product between a level-1 ciphertext and a level-3 ciphertext is defined.

[5] Abuse of notation in this section. Exponentations should be replaced by multiplications, for level-1 ciphertexts, where it operates on additive groups.

Three configurations are possible.

- $\beta \in (E(\mathbb{F}_p)[r]^2 \times \mu_r^4) \cup ((E[r] \cap \mathrm{Ker}(\pi - p))^2 \times \mu_r^4)$
- $\beta \in (\mu_r^4 \times E(\mathbb{F}_p)[r]^2) \cup (\mu_r^4 \times (E[r] \cap \mathrm{Ker}(\pi - p))^2)$
- $\beta \in \mu_r^4 \times \mu_r^4$

The three corresponding values of $\alpha$ are:

- $e(\mathrm{Enc}(a_1 a_2), \mathrm{Enc}(1))\beta_2^{a_1} e(a_2\beta_1, \mathrm{Enc}(1))e(u, v_1)e(u_1, v)$
- $e(\mathrm{Enc}(a_1 a_2), \mathrm{Enc}(1))\beta_1^{a_2} e(a_1\beta_2, \mathrm{Enc}(1))e(u, v_1)e(u_1, v)$
- $e(\mathrm{Enc}(a_1 a_2), \mathrm{Enc}(1))\beta_2^{a_1}\beta_1^{a_2} e(u, v_1)e(u_1, v)$

The first two cases permit to evaluate the same products since the multiplication is commutative over $\mathbb{F}_2$. We choose to limit outself to the first case where the first ciphertext has level one, and the second ciphertext has level two. Once again, in the first case, we restrict, for convenience, $\beta$ in the product group $(E(\mathbb{F}_p)[r]^2 \times \mu_r^4)$. In every instance, $\alpha \in \mu_r^4$. The number of successive multiplications is limited to one because the scheme BGN-F-CF evaluates ciphertexts up to level 4. Notice, the computation of a level-3 ciphertext needs the computation of $4 \times 4$ pairings instead of $3 \times 4$ pairings for the computation of a level-4 ciphertext. The additional pairings are an extra part of the computation cost when we multiply two ciphertexts of different levels.

# 7 Add level-$l$ ciphertexts with $3 \leq l \leq 4$

On input, there are two level-$l$ ciphertexts $(\alpha_1, \beta_1)$ and $(\alpha_2, \beta_2)$, with $l \in [\![3, 4]\!]$. The two ciphertexts are in the same ambient space. On output, there is one level-$l$ ciphertext $(\alpha, \beta)$.

$$\alpha = \alpha_1 \oplus \alpha_2 = \alpha_1\alpha_2 e(u, v_1)e(u_1, v)$$

For every instance, $\alpha, \alpha_1, \alpha_2 \in \mu_r^4$.

$$\beta = (\beta_1, \beta_2)$$

Each addition and multiplication (see Section 6) to obtain a $l$-level ciphertext, extend the ciphertext size. For this reason, we operate a limited number of such additions in practice.

After $A$ additions of different level-$l$ ciphertexts with $3 \leq l \leq 4$, there are three cases:

- $\beta \in (E(\mathbb{F}_p)[r]^2 \times \mu_r^4)^B \cup ((E[r] \cap \mathrm{Ker}(\pi - p))^2 \times \mu_r^4)^B$
- $\beta \in (\mu_r^4 \times E(\mathbb{F}_p)[r]^2)^B \cup (\mu_r^4 \times (E[r] \cap \mathrm{Ker}(\pi - p))^2)^B$
- $\beta \in (\mu_r^4 \times \mu_r^4)^B$

Note, the integer $B$ do not depend on the value of $A$ but on the ciphertext spaces of each term of the sum.

## 8 Decrypt level-$l$ ciphertext with $3 \leq l \leq 4$

On input a ciphertext $(\alpha, \beta)$ obtained with $A$ additions of different level-$l$ ciphertexts with $3 \leq l \leq 4$. $\alpha$ is a 2-level ciphertext.

$$\beta \coloneqq (\beta_{1,1}, \beta_{2,1}, \beta_{1,2}, \beta_{2,2}, \ldots, \beta_{1,B}, \beta_{2,B})$$

where $\forall\, i, j \in [\![1, B]\!]$, $\beta_{i,j}$ is either a level-1 ciphertext or a level-2 ciphertext. On output a plaintext $m \in \mathbb{F}_2$.

$$m = \mathrm{Dec}(\alpha) + \sum_{i=1}^{B} \mathrm{Dec}(\beta_{1,i})\,\mathrm{Dec}(\beta_{2,i})$$

## 9 Symbol table

| C(++) program | This document | Remark |
|---|---|---|
| $bn\_v$ | $v$ | $bn$ stands for Barreto-Naehrig. |
| $bn\_u$ | $x_0$ | |
| $bn\_p$ | $p$ | |
| $bn\_r$ (or $bn\_n$) | $r$ | The notation $bn\_n$ is used in dclxvi library. |
| $bit\_clair$ | $m$ | |
| $bit\_urandom$ | $b$ | |
| $bit\_chiffre$ | $c$ | It is a C++ class, not one bit. |
| $bit\_chiffre.bit\_masque$ | $a$ | |
| $public\_key.bipoint\_curve\_groupelt$ | $u$ | |
| $bipoint\_curve\_subgroupelt$ | $u_1$ | |
| $bit\_chiffre.bipoint\_curve$ | $bu + u_1$ | |
| $public\_key.bipoint\_twist\_groupelt$ | $v$ | |
| $bipoint\_twist\_subgroupelt$ | $v_1$ | |
| $bit\_chiffre.bipoint\_twist$ | $bv + v_1$ | |
| $bn\_curvegen$ | $g$ | $bn\_curvegen$, $bn\_twistgen$ are fixed in dclxvi library. |
| $bn\_twistgen$ | $h$ | |
| $public\_key.bipoint\_curvegen$ | $(i_1 g, j_1 g)$ | $(i_1 g, j_1 g)$ and $(i_2 h, j_2 h)$ generate subgroups. |
| $public\_key.bipoint\_twistgen$ | $(i_2 h, j_2 h)$ | Subgroups are cyclic, associated groups are not. |
| $bipoint\_pi\_1\_chiffre$ | $\pi_1(bu + u_1)$ | |
| $bipoint\_pi\_2\_chiffre$ | $\pi_2(bv + v_1)$ | |
| $quadripoint\_pi\_T\_chiffre$ | $\pi_T(\beta)$ | $\beta \in \mu_r^4$ (part of a level-2 ciphertext) |
| $chiffre\_produit$ | $\mathrm{Enc}(a_1 a_2)$ | |