Chosen ciphertext attack on ZHFE

Yasufumi Hashimoto

Abstract

HFE (Patarin, Eurocrypt’96) is one of the most famous multivariate public key cryptosystems. Unfortunately, HFE has a serious trade-off between security and efficiency, which lacks HFE’s practicality. Recently, Porras et al. proposed a new encryption scheme ZHFE at PQCrypto 2014. While its construction is similar to HFE, the security seems more than HFE. The present paper proposes a chosen ciphertext attack (CCA) on ZHFE. The CCA reduces the problem of recovering the univariate polynomial for decryption to the min-rank problem on HFE. Thus the CCA security of ZHFE is almost the same as the security of HFE against the min-rank attack.

Keywords

HFE, ZHFE, chosen ciphertext attack, multivariate public key cryptosystem (MPKC), post quantum cryptography

Research Activity Group

Algorithmic Number Theory and Its Applications

1. Introduction

Hidden Field Equation (HFE) [1] is one of the most famous public key cryptosystems whose public keys are sets of multivariate quadratic forms over finite fields. The quadratic forms in HFE are generated by a univariate polynomial over an extension field. It is known that both the decryption speed and the security of HFE highly depend on the degree of the univariate polynomial [2–7]. This causes a serious trade-off between efficiency and security, and then the original HFE has not been considered to be practical.

Recently, a new encryption scheme called ZHFE was proposed by Porras et al. at PQCrypto 2014 [8]. The quadratic forms in ZHFE are generated by two univariate polynomials over an extension field with a good relation. While its construction is similar to HFE, it has been considered that ZHFE is more secure than HFE against known attacks, e.g., the direct attacks, the min-rank attacks and the differential attacks [8–10].

The present paper proposes a new attack on ZHFE, a chosen ciphertext attack (CCA). The CCA security of ZHFE has been quite important for cryptosystems. In fact, Bleichenhacher showed that CCA can recover information of the plaintext of RSA PKCS #1 [11]. However, at the best of our knowledge, there have been few works on CCA security of multivariate public key cryptosystems. Our CCA on ZHFE is roughly described as follows. First, choose sufficiently many ciphertexts randomly and decrypt them. Next, recover a candidate of the univariate polynomials over an extension field used in the decryption process by using the plaintext-ciphertext pairs. After that, take a difference of its candidate and use the min-rank attack on its difference to recover the desired polynomial. Once such a polynomial is found, the attacker can recover plaintexts of arbitrary ciphertexts without the secret key. Since the “difference” is equivalent to a univariate polynomial on HFE, the complexity of our attack is almost the same as the complexity of the min-rank attack on HFE of similar size. This result means that the CCA security of ZHFE is almost the same as the security of HFE against the min-rank attack, and then ZHFE also has a serious trade-off between efficiency and security.

2. HFE

We first give a short survey on HFE [1]. Let $n, d \geq 1$ be integers, $k$ a finite field and $q := \# k$. Denote by $K$ an $n$-extension field of $k$. Define the polynomial map $G : K \to K$ by

$$G(X) = \sum_{0 \leq i \leq d} \alpha_i X^{q^i} + \sum_{0 \leq i \leq d} \beta_i X^{q^i} + \gamma,$$

where $\alpha_{ij}, \beta_i, \gamma \in K$. HFE is constructed as follows.

Secret key. Two invertible affine (or linear) maps $S, T : k^n \to k^n$ and the polynomial map $G : K \to K$ defined in (1).

Public key. The quadratic map

$$F := T \circ \phi^{-1} \circ G \circ \phi \circ S : k^n \to k^n,$$

where $\phi : k^n \to K$ is a one-to-one map.

Encryption. For a plaintext $p \in k^n$, the ciphertext is $c := F(p) \in k^n$.

Decryption. Compute $Y := \phi(T^{-1}(c)) \in K$ and find a solution $X \in K$ of the univariate polynomial equation $G(X) = Y$.

The plaintext is $p = S^{-1}(\phi^{-1}(X)) \in k^n$.

The univariate equation $G(X) = Y$ is solved usually by the Berlekamp algorithm with the complexity $O(D^3 +
$n D^2 \log q$ where $D$ is the degree of $G$ [12]. Since $D \leq 2q^d$, the value $q^d$ should not be large.

On the other hand, it has been known that, if $d$ is small, the Gröbner basis algorithm can recover the plaintext of HFE effectively [2]. In fact, the degree of regularity of the polynomial system $\{f_1(x) - y_1, \ldots, f_n(x) - y_n\}$ is bounded by $\frac{1}{2} (q - 1) \log_q (2q^d - 1) + 1 + 2 [5, 6].$

Furthermore, the min-rank attack is also available on HFE [4, 7]. Let $x = (x_1, \ldots, x_n)^t \in k^n$, $\{\theta_1, \ldots, \theta_n\}$ a basis of $K$ over $k$, $X := x_1 \theta_1 + \cdots + x_n \theta_n$, $X := (X, X^q, \ldots, X^{q^{n-1}})^t$ and $\Theta := \left( \theta_i^{q^{j-1}} \right)_{1 \leq i, j \leq n}$. Since

$$\Theta x = X,$$

it is easy to see that the one-to-one map $\phi : k^n \rightarrow K$ is given by $\Theta$. Then the quadratic forms $f_1(x), \ldots, f_n(x)$ in the public key is described by

$$F(x) = \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix} = T \Theta^{-1} \begin{pmatrix} G(\phi(Sx)) \\ G(\phi(Sx)^q) \\ \vdots \\ G(\phi(Sx)^{q^{n-1}}) \end{pmatrix}. \quad (3)$$

Recall (1) that the polynomial $G$ is expressed by

$$G(X) = X^t \left( ^{*d+1} \right) X + (\text{linear form of } X).$$

Thus there exist constants $\beta_1, \ldots, \beta_n \in K$ such that the rank of $\sum_{1 \leq i \leq n} \beta_i F_1$ is at most $d + 1$, where $F_1, \ldots, F_n$ are the coefficient matrices of $f_1(x), \ldots, f_n(x)$ and these constants give partial information of $T \Theta^{-1}$. The min-rank attack by Bettale et al. [7] uses this fact. Their approach is to generate a system of polynomial equations of $n$ variables and of degree at most $d + 2$ from the determinants of $(d + 2) \times (d + 2)$ minor matrices of $\sum_{1 \leq i \leq n} \beta_i F_1$ and to solve this system by the Gröbner basis algorithm. The complexity of this attack on HFE is estimated by $n^{d+2} w \ll n^{d+2} w$ under several conditions, where $2 \leq w \leq 3$ is the exponent of the Gaussian elimination [7].

As described above, both the decryption speed and the security of HFE are in exponential time of $d$, and then it has not been considered that the original HFE itself is a practical encryption scheme.

3. ZHFE

Next, we describe ZHFE [8]. Let $n, m, D, d \geq 1$ be integers with $m := 2n$ and $d := \lfloor \log_q D \rfloor$. Define three univariate polynomials $G_1, G_2, \Psi$ over $K$ such that $G_1(X), G_2(X)$ are quadratic forms of $X, X^q, \ldots, X^{q^{n-1}}$ and there exist constants $\alpha_{ij} \in K$ ($1 \leq i \leq 4, 1 \leq j \leq n$) such that

$$\Psi(X) := X \cdot \left( \sum_{1 \leq i \leq n} \left( \alpha_{1j} G_1(X)^{q^{i-1}} + \alpha_{2j} G_2(X)^{q^{i-1}} \right) \right) + X^q \cdot \left( \sum_{1 \leq i \leq n} \left( \alpha_{3j} G_1(X)^{q^{i-1}} + \alpha_{4j} G_2(X)^{q^{i-1}} \right) \right)$$

is of degree at most $D$. Denote by $G : K \rightarrow K^2$ the polynomial map with $G(X) := (G_1(X), G_2(X))$. The encryption scheme ZHFE [8] is constructed as follows.

**Secret key.** The polynomials $\Psi, G_1, G_2$, the constants $\{\alpha_{ij}\}$ and two invertible affine maps $S : k^n \rightarrow k^n$, $T : k^m \rightarrow k^m$.

**Public key.** The quadratic map

$$F := T \circ \phi_2^{-1} \circ G \circ \phi \circ S : k^n \rightarrow k^m,$$

where $\phi_2 : k^m \rightarrow K^2$ is a one-to-one map.

**Encryption.** For a plaintext $p \in k^n$, the ciphertext is $c := F(p) \in k^m$.

**Decryption.** Let $(Y_1, Y_2) := \phi_2(T^{-1}(c)) \in K^2$. Find a non-trivial solution $X \in K$ of the univariate polynomial equation

$$\Psi(X, (Y_1, Y_2)) := \psi(X) - X \cdot \left( \sum_{1 \leq i \leq n} \left( \alpha_{1j} Y_1^{q^{i-1}} + \alpha_{2j} Y_2^{q^{i-1}} \right) \right)$$

$$- X^q \cdot \left( \sum_{1 \leq i \leq n} \left( \alpha_{3j} Y_1^{q^{i-1}} + \alpha_{4j} Y_2^{q^{i-1}} \right) \right) = 0$$

(7)

degree of at most $D$, where the constants $\alpha_{ij} \in K$ are given in (4). Output $x = S^{-1}(\phi^{-1}(X)) \in k^n$ as the plaintext.

Since $\Psi(X, (Y_1, Y_2))$ is a linear combination of

$$\left\{ X \cdot (G_1(X) - Y_1)^{q^i}, X \cdot (G_2(X) - Y_2)^{q^i}, \right\}_{0 \leq i \leq n-1},$$

the equation $\Psi(X, (Y_1, Y_2)) = 0$ has a solution if $G_1(X) = Y_1$ and $G_2(X) = Y_2$. Then at least one of solutions of the equation $\Psi(X, (Y_1, Y_2)) = 0$ gives the correct plaintext. Similar to HFE, the complexity of the decryption for ZHFE is $O(D^3 + n D^2 \log q)$, which means that $D$ cannot be too large also for ZHFE.

The security of ZHFE against known attacks has been studied in [8-10]. Based on these works, we can consider that ZHFE is more secure than HFE of similar size against the direct attacks, the min-rank attack and the differential attacks.

4. Chosen ciphertext attack on ZHFE

In this section, we propose a chosen ciphertext attack on ZHFE. The aim in this attack is to recover an invertible affine map $S' : k^n \rightarrow k^n$ and a polynomial in the form

$$\Phi(X, (Y_1, Y_2))$$
Choose sufficiently many ciphertexts $y_1, \ldots, y_N \in k^m$ randomly and try to decrypt them. If $y_1, \ldots, y_L \in \{y_1, \ldots, y_N\}$ are successfully decrypted, we denote by $\tilde{y}_i := y_i$ and $x_i \in k^n$ the "plaintext" corresponding to $\tilde{y}_i$. For $y \in k^m$, the decryption is by solving the univariate polynomial equation $X, \phi_2(T(y)) = 0$. It has a non-trivial solution with non-negligible probability even if $y \notin F(k^n)$. Note that its probability is experimentally around 1/3.

**Step 1.** Choose sufficiently many "ciphertexts" $y_1, \ldots, y_N \in k^m$ randomly and try to decrypt them. If $y_1, \ldots, y_{L'} \in \{y_1, \ldots, y_N\}$ are successfully decrypted, we denote by $\tilde{y}_i := y_i$ and $x_i \in k^n$ the "plaintext" corresponding to $\tilde{y}_i$. For $y \in k^m$, the decryption is by solving the univariate polynomial equation $X, \phi_2(T(y)) = 0$. It has a non-trivial solution with non-negligible probability even if $y \notin F(k^n)$. Note that its probability is experimentally around 1/3.

**Step 2.** Define the map $F(X) = (F_1(X), F_2(X))$ by $F := \phi_2 \circ F \circ \phi^{-1} : k \rightarrow k^2$. Find $a_{1ij}, a_{2ij}, b_{1i}, b_{2i} \in k$ $(1 \leq i, j \leq n)$ such that the polynomial

$$
\hat{\Phi}(X, \langle Y \rangle)
= \sum_{0 \leq i, j \leq n-1} a_{1ij}F_1(X)Y_i^j + \sum_{0 \leq i, j \leq n-1} a_{2ij}F_2(X)Y_i^j
+ \sum_{0 \leq i \leq n-1} b_{1i}(F_1(X) - Y_i)^j + b_{2i}(F_2(X) - Y_i)^j
$$

satisfies

$$
\hat{\Phi}(\phi(x), \phi(y)) = 0
$$

for any $1 \leq i, j \leq L$.

Recall that the pair $(x_i, \tilde{y}_i)$ satisfies $\Psi(\phi(S(x_i)), \phi\left(T^{-1}(\tilde{y}_i)\right)) = 0$. The equation (2) tells us that the following relations hold for $Z := \phi(x), \langle Y \rangle := \phi_2(\tilde{y}_i), U := \phi(S(x_i)), \langle V \rangle := \phi_2(T^{-1}(\tilde{y}_i))$, $G(X)$ and $F_i(X)$,

$$
\left(U, U^q, \ldots, U^{q^{n-1}}\right)^t = \Theta S\Theta^{-1}\left(Z, Z^q, \ldots, Z^{q^{n-1}}\right)^t,
$$

$$
\left(V, V^q, \ldots, V^{q^{n-1}}\right)^t = \Theta T\Theta^{-1}\left(Y_1, Y_2, Y_1^q, \ldots, Y_2^{q^{n-1}}\right)^t,
$$

$$
\left(G_1(X), G_2(X), G_1(X)^q, \ldots, G_2(X)^{q^{n-1}}\right)^t = \Theta T\Theta^{-1}\left(Y_1, Y_2, Y_1^q, \ldots, Y_2^{q^{n-1}}\right)^t,
$$

where $\Theta_x := \Theta \otimes I_3$. Applying (8) into the definition (5) of $\hat{\Psi}$, we see that $(x_i, \tilde{y}_i)$ satisfies $\hat{\Phi}(\phi(x), \phi(y)) = 0$ for some $a_{1ij}, a_{2ij}, b_{1i}, b_{2i} \in k$. Then the polynomial $\hat{\Phi}$ is a candidate of $\Phi$ to be recovered.

Since the number of $\{a_{1ij}, a_{2ij}, b_{1i}, b_{2i}\}$ is $2n^2 + 2n$ and the probability that $y_i$ is successfully decrypted is about $1/3$, we need $L \gg 2n^2$ and $N \gg 6n^2$. Thus the complexity of Step 1 is $N \cdot O(D^n + nD^2 \log q) = O(n^2 D^n + n^2 D^2 \log q)$ and that of Step 2 is $L^n = O(n^2W)$.

Remark. That $\hat{\Phi}(X, \langle Y \rangle)$ does not necessarily coincide with $\Psi(\phi \circ S \circ \phi^{-1})(X)$, $(\phi_2 \circ T^{-1} \circ \phi_2^{-1})(Y)$ since, if the equation $\Psi(\phi(S(x_i)), \phi_2(T^{-1}(\tilde{y}_i)) = 0$ holds, $\Psi(\phi(S(x_i)), \phi_2(T^{-1}(\tilde{y}_i))^q = 0$ simultaneously holds for $0 \leq i \leq n-1$. Then $\Phi(X, \langle Y \rangle)$ is a linear combination of $n$ polynomials

$$
\left\{ \Psi(\phi \circ S \circ \phi^{-1})(X), (\phi_2 \circ T^{-1} \circ \phi_2^{-1})(Y)^q \right\},
$$

$0 \leq i \leq n-1$.

To recover $\Psi$ itself, we need further tasks as given in Step 3-5.

We also remark that one can generate plaintext-ciphertext pairs $(x, y)$ by encrypting chosen plaintexts $x \in k^n$, not by decrypting chosen ciphertexts $y \in k^m$ as Step 1. However, if the attacker uses such pairs $(x, y) = (x, F(x))$, the equation (7) holds for arbitrary $a_{1ij}, a_{2ij}, b_{1i}, b_{2i}$ since $F_i(X) = Y_1, F_2(X) = Y_2$ hold for $X_1, \langle Y \rangle \in k$ corresponding to $x, y$. It is useless to recover the polynomial $\hat{\Phi}$ and then the attacker requires pairs $(x, y)$ derived from chosen ciphertexts.

**Step 3.** Choose a non-zero constant $C \in k$ and take a difference

$$
\Delta_C \hat{\Phi}(X, \langle Y \rangle) := \hat{\Phi}(X+C, \langle Y \rangle) - \hat{\Phi}(X, \langle Y \rangle).
$$

Denote by $H_1, \ldots, H_{n-1}$ the $n \times n$ matrices with $K$-entries such that

$$
\Delta_C \hat{\Phi}(X, \langle Y \rangle)^q = X^t H_i X + \text{(linear form of } X).
$$

Since the polynomial $\hat{\Phi}(X, \langle Y \rangle)$ is a linear combination of

$$
\left\{ \Psi(\phi \circ S \circ \phi^{-1})(X), (\phi_2 \circ T^{-1} \circ \phi_2^{-1})(Y)^q \right\},
$$

$0 \leq i \leq n-1$,

the difference $\Delta_C \hat{\Phi}(X, \langle Y \rangle)$ is a linear combination of

$$
\left\{ \Delta_C \Psi(\phi \circ S \circ \phi^{-1})(X), (\phi_2 \circ T^{-1} \circ \phi_2^{-1})(Y)^q \right\},
$$

$0 \leq i \leq n-1$.

Recall that $\hat{\Phi}$ and $\hat{\Psi}$ are cubic forms of $X$. This fact is inconvenient for the next step. On the other hand, choosing a constant $C \in K \setminus \{0\}$ and taking a difference $\Delta_C \hat{\Phi}$, the attacker obtains quadratic forms of $X$ and their coefficient matrices $H_i$. These matrices are useful for the attacker.

**Step 4.** Find $u_0, \ldots, u_{n-1} \in K$ such that the rank of $W := \sum_{0 \leq i \leq n-1} u_i H_i$ is at most $d + 1$.

Since $\Psi(X, \langle Y \rangle)$ is a cubic form of $X = (X, X^q,$
expressed by of HFE and then is equivalent to a public key of HFE. Thus we can find such that and the polynomial \( S(w, ) = \sum_{i=0}^{d-1} u_i \Phi(X, Y_i)^q \).

Since the polynomial \( S(w, ) \) is not large, the leading term of this polynomial is \( 0 \cdot D^{q(d+2)} \). The total complexity of our attack is \( O(n^2 D^3 + n^3 D^3 \log q + (q+1)D^2) = O(n^2 q^{d+2} + n^3 q^{d+2} + n^{d+2}q^d) \). Since \( q^d \) is not large, the leading term of this attack is \( 0(n^2 q^{d+2}) \), which is almost the same as the complexity of the min-rank attack on HFE of similar size.

Since the polynomial \( \Phi((o \circ S') \circ o^{-1})(X, Y_i, Y_j) \) is of degree at most \( D \), the attacker can decrypt a given ciphertext easily.

\[ \Delta_c \Psi(X, Y_1, Y_2) = X^{t(q+1)} X + (\text{linear form of } X, Y_1, Y_2). \]

This means that \( \Delta_c \Psi \) is equivalent to a core polynomial \( G \) of HFE and then \( \Phi \) is equivalent to a public key of HFE. Thus we can find \( u_0, \ldots, u_{n-1} \in X \) by the min-rank attack with the complexity \( (n+2)(d+2)^\omega \).

**Step 5.** Find an invertible \( n \times n \) matrix \( S' \) with \( k \)-entries such that

\[
(\Theta S' \Theta^{-1})^t W(\Theta S' \Theta^{-1}) = \begin{pmatrix} *_{d+1} \\ \end{pmatrix}
\]

Output \( S' \) and the polynomial

\[
\Phi(X, Y_1, Y_2) := \sum_{0 \leq i \leq n-1} u_i \Phi(X, Y_i)^q.
\]

Once the attacker gets \( u_0, \ldots, u_{n-1} \), he/she can find \( S' \) by a similar approach proposed in [4,7] for HFE. We thus conclude that \( \Phi \) is the polynomial to be recovered in our attack and the total complexity of our attack is \( O(n^2 D^3 + n^3 D^3 \log q + (n+2)(d+2)^\omega) = O(n^2 q^{d+2} + n^3 q^{d+2} + n^{d+2}q^d) \). Since \( q^d \) is not large, the leading term of this attack is \( 0(n^2 q^{d+2}) \), which is almost the same as the complexity of the min-rank attack on HFE of similar size.

Since the polynomial \( \Phi((o \circ S') \circ o^{-1})(X, Y_1, Y_2) \) is of degree at most \( D \), the attacker can decrypt a given ciphertext easily.

### 5. Experiments

We implemented our attack by using Magma [13] ver.2.22-3 on Windows 8.1, Core(TM) i7-4800MQ, 2.70GHz, and succeeded to recover equivalent keys for small \( n \). Table 1 describes the running times for \( (q, D) = (3, 21), (5, 55) \) and \( (q, D) = (7, 105) \). In this table, “Total” means the total running times of our attack and “MR” means the running times of the min-rank phase (Step 4). Remark that, when \( n \) is small, the ratio MR/Total is small. However, MR will grow rapidly and the ratio will be close to 1 for large \( n \).

### 6. Conclusion

ZHFE is a new multivariate encryption scheme, and had been considered to be more secure than HFE [8-10]. However, by using sufficiently many pairs of plaintext-ciphertext given from randomly chosen “ciphertexts”, the attacker can reduce the problem of recovering a polynomial equivalent to \( \Psi \) to the problem of recovering an equivalent secret key of HFE. Then the CCA security of ZHFE is similar to the security of HFE against the min-rank attack, which means that ZHFE also has a serious trade-off between efficiency and security similar to HFE. We thus cannot recommend ZHFE as a practical encryption scheme.

### Acknowledgment

The author would like to thank the anonymous reviewer for reading the previous manuscript carefully and giving helpful comments. He was supported by CREST, JST and JSPS Grant-in-Aid for Young Scientists (B) no. 26800020.

### References

[1] J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, LNCS, Vol. 1070, pp.33–48, Springer-Verlag, Berlin, 1997.
[2] J.C. Faugère and A. Joux, Algebraic cryptanalysis of Hidden Field Equations (HFE) using Grobner bases, LNCS, Vol. 2729, pp.44–60, Springer-Verlag, Berlin, 2003.
[3] J.C. Faugère, A new efficient algorithm for computing Grobner bases \((F_1)\), J. Pure Appl. Alg., 139 (1999), 61–88.
[4] A. Kipnis and A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, LNCS, Vol. 1666, pp.19–30, Springer-Verlag, Berlin, 1999.
[5] L. Granboulan, A. Jou and J. Stern, Inverting HFE is quasipolynomial, LNCS, Vol. 4117, pp.345–356, Springer-Verlag, Berlin, 2006.
[6] J. Ding and T. J. Hodges, Inverting HFE systems is quasipolynomial for all fields, LNCS, Vol. 6841, pp.724–742, Springer-Verlag, Berlin, 2011.
[7] L. Bettale, J.C. Faugère and L. Perret, Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic, Design. Code. Cryptogr., 69 (2013), 1–52.

### Table 1. Experiments of our attack.

| \( q \) | \( D \) | \( n \) | \( m \) | Total (MR) |
|-----|-----|-----|-----|-----------|
| 3   | 21  | 10  | 20  | 2.81s (2.81s) |
| 3   | 21  | 11  | 22  | 6.73s (6.27s) |
| 3   | 21  | 12  | 24  | 11.9s (11.1s) |
| 3   | 21  | 13  | 26  | 29.6s (21.4s) |
| 3   | 21  | 14  | 28  | 45.5s (37.3s) |
| 3   | 21  | 15  | 30  | 79.2s (66.0s) |
| 5   | 55  | 9   | 18  | 21.6s (1.64s) |
| 5   | 55  | 10  | 20  | 21.9s (3.32s) |
| 5   | 55  | 11  | 22  | 76.6s (7.98s) |
| 5   | 55  | 12  | 24  | 41.7s (13.4s) |
| 5   | 55  | 13  | 26  | 144.2s (13.4s) |
| 5   | 55  | 14  | 28  | 90.3s (44.7s) |
| 5   | 55  | 15  | 30  | 160.0s (75.9s) |
| 7   | 105 | 8   | 16  | 60.5s (0.81s) |
| 7   | 105 | 9   | 18  | 108s (1.80s) |
| 7   | 105 | 10  | 20  | 122s (4.52s) |
| 7   | 105 | 11  | 22  | 289s (5.35s) |
| 7   | 105 | 12  | 24  | 177s (14.9s) |
| 7   | 105 | 13  | 26  | 488s (28.8s) |
| 7   | 105 | 14  | 28  | 299s (46.0s) |
| 7   | 105 | 15  | 30  | 450s (80.6s) |