A Brief Retrospective Look at the Cayley-Purser Public-key Cryptosystem, 19 Years Later

Douglas R. Stinson

David R. Cheriton School of Computer Science
University of Waterloo

49th Southeastern Conference
Boca Raton, March 5–9, 2018

Background

- When she was only 16 years of age, Sarah Flannery won the EU Young Scientist of the Year Award for 1999.
- Her project consisted of a proposal of a public-key cryptosystem based on 2 by 2 matrices with entries from $\mathbb{Z}_n$, where n is the product of two distinct primes p and q.
- She named the cryptosystem as the Cayley-Purser algorithm.
- Because this algorithm was faster than the famous RSA public-key cryptosystem, it garnered an incredible amount of press coverage in January 1999.
- However, at the time of this press coverage, the algorithm had not undergone any kind of serious peer review.
- The Cayley-Purser algorithm was shown to be insecure, as reported by Bruce Schneier in December, 1999.
- Ms Flannery later wrote an interesting book, entitled In Code: A Mathematical Journey [1], which recounts her experiences relating to her work on this cryptosystem.

Press Coverage

- On January 13, 1999, the BBC News published an article entitled "Teenager's email code is a cracker."

  This report led to world-wide news coverage.

- "She has also proven that her code is as secure as RSA," says Dr. Flannery (her father). "It wouldn't be worth a hat of straw if it was not."

  This is a quote from the BBC article. Unfortunately, the cryptosystem turned out not to be secure.

- "She knows what she's talking about," said Ronald Rivest. "But there's not enough information to evaluate her work." (ZDNet, January 20, 1999.)

  Like virtually everything Ron says, this was an eminently sensible statement.

Press Coverage (cont.)

- "Who is the authoritative voice which is attesting to this breakthrough?" asked D. James Bidzos, president of RSA Data Security (ZDNet, January 20, 1999).

  One of the early sceptical voices.

- Bruce Schneier, on Dec. 15, 1999, reported: "Flannery's paper, describing the Cayley-Purser algorithm, has been published on the Internet by an unknown source. It's interesting work, but it's not secure. Flannery herself publishes a break of the algorithm in an appendix."

  This is the earliest report (of which I am aware) of a publicly available description of the cryptosystem and its cryptanalysis.

Cayley-Purser Algorithm: Setup

- Let $n = pq$, where p and q are large distinct primes.
- $\mathbb{GL}(2, n)$ denotes the 2 by 2 invertible matrices with entries from $\mathbb{Z}_n$.
- Let $\boldsymbol{A}, \boldsymbol{C} \in \mathbb{GL}(2, n)$ be chosen such that $\boldsymbol{AC} \neq \boldsymbol{CA}$.
- Define $\boldsymbol{B} = \boldsymbol{C}^{-1}\boldsymbol{A}^{-1}\boldsymbol{C}$.
- Then choose a secret, random positive integer r and let $\boldsymbol{G} = \boldsymbol{C}^r$.

The public key consists of $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{G}, \boldsymbol{n}$.

The private key consists of $\boldsymbol{C}, \boldsymbol{p}, \boldsymbol{q}$.

Cayley-Purser Algorithm: Encryption

Let $\boldsymbol{X} \in \mathbb{GL}(2, n)$ be the plaintext to be encrypted. The following computations are performed:

1. choose a secret, random positive integer s
2. compute $D = \boldsymbol{G}^s$
3. compute $\boldsymbol{E} = D^{-1}\boldsymbol{A}D$
4. compute $K = D^{-1}\boldsymbol{B}D$
5. compute $\boldsymbol{Y} = K\boldsymbol{X}K$
6. the ciphertext is $(\boldsymbol{E}, \boldsymbol{Y})$.

Cayley-Purser Algorithm: Decryption

Let $(\boldsymbol{E}, \boldsymbol{Y}) \in \mathbb{GL}(2, n) \times \mathbb{GL}(2, n)$ be the ciphertext to be decrypted. The following computations are performed:

1. compute $L = \boldsymbol{C}^{-1}\boldsymbol{E}\boldsymbol{C}$ (note: $L = K^{-1}$)
2. compute $\boldsymbol{X} = L\boldsymbol{Y}L$

Important observation [1, p. 290]
Any scalar multiple of $\boldsymbol{C}$ can be used in place of $\boldsymbol{C}$ in the decryption process, because

$$(\mu\boldsymbol{C})^{-1}\boldsymbol{E}(\mu\boldsymbol{C}) = \boldsymbol{C}^{-1}\boldsymbol{E}\boldsymbol{C} = L. \tag{1}$$

Linear Algebra Attack

- This is apparently a new attack.
- We make use of the following two equations involving C:

$$CB = A^{-1}C \tag{2}$$

and

$$CG = GC \tag{3}$$

- Equation (2) follows from the formula $B = C^{-1}A^{-1}C$.
- Equation (3) holds because G is a power of C and hence G and C commute.

Linear Algebra Attack (cont.)

- Let the private key $\boldsymbol{C}$ be written as

$$\boldsymbol{C} = \begin{pmatrix} \boldsymbol{a} & \boldsymbol{b} \\ \boldsymbol{c} & \boldsymbol{d} \end{pmatrix}, \tag{4}$$

  where the unknowns $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d} \in \mathbb{Z}_n$.
- Then (2) and (3) each yield four homogeneous linear equations (in $\mathbb{Z}_n$) in the four unknowns $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}$.
- The solution space of (2) is a 2-dimensional subspace of $(\mathbb{Z}_n)^4$, as is the solution space of (3).
- However, when we solve all eight equations simultaneously, we get precisely the scalar multiples of $\boldsymbol{C}$ (i.e., the solution space for $\boldsymbol{C}$ is a 1-dimensional subspace of $(\mathbb{Z}_n)^4$).

Toy Example

Suppose $p = 193$ and $q = 149$, so $n = 28757$. Suppose we define

$$\boldsymbol{A} = \begin{pmatrix} 16807 & 19399 \\ 7483 & 18143 \end{pmatrix}$$

and

$$\boldsymbol{C} = \begin{pmatrix} 2910 & 1657 \\ 5341 & 24803 \end{pmatrix}.$$

Then

$$\boldsymbol{B} = \begin{pmatrix} 11947 & 1712 \\ 4630 & 14946 \end{pmatrix}.$$

Finally, suppose $\boldsymbol{G} = \boldsymbol{C}^7$; then

$$\boldsymbol{G} = \begin{pmatrix} 1438 & 1433 \\ 20759 & 24068 \end{pmatrix}.$$

Toy Example (cont.)

The system of linear equation to be solved is

$$\left(\begin{array}{cccc} 24034 & 4630 & 19287 & 0 \\ 1712 & 27033 & 0 & 19287 \\ 9570 & 0 & 1724 & 4630 \\ 0 & 9570 & 1712 & 4723 \\ \hline 0 & 20759 & 27324 & 0 \\ 1433 & 22630 & 0 & 27324 \\ 7998 & 0 & 6127 & 20759 \\ 0 & 7998 & 1433 & 0 \end{array}\right) \left(\begin{array}{c} \boldsymbol{a} \\ \boldsymbol{b} \\ \boldsymbol{c} \\ \boldsymbol{d} \end{array}\right) = \left(\begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \end{array}\right).$$

The solution to this system is

$$(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}) = \mu(28365, 13928, 25231, 28756),$$

$\mu \in \mathbb{Z}_n$. It is straightforward to verify that this solution space indeed consists of all the scalar multiples of $\boldsymbol{C}$.

Cayley-Hamilton Attack

- This attack was presented in [1, pp. 290–292].
- The Cayley-Hamilton theorem states that every square matrix over a commutative ring satisfies its own characteristic polynomial.
- For 2 by 2 matrices, the characteristic polynomial is quadratic and it follows that any power of $\boldsymbol{G}$ can can be expressed as a linear combination of $\boldsymbol{G}$ and I_2.
- $\boldsymbol{C}$ is a power of $\boldsymbol{G}$, so $\boldsymbol{C} = \boldsymbol{\alpha} I_2 + \boldsymbol{\beta} \boldsymbol{G}$, for scalars $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$.
- Since we only have to determine $\boldsymbol{C}$ up to a scalar multiple, we can WLOG take $\boldsymbol{\beta} = 1$, and write $\boldsymbol{C} = \boldsymbol{\alpha} I_2 + \boldsymbol{G}$.

Cayley-Hamilton Attack (cont.)

- Suppose we substitute this expression for $\boldsymbol{C}$ into (2).
- Then we obtain

$$(\boldsymbol{\alpha} I_2 + \boldsymbol{G})\boldsymbol{B} = \boldsymbol{A}^{-1}(\boldsymbol{\alpha} I_2 + \boldsymbol{G}).$$

- Rearranging, we have

$$\boldsymbol{\alpha}(\boldsymbol{B} - \boldsymbol{A}^{-1}) = \boldsymbol{A}^{-1}\boldsymbol{G} - \boldsymbol{G}\boldsymbol{B}.$$

- If we compute the two matrices $\boldsymbol{B} - \boldsymbol{A}^{-1}$ and $\boldsymbol{A}^{-1}\boldsymbol{G} - \boldsymbol{G}\boldsymbol{B}$, we can compare any two corresponding nonzero entries of these two matrices to determine $\boldsymbol{\alpha}$.

Toy Example

We use the same parameters as in the previous example. First we compute

$$\boldsymbol{B} - \boldsymbol{A}^{-1} = \begin{pmatrix} 24034 & 20999 \\ 14200 & 4723 \end{pmatrix}.$$

and

$$\boldsymbol{A}^{-1}\boldsymbol{G} - \boldsymbol{G}\boldsymbol{B} = \begin{pmatrix} 17977 & 4614 \\ 25427 & 10780 \end{pmatrix}.$$

From this, we see that

$$28534(\boldsymbol{B} - \boldsymbol{A}^{-1}) = \boldsymbol{A}^{-1}\boldsymbol{G} - \boldsymbol{G}\boldsymbol{B}.$$

Hence, $\boldsymbol{\alpha} = 28534$ and

$$28534 I_2 + \boldsymbol{G} = \begin{pmatrix} 1215 & 1433 \\ 20759 & 23845 \end{pmatrix}$$

should be a multiple of $\boldsymbol{C}$. In fact, it can be verified that

$$\begin{pmatrix} 1215 & 1433 \\ 20759 & 23845 \end{pmatrix} = 5485\boldsymbol{C}.$$

Slavin's Public-Key Cryptosystem

Keith Slavin patented a modified version of Cayley-Purser in 2008.

	Cayley-Purser	Slavin
setup	$\boldsymbol{B} = \boldsymbol{C}^{-1}\boldsymbol{A}^{-1}\boldsymbol{C}$ $\boldsymbol{G} = \boldsymbol{C}^{r}$	$\boldsymbol{B} = \boldsymbol{C}\boldsymbol{A}\boldsymbol{C}$ $\boldsymbol{G} = \boldsymbol{C}^{r}$
encryption	$D = \boldsymbol{G}^{s}$ $\boldsymbol{E} = D^{-1}\boldsymbol{A}D$ $K = D^{-1}\boldsymbol{B}D$ $\boldsymbol{Y} = K\boldsymbol{X}K$ the ciphertext is $(\boldsymbol{E}, \boldsymbol{Y})$	$D = \boldsymbol{G}^{s}$ $E = D\boldsymbol{A}D$ $K = D\boldsymbol{B}D$ $\boldsymbol{Y} = e_K(\boldsymbol{X})$ the ciphertext is $(\boldsymbol{E}, \boldsymbol{Y})$
decryption	$K^{-1} = \boldsymbol{C}^{-1}\boldsymbol{E}\boldsymbol{C}$ $\boldsymbol{X} = K^{-1}\boldsymbol{Y}K^{-1}$	$K = \boldsymbol{C}\boldsymbol{E}\boldsymbol{C}$ $\boldsymbol{X} = d_K(\boldsymbol{Y})$

In Slavin's cryptosystem, it does not suffice to compute a scalar multiple of $\boldsymbol{C}$ to determine K.

An Attack

Slavin makes the following observation in his patent [2].

Lemma 1
Define $M = \boldsymbol{BGB}^{-1}$ *and* $N = \boldsymbol{AGA}^{-1}$. *Then* $M = \boldsymbol{C}N\boldsymbol{C}^{-1}$.

- By using the linear algebra attack or the Cayley-Hamilton attack, it is possible to compute a scalar multiple C' of the unknown matrix $\boldsymbol{C}$.
- Thus we can write $\boldsymbol{C} = \boldsymbol{\mu}C'$ for some unknown value $\boldsymbol{\mu} \in {\mathbb{Z}_n}^*$.
- From the equation $\boldsymbol{B} = \boldsymbol{CAC}$, we obtain $\boldsymbol{B} = \boldsymbol{\mu}^2 C'\boldsymbol{A}C'$.
- Since C' is a known matrix, we can compute the value of $\boldsymbol{\mu}^2$.
- It is infeasible to compute $\boldsymbol{\mu}$, but it doesn't matter!
- From the equation $K = \boldsymbol{CEC}$, we obtain $K = \boldsymbol{\mu}^2 C'\boldsymbol{E}C'$, so we can compute K and then decrypt the ciphertext $(\boldsymbol{E}, \boldsymbol{Y})$.

References

[1] Sarah Flannery with David Flannery. **In Code: A Mathematical Journey.** Workman Publishing Company, 2001.

[2] Keith R. Slavin. **Public Key Cryptography Using Matrices.** United States Patent No. US 7,346,162 B2. March 18, 2008.

Thank You For Your Attention!