

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG



ĐỒ ÁN TỐT NGHIỆP
NGÀNH KHOA HỌC MÁY TÍNH

Cài đặt bảo mật cho các thiết bị IoT

Sinh viên thực hiện:

Đặng Quang Trung 20134145 CNTT2.03-K58

Giảng viên:

TS. Trần Vĩnh Đức

Hà Nội 21-04-2018

Lời cảm ơn

Trước khi trình bày nội dung của đề án này, tôi xin được gửi lời cảm ơn sâu sắc và chân thành nhất đến TS. Trần Vĩnh Đức, người đã tận tình hướng dẫn tôi trong suốt quá trình thực hiện đề án này cũng như những năm tháng học tại trường Đại học Bách Khoa Hà Nội. Đồng thời tôi cũng xin bày tỏ lòng biết ơn đến các thầy cô trường Đại học Bách Khoa Hà Nội, Viện công nghệ thông tin và truyền thông, đặc biệt là các thầy cô bộ môn Khoa học máy tính đã tận tình chỉ dạy cho tôi trong những năm tháng học tập ở trường.

Đồng thời tôi xin gửi lời cảm ơn đến gia đình, bạn bè đã luôn ở bên tôi, động viên và giúp đỡ tôi trong suốt quá trình học tập và thực hiện đề án tốt nghiệp.

Mục lục

Lời cảm ơn	1
Danh sách hình vẽ	5
Mở đầu	5
1 Cơ sở lý thuyết	7
1.1 Cơ sở mật mã	7
1.2 Mật mã khóa đối xứng	8
1.3 Mật mã khóa công khai	9
1.4 Chữ ký điện tử và Hàm băm	12
1.5 Hệ thống chứng thực và Chứng thư số	17
2 Mật mã dựa trên đường cong Elliptic	20
2.1 Lý thuyết số	20
2.2 Đường cong Elliptic	21
2.3 Mật mã dựa trên đường cong Elliptic	32
3 Chứng thư số ẩn dựa trên đường cong Elliptic	36
3.1 Hàm băm	36
3.2 Hàm băm một số nguyên modul n	37
3.3 Khởi tạo một số ngẫu nhiên	37
3.4 Các tham số khởi tạo và hợp lệ	37
3.5 Sơ đồ chứng thư số thực ECQV	37
3.5.1 Tổng quan	37
3.5.2	38
4 Cài đặt cho thiết bị IoT	39
Tài liệu tham khảo	41

Bảng chữ viết tắt

Danh sách hình vẽ

2.1	Hai ví dụ minh họa về đường cong elliptic	22
2.2	Luật cộng trên đường cong elliptic	22
2.3	Cộng điểm P với chính nó	24
2.4	Đường thẳng đứng L đi qua $P = (a, b)$ và $P' = (a, -b)$	25
2.5	33
2.6	34
2.7	35
3.1	38

Giới thiệu chung

Mật mã học là một lĩnh vực liên quan với các kỹ thuật ngôn ngữ và toán học để đảm bảo an toàn thông tin, cụ thể là trong thông tin liên lạc. Về phương diện lịch sử, mật mã học gắn liền với quá trình mã hóa, điều này có nghĩa là nó gắn với các cách thức để chuyển đổi thông tin từ dạng này sang dạng khác nhưng ở đây là từ dạng thông thường có thể nhận thức được thành dạng không thể nhận thức được, làm cho thông tin trở thành dạng không thể đọc được nếu như không có các kiến thức bí mật. Quá trình mã hóa được sử dụng chủ yếu để đảm bảo tính bí mật của các thông tin quan trọng, chẳng hạn trong công tác tình báo, quân sự hay ngoại giao cũng như các bí mật về kinh tế, thương mại. Trong những năm gần đây, lĩnh vực hoạt động của mật mã hóa đã được mở rộng: mật mã hóa hiện đại cung cấp cơ chế cho nhiều hoạt động hơn là chỉ duy nhất việc giữ bí mật và có một loạt các ứng dụng như: chứng thực khóa công khai, chữ ký số, bầu cử điện tử hay tiền điện tử. Ngoài ra, những người không có nhu cầu thiết yếu đặc biệt về tính bí mật cũng sử dụng các công nghệ mật mã hóa, thông thường được thiết kế và tạo lập sẵn trong các cơ sở hạ tầng của công nghệ tính toán và liên lạc viễn thông.

Mật mã học là một lĩnh vực liên ngành, được tạo ra từ một số lĩnh vực khác. Các dạng cổ nhất của mật mã hóa chủ yếu liên quan với các kiểu mẫu trong ngôn ngữ. Gần đây thì tầm quan trọng đã thay đổi và mật mã hóa sử dụng và gắn liền nhiều hơn với toán học, cụ thể là toán học rời rạc, bao gồm các vấn đề liên quan đến lý thuyết số, lý thuyết thông tin, độ phức tạp tính toán, thống kê và tổ hợp. Mật mã hóa cũng được coi là một nhánh của công nghệ, nhưng nó được coi là không bình thường vì nó liên quan đến các sự chống đối ngầm (xem công nghệ mật mã hóa và công nghệ an ninh). Mật mã hóa là công cụ được sử dụng trong an ninh máy tính và mạng.

Hiện nay, cùng với sự phát triển của tính toán khắp nơi, các hệ thống vạn vật kết nối (internet of things - IoT) ngày càng thu hút được sự quan tâm của các chuyên gia cũng như các nhà ứng dụng. Vấn đề an toàn thông tin trong hệ thống IoT với các thiết bị nhỏ gọn, năng lực tính toán thấp, trở thành một chủ đề nóng hiện nay. Với khả năng tính nhanh, an toàn chi phí thấp, mật mã tính toán trên đường cong Elliptic tiêu biểu cho hệ mã trao đổi khóa của các thiết bị IoT.

Nội dung chính của đề án bao gồm 4 chương:

- **Chương 1:** Cơ sở lý thuyết
- **Chương 2:** Mật mã dựa trên đường cong Elliptic
- **Chương 3:** Chứng thư số ẩn dựa trên đường cong Elliptic
- **Chương 4:** Cài đặt cho thiết bị IoT

Chương 1

Cơ sở lý thuyết

Trong chương này sẽ trình bày cơ sở lý thuyết chung bao quát cho các hệ mật mã, nó sẽ cung cấp một số khái niệm và các kiến thức quý giá, hỗ trợ đắc lực cho việc làm quen với lĩnh vực này.

1.1 Cơ sở mật mã

Mật mã là một lĩnh vực khoa học chuyên nghiên cứu về các phương pháp và kỹ thuật đảm bảo an toàn và bảo mật trong truyền tin liên lạc với giả thiết sự tồn tại của các thể lực thù địch, những kẻ muốn ăn cắp thông tin để lợi dụng và phá hoại. Tên gọi trong tiếng Anh, Cryptology được dẫn giải nguồn gốc từ tiếng Hy Lạp, trong đó kryptos nghĩa là “che giấu”, logos nghĩa là “từ ngữ”.

Các nhà nghiên cứu lĩnh vực này quan tâm xây dựng hoặc phân tích (để chỉ ra điểm yếu) các giao thức mật mã (cryptographic protocols), tức là các phương thức giao dịch có đảm bảo mục tiêu an toàn cho các bên tham gia (với giả thiết môi trường có kẻ đối địch, phá hoại).

Ngành Mật mã (cryptology) thường được quan niệm như sự kết hợp của 2 lĩnh vực con:

1. Sinh, chế mã mật (cryptography): nghiên cứu các kỹ thuật toán học nhằm cung cấp các công cụ hay dịch vụ đảm bảo an toàn thông tin.
2. Phá giải mã (cryptanalysis): nghiên cứu các kỹ thuật toán học phục vụ phân tích phá mật mã và/hoặc tạo ra các đoạn mã giả nhằm đánh lừa bên nhận tin

Hai lĩnh vực con này tồn tại như hai mặt đối lập, "đấu tranh để cùng phát triển" của một thể thống nhất là ngành khoa học mật mã (cryptology).

Mặc dù mật mã có thể coi là một ngành toán học phát triển cao, đòi hỏi tư duy cao để nắm được các thành tựu hiện đại của nó, nhưng cơ sở xuất phát ban đầu của nó lại là một mô hình thực tiễn khá đơn giản như sau:

hình vẽ

Như vậy trong một hệ thống mật mã khái quát sẽ có các thành phần sau:

- **Văn bản trơ**(plaintext X): tức là thông điệp nguyên gốc chưa được mã hóa.

- **Văn bản mã hóa**(ciphertext Y): tức là thông điệp đã được mã hóa.
- **Thuật toán mã hóa**(enciphering algorithm $E_z(X)$): là các giao thức hoặc hướng dẫn có tác dụng chuyển đổi văn bản trờn thành văn bản mã hóa. Đối với các hệ thống mật mã truyền thống, chỉ có người gửi thông điệp biết được thuật toán mã hóa, tuy nhiên đối với các hệ thống dùng mật mã hóa khóa công khai (Public key code - PKC), tất cả mọi người đều có thể biết thuật toán mã hóa mà không ảnh hưởng tiêu cực đến an ninh của hệ thống.
- **Khóa mã hóa**(enciphering key Z): là một hoặc nhiều đối tượng (thường là các con số hay là các hướng dẫn quan trọng nào đó) được dùng trong việc mã hóa văn bản trờn. Ngoại trừ trong hệ thống PKC, để đảm bảo bí mật an toàn thì khóa mã hóa thường chỉ được người gửi biết.
- **Thuật toán giải mã**(deciphering algorithm $D_z(Y)$): là các giao thức hoặc hướng dẫn có tác dụng chuyển đổi văn bản mã hóa trở về văn bản trờn. Để đảm bảo bí mật, chỉ có người nhận thông điệp biết được thuật toán giải mã.
- **Khóa giải mã**(deciphering key Z'): là một hoặc nhiều đối tượng (thường là các con số hay là các hướng dẫn quan trọng nào đó) được dùng trong việc giải mã văn bản bị mã hóa. Để đảm bảo bí mật, chỉ có người nhận thông điệp biết được khóa giải mã.
- **Sản phẩm mật mã**(Cryptography Product): bao gồm các hệ thống thiết bị, module, mạch tích hợp và các chương trình phần mềm mã hoá chuyên dụng có tích hợp các thuật toán mật mã, được thiết kế, chế tạo để bảo vệ thông tin giao dịch điện tử và lưu trữ dưới dạng số hoá, trong đó sử dụng "Thuật toán mã đối xứng" hoặc "Thuật toán mã không đối xứng".

1.2 Mật mã khóa đối xứng

Trong mật mã học, các thuật toán khóa đối xứng (symmetric-key algorithms) là một lớp các thuật toán mật mã hóa trong đó các khóa dùng cho việc mật mã hóa và giải mã có quan hệ rõ ràng với nhau (có thể dễ dàng tìm được một khóa nếu biết khóa kia). Mã khóa loại này không công khai.

Khóa dùng để mã hóa có liên hệ một cách rõ ràng với khóa dùng để giải mã có nghĩa chúng có thể hoàn toàn giống nhau, hoặc chỉ khác nhau nhờ một biến đổi đơn giản giữa hai khóa. Trên thực tế, các khóa này đại diện cho một bí mật được phân hưởng bởi hai bên hoặc nhiều hơn và được sử dụng để giữ gìn sự bí mật trong kênh truyền thông tin.

Thuật toán đối xứng có thể được chia ra làm hai thể loại, mật mã dòng (stream ciphers) và mật mã khối (block ciphers). Mật mã dòng mã hóa từng bit của thông điệp trong khi mật mã khối gộp một số bit lại và mật mã hóa chúng như một đơn vị. Cỡ khối được dùng thường là các khối 64 bit(128 bit). Ngày nay được ưa chuộng sử dụng hơn là mật mã khối (block cipher) – trong đó từng khối nhiều ký tự được mã hóa cùng một lúc. Trong mật mã khối, các tham số quan trọng là kích thước (độ dài khối) và kích thước khóa. Các khái niệm này được minh họa qua ví dụ sau đây.

key	000	001	010	011	100	101	110	111
0	001	111	110	000	100	010	101	011
1	001	110	111	100	011	010	000	101
2	001	000	100	101	110	111	010	011
3	100	101	110	111	000	001	010	011
4	101	110	100	010	011	001	011	111

Qua ví dụ đơn giản này (chỉ có tính chất minh họa), ta thấy rằng nếu các tham số kích thước khối và khóa qua nhỏ thì mật mã rất dễ bị phá bằng các tấn công thông qua phân tích thống kê. Chẳng hạn trong ví dụ trên, nếu kẻ thù nhận được một khối mã ciphertext 001 thì nó có thể dễ dàng suy ra plaintext tương ứng chỉ có thể là 000 hoặc 101 (nhờ thống kê trên bảng biến đổi mã).

Vì vậy, các điều kiện cần cho mật mã khối an toàn là:

- Kích thước khối phải đủ lớn để chống lại các loại tấn công phá hoại bằng phương pháp thống kê. Tuy nhiên cần lưu ý rằng kích thước khối lớn sẽ làm thời gian trễ lớn.
- Không gian khóa phải đủ lớn (tức là chiều dài khóa phải đủ lớn) để chống lại tìm kiếm vét cạn. Tuy nhiên mật khác, khóa cần phải đủ ngắn để việc làm khóa, phân phối và lưu trữ được hiệu quả.

Về các nguyên lý thiết kế mật mã khối, người ta đã ghi nhận 2 nguyên tắc cơ sở sau để có bảo mật cao, đó là việc tạo ra confusion (tính hỗn loạn, rắc rối) và diffusion (tính khuếch tán).

Confusion. (Hỗn loạn, rắc rối) Sự phụ thuộc của bản mã đối với bản rõ phải thực phức tạp để gây rắc rối, cảm giác hỗn loạn đối với kẻ thù có ý định phân tích tìm qui luật để phá mã. Quan hệ hàm số của mã-tin là phi tuyến (non-linear).

Diffusion. (Khuếch tán) Làm khuếch tán những mẫu văn bản mang đặc tính thống kê (gây ra do dư thừa của ngôn ngữ) lẫn vào toàn bộ văn bản. Nhờ đó tạo ra khó khăn cho kẻ thù trong việc dò phá mã trên cơ sở thống kê các mẫu lặp lại cao. Sự thay đổi của một bit trong một khối bản rõ phải dẫn tới sự thay đổi hoàn toàn trong khối mã tạo ra.

Một cách đơn giản nhất, confusion có thể được thực hiện bằng phép thay thế (substitution) trong khi diffusion được tạo ra bằng các phép chuyển đổi chỗ (transposition/permutation) hay hoán vị. Toàn bộ sơ đồ biến đổi mật mã sẽ là một lưới các biến đổi thay thế-hoán vị (substitution-permutation network).

1.3 Mật mã khóa công khai

Giới thiệu

Mật mã hóa khóa công khai là một dạng mật mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa chung bí mật trước đó. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai và khóa cá nhân (hay khóa bí mật).

Trong hệ mã khóa công khai, mỗi người sử dụng có hai khóa, một được gọi là khóa bí mật (secret key hay private key) và một được gọi là khóa công khai (public key). Khóa

thứ nhất chỉ mình user biết và giữ bí mật, còn khoá thứ hai thì anh ta có thể tự do phổ biến công khai. Khoá thứ nhất thường đi liền với thuật toán giải mã, còn khoá thứ hai thường đi liền với thuật toán sinh mã, tuy nhiên điều đó không phải là bắt buộc. Ta hãy ký hiệu chúng là z (khóa riêng) và Z (khóa công khai)

Hoạt động của chúng là đối xứng

$$X = D(z, E(Z, X)) \quad (1.1)$$

$$X = E(Z, D(z, X)) \quad (1.2)$$

Trong đó hệ thức (1.1) biểu tượng cho bài toán truyền tin mật: bất kỳ người sử dụng nào khác như B, C, D ... muốn gửi tin cho A chỉ việc mã hoá thông tin với khoá công khai (Z_A) của A rồi gửi đi. Chỉ có A mới có thể khoá riêng để giải mã (z_A) và đọc được tin, kẻ nghe trộm Eve không thể giải mã để lấy được tin vì không có khoá z_A .

Còn hệ thức (1.2) sẽ được sử dụng để xây dựng các hệ chữ ký điện tử trong đó thao tác Ký chính là thực hiện $E(Z_A)$ còn kiểm định chữ ký là thông qua gọi $D(z_A)$.

Hệ mật mã theo nguyên tắc nói trên được gọi là hệ mã với khoá công khai (public key cryptosystems) hay còn được gọi là mã khóa phi đối xứng (asymmetric key cryptosystems). Ta sẽ viết tắt hệ thống kiểu này bằng PKC.

Hệ thống mật mã hóa khóa công khai có thể sử dụng với các mục đích:

- **Mã hóa:** giữ bí mật thông tin và chỉ có người có khóa bí mật mới giải mã được
- **Tạo chữ ký số:** cho phép kiểm tra một văn bản có phải đã được tạo với một khóa bí mật nào đó hay không.
- **Thỏa thuận khóa:** cho phép thiết lập khóa dùng để trao đổi thông tin mật giữa 2 bên.

Thông thường, các kỹ thuật mật mã hóa khóa công khai đòi hỏi khối lượng tính toán nhiều hơn các kỹ thuật mã hóa khóa đối xứng nhưng những lợi điểm mà chúng mang lại khiến cho chúng được áp dụng trong nhiều ứng dụng.

Hệ thống khóa công khai

RSA là hệ mật mã khóa công khai phổ biến và cũng đa năng nhất trong thực tế, phát minh bởi Rivest, Shamir & Adleman (1977). Nó là chuẩn mật mã bất thành văn đối với PKC, cung cấp đảm bảo tính mật, xác thực và chữ ký điện tử.

Cơ sở thuật toán RSA dựa trên tính khó của bài toán phân tích các số lớn ra thừa số nguyên tố: không tồn tại thuật toán thời gian đa thức (theo độ dài của biểu diễn nhị phân của số đó) cho bài toán này. Chẳng hạn, việc phân tích một hợp số là tích của 2 số nguyên tố lớn hàng trăm chữ số sẽ mất hàng ngàn năm tính toán với một máy PC trung bình có CPU khoảng trên 2Ghz.

Thuật toán RSA

Xây dựng: Chọn các tham số

1. Chọn hai số nguyên tố lớn p và q . Tính $n = p \times q$ và $m = \phi(n) = (p-1) \times (q-1)$.
2. Chọn e , $1 \leq e \leq m-1$, sao cho $\gcd(e, m) = 1$.
3. Tìm d sao cho $e \cdot d = 1 \pmod{m}$, tức là tính $d = e^{-1} \pmod{m}$, giải theo thuật toán gcd mở rộng.

Khoá công khai (Public key) là (e, n)

Khoá dùng riêng (Private key) là d, p, q

Giả sử X là một khối tin gốc (plaintext), Y là một khối mã tương ứng của X , và (z_A, Z_A) là các thành phần công khai và riêng của khoá của Alice

Sinh Mã. Nếu Bob muốn gửi một thông báo mã hoá cho Alice thì anh ta chỉ việc dùng khoá công khai của Alice để thực hiện:

$$Y = E_{Z_A}(X) = X^e \pmod{n}$$

Giải mã. Khi Alice muốn giải mã Y , cô ta chỉ việc dùng khoá riêng $z_A = d$ để thực hiện như sau:

$$D_{z_A}(Y) = Y^d \pmod{n}$$

Hệ Rabin

Hệ Rabin cũng xây dựng trên việc lấy $n = p \times q$ làm bí mật. N được coi là khoá công khai (PK) còn (p, q) là khoá bí mật (SK).

Mã hoá là việc thực hiện:

$$Y = X^2 \pmod{n}$$

còn giải mã là việc tính căn bậc hai:

$$X = \sqrt{Y} \pmod{n} \quad (1.3)$$

Có thể thấy, nếu biết $n = p \times q$ thì dễ dàng tìm được nghiệm cho phương trình này, còn nếu không thì việc tìm nghiệm là khó tương đương với bài toán PTTSNT số n .

Khi biết $N = p \times q$ thì 1.3 được giải ra có bốn nghiệm do đó để xác định được đâu là bản rõ gốc phải có mẹo để chọn được đúng giá trị cần thiết trong số 4 nghiệm đó

Hệ Rabin có một số ưu điểm so với RSA:

- Tính an toàn được chứng minh hoàn toàn tương đương với bài toán PTTSNT, nói cách khác tính ATBM của Rabin là có thể chứng minh được (provable)
- Ngoại trừ trường hợp RSA hoạt động với e nhỏ còn thuật toán sinh mã của Rabin nhanh hơn nhiều so với RSA là hệ đòi hỏi phải tính lũy thừa. Thời gian giải mã thì tương đương nhau.

Nhược điểm: Vì phương trình giải mã cho 4 nghiệm nên làm khó dễ việc giải mã. Thông thường, bản rõ trước khi được mã hoá cần được nối thêm vào đuôi một chuỗi số xác định để làm dấu vết nhận dạng (chẳng hạn nối thêm 20 số 0 – như vậy trong số 4 nghiệm giải ra, chuỗi nào tận cùng bằng 20 con 0 thì đúng là bản rõ cần nhận). Vì lý do này nên Rabin thường được dùng chủ yếu cho chứng thực (chữ ký điện tử).

Hệ El-Gamal

Tạo khóa:

Alice chọn một số nguyên tố p và hai số nguyên ngẫu nhiên g và u , cả hai đều nhỏ hơn p . Sau đó tính

$$y = g^u \pmod{p}$$

Bây giờ khóa công khai của Alice được lấy là (p, g, y) , khóa mật là u .

Sinh mã:

1. Nếu Bob muốn mã hoá một tin X để truyền cho Alice thì trước hết anh ta chọn một số ngẫu nhiên k sao cho $(k, p-1) = 1$
2. Tính

$$a = g^k \pmod{p} \quad b = y^k X \pmod{p}$$

Mã là $Y = (a, b)$ và có độ dài gấp đôi bản rõ.

Giải mã: Alice nhận được $Y = (a, b)$ và giải ra X theo công thức sau:

$$X = \frac{b}{a^u} \pmod{p}$$

1.4 Chữ ký điện tử và Hàm băm

Chữ ký điện tử

Khái niệm chữ ký điện tử được hai nhà bác học Diffie và Hellman đề xuất trong cùng bài báo nổi tiếng của các ông khai sáng nguyên lý của hệ thống mật mã công khai (1976). Ý tưởng về mô phỏng chữ ký tay trên văn bản trong đời thường đã có từ lâu, nhưng thực sự chỉ có thể thực hiện được cùng với sự ra đời của hệ mật mã KCK (khóa công khai). Như đã biết, hệ thống mật mã đối xứng đã được sử dụng phổ biến trước đó không có tính chất đại diện duy nhất cho một cá nhân. Trong khi đó, một hệ mã hóa khóa công khai (hay còn gọi là phi đối xứng) có thể được xem là được tạo lập để giúp bảo mật truyền tin trong liên lạc giữa 1 cá nhân và phần còn lại của xã hội. Nhờ có mật mã KCK, khái niệm chữ ký điện tử mới được hiện thực hóa và giúp cho giao dịch kinh tế thương mại trong đời sống có thể đi vào số hóa hoàn toàn, qua đó thúc đẩy hoạt động dịch vụ trực tuyến trên Internet phát triển như ngày nay.

Chữ ký điện tử hay chữ ký và chữ ký tay thực ra không phải hoàn toàn tương tự. Chữ ký tay là dấu vết của con người tác động lên cùng bản giấy đã mang chứa văn bản (in/viết sẵn). Phần chữ ký tay và phần văn bản có sẵn là độc lập, không có quan hệ ràng buộc nào. Do các qui luật của thế giới vật lý, người ta không thể đánh tráo chữ ký theo kiểu đơn giản là xé bỏ phần tờ giấy chứa chữ ký và ghép nối vào một phần giấy mang chữ ký tạo mới khác. Tuy nhiên trong thế giới số hóa, các qui luật vật lý này không có mặt, và bất cứ lập trình viên nào cũng có thể tha hồ cắt ghép văn bản số hóa mà không bị phát hiện.

Sơ đồ chữ ký cơ bản

Do đó, nguyên lý tạo chữ ký điện tử là khác hẳn và phức tạp hơn. Khi có một văn bản ở dạng nhị phân X , người ta phải tạo ra một chữ ký ở dạng nhị phân S sao cho S phụ thuộc hàm vào X , tức là $S = f(X)$, hơn nữa quan hệ hàm này là bí mật (có tham số khóa bí mật) đối với người ngoài. Do đó nếu có kẻ nào thử đánh tráo (tức giả mạo) chữ ký, quan hệ hàm $S = f(X)$ sẽ không còn đúng và bị phát hiện.

Tuy nhiên việc phát hiện xem một văn bản có chữ ký có là chuẩn hay bị giả mạo lại phải là một thao tác mà ai cũng làm được dễ dàng, không cần đến khóa bí mật kia (do người chủ chữ ký nắm giữ). Vì vậy hệ thống chữ ký điện tử được xây dựng trên nguyên tắc sử dụng hai thuật toán riêng rẽ cho việc tạo chữ ký và kiểm định chữ ký, thông qua việc sử dụng cặp 2 hàm toán học đối lập nhau, một cần khóa bí mật còn một thì không. Chính do điều này, mật mã khóa công khai đã được khai thác để giúp hiện thực điểm chốt của cơ chế đặc biệt này.

Giả sử Alice đã thiết lập một hệ mật mã KCK với thành phần khóa bí mật z_A và công khai Z_A , tức là có hàm sinh mã $E_{Z_A}()$ và hàm giải mã $D_{z_A}()$, khi đó Alice có thể tạo chữ ký điện tử bằng hàm $D_{z_A}()$ và bất kỳ người nào khác sẽ kiểm tra bằng hàm $E_{Z_A}()$. Cụ thể là, với văn bản nhị phân X , Alice sẽ tạo được chữ ký $S = D_{z_A}(X)$, văn bản có chữ ký sẽ là $Y = X||S$. Khi văn bản này đến tay Bob, Bob sẽ kiểm tra tính hợp lệ bằng việc tính $X' = E_{Z_A}(S)$ và đối chiếu $X = X'$? Lưu ý, Bob sẽ cần kiểm được khóa công khai của Alice, Z_A , bằng một cách nào đó.

Như vậy nếu Bob đã nhận được văn bản có chữ ký $X||S$ và dùng khóa công khai của Alice để kiểm định thành công, văn bản đó trở thành bằng chứng, ngay cả khi Alice có muốn chối cãi đã tạo ra và ký nó cũng không được. Bởi vì chỉ duy nhất Alice mới sở hữu khóa d_A bí mật để tạo ra được chữ ký hợp lệ mà thôi. Ta gọi tính chất này của chữ ký điện tử là tính không thể chối cãi được (non-repudiation). Ngay cả khi Alice có khiếu nại bị oan với lý do chữ ký tạo ra bởi một kẻ đã ăn cắp được khóa bí mật của cô ta, thì điều này cũng không thể chứng minh được.

Công chứng: Để có thể đảm bảo phòng tránh được tình trạng chữ ký giả mạo do kẻ gian ăn cắp được khóa bí mật của người bị hại, người ta đã giới thiệu thêm hệ thống công chứng – public notary. Ý tưởng thực hiện: có thêm một bên thứ ba tham gia, vô tư và có thẩm quyền hợp pháp, được gọi là công chứng viên (public notary), sẽ được thuê để ký xác nhận thêm vào sau chữ ký của Alice đối với những văn bản quan trọng mà Alice ký. Văn bản đầy đủ chữ ký sẽ có dạng $Y = X||S_A||S_N$ trong đó chữ ký của công chứng viên S_N là ký trên văn bản $X||S_A$.

Bằng chứng biên nhận: Trong truyền tin liên lạc, chữ ký điện tử có thể sử dụng để đảm bảo tính chính xác của tài liệu (bằng chữ ký của bên gửi A), và bên nhận B có thể gửi lại chữ ký của mình vào tài liệu đã nhận như là bằng chứng để A biết là B đã thực sự nhận được tài liệu đó. Nếu thủ tục này được thực hiện, sau này A có thể chứng minh được là mình đã gửi tài liệu cho B, ngay cả khi lúc đó B muốn chối cũng không được.

$$A \rightarrow B : Y = E_{Z_B}(X||D_{z_A}(X))$$

$$B : \text{tính } E_{z_B}(Y) \text{ thu được } X \text{ và } S = D_{z_A}(X), \text{ kiểm tra xem } X \stackrel{?}{=} E_{z_A}(S)$$

$$B \rightarrow A : Y' = E_{Z_A}(D_{z_B}(X))$$

A : tính $S_B(X) = D_{z_A}(Y')$, đó chính là chữ ký của B trên X , bằng chứng xác nhận B đã nhận được tài liệu X chính xác.

Nhược điểm của hệ chữ ký cơ sở

Hệ chữ ký điện tử theo tiếp cận ban đầu nói trên, tức là sử dụng D_z để ký và E_Z để kiểm định, là khá đơn giản và phạm phải nhược điểm lớn:

- Chữ ký quá dài, dài đúng bằng tài liệu: Với văn bản dài, ta cần dùng việc chia khối rồi ký lên nhiều khối; cụ thể là $X = X_1 || X_2 || X_3 || \dots || X_t \rightarrow S = S_A(X_1) || S_A(X_2) || S_A(X_3) || \dots || S_A(X_t)$. Rõ ràng số lượng khối trên văn bản đã ký nhiều gấp đôi ban đầu.
- Không những dài, việc thực hiện nhiều lần thuật toán KCK (ký lên từng khối) sẽ làm thủ tục ký có thể diễn ra rất lâu, thời gian tỷ lệ với độ dài văn bản. Điều này là không chấp nhận được với các giao dịch trực tuyến.
- Kẻ tấn công có thể dễ dàng phá hệ thống chữ ký này bằng kiểu tấn công lắp ghép khối (thay đổi thứ tự, thêm hay bớt khối ...).

Vì vậy hệ thống chữ ký điện tử đơn giản kiểu này đã không được sử dụng. Giải pháp đầy đủ là có thêm sự hỗ trợ của hàm băm, tức là "Băm" tài liệu trước khi ký, sẽ được trình bày tiếp theo đây.

Hàm băm và ứng dụng chữ ký điện tử

Một hàm băm H sẽ lấy ở đầu vào là một thông tin X có kích thước bất kỳ và sinh kết quả ra là một chuỗi $h_X = h(X)$ có độ dài cố định, thường là nhỏ hơn nhiều so với kích thước của X . Chuỗi này thường được gọi là cốt yếu, hay cốt (digest) của thông tin X .

Ví dụ: Thông tin X có thể là một tệp độ dài hàng trăm Kb trong khi cốt của nó chỉ là một khối có độ dài 128bit. Tất nhiên, điều đó dẫn đến khả năng có thể có 2 thông tin $X \neq X'$ mà cho cùng một cốt giống nhau với một hàm băm, tức là $H(X) = H(X')$. Trường hợp này gọi là đụng độ (collision).

Tuy nhiên với hàm băm thiết kế tốt, đụng độ là gần như không thể xảy ra được trên thực tế. Nói cách khác nếu cố đi tìm, khối lượng tính toán phải thực hiện là rất lớn, không khả thi với công cụ tính toán hiện thời.

Hàm băm có ứng dụng chủ chốt trong các hệ chữ ký điện tử được sử dụng hiện nay. Thay vì ký (tức là thực hiện thuật toán D_{z_A}) lên văn bản X , Alice cần thực hiện việc ký lên h_X , như vậy văn bản đã ký sẽ có dạng $X || D_{z_A}(H(X))$.

Để đảm bảo an toàn cao, chống được tấn công giả mạo chữ ký, chúng ta cần sử dụng các hàm băm mật mã (cryptographic hash function) với các thuộc tính như sau:

1. Lấy đầu vào là một xâu với độ dài bất kỳ và sinh ra một xâu với độ dài cố định.
2. Có tính một chiều: biết X , có thể dễ dàng tính được giá trị băm h_X , nhưng không thể tính ngược được X khi chỉ biết h_X , với công cụ tính toán hiện nay (bất khả thi về tính toán).
3. Có tính phi đụng độ cao (collision free), tức là thực tế không thể tìm được hai thông tin $X \neq X'$ sao cho $H(X) = H(X')$. Tất nhiên, đây là bất khả thi về mặt tính toán.

hình

Đụng độ

Rõ ràng là với không gian giá trị băm nhỏ hơn không gian tin về mặt kích thước thì chắc chắn sẽ tồn tại đụng độ (collision), nghĩa là có hai bản rõ $X \neq X'$ mà giá trị băm của chúng giống nhau nghĩa là $h_X = h_{X'}$. Điều này có thể thấy rõ ràng qua nguyên lý Diricle - Nếu có $n+1$ con thỏ được thả vào n cái chuồng thì phải tồn tại ít nhất một cái chuồng mà trong đó có ít ra là hai con thỏ ở chung.

Trong thực tế người ta thường chọn không gian băm cỡ khoảng 64bit, 128 bit ... Trong khi đó các văn bản thực tế lớn hơn nhiều, cỡ Kb trở lên, cho nên việc tồn tại đụng độ là chắc chắn. Tuy nhiên nếu sử dụng hàm băm mật mã có không gian băm lớn được chế tạo tốt (an toàn) thì việc tìm ra đụng độ đòi hỏi khối lượng tính toán lớn đến mức phi thực tế (infesible computation).

Việc chế tạo các hàm băm phi đụng độ là rất khó. Nhiều hàm băm được phát minh bởi các nhóm có tên tuổi trên thế giới sau một thời gian xuất hiện đã bị những người khác chỉ ra những đụng độ tồn tại và không được công nhận là an toàn nữa.

Các kỹ thuật làm hàm băm

Các kỹ thuật để chế tạo được hàm băm có thể chia ra làm ba loại:

- Dựa trên việc áp dụng các hệ mã khối theo mật mã khoá bí mật đối xứng (SKC).
- Dựa trên các phép toán số học đồng dư.
- Các hàm thiết kế băm đặc biệt.

Các hàm băm chế từ hệ SKC

Sơ đồ Rabin-Matyas-Davies-Price (RMDP)

$$\begin{aligned} X &= X_1 X_2 \dots \\ H_0 &= 0 \text{ (hay một số ngẫu nhiên nào đó)} \\ H_i &= E_{x_i}(H_{i-1}) \end{aligned}$$

Ở đây, tất nhiên các TIN phải được chặt thành các khối có kích cỡ bằng khoá của hệ mã E. Giá trị băm là $H(X) = (H_0, H_t)$.

Người ta chứng minh được rằng với không gian băm chỉ là 64bit thì $H(X)$ không phải là một chiều, tức là cho $Y = H(X)$, việc tìm ngược được X là khả thi.

Sơ đồ Davies-Meyer (DM hash)

$$\begin{aligned} X &= X_1 X_2 \dots \\ H_0 &= \text{vector khởi tạo là một số ngẫu nhiên nào đó} \\ H_i &= E_{x_i}(H_{i-1}) \oplus H_{i-1} \end{aligned}$$

- Việc xây dựng các hàm băm từ các mã khối đòi hỏi phải có phân tích tính an toàn một cách cẩn thận.

- DM được coi như là an toàn nếu sử dụng với các mã khối kích thước 128bit.
- Không có hệ nào khác đã được đề xuất mà được chứng minh là an toàn.

Các hàm băm dựa trên các phép toán số học đồng dư

QCMDC (Quadratic Congruential Manipulation Detection Code)

Được đề xuất bởi Jueneman (1983).

Bản rõ được chia thành các khối m bit. H_0 là giá trị khởi đầu được chọn ngẫu nhiên và giữ bí mật (vì thế vẫn được gọi là hàm băm có khóa - keyed hash function).

Các bước xây dựng hàm băm như sau:

$$\begin{aligned} M &\text{ là một số nguyên tố sao cho } M \geq 2^{m-1}, \\ H_i &= (H_{i-1} + X_i)^2 \pmod{M} \\ M &\text{ là lũy thừa của 2.} \end{aligned}$$

Hệ này đã bị phá (Coppersmith).

Davies-Price (1985)

Chia văn bản thành các khối có m -d bit:

$$\begin{aligned} X &= X_1 X_2 X_3 \dots X_n \\ H_i &= (H_{i-1} \oplus X_i)^2 \pmod{M}, H_0 = 0 \end{aligned}$$

Hệ này bị chứng minh là không đảm bảo tính một chiều (Girault)

Các hàm băm được chế tạo đặc biệt

Ngoài các kỹ thuật thông thường nói trên người ta đã tìm nhiều cách rất riêng biệt khác nhau để chế tạo ra những hàm băm có độ tin cậy cao. Thông thường những sơ đồ này rất phức tạp và có những cấu trúc đặc biệt, nên không trình bày đầy đủ ở đây. Sau đây là một số các hàm băm nổi tiếng.

MD5 (Rivest 1992)

Đây là một trong các hàm băm có tiếng nhất và được sử dụng thông dụng:

- + Nó lấy vào các khối đầu vào 512 bit và sinh ra các giá trị băm 128 bit.
- + Được tin là phi dụng độ và một chiều (one - way)
- + Thuật toán MD5 được thiết kế cho phép chạy tốt nhất trên các máy tính 32 bit. Nó sử dụng các phép toán đơn giản như phép cộng modulo 32, do đó thích hợp với việc mã hoá cho các bộ xử lý 32 bit.

SHA (Secure Hash Function)

Đây là một thuật toán được đề xuất và bảo trợ bởi cơ quan NIST để sử dụng đối với hệ chữ ký DSA (cũng là một dự chuẩn cho chữ ký điện tử). Nó cho giá trị băm là 160 bit và được thiết kế với cùng một tiếp cận như MD5.

HAVAL

Một hệ băm của Australia cho phép thay đổi kích thước giá trị băm. Cấu trúc rất giống như MD5.

Snefru Mkle (1989)

- + Là hàm băm có khóa (keyed hash function)
- + Cho phép 1 trong 2 lựa chọn kích thước giá trị băm là 128 bit và 256 bit.
- + Eli Biham đã chỉ ra một dụng độ cho trường hợp 128 bit.

1.5 Hệ thống chứng thực và Chứng thư số

Hệ thống chứng thực

Hệ thống chứng thực là một hạ tầng an ninh mạng được xây dựng trên một hạ tầng cơ sở khóa công khai (PKI) cung cấp các giải pháp đảm bảo an toàn cho các hoạt động (gọi chung là giao dịch) thông qua mạng.

Tại sao lại phải sử dụng hệ thống chứng thực?

- Hệ thống chứng thực cung cấp các dịch vụ đảm bảo an toàn cho các giao dịch thông qua mạng. Các dịch vụ cơ bản mà một hệ thống chứng thực cung cấp bao gồm:
- Dịch vụ xác thực: nhằm xác định xem ai đang giao dịch với mình.
- Dịch vụ bảo mật: đảm bảo tính bí mật của thông tin, người không có thẩm quyền không thể đọc được nội dung của thông tin.
- Dịch vụ toàn vẹn: khẳng định thông tin có bị thay đổi hay không.
- Dịch vụ chống chối bỏ: cung cấp các bằng chứng chống lại việc chối bỏ một hành động đã thực hiện hay đã diễn ra
- Như vậy sử dụng hệ thống chứng thực sẽ đảm bảo, bí mật, toàn vẹn cho thông tin được truyền qua mạng, xác thực được người dùng và chống chối bỏ các hành động hay sự kiện đã xảy ra.

Hệ thống chứng thực gồm những thành phần nào?

- Hệ thống chứng thực gồm 2 thành phần:
 - Thành phần thực hiện các nhiệm vụ về quản lý chứng thư số như: đăng ký và phát hành, thu hồi ... chứng thư số.
 - Thành phần thực hiện chức năng xác định xem một chứng thư số có hợp lệ hay không

Cơ quan chứng thực (CA) là gì?

Cơ quan chứng thực (Certification Authority - CA) có thẩm quyền cấp phát, thu hồi, quản lý chứng thư số cho các thực thể thực hiện các giao dịch an toàn. Cơ quan chứng thực là một thành phần chính của hệ thống chứng thực.

Cơ quan đăng ký (RA) là gì?

Cơ quan đăng ký (Registration Authority) là một thành phần trong hệ thống chứng thực có nhiệm vụ tiếp nhận và xác minh các yêu cầu về chứng thư số của người sử dụng đồng thời gửi các yêu cầu đã xác minh cho cơ quan chứng thực (CA) thực hiện yêu cầu đó.

Hệ thống chứng thực có những ứng dụng gì?

- Một số ứng dụng của hệ thống chứng thực:
- Nhóm các dịch vụ chính phủ điện tử e-Government:
 - Hóa đơn điện tử (E-Invoice)
 - Thuế điện tử (E-Tax Filing)
 - Hải quan điện tử (E-Customs)
 - Bầu cử điện tử (E-Voting)
 - E-Passport
 - PKI-based National ID Card
 - Các dịch vụ của chính phủ cho doanh nghiệp G2B (các ứng dụng đăng ký kê khai, thăm dò qua mạng đối với các doanh nghiệp)
 - Các dịch vụ của chính phủ cho công dân G2C (dịch vụ y tế ...).
- Nhóm các dịch vụ ngân hàng trực tuyến (Online Banking)
 - Thanh toán trực tuyến (E-Payment)
 - Tiền điện tử (E-Billing)
 - Kinh doanh chứng khoán trực tuyến (Online security trading)
 - Đấu thầu trực tuyến (E-Procurement)
 - Bảo hiểm trực tuyến (E-Insurance)
 - Quản lý tài liệu
 - Bảo mật email

Chứng thư số

Để thực hiện được các giao dịch an toàn qua mạng, các bên tham gia cần phải có "chứng thư số". Chứng thư số là một cấu trúc dữ liệu chứa các thông tin cần thiết để thực hiện các giao dịch an toàn qua mạng. Chứng thư số được lưu giữ trên máy tính dưới dạng một tập tin (file).

Nội dung chứng thư số bao gồm:

- Tên chủ thể chứng thư số.
- Khoá công khai.
- Một số thông tin khác như, tên của CA cấp chứng chỉ số đó, hạn dùng, thuật toán ký
- Chữ ký số của CA cấp chứng thư số đó.

Mục đích của chứng thư số dùng để nhận diện một đối tượng khi tham gia giao dịch trên mạng.

Ứng dụng chứng thư số để làm gì?

- Với chứng thư số người dùng có thể:
 - Xác định danh tính người dùng khi đăng nhập vào một hệ thống (xác thực).
 - Ký số các tài liệu Word, PDF hay một tệp liệu.
 - Mã hóa thông tin để đảm bảo bí mật khi gửi và nhận trên mạng.
 - Thực hiện các kênh liên lạc trao đổi thông tin bí mật với các thực thể trên mạng như thực hiện kênh liên lạc mật giữa người dùng với webserver.

Chương 2

Mật mã dựa trên đường cong Elliptic

giới thiệu

2.1 Lý thuyết số

Nhóm

Một nhóm $(G, +)$ là tập hợp các phần tử G cùng với phép toán hai ngôi $+$ kết hợp thành phần tử thứ ba thỏa mãn bốn tiên đề của nhóm (với $a, b, c, e \in G$):

- Tính đóng: $\forall a, b : (a + b) \in G$
- Tính kết hợp: $\forall a, b, c : (a + b) + c = a + (b + c)$
- Phần tử đơn vị: $\exists e \forall a : a + e = e + a = a$
- Tính khả nghịch: $\forall a \exists b : a + b = b + a = e$

e được gọi là phần tử đơn vị (ví dụ nhóm số nguyên phần tử đơn vị là 0). Một nhóm được gọi là abelian khi thỏa mãn điều kiện:

- Tính giao hoán: $\forall a, b : a + b = b + a$

Cho \cdot là phép nhân kết quả của phép cộng lặp đi lặp lại nhiều lần của 1 phần tử. Cho nhóm (G, \cdot) là nhóm và x^n được định nghĩa như sau:

$$\begin{aligned}x^0 &= \infty \\ x^{n+1} &= x^n \cdot x \text{ with } n \in \mathbb{N}\end{aligned}$$

∞ là phép nhân phần tử đơn vị. Cấp (order) r của một phần tử x được định nghĩa như một số nguyên nhỏ $r > 0$ sao cho $x^r = \infty$. Nếu một nhóm có phần tử g sao cho $\{g^n | n \in \mathbb{Z}\}$ là tất cả phần tử trong nhóm, g được gọi là phần tử sinh của nhóm vòng.

Vành

Một vành được gọi là nhóm abelian với phép toán hai ngôi thỏa mãn luật kết hợp và phân phối trên nhóm abelian:

$$\forall a, b, c \in G : a \cdot (b + c) = a \cdot b + a \cdot c$$

Trường

Một trường là một vành giao hoán khác 0, chứa một nghịch đảo nhân cho mọi phần tử khác không. Như một vành, các phần tử khác không tạo thành một nhóm abelian dưới phép nhân.

Ví dụ về trường:

- Trường số thực (\mathbb{R})
- Trường số phức (\mathbb{C})
- Trường số hữu tỉ (\mathbb{Q})

2.2 Đường cong Elliptic

Một đường cong elliptic curve được xác định bởi phương trình đường cong và một số trường tọa độ cơ bản.

Tất cả tọa độ thỏa mãn phương trình đường cong sẽ tạo thành một đường cong E. Tọa độ là cặp các phần tử trong trường hữu hạn. Phương trình đường cong phụ thuộc vào việc lựa chọn hệ tọa độ cực (mặc định thường là hệ tọa độ affine). Đường cong elliptic có một số luật quan trọng. Luật cộng (add) cho phép cộng hai điểm trên đường cong. Luật doubling cho phép nhân một điểm trên đường cong với một số biểu diễn được thành 2^k . Luật nhân cho phép nhân một điểm trên đường cong với một số (hay cộng nhiều lần điểm đây với chính nó). Mọi đường cong đều có điểm đơn vị định nghĩa là ∞ . Nó có xác định luật cộng riêng.

$E(GF(p^k))$ là tập hợp các điểm thỏa mãn phương trình đường cong (và cả điểm ∞). Lực lượng $|E(GF(p^k))|$ được định nghĩa là cấp (order) của đường cong. Nếu muốn xác định một số phần tử của $E(GF(p^k))$ như một điểm sinh. Nó tạo ra nhóm con khác theo luật:

$$h = \frac{|E(GF(p^k))|}{o}$$

h được gọi là cofactor và o được gọi là cấp(order) của điểm sinh.

Số lượng điểm sinh của trường $GF(n)$ là $\phi(n-1)$ ở đây ϕ là một hàm Ô-le của Euler. Điều này cũng là yếu tố cho phép nhân trong nhóm vòng[*].

Đường cong elliptic có một số phương trình đường như *Weierstrass Curve*, *Montgomery Curve*, *Edwards Curve*, *Twisted Edwards Curve*, ... chúng ta sẽ xem xét các luật cộng, doubling, nhân và các tính chất của các luật của các đường cong ở phần tiếp theo.

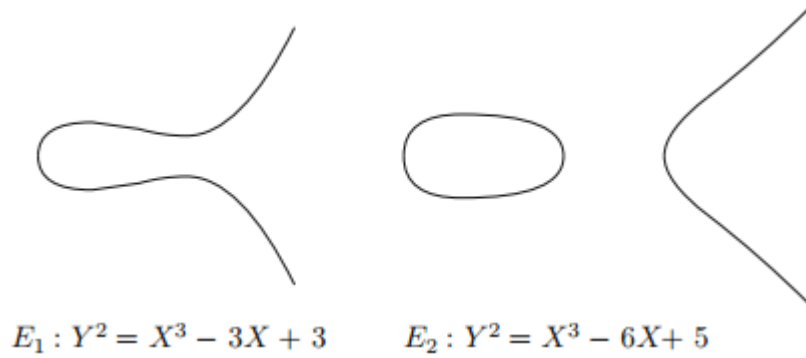
Luật cộng

Một đường cong elliptic là tập hợp các nghiệm của phương trình:

$$Y^2 = X^3 + AX + B.$$

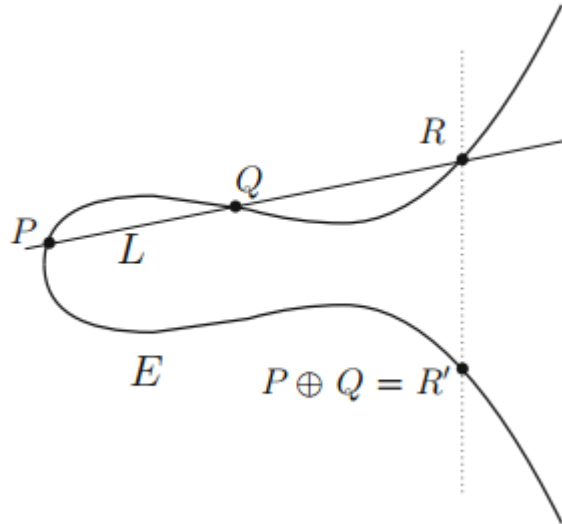
Phương trình này được gọi là phương trình Weierstrass. Ta có hai ví dụ về đường cong elliptic

$$E_1 : Y^2 = X^3 - 3X + 3 \quad \text{và} \quad E_2 : Y^2 = X^3 - 6X + 5$$



Hình 2.1: Hai ví dụ minh họa về đường cong elliptic

Một đặc điểm của đường cong elliptic là lấy hai điểm bất kì trên đường cong và cộng chúng lại để tạo ra một điểm thứ ba nằm trên đường cong. Nhưng không giống như luật cộng thông thường chúng ta sẽ mô tả luật cộng thông qua hình học.



Hình 2.2: Luật cộng trên đường cong elliptic

Cho P và Q là hai điểm trên đường cong elliptic E , như hình 2.2. Kẻ đường thẳng L đi qua P và Q . Đường thẳng L cắt đường cong E tại ba điểm, trong đó có hai điểm P

và Q và một điểm khác là R . Chúng ta lấy điểm R và chiếu nó theo trục x để lấy được điểm mới R' . Điểm R' được gọi là "tổng của P và Q ", có thể thấy phép cộng này không giống như các phép cộng thông thường. Chúng ta có thể kí hiệu phép cộng bởi \oplus .

$$P \oplus Q = R'$$

Một ví dụ về luật cộng. Cho đường cong E có phương trình:

$$Y^2 = X^3 - 15X + 18 \quad (2.1)$$

Cho hai điểm $P = (7, 16)$ và $Q = (1, 2)$ nằm trên đường cong E . Đường thẳng L đi qua hai điểm có phương trình:

$$L : Y = \frac{7}{3} - \frac{1}{3}X \quad (2.2)$$

Để tìm được giao điểm của đường thẳng L và đường cong E . Chúng ta sẽ thay phương trình 2.2 vào 2.1 Ta có:

$$\begin{aligned} \left(\frac{7}{3} - \frac{1}{3}X\right)^2 &= X^3 - 15X + 18, \\ \frac{49}{9}X^2 - \frac{14}{3}X + \frac{49}{9} &= X^3 - 15X + 18, \\ 0 &= X^3 - \frac{49}{9}X^2 - \frac{121}{3}X + \frac{161}{9} \end{aligned}$$

Chúng ta cần tìm nghiệm của đa thức. Nhìn chung để tìm nghiệm của đa thức là khó. Tuy nhiên như chúng ta đã biết $L \cap E$ Tại hai điểm P và Q nên ta có hai là $X = 7$ và $X = 1$, vì thế chúng ta có thể dễ dàng tìm được nghiệm thứ ba còn lại:

$$X^3 - \frac{49}{9}X^2 - \frac{121}{3}X + \frac{161}{9} = (X - 7) \cdot (X - 1) \cdot \left(X + \frac{23}{9}\right)$$

vì vậy điểm thứ ba là giao điểm của L và E sẽ có tọa độ $X = -\frac{23}{9}$. Chúng ta sẽ tìm tọa độ Y theo X bằng cách thay X vào phương trình 2.2 kết quả $R = \left(-\frac{23}{9}, -\frac{170}{27}\right)$. Cuối cùng chúng ta sẽ chiếu R theo trục tọa độ X đạt được

$$P \oplus Q = \left(-\frac{23}{9}, \frac{170}{27}\right).$$

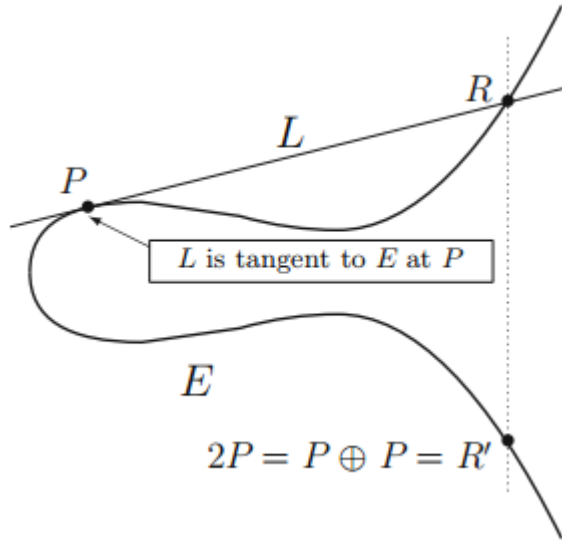
Có một số vấn đề, đầu tiên ta có thể nhìn thấy trong hình 2.2 nếu như Q tiệm cận đến P hay nói cách khác là ta thực hiện phép cộng điểm P với chính nó. Khi đó đường thẳng L trở thành tiếp tuyến của E tại P thấy hình 2.3. Do đó việc thực hiện phép cộng điểm P với chính nó chúng ta chỉ đơn giản là kéo dài tiếp tuyến L tại P cắt E tại P và một điểm còn lại là R và chúng ta vẫn xử lý như trước. Theo một nghĩa nào đó L vẫn cắt E tại 3 điểm nhưng điểm P được tính là hai.

Ví dụ tiếp tục với đường cong E với phương trình 2.1 và điểm P ở ví dụ trên, chúng ta sẽ tính $P \oplus P$ hệ số góc tiếp tuyến của E ở P được tính bởi đạo hàm phương trình 2.1. Do đó ta có:

$$2Y \frac{dY}{dX} = 3X^2 - 15 \Rightarrow \frac{dY}{dX} = \frac{3X^2 - 15}{2Y}$$

Thay tọa độ điểm $P = (7, 16)$ vào ta được hệ số góc $\lambda = \frac{33}{8}$ và đường thẳng tiếp tuyến với E tại P có phương trình

$$L : Y = \frac{33}{8}X - \frac{103}{8} \quad (2.3)$$



Hình 2.3: Cộng điểm P với chính nó

Từ 2.3 và 2.1 ta có:

$$\begin{aligned} \left(\frac{33}{8}X - \frac{103}{8}\right)^2 &= X^3 - 15X + 18, \\ X^3 - \frac{1089}{64}X^2 + \frac{2919}{32}X - \frac{9457}{64} &= 0, \\ (X - 7)^2 \cdot \left(X - \frac{193}{64}\right) &= 0. \end{aligned}$$

Tọa độ X của điểm P là nghiệm kép của phương trình ta dễ dàng tìm được nghiệm còn lại $X = \frac{193}{64}$, thay X vào 2.3 tìm được $Y = -\frac{223}{512}$. Từ đó ta thu được kết quả của phép cộng

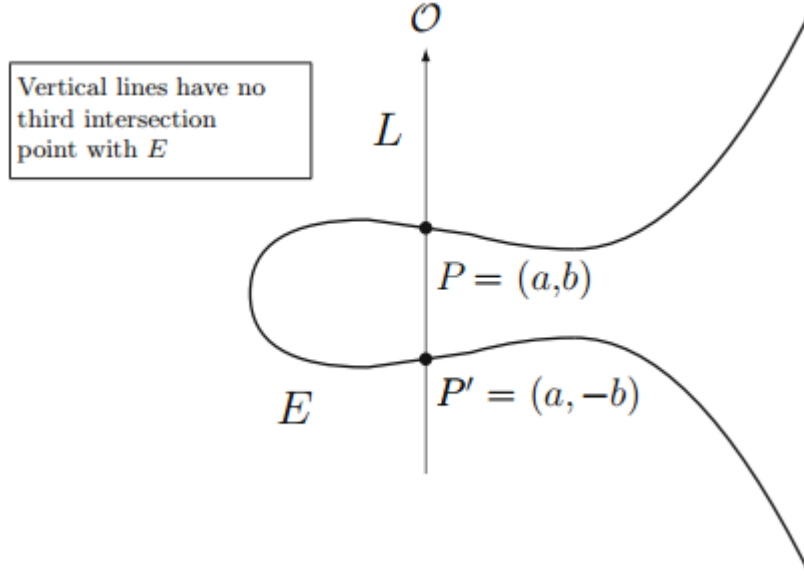
$$P \oplus P = \left(\frac{193}{64}, \frac{223}{512}\right).$$

Vấn đề thứ hai với luật cộng phát sinh là nếu như chúng ta cộng điểm $P = (a, b)$ với điểm đối của nó $P' = (a, -b)$ đường thẳng đi qua P và P' là $x = a$ và nó chỉ cắt đường cong tại 2 điểm P và P' (hình 2.2) không có điểm thứ ba xuất hiện chúng ta sẽ thêm một điểm O nằm ở vô cùng và điểm này không tồn tại trong mặt phẳng XY, chúng ta giả định nó luôn nằm trên đường thẳng dọc và chúng ta sẽ xét phép cộng như sau

$$P \oplus P' = O.$$

Nếu cộng điểm O với điểm P nằm trên E sẽ như nào? Đường thẳng L đi qua O và P là đường theo chiều dọc đi qua P khi đó O nằm trên đường dọc này và đường thẳng sẽ cắt E tại điểm P , O và điểm $P' = (a, -b)$. Nên phép cộng P với O , chúng ta lấy hình chiếu của P' qua trục X sẽ thu được điểm P ban đầu. Nói một cách khác $P \oplus O = P$, vì vậy O giống như số không trong phép cộng của đường cong elliptic

Qua đây có một số định nghĩa về đường cong elliptic



Hình 2.4: Đường thẳng đứng L đi qua $P = (a, b)$ và $P' = (a, -b)$

Định nghĩa 2.1 Một đường cong E là tập các nghiệm của phương trình Weierstrass

$$E : Y^2 = X^3 + AX + B,$$

cùng với điểm O , với hằng số A, B thỏa mãn điều kiện

$$4A^3 + 27B^2 \neq 0,$$

Luật cộng trên E được định nghĩa như sau. Cho P và Q là hai điểm trên E . Cho L là đường thẳng qua P và Q , hoặc là tiếp tuyến của E tại P nếu như $P = Q$. Giao điểm của E và L có chứa ba điểm P, Q, R phép cộng sẽ được tính thích hợp với điểm O nằm trên đường dọc vô cùng. Điểm $R = (a, b)$, tổng của P và Q được định nghĩa là $R' = (a, -b)$ hình chiếu của R qua trục X . Tổng này được định nghĩa là $P \oplus Q$ hay đơn giản hơn là $P + Q$.

Hơn nữa, nếu $P = (a, b)$ chúng ta định nghĩa điểm đối $-P = (a, -b)$, chúng ta định nghĩa $P - Q$ trở thành $P + (-Q)$. Tương tự phép cộng lặp nhiều lần được biểu diễn như phép nhân một điểm với một số nguyên,

$$nP = \underbrace{P + P + P + \dots + P}_n.$$

Định lý 2.1 Cho đường cong E . Luật cộng trên đường cong E thỏa mãn tính chất:

- (a) $P + O = O + P = P \forall P \in E$ (phần tử đơn vị)
- (b) $P + (-P) = O \forall P \in E$ (phần tử nghịch)
- (c) $(P + Q) + R = P + (Q + R) \forall P, Q, R \in E$ (kết hợp)
- (d) $P + Q = Q + P \forall P, Q \in E$ (giao hoán)

Hay nói cách khác tập các điểm thuộc E với luật cộng tạo thành nhóm abelian

Định lý 2.2 Thuật toán Cộng trên đường cong elliptic với phương trình đường cong Weierstrass. Cho

$$E : Y^2 = X^3 + AX + B$$

là một đường cong elliptic và hai điểm P_1 và P_2 nằm trên đường cong E .

- (a) Nếu $P_1 = O$ thì $P_1 + P_2 = P_2$.
- (b) trái lại $P_2 = O$ thì $P_1 + P_2 = P_1$.
- (c) trái lại $P_1 = (x_1, y_1)$ và $P_2 = (x_2, y_2)$
- (d) nếu $x_1 = x_2$ và $y_1 = -y_2$ thì $P_1 + P_2 = O$.
- (e) trái lại, định nghĩa λ bằng

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2, \end{cases}$$

và

$$x_3 = \lambda^2 - x_1 - x_2 \quad \& \quad y_3 = \lambda(x_1 - x_3) - y_1$$

Phép cộng $P_1 + P_2 = (x_3, y_3)$

Đường cong Elliptic trên trường hữu hạn

Trong phần trước chúng ta đã xem xét lý thuyết về đường cong bằng hình học. Ví dụ tổng của hai điểm phân biệt P và Q trên đường cong E được định nghĩa bởi đường thẳng L đi qua hai điểm P và Q sau đó tìm điểm thứ ba là giao điểm của L và E như minh họa hình[?]. Tuy nhiên để áp dụng lý thuyết elliptic vào mật mã, chúng ta cần nhìn đường cong và các điểm của nó có tọa độ nằm trong trường hữu hạn F_p điều này dễ làm.

Định nghĩa 2.2 Cho $p \geq 3$ là một số nguyên tố. Một đường cong elliptic trên trường F_p có công thức

$$E : Y^2 = X^3 + AX + B \text{ với } A, B \in F_p \text{ thỏa mãn } 4A^3 + 27B^2 \neq 0.$$

Với tập các điểm trên E với tọa độ nằm trong trường F_p

$$E(F_p) = \{(x, y) : x, y \in F_p \text{ thỏa mãn } y^2 = x^3 + Ax + B\} \cup \{O\}$$

Xem xét ví dụ với đường cong elliptic

$$E : Y^2 = X^3 + 3X + 8 \text{ trên trường } F_{13}$$

Chúng ta có thể tìm thấy các điểm của $E(F_{13})$ bằng cách thay lần lượt các giá trị của $X = 0, 1, 2, \dots, 12$ và kiểm tra với giá trị X kết quả của phương trình $X^3 + 3X + 8$ có phải là một bình phương với modulo 13 không. Ví dụ thay $X = 0$ cho kết quả là 8 và 8 không phải là bình phương với modulo 13. Tiếp theo $X = 1$ cho kết quả 12 và 12 là căn bậc hai của modul 13.

$$5^2 \equiv 12(mod13) \text{ và } 8^2 \equiv 12(mod13) \text{ trên trường } F_{13}$$

Điều này sẽ cho hai điểm $(1, 5)$ và $(1, 8)$ trong trường F_{13} . Tiếp tục tính với các giá trị X ta thu được danh sách các điểm.

$$E(F_{13}) = \{O, (1, 5), (1, 8), (2, 3), (2, 10), (9, 6), (9, 7), (12, 2), (12, 11)\}$$

Giả sử chúng ta có hai điểm $P = (x_1, y_1)$ và $Q = (x_2, y_2)$ là hai điểm nằm trên $e(F_p)$. Chúng ta sẽ định nghĩa phép cộng $P + Q$ là điểm có tọa độ (x_3, y_3) thực hiện phép toán cộng (định lý 2.2). Chú ý rằng thuật toán này chỉ sử dụng các phép toán cộng, trừ, nhân, chia liên quan đến các hệ số của đường cong E và các điểm P và Q . Khi các hệ số và tọa độ nằm trong trường F_p , chúng ta sẽ có điểm (x_3, y_3) với tọa độ trong trường F_p .

Định lý 2.3 Cho E là một đường cong trên trường F_p và hai điểm P và Q nằm trong $E(F_p)$.

- (a) Thuật toán cộng đường cong elliptic (định lý 2.2) áp dụng với P và Q tạo điểm trong $E(F_p)$. Chúng ta định nghĩa $P + Q$.
- (b) Luật cộng trên $E(F_p)$ thỏa mãn tất cả các tính chất của định lý 2.1. Hay nói cách khác luật cộng $E(F_p)$ nằm trong một nhóm hữu hạn phần tử.

Xét ví dụ thuật toán cộng (định lý 2.2) với hai điểm $P = (9, 7)$ và $Q = (1, 8)$ trong $E(F_{13})$. Bước thứ e của thuật toán sẽ được tính đầu tiên

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8 - 7}{1 - 9} = \frac{1}{-8} = \frac{1}{5} = 8,$$

Ở đây các phép tính được thực hiện trên trường \mathbb{F}_{13} vì vậy $-8 = 5$ và $\frac{1}{5} = 5^{-1} = 8$. Tiếp theo tính

$$v = y_1 - \lambda x_1 = 7 - 8 \cdot 9 = -65 = 0$$

Cuối cùng phép cộng sẽ có kết quả

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 = 64 - 9 - 1 = 54 = 2, \\ y_3 &= -(\lambda x_3 + v) = -8 \cdot 2 = -16 = 10 \end{aligned}$$

Hay $P + Q = (1, 8) + (9, 7) = (2, 10)$ in $E(F_{13})$. Tương tự ta có thể tính thuật toán cộng $P = (9, 7)$ với chính nó. Tính

$$\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot 9^2 + 3}{2 \cdot 7} = \frac{246}{14} = 12 \text{ và } v = y_1 - \lambda x_1 = 7 - 12 \cdot 9 = 3$$

Ta có kết quả là

$$x_3 = \lambda^2 - x_1 - x_2 = (12)^2 - 9 - 9 = 9 \text{ và } y_3 = -(\lambda x_3 + v) = -(12 \cdot 9 + 3) = 6,$$

vì vậy $P + P = (9, 7) + (9, 7) = (9, 6)$ trong trường $E(\mathbb{F}_{13})$

Thuật toán Double-and-Add

Xuất phát từ việc khó phục hồi lại giá trị của n từ điểm P và $Q = n \cdot P$ trong $E(\mathbb{F}_p)$ đây là vấn đề khó của ECDLP. Tuy nhiên để sử dụng

$$\mathbb{Z} \rightarrow E(\mathbb{F}_p), \quad n \mapsto nP,$$

cho mật mã, chúng ta cần thực hiện phép tính nP hiệu quả khi biết giá trị của n và P . Nếu như n lớn thì chúng ta chẳng muốn tính nP bằng cách $P, 2P, 3P, 4P, \dots$. Các toán tử sử dụng trong tính toán đường cong elliptic được viết như phép cộng vì thế chúng ta sẽ gọi nó là "doubling-and-add". Ý tưởng cơ bản của thuật toán là chúng ta sẽ phân tích số n thành biểu diễn nhị phân

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 4 + n_3 \cdot 8 + \dots + n_r \cdot 2^r \text{ với } n_0, n_1, \dots, n_r \in \{0, 1\}.$$

Nếu chúng ta giả sử $n_r = 1$. Chúng ta có thể tính

$$Q_0 = P, \quad Q_1 = 2Q_0, \quad Q_2 = 2Q_1, \dots, Q_r = 2Q_{r-1}.$$

Chú ý rằng Q_i , đơn giản chỉ là gấp hai lần Q_{i-1} vì vậy

$$Q_i = 2^i P.$$

Các điểm là được biểu diễn như là phép với một số mũ cơ số 2, tính toán các điểm này yêu cầu r phép doubling. Cuối cùng chúng ta tính được nP sử dụng r phép cộng

$$nP = n_0 Q_0 + n_1 Q_1 + n_2 Q_2 + \dots + n_r Q_r.$$

Do đó tổng thời gian tính toán nP tối đa là $2r$ phép toán trong $E(\mathbb{F}_p)$. Chú ý rằng $n \geq 2^r$, vì vậy không lớn hơn $2 \log_2(n)$ phép toán để tính nP . Điều này tạo nên sự linh hoạt khi tính nP thậm trí cả khi giá trị của n là lớn. Thuật toán tổng quát Double-and-Add.

Algorithm 1 The double-and-add algorithm for elliptic curves

Input: Điểm P nằm trường elliptic và số nguyên $n \geq 1$

- 1: Set $Q = P$ and $R = O$.
 - 2: Loop while $n > 0$
 - 3: If $n \equiv 1 \pmod{2}$, set $R = R + Q$.
 - 4: $Q = 2Q$ and $n = \lfloor n/2 \rfloor$.
 - 5: If $n > 0$, continue with loop at Step 2.
 - 6: Return the point R , which equals nP .
-

Montgomery curve

Trong toán học những đường cong Montgomery là một dạng của đường cong elliptic, khác với Weierstrass, được giới thiệu bởi Peter L. Montgomery vào năm 1987. Nó được sử dụng cho một số tính toán nhất định, và đặc biệt trong mật mã ứng dụng khác nhau.

Một đường cong Montgomery trên trường \mathbb{K} được định nghĩa bởi phương trình

$$M_{A,B} : By^2 = x^3 + Ax^2 + x$$

với điều kiện $A, B \in \mathbb{K}$ và với $B(A^2 - 4) \neq 0$. Đường cong này được xem xét trên một trường hữu hạn $\mathbb{K}(\mathbb{K} = \mathbb{F}_q)$ với hai đặc điểm khác như $A \in \mathbb{K} \setminus \{-2, 2\}, B \in \mathbb{K} \setminus \{0\}$

Luật cộng

Cho hai điểm $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ trên đường cong Montgomery $M_{A,B}$ trong hệ tọa độ affine, điểm $P_3 = P_1 + P_2$ biểu diễn hình học, điểm thứ ba là giao điểm giữa $M_{A,B}$ và đường thẳng đi qua P_1 và P_2 . Có thể tìm tọa độ (x_3, y_3) của P_3 , theo cách sau:

- 1, Xem xét một đường thẳng $y = lx + m$ trong mặt phẳng affine và để nó đi qua P_1 và P_2 (áp đặt điều kiện), theo cách này, người ta có được $l = \frac{y_2 - y_1}{x_2 - x_1}$ và

$$m = y_1 - \left(\frac{y_2 - y_1}{x_2 - x_1} \right) x_1$$

- 2, giao của đường thẳng với đường cong $M_{A,B}$, thay thế y biến trong phương trình đường cong với $y = lx + m$ phương trình thu được:

$$x^3 + (A - Bl^2)x^2 + (1 - 2Blm)x - Bm^2 = 0.$$

Như đã được quan sát trước đây, phương trình này có ba giải pháp tương ứng với tọa độ x của P_1, P_2 và P_3 . Đặc biệt phương trình này có thể được viết lại thành:

$$(x - x_1)(x - x_2)(x - x_3) = 0$$

- 3, So sánh các hệ số của hai phương trình giống hệt nhau đã nêu ở trên, đặc biệt là các hệ số của các số hạng thứ hai, thu được:

$$-x_1 - x_2 - x_3 = A - Bl^2$$

Vì thế, x_3 có thể được viết dưới dạng x_1, y_1, x_2, y_2 , như:

$$x_3 = B \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - A - x_1 - x_2$$

- 4, Để tìm tọa độ y của điểm P_3 , thay thế giá trị x_3 vào đường thẳng $y = lx + m$. Lưu ý rằng điều này sẽ không cho điểm P_3 trực tiếp. Thật vậy, với phương pháp này ta tìm thấy tọa độ của điểm R sao cho $R + P_1 + P_2 = P_\infty$, nhưng kết quả cần là tổng giữa P_1 và P_2 , thì cần phải quan sát rằng: $R + P_1 + P_2 = P_\infty$ nếu và chỉ nếu $-R = P_1 + P_2$. Vì vậy, cho điểm R , nó là cần tìm $-R$, nhưng điều này có thể được thực hiện dễ dàng bằng cách thay đổi dấu y tọa độ của R . Nói cách khác, nó sẽ là cần thay đổi dấu của y bằng cách thay thế giá trị x_3 trong phương trình đường thẳng. Tóm lại tọa độ của điểm $P_3 = (x_3, y_3)$, $P_3 = P_1 + P_2$ là:

$$x_3 = \frac{B(y_2 - y_1)^2}{(x_2 - x_1)^2} - A - x_1 - x_2 = \frac{B(x_2 y_1 - x_1 y_2)^2}{x_1 x_2 (x_2 - x_1)^2}$$
$$y_3 = \frac{(2x_1 + x_2 + A)(y_2 - y_1)}{x_2 - x_1} - \frac{B(y_2 - y_1)^3}{(x_2 - x_1)^3} - y_1$$

Doubling

Cho một điểm P_1 trên đường cong Montgomery $M_{A,B}$, điểm $[2]P_1$ đại diện cho điểm hình học của điểm giao nhau thứ ba giữa đường cong và đường tiếp tuyến tại P_1 ; vì vậy,

để tìm tọa độ của điểm $P_3 = 2P_1$, trong trường hợp này, đường thẳng $y = lx + m$ phải tiếp xúc với đường cong tại P_1 , do đó, nếu $M_{A,B} : f(x, y) = 0$ với

$$f(x, y) = x^3 + Ax^2 + x - By^2$$

giá trị của l biểu diễn hệ số góc của đường thẳng, cho bởi:

$$l = - \frac{\partial f}{\partial x} \bigg/ \frac{\partial f}{\partial y}$$

Vì vậy $l = \frac{3x_1^2 + 2Ax_1 + 1}{2By_1}$ và tọa độ điểm $P_3, P_3 = 2P_1$ là:

$$\begin{aligned} x_3 &= Bl^2 - A - x_1 - x_1 = \frac{B(3x_1^2 + 2Ax_1 + 1)^2}{(2By_1)^2} - A - x_1 - x_1 \\ &= \frac{(x_1^2 - 1)^2}{4By_1^2} = \frac{(x_1^2 - 1)^2}{4x_1(x_1^2 + Ax_1 + 1)} \\ y_3 &= (2x_1 + x_1 + A)l - Bl^3 - y_1 \\ &= \frac{(2x_1 + x_1 + A)(3x_1^2 + 2Ax_1 + 1)}{2By_1} - \frac{B(3x_1^2 + 2Ax_1 + 1)^3}{(2By_1)^3} - y_1. \end{aligned}$$

Edwards curve

Trong toán học, các đường cong Edwards là một họ các đường cong elip được Harold Edwards nghiên cứu năm 2007. Khái niệm về các đường cong elliptic trên các trường hữu hạn được sử dụng rộng rãi trong mã hóa đường cong elip. Các ứng dụng của các đường cong Edwards tới mật mã được Bernstein và Lange phát triển: chúng đã chỉ ra một số ưu điểm của dạng Edwards so với dạng Weierstrass.

Phương trình của một đường cong Edwards trên một trường K mà không có đặc tính 2 là:

$$x^2 + y^2 = 1 + dx^2y^2$$

cho một số vô hướng $d \in K \setminus \{0, 1\}$. Ngoài ra dạng sau với các tham số c và d được gọi là đường cong Edwards:

$$x^2 + y^2 = c^2(1 + dx^2y^2)$$

trong đó $c, d \in K$ với $cd(1 - c^4 \cdot d) \neq 0$

Mỗi đường cong Edwards tương đương với đường cong elip ở dạng Weierstrass, và do đó thừa nhận luật nhóm đại số một khi ta chọn một điểm để phục vụ như là một phần tử trung lập. Nếu K là hữu hạn, thì một số lượng đáng kể tất cả các đường cong elliptic trên K có thể được viết dưới dạng đường cong Edwards. Thông thường các đường cong elip ở dạng Edwards được xác định có $c = 1$, không mất tính tổng quát. Trong các phần sau, giả sử rằng $c = 1$.

Luật cộng

Trên bất kỳ đường cong elliptic nào, có một điểm gọi là phần tử đơn vị. Đối với đường cong Edwards, lấy phần tử trung tính là điểm $(0, 1)$, tổng các điểm (x_1, y_1) và (x_2, y_2) được đưa ra bởi công thức:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

Nghịch đảo của bất kì điểm nào (x_1, y_1) là $(-x_1, y_1)$. Người ta kiểm tra rằng điểm $(0, -1)$ có cấp là 2, và điểm $(\pm 1, 0)$ có cấp là 4. Trong thực tế, một đường cong Edwards luôn luôn có một điểm có cấp là 4 với tọa độ trong trường K . Nếu d không phải là một bình phương trong K và $(x_1, y_1), (x_2, y_2) \in \{(x, y) | x^2 + y^2 = 1 + dx^2y^2\}$, không có điểm đặc biệt có mẫu số $1 + dx_1x_2y_1y_2$ hoặc $1 - dx_1x_2y_1y_2$ bằng 0. Do đó, luật cộng Edwards là hoàn hảo khi d không phải là một bình phương trong trường K . Điều này có nghĩa là các công thức sẽ làm việc tốt và không có lỗi với các phép toán doubling, phần tử đơn vị, phần tử âm. Nói cách khác, nó được định nghĩa cho tất cả các cặp điểm đầu vào trên đường cong Edwards trên K và kết quả cho tổng của các điểm đầu vào. Nếu d là một bình phương trong K , thì phép toán tương tự có thể có các điểm đặc biệt, tức là có thể có cặp (x_1, y_1) và (x_2, y_2) trong đó $1 + dx_1x_2y_1y_2 = 0$ hoặc $1 - dx_1x_2y_1y_2 = 0$. Một trong những tính năng hấp dẫn của luật cộng của Edwards là nó được thống nhất mạnh mẽ, tức là nó cũng có thể được sử dụng để gấp đôi một điểm, đơn giản hóa việc bảo vệ chống lại tấn công bên kênh. Công thức cộng ở trên nhanh hơn các công thức thống nhất khác và có tính chất hoàn chỉnh mạnh.

Doubling

Doubling có thể được thực hiện với chính xác công thức tương tự như cộng. Doubling đề cập đến trường hợp trong đó các đầu vào (x_1, y_1) và (x_2, y_2) được biết là bằng nhau. Vì (x_1, y_1) nằm trên đường cong Edwards, ta có thể thay thế hệ số bằng $(x_1^2 + y_1^2 - 1)/x_1^2y_1^2$ như sau:

$$\begin{aligned} 2(x_1, y_1) &= (x_1, y_1) + (x_1, y_1) \\ 2(x_1, y_1) &= \left(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1 - dx_1^2y_1^2} \right) \\ &= \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - x_1^2 - y_1^2} \right) \end{aligned}$$

Điều này làm giảm mức độ mẫu số từ 4 đến 2, được phản ánh trong doubling. Luật cộng chung trong các tọa độ Edwards mất $10M + 1S + 1C + 1D + 7a$ và chi phí phép doubling là $3M + 4S + 3C + 6a$. Trong đó M là phép nhân trường, S là các phép bình phương trong trường, D là chi phí nhân với một tham số đường cong có thể lựa chọn và một trường bổ sung.

Twisted Edwards curve

Trong hình học đại số, các đường cong Twisted Edwards là mô hình mặt phẳng của các đường cong elip, một sự tổng quát của các đường cong Edwards được giới thiệu bởi Bernstein, Birkner, Joye, Lange và Peters trong năm 2008. Bộ đường cong được đặt tên theo nhà toán học Harold M. Edwards. Đường cong Elliptic rất quan trọng trong mật mã khóa công khai và các đường cong Twist Edwards nằm ở trung tâm của một lược đồ chữ ký điện tử gọi là EdDSA mang lại hiệu năng cao trong khi tránh các vấn đề bảo mật xuất hiện trong các chương trình chữ ký số khác.

Như tên cho thấy, mỗi đường cong Twist Edwards là một xoắn của một đường cong Edwards. Đường cong Twist Edwards $E_{a,d}$ trên một trường \mathbb{K} trong đó $\text{char}(\mathbb{K}) \neq 2$ là một đường cong mặt phẳng affine được xác định bởi phương trình:

$$E_{E_{a,d}} : ax^2 + y^2 = 1 + dx^2y^2$$

Ở đây a, d là các phần tử khác 0 của \mathbb{K} . Đường cong Edwards là đường cong Twist Edwards với $a = 1$. Mỗi đường cong Twist Edwards đều tương đương với đường cong elip ở dạng Montgomery và ngược lại.

Luật cộng

Cho \mathbb{K} là một trường có đặc điểm là khác 2. Để (x_1, y_1) và (x_2, y_2) là điểm trên đường cong Twist Edwards. Phương trình của đường cong Twist Edwards được viết như:

$$E_{E,a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$

Tổng của (x_1, y_1) và (x_2, y_2) trên $E_{E,a,d}$ là:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

Phần tử đơn vị là $(0, 1)$ và âm của điểm (x_1, y_1) là $(-x_1, y_1)$. Công thức này cũng làm việc với doubling. Nếu a là một bình phương trong \mathbb{K} và d không phải bình phương trong \mathbb{K} , công thức trên là hoàn tất. Điều này có nghĩa là chúng ta có thể công thức cho tất cả các cặp điểm mà không xảy ra ngoại lệ.

Doubling

Doubling có thể được thực hiện với chính xác công thức tương tự như phép cộng. Doubling một điểm (x_1, y_1) trên đường cong $E_{E,a,d}$ là: $[2](x_1, y_1) = (x_3, y_3)$ ở đây

$$x_3 = \frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1} = \frac{2x_1y_1}{ax_1^2 + y_1^2}$$

$$y_3 = \frac{y_1y_1 - ax_1x_1}{1 - dx_1x_1y_1y_1} = \frac{y_1^2 - ax_1^2}{2 - ax_1^2 - y_1^2}.$$

2.3 Mật mã dựa trên đường cong Elliptic

Chúng ta bắt đầu với ứng dụng đơn giản nhất, trao đổi khóa Diffie – Hellman, ít liên quan đến việc thay thế vấn đề logarit rời rạc cho trường \mathbb{F}_p hữu hạn với bài toán logarit rời rạc cho đường cong elip $E(\mathbb{F}_p)$. Sau đó chúng ta sẽ mô tả các tương tự elliptic của hệ thống mã khóa công khai Elgamal và thuật toán chữ ký số (DSA).

Trao đổi khóa với Elliptic Diffie-Hellman

Alice và Bob đồng ý sử dụng một đường cong elliptic đặc biệt $E(\mathbb{F}_p)$ và một điểm cụ thể $P \in E(\mathbb{F}_p)$. Alice chọn số nguyên n_A bí mật và Bob chọn số nguyên n_B bí mật. Họ tính toán các bội số liên quan

$$\overbrace{Q_A = n_A P}^{Alice} \quad \text{and} \quad \overbrace{Q_B = n_B P}^{Bob}$$

và họ trao đổi các giá trị của Q_A và Q_B . Sau đó Alice sử dụng hệ số bí mật của mình để tính toán $n_A Q_B$, và Bob tương tự tính toán $n_B Q_A$. Bây giờ họ có giá trị bí mật được chia sẻ

$$n_A Q_B = (n_A n_B)P = n_B Q_A,$$

mà họ có thể sử dụng như một chìa khóa để giao tiếp riêng tư thông qua một mật mã đối xứng. Tổng quát trao đổi khóa elliptic Diffie–Hellman

Public parameter creation	
A trusted party chooses and publishes a (large) prime p , an elliptic curve E over \mathbb{F}_p , and a point P in $E(\mathbb{F}_p)$.	
Private computations	
Alice	Bob
Chooses a secret integer n_A . Computes the point $Q_A = n_A P$.	Chooses a secret integer n_B . Computes the point $Q_B = n_B P$.
Public exchange of values	
Alice sends Q_A to Bob $\xrightarrow{\hspace{2cm}}$ Q_A	
$Q_B \xleftarrow{\hspace{2cm}}$ Bob sends Q_B to Alice	
Further private computations	
Alice	Bob
Computes the point $n_A Q_B$. The shared secret value is $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.	Computes the point $n_B Q_A$.

Hình 2.5:

Hệ thống mã khóa công khai Elgamal

Alice và Bob đồng ý sử dụng một số nguyên tố p cụ thể, đường cong elliptic E và điểm $P \in E(\mathbb{F}_p)$. Alice chọn một số nhân n_A bí mật và điểm $Q_A = n_A P$ làm khóa công khai của cô ấy. Nội dung của Bob là một điểm $M \in E(\mathbb{F}_p)$. Anh ta chọn một số nguyên k là yếu tố ngẫu nhiên của anh ấy và các tính toán

$$C_1 = kP \quad \text{and} \quad C_2 = M + kQ_A.$$

Anh ấy sẽ gửi hai điểm (C_1, C_2) đến Alice và Alice sẽ tính:

$$C_2 - n_A C_1 = (M + kQ_A) - n_A(kP) = M + k(n_A P) - n_A(kP) = M$$

để phục hồi bản rõ. Tổng quát hệ mã khóa công khai Elgamal

Trong thực tế, hệ mã khóa công khai Elgamal elliptic hoạt động tốt, nhưng có một số khó khăn thực tế

- 1, Không có cách rõ ràng để đính kèm các tin nhắn văn bản vào các điểm trong $E(\mathbb{F}_p)$
- 2, Hệ thống mã hóa elgamal elliptic có hệ số mở rộng 4 đến 1, so với tỷ lệ mở rộng 2 đến 1 của Elgamal khi sử dụng \mathbb{F}_p .

Public parameter creation	
A trusted party chooses and publishes a (large) prime p , an elliptic curve E over \mathbb{F}_p , and a point P in $E(\mathbb{F}_p)$.	
Alice	Bob
Key creation	
Choose a private key n_A . Compute $Q_A = n_A P$ in $E(\mathbb{F}_p)$. Publish the public key Q_A .	
Encryption	
	Choose plaintext $M \in E(\mathbb{F}_p)$. Choose a random element k . Use Alice's public key Q_A to compute $C_1 = kP \in E(\mathbb{F}_p)$. and $C_2 = M + kQ_A \in E(\mathbb{F}_p)$. Send ciphertext (C_1, C_2) to Alice.
Decryption	
Compute $C_2 - n_A C_1 \in E(\mathbb{F}_p)$. This quantity is equal to M .	

Hình 2.6:

Lý do ElGamal elip có một mở rộng thông điệp 4 đến 1 nằm trong thực tế là bản rõ M là một điểm duy nhất trong $E(\mathbb{F}_p)$. Bản mã (C_1, C_2) bao gồm bốn số modulo p , vì mỗi điểm trong $E(\mathbb{F}_p)$ có hai tọa độ. Các phương pháp khác nhau đã được đề xuất để giải quyết những vấn đề này. Khó khăn trong việc liên kết các bản rõ với các điểm có thể được phá vỡ bằng cách chọn M ngẫu nhiên và sử dụng nó làm mặt nạ cho bản rõ thô thực sự. Với ví dụ Alice và Bob. Thật không may, vì Alice phải tính toán $C_2 - n_A C_1$, cô ấy cần các giá trị chính xác của cả hai tọa độ x và y của C_1 và C_2 . Tuy nhiên, tọa độ x của một điểm xác định tọa độ y lên để thay đổi dấu, vì vậy Bob có thể gửi thêm một bit, ví dụ

$$\lambda = \begin{cases} 0 & \text{if } 0 \leq y \leq \frac{1}{2}p, \\ 1 & \text{if } \frac{1}{2} < y < p \end{cases}$$

Theo cách này, Bob chỉ cần gửi các tọa độ x của C_1 và C_2 , cộng thêm hai bit phụ. Ý tưởng này đôi khi được gọi là nén điểm.

Thuật toán chữ ký số với Elliptic

Thuật toán chữ ký số với Elliptic được mô tả sau đây:
tương tự như thuật toán chữ ký số đơn giản của DSA. ECDSA đang được sử dụng rộng rãi, đặc biệt là trong các tình huống mà kích thước chữ ký là quan trọng.

Để chứng minh rằng ECDSA hoạt động, tức là bước xác minh thành công trong việc

Public parameter creation	
A trusted party chooses a finite field \mathbb{F}_p , an elliptic curve E/\mathbb{F}_p , and a point $G \in E(\mathbb{F}_p)$ of large prime order q .	
Samantha	Victor
Key creation	
Choose secret signing key $1 < s < q - 1$. Compute $V = sG \in E(\mathbb{F}_p)$. Publish the verification key V .	
Signing	
Choose document $d \bmod q$. Choose random element $e \bmod q$. Compute $eG \in E(\mathbb{F}_p)$ and then, $s_1 = x(eG) \bmod q$ and $s_2 \equiv (d + ss_1)e^{-1} \pmod{q}$. Publish the signature (s_1, s_2) .	
Verification	
	Compute $v_1 \equiv ds_2^{-1} \pmod{q}$ and $v_2 \equiv s_1s_2^{-1} \pmod{q}$. Compute $v_1G + v_2V \in E(\mathbb{F}_p)$ and verify that $x(v_1G + v_2V) \bmod q = s_1$.

Hình 2.7:

xác minh chữ ký hợp lệ, chúng ta tính toán:

$$\begin{aligned}
v_1G + v_2V &= ds_2^{-1}G + s_1s_2^{-1}(sG) \\
&= (d + ss_1)s_2^{-1}G \\
&= (es_2)s_2^{-1}G \\
&= eG \in E(\mathbb{F}_p).
\end{aligned}$$

Do đó:

$$x(v_1G + v_2V) \bmod q = x(eG)$$

Chữ kí được chấp nhận là hợp lệ.

Chương 3

Chứng thư số ẩn dựa trên đường cong Elliptic

Trong chương này xác định sơ đồ chứng thư số ẩn của Elliptic Curve Qu-Vanstone (ECQV). Sơ đồ chứng thư số ẩn ECQV được xem như là một lược đồ chứng thư với mục đích chung cho các ứng dụng trong các hệ thống máy tính và truyền thông. Nó đặc biệt thích hợp cho các môi trường ứng dụng nơi có các tài nguyên như băng thông, sức mạnh tính toán và lưu trữ bị hạn chế. ECQV cung cấp giải pháp thay thế hiệu quả hơn cho chứng chỉ truyền thống.

Mục đích của chương này là để xem xét việc triển khai sơ đồ chứng thư số ẩn

3.1 Hàm băm

Hàm băm được sử dụng trong lược đồ ECQV để tính toán thông điệp của chứng chỉ được tạo hoặc xác minh. Hàm băm cũng được sử dụng trong việc tạo và xác thực tham số miền elliptic ngẫu nhiên một cách chính xác, và cũng có thể được sử dụng trong các quá trình tạo số ngẫu nhiên.

Mức độ bảo mật kết hợp với hàm băm phụ thuộc vào ứng dụng của nó. Trường hợp tránh xung đột là cần thiết, mức độ bảo mật tối đa bằng một nửa độ dài đầu ra (tính theo bit) của hàm băm. Trường hợp tránh xung đột là không cần thiết, mức độ bảo mật tối đa là độ dài đầu ra (tính theo bit) của hàm băm. Khả năng tránh xung đột nói chung là cần thiết để tính toán thông điệp cho chữ ký số.

Hàm băm được sử dụng bởi sơ đồ ECQV sẽ được chấp nhận hàm băm, như được chấp thuận trong mục đăng ký X9 00003, tiêu chuẩn băm an toàn (SHS). Mức độ bảo mật của hàm băm được phê duyệt được coi là tối đa một nửa độ dài đầu ra của nó cho các mục đích của tiêu chuẩn này. Danh sách một số hàm băm tiêu chuẩn SHA-1, SHA-2, MD5,

Hàm băm được sử dụng để tính toán chứng thư ẩn sẽ là hàm băm có mức bảo mật ít nhất là mức bảo mật của việc triển khai ECQV. Hàm băm được sử dụng cho các xác định tham số elliptic sẽ là hàm băm có mức bảo mật là mức độ bảo mật của việc triển khai sơ đồ ECQV (ngoại trừ các xác định tham số elliptic ngẫu nhiên trong [SEC 2] được tạo bằng cách sử dụng SHA-1).

3.2 Hàm băm một số nguyên modul n

Trong nhiều bước của ECQV, một chuỗi octet (mỗi một ký tự trong xâu được biểu diễn bởi 8 bits) chiều dài tùy ý được băm bằng hàm băm mật mã H , và sau đó được chuyển đổi thành một số nguyên modulo n . Phần này chỉ định hàm kết quả, ký hiệu $H_n : \{0, 1, \dots, 255\}^* \rightarrow [0, \dots, n - 1]$, ánh xạ các chuỗi octet có độ dài tùy ý đến các số nguyên modulo n .

Input

1. Một chuỗi octet có chiều dài tùy ý S .
2. Hàm băm H băm chuỗi octet chiều dài tùy ý thành các chuỗi bit dài của hashlen.
3. Số nguyên n .

Action

1. Tính toán $h = H(S)$, một chuỗi bit dài hashlen bits.
2. Lấy một số nguyên e từ h như sau:
 - 2.1 Đặt E bằng $\lfloor \log_2 n \rfloor$ bits trái nhất của h .
 - 2.2 convert xâu bit E thành xâu octet E' , sử dụng Bit-String-to-Octet-String trong [SEC 1].
 - 2.3 convert xâu octet E' thành số nguyên e sử dụng Octet-String-to-Integer trong [SEC 1].

Output Số nguyên e , nằm trong khoảng $[0, \dots, n - 1]$.

Lưu ý rằng nếu miền H bị giới hạn ở kích thước tối đa thì miền H_n bị hạn chế theo cùng một cách.

3.3 Khởi tạo một số ngẫu nhiên

Với tiêu chuẩn chứng thư số, tất cả các giá trị ngẫu nhiên phải được tạo bằng trình tạo số ngẫu nhiên được chấp thuận có mức độ bảo mật ít nhất là mức độ bảo mật của việc thực hiện ECQV. Trình tạo số ngẫu nhiên phải tuân thủ ANSI X9.82 hoặc NIST Special Publication 800-90A [NIST 800-90A]. Một bộ tạo số ngẫu nhiên phù hợp cũng được mô tả trong [SEC 1, 3.10]

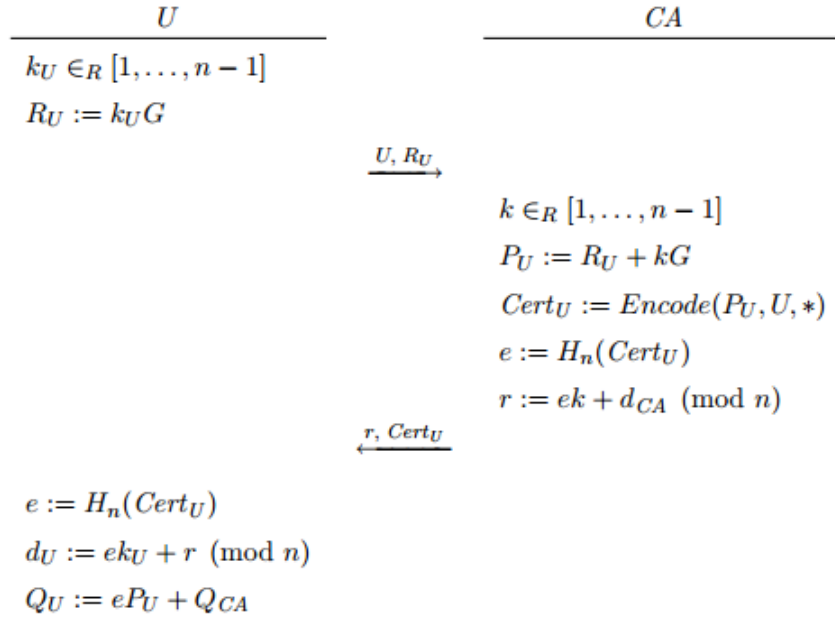
3.4 Các tham số khởi tạo và hợp lệ

3.5 Sơ đồ chứng thư số thực ECQV

3.5.1 Tổng quan

Sơ đồ chứng chỉ số ẩn được sử dụng bởi ba thực thể - Tổ chức phát hành chứng chỉ CA, người yêu cầu chứng chỉ U và bộ xử lý chứng chỉ V . Người yêu cầu U sẽ nhận được

chứng chỉ số ẩn từ CA, xác nhận danh tính của U và cho phép V lấy khóa công khai của U.



Hình 3.1:

Sơ đồ chứng thư số ẩn bao gồm sáu phần. Những phần này sẽ được mô tả chi tiết.

ECQV_Setup: Trong bước này, CA thiết lập các tham số đường cong elliptic, hàm băm, định dạng mã hóa chứng chỉ và tất cả các bên đã chọn một trình tạo số ngẫu nhiên. CA tạo ra một cặp khóa. Tất cả các bên phải nhận được bản sao xác thực các thông số và khóa công khai của CA.

Cert_Request: Người yêu cầu U phải tạo một yêu cầu cho một chứng chỉ, được gửi đến CA. Thành phần mật mã của yêu cầu là khóa công khai, được tạo ra bằng cách sử dụng cùng thủ tục như CA sử dụng trong khi thiết lập ECQV.

Cert_Generate: Khi nhận được yêu cầu chứng chỉ từ U, CA xác nhận danh tính của U và tạo chứng chỉ số ẩn. CA gửi phản hồi cho U.

Cert_PK_Extraction: Với chứng chỉ số ẩn cho U người dùng, thông số và khóa công khai của CA, thuật toán trích xuất khóa công khai tính toán khóa công khai của U.

Cert_Reception: Sau khi nhận được phản hồi cho yêu cầu chứng chỉ của mình, U đảm bảo tính hợp lệ của cặp khóa được chứng nhận ngầm

3.5.2

Chương 4

Cài đặt cho thiết bị IoT

Kết luận và hướng phát triển

Tài liệu tham khảo

- [1] Sách Giáo trình Cơ sở An toàn Thông tin thầy Nguyễn Văn Khanh - Đại học Bách Khoa.