The GH Public-key Cryptosystem

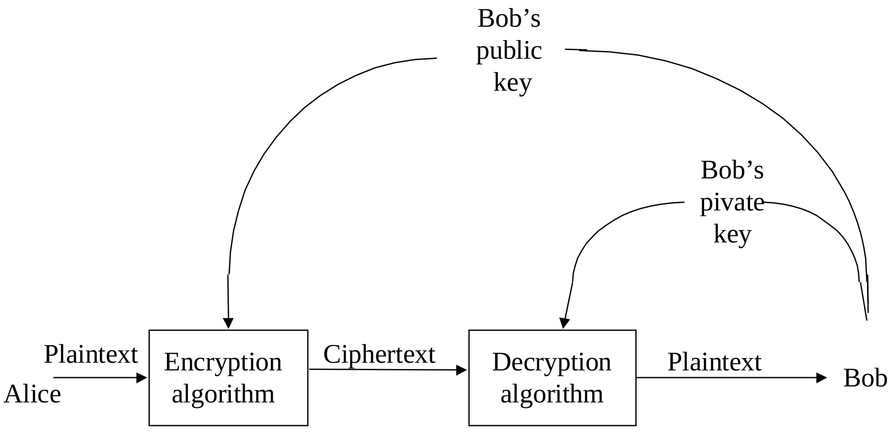
Guang Gong
Dept. of Electrical and Computer Engineering
University of Waterloo
ggong@shannon1.uwaterloo.ca
http://www.cacr.math.uwaterloo.ca/~ggong

Presentation Outline

- Overview for Public-key Cryptography
- The GH Public-key Cryptosystem
- Related Cryptosystems and Comparison

Public-Key Cryptography

- A Model for Public-Key Cryptography
- Requirements for Public-Key Cryptography
- Security of Public-Key Cryptosystems
- Widely Used Public-Key Cryptosystems



Simplified Model of Public-Key Encryption

Requirements for Public-key Cryptography

One-way function:

$$\begin{tikzcd} x \arrow[rr, shift left=1.5, "\text{easy}"] & & f(x) \arrow[ll, shift left=1.5, "\text{infeasible}"'] \end{tikzcd}$$

Trapdoor one-way function:

$$\begin{tikzcd} x \arrow[rr, shift left=1.5, "\text{easy}"] & & f_k(x) \arrow[ll, shift left=1.5, "\text{infeasible if } k \text{ is unknown}"', "\text{easy if } k \text{ is known}"] \end{tikzcd}$$

Security of Public-Key Cryptosystems

Based on the difficulty of different computational problems. Most important ones are

- Factoring large integers
- Finite field discrete logarithms
- Elliptic curve discrete logarithms

Public-key Cryptosystems

- DH (Diffie-Hellman) key agreement, 1976
- RSA, 1978
- DSS (Digital Signature Standard), NIST 1994, (a variation of ElGamal digital signature scheme, 1985)
- Elliptic curve public-key cryptosystems (ECC), Koblitz 1987, Miller 1985, Menezes and Vanstone 1990

DH Key Agreement Protocol

System public parameters:

p: a prime number

g: a primitive element in $GF(p)$.

Alice:

Private key: e, $0<e<p$, and $\gcd(e, p-1)=1$

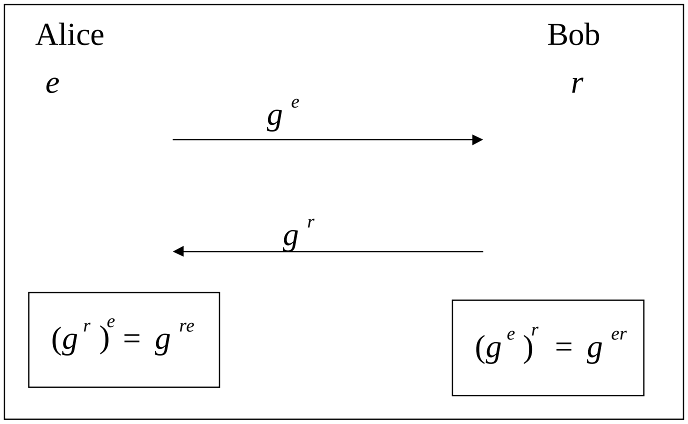
Public key: $y_A = g^e$

Bob:

Private key: r, $0<r<p$, and $\gcd(r, p-1)=1$

Public key: $y_B = g^r$

DH Key Agreement Protocol (Con.)



Alice

e

Bob

r

g^e

g^r

$(g^r)^e = g^{re}$

$(g^e)^r = g^{er}$

DH Key Agreement Protocol (Con.)

- Underline mathematical structure: finite fields
- Security: based on the difficulty of solving the discrete logarithm in a finite field $GF(p)$:

  Known g, y_A , y_B: $y_A = g^e$ and $y_B = g^r$

  Solving for e or r in $GF(p)$
- Fast evaluation for exponentiation

The GH (Gong-Harn) Public-key Cryptosystem

- Preliminaries
- Third-order Characteristic Sequences
- Motivation of GH-PKS
- Two Theorems on 3rd-order Characteristic sequences
- GH-DH Key Agreement Protocol

Preliminaries

- Finite Fields and Trace Functions
- Linear Feedback Shift Register (LFSR) Sequences
- Irreducible Polynomials and LFSR Sequences

Finite Fields

- Finite Field GF(p), a field with p elements, where p is a prime, operations performed by modulo p.

- $GF(p^n)$, an extension of GF(p), defined by an irreducible polynomial over GF(p) of degree n.

GF(11)={ 0, 1, 2, 3, 4, 5, 6, 7, 8 , 9, 10}

$2^0 \equiv 1 \bmod 11$,

$2^1 \equiv 2 \bmod 11$,

$2^2 \equiv 4 \bmod 11$,

$2^3 \equiv 8 \bmod 11$,

$2^4 \equiv 5 \bmod 11$,

$2^5 \equiv 10 \bmod 11$

$2^6 \equiv 9 \bmod 11$

$2^7 \equiv 7 \bmod 11$

$2^8 \equiv 3 \bmod 11$

$2^9 \equiv 6 \bmod 11$

$2^{10} \equiv 1 \bmod 11$

2 is a primitive element of GF(11)

GF(3^2), defined by $h(x) = x^2 - x + 2$

(1, α)		(1, α)	
1 0	$= \alpha^0$	0 1	$= \alpha$
1 1	$= \alpha^2$	1 2	$= \alpha^3$
2 0	$= \alpha^4$	0 2	$= \alpha^5$
2 2	$= \alpha^6$	2 1	$= \alpha^7$

$\alpha^8 = 1$ (α, a root of $h(x)$)

Trace Functions

A trace function from GF(q^n) to GF(q) is defined by

$$Tr(x) = x + x^q + \ldots + x^{q^{n-1}}$$

where q is a prime or a power of a prime.

For example, $n = 3$ and $q = 5$, the trace function from GF(5^3) to GF(5):

$$Tr(x) = x + x^5 + x^{5^2}, \ x \in \text{GF}(5^3)$$

LFSR Sequences

- K = GF(q) where $q = p^n$,
- $f(x) = x^r - c_{r-1} x^{r-1} - \ldots - c_1 x - c_0$, $c_i \in K$,
- $\{s_i\} = s_0, s_1, s_2, \ldots , \ s_i \in K.$

If the sequence $\{s_i\}$ satisfies the following linear recursive relation

$$s_{k+r} = \sum c_i s_{k+i} , k = 0, 1, 2, \ldots,$$

then we say that $\{s_i\}$ is an LFSR sequence of order r over K (*generated by f(x)*).

LFSR Sequences (Con.)

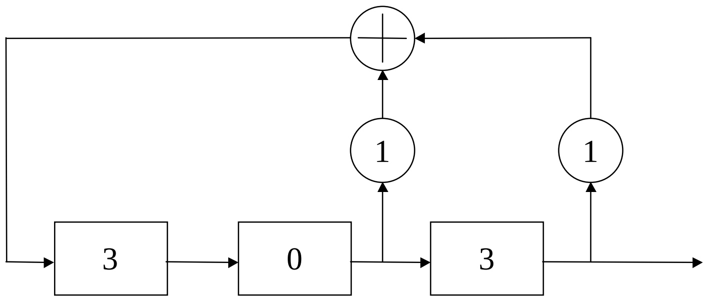
Example 1. Let K = GF(5), r = 3 and $f(x) = x^3 + x - 1$ which is irreducible over K.

An LFSR sequence generated by $f(x)$:

3 0 3 3 2 0 1 2 4 4
3 0 1 3 4 3 4 1 4 3
2 1 1 1 0 0 1 0 4 1
1 ...

which has period $31 = 5^2 + 5 + 1$.

LFSR Sequences (Con.)



3rd-Order LFSR

Irreducible Polynomials and Sequences

- We say that $f(x)$ has period t if t is the smallest integer such that $f(x)$ divides $x^t - 1$.
- If $f(x)$ is irreducible over K, then period of $f(x)$ is equal to period of the sequence $\{s_i\}$.

Third-order Characteristic Sequences

Let

$$f(x) = x^3 - a\,x^2 + bx - 1,\ a, b \in GF(q),$$

be irreducible over K. Let $\{s_i\}$ be an LFSR sequence generated by $f(x)$. If an initial state of $\{s_i\}$ is given by

$$s_0 = 3,\ s_1 = a, \text{ and } s_2 = a^2 - 2b,$$

then $\{s_i\}$ is called a characteristic sequence.

Third-order Characteristic Sequences (Con.)

Profiles:

- period : a factor of $q^2 + q + 1$
- trace representation:

$s_k = Tr(\alpha^k) = \alpha^k + \alpha^{kq} + \alpha^{kq^2}$, $k = 0, 1, \ldots$

where α is a root of $f(x)$ in the extension field GF(q^3).

Motivation of GH-PKS

- Develop a PKC whose security is based on the difficulty of solving the discrete logarithm (DL) in GF(q^3), but all computation are performed in GF(q).
- Ideal candidate: LFSR sequences of order 3.

Motivation of GH-PKS (Con.)

Two issues need to be solved:

- Commutative law among the terms of 3rd-order char. sequences.
- Fast computation algorithm for evaluating s_k, the k^{th} term of the sequence.

Two Theorems

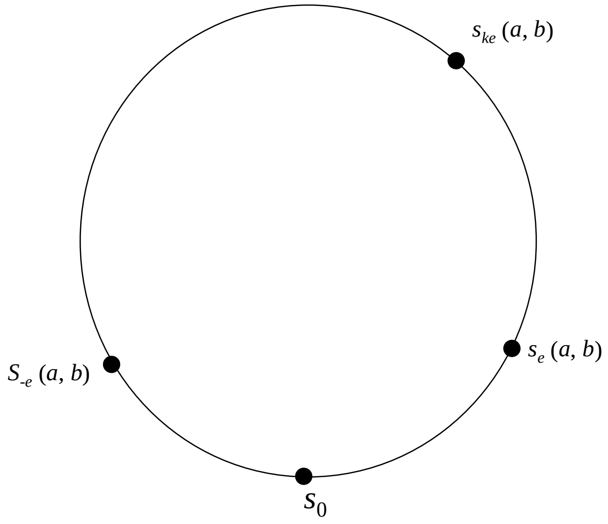
We denote $s_k = s_k(a, b)$.

Theorem 1 (Commutative Law).

Let $f(x) = x^3 - a x^2 + bx - 1$ be irreducible over GF(q) and $\{s_i\}$ be the char. sequence generated by $f(x)$. Then for any positive integers k and e,

$$s_k(s_e(a, b), s_{-e}(a, b)) = s_{ke}(a, b)$$

where $s_{-e}(a, b) = s_e(b, a)$ which is the reciprocal sequence of the sequence $\{s_i(a, b)\}$.



Theorem 2 (Fast Evaluation Algorithm)

Let $k = \sum_{i=0}^{r} k_i 2^{r-i}$ be the binary representation of *k*. Let $T_0 = k_0 \neq 0$ and $T_j = k_j + 2T_{j-1}$, $1 \leq j \leq r$. So, $T_r = k$. Then the *k*th terms of a pair of the reciprocal char. sequences can be computed iteratively as follows:

For $k_j = 0$,

$$s_{T_j - 1} = s_{T_{j-1}} s_{T_{j-1}-1} - b s_{-T_{j-1}} + s_{-(T_{j-1}+1)} ,$$

$$s_{T_j} = s^2_{T_{j-1}} - 2s_{-T_{j-1}} \text{, and}$$

$$s_{T_j+1} = s_{T_{j-1}} s_{T_{j-1}+1} - a s_{-T_{j-1}} + s_{-(T_{j-1}-1)} .$$

For $k_j = 1$,

$$s_{T_j - 1} = s^2_{T_{j-1}} - 2s_{-T_{j-1}} ,$$

$$s_{T_j} = s_{T_{j-1}} s_{T_{j-1}+1} - a s_{-T_{j-1}} + s_{-(T_{j-1}-1)} \text{, and}$$

$$s_{T_j+1} = s^2_{T_{j-1}+1} - 2s_{-(T_{j-1}+1)} .$$

Thus evaluation of a pair of the *k*th terms s_k and s_{-k} needs 9log*k* multiplications in GF(*q*) in average.

GH-DH Key Agreement Protocol

Key generation phase:

System public parameters:

p: a prime number and $q = p^2$

$f(x) = x^3 - a x^2 + bx - 1$:irreducible over GF($q$) with period $Q = q^2 + q + 1$.

Alice:

Private key: e, $0<e<Q$, and $\gcd(e, Q) = 1$

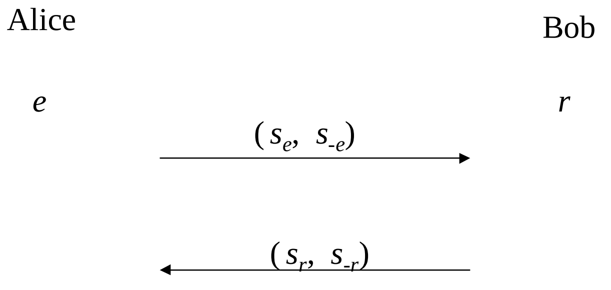
Public key: (s_e, s_{-e})

Bob:

Private key: r, $0<r<Q$, and $\gcd(r, Q) = 1$

Public key: (s_r, s_{-r})

Key distribution phase


Alice

Bob

e

r

(s_e, s_{-e})

(s_r, s_{-r})

$s_e(s_r, s_{-r}) = s_{er}$
$s_{-e}(s_r, s_{-r}) = s_{-er}$

$s_r(s_e, s_{-e}) = s_{re}$
$s_{-r}(s_e, s_{-e}) = s_{-re}$

common key: (s_{er}, s_{-er})

Example 2. For simplicity, we will use $q = p = 5$ to demonstrate the GH-DH key agreement protocol.
System parameters: $q = p = 5$ and $f(x) = x^3 + x - 1$.

- **Alice:**

$e = 4$, $(s_4, s_{-4}) = (3, 4)$

Using Bob's public-key to form a pair of the reciprocal polynomials:

$f_9(x) = x^3 - x^2 - 1$ and

$f_{-9}(x) = x^3 + x - 1$

$f_9(x)$: 3 1 1 4 $\boxed{0}$ 1 0 …

$f_{-9}(x)$: 3 0 3 3 $\boxed{2}$ 0 1 ...

$s_4(s_9, s_{-9}) = 0$ and $s_{-4}(s_9, s_{-9}) = 2$

Common key: (0, 2)

- **Bob:**

$r = 9$, $(s_9, s_{-9}) = (1, 0)$

Using Alic's public-key to form a pair of the reciprocal polynomials:

$f_4(x) = x^3 - 3x^2 + 4x - 1$ and

$f_{-9}(x) = x^3 - 4x^2 + 3x - 1$

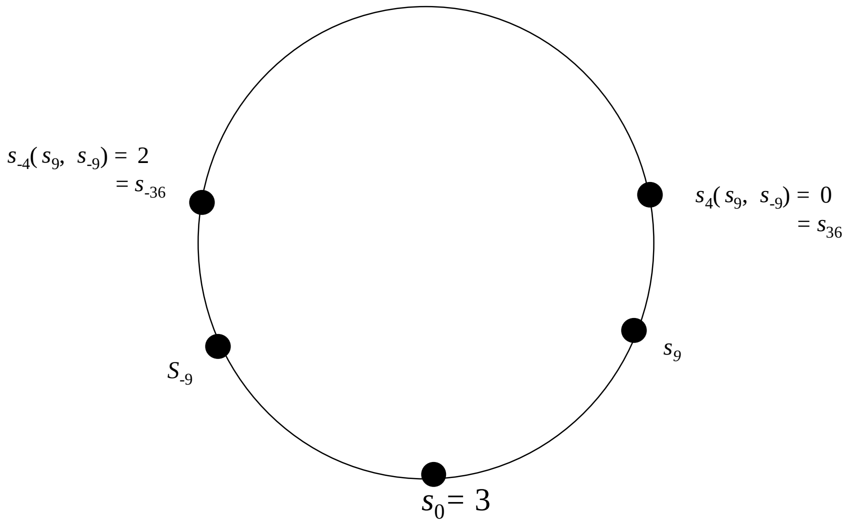
$f_4(x)$: 3 3 1 4 1 3 4 1 0 $\boxed{0}$ …

$f_{-4}(x)$: 3 4 0 1 3 4 3 3 2 $\boxed{2}$ ...

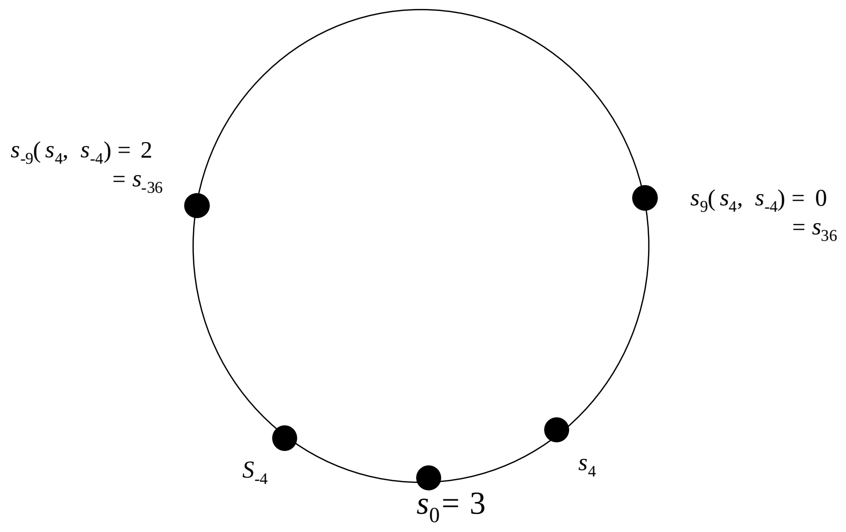
$s_9(s_4, s_{-4}) = 0$ and $s_{-9}(s_4, s_{-4}) = 2$

Common key: (0, 2)

Alice



Bob



$s_{-9}(s_4, s_{-4}) = 2$
$= s_{-36}$

$s_9(s_4, s_{-4}) = 0$
$= s_{36}$

S_{-4}

s_4

$s_0 = 3$

Profile of GH-DH

- Security: the difficulty of solving discrete logarithm in the finite field $GF(p^6)$
- One-to-one correspondence between the private key space and the public key space
- 170 bits GH-DH ⇔ 170 bits EC-DH
  ⇔ 1024 bit RSA
  ⇔ 1024 bits DH

Related Cryptosystems and Comparison

- XTR Public-key Cryptosystem
- Comparison among GH-DH, EC-DH, DH (RSA), and XTR-DH

XTR (Lanstra and Verheul, Crypto'2000) — A Special Case of GH

XTR: System public parameters:

p: a prime number and $q = p^2$

$f(x) = x^3 - a x^2 + a^p x - 1$:irreducible over GF($q$) with period Q, | $p^2 - p + 1$.

Alice:

Private key: e, $0<e<Q$

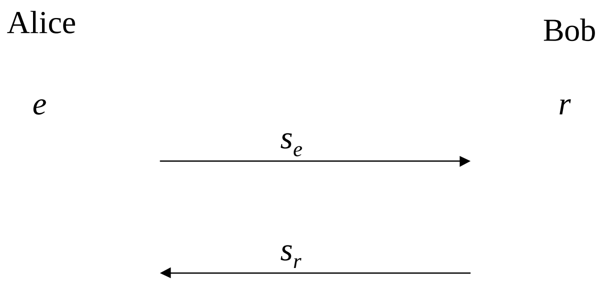
Public key: s_e

Bob:

Private key: r, $0<r<Q$

Public key: s_r

XTR (Con.)



Alice

Bob

e

r

s_e

s_r

$s_e(s_r,\ s_r^{\ p}) = s_{er}$

$s_r(s_e,\ s_e^{\ p}) = s_{re}$

common key: s_{er}

	GH-DH	XTR	EC-DH	DH
security level: the discrete logarithm in GF(p^6)	170-bit p	170-bit p	170-bit p	1024-bit $p_{DH:}$ $\log p_{DH} \approx 6\log p$
, where S, the set of all private keys; T, the set of all possible public keys	v, a 1-1 map	v, multiple to one map	v, a 1-1 map	v, a 1-1 map
user private key size:	4log$p$-bit	2log$p$-bit	logp-bit	6log$p$-bit
user public key size	4log$p$-bit	2log$p$-bit	2log$p$-bit	6log$p$-bit
common key size: C_{key}	4log$p$-bit	2log$p$-bit	2log$p$-bit	6log$p$-bit
communication involved in each key distribution : T_{key}	4log$p$-bit	2log$p$-bit	2log$p$-bit	6log$p$-bit
Ratio *I*: communication cost per one bit common key	**1**	**1**	**1**	**1**
computation cost of each section	20log$p$ modulo p multiplication	8log$p$ modulo p multiplication	1.5log$p$ additions of points on an elliptic curve	1.5logp_{DH} modulo p_{DH} multiplication $\approx 36\times 1.5\log p^6$ modulo p multiplication
Ratio *J*: computation cost per one bit common key	20log$p$/4log$p$ **= 5**	8log$p$/2log$p$ = **4**	**>>10**	$\approx 36\times 1.5\log p^6$ /6logp = **54**

Reference

G. Gong and L. Harn, Public-key cryptosystems based on cubic finite field extensions, *IEEE Trans. on Inform. Theory*, vol. IT-45, No.7, November 1999, pp. 2601-2605.

GH-RSA is also discussed in this paper.

References of Related Work

- W. Diffie and M.E. Hellman, “New directions in cryptography,” *IEEE Trans. On Inform. Theory*, vol. IT-22, November 1976, pp.644-654.

  Comments: Exponentiation in DH can be considered as evaluating k^{th} term of a first order LFSR sequence over GF(q).
- W.B. Müller and W. Nöbauer, "Cryptanalysis of the Dickson-scheme, " *Advances in Cryptology, Proceedings of Eurocrypt'85*, pp. 71-76.

  P. Smith, "LUC public-key encryption, " *Dr. Dobb's Journal*, pp. 44-49, January 1993.

  Comments: The mathematical function used in this family of the public-key cryptosystems is a 2nd-order LFSR characteristic sequence over GF(p) or Z_n.
- A.K. Lenstra and E.R. Verheul, The XTR public key systems, *Advances in Cryptology, Proceedings of Crypto2000*, pp. 1-19, August, 2000.

  Comments: the mathematical function is a 3rd-order LFSR characteristic sequence over GF(p^2) which is a special case of the sequences used in the GH public key cryptosystem.