主流的密码学 hardness/computational 假设

1. Discrete logarithm problem

Let g为 a known element of prime order r in a group (with group operation written multiplicatively). Let $G=<g>$ be the group generated by g.

常用的group选择有：

- multiplicative group of a finite field;
- algebraic torus over a finite field;
- elliptic curve over a finite field;
- divisor class group of a curve over a finite field。

Discrete logarithm problem常用假设有：

- DLP: discrete logarithm problem。常用于Schnorr signatures, DSA signatures。
  已知$h\in G$，找到x使得$h=g^x$。
- CDH: computational Diffie-Hellman problem。常用于 Diffie-Hellman key exchange and variants, Elgamal encryption and variants, BLS signatures and variants。
  已知$g^a, g^b\in G$，计算g^{ab}。
- SDH: static Diffie-Hellman problem。
  Fix $g, g^a\in G$. Given $h\in G$，计算h^a。
- gap-CDH: Gap Diffie-Hellman problem。常用于 ECIES proof in the Random Oracle Model, Chaum undeniable signature。
  已知$g^a, g^b\in G$，计算g^{ab}，when the algorithm has access to an oracle which solves the DDH problem。
- DDH: decision Diffie-Hellman problem。常用于 Diffie-Hellman key exchange and variants, Elgamal encryption and variants.
  已知$g^a, g^b, h\in G$，判断$h=g^{ab}$是否成立?
- Strong-DDH: strong decision Diffie-Hellman problem
  已知$g, g^a, g^b, g^{b^{-1}}, h\in G$，判断$h=g^{ab}$是否成立?
- sDDH: skewed decision Diffie-Hellman problem。
  Let f 为任意的uninvertible function with domain $\mathbb{Z}_r$。已知$f(a), g^b, h\in G$，判断$h=g^{ab}$是否成立?
- PDDH: parallel decision Diffie-Hellman problem。
  已知$g^{x1},\cdots,g^{xn},h_1,\cdots,h_n\in G$，判断$h_1=g^{x1x2},\cdots,h_{n-1}=g^{x_{n-1}x_n},h_n=g^{x_nx1}$是否成立?
- Square-DH: Square Diffie-Hellman problem. The best known algorithm for Square-DH is to actually solve the DLP.
  已知$g^a\in G$，计算g^{a^2}。
- I-DHI: I-Diffie-Hellman inversion
  to actually solve the DHP.

已知$g^a, g^{a^2}, \cdots, g^{a^l} \in G$，计算$g^{1/a}$。

- l-DDHI: l-Decisional Diffie-Hellman inversion problem
  已知$g^a, g^{a^2}, \cdots, g^{a^l}, v \in G$，判断$v = g^{1/a}$是否成立?
- REPRESENTATION: Representation problem. The best known algorithm for REPRESENTATION is to solve the DLP.
  已知$g_1, \cdots, g_k, h \in G$，找到$a_1, \cdots, a_k$使得$h = g_1^{a1} \cdots g_k^{ak}$ 成立。
- LRSW: LRSW Problem. The best known algorithm for LRSW is to solve the DLP.
  已知g, g^x, g^y，已知 oracle O（输入为 s，其选择一个随机值 $a = g^z$，然后其输出为(a, a^{sy}, a^{x+sxy})），对于任意的t（not one of the 输入s）和$b \neq 1$值 计算$(t, b, b^{ty}, b^{x+txy})$。
- Linear: Linear problem。The best known algorithm for Linear is to solve the DLP。
  已知$g^a, g^b, g^{ac}, g^{bd} \in G$，计算$g^{c+d}$。
- D-Linear1: Decision Linear problem (version 1)
  已知$g^a, g^b, g^{ac}, g^{bd}, v \in G$，判断$v = g^{c+d}$是否成立?
- l-SDH: l-Strong Diffie-Hellman problem
  已知$g^a, g^{a^2}, \cdots, g^{a^l} \in G$，找到$w \in F_q$并计算$g^{1/(a+w)}$。
- c-DLSE: Discrete Logarithm with Short Exponents。The best known algorithm for the c-DLSE is to use the baby-step-giant-step or Pollard kangaroo algorithms for solving the DLP in a short interval. 常用于 Gennaro pseudorandom generator。
  Let $G = \mathbb{Z}_p^*$ 其中$p - 1 = 2q$，p, q均为primes，let c为integer。已知 $g^x \mod p$ 且 $0 \leq x \leq 2^c$，求解相应的x值。
- CONF: (conference-key sharing scheme)。常用于Okamoto's conference-key sharing scheme。
  已知$g^a, g^b, g^{ab} \in G$，计算g^b。
- 3PASS: 3-Pass Message Transmission Scheme。常用于Shamir's 3-pass message transmission scheme。
  已知$A, B, C \in G$，找到相应的s使得$A = s^a, B = s^b, C = s^{ab}$成立。
- LUCAS: Lucas Problem。
  已知$p, z \in < V_t(m) >$，找到相应的x，使得$V_x(m) = z$成立。其中$V_t(m)$的定义为：$V_0(m) = 2, V_1(m) = m, V_t(m) = mV_{t-1}(m) - V_{t-2}(m)$。
- XLP: x-Logarithm Problem。
  对于Elliptic curve $E(\mathbb{F}_q)$上的任意一点 $P = (x, y) \in \mathbb{F}_q^2$，将$x(P) = \bar{x}$ 表示为P点$ X坐标的二进制表示。对任意的group element g^a，$x = x(g^a)$，是否能区分g^a和g^x?
- MDHP: Matching Diffie-Hellman Problem。常用于E-Cash。
  Let g be a generator of group G having order q，let $a_0, b_0, a_1, b_1 \in \mathbb{Z}_q$ and $r \in_R \{0, 1\}$。已知$(g^{a_0}, g^{a_0 b_0}, g^{a_1}, g^{a_1 b_1})$和$(g^{b_r}, g^{b_{1-r}})$，找到相应的$r$。
- DDLP: Double Discrete Logarithm Problem。常用于Public verifiable secret sharing。
  Let p, q 为素数且$q = (p - 1)/2$，设置G为group of order p with generator g，$h \in \mathbb{Z}_p^*$为an element of order q。已知$g, h, a = g^{(h^x)}$，求解x。
- rootDLP: Root of Discrete Logarithm Problem。常用于Camenisch and Stadler group signature scheme。
  已知group generator g, positive integer e 和 $a \in G$，计算x使得$a = g^{(x^e)}$成立。
- n-M-DDH: Multiple Decision Diffie-Hellman Problem。常用于 Group key exchange。
  Let $n \geq 2$，$D = (g^{x_1}, \cdots, g$

为随机值；$D_{random} = (g_1, \cdots, g_n, \{g_{ij}\}_{1\leq i<j\leq n})$为a random tuple in G。很难区分D和D_{random}。

- l-HENSEL-DLP: l-Hensel Discrete Logarithm Problem。
Let G为a subgroup or prime order r in $\mathbb{Z}_p^*$，其中p为a prime with polynomial binary length；Let $1 < g < p$ be an integer满足$g^r \equiv 1(\mod p^{l-1}), g^r \not\equiv 1 \mod p^l)$，其中$l > 1$且为整数。已知$g^x \mod p$，$x$为$[1, r-1]$范围内的随机数，计算$g^x \mod p^l$。

- DLP(Inn(G)): Discrete Logarithm Problem over Inner Automorphism Group。
常用于MOR Public Key Cryptosystem。
已知$\phi, \phi^s \in Inn(G)$ for $s \in \mathbb{Z}$，求解$s(\mod |\phi|)$。

- IE: Inverse Exponent。
为l-DHI （l-Diffie-Hellman inversion problem） $l = 1$的特例情况。

- TDH: The Twin Diffie-Hellman Assumption。
Let G 为 a cyclic group with generator g，and of prime order q。定义$dh(X, Y) = Z$，其中$X = g^x, Y = g^y, Z = g^{xy}$。定义twin DH function $2dh: G^3 \rightarrow G^2$ $(X_1, X_2, Y) \rightarrow (dh(X_1, Y), dh(X_2, Y))$。定义相应的twin DH predicate为：$2dhp(X_1, X_2, \hat{Y}, \hat{Z}_1, \hat{Z}_2) = 1\, iff\ 2dh(X_1, X_2, \hat{Y}) = (\hat{Z}_1, \hat{Z}_2)$。
twin DH assumption是指：已知random $X_1, X_2, Y \in G$，计算$2dh(X_1, X_2, Y)$很难。
strong twin DH assumption是指：已知$X_1, X_2, Y \in G$ along with access to a decision oracle for the predicate $2dhp(X_1, X_2, \cdot, \cdot, \cdot)$ which on input $(\hat{Y}, \hat{Z}_1, \hat{Z}_2)$ returns $2dhp(X_1, X_2, \hat{Y}, \hat{Z}_1, \hat{Z}_2)$，计算$2dh(X_1, X_2, Y)$很难。

- XTR-DL: XTR discrete logarithm problem。Most protocols based on DLP can be used with XTR.
Let $Tr(g)$ 为an XTR representation of an element of the XTR subgroup of $\mathbb{F}_{p^6}^*$，已知t，求解x使得$t = Tr(g^x)$成立。

- XTR-DH: XTR Diffie-Hellman problem。Most protocols based on DLP can be used with XTR.
Let $Tr(g)$ 为an XTR representation of an element of the XTR subgroup of $\mathbb{F}_{p^6}^*$，已知t_1, t_2，求解t_3使得$t_1 = Tr(g^x), t_2 = Tr(g^y), t_3 = Tr(g^{xy})$成立。

- XTR-DHD: XTR decision Diffie-Hellman problem.Most protocols based on DLP can be used with XTR.
Let $Tr(g)$ 为an XTR representation of an element of the XTR subgroup of $\mathbb{F}_{p^6}^*$，已知$t_1 = Tr(g^x), t_2 = Tr(g^y), t_3$，判断$t_3 = Tr(g^{xy})$是否成立?

- CL-DLP: discrete logarithms in class groups of imaginary quadratic orders。常用于key exchange。
为standard discrete logarithm problems in a class group of imaginary quadratic orders。

- TV-DDH: Tzeng Variant Decision Diffie-Hellman problem。常用于Conference key agreement.
Let $p, q = 2p+1$均为素数，let $G \subseteq \mathbb{F}_p^*$ 为subgroup of order q。$h \in G$为$[1, p-1]$内的整数，$h \mod q$为$[0, q-1]$内整数。已知$g_1, g_2 \in G$ 且 $0 \leq u_1, u_2 < q$，取任意整数a，判断$u_1 = g_1^a \mod q, u_2 = g_2^a \mod q$是否成立?

- n-DHE: n-Diffie-Hellman Exponent problem。常用于 Broadcast encryption, accumulators.
对于a group G of prime order q，let $g_i = g^{\lambda^i}, \lambda \leftarrow \mathbb{Z}_q$，已知$\{g, g_1, g_2, \cdots, g_n, g_{n+2}, \cdots, g_{2n}\} \in G^{2n}$，计算$g_{n+1}$。

2. Factoring

Factoring problems通常针对的是products of two random primes。如$n = pq, n \in \mathbb{N}$，其中p, q均为素数。
通常基于安全考虑，定义强素数的形式为$p = 2p' + 1$，其中p和p'均为素数。

- FACTORING: integer factorisation problem
  已知正整数$n \in \mathbb{N}$，寻找其素数因式分解 $n = p_1^{e1} p_2^{e2} \cdots p_k^{ek}$，其中$p_i$为pairwise distinct 素数，$e_i > 0$。
- SQRT: square roots modulo a composite
  已知复合正整数$n \in \mathbb{N}$ 和 a square a modulo n，求a modulo n的平方根，即求解integer x 使得 $x^2 \equiv a \ (mod\ n)$。
  常用于Rabin encryption。
- $CHARACTER^d$: character problem
  Let n和d为正整数，已知$x \in \mathbb{Z}_n^*$，设计算法$\chi(x)$，其中χ为a non-trivial character of $\mathbb{Z}_n^*$ of order d。
  常用于Undeniable Signautres。
  可看成是quadratic residuosity problem的generalisation。
- $MOVA^d$: character problem
  Let $n \in \mathbb{Z}, s \in \mathbb{Z}^+$，$\chi$为a character of order d on $\mathbb{Z}_n^*$。已知s个pairs $(\alpha_i, \chi(\alpha_i))$，其中$\alpha_i \in \mathbb{Z}_n^*$ for all $i \in [1, \cdots, s]$，$x \in \mathbb{Z}_n^*$，计算$\chi(x)$。
  常用于Undeniable Signautres。
- $CYCLOFACT^d$: factorisation in Z[θ]
  Let θ 为 d^{th} root of unity，σ 为 an element of $\mathbb{Z}[\theta]$，求σ的因式分解。
- $FERMAT^d$: factorisation in Z[θ]
  Let θ 为 d^{th} root of unity，$n \in \mathbb{Z}$ 使得$n = \pi\bar{\pi}$ for some $\pi \in \mathbb{Z}[\theta]$。已知$n$，求$\pi$。
- RSAP: RSA problem
  已知正整数n为至少2个素数的乘积，已知整数e (coprime with $\varphi(n)$) 和整数c，求整数m使得$m^e \equiv c \ (mod\ n)$成立。
- Strong-RSAP: strong RSA problem
  已知正整数n为至少2个素数的乘积，已知整数c，求奇数$e \geq 3$和整数m，使得$m^e \equiv c \ (mod\ n)$成立。
- Difference-RSAP: Difference RSA problem
  已知正整数n为至少2个素数的乘积，已知an element $D \in \mathbb{Z}_n^*$ 和 $m - 1$ 个pairs (x_i, y_i) 使得 $x_i^e - y_i^e = D \ (mod\ n)$，求解新的pair $x_m^e - y_m^e = D \ (mod\ n)$ 成立。
- Partial-DL-ZN2P: Partial Discrete Logarithm problem in $\mathbb{Z}_{n^2}^*$
  已知正整数$n = pq$，其中$p = 2p' + 1, q = 2q' + 1$，p, p', q, q'均为素数，已知an element $g \in \mathbb{Z}_{n^2}^*$ of maximal order in $G = QR_{n^2}$ 和 $h = g^a \ mod\ n^2$ for some $a \in \{1, \cdots, ord(G)\}$，求解整数$x$使得$x = a \ (mod\ n)$。
  常用于homomorphic public key encryption, public key encryption with double trapdoor decryption mechanism。
- DDH-ZN2P: Decision Diffie-Hellman problem over $\mathbb{Z}_{n^2}^*$
  已知正整数$n = pq$，其中$p = 2p' + 1, q = 2q' + 1$，p, p', q, q'均为素数，已知an element $g \in \mathbb{Z}_{n^2}^*$ of maximal order in $G = QR_{n^2}$ 和 elements $X = g^x \ mod\ n^2, Y = g^y \ mod\ n^2$ for some $x, y \in \{1, \cdots, ord(G)\}$ 以及 $Z \in G$，判断$Z = g^{xy} \ mod\ n^2$是否成立。
  常用于public key encryption with double trapdoor decryption mechanism。
- Lift-DH-ZN2P: Lift Diffie-Hellman problem over $\mathbb{Z}_{n^2}^*$
  已知正整数$n = pq$，其中$p = 2p' + 1, q = 2q' + 1$，p, p', q, q'均为素数，已知an element $g \in \mathbb{Z}_{n^2}^*$ of maximal order in $G = QR_{n^2}$ 和 elements $X = g^x \ mod\ n^2, Y = g^y \ mod\ n^2$ for some $x, y \in \{1, \cdots, ord(G)\}$ 以及 $Z = g^{xy} \ mod\ n$，求$Z' = g^{xy}$
  常用于public key encryption wit

- EPHP: Election Privacy Homomorphism problem
  已知固定的小素数e、素数p 使得 $e|(p-1)$、素数q使得$e \nmid (q-1)$，有$n = pq$、$g \in \mathbb{Z}_n$ 且e divides the order of g。由g作为generator生成的group表示为G。
  EPHP是指：已知$w \in G$、$v \in [0, e]$，是否存在$r \in N$，使得$w = g^{v+er}$成立。存在的概率应高于$(e-1)/e$。
  常用于homomorphic public key encryption 和 electronic voting protocols。

- AERP: Approximate e-th root problem
  已知正整数$n = p^2 q$，其中p, q为素数且$|n| = 3k$，已知整数$e \geq 4$、$y \in \mathbb{Z}_n$，求整数x，使得$(x^e \ mod \ n) \in I_k(y)$成立，其中$I_k(y) = \{u | y \leq u < y + 2^{2k-1}\}$。
  常用于ESIGN signature scheme。

- l-HENSEL-RSAP: l-Hensel RSA
  已知$N = pq$，e coprime with $\phi(N)$，$x^e \ (mod \ N)$ for a random integer $1 < x < N$，求$x^e \ (mod \ N^l)$。
  常用于public-key encryption。

- DSeRP: Decisional Small e-Residues in $\mathbb{Z}_{n^2}^*$
  已知正整数$n = pq$，其中p, q为素数，已知整数 $e > 2$ 使得 $gcd(e, n(p-1)(q-1)) = 1$，是否能区分 $D_0 = \{c = r^e \ mod \ n^2 | r \in_R \mathbb{Z}_n\}$ distribution 和 $D_1 = \{c \in_R \mathbb{Z}_{n^2}\}$ distribution。
  常用于Semantically secure public key encryption from Paillier-related assumptions。

- DS2eRP: Decisional Small 2e-Residues in $\mathbb{Z}_{n^2}^*$
  已知正整数$n = pq$，其中p, q为素数，$p = q = 3 \ mod \ 4$，已知整数e 使得 $gcd(e, n(p-1)(q-1)) = 1$且$|n|/2 < 3 < |n|$，是否能区分 $D_0 = \{c = r^{2e} \ mod \ n^2 | r \in_R QR_n\}$ distribution 和 $D_1 = \{c \in_R QR_{n^2}\}$ distribution。
  常用于Semantically secure public key encryption mixing Paillier and Rabin functions。

- DSmallRSAKP: Decisional Reciprocal RSA-Paillier in $\mathbb{Z}_{n^2}^*$
  已知正整数$n = pq$，其中p, q为素数，已知an element α使得 $(\alpha/p) = (\alpha/q) = -1$，已知整数$e$使得$|n|/2 < e < |n|$，是否能区分 $D_0 = \{(n, e, \alpha, c) | c = (r + \frac{\alpha}{r})^e \ mod \ n^2, r \in_R \mathbb{Z}_n \ s.t. \ (r/n) = 1, (\alpha/r \ mod \ n) > r\}$ distribution 和 $D_1 = \{(n, e, \alpha, c) | c = (r + \frac{\alpha}{r})^e \ mod \ n^2, r \in_R \mathbb{Z}_{n^2}\}$ distribution。
  常用于Semantically secure public key encryption from Paillier-related assumptions。

- HRP: Higher Residuosity Problem
  已知n和a为正整数，且$a|\phi(n)$，已知$x \in \mathbb{Z}_n^*$，判断是否存在y，使得$y^a = x$。
  常用于：convertible group signature，public key encrytpion。

- ECSQRT: Square roots in elliptic curve groups over $\mathbb{Z}/n\mathbb{Z}$
  已知$E(\mathbb{Z}/n\mathbb{Z})$ 为 elliptic curve group over $\mathbb{Z}/n\mathbb{Z}$，已知a point $Q \in E(\mathbb{Z}/n\mathbb{Z})$，计算所有points $P \in E(\mathbb{Z}/n\mathbb{Z})$ 使得 $2P = Q$。

- RFP: Root Finding Problem
  计算多项式$f(x)$ over the ring $\mathbb{Z}_n$的所有roots，其中$n = pq$，p, q为2个大素数。

- phiA: PHI-Assumption
  设$PRIMES_a$ 为the set of all primes of length a，H_a为the set of the composite integers that are product of two primes of length a。
  若$p|\phi(m)$，则称composite integer m ϕ-hides a prime p。
  $H^b(m)$表示the set of b-bit primes p that are ϕ-hidden by m; $\bar{H}^b(m)$表示the set $PRIMES_b - H^b(m)$。
  ϕ-Hidding假设：存在e, f, g, h

，$Pr[m \leftarrow H^k; p_0 \leftarrow H^k(m); p_1 \leftarrow \bar{H}^k(m); b \leftarrow 0,1 : C(m, p_b) = b] > 1/2 + 2^{-gk}$。
ϕ-Sampling假设：存在$e, f, g, h > 0$，使得对于$\forall k > h$，存在a sampling algorithm $S()$ 使得for all k-bit primes p，$S(p)$ 输出a random k^f-bit number $m \in H_{k^f}^k$ that ϕ-hides p together with m's integer factorization。

- C-DRSA: Computational Dependent-RSA problem
已知(N, e)和$\alpha \in \mathbb{Z}_n^*$，求$(a+1)^e (\mod n)$ 其中 $\alpha = a^e (\mod n)$。

- D-DRSA: Decisional Dependent-RSA problem
已知(N, e)、$\alpha = a^e (\mod n)$和$\gamma \in \mathbb{Z}_n^*$，是否能区分$\gamma = (a+1)^e (\mod n)$和$\gamma = c^e (\mod n)$，其中 a, c为$\mathbb{Z}_n^*$中的随机数。

- E-DRSA: Extraction Dependent-RSA problem
已知(N, e)、$\alpha = a^e (\mod n)$和$\gamma = (a+1)^e (\mod n)$，求$a(\mod n)$。

- DCR: Decisional Composite Residuosity problem
已知composite n和integer z，判断z是否为n-residue modulo n^2。

- CRC: Composite Residuosity Class problem
$B_\alpha \subset \mathbb{Z}_{n^2}^*$ 表示：the set of elements of order $n\alpha$。
B表示：B_α的disjoint union for $\alpha = 1, \cdots, \lambda$，其中$\lambda = \lambda(n)$为the Carmichael's function taken on n。
已知a composite $n, w \in \mathbb{Z}_{n^2}^*, g \in B$，计算the n-residuosity class of w with respect to $g : [w]_g$。

- DCRC: Decisional Composite Residuosity Class problem
$B_\alpha \subset \mathbb{Z}_{n^2}^*$ 表示：the set of elements of order $n\alpha$。
B表示：B_α的disjoint union for $\alpha = 1, \cdots, \lambda$，其中$\lambda = \lambda(n)$为the Carmichael's function taken on n。
已知a composite $n, w \in \mathbb{Z}_{n^2}^*, g \in B, x \in \mathbb{Z}_n$，判断$x = [w]_g$是否成立。

- GenBBS: generalised Blum-Blum-Shub assumption
已知a composite positive integer $n \in \mathbb{N}$ 和 一系列 $g, g^2 (\mod n), g^4 (\mod n), g^8 (\mod n), \cdots, g^{2^{2^k}} (\mod n)$，是否能区分$g^{2^{2^{k+1}}} (\mod n)$ 和 $r^2 (\mod n)$。

3. Product groups

本节主要关注的是products of two groups of known prime order，常用于pairing based cryptography，但是在本节讨论的是 pairing之外的安全假设。
主要有3种分类：
1）Type 1：$G_1 = G_2$，均为group of prime order q；
2）Type 2：$G_1 \neq G_2$，均为group of prime order q，但是存在efficiently computable homomorphism $\psi : G_2 \rightarrow G_1$；
3）Type3：$G_1 \neq G_2$，均为group of prime order q，且不存在efficiently computable homomorphism $\psi : G_2 \rightarrow G_1$。

以g_i表示a generator of G_i，则对于Type 1有$g_1 = g_2$。
对于$a \in G_i, b \in G_j$，若$\log_{g_i} a = \log_{g_j} b$，则表示为$a \sim b$

- co-CDH: co-Computational Diffie-Hellman Problem
已知g_i^a，求g_{3-i}^a。

- PG-CDH: Computational Diffie-Hellman Problem for Product Groups
已知$g_i, g_i^x, g_i^y, g_{3-i}, g_{3-i}^x, g_{3-i}^y$，求$g_i^{xy}$。

- XDDH: External Decision Diffie-Hellman Problem
已知g_i^a, g_j^b和$v \in G_k$，判断$v = g_k^{ab}$是否成立。

- D-Linear2: Decision Linear Problem (version 2)
已知$g \in G_1, g^a, g^b, g^{ac}, g^{bd}$ 和
否成立。

- PG-DLIN: Decision Linear Problem for Product Groups
  已知$g_{i1},g_{i2},g_{i3}\in G_i,g_{i1}^x,g_{i2}^y$ 和 $g_{j1},g_{j2},g_{j3}\in G_j,g_{k1}^x,g_{k2}^x$，使得$g_{i1}\sim g_{j1},g_{i2}\sim g_{j2},g_{i3}\sim g_{j3}$，判断$v=g_{l1}^{x+y}$是否成立。

- FSDH: Flexible Square Diffie-Hellman Problem
  已知$g_2^a\in G_2$，对于任意选择的$h\in G_1$，求(h,h^a,h^{a^2})。

- KSW1: Assumption 1 of Katz-Sahai-Waters
  对于所有的p.p.t. adversaray A，security parameter 为n的情况下，以下情况成立的概率可忽略：
  运行$G(1^n)$ 获取$(p,q,r,G,G_T,\hat{t})$。
  设置$N=pqr$，并令g_p,g_q,g_r分别为generators of G_p,G_q,G_r。
  选择随机的$Q_1,Q_2,Q_3\in G_q$，随机的$R_1,R_2,R_3\in G_r$，随机的$a,b,s\in\mathbb{Z}_p$以及随机的bit v.
  A 已知 $(N,G,G_T,\hat{t})$ 和 $g_p,g_r,g_qR_1,g_p^b,g_p^{b^2},g_p^ag_q,g_p^{ab}Q_1,g_p^s,g_p^{bs}Q+2R_2$，若$v=0$，则告知$A$ $T=g_p^{b^2s}Q_3R_3$值。
  A输出v'使得$v'=v$的概率可忽略。

4. Pairings

2008年《Pairings for cryptographers》中指出，pairings over groups of known prime order 表示为：

$$\hat{t}:G_1\times G_2\to G_T$$

若其中 G_1,G_2,G_T**都具有相同的prime order** l，则可分为以下三大类：
1）Type 1：$G_1=G_2$；【通常使用supersingular curves，这些supersingular curves又分为两类：一类是over fields of characteristic 2 or 3 (with embedding degree 4 or 6 respectively)；另一类是over fields of large prime characteristic (with embedding degree 2)。】
2）Type 2：$G_1\neq G_2$，但是存在efficiently computable homomorphism $\phi:G_2\to G_1$；【通常使用ordinary curves，且the homomorphism from G_2 to G_1 is the trace map。】
3）Type3：$G_1\neq G_2$，且不存在efficiently computable homomorphism $\phi:G_2\to G_1$。【通常使用ordinary curves，且G_2为the kernel of the trace map。】

若G_2 为non-cyclic group of order l^2，则可称为Type 4。

Table 1
Properties of the types of pairing groups

Type	Hash to G_2	Short G_1	Homomorphism	Poly time generation
1 (small char)	✓	×	✓	×
1 (large char)	✓	×	✓	✓
2	×	✓	✓	✓
3	✓	✓	×	✓

Table 2
Recommend key sizes

Author	κ	ECC-style	RSA-style
NIST [20]	80	160	1024
	128	256	3072
	256	512	15360
Lenstra [13]	80	160	1329
	128	256	4440
	256	512	26268
ECRYPT [21]	80	160	1248
	128	256	3248
	256	512	15424

Table 3
Comparison of efficiency and bandwidth properties

Type	κ	H1(3)	H2(3)	M2	S1	S2(4)	E1	E2(5)	E3(6)	P	F
Type 1	80	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	1	⋆⋆	1	8/7	⋆⋆⋆	⋆
(char 2)	256	⋆	⋆	⋆⋆	⋆⋆⋆	1	⋆	1	8/7	⋆	⋆
Type 1	80	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	1	⋆⋆⋆	1	3	⋆⋆⋆	⋆
(char 3)	256	⋆	⋆	⋆⋆	⋆⋆⋆	1	⋆	1	3	⋆	⋆
Type 1	80	⋆⋆	⋆⋆	⋆	⋆⋆⋆	1	⋆	1	1/4	⋆⋆⋆	⋆⋆⋆
(char p)	256	⋆	⋆	⋆	⋆⋆	1	⋆	1	1/4	⋆	⋆⋆⋆
Type 2	80	⋆⋆⋆		⋆	⋆⋆⋆	k	⋆⋆⋆	k^2	$k^2/16$	⋆/⋆⋆⋆(10)	⋆⋆⋆
	256	⋆⋆/⋆⋆⋆(7)		⋆	⋆/⋆⋆⋆(8)	k	⋆⋆/⋆⋆⋆(9)	k^2	$k^2/16$	⋆/⋆⋆⋆(10)	⋆⋆⋆
Type 3	80	⋆⋆⋆	⋆	⋆⋆⋆	⋆⋆	d	⋆⋆⋆	d^2	$k^2/16$	⋆⋆⋆	⋆⋆⋆
	256	⋆⋆/⋆⋆⋆(7)	⋆⋆	⋆⋆	⋆/⋆⋆⋆(8)	d	⋆⋆/⋆⋆⋆(9)	d^2	$k^2/16$	⋆⋆⋆	⋆⋆⋆

H1: Can one hash to G_1 efficiently?
H2: Can one hash to G_2 efficiently?
M2: Can one test membership in G_2 efficiently? (Note that many protocols implicitly require membership tests for their security guarantees to hold.)
S1: Is there a short representation for elements of G_1? (Meaning, in a system with security level κ, can elements of G_1 be represented with roughly the minimum number, say $\leq 2\kappa + 10$, of bits?)
S2: What is the ratio of the size of the representation of elements of G_2 to the size of the representation of elements of G_1?
E1: Are group operations in G_1 efficient? (Meaning, in a system with security level κ, are operations in G_1 efficient when compared with usual elliptic curve cryptography in a group with security level κ?)
E2: What is the ratio of the complexity of group operations in G_2 to the complexity of group operations in G_1?
E3: What is the ratio of the complexity of group operations in G_T to the complexity of those in G_1?
P: Is the pairing efficient? (Meaning, how does the speed of pairing computation compare with alternative groups of the same security level?)
F: Is there wide flexibility in choosing system parameters? (Meaning, is it necessary for all users to share one curve, or is there plenty of freedom for users to generate their own curves of any desired security level κ?)

具体举例为：

- Type 1：

Type 1: Type 1 curves are supersingular. The group G_1 is always a subgroup of $E(\mathbb{F}_q)$. There is a "distortion map" ψ which maps G_1 into $E(\mathbb{F}_{q^k})$ and the pairing of $P, Q \in G_1$ is obtained by computing $e(P, \psi(Q))$. An example is $y^2 = x^3 + x$ over $\mathbb{F}_p$, where $p \equiv 3 (\mathrm{mod}\ 4)$; in this case $\psi(x, y) = (-x, iy)$, where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$.

For our analysis of the Type 1 case we only consider supersingular elliptic curves with embedding degree $k = 6$ (in characteristic 3), $k = 4$ (in characteristic 2), or $k = 2$ (for large prime characteristic). Hence we do not consider the cases $k = 1$ or $k = 3$ with large prime characteristic (these cases are not very thoroughly studied, but it is clear that from a high-level view their behaviour is broadly comparable to the case $k = 2$). Similarly, we do not consider supersingular hyperelliptic curves, as from a high-level point of view their performance characteristics are similar to the case of supersingular elliptic curves.

Note that testing membership of P in G_1 can be done by checking that P is defined over $\mathbb{F}_q$ and then checking that $[l]P = 0$. For many applications it is sufficient to perform the check that $[h]P \neq 0$ for the cofactor h, which is cheaper if h is small.

- Type 2：

Type 2: Take any pairing friendly curve E over $\mathbb{F}_q$ with embedding degree $k > 1$ and define G_1 to be the subgroup of $E(\mathbb{F}_q)$ of order l. We choose a random point $Q \in E(\mathbb{F}_{q^k})[l]$ and define $G_2 = \langle Q \rangle$. It is necessary that Q be published as a system parameter so that other users know what G_2 is. Define the trace map $\mathrm{Tr} : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q)$ by

$$\mathrm{Tr}(Q) = \sum_{i=0}^{k-1} \pi^k(Q),$$

where π is the q-power Frobenius map. With overwhelming probability, $\mathrm{Tr}(Q) \neq 0$ and so $\phi = \mathrm{Tr}$ is a non-trivial group homomorphism from G_2 to G_1. In general it seems to be a hard computational problem to compute a non-trivial group homomorphism from G_1 to G_2.

The advantage of the Type 2 setting is that we can use any curve and still get a homomorphism from G_2 to G_1. The disadvantage is that the group G_2 has no special structure. It seems to be impossible to sample randomly from G_2 except by computing multiples of the generator Q, hence we cannot securely hash to G_2. To test if $R \in G_2$ we follow the method of [9]: first check that $[l]R = 0$ (note that for high security levels the cofactor h for G_2 in $E(\mathbb{F}_{q^k})$ is typically larger than l, so it is not faster to compute $[h]R$; though instead one could compute $[h]\mathrm{Tr}(R)$ and $[h](kR - \mathrm{Tr}(R))$) and then test whether

$$e(kQ - \mathrm{Tr}(Q), \mathrm{Tr}(R)) = e(kR - \mathrm{Tr}(R), \mathrm{Tr}(Q)).$$

Hence, membership testing requires some form of point multiplication plus two pairing computations, and so could be a serious overhead.

- Type 3：

Type 3: Take any pairing friendly curve E over $\mathbb{F}_q$ of embedding degree $k > 1$. Define G_1 to be the subgroup of $E(\mathbb{F}_q)$ of order l. An equivalent way to say this is that G_1 is the kernel of $(\pi - 1)$ on $E[l]$, where π is the q-power Frobenius. Define G_2 to be the kernel of $(\pi - q)$ on $E[l]$.

The difference between the Type 3 and Type 2 cases is striking: in the Type 3 case G_2 is precisely the kernel of the trace map, so the trace map is trivial on G_2. In general there seems to be no efficiently computable homomorphism from G_2 to G_1. On the other hand, one can sample from G_2 by taking a random point $R \in E[l]$ and computing $\pi(R) - R \in G_2$; hence we can hash to G_2. Also, one can test membership of G_2 efficiently by checking that the point has order l (in this case, one can check the order using a twist of the curve, and so sometimes a cofactor test is efficient) and that the trace is zero (which is fast). Further, the Type 3 case allows very efficient pairing implementation due to the ate pairing.

We comment that for Types 2 and 3 we consider ordinary curves which will be generated using the CM method. There are many papers in the literature on this topic, and a wide choice of curves is available (see [10]). The main focus of research has been trying to get $l \approx q$ so that one can represent elements of G_1 in an optimal way. This has not been achieved for all values of k and more research on this topic is welcome. But we feel that a sufficiently flexible array of curves is available nowadays so that implementors could get an acceptable size of elements of G_1 for any large security level. A point however which is overlooked is that for large security levels and certain choices of (k, q) it is not always the case that $l \approx q$ is optimal in terms of efficiency.

Among the various methods for generating ordinary curves, some simply require evaluating one or more polynomials at integer values until primes are found, while others require the solution of Pell equations or finding large prime factors of $l^k - 1$. Any method for generating system parameters which involves solving Pell equations has dubious theoretical merits, since only finitely many solutions will be expected [14]. Similarly, any method that requires factoring will not be polynomial time. Hence, to ensure flexibility in the choice of parameters we assume that curves are generated using methods which only require that certain polynomials represent primes.

若$\log_{g1} a = \log_{g2} b$，则表示为$a \sim b$。
Pairing 相关假设有：【注意，有的assumption并不适于所有的pairing type。Certain assumptions are provably false w.r.t. certain group types.】

- BDHP: Bilinear Diffie-Hellman Problem。
  已知g_i^a, g_j^b和g_k^c，计算$\hat{t}(g_1, g_2)^{abc}$。
  其中$i, j, k \in \{1, 2\}$，对应有四种可能的组合$(i, j, k) \in \{(1,1,1), (1,1,2), (1,2,2), (2,2,2)\}$，也可称为$BDHP_{i,j,k}$。
  – 对于Type 1 pairing，以上四种组合是等价的。
  – 对于Type 2 pairing，具有$BDHP_{2,2,2} \leq_P BDHP_{1,2,2} \leq_P BDHP_{1,1,2} \leq_P BDHP_{1,1,1}$。
  – 对于Type 3 pairing，这四种组合have no known reductions between them。

- DBDH: Decision Bilinear Diffie-Hellman Problem。常用于 Boneh-Franklin ID-based encryption scheme。
  已知g_i^a, g_j^b, g_k^c和$\hat{t}(g_1, g_2)^z$，判断$\hat{t}(g_1, g_2)^{abc} = \hat{t}(g_1, g_2)^z$是否成立。

- B-DLIN: Bilinear Decision-Linear Problem

  Definition: Given $g_{i1}, g_{i2}, g_{i3} \in G_i, g_{i1}^x, g_{i2}^y$ and $g_{3-i,1}, g_{3-i,2}, g_{3-i,3} \in G_{3-i}$ such that $g_{i1} \sim g_{3-i,1}, g_{i2} \sim g_{3-i,2}, g_{i3} \sim g_{3-i,3}$ and g_{j1}^x, g_{j2}^x to decide if $v = \hat{t}(g_{11}, g_{21})^{x+y}$. v?

- l-BDHI: l-Bilinear Diffie-Hellman Inversion Problem
  已知$g_i^a, g_i^{a^2}, g_i^{a^3}, \cdots, g_i^{a^l}$，计算$\hat{t}(g_1, g_2)^{1/a}$。其中$i \in \{1, 2\}$。

- l-DBDHI: l-Bilinear Decision Diffie-Hellman Inversion Problem
  已知$g_i^a, g_i^{a^2}, g_i^{a^3}, \cdots, g_i^{a^l}$和$v \in G_T$，判断$v = \hat{t}(g_1, g_2)^{1/a}$是否成立？其中$i \in \{1, 2\}$。

- l-wBDHI: l-weak Bilinear Diffie-Hellman Inversion Problem。
  已知$g_i^a, g_i^{a^2}, g_i^{a^3}, \cdots, g_i^{a^l}$和$g_j^b$，计算$\hat{t}(g_1, g_2)^{a^{l+1}b}$。其中$i \in \{1, 2\}$。

- l-wDBDHI: l-weak Decisional Bilinear Diffie-Hellman Inversion Problem
  已知$g_i^a, g_i^{a^2}, g_i^{a^3}, \cdots, g_i^{a^l}, g_j^b$和$v \in G_T$，判断$v = \hat{t}(g_1, g_2)^{a^{l+1}b}$是否成立？其中$i \in \{1, 2\}$。

- KSW2: Assumption 2 of Katz-Sahai-Waters。首次用于 the construction of a predicate encryption scheme supporting the inner product。（KATZ等人2008年论文《Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products》）
  – 运行$G(1^n)$来获取$(p, q, r, G, G_T, \hat{t})$；
  – 设置$N = pqr$，let g_p, g_q, g_r分别为G_p, G_q, G_r的generators；
  – 选择随机数$h \in G_p; Q_1, Q_2 \in G_q; s, \gamma \in \mathbb{Z}_q$以及random bit v；
  – p.p.t. adversary A 的输入有(
  $g_p, g_q, g_r, h, g_p^s, h^s Q_1, g_p^\gamma Q_2,$

$\hat{t}(g_p, h)^{\gamma s}$；当$v=1$时，给$A$的输入为a random element of G_T。A的输出为a bit v'，且其succeed if $v'=v$。

- MSEDH: Multi-sequence of Exponents Diffie-Hellman Assumption。用于Delerabl´ee and Pointcheval dynamic threshold public-key encryption scheme。
  – Let $B=(p,G_1,G_2,G_T,\hat{t}(\cdot,\cdot))$为a bilinear map group system，let l,m,t为3个整数，let g_0为G_1的generator，h_0为G_2的generator。
  – 输入为2个random coprime polynomials f和g，分别具有degree l和m，分别具有pairwise distinct roots $x_1,\cdots,x_l$和$y_1,\cdots,y_m$。同时有$T\in G_T$以及如下的exponentiations 序列：

$$
\begin{array}{cc}
x_1,\ldots,x_\ell, & y_1,\ldots,y_m, \\
g_0, g_0^{\gamma},\ldots,g_0^{\gamma^{\ell+t-2}}, & g_0^{k\cdot\gamma\cdot f(\gamma)}, \\
g_0^{\alpha}, g_0^{\alpha\cdot\gamma},\ldots,g_0^{\alpha\cdot\gamma^{\ell+t}}, & \\
h_0, h_0^{\gamma},\ldots,h_0^{\gamma^{m-2}}, & \\
h_0^{\alpha}, h_0^{\alpha\cdot\gamma},\ldots,h_0^{\alpha\gamma^{2m-1}}, & h_0^{k\cdot g(\gamma)},
\end{array}
$$

  判断T是否与$\hat{t}(g_0,h_0)^{k\cdot f(\gamma)}$相等或者与$G_T$中的某随机元素相同?

- SXDH assumption: the SXDH assumption states that there are prime-order groups (G_1,G_2,G_T) that admits a bilinear map $e: G_1\times G_2\rightarrow G_T$ such that the Decisional Diffie-Hellman (DDH) assumption holds in both G_1 and G_2 . 首次在2005年论文《Correlation-Resistant Storage via Keyword-Searchable Encryption》中提出：

  Assumption 1 *(Symmetric External Diffie-Hellman assumption, or SXDH): Both $\mathbb{G}_1$ and $\mathbb{G}_2$ are DDH-hard groups, i.e., given (P_0,P_1,P_2,P_3) in $\mathbb{G}_1^4$ it is infeasible to decide if there is a value x such that $P_1=xP_0$ and $P_3=xP_2$ simultaneously. The same requirement must hold for $\mathbb{G}_2$.*

  Variants of DDH and CDH. The *decisional Diffie-Hellman (DDH) problem* in a group $\mathbb{G}$ is, given (G,G^a,G^b,G^c), to decide whether $c=ab$. The *symmetric external Diffie-Hellman (SXDH) assumption* in a bilinear group states that DDH is hard in both groups.

  Assumption 1 (SXDH). *For $\Lambda=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,G,H)\leftarrow\mathcal{G}(1^\lambda)$, the decisional Diffie-Hellman assumption holds in both $\mathbb{G}_1$ and $\mathbb{G}_2$.*

  而在 2019年论文《Proofs for Inner Pairing Products and Applications》中指出，SXDH assumption仅在Type 3 pairings 下成立，因此任何基于SXDH assumption的设计均对应应采用Type 3 pairing。

- DBP: double pairing assumption。在2016年论文《Structure-Preserving Signatures and Commitments to Group Elements》中提出。

均针对Type 3 pairing

Variants of DDH and CDH. The *decisional Diffie-Hellman (DDH) problem* in a group $\mathbb{G}$ is, given (G, G^a, G^b, G^c), to decide whether $c = ab$. The *symmetric external Diffie-Hellman (SXDH) assumption* in a bilinear group states that DDH is hard in both groups.

Assumption 1 (SXDH). *For $\Lambda = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, H) \leftarrow \mathcal{G}(1^\lambda)$, the decisional Diffie-Hellman assumption holds in both $\mathbb{G}_1$ and $\mathbb{G}_2$.*

The *2-out-of-3 CDH* assumption [KP06] states that given (G, G^a, H), it is hard to output (G^r, H^{ar}) for an arbitrary $r \neq 0$. To break the *Flexible CDH* assumption [LV08, CLY09], an adversary must additionally compute G^{ar}. We further weaken the assumption by defining a solution as $(G^r, G^{ar}, H^r, H^{ar})$, and generalize it to asymmetric groups by letting $G \in \mathbb{G}_1$ and $H \in \mathbb{G}_2$. The *asymmetric weak flexible CDH* is defined as follows:

Assumption 2 (AWF-CDH). *Let $G \in \mathbb{G}_1$, $H \in \mathbb{G}_2$ and $a \in \mathbb{Z}_p$ be random. Given $(G, A = G^a, H)$, it is hard to output $(G^r, G^{ar}, H^r, H^{ar})$ with $r \neq 0$, i.e., a tuple (R, M, S, N) that satisfies*

$$e(A, S) = e(M, H) \qquad e(M, H) = e(G, N) \qquad e(R, H) = e(G, S) \qquad (1)$$

Given a DDH instance (G, G^a, G^b, G^c), solving AWF-CDH for (G, G^a, H) yields $(G^r, G^{ar}, H^r, H^{ar})$; thus $G^c = G^{ab}$ can be checked by $e(G^{ab}, H^r) = e(G^b, H^{ar})$. We have thus

Lemma 1. *The AWF-CDH assumption holds if the decisional Diffie-Hellman assumption is hard in $\mathbb{G}_1$.*

The Double Pairing Assumption. The double pairing problem is given random $G_R, G_T \in \mathbb{G}_1$ to find non-trivial $R, S \in \mathbb{G}_2$ satisfying $e(G_R, R)e(G_T, T) = 1$.

Assumption 3 (DBP). *For all nonuniform polynomial-time adversaries $\mathcal{A}$*

$$\Pr\Big[\Lambda \leftarrow \mathcal{G}(1^\lambda);\ G_R, G_T \leftarrow \mathbb{G}_1;\ (R, T) \leftarrow \mathcal{A}(\Lambda, G_R, G_T) : \\ (R, T) \in \mathbb{G}_2^* \times \mathbb{G}_2^* \quad \wedge \quad e(G_R, R)e(G_T, T) = 1\Big] = \mathrm{negl}(\lambda).$$

We show in the full papers the following lemma:

Lemma 2. *The double pairing assumption holds if the decisional Diffie-Hellman assumption is hard in $\mathbb{G}_1$.*

5. Lattices

基础可参看博客 如何保护今日加密数据以抵抗量子攻击？ 。
A lattice Λ of dimension n 为 a discrete subgroup of $\mathbb{R}^d$，其中$d \geq n$。
密码学中的实际应用，通常使用的为lattices in $\mathbb{Z}^d$。
A lattice is specified by a $d \times n$ basis matrix B, consisting of n linearly indepedent basis vectors $\vec{b}_i \in \mathbb{R}^d$。
以$\Lambda(B)$来表示the lattice spanned by the basis B。

5.1 Main Lattice Problems

- SVP$_\gamma^p$: (Approximate) Shortest vector problem
  已知a basis $B \in \mathbb{Z}^{m\times n}$ 和 $\gamma > 0$，求 a nonzero lattice vector $v \in B\mathbb{Z}^n \setminus \{0\}$，使得$\| v \|_p \leq \gamma\lambda_1^p(B)$。
- CVP$_\gamma^p$: (Approximate) Closest vector problem
  已知a basis $B \in \mathbb{Z}^{m\times n}$ 、$\gamma > 0$ 和 $t \in B\mathbb{R}^n$，求 a nonzero lattice vector $v \in B\mathbb{Z}^n$，使得$\| t - v \|_p \leq \gamma\lambda_1^p(B)$。
- GapSVP$_\gamma^p$: Decisional shortest vector problem
  已知a basis $B \in \mathbb{Z}^{m\times n}$ 、$d, \gamma > 0$ 和 lattice vector $v \in B\mathbb{Z}^n \setminus \{0\}$，是否能区分 $min\{\| v \|_p : v \in B\mathbb{Z}^n \setminus \{0\}\} \leq d$ 和 $min\{\| v \|_p : v \in B\mathbb{Z}^n \setminus \{0\}\} > \gamma d$。
- GapCVP$_\gamma^p$: Decisional closest vector problem
  已知a basis $B \in \mathbb{Z}^{m\times n}$ 、$d, \gamma > 0$ 和 lattice vector $t \in B\mathbb{R}^n$，是否能区分 $min\{\| t - v \|_p : v \in B\mathbb{Z}^n\}$

5.2 Modular Lattice Problems

Modular lattice problems are typically defined as average-case problems.

- SIS$^p(n, m, q, \beta)$: Short integer solution problem
  设q为prime，$A \in \mathbb{Z}_q^{n\times m}$，其中$A$为chosen from a distribution negligibly close to uniform over $\mathbb{Z}_q^{n\times m}$，则$\Lambda_q^{\perp}(A) = \{\vec{x} \in \mathbb{Z}^m : A\vec{x} \equiv \vec{0}(\mod q)\}$ 为a m-dimensional lattice。
  求 a vector $\vec{v} \in \Lambda_q^{\perp}(A)$ 使得 $\| \vec{v} \| \leq \beta$。
- ISIS$^p(n, m, q, \beta)$: Inhomogeneous short integer solution problem
  设q为prime，$A \in \mathbb{Z}_q^{n\times m}$，$\vec{y} \in \mathbb{Z}^n$，其中$A$和$\vec{y}$为chosen from a distribution negligibly close to uniform over $\mathbb{Z}_q^{n\times m}$ 和 $\mathbb{Z}_q^n$。
  求 a vector $\vec{v} \in \{\vec{x} \in \mathbb{Z}^m : A\vec{x} \equiv \vec{y}(\mod q)\}$ 使得 $\| \vec{v} \| \leq \beta$。
- LWE(n, q, ϕ): Learning with errors problem
  $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ 表示 the additive group on the reals modulo one。
  $A_{s,\phi}$ 表示 the distribution on $\mathbb{Z}_q^n \times \mathbb{T}$ obtained by choosing a vector $\vec{a} \in \mathbb{Z}_q^n$ uniformly at random，choosing e according to a probability distribution ϕ on $\mathbb{T}$，输出 $(\vec{a}, <\vec{a}, s>/q + e)$ for some fixed vector $\vec{s} \in \mathbb{Z}_q^n$。
  The search verion of the learning with errors problem "LWE(n, q, ϕ)" 为：
  求the secret $s \in \mathbb{Z}_q^n$，given access to polynomially many samples of choice from $A_{s,\phi}$。
  The decision version为：是否能区分the probability distribution $A_{s,\phi}$ from the unifrom random distribution。

5.3 Miscellaneous Lattice Problems

- USVP$^p(n, \gamma)$: Approximate unique shortest vector problem
  设Λ为an n-dimensional lattice，求 $\vec{v} \in \Lambda \setminus \{\vec{0}\}$，使得$\| \vec{p} \| \leq \gamma\lambda_1^{(p)}(\Lambda)$，其中$\lambda_1^{(p)}(\Lambda)$为the first successive minimum of Λ in the p-norm and the shortest lattice vector $\vec{i}$ is γ-unique。
  换句话说，for all $\vec{w} \in \Lambda$ with $\lambda_1^{(p)} \leq \| \vec{w} \| \leq \gamma\lambda_1^{(p)}(\Lambda)$，有$\vec{w} = z\vec{u}$ for some $z \in \mathbb{Z}$。
- SBP$^p(n, \gamma)$: Approximate shortest basis problem
  设$\Lambda \subseteq \mathbb{R}^d$为$n$-dimensional lattice，求a basis B of Λ 使得 for all $B' \in \{B \in \mathbb{Q}^{d\times n} : \Lambda = \Lambda(B)\}$ $max_{i=1}^n\{\| \vec{b}_i \|\} \leq \gamma max_{i=1}^n\{\| \vec{b}'_i \|_p\}$
- SLP$^p(n, \gamma)$: Approximate shortest length problem
  设$\Lambda \subseteq \mathbb{R}^d$为$n$-dimensional lattice，求the approximate length (w.r.t the p-norm) $\lambda^{(p)}$ of the shortest vector $\vec{v} \in \Lambda \setminus \{\vec{0}\}$ 使得 $\lambda_1^{(p)}(\Lambda) \leq \lambda^{(p)} \leq \gamma\lambda_1^{(p)}(\Lambda)$，其中$\lambda_1^{(p)}$ 表示 the first successive minimum of Λi n the p-norm。
- SIVP$^p(n, \gamma)$: Approximate shortest independent vector problem
  设$\Lambda \subseteq \mathbb{R}^d$为$n$-dimensional lattice，求 linearly indepedent vectors $\vec{v}_1, \cdots, \vec{v}_n \in \Lambda$ with $max_{i=1}^n \| \vec{v}_i \| \leq \gamma\lambda_n^{(p)}(\Lambda)$，其中$\lambda_n^{(p)}(\Lambda)$ 为the n-th successive minimum of Λi n the p-norm。
- hermiteSVP: Hermite shortest vector problem
  已知a basis matrix $B \in \mathbb{Z}^{m\times n}(m \geq n)$ 和 $\gamma \geq 1$，求a nonzero vector v of norm $\| v \| \leq \gamma det(L(B))^{1/n}$。
- CRP: Covering radius problem
  已知an approximation factor $\gamma \geq 1$，the input to CRP is a pair (B, r)，其中B为a basis matrix $B \in \mathbb{Z}^{m\times n}$ 以及 $r \in \mathbb{R}$。是否能区分 $\rho(L(B)) \leq r$ 和 $\rho(L(B)) > \gamma \cdot r$。

5.4 Ideal Lattice Problems

设$R=\mathbb{Z}[x]/\langle f\rangle$为the ring of integer polynomials modulo some monic polynomial f of degree n。
由于R为isomorphic to $\mathbb{Z}^n$ as an additive group，且 ideals in R 为 by definition subgroups，两者都对应为lattices。这种形式的latttice称为 “ideal lattices” with respect to f。

- Ideal-SVP$_\gamma^{f,p}$: (Approximate) Ideal shortest vector problem / Shortest polynomial problem
  已知an ideal I in $\mathbb{Z}[x]/<f>$，求a polynomial $g\in I\setminus\{0\}$，使得$\| g \mod f \|_p\leq \gamma\lambda_1^p(I)$。
- Ideal-SIS$_{q,m,\beta}^{f,p}$: Ideal small integer solution problem
  已知n和$g_1,\cdots,g_m$ chosen uniformly at random from $\mathbb{Z}_q[x]/<f>$，求$e_1,\cdots,e_m$ in $\mathbb{Z}[x]$，使得$\sum_{i\leq m}e_ig_i=0(\mod q)$且$\| e \|_p\leq\beta$，其中$e$ is obtained by concatenating the coefficients of all e_i's。

6. Miscellaneous Problems

- KEA1: Knowledge of Exponent assumption。参见2004年论文《The Knowledge-of-Exponent Assumptions and 3-Round Zero-Knowledge Protocols》：
  背景知识为：Let q be a prime such that $2q+1$ is also prime, and let g be a generator of the order q subgroup of Z_{2q+1}^*。假设输入有q,g,g^a，想要输出a pair $(C,Y),Y=C^a$。可实现的方式之一是pick some $c\in\mathbb{Z}_q$，设置$C=g^c$，则有$Y=(g^a)^c=C^a$成立。直观上来说，KEA1假设是指这是唯一的方式。对于任意的adversary能输出such a pair的，其肯定知道相应的c值使得$g^c=C$。在以下的正式定义中引入了extractor可返回相应的c值：
  KEA1 (Knowledge of Exponent assumption) 的定义为： For any adversary A that takes input q,g,g^a，返回(C,Y)其中$Y=C^a$，即意味着存在an extractor $\bar{A}$，对于与adversary相同的输入，可返回c值，使得$g^c=C$。
- MQ: Multivariable Quadratic equations。多变量二次方程式。
  已知a system of m quadratic polynomial equations in n variables each, $\{y_1=p_1(x_1,\cdots,x_n),\cdots,y_m=p_m(x_1,\cdots,x_n)\}$，求解$x\in\mathbb{F}^n$ 为 in general an NP-problem。
- CF: Given-weight codeword finding。常用于: McEliece public key cryptosystem (finding the shortest codeword).
  已知$n\times k$ binary linear code C和相应的$n\times(n-k)$ parity check matrix H，求解vector $\vec{x}$使得$\vec{x}H=0$成立且 x has weight w。
- ConjSP: Braid group conjugacy search problem。
  已知$x,y\in B_n$，求解$a\in B_n$使得$a^{-1}xa=y$成立。
- GenConjSP: Generalised braid group conjugacy search problem。用于 Public-key cryptosystem due to Ko, Lee, Cheon, Han, Kang and Park。
  已知$x,y\in B_n$，求解$a\in B_m,m\leq n$使得$a^{-1}xa=y$成立。
- ConjDecomP: Braid group conjugacy decomposition problem。
  已知$x,y\in B_n$，$y=bxb^{-1}$ for some $b\in B_n$，求解$a',a''\in B_m,m<n$使得$a'xa''=y$成立。
- ConjDP: Braid group conjugacy decision problem。
  已知$x,y\in B_n$，判断x和y是否conjugate? 即是否存在$a\in B_n$使得$a^{-1}xa=y$成立?
- DHCP: Braid group decisional Diffie-Hellman-type conjugacy problem。常用于 Public-key cryptosystem, pseudorandom number generator, pseudorandom synthesizer。
  已知$a,w_l^{-1}aw_l,w_u^{-1}aw_u$，判断$x_u^{-1}x_l^{-1}ax_lx_u=w_u^{-1}w_l^{-1}aw_lw_u$是否成立? for $a\in B_n,x_l,w_l\in B_l$ a

- ConjSearch: (multiple simlutaneous) Braid group conjugacy search problem。
  Let B be a braid group, $\bar{g} = (g_1, \cdots, g_k)$ and $\bar{h} = (h_1, \cdots, h_k)$ be two tuples of elements of B。查找$x \in B$使得$\bar{h} = x^{-1}\bar{g}x$成立。

- SubConjSearch: subgroup restricted Braid group conjugacy search problem。
  常用于Anshel- Anshel- Goldfeld key exchange protocol (AAG)。
  Let B be a braid group, and A a subgroup of B generated by some $\{a_1, \cdots, a_r\}$ and let $\bar{g} = (g_1, \cdots, g_k)$ and $\bar{h} = (h_1, \cdots, h_k)$ be two tuples of elements of B。查找$x \in A$, as a word in $\{a_1, \cdots, a_r\}$，使得$\bar{h} = x^{-1}\bar{g}x$成立。

- LINPOLY : A linear algebra problem on polynomials。
  Let W be a linear space of dimension $\leq n$ consisting of quadratic forms in n variables $X_1, \cdots, X_n$。已知$V = \sum_{1\leq i\leq n} X_i W$，is it possible (and how) to uniquely determine W? For any subspace L' of the linear space L generated by $X_1, \cdots, X_n$。Let $(V : L') \leftarrow r \in K[X_1, \cdots, X_n] : rL' \subseteq V$ where K is a finite field。
  猜想：For randomly chosen W, the probability ρ that $(V : L) = W$ are very close to 1, when $n > 2$。

- HFE-DP: Hidden Field Equations Decomposition Problem。 It is the basis of the HFE crypto system.
  Let F be a finite field of order q and $S, T \in Aff^{-1}$ be two invertible, affine transformations over the vector space F^n。Denote $E := GF(q^n)$ an extension field over F and $\phi : F^n \rightarrow E$ the bijection between this extension field and the corresponding vector space. We have $\phi^{-1}(\phi(a)) = a, \forall a \in F^n$。
  Now let $P(X) := \sum_{i,j<D, q^i+q^j<D} C_{i,j} X^{q^i+q^j} + \sum_{q^i<D} B_i X^{q^i} + A$ for finite field elements $C_{i,j}, B_i, A \in E$ the inner polynomial. This gives the public key:
  $\mathcal{P}(x) := T \circ P \circ S(x)$
  or more precisely:
  $\mathcal{P}(x) := T \circ \phi^{-1} \circ P \circ \phi \circ S(x)$
  HFE Decomposition problem是指：已知公钥$\mathcal{P}$，找到对应的私钥(S, P, T)。

- HFE-SP: Hidden Field Equations Solving Problem。
  Let F be a finite field of order q and $S, T \in Aff^{-1}$ be two invertible, affine transformations over the vector space F^n。Denote $E := GF(q^n)$ an extension field over F and $\phi : F^n \rightarrow E$ the bijection between this extension field and the corresponding vector space. We have $\phi^{-1}(\phi(a)) = a, \forall a \in F^n$。
  Now let $P(X) := \sum_{i,j<D, q^i+q^j<D} C_{i,j} X^{q^i+q^j} + \sum_{q^i<D} B_i X^{q^i} + A$ for finite field elements $C_{i,j}, B_i, A \in E$ the inner polynomial. This gives the public key:
  $\mathcal{P}(x) := T \circ P \circ S(x)$
  or more precisely:
  $\mathcal{P}(x) := T \circ \phi^{-1} \circ P \circ \phi \circ S(x)$
  Hidden Field Equations Solving Problem是指：已知$y \in F^n$，找到$x \in F^n$使得$y = \mathcal{P}(x)$成立。

- MKS: Multiplicative Knapsack。Naccache and Stern 用于构建 trapdoor one-way permutation。
  已知正整数p, c, n以及a set $\{v_i\} \in \{1, \cdots, p-1\}^n$，找到a binary vector x使得$c = \prod_{i=1}^n v_i^{x_i}$成立。

- BP: Balance Problem。常用于Incremental hashing。
  已知a group G和 a set $\{v_i\} \in G^n$，找到disjoint subsets I, J, not both empty，使得$\bigodot_{i\in I} v_i = \bigodot_{j\in J} v_j$成立。

- AHA: Adaptive Hardness Assumptions.
  We consider adaptive strengthenings of standard general hardness assumptions, such as the existe
  generators.

– A collection of adaptive $1-1$ one-way functions is a family of $1-1$ functions $F_n=\{f_s:\{0,1\}^n\to\{0,1\}^n\}$ such that for every s, it is hard to invert $f_s(r)$ for a random r, even for an adversary that is granted access to an "inversion oracle" for $f_{s'}$ for ever $s'\neq s$. In other words, the function f_s is one-way, even with access to an oracle that invert all the functions in the family。
– A sf collection of adaptive pseudo-random generators is a family of $1-1$ functions $G_n=\{G_s:\{0,1\}^n\to\{0,1\}^n\}$ such that for every s, it is hard to invert G_s is pseudo-random, even for an adversary that is granted access to an oracle whether given y is in the range of $G_{s'}$ for $s'\neq s$.

- SPI: Sparse Polynomial Interpolation。常用于Identification scheme。参见2000年论文《AN IDENTIFICATION SCHEME BASED ON SPARSE POLYNOMIALS》
已知$A,a_0,\cdots,a_k,C_1,\cdots,C_k\in\mathbb{F}_q$，找到 a polynomial $f(x)\in\mathbb{F}[x]$ of degree at most $q-1$ 使得 $f(0)=A,f(a_0)=0,f(a_i)=C_i$ for $1\leq i\leq k$ and $f(x)-A$ has coefficients in $\{0,1\}$。

- SPP: Self-Power Problem。若该问题可破解，在可伪造ElGamal signature scheme中类型2和4的签名。
已知prime p和$c\equiv x^x \mod p$，求解x。

- VDP: Vector Decomposition Problem。常用于AN IDENTIFICATION SCHEME BASED ON SPARSE POLYNOMIALS，AN IDENTIFICATION SCHEME BASED ON SPARSE POLYNOMIALS。
已知a two-dimensional vector space V over a finite field, with basis e_1,e_2，和 a vector v in V。找到 a multiple u of e_1 使得 $v-u$ is a multiple of e_2。

- 2-DL: 2-generalized Discrete Logarithm Problem。
已知a group G of exponent r and order r^2, with generators P_1,P_2, and an element Q in G。找到 a pair of integers (a,b) 使得$Q=aP_1+bP_2$成立。

参考资料

[1] Can you give me a summary of cryptographic hardness assumptions?
[2] 2013年报告《Final Report on Main Computational Assumptions in Cryptography》
[3] European Network of Excellence in Cryptology II
[4] 2012年 Cryptographic Primitives and Hard Problems in Cryptography wiki
[5] 2015年论文《Cryptographic Assumptions: A Position Paper》