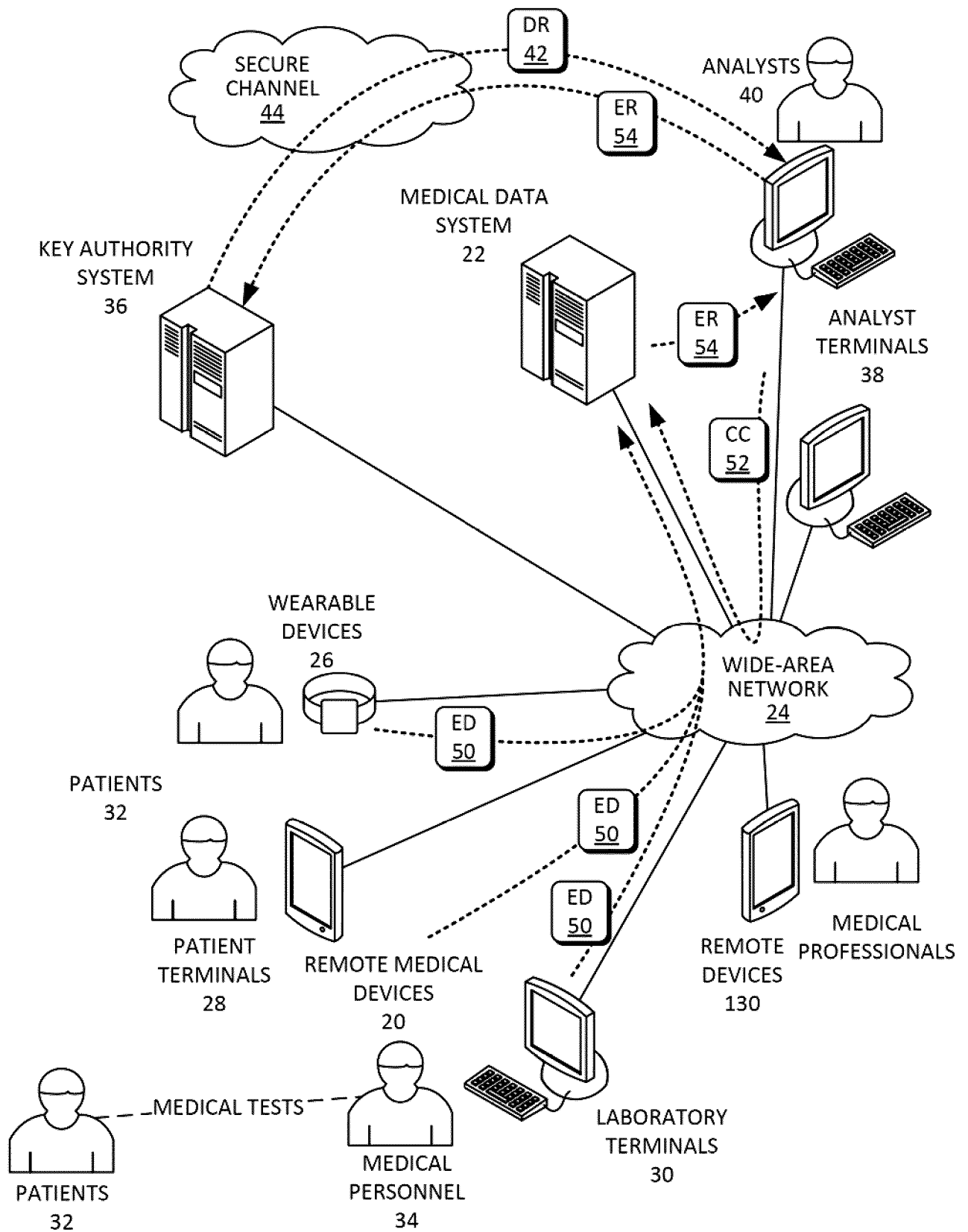
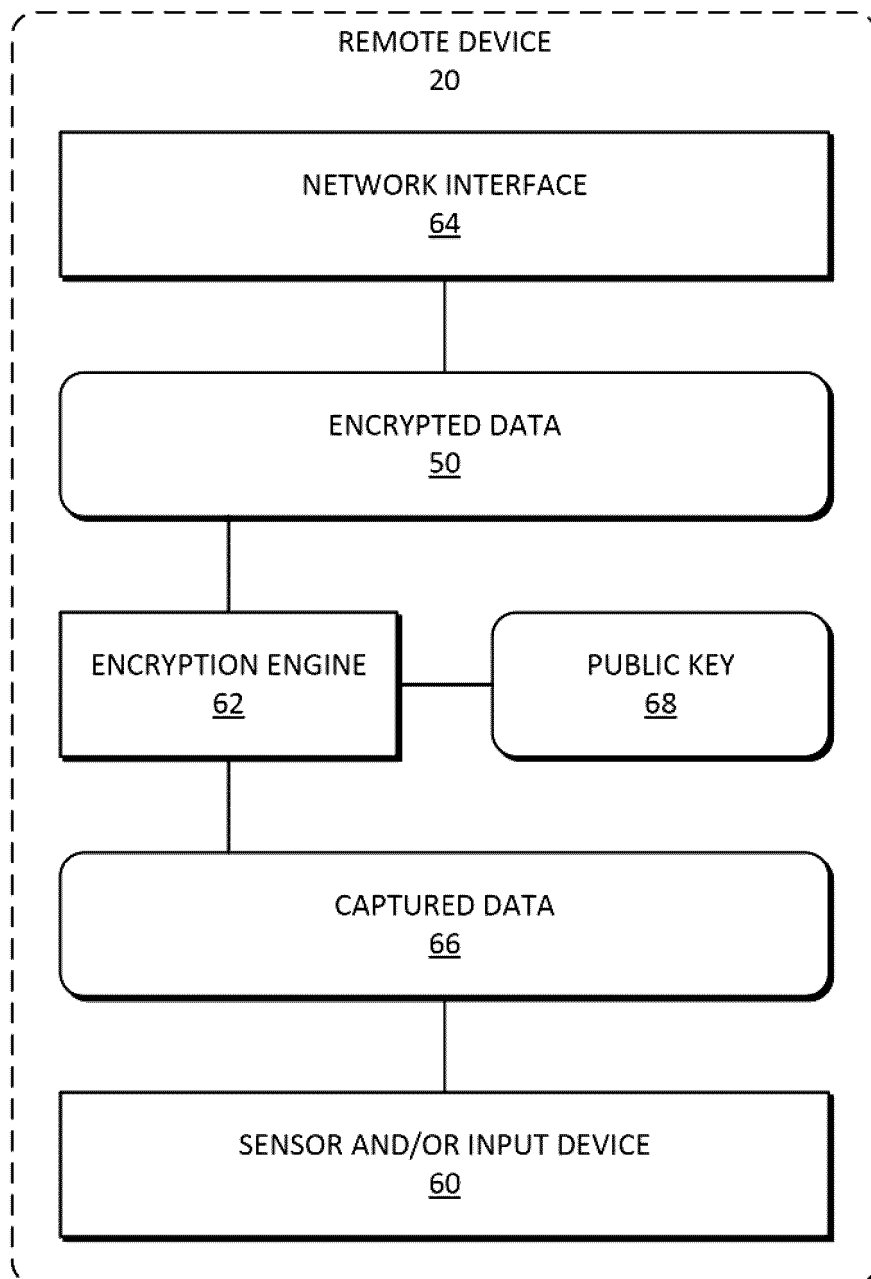


**FIG. 1**

**FIG. 2**

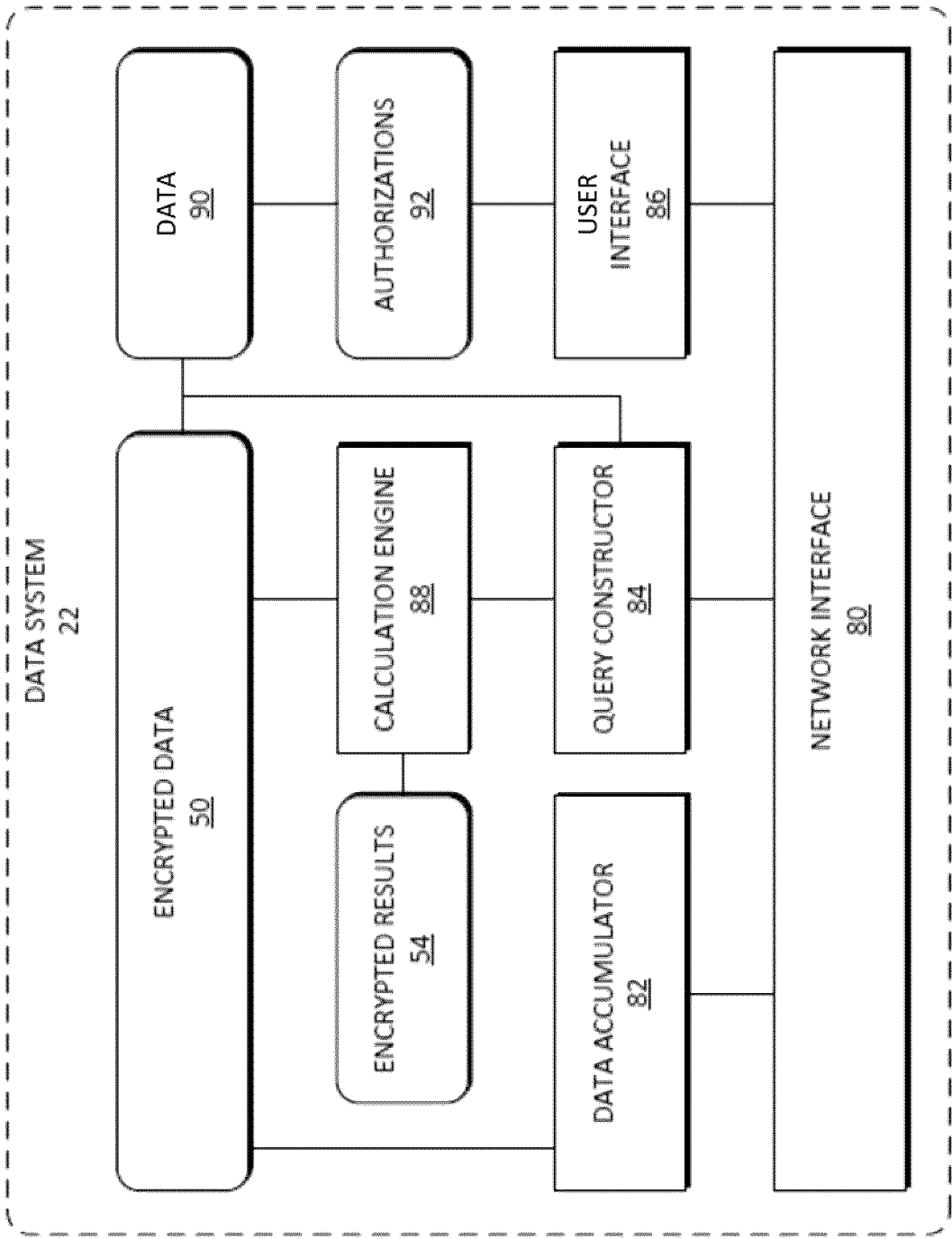
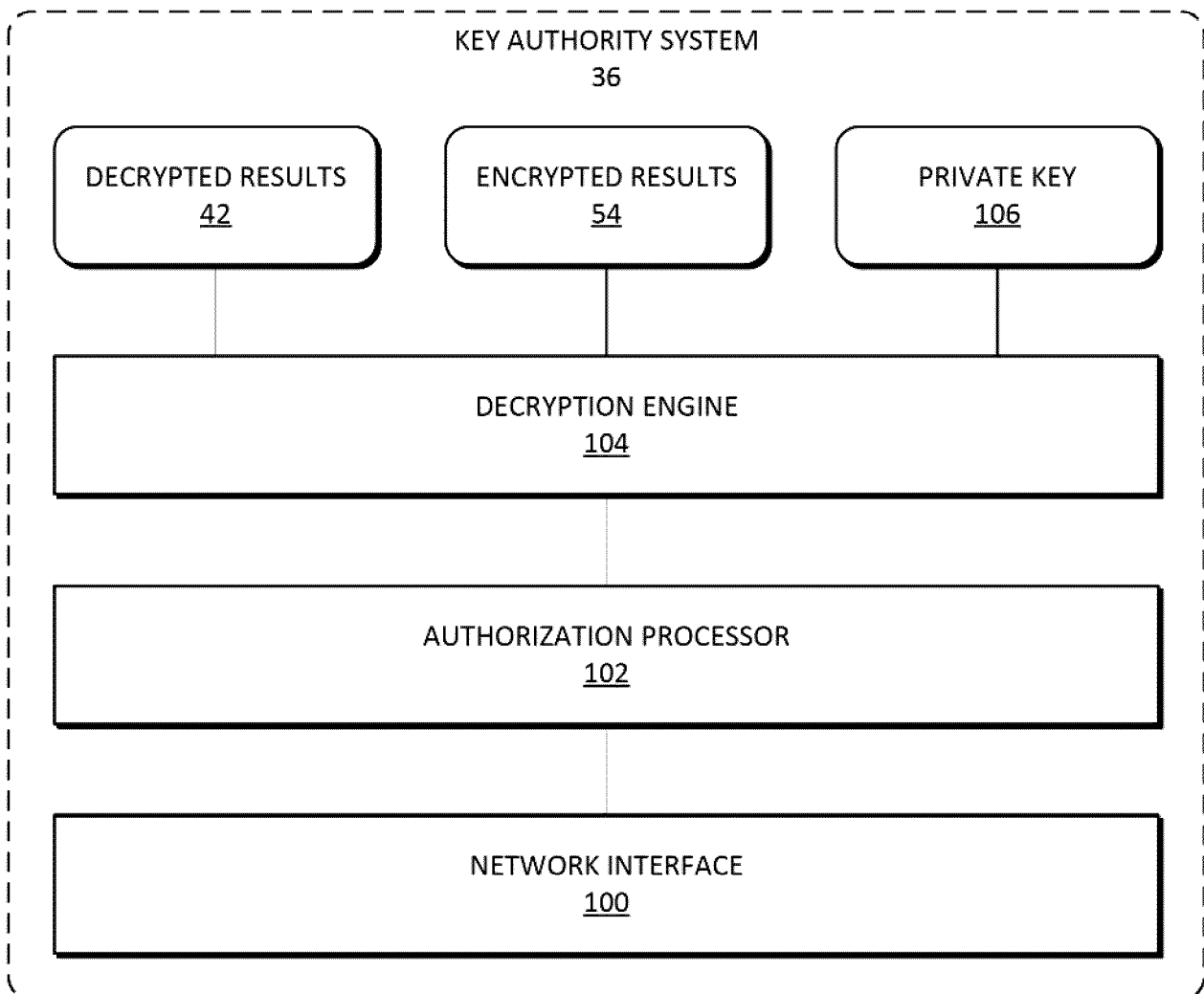


FIG. 3

**FIG. 4**

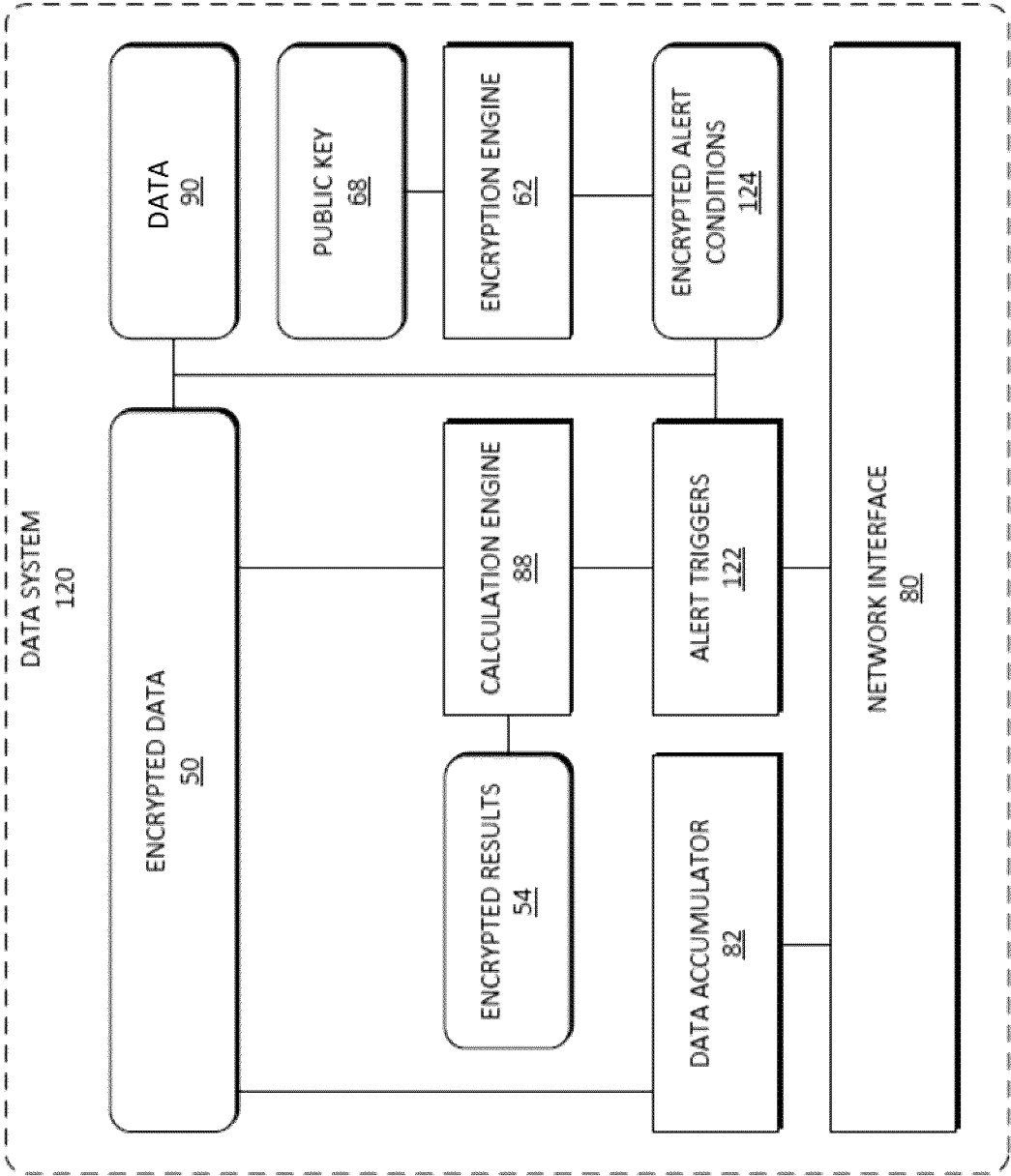


FIG. 5

$$\alpha_{y\ell \times y} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 2 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 2^\ell & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 2^\ell & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 2^\ell \end{pmatrix}$$

FIG. 6A

$$\text{pk} = h_{1 \times 1} = g_{1 \times 1} \cdot f_{1 \times 1}^{-1} \in R_q \quad \text{sk} = f_{1 \times 1} \in R_q$$

FIG. 6B

$$C_{\ell \times 1} = \mu \cdot \text{BDI}(I_{\ell \times \ell}) + S_{\ell \times 1} \cdot h_{1 \times 1} + E_{\ell \times 1}$$

FIG. 6C

$$\begin{aligned} \text{BD}(C) \cdot D \cdot f &= \text{BD}(C) \cdot (\mu_2 \cdot \text{BDI}(I) + S_2 \cdot h + E_2) \cdot f \\ &= \text{BD}(C) \cdot (\mu_2 \cdot \text{BDI}(I) \cdot f + S_2 \cdot g + E_2 \cdot f) \\ &= \mu_2 \cdot C \cdot f + \text{BD}(C) \cdot (S_2 \cdot g + E_2 \cdot f) \\ &= \mu_2 \cdot (\mu_1 \cdot \text{BDI}(I) \cdot f + S_1 \cdot g + E_1 \cdot f) \\ &\quad + \text{BD}(C) \cdot (S_2 \cdot g + E_2 \cdot f) \\ &= \mu_2 \cdot \mu_1 \cdot \text{BDI}(I) \cdot f + \mu_2 \cdot (S_1 \cdot g + E_1 \cdot f) \\ &\quad + \text{BD}(C) \cdot (S_2 \cdot g + E_2 \cdot f) \\ &= \mu_2 \cdot \mu_1 \cdot \text{BDI}(I) \cdot f + \mu_2 \cdot \text{error}_1 \\ &\quad + \text{BD}(C) \cdot \text{error}_2 \\ &= \mu_2 \cdot \mu_1 \cdot \text{BDI}(I) \cdot f + \text{error} \end{aligned}$$

FIG. 6E

$$\begin{aligned} C_{\ell \times 1} \cdot f_{1 \times 1} &= (\mu \cdot \text{BDI}(I_{\ell \times \ell}) \\ &\quad + S_{\ell \times 1} \cdot h_{1 \times 1} + E_{\ell \times 1}) \cdot f_{1 \times 1} \\ &= \mu \cdot \text{BDI}(I_{\ell \times \ell}) \cdot f_{1 \times 1} \\ &\quad + S_{\ell \times 1} \cdot h_{1 \times 1} \cdot f_{1 \times 1} + E_{\ell \times 1} \cdot f_{1 \times 1} \\ &= \mu \cdot \text{BDI}(I_{\ell \times \ell}) \cdot f_{1 \times 1} \\ &\quad + S_{\ell \times 1} \cdot g_{1 \times 1} + E_{\ell \times 1} \cdot f_{1 \times 1} \\ &= \mu \cdot \text{BDI}(I_{\ell \times \ell}) \cdot f_{1 \times 1} + \text{error} \end{aligned}$$

FIG. 6D

$$\text{error}_f(B, n, q) < q/2$$

FIG. 6F

$$n > \log q(\lambda + 110)/7.2$$

FIG. 6G

$$\begin{aligned} c_{AA} &= \text{Enc}(\text{gene} == AA) \\ c_{Aa} &= \text{Enc}(\text{gene} == Aa) \\ c_{aa} &= \text{Enc}(\text{gene} == aa) \end{aligned}$$

FIG. 6H

$$\begin{aligned} \alpha &= (4N_{AA}N_{aa} - N_{Aa}^2)^2 & \beta_1 &= 2(2N_{AA} + N_{Aa})^2 \\ \beta_2 &= (2N_{AA} + N_{Aa})(2N_{aa} + N_{Aa}) & \beta_3 &= 2(2N_{aa} + N_{Aa})^2 \end{aligned}$$

FIG. 6I

$$N_{AA} = \sum_i c_{AA}^{(i)} \qquad N_{Aa} = \sum_i c_{Aa}^{(i)}$$

FIG. 6J

Parameter	RLWE	Present Invention
λ		80
n		1024
ℓ		31
σ_k, σ_c		10
SK size		$n \times \ell = 3.968 \text{ K Bytes}$
PK size		$n \times \ell = 3.968 \text{ K Bytes}$
Ctxt size		$\ell \times n \times \ell = 123.008 \text{ K Bytes}$

FIG. 7

	AA	Aa	aa
Unaffected	z_{00}	z_{01}	z_{02}
Affected	z_{10}	z_{11}	z_{12}

FIG. 8

$$X^2 = \frac{\alpha}{2N} \left(\frac{1}{\beta_1} + \frac{1}{\beta_2} + \frac{1}{\beta_3} \right)$$

FIG. 6K

$$X^2 = \frac{\alpha}{\beta}$$
FIG. 6L

$$\alpha = N \left(\sum_{i=0}^2 w_i (N_{0i} R_1 - N_{1i} R_0) \right)^2$$

$$\beta = R_0 R_1 \left(\sum_{i=0}^2 w_i^2 C_i (N - C_i) - 2 w_1 w_2 C_1 C_2 \right)$$

$$N_{xy} = \sum_i z_{xy}^{(i)}, \quad \text{where } x \in \{0, 1\}, \quad y \in \{0, 1, 2\}$$

FIG. 6M

$$P(x) = \frac{e^x}{e^x - 1}$$

FIG. 6N

$$x = 0.072 \cdot a + 0.013 \cdot sys - 0.029 \cdot dia + 0.008 \cdot chol - 0.053 \cdot ht + 0.021 \cdot wt$$

FIG. 6O

$$P(x) = \frac{e^x}{e^x - 1} = \frac{1}{2} + \frac{1}{4}x - \frac{1}{48}x^3 + \frac{1}{480}x^5 - \frac{17}{80640}x^7 + O(x^9)$$

FIG. 6P

$$z = 72 \cdot a + 13 \cdot sys - 29 \cdot dia + 8 \cdot chol - 53 \cdot ht + 21 \cdot wt$$

FIG. 6Q

$$F(z) = 40320 + 20160z - 1680z^3 + 168z^5 - 17z^7$$

FIG. 6R

	AA	Aa	aa	Sum
Unaffected	N ₀₀	N ₀₁	N ₀₂	R ₀
Affected	N ₁₀	N ₁₁	N ₁₂	R ₁
Sum	C ₀	C ₁	C ₂	N

FIG. 9

$$z_0 = 0 \quad z_{i+1} = (1 - (a_i - b_i)^2)z_i + a_i(1 - b_i)$$

FIG. 6S

$$z_0 = 0, \quad z_{i+1} = \begin{cases} (1 - a_i)z_i + a_i & \text{if } b_i = 0 \\ a_i z_i & \text{if } b_i = 1 \end{cases}$$

FIG. 6T

Category	Systolic mm Hg	Diastolic mm Hg
Hypotension	< 90	< 60
Desired	90 – 119	60 – 79
Prehypertension	120 – 139	80 – 89
Stage 1 hypertension	140–159	90–99
Stage 2 hypertension	160–179	100–109
Hypertensive emergency	≥ 180	≥ 110

FIG. 10

Function 1: Secure Blood Pressure Classification

Input: Encrypted Blood Pressure Sys_Enc, Dia_Enc

Output: Blood Pressure Classification

Sys_Ref = [90, 120, 140, 160, 180]

Dia_Ref = [60, 80, 90, 100, 110]

For each number "i" in the reference lists {

 Res_Sys += Check_Greater(Sys_Enc, Sys_Ref[i]);

 Res_Dia += Check_Greater(Dia_Enc, Dia_Ref[i]);

}

Return Res_Sys and Res_Dia

FIG. 11

$$x_0 = b_0(1 - a_0) \qquad y_0 = c_0(1 - b_0) \qquad z_0 = 0$$

FIG. 6U

$$\begin{aligned} x_{i+1} &= (1 - (b_i - a_i)^2)x_i + b_i(1 - a_i) \\ y_{i+1} &= (1 - (c_i - b_i)^2)y_i + c_i(1 - b_i) \\ z_{i+1} &= (1 - (b_i - a_i)^2)(1 - (c_i - b_i)^2)z_i + (1 - (b_i - a_i)^2)c_i(1 - b_i)x_i \\ &\quad + (1 - (c_i - b_i)^2)b_i(1 - a_i)y_i \end{aligned}$$

FIG. 6V

$$\mu = \sum_{i=0}^l \mu_i \cdot 2^i$$

FIG. 6W

Item	Specification
CPU	Intel Core-i7 5930K
# of CPU Cores	4
# of Threads	8
CPU Frequency	3.5 GHz
Cache Size	15 MB
System Memory	32 GB DDR4
Operating System	Windows 8.1 64-bits
Programming IDE	Visual Studio 2012 Ultimate edition
GPU	NVIDIA GeForce GTX980
Maxwell Version	GM204
# of CUDA Cores	2048
GPU Core Frequency	1126 MHz
GPU Memory	4 GB
GPU L2 Cache	2 MB

FIG. 12

Operation	Present Invention		"Khedr 2014" (GPU) (msec)	GPU Speedup over "Khedr 2014" (Sec)	"Lbos 2014" (CPU) (Sec)	GPU Speedup over "Lbos 2014" (Sec)	"Lauter 2014" (CPU) (Sec)	GPU Speedup over "Lauter 2014" (Sec)
	(CPU) (msec)	(GPU) (msec)						
Encrypt	23	0.16	23	143×	0.58	3625×	0.78	4875×
Decrypt	5	1	5	5×	0.55	550×	0.74	740×
Add	0.25	0.07	0.2	2.85×	0.001	14.29×	0.003	42.86×
Multiply	87.8	0.838	3.477	4.15×	5.1	6085.92×	0.24	286.4×

FIG. 13

Application	This Work	"Lauter 2014"	Speedup over "Lauter 2014"	"Lbos 2014"	Speedup over "Lbos 2014"	"Cheon 2014"	Speedup over "Cheon 2014"
Pearson							
Goodness	8.452	1360	160.9×	NA	NA	NA	NA
-of-fit Test							
CAAT	22.28	3630	162.9×	NA	NA	NA	NA
Predictive analysis eqn. of FIG. 6Q	0.77	NA	NA	196	254.5×	NA	NA
Predictive analysis eqn. of FIG. 6R	13.69	NA	NA	80,000	5834.7×	NA	NA
Relational							
Operation	$t_1 = 2.514 \times k$	NA	NA	NA	NA	$t_2 = 30.75 \times k$	12.2×
Blood							
Pressure	$6 \times t_1$	NA	NA	NA	NA	$6 \times t_2$	12.2×

FIG. 14

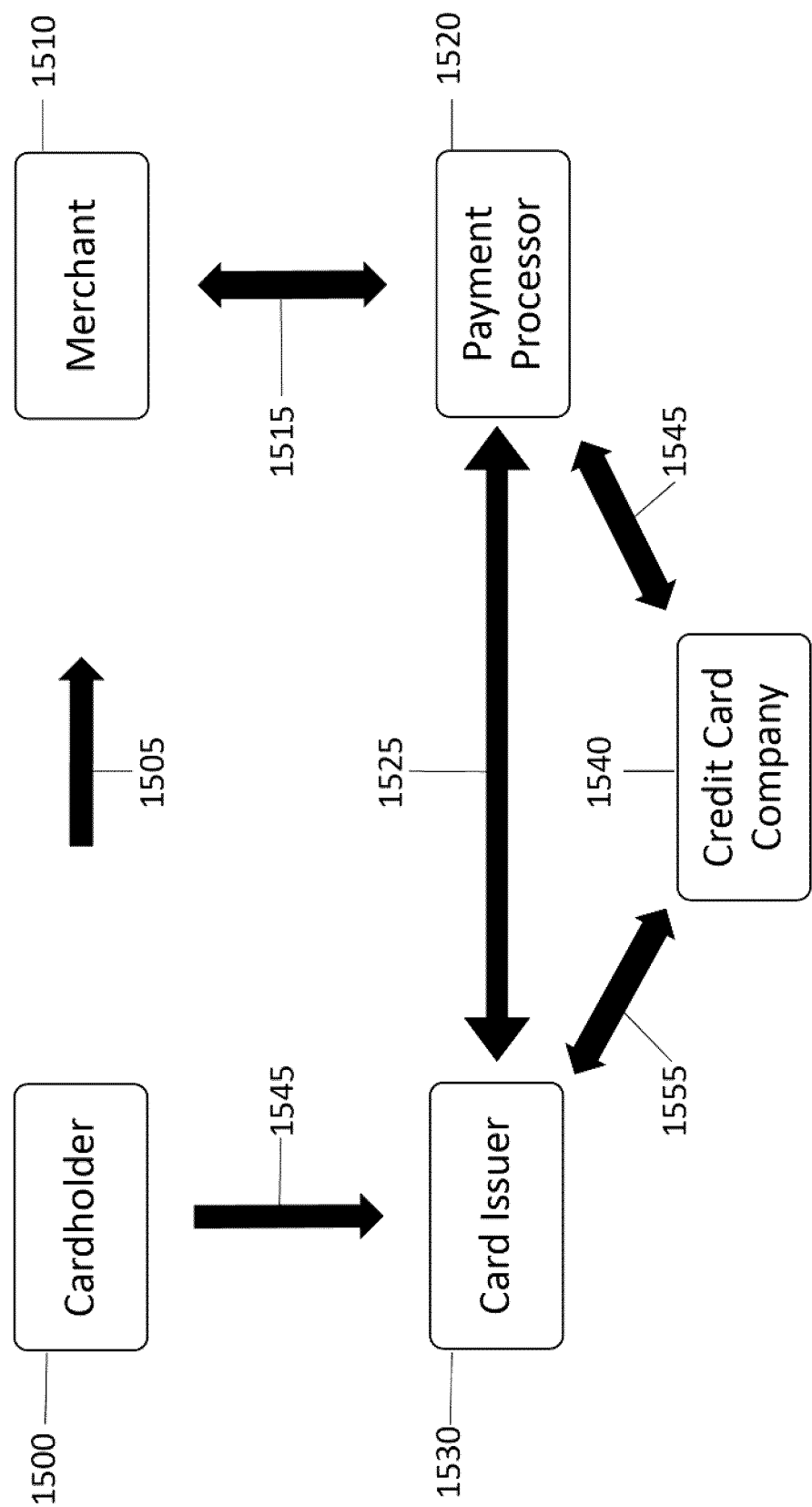


FIG. 15

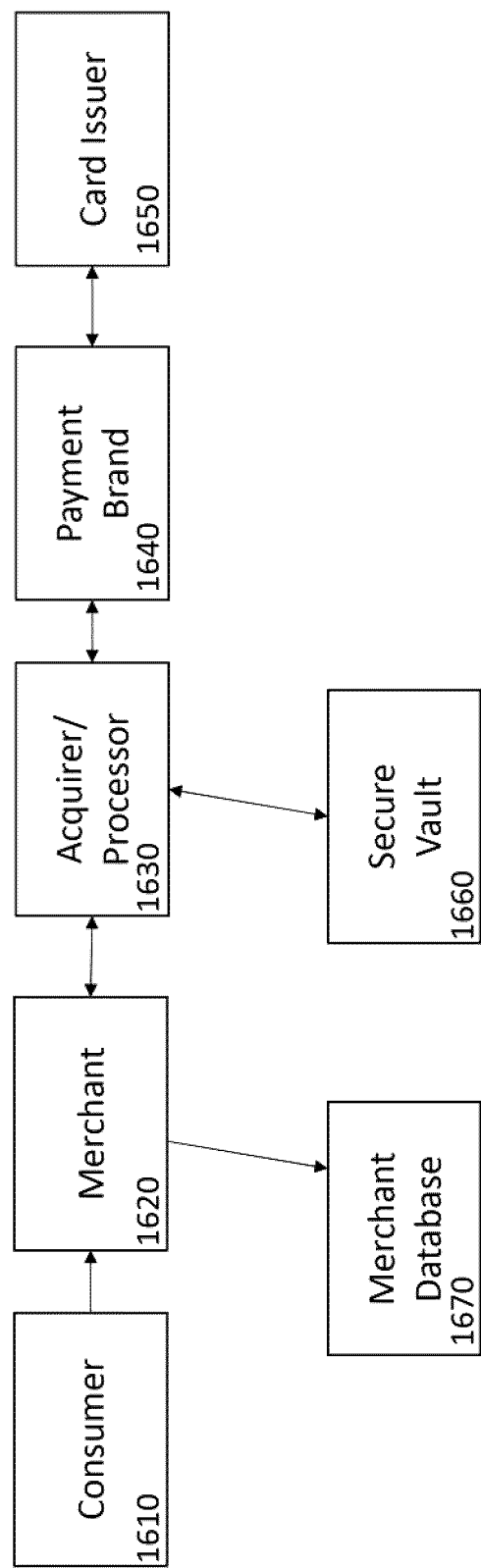


FIG. 16

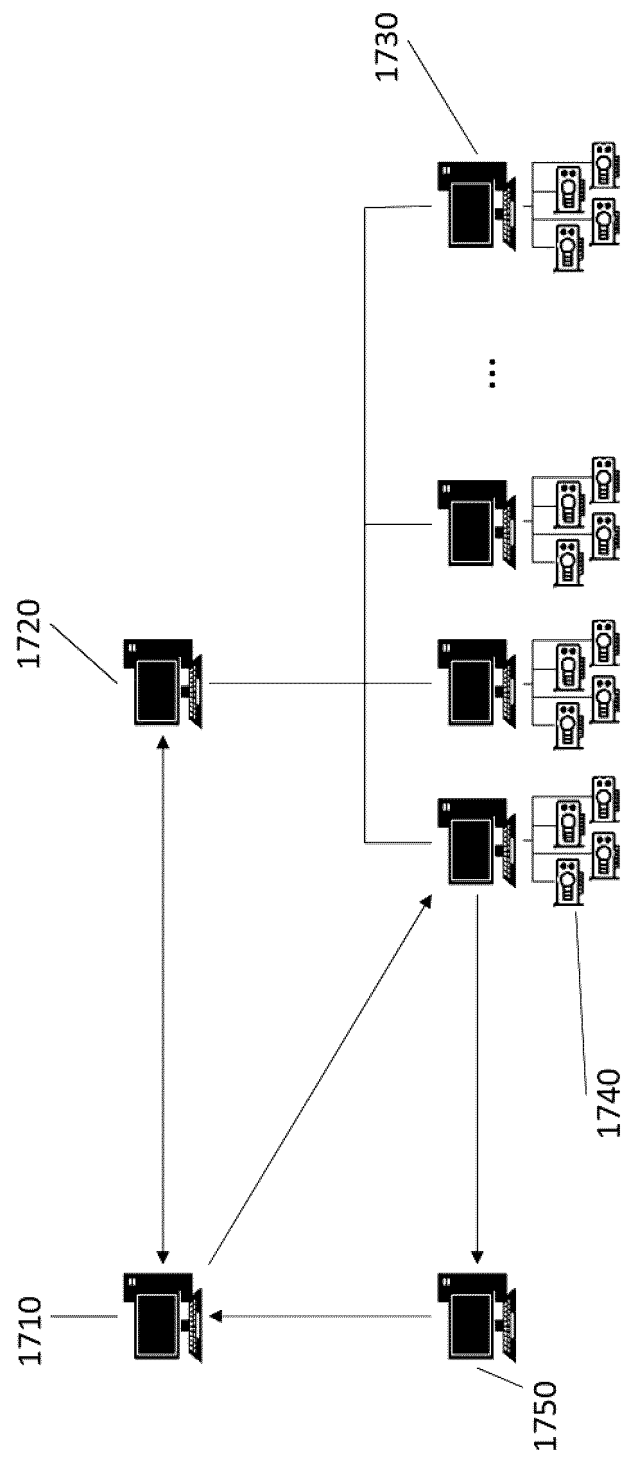


FIG. 17

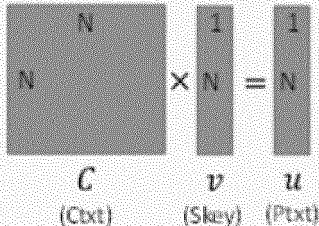
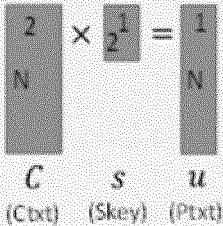
GSW Scheme	Present Invention
• Secret Key Size Reduction (Decryption Function)	
	

FIG. 18

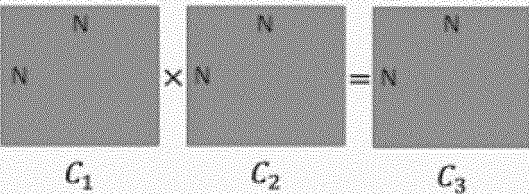
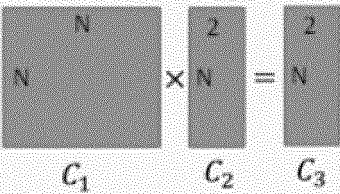
GSW Scheme	Present Invention
• Ctxt Size Reduction ($N = 2 \times \log(q)$)	
	
• Flatten Function Removal (Ctxt Operations)	
$C_{op} = Flatten(C_1 \times C_2)$	$C_{op} = C_1 \times C_2$

FIG. 19

Function : Multiply " v " Ciphertexts Function
Input: " v ", Ctxts: $C_1, C_2, \dots, C_v$
Output: C_{accum}
The multiplication result of " v " input Ctxts.
$C_{accum} = C_1$
For i from 2 to v {
$C_{accum} = C_{accum} \times C_i$
}
Return C_{accum}

FIG. 20

Parameter Selection and Keys/Ctxt Sizes.

Parameter	EXAMPLE SELECTION
λ	80
n	1024
ℓ	31
N	$2 \cdot \ell = 62$
σ_k, σ_c	10
SK size	$2 \times n \times \ell = 7.936 \text{ KBytes}$
PK size	$2 \times n \times \ell = 7.936 \text{ KBytes}$
Ctxt size	$N \times 2 \times n \times \ell = 492.032 \text{ KBytes}$

FIG. 21

$$A_{1 \times 2} \cdot s_{2 \times 1} = b - a \cdot t = e$$

FIG. 22a

$$C_{N \times 2} = \mu \cdot \text{BDI}(I_{N \times N}) + r_{N \times 1} \cdot A_{1 \times 2} + E_{N \times 2}$$

FIG. 22b

$$\begin{aligned} C_{N \times 2} \cdot s_{2 \times 1} &= (\mu \cdot \text{BDI}(I_{N \times N}) \\ &\quad + r_{N \times 1} \cdot A_{1 \times 2} + E_{N \times 2}) \cdot s_{2 \times 1} \\ &= \mu \cdot \text{BDI}(I_{N \times N}) \cdot s_{2 \times 1} \\ &\quad + r_{N \times 1} \cdot A_{1 \times 2} \cdot s_{2 \times 1} + E_{N \times 2} \cdot s_{2 \times 1} \\ &= \mu \cdot \text{BDI}(I_{N \times N}) \cdot s_{2 \times 1} \\ &\quad + r_{N \times 1} \cdot e + E_{N \times 2} \cdot s_{2 \times 1} \\ &= \mu \cdot \text{BDI}(I_{N \times N}) \cdot s_{2 \times 1} + \text{error} \end{aligned}$$

FIG. 22c

$$\begin{aligned} \text{BD}(C) \cdot D \cdot s &= \text{BD}(C) \cdot (\mu_2 \cdot \text{BDI}(I) + r_2 \cdot A + E_2) \cdot s \\ &= \text{BD}(C) \cdot (\mu_2 \cdot \text{BDI}(I) \cdot s + r_2 \cdot e + E_2 \cdot s) \\ &= \mu_2 \cdot C \cdot s + \text{BD}(C) \cdot (r_2 \cdot e + E_2 \cdot s) \\ &= \mu_2 \cdot (\mu_1 \cdot \text{BDI}(I) \cdot s + r_1 \cdot e + E_1 \cdot s) \\ &\quad + \text{BD}(C) \cdot (r_2 \cdot e + E_2 \cdot s) \\ &= \mu_2 \cdot \mu_1 \cdot \text{BDI}(I) \cdot s + \mu_2 \cdot (r_1 \cdot e + E_1 \cdot s) \\ &\quad + \text{BD}(C) \cdot (r_2 \cdot e + E_2 \cdot s) \\ &= \mu_2 \cdot \mu_1 \cdot \text{BDI}(I) \cdot s + \mu_2 \cdot \text{error}_1 \\ &\quad + \text{BD}(C) \cdot \text{error}_2 \\ &= \mu_2 \cdot \mu_1 \cdot \text{BDI}(I) \cdot s + \text{error} \end{aligned}$$

FIG. 22d

$$F(x_1, \dots, x_v) = \sum_{(y_1, \dots, y_v) \in S} \left(\prod_{i=1}^v \overline{(x_i \oplus y_i)} \right)$$

FIG. 22e

$$\text{error}_f(B, n, q) < q/2$$

FIG. 22f

$$n > \log q(\lambda + 110)/7.2$$

FIG. 22g