Multivariate-quadratic signatures

MQ-based identification scheme

Tanja Lange

Eindhoven University of Technology

SAC – Post-quantum cryptography

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.
Let $G = (g_1, g_2, \ldots, g_m)$. For

$$f_k(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(k)} x_i + 0$$

we see the linear terms cancel.

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.
Let $G = (g_1, g_2, \ldots, g_m)$. For

$$f_k(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(k)} x_i + 0$$

we see the linear terms cancel.

$$\begin{aligned} g_k(\mathbf{x}, \mathbf{y}) &= \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} (x_i + y_i)(x_j + y_j) \\ &\quad - \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} x_i x_j - \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} y_i y_j \\ &= \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} (x_i y_j + x_j y_i) \end{aligned}$$

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.
Let $G = (g_1, g_2, \ldots, g_m)$. For

$$f_k(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(k)} x_i + 0$$

we see the linear terms cancel.

$$\begin{aligned} g_k(\mathbf{x}, \mathbf{y}) &= \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} (x_i + y_i)(x_j + y_j) \\ &\quad - \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} x_i x_j - \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} y_i y_j \\ &= \sum_{1 \leq i \leq j \leq n} a_{i,j}^{(k)} (x_i y_j + x_j y_i) \end{aligned}$$

Thus $G(\mathbf{x} + \mathbf{z}, \mathbf{y}) = G(\mathbf{x}, \mathbf{y}) + G(\mathbf{z}, \mathbf{y})$, $G(\mathbf{x}, \mathbf{y} + \mathbf{z}) = G(\mathbf{x}, \mathbf{y}) + G(\mathbf{x}, \mathbf{z})$.

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.

- Prover picks $\mathbf{r}_0, \mathbf{t}_0 \in \mathbf{F}_q^n$, $\mathbf{e}_0 \in \mathbf{F}_q^m$, puts $\mathbf{r}_1 = \mathbf{s} - \mathbf{r}_0$
  Computes and sends $c_0 = H(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0), c_1 = H(\mathbf{r}_1, G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$.

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.

- Prover picks $\mathbf{r}_0, \mathbf{t}_0 \in \mathbf{F}_q^n$, $\mathbf{e}_0 \in \mathbf{F}_q^m$, puts $\mathbf{r}_1 = \mathbf{s} - \mathbf{r}_0$
  Computes and sends $c_0 = H(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0), c_1 = H(\mathbf{r}_1, G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$.
- Verifier picks and sends random $\alpha \in \mathbf{F}_q$. (First challenge).

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.

- Prover picks $\mathbf{r}_0, \mathbf{t}_0 \in \mathbf{F}_q^n$, $\mathbf{e}_0 \in \mathbf{F}_q^m$, puts $\mathbf{r}_1 = \mathbf{s} - \mathbf{r}_0$
  Computes and sends $c_0 = H(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0), c_1 = H(\mathbf{r}_1, G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$.
- Verifier picks and sends random $\alpha \in \mathbf{F}_q$. (First challenge).
- Prover computes and sends $\mathbf{t}_1 = \alpha\mathbf{r}_0 - \mathbf{t}_0, \mathbf{e}_1 = \alpha F(\mathbf{r}_0) - \mathbf{e}_0$.

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.

- Prover picks $\mathbf{r}_0, \mathbf{t}_0 \in \mathbf{F}_q^n$, $\mathbf{e}_0 \in \mathbf{F}_q^m$, puts $\mathbf{r}_1 = \mathbf{s} - \mathbf{r}_0$
  Computes and sends $c_0 = H(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0), c_1 = H(\mathbf{r}_1, G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$.
- Verifier picks and sends random $\alpha \in \mathbf{F}_q$. (First challenge).
- Prover computes and sends $\mathbf{t}_1 = \alpha\mathbf{r}_0 - \mathbf{t}_0, \mathbf{e}_1 = \alpha F(\mathbf{r}_0) - \mathbf{e}_0$.
- Verifier picks and sends random bit $b \in \{0, 1\}$, (Second challenge).

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.

- Prover picks $\mathbf{r}_0, \mathbf{t}_0 \in \mathbf{F}_q^n$, $\mathbf{e}_0 \in \mathbf{F}_q^m$, puts $\mathbf{r}_1 = \mathbf{s} - \mathbf{r}_0$
  Computes and sends $c_0 = H(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0), c_1 = H(\mathbf{r}_1, G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$.
- Verifier picks and sends random $\alpha \in \mathbf{F}_q$. (First challenge).
- Prover computes and sends $\mathbf{t}_1 = \alpha\mathbf{r}_0 - \mathbf{t}_0, \mathbf{e}_1 = \alpha F(\mathbf{r}_0) - \mathbf{e}_0$.
- Verifier picks and sends random bit $b \in \{0, 1\}$, (Second challenge).
- Prover sends $\mathbf{r} = \mathbf{r}_b$.

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.

- Prover picks $\mathbf{r}_0, \mathbf{t}_0 \in \mathbf{F}_q^n$, $\mathbf{e}_0 \in \mathbf{F}_q^m$, puts $\mathbf{r}_1 = \mathbf{s} - \mathbf{r}_0$
  Computes and sends $c_0 = H(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0), c_1 = H(\mathbf{r}_1, G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$.
- Verifier picks and sends random $\alpha \in \mathbf{F}_q$. (First challenge).
- Prover computes and sends $\mathbf{t}_1 = \alpha\mathbf{r}_0 - \mathbf{t}_0, \mathbf{e}_1 = \alpha F(\mathbf{r}_0) - \mathbf{e}_0$.
- Verifier picks and sends random bit $b \in \{0, 1\}$, (Second challenge).
- Prover sends $\mathbf{r} = \mathbf{r}_b$.
- For $b = 0$ the verifier checks $H(\mathbf{r}, \alpha\mathbf{r} - \mathbf{t}_1, \alpha F(\mathbf{r}) - \mathbf{e}_1)$ matches c_0.

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.

- Prover picks $\mathbf{r}_0, \mathbf{t}_0 \in \mathbf{F}_q^n$, $\mathbf{e}_0 \in \mathbf{F}_q^m$, puts $\mathbf{r}_1 = \mathbf{s} - \mathbf{r}_0$
  Computes and sends $c_0 = H(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0), c_1 = H(\mathbf{r}_1, G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$.
- Verifier picks and sends random $\alpha \in \mathbf{F}_q$. (First challenge).
- Prover computes and sends $\mathbf{t}_1 = \alpha\mathbf{r}_0 - \mathbf{t}_0, \mathbf{e}_1 = \alpha F(\mathbf{r}_0) - \mathbf{e}_0$.
- Verifier picks and sends random bit $b \in \{0, 1\}$, (Second challenge).
- Prover sends $\mathbf{r} = \mathbf{r}_b$.
- For $b = 0$ the verifier checks $H(\mathbf{r}, \alpha\mathbf{r} - \mathbf{t}_1, \alpha F(\mathbf{r}) - \mathbf{e}_1)$ matches c_0.
- For $b = 1$ the verifier checks
  $H(\mathbf{r}, \alpha(\mathbf{p} - F(\mathbf{r})) - G(\mathbf{t}_1, \mathbf{r}) - \mathbf{e}_1)$ matches c_1.

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.

- Prover picks $\mathbf{r}_0, \mathbf{t}_0 \in \mathbf{F}_q^n$, $\mathbf{e}_0 \in \mathbf{F}_q^m$, puts $\mathbf{r}_1 = \mathbf{s} - \mathbf{r}_0$
  Computes and sends $c_0 = H(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0), c_1 = H(\mathbf{r}_1, G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$.
- Verifier picks and sends random $\alpha \in \mathbf{F}_q$. (First challenge).
- Prover computes and sends $\mathbf{t}_1 = \alpha\mathbf{r}_0 - \mathbf{t}_0, \mathbf{e}_1 = \alpha F(\mathbf{r}_0) - \mathbf{e}_0$.
- Verifier picks and sends random bit $b \in \{0, 1\}$, (Second challenge).
- Prover sends $\mathbf{r} = \mathbf{r}_b$.
- For $b = 0$ the verifier checks $H(\mathbf{r}, \alpha\mathbf{r} - \mathbf{t}_1, \alpha F(\mathbf{r}) - \mathbf{e}_1)$ matches c_0.
- For $b = 1$ the verifier checks
  $H(\mathbf{r}, \alpha(\mathbf{p} - F(\mathbf{r})) - G(\mathbf{t}_1, \mathbf{r}) - \mathbf{e}_1)$ matches c_1.

Fiat-Shamir means that $H'(m)$ defines challenges α and b.

Sakumoto–Shirai–Hiwatari Identification scheme

Signer/prover picks random system F, secret $\mathbf{s}$, computes $F(\mathbf{s}) = \mathbf{p}$.

Public key: $(F, \mathbf{p})$. Private key: $\mathbf{s}$. Assume $c^{(k)} = 0$ for $1 \leq k \leq m$

Let $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})$. This is bilinear.

- Prover picks $\mathbf{r}_0, \mathbf{t}_0 \in \mathbf{F}_q^n$, $\mathbf{e}_0 \in \mathbf{F}_q^m$, puts $\mathbf{r}_1 = \mathbf{s} - \mathbf{r}_0$
  Computes and sends $c_0 = H(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0), c_1 = H(\mathbf{r}_1, G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$.
- Verifier picks and sends random $\alpha \in \mathbf{F}_q$. (First challenge).
- Prover computes and sends $\mathbf{t}_1 = \alpha\mathbf{r}_0 - \mathbf{t}_0, \mathbf{e}_1 = \alpha F(\mathbf{r}_0) - \mathbf{e}_0$.
- Verifier picks and sends random bit $b \in \{0, 1\}$, (Second challenge).
- Prover sends $\mathbf{r} = \mathbf{r}_b$.
- For $b = 0$ the verifier checks $H(\mathbf{r}, \alpha\mathbf{r} - \mathbf{t}_1, \alpha F(\mathbf{r}) - \mathbf{e}_1)$ matches c_0.
- For $b = 1$ the verifier checks
  $H(\mathbf{r}, \alpha(\mathbf{p} - F(\mathbf{r})) - G(\mathbf{t}_1, \mathbf{r}) - \mathbf{e}_1)$ matches c_1.

Fiat-Shamir means that $H'(m)$ defines challenges α and b.

Verification works for valid messages:

$$\alpha(\mathbf{p}-F(\mathbf{r}_1))-G(\mathbf{t}_1,\mathbf{r}_1)-\mathbf{e}_1 = \alpha(F(\mathbf{s})-F(\mathbf{r}_1))-G(\alpha\mathbf{r}_0-\mathbf{t}_0,\mathbf{r}_1)-\alpha F(\mathbf{r}_0)+\mathbf{e}_0$$

$$= \alpha(F(\mathbf{s}) - F(\mathbf{r}_1) - G(\mathbf{r}_0, \mathbf{r}_1) - F(\mathbf{r}_0)) + G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0 = G(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0$$